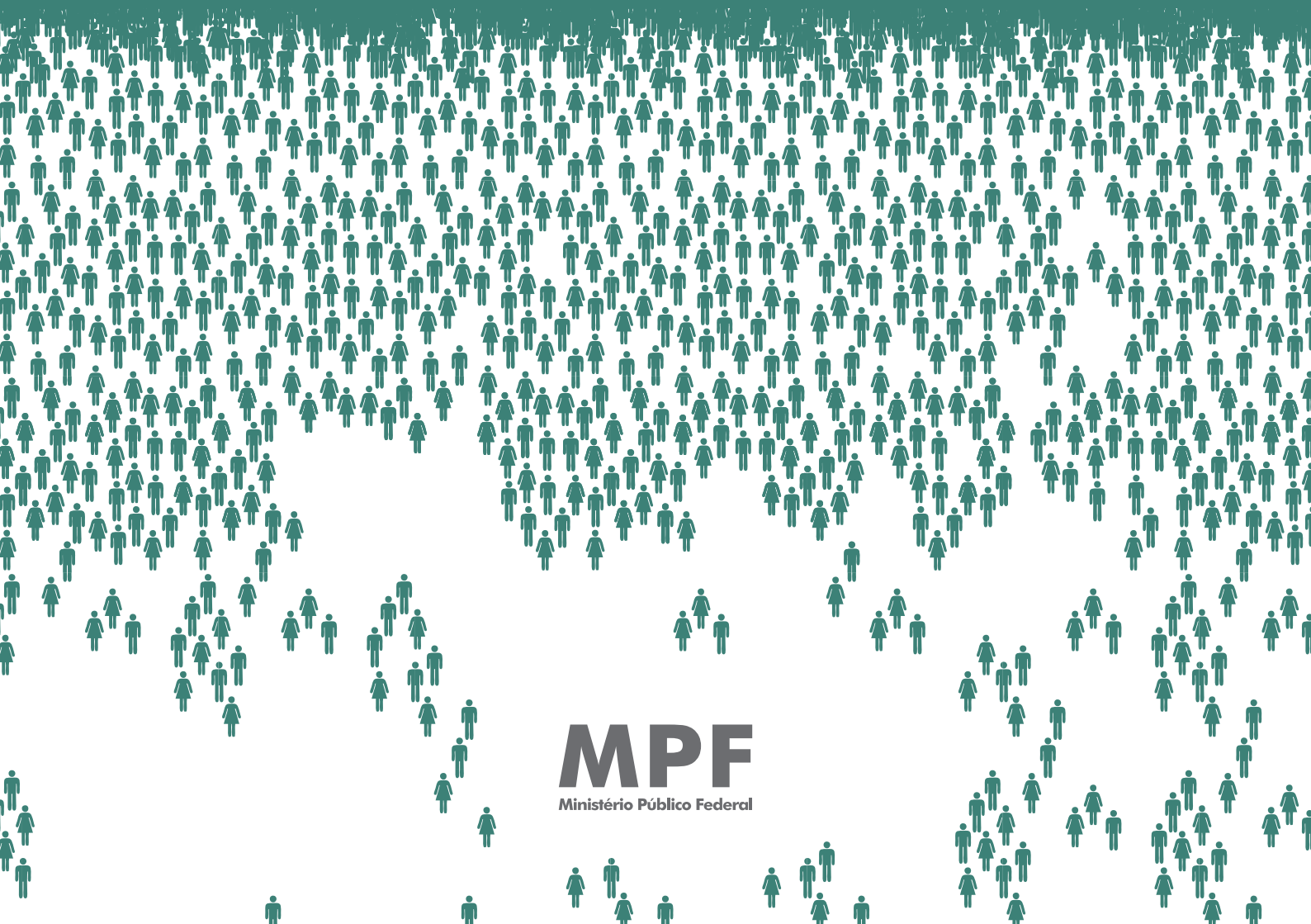
2ª CÁMARA DE COORDINACIÓN Y REVISIÓN

MATERIA CRIMINAL Y CONTROL EXTERNO DE LA ACTIVIDAD POLICIAL

MANUAL DE ACTUACÍON SOBRE DELITOS INFORMÁTICOS

2016



MPF

Ministério Público Federal

Ministerio Público Federal
2ª Cámara de Coordinación y Revisión

MANUAL DE ACTUACÍON SOBRE
DELITOS INFORMÁTICOS

MPF
Brasília-DF, Brasil
2016

Coordinación y Organización
2ª Cámara de Coordinación y Revisión

Ministerio Público Federal
2ª Cámara de Coordinación y Revisión - Materia Criminal y Control Externo de la Actividad Policial
SAF Sul, Quadra 4, Conjunto C
Teléfono (61) 3105-5100
70050-900 – Brasília-DF - Brasil
www.mpf.mp.br

CAPÍTULO 1
CONCEPTOS INTRODUCTORIOS

Diría, sin mucho rodeo
Al principio era el medio
Y el medio era bueno
Después es que vino el verbo
Un poco más lerdo
Que hizo todo mucho más difícil
Creó lo real, creó lo ficticio
Creó lo natural, creó el artificio
Creó el final, creó el inicio
El inicio que ahora acabó en eso
Luiz Tatit, en El Medio

1.1 Nombres y Números en la red

Comprender la forma como las computadoras son identificadas en Internet es requisito fundamental para el trabajo de investigación. Toda computadora en Internet posee un identificador único, que conocemos como dirección IP. IP es el acrónimo de Internet Protocol, o Protocolo de Internet en español. En términos técnicos, una dirección IP es un número entero de 32 bits[1], separado en cuatro porciones de 8 bits (también denominados octetos, o bytes) cada. A continuación aparece el ejemplo de una dirección IP de la manera como es interpretado por la computadora, en notación digital binaria simbolizada por 0s y 1s:

11001000 10001110 01001110 01011001

[1] Bit es una simplificación para el término "dígito binario" (Binary digit en inglés). Un bit es la menor unidad de información que puede ser almacenada o transmitida. El bit en la computación es representado por los valores 0 (cero) o 1 (uno), a pesar de que físicamente sea una carga eléctrica por debajo o por encima de un nivel estándar, generalmente almacenada en un capacitor dentro de un dispositivo de memoria. Ver http://pt.wikipedia.org.br/wiki/Bit para más detalles.

En el ejemplo anterior es evidente la inviabilidad de adoptar la base binaria en nuestro cotidiano. Sería muy difícil para las personas recordar una dirección como esta cada vez que necesite conectarse a una computadora en Internet. Sabemos sin embargo que los programas de computadora, de una manera general, realizan la conversión de los dígitos binarios para la base decimal, facilitando la comprensión y memorización por seres humanos. Veamos la misma dirección IP ilustrada anteriormente, ahora convertido para la base decimal, donde cada octeto pasa a ser separado por un punto:

11001000 10001110 01001110 01011001 – 200.142.78.89

Podemos concordar que la memorización en base decimal es menos dispendiosa, no obstante, cuatro porciones de dígitos en cualquier base aun no es la mejor manera de representar la dirección de una página en Internet. Por este y otro factores, surgió la necesidad de **atribuir nombres a los números**, o sea, de establecer un sistema en Internet que fuese capaz de traducir las direcciones IP (incluso representadas en base decimal) en nombres, conforme es ilustrado en la secuencia de conversiones siguientes:

11001000 10001110 01001110 01011001 – 200.142.78.89

11001000 10001110 01001110 01011001 – 200.142.78.89 – www.exemplo.com

En la sección 1.3 **Conceptos introductorios** veremos con más detalles como nació este sistema de traducción de números en nombres, como funciona, y por que es fundamental conocerlo para los propósitos de la investigación de crímenes en Internet.

1.2 Distribución de direcciones IP en Internet

La ubicación de direcciones IPs en Internet debe ser realizada de forma muy bien organizada, a fin de cuentas es necesario garantizar que cada uno de los millones de hosts[2] sea únicamente identificado en la red mundial de computadoras. En otras palabras, **no debe existir más de un host compartiendo la misma dirección IP en Internet**. Para este fin es adoptado un modelo jerárquico, para lo que una organización localizada en los Estados Unidos, denominada IANA (Internet Assigned Numbers Authority) o Autoridad para Atribución de Números de Internet , aparece en el nivel más alto de esta estructura.[3] La IANA asigna grandes bloques de direcciones IP para organizaciones conocidas como RIRs (Regional Internet Registries) o Registros Regionales de Internet , que a su vez asignan sub-bloques para los NIRs (National Internet Registries) o Registros Nacionales de Internet , para los LIRs (Local Internet Registries) o Registros Locales de Internet o directamente para grandes operadores de red y proveedores de acceso a Internet (también conocidos por ISPs - Internet Service Providers). Los ISPs finalmente son los responsables del suministro de IPs para las residencias, empresas y otras organizaciones menores, que en el lenguaje técnico son referidos como Sitios o Usuarios Finales.

[2] Un host es cualquier dispositivo conectado a una red. En general son computadoras personales, servidores de red y ruteadores. Todo host en Internet posee una dirección IP única y pública.
[3] Más detalles sobre esta y otras organizaciones que trabajan en el mantenimiento de la red son abordados en el capítulo 2

Tabla 1.1: Registros Regionales de Internet

Sigla	Nombre	Amplitud
ARIN	American Registry for Internet Numbers	Cañada, islas del Caribe, Atlántico Norte y Estados Unidos
RIPE NCC	Reseaux IP Europeens Network Coordination Centre	Europa y partes de Asia Central
APNIC	Asia-Pacific Network Information Centre	Región del Pacifico asiático
LACNIC	Latin America and Caribbean Internet Addresses Registry	America Latina y regiones del Caribe
AfriNIC	African Network Information Centre	África

Actualmente existen cinco RIRs en operación, conforme muestra la tabla 1.1. La figura 1.1 ilustra este modelo jerárquico de ubicación de direcciones involucrando las entidades aquí mencionadas. La IANA suministra además una tabla actualizada que informa cuales bloques de direcciones IP están asignados para cada RIR.[4]

[4] Disponible en http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space. xml

El sistema de registro de Internet: definiciones
Las definiciones siguientes están basadas en el capítulo 1 del documento Políticas Públicas de Administración de Recursos Internet en el área de América Latina y el Caribe del LACNIC[a].

IANA (Internet Assigned Number Authority): responsable de asignar parte del espacio global de dirección IPV4 y los números de sistemas autónomos a los Registros Regionales de acuerdo con las necesidades establecidas.

Registro de Internet (IR): una organización responsable de la asignación de espacios de direcciones IPV4 a sus miembros o clientes y del registro de esa distribución. Los IRs están clasificados de acuerdo con su función principal y alcance territorial.

Registro de Internet Regional (RIR): establecidos y autorizados por comunidades regionales respectivas, y reconocidos por la IANA para servir y representar grandes regiones geográficas. La función principal de un RIR es administrar y distribuir los recursos de Internet dentro de las respectivas regiones.

Registro de Internet Nacional (NIR): distribuye principalmente los recursos de Internet a sus miembros o constituyentes, los cuales son generalmente LIRs.

Registro de Internet Local (LIR): un IR que designa recursos de Internet a los usuarios de los servicios de red. Los LIRs son generalmente ISPs, cuyos clientes son principalmente usuarios finales o incluso otros ISPs.

Proveedor de Servicios de Internet (ISP): designa principalmente espacio de direcciones IPV4 a los usuarios finales de los servicios de red que proveen. Sus clientes pueden ser otros ISPs. Los ISP no tienen restricciones geográficas como los NIRs.

Sitio Final o Usuario Final (EU): definido como un usuario final (suscriptor) que tiene una relación de negocios o legal (misma entidad o entidades asociadas) con un proveedor de servicios de Internet.

[a] Disponible en http://lacnic.net/pt/politicas/manual2.html

Direcciones IP públicas, privadas y reservadas

No todas las combinaciones posibles de direcciones IP están disponibles para hosts en Internet. Computadoras que utilizan algunas clases de direcciones reservadas no pueden ser alcanzadas en la red mundial de computadoras. La tabla 1.2 ilustra algunas clases de IP reservados para redes privadas, consecuentemente no alcanzables en Internet.[5]

Figura 1.1: Estructura jerárquica de distribución de IPv4.
Fuente: http://lacnic.net

Tabla 1.2: Clases de direcciones IP para uso en redes privadas

Inicio	Fin	Nº de direcciones
10.0.0.0	10.255.255.255	16.777.216

172.16.0.0	172.31.255.255	1.048.576
192.168.0.0	192.168.255.255	65.536

[5] Note que, conforme informa el LACNIC: Cualquier organización puede usar estas direcciones IPv4 en sus redes privadas sin la necesidad de solicitarlos a algún Registro de Internet (http://lacnic.net/pt/politicas/manual3.html).

De un modo general, los internautas no están interesados en ser accedidos. Por tanto se hace innecesario poseer una dirección IP pública. Consecuentemente, algunos proveedores de acceso designan a sus clientes direcciones IP pertenecientes a las clases que listamos en la tabla 1.2, conocidos también como IP privados. Tal estrategia se viabiliza por medio de técnicas de mapeo de direcciones IP (NAT - Network Address Translation). De esta manera, con un único IP público es posible dar acceso a millares de computadoras dotados de IPs privados a Internet. La figura 1.2 ilustra el funcionamiento del NAT adoptado por un ISP que suministra acceso a la red para clientes residenciales.

Es oportuno listar aquí algunas implicaciones prácticas del uso de este recurso por parte de los proveedores de Internet:

- Internauta
- Encontrará dificultades si quiere utilizar su computadora para hospedar algún contenido o proveer algún servicio en Internet;
- Reduce la posibilidad de intrusiones por otros internautas a su computadora, una vez que su IP no es (inmediatamente) alcanzable en Internet.

• Proveedor de acceso
- Reduce costos con ubicación de direcciones IP públicas en Internet;
- Contribuye para desacelerar la escasez del IPv4 en Internet (Ver el tópico siguiente 1.2.1 para comprender esta situación.)

• Autoridades
- Pueden encontrar dificultades en las investigaciones, una vez que la violación de la confidencialidad telemática de un único IP público puede abarcar una diversidad de clientes del proveedor de acceso. Para contornear tal hecho, el proveedor debe almacenar los logs de sus usuarios, mapeando la dirección IP privada utilizada por cada cliente en cada conexión, de modo que sea posible localizarlo posteriormente.

Figura 1.2: Funcionamiento del sistema de traducción de direcciones (NAT). Fuente: GAO, Internet Protocol version 6, Federal Agencies Need to Plan for Transition and Manage Security Risks - http://www.gao.gov

1.2.1 IPv4 x IPv6

Normalmente mencionamos la sigla IP cuando en realidad queremos hablar sobre IPv4, que es la cuarta revisión del Internet Protocol, conforme como especificado en la RFC 7916. El hecho es que IPv4 representa la primera versión de este protocolo que fue ampliamente utilizada. No obstante, ya en etapa bastante avanzada está el desarrollo de su sexta revisión, el IPv6, a pesar de que aun es poco popular para clientes residenciales. Este esfuerzo fue motivado especialmente por el hecho de que la cantidad de

direcciones IPv4 disponibles inevitablemente se agotaría. Como vimos, una dirección IPv4 está compuesta por 32 bits, o sea, sería posible con este protocolo obtener 232 (4.294.967.296) combinaciones distintas. Sin embargo, vimos que hay rangos de direcciones reservadas para fines específicos, como los aproximadamente 18.000.000 reservados para redes privadas (y otros 270.000.000 para multicasting), reduciendo el número de direcciones disponibles para Internet. La previsión acerca de esta extracción se concretizó el 3 de febrero de 2011, cuando la IANA anunció una "nueva era en Internet:"[7]

> *El Registro de Direcciones de Internet para América Latina y el Caribe, LACNIC, comunica que las existencias centrales de direcciones IPv4 administrado por la IANA (Internet Assigned Numbers Authority) finalmente se han agotado, lo que desencadena el proceso irreversible de cambio del protocolo de Internet. Según la política global acordada por la comunidad de Internet en todas las regiones, hoy fueron entregados los últimos bloques disponibles de direcciones IPv4 correspondiendo uno para cada uno de los cinco Registros Regionales de Internet (RIR) en todo el mundo.*

[6] http://tools.ietf.org/html/rfc791
[7] http://lacnic.net/pt/anuncios/2011-agotamiento-ipv4.html

Por tanto es inevitable la migración de los servicios en Internet para IPv68. El IPv6 utiliza direcciones de 128 bits, soportando así un monto de 340 undecillones (2128) de combinaciones distintas, además de otras características que deben cambiar la forma como Internet es utilizada, viabilizando que los más diversos equipos se mantengan constantemente conectados en la gran red, como por ejemplo fogones, refrigeradores, cafeteras, lámparas, cámaras de vigilancia etc.[9]

Este proceso ha ocurrido gradualmente alrededor del mundo. En Brasil hay un proyecto bajo coordinación del Centro de Estudios e Investigaciones en Tecnología de Redes y Operaciones (CEPTRO.br) que tiene como objetivo auxiliar el avance en el país del IPv6.br. El siguiente fragmento resume bien sus objetivos:

> *Queremos, en este sitio Web, alertar a todos sobre la necesidad de la implantación del IPv6. Intentaremos, además de esto, suministrar herramientas que permitan una mejor comprensión de la cuestión y auxilien, de hecho, a la implantación. Las colaboraciones son bienvenidas e incentivadas en este espacio. ¡Algunos de los artículos son escritos por el equipo de NIC.br, pero usted puede también escribir sus artículos, presentar su case, o hacer comentarios en los artículos ya existentes! 10*

[8] Protocolo especificado en la RFC 2460: http://tools.ietf.org/html/rfc2460
[9] Más detalles en http://ipv6.br/IPV6/AyudaIPV6Usuario

El website de IPv6.br es una excelente fuente de recursos para aclarar dudas sobre este nuevo protocolo. Hay documentación disponible específica para usuarios finales, gestores, gobierno, ingenieros y proveedores de Internet.

1.3 El Sistema de Nombres de Dominios (DNS)

1.3.1 Breve historia del DNS

En la década de 1970, la red antecesora de Internet, ARPAnet (Advanced Research Projects Agency Network), mantenida por el Departamento de Defensa Norteamericano, poseía solamente algunas centenas de computadoras interconectadas. Para cada host (naturalmente identificado por un número, como vimos en la sección anterior) era atribuido un nombre, y así cada uno de estos hosts almacenaba una lista que relacionaba los nombres y respectivos números de todos los otros hosts de la red, conforme ilustrado en la figura 1.3:

Se un host cambiaba de nombre en la red, era necesario informar a una computadora central su nuevo nombre. Esta computadora reunía periódicamente todas las alteraciones de nombre en la red y ofrecía una o dos veces por semana la lista actualizada de hosts con sus respectivos nombres. Esta lista era un archivo en formato texto denominado HOSTS.TXT [11]

[10] http://www.ipv6.br

Figura 1.3: Estructura del precursor del DNS, el archivo hosts.txt de ARPANET

En la medida en que la red fue creciendo, fue insostenible mantener la lista de hosts actualizada y consistente utilizando el método original de distribución del archivo de texto HOSTS.TXT. El tráfico de red en el servidor que suministraba el archivo HOSTS.TXT era inmenso (pues el archivo siempre crecía a cada nuevo host en la red), y además había conflictos frecuentes de nombres (dos hosts con el mismo nombre). Los ingenieros coincidieron que era el momento de desarrollar un sistema descentralizado y más eficiente para el mantenimiento de esta lista de hosts en ARPAnet. El Sistema de Nombres de Dominios (DNS), como es conocido hoy, fue especificado e implementado para resolver este problema. Una referencia sobre este asunto puede ser encontrada en [Albitz 2001]. La especificación del DNS es descrita en la RFC 1035.[12]

[11] Se puede hacer analogía a una agenda telefónica, que a su vez relaciona nombres de personas con sus respectivos números. El archivo HOSTS.TXT era una agenda que relacionaba nombres de los hosts con sus respectivos identificadores numéricos en la red.

1.3.2 Qué es DNS

El Sistema de Nombre de Dominios es una base de datos distribuída en Internet. En una analogía, podemos afirmar que se trata del antiguo archivo HOSTS.TXT de ARPAnet, ahora suministrado simultáneamente por millones de hosts en Internet, de forma descentralizada y jerárquicamente organizada, distribuyendo entonces la responsabilidad de las actualizaciones, que en ARPAnet era de una única entidad (un único host). La figura 1.5 ilustra la estructura del DNS actual.

[12] http://www.faqs.org/rfcs/rfc1035.html

1.3.3 Organización jerárquica del DNS

Figura 1.4: Organización jerárquica del DNS

Buscándose viabilizar la distribución de las responsabilidades sobre la manutención de los nombres de los millones de hosts en Internet, un **modelo jerárquico** fue propuesto para el Sistema de Nombre de Dominios (DNS). Vienen de este modelo los conceptos de dominios, zonas y subdominios en Internet.

Podemos imaginar la estructura del DNS como un árbol, donde cada nivel de altura de este árbol es un **dominio** administrado por una organización diferente. Las hojas son los hosts y cada organización puede **delegar** la gestión de **zonas** o **subdominios** para otras organizaciones o departamentos internos de ella misma. La figura 1.4 ilustra esta estructura, con ejemplos reales de algunos dominios de Internet y respectivas instituciones responsables de su manutención. La leyenda a continuación es un guía para comprenderla mejor.

Comprendiendo la figura 1.4

• En la cima de la jerarquía del Sistema de Nombres de Dominios están los servidores raíz (root servers), aquellos que delegan autoridad directamente para las entidades que administran los TLDs Top Level Domains o Dominios de Primer Nivel. Los servidores raíz son mantenidos por 13 organizaciones que operan en diversos países, ofreciendo un alto grado de disponibilidad del servicio. La raíz (o sea, la representación del más alto nivel) de un nombre de dominio en Internet es representada por un . (punto, sin aspas). Veremos en el capítulo 2 Una Introducción a la Gobernanza de Internet que la ICANN (Internet Corporation for Assigned Names and Numbers) es responsable de la coordinación de las actividades de manutención de los servidores raíz y otros identificadores exclusivos en Internet.

• Debajo de los servidores raíz están los TLDs, que pueden ser un gTLD (generic TLD --- TLD genérico) o un ccTLD (country code TLD - TLD de país). El primero se refiere a dominios genéricos, como .com, .net, .org, .info y están compuestos necesariamente por más de dos letras. El segundo se refiere a dominios reservados para la identificación de países y poseen solamente dos letras que lo identifican, como por ejemplo .br (Brasil), .fr (Francia), .cn (China) etc.

• Debajo de los dominios .br, .gov y .mpf encontramos el subdominio .prsp, administrado por la Procuraduría de la República en el Estado de São Paulo.

• El nombre ciberneticos.prsp.mpf.gov.br es considerado un FQDN (Full Qualified Domain Name) o Dominio Completamente Expresado, pues él representa un (y solamente un) host en Internet. Note que su dirección es absoluta en el árbol jerárquico del Sistema de Nombres de Dominios, incluyendo desde el nombre del host (cibernéticos) hasta el dominio de primer nivel (br).

Resumiendo en pocas palabras la figura 1.4, podemos decir que el DNS está organizado de manera jerárquica, donde cada dominio es administrado por una organización, que a su vez delega subdominios para otras y así en adelante, distribuyendo las responsabilidades de mantenimiento entre ellas. Es importante notar también que fallas en el mantenimiento de un dominio no interfieren en el funcionamiento de aquellos jerárquicamente por encima, al paso que lo opuesto procede. Así, podemos inferir que

mientras más alto (o cerca de la raíz) sea un dominio de Internet, mayor es la responsabilidad en el mantenimiento. Conoceremos mejor en el capítulo 2 **Una Introducción a la Gobernanza de Internet** los actores que comparten las responsabilidades de estos recursos críticos de Internet.

1.3.4 Cómo funciona el DNS

Toda organización que posee un dominio en Internet debe también suministrar un servicio de traducción de nombres siguiendo las especificaciones del DNS. Esto ocurre porque la organización que es dueña del dominio será aquella que decidirá sobre los nombres de sus hosts y subdominios, de manera que estos sean fácilmente alcanzados en Internet. En la práctica, esto consiste en suministrar como mínimo dos hosts (conocidos como primario y secundario) conteniendo una lista que mapea nombres y números (direcciones IP) de los hosts referentes a su dominio. Estos dos hosts serán parte de la gran red de **servidores DNS** dentro de Internet.

Figura 1.5: Estructura general del Sistema de Nombre de Dominios. Fuente: Wikipedia, Domain Name System
http://en.wikipedia.org/wiki/Domain_Name_System

En nuestro ejemplo la ICANN delega el dominio .br para el Registro.br (que es el National Internet Registry brasileño), que delega el .gov.br para el gobierno federal, que delega el .mpf.gov.br para el Ministerio Público Federal. El MPF, a su vez, puede delegar para las Procuradurías sus respectivos subdominios, como en nuestro ejemplo es hecho para el .prsp.mpf.gov.br, dejado bajo responsabilidad de la Procuraduría de la República en el Estado de São Paulo.

Una consulta por mpf.gov.br en la base de datos WHOIS[13] del Registro.br certifica que el MPF ofrece dos servidores DNS en Internet.

[13] Ver 1.5.1 Conceptos introductorios

1	Servidor DNS:	agata.mpf.gov.br 200.142.58.18
2	status DNS:	17/01/2010 AA
3	último AA:	17/01/2010
4	Servidor DNS:	onix.mpf.gov.br 200.142.58.19
5	status DNS:	17/01/2010 AA
6	último AA:	17/01/2010
7	creado:	01/01/1996
8	modificado:	27/11/2008
9	status:	publicado

Las líneas 1 y 4 exhiben los hosts que sirven el DNS para el dominio mpf.gov.br. En caso que haya una falla en uno de ellos el otro asumirá automáticamente la responsabilidad del mapeo de los nombres. Las líneas 2 y 5 muestran que estos dos servidores DNS poseen autoridad (sigla AA) sobre el dominio consultado. O sea, fueron previamente autorizados por el dominio superior a ellos (.gov.br). Veremos como esto funciona en la práctica al interpretar los pasos ilustrados en la figura 1.6, que exhibe las etapas de conexión involucrando al Sistema de Nombre de Dominios en una conexión rutinaria a una página Web en Internet.

Figura 1.6: Funcionamiento del DNS

Comprendiendo la figura 1.6

1. El internauta intenta acceder al website del Ministerio Público Federal (http://www. mpf.gov. br). De forma transparente y automática, su sistema operativo intentará resolver [a] el nombre www.mpf.gov.br para que logre efectuar la conexión. Esto significa que su sistema operativo le preguntará al servidor DNS de su proveedor de acesso [b] cual es la dirección IP del host de nombre www.mpf.gov.br en Internet.

2. El servidor DNS del proveedor de acceso aun no conoce la dirección IP asociada a este nombre y no tiene idea de quien conoce. Ante la duda, él le pregunta a uno de los servidores DNS raíz (root servers).

3. El servidor DNS raíz posee en su lista solamente los Dominios de Primer Nivel (TLDs), por tanto no está apto para responder cual es la dirección IP del host www.mpf.gov.br. No obstante él sabe cual es el servidor DNS responsable del dominio .br y suministra esta información para el servidor DNS del proveedor de acceso.

4. El servidor DNS del proveedor le pregunta entonces al servidor DNS responsable del dominio .br. Este, como es de esperarse, tiene en su lista solamente las direcciones IP de los servidores de segundo nivel, o sea, aquellos debajo del .br.

5. El servidor DNS responsable del .br, mantenido por el Registro.br, informa cual es el servidor que responde por el dominio debajo del suyo, el .gov.br.

6. Con la respuesta anterior, el servidor DNS del proveedor le pregunta al .gov.br quien puede finalmente suministrar información sobre el .mpf.gov.br.

7. El servidor .gov.br busca en su lista y encuentra el servidor que puede suministrar esta información, y envía al servidor DNS del proveedor la dirección del mpf.gov.br.

8. El servidor DNS del proveedor contacta al mpf.gov.br y pregunta cuál es la dirección IP del hostwww.mpf.gov.br. El servidor DNS mpf.gov.br que es responsable de este subdominio tiene en su lista que la dirección IP de www.mpf.gov.br es 200.142.58.20.

9. El servidor DNS mpf.gov.br informa entonces esta dirección (200.142.58.20) para que el servidor DNS del proveedor realice su última consulta.

10. El servidor DNS del proveedor responde finalmente a la requisición del usuario, informando que la dirección www.mpf.gov.br que él quiere acceder tiene la dirección IP 200.142.58.20. En este momento la computadora del internauta estará apta para realizar la conexión con http:// www.mpf.gov.br. Se nota por tanto que quien necesita conocer la dirección IP es el sistema, y no el usuario — este es uno de los mayores beneficios de la utilización del DNS en Internet.

[a] En el lenguaje técnico, resolver un nombre significa descubrir la dirección IP de este nombre en la red a partir de una consulta en un sistema de resolución de nombres, que en Internet es el Sistema de Nombre de Dominios (DNS).
[b] Toda computadora personal posee una configuración de DNS . Generalmente el proveedor de acceso suministra dos direcciones IP que corresponden a los servidores primario y secundario.

1.4 Sistema Autónomo o Autonomous System (LAS)

Además de las direcciones IP y nombres de dominios, se hace presente un tercer componente importante - aunque poco popular - en la estructura compleja que compone a Internet. Se trata de los Sistemas Autónomos que, representados numéricamente, identifican únicamente redes menores dentro de la gran red mundial.

1.4.1 Internet como una red de dos niveles

Los datos que transitan en Internet son transferidos en pequeños fragmentos, que parten de un origen e intentan alcanzar su destino en la red. Sin embargo, antes de alcanzarlo, estos paquetes de datos encuentran en el camino una serie de equipos conocidos como ruteadores. De una manera general, los ruteadores indican cual es el mejor camino que los datos deben seguir a partir de aquel punto, buscando alcanzar su destino de forma eficiente (y considerando una serie de factores de orden técnico en el momento de la transmisión).

Ocurre que algunas organizaciones son tan grandes al punto de necesitar de una política de enrutamiento específica para sus redes internas (incluso siendo estas geográficamente distantes). Este escenario nos permite considerar que en Internet hay una arquitectura de enrutamiento de dos niveles. El primer nivel es formado por los ruteadores que conectan entre si a las computadoras localizados dentro de redes menores, que a su vez se conectan a Internet. Estos ruteadores en general guardan un mapa estático de la topología de la red a las cuales están localizadas y utilizan directrices apropiadas para el tratamiento del flujo de datos que en ellas transitan [14]. Es fácil inferir por tanto que dada la dimensión de Internet, protocolos de mejor camino estático como los vistos en el primer nivel no se adecuan a la complejidad de la gran red a nivel global. Se tiene así el segundo nivel en la jerarquía, donde están los ruteadores que interconectan las redes que componen la Internet. En este nivel, los ruteadores no conocen la estructura interna de cada red, pero guardan las informaciones necesarias para que los paquetes de datos alcancen los bordes de estas redes. Estas redes autónomas [15] que se interconectan en este segundo nivel son denominadas Sistemas Autónomos y no son identificadas a través de direcciones IP, sino por una secuencia numérica conocida como ASN (Autonomous System Number). El protocolo utilizado por estos ruteadores de borde es el BGPv4 (Border Gateway Protocol), descrito en la RFC 4271 [16]

1.4.2 Asignación de números AS en Internet

Así como ocurre con la distribución de direcciones IP, la IANA es la organización responsable de la administración de números AS en la cima de la jerarquía mencionada en el 1.2. Bloques de 1024 números son asignados para los RIRs (Regional Internet Registries) periódicamente. Por ejemplo, el Registro.br, actualmente clasificado como un NIR (National Internet Registre), administra los recursos de numeración de ASs en Brasil de acuerdo con la estructura jerárquica ilustrada en la figura 1.7. Los requisitos y

otros detalles sobre el proceso de asignación de direcciones IP y números AS en Brasil pueden ser consultados en el sitió Web de Registro.br[17].

[14] El protocolo de enrutamiento utilizado por estas redes son referenciados como IGP (Interior Gateway Protocol), este que a su vez implementa comúnmente uno de los siguientes protocolos: Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (ISIS) y Enhanced Interior Gateway Routing Protocol (EIGRP)
[15] Autónomas, en el sentido que en operan independientemente de las demás, administradas por políticas de enrutamiento interno propias y por una única entidad técnica/administrativa.
[16] http://tools.ietf.org/html/rfc4271

No existen muchas bases públicas que reúnan y ofrezcan informaciones de Sistemas Autónomos en Internet. Recomendamos la utilización de una extensión del navegador Firefox para este fin. Su utilización es gratuita y su código está disponible en el repositorio oficial de extensiones de Mozilla[18]. La figura 1.8 muestra el ASnumber 1.6 en funcionamiento y exhibiendo las informaciones de Sistema Autónomo referentes al local de hospedaje del sitio Web http://www. transparencia.org.br. Se nota que este posee la identificación AS4230 y pertenece a la red autónoma de la empresa Embratel. Otro recurso bastante útil para la verificación de Sistemas Autónomos es el servicio gratuito RobTex Swiss Army Knife Internet Tool[19], que suministra una interfaz de búsqueda, gráficos, relaciones entre ASs y otras funcionalidades, vía Web.

[17] http://registro.br/proveedor/numeracao/
[18] https://addons.mozilla.org/en-US/firefox/addon/asnumber/
[19] http://www.robtex.com

Figura 1.7: Jerarquía de los recursos de numeración de IPs y ASs (http://registro.br)

Figura 1.8: Extensión para el Firefox que exhibe datos de Sistema Autónomo

1.5 Recolectando informaciones en la red a partir de un IP o nombre de dominio

Los tópicos anteriores abordan cuestiones fundamentales al respecto de los nombres de dominio, números IP y ASs (sistemas autónomos) en la red mundial de computadoras. Suministran también un panorama acerca de la estructura y de las organizaciones que guían las decisiones y la manutención de Internet tal como ella es hoy [20]. En posesión de este conocimiento, proseguiremos con la exposición de las técnicas básicas de adquisición de datos en Internet por medio de los componentes tratados hasta aquí.

1.5.1 Utilizando el whois para consultar bases de datos WHOIS

En el 1.2 destacamos los cuidados necesarios para que una dirección IP sea únicamente identificada en la red mundial de computadoras. Vimos también un poco sobre la estructura organizacional que asegura, de forma jerárquica, la distribución de IPs y nombres de dominio en Internet. Veremos en este tópico más detalles acerca de las bases de datos públicas que son mantenidas por las organizaciones involucradas en este modelo de gobernanza (RIRs, NIRs, LIRs etc).

Para este tipo de base de datos se da el nombre de WHOIS. De una manera general, las bases WHOIS suministran informaciones de contacto de la persona (individuo o corporación) responsable del registro de un nombre de dominio o dirección IP en

Internet. O sea, podemos buscar en las bases WHOIS quien debe responder legalmente por una ocurrencia criminal en la red.

[20] Más detalles en el capítulo 2 Una Introducción a la Gobernanza de Internet

La herramienta más popular para la recogida de informaciones referentes a un nombre de dominio o dirección IP en Internet es whois. Sistemas GNU/Linux, MacOS y otros Unix en general poseen este software disponible en la instalación estándar. Los usuarios del sistema operativo Windows necesitan hacer el download del software[21].

El software whois realiza consultas en bases de datos WHOIS y exibe en la pantalla las informaciones de registro al respecto de una determinada dirección IP o nombre de dominio, como veremos a continuación.

1.5.2 Recolectando informaciones del "dueño" de un nombre de dominio

Una manera de comprender los campos de una base WHOIS es disecar cada una de las informaciones retornadas en una búsqueda dada. Como ejemplo, realizamos una consulta por el nombre de dominio wikipedia.org. Vea el resultado a continuación:

1	Domain ID:D51687756-LROR
2	Domain Name:WIKIPEDIA.ORG
3	Created On:13-Jan-2001 00:12:14 UTC
4	Last Updated On:08-Jun-2007 05:48:52 UTC
5	Expiration Date:13-Jan-2015 00:12:14 UTC
6	Sponsoring Registrar:GoDaddy.com, Inc. (R91-LROR)
7	Status: CLIENT DELETE PROHIBITED
8	Status: CLIENT RENEW PROHIBITED
9	Status: CLIENT TRANSFER PROHIBITED
10	Status: CLIENT UPDATE PROHIBITED
11	Registrant I D:GODA-09495921
12	Registrant Name: DNS Admin
13	Registrant Organization: Wikimedia Foundation, Inc.
14	Registrant Street1:P.O. Box 78350
15	Registrant Street2:
16	Registrant Street3:
17	Registrant City: San Francisco
18	Registrant State/Province: California
19	Registrant Postal Code:94107-8350
20	Registrant Country: US
21	Registrant Phone:+1.4158396885
22	Registrant Phone Ext.:
23	Registrant FAX:+1.4158820495
24	Registrant FAX Ext.:
25	Registrant Email:dns-admingwikimedia.org
26	Admin ID:GODA-29495921
27	Admin Name: DNS Admin
28	Admin Organization: Wikimedia Foundation, Inc.
29	Admin Street1:P.O. Box 78350

30	Admin Street2:
31	Admin Street3:
32	Admin City: San Francisco
33	Admin State/Province: California
34	Admin Postal Code:94107-8350
35	Admin Country: US
36	Admin Phone:+1.4158396885
37	Admin Phone Ext.:
38	Admin FAX:+1.4158820495
39	Admin FAX Ext.:
40	Admin Email:dns-admingwikimedia.org
41	Tech ID:GODA-19495921
42	Tech Name: DNS Admin
43	Tech Organization: Wikimedia Foundation, Inc.
44	Tech Streetl: P.O. Box 78350
45	Tech Street2:
46	Tech Street3:
47	Tech City: San Francisco
48	Tech State/Province: California
49	Tech Postal Code:94107-8350
50	Tech Country: US
51	Tech Phone:+1.4158396885
52	Tech Phone Ext.:
53	Tech FAX:+1.4158820495
54	Tech FAX Ext.:
55	Tech Email:dns-admingwikimedia.org
56	Name Server:NSO.WIKIMEDIA.ORG
57	Name Server:NS1.WIKIMEDIA.ORG
58	Name Server:NS2.WIKIMEDIA.ORG

[21] Puede ser encontrado en http://technet.microsoft.com/pt-br/sysinternals/bb897435.aspx

En este ejemplo tenemos una consulta en una base WHOIS que suministra informaciones del responsable del registro del dominio wikipedia.org. Las líneas 3, 4 y 5 suministran las fechas de creación, última actualización y expiración del dominio consultado respectivamente.

La línea 6 indica que el dominio fue registrado a través de la empresa GoDaddy.com, Inc, que debe ofrecer informaciones de contacto del cliente que registró el nombre de dominio en cuestión. En algunas ocasiones, la empresa de registro posee también informaciones privadas sobre el cliente, como datos de la tarjeta de crédito y otras que pueden ser solicitadas por la justicia.

En las líneas 11 a la 25 están las informaciones del dueño del dominio, que es la organización Wikimedia Foundation, Inc.. Es muy probable que en el caso de Wikipedia todas las informaciones retornadas en esta consulta sean verídicas. No obstante, la única información realmente confiable en este caso es la dirección de email publicada, una vez que este es el medio de contacto entre el dueño del registro (cliente

comprador del nombre de dominio) y la empresa de registro (empresa que vende el nombre de dominio).

Registry x Registrar x Registrant

Es importante familiarizarse con los términos técnicos utilizados para designar los diferentes papeles en el modelo de registro de nombres de dominios en Internet. A continuación aparece una lista con explicaciones de algunos términos populares en este asunto:

Registry: un Registry Operator, o simplemente Registry es una organización responsable de la base de datos de uno o más dominios de Internet del más alto nivel (TLDs). Estas organizaciones se localizan jerárquicamente debajo de la IANA (Internet Assigned Numbers Authority) y son responsables de la gestión de dominios como .com, .us, .org etc. Podemos decir que el Registry brasileño es el Registro.br, mientras que el Nominet UK es el Registry del Reino Unido.

Registrant: el cliente final. O sea, aquel individuo o entidad que tiene interés en ser dueño de un nombre de dominio, efectuando la compra, mediante el pago de una tasa anual, directamente con el Registry o por intermedio de un Registrar.

Registrar: un intermediario entre el registry y el registrant, que en general agrega otros servicios en la venta de dominios. En Brasil este servicio es ofrecido por algunos proveedores de Internet. Es importante enfatizar que, a pesar de que pueda haber diversos Registrars comercializando nombres de dominio bajo un mismo TLD, debe existir solamente un Registry autorizado por la IANA para gestionar la base de este TLD.

Algunas bases WHOIS suministran informaciones extras como los contactos técnicos y administrativos y servidores DNS asociados al dominio. En nuestro ejemplo estas informaciones están presentes en las líneas que comienzan con Admin, Tech y Name Server, respectivamente. No hay información nueva en los contactos técnico y administrativo, pero podemos notar que los tres servidores DNS que resuelven el nombre de dominio wikipedia.org poseen el nombre de dominio wikimedia.org. Podríamos por tanto inferir que existe una relación entre la Wikimedia Foundation, Inc. y el wikipedia.org incluso si las informaciones de contacto administrativo fuesen ocultadas. En algunos casos conocer esta relación entre dominios puede ser bastante útil para la investigación.

El software whois presente en el GNU/Linux intenta adivinar cual base de datos es más apropiada para ejecutar la consulta, por medio del dominio suministrado por el usuario. En caso que no lo logre, él envía la consulta para whois.arin.net, que es la base WHOIS de la ARIN (American Registry for Internet Numbers). Otros softwares pueden funcionar de manera diferente. Según [Jones 2006, pág. 24], el whois presente en el sistema operativo Mac OS X siempre consulta la base WHOIS de la ARIN, que si no es responsable de tal asignación, responde con una referencia con la dirección de otro RIR, para que la aplicación pueda repetir la búsqueda accediendo a la base WHOIS apropiada.

Veamos un ejemplo donde son consultadas informaciones de contacto acerca del registro del dominio wikipedia.org.br. Se nota que este está registrado en Brasil, por tanto asignado por el Registro.br:

1	% Copyright (c) Nic.br	
2	% La utilización de los datos siguientes está permitida solamente conforme	
3	% descrito en el Término de Uso (http://registro.br/término), siendo	
4	% prohibida su distribución, comercialización o reproducción,	
5	% en particular para fines publicitarios o propósitos	
6	% similares.	
7	% 2011-02-07 18:20:00 (BRST-02:00)	
8		
9	dominio:	wikipedia.org.br
10	entidad:	Alex Hubner
11	documento:	055.070.346/0001-58
12	responsable:	Alex Hubner
13	país:	BR
14	ID entidad:	AMH2
15	ID admin:	AMH2
16	ID técnico:	AMH2
17	ID cobro:	AMH2
18	servidor DNS:	ns01.domaincontrol.com
19	status DNS:	04/02/2011 AA
20	último AA:	04/02/2011
21	servidor DNS:	ns02.domaincontrol.com
22	status DNS:	04/02/2011 AA
23	último AA:	04/02/2011
24	creado:	19/06/2006 #2878615
25	expiración:	19/06/2011
26	modificado:	02/12/2010
27	status:	publicado
28		
29	ID:	AMH2
30	nombre:	Alex Hubner
31	e-mail:	alex@hubner.net.br
32	creado:	27/02/1998
33	modificado:	17/01/2011
34		
35	% Problemas de seguridad y spam también deben ser reportados al	
36	% cert.br, http://cert.br/, respectivamente para cert@cert.br	
37	% email-abuse@cert.br	
38	%	
39	% whois.registro.br acepta solamente consultas directas. Tipos de	
40	% consultas son: dominio (.br), ticket, proveedor, ID, bloque	
41	% CIDR, IP y ASN.	

Tenemos aquí un formato bien diferente de aquel exhibido en el ejemplo anterior. El NIR brasileño (Registro.br) ofrece además una interfaz de consulta online, donde el usuario puede obtener informaciones adicionales de contacto del dueño de dominio ---

las cuales no son exhibidas en las consultas realizadas a través de aplicaciones de terceros. En este caso será necesario pasar por un CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart), conforme ilustrado en la figura 1.9.[22].

A pesar de algunos esfuerzos, no hay una especificación formal que defina la estructura de las informaciones presentes en bases WHOIS. Veremos en algunos ejemplos como las respuestas de bases WHOIS mantenidas por diferentes organizaciones difieren unas de las otras. La ICANN determina que las informaciones en estas bases sean verídicas, sin embargo no obliga que sean estandarizadas, y ni siquiera que estén disponibles online en tiempo integral.

Ante la carencia de un estándar de registro en las bases WHOIS, se ve el surgimiento empresas que ofrecen una capa intermedia de consulta para que los resultados estén, como en el lenguaje técnico, en machine-readable format, o sea, en un formato que pueda ser interpretado sintéticamente por una computadora. La empresa Hexillion ofrece un producto denominado RegistryFusion^{T} M unified Whois para este propósito. En este caso, los datos consultados son retornados en formato estandarizado utilizando marcación XML.[23]

[22] Para más detalles sobre CAPTCHA, ver 3.8.1.1 Aspectos técnicos de la investigación

Figura 1.9: Opción de visualizar informaciones adicionales de WHOIS en el Registro.br

1.5.3 Recolectando informaciones del "dueño" de una dirección IP

Es posible también obtener informaciones de registro de una dirección IP, tal como ocurre para nombres de dominio. En las consultas anteriores sobre Wikipedia, identificamos los contactos de responsables del gTLD y del ccTLD brasileño [24] de este sitio Web. Sin embargo, aun no tenemos información sobre el local donde su contenido está hospedado. O mejor, donde la computadora que suministra Wikipedia está geográficamente localizada. En esta etapa la investigación por informaciones de registro de dirección IP es fundamental. Recordando que, al comprar un nombre de dominio, el individuo tiene libertad para asociarlo a cualquier dirección IP. Por tanto, **el nombre de dominio por si sólo nunca revela la localización geográfica de un sitio Web en Internet**. En nuestro caso, será necesario conocer la dirección IP asociada al nombre de dominio wikipedia.org. Utilizando el método descrito en el tópico 1.5.4 **Conceptos introductorios** verificamos que se trata del IP 208.80.152.2. Ejecutando entonces la búsqueda a través del software whois obtenemos el siguiente resultado (algunos campos de menor relevancia fueron omitidos):

1	NetRange:	208.80.152.0-208.80.155.255
2	CIDR:	208.80.152.0/22
3	OriginAS:	AS14907
4	NetName:	WIKIMEDIA
5	NetHandle:	NET-208-80-152-0-1
6	Parent:	NET-208-0-0-0-0
7	NetType:	Direct Assignment
8	NameServer:	NSO.WIKIMEDIA.ORG
9	NameServer:	NS2.WIKIMEDIA.ORG

10	NameServer:	NS1.WIKIMEDIA.ORG
11	Comment:	http://www.wikimediafoundation.org
12	Reg Date:	2007-07-23
13	Updated:	2007-07-23
14	Ref:	http://whois.arin. net/rest/net/
	NET-208-80-152-0-1	
15		
16	OrgName:	Wikimedia Foundation Inc.
17	Orgld:	WIKIM
18	Address:	149 New Montgomery Street
19	Address:	3rd Floor
20	City:	San Francisco
21	StateProv:	CA
22	PostalCode:	94105
23	Country:	US
24	Reg Date:	2006-05-30
25	Updated:	2009-12-28
26	Ref:	http://whois.arin.net/rest/org/
27	WIKIM	
28	OrgTechHandle:	RTA40-ARIN
29	OrgTechName:	Tarnell, River
30	OrgTechPhone:	+1-415-839-6885
31	OrgTechEmail:	river@wikimedia.org
32	OrgTechRef:	http://whois.arin.net/rest/poc/
	RTA40-ARIN	

[23] http://hexillion.com/whois/
[24] ver 1.3.3 Conceptos introductorios para comprender estas siglas

El primer bloque, representado por las líneas 1 a la 14, suministra informaciones sobre la red en que se encuentra la dirección IP consultado. Se ve aquí un AS (Sistema Autónomo) (ver 1.4 para más detalles) de número (AS Number) AS14907 (línea 3) e identificado por WIKIMEDIA (línea 4). Este AS abarca un rango de direcciones IP que incluye desde 208.80.152.0 a 208.80.155.255 (líneas 1-2). Esto significa un monto de 1022 direcciones asignadas exclusivamente para la red de la Wikimedia Foundation (línea 11). Las líneas 6 y 7 indican que la atribución de las direcciones IP fue realizada directamente con el RIR American Registry for Internet Numbers. El registro de este sistema autónomo fue efectuado el 23/07/2007 y no sufrió actualizaciones desde entonces (líneas 12-13).

El segundo bloque (líneas 16 a la 26) suministra informaciones de contacto de la institución responsable de la dirección IP consultada. Podemos decir que los campos en este bloque son de cierta forma intuitivos: nombre, dirección, fechas de registro y actualización de datos de la organización en la base del American Registry for Internet Numbers.

Las líneas 28 a la 32 exhiben informaciones del contacto técnico de la organización (Wikimedia Foundation), que a su vez es responsable de la dirección IP consultada.

Líneas posteriores a la 32 fueron omitidas. Estas suministraban solamente algunos contactos adicionales de Wikimedia.

1.5.4 Consultas en registros de DNS

Una herramienta bastante popular para la realización de consultas DNS en Internet es el dig (domain information groper). En sistemas Unix y similares este software es ofrecido en la instalación estándar. [25] El dig básicamente realiza preguntas a servidores DNS y exhibe sus respuestas. O sea, esta simple herramienta puede ayudar al investigador a reconocer una dirección IP a partir de un nombre de dominio o incluso un nombre de dominio a partir de un dado IP en algunas situaciones. A continuación algunos ejemplos:

```
1  $ dig wikileaks.ca
2
3  ; «» DiG 9.6-ESV-R3 «» wikileaks.ca
4  ;; global options: +cmd
5  ;; Got answer:
6  ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38113
7  ;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2
8
9  ;; QUESTION SECTION:
10 ;wikileaks.ca.  IN      A
11
12 ;; ANSWER SECTION:
13 wikileaks.ca. 238     IN A    213.251.145.96
14
15 ;; AUTHORITY SECTION:
16 wikileaks.ca. 7138    IN      NS      nsl2.zoneedit.com.
17 wikileaks.ca. 7138    IN      NS      ns9.zoneedit.com.
18
19 ;; ADDITIONAL SECTION:
20 ns9.zoneedit.com.     3060    IN A 66.240.231.42
21 nsl2.zoneedit.com.    3041    IN A 209.62.64.46
22
23 ;; Query time: 335 msec
24 ;; SERVER: 172.18.5.133#53(172.18.5.133)
25 ;; WHEN: Fri Feb      4 16:59:24 2011
26 ;; MSG SIZE  rcvd: 127
```

[25] En sistemas Debian GNU/Linux y derivados, el dig es parte del paquete dnsutils.

- 8-9: sección que reproduce la **pregunta** (consulta) enviada para el servidor
- 11-12: sección referente a la respuesta. En este caso, es lo que nos interesa. Verificamos que el nombre de dominio wikileaks.ca apunta para la dirección IP 213.251.145.96. Si no hubiere dirección IP mapeada para un dado nombre de dominio, esta sección será automáticamente omitida.
- 14-16: aquí están los servidores DNS con autoridad para responder por el nombre de dominio wikileaks.ca.

• 18-20: adicionalmente informan las direcciones IP de los servidores DNS responsables del mapeo del dominio wikileaks.ca.

El dig posee diversas opciones de consulta y formateo de las respuestas. Por ejemplo, ejecutando el mismo comando anterior con la opción +short, tenemos una respuesta (¡mucho!) más resumida:

1	$ dig wikileaks_ca 4-short
2	
3	213.251.145.96

A continuación aparece otro ejemplo. En este buscamos conocer algunas informaciones acerca de la estructura que hospeda el website de la Recaudación Federal de Brasil:

1	$ dig www.receita.fazenda.gov.br +noall +answer +authority
	+comments
2	
3	; <c» DiG 9.6-ESV-R3 «» www.receita.fazenda.gov.br
	+noall +answer [...]
4	;; global options: +cmd
5	;; Got answer:
6	;; -»HEADER«- opcode: QUERY, status: NOERROR, id: 46336
7	;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 0
8	
9	;;ANSWER SECTION:
10	www.receita.fazenda.gov.br. 21554 IN A
	161.148.231.100
11	
12	;; AUTHORITY SECTION:
13	receita.fazenda.gov.br. 21554 IN NS antares.serpro. gov.br.
14	receita.fazenda.gov.br. 21554 IN NS centauro.serpro.gov.br.
15	receita.fazenda.gov.br. 21554 IN NS andromeda.serpro.gov.br.
16	receita.fazenda.gov.br. 21554 IN NS canisvenatici.serpro.gov.br.
17	receita.fazenda.gov.br. 21554 IN NS trifid.serpro.gov.br.

Notamos en la línea número 10 que la dirección IP correspondiente a www.receita.fazenda.gov.br es 161.148.231.100. Se ve también que cinco servidores poseen autoridad para responder requisiciones referentes al dominio consultado. Estos forman parte de la infraestructura del SERPRO (Servicio Federal de Procesamiento de Datos). El monto de servidores disponibles (cinco) representa una forma de amenizar impactos de eventuales fallas por medio de redundancia de los servicios. O sea, aunque cuatro servidores DNS estén indisponibles por alguna razón, habría un último respondiendo las requisiciones, garantizando que el sitio Web de la Recaudación Federal permaneciese accesible.

Además podemos intentar descubrir si hay más servicios de Internet hospedados en la misma dirección IP que hospeda el sitio Web de la Recaudación Federal. El dig nos permite consultar nombres de dominios asociados a direcciones IP (observe la opción -x suministrada en el comando a continuación). En el lenguaje técnico, esta sería una consulta de **DNS reverso**:

1	$ dig -x 161.148.231.100 +short
2	
3	www.rfb.fazenda.gov.br.
4	www.receita.fazenda.gov.br.
5	ftp.receita.fazenda.gov.br.

Note que la respuesta anterior exhibe más dos nombres de dominio asociados a la dirección IP consultada. Este ejemplo demuestra que las consultas DNS pueden ser un medio eficiente para recolectar informaciones importantes en una investigación. En nuestro caso, fue posible verificar la relación entre organizaciones y servicios distintos a partir de una única dirección IP. Vale resaltar que todas estas informaciones son públicas y son obtenidas de manera no intrusiva. Los únicos requisitos para conocerlas y correlacionarlas son (1) la comprensión básica del asunto y (2) las herramientas necesarias para las consultas, que son libres y gratuitas.

Para comprender más profundamente los detalles técnicos que guían la estructura del DNS, recomendamos la lectura de [Albitz 2001].

1.5.5 Utilizando el traceroute para consultar el camino entre dos hosts

Considere una situación en que buscamos informaciones acerca de la dirección IP 200.169.117.22. Una consulta DNS utilizando la herramienta dig, siguiendo las instrucciones del tópico anterior, nos retorna lo siguiente:

1	$ dig -x 200 .169 .117.22 +short
2	
3	200-169-117-22. claro.net.br.

Ya podemos por tanto inferir cual es el proveedor de acceso responsable por la designación de esta dirección IP. Una consulta en la base WHOIS nos suministra además las siguientes informaciones:

1	% Copyright (c) Nic.br	
2	%La utilización de los datos siguientes es permitida solamente conforme	
3	%descrito en el Término de Uso (http://registro.br/término), siendo	
4	% prohibida su distribución, comercialización o reproducción,	
5	I%en particular para fines publicitarios o propósitos	
6	%similares.	
7	%2011-02-04 20:40:32 (BRST -02:00)	
8		
9	inetnum:	200.169.112/20
10	asn:	AS22085
11	ID abusos:	CLV199

12	entidad:	Claro S/A
13	documento:	040.432.544/0001-47
14	responsable:	BCP SA
15	dirección:	Rua Florida, 1970, 4o. andar
16	dirección:	04565-001 - Sao Paulo - SP
17	país:	BR
18	teléfono:	(11) 94156955 [97632]
19	ID entidad:	CLV199
20	ID técnico:	CLV199
21	inetrev:	200.169.117/24
22	servidor DNS:	ns01.claro.net.br

```
23  status DNS:    02/02/2011 AA
24  último AA:     02/02/2011
25  servidor DNS:  ns02.claro.net.br
26  status DNS:    02/02/2011 AA
27  último AA:     02/02/2011
28  servidor DNS:  ns03.claro.net.br
29  status DNS:    02/02/2011 AA
30  último AA:     02/02/2011
31  servidor DNS:  ns04.claro.net.br
32  status DNS:    02/02/2011 AA
33  último AA:     02/02/2011
34  creado:07/08/2001
35  modificado:    30/09/2008
36
37  ID:      CLV1 99
38  nombre:        CLaro - Voz/Dados
39  e-mail:  ContatoRegistro@claro.com.br
40  creado:21/03/2006
41  modificado:    14/07/2008
42
43  % Problemas de seguridad y spam también deben ser reportados al
44  % cert.br, http://cert.br/, respectivamente para cert@cert.br % e
45  abuse@cert.br
46
47  % whois.registro.br acepta solamente consultas directas. Tipos de
48  % consultas son: dominio (.br), ticket, provedor, ID, bloque
49  % CIDR, IP eASN.
```

Además de las informaciones de contacto de la persona jurídica que aparece en la respuesta de la base WHOIS del Registro.br, la línea 38 nos ofrece otro dato importante. **CLaro - Voz/Datos** es dato suficiente para inferir que la dirección IP consultada pertenece a la estructura de voz y datos de la empresa, y por tanto puede haber sido utilizado por un aparato móvil con conexión a Internet 2.5G o 3G (ver 1.7.6 para conocer más sobre estos tipos de acceso). Esta suposición puede ganar fuerza después de una consulta que exhibimos a continuación, utilizando la herramienta traceroute:

```
1  $       traceroute      200.169.117.22
2  traceroute to 200.169.117.22 (200.169.117.22), 30 hops max
3  1       10.1.1.1        (10.1.1.1)
```

4	2	dsldevice.Ian (192.168.1.254)
5	3	* * *
6	4	201-0-93-225.dsl.telesp.net.br (201.0.93.225)
7	5	201-0-5-121.dsl.telesp.net.br (201.0.5.121)
8	6	200-100-98-81.dial-up.telesp.net.br (200.100.98.81)
9	7	213.140.50.69 (213.140.50.69)
10	8	Xe5-1-1-0-grtmiabr3.red.telefonica-wholesale.net
	(84.16.15.46)	
11	9	So7-0-0-0-grtmiana3. red .telefon ica-wholesale .net
	(213.140.37.65)	
12	10	CLAROBRASIL-2-1-2-0-grtmiana3.red.telefonica-wholesale. net.10.16.84...
13	11	* * *
14	12	
15	13	* * *
16	14	201-23-188-98.gprs.claro.net.br (201.23.188.98)
17	15	* * *
18	[- - -]	

Como el propio nombre lo indica, traceroute camina por los ruteadores presentes entre el origen (local donde el traceroute es ejecutado) y el destino consultado. Para cada equipo, el software intenta recolectar algunas informaciones, como el tiempo de respuesta (omitido en el ejemplo) y el nombre de dominio asociado a él.[26] Tales informaciones, cuando están disponibles, son exhibidas en orden temporal. En el ejemplo anterior, las líneas 1 y 2 indican las direcciones IP de la red por la cual se dio el origen de la consulta. Se nota en las líneas 4, 5 y 6 que Telesp es el proveedor que suministra acceso a Internet para esta red. La línea 7 es un ejemplo de ruteador que no posee (o al menos no suministró) un nombre de dominio asociado. Las líneas 8, 9 y 10 parecen indicar la entrada del paquete en la estructura de red proveedor de acceso de la dirección IP de destino. Se nota especialmente en la línea 10 la indicación de un equipamiento que conecta la red de Telefónica International Wholesale Services y de Claro Brasil. Finalmente, al llegar a la línea 14, tendremos finalmente una fuerte evidencia de que la dirección IP de destino está asignada para una red GPRS (2.5G) de la operadora Claro, y que el aparato que fue utilizado en el evento que estamos rastreando se conectó a partir de una ERB (estación radio-base) localizada en un área de cobertura en que la empresa Telefónica opera.

[26] Técnicamente hablando, él utiliza el campo ttl (time to live) del protocolo IP para inducir una respuesta ICMP TIME_EXCEEDED de cada ruteador. Con la respuesta, él realiza una consulta de DNS reverso para intentar obtener el nombre de dominio asociado.

Todas las informaciones recolectadas a través de los recursos citados anteriormente pueden ser obtenidas directamente con los proveedores de acceso por las autoridades brasileñas. No obstante, hay situaciones en que es imprescindible la anticipación del investigador, que en cuestión de segundos puede encontrar el camino más corto para localización del blanco o de cual institución está apta para auxiliar en este proceso de manera más ágil.

El NTCCC/PR/SP desarrolló una serie de herramientas de uso interno para facilitar diferentes tipos de investigación en Internet, valiéndose de la integración de algunos

softwares libres disponibles como el propio whois, dimitry[27], youtube-dl [28], webpy [29], ffmpegthumbnailer [30], dn-sutils, webkit2png, etc. La elaboración de sistemas en este sentido ayuda al proceso de automatización y generación de informes necesarios para los autos. Las figuras 1.10 y 1.11 ilustran ejemplos de informes generados por los sistemas del NTCCC/PR/SP.

[27] http://www.mor-pah.net/index.php?file=projects/dmitry
[28] http://rg3.github.com/youtube-dl/
[29] http://webpy.org/
[30] http://code.google.com/p/*mpegthumbnailer/

Figura 1.10: Informe generado automáticamente por el NTCCC - recogida de screenshots

1.6 Fecha y hora en Internet

Es cierto que las correlaciones de eventos en una escala cronológica son fundamentales para la comprensión de los hechos. Para los propósitos de la investigación, una eventual falta o falla en la adquisición del período exacto de una conexión en Internet puede comprometer todo el procedimiento, o aun peor, causar perjuicios a terceros que no poseen ninguna relación con el crimen investigado.

Veremos en este tópico **quién** define y **cómo** se define el tiempo en Internet, exponiendo las tecnologías que posibilitan la sincronización de horario en los millones de hosts conectados a la red mundial de computadoras.

1.6.1 Un ejemplo de la importancia de la sincronización de relojes en Internet

Considere la siguiente sucesión de eventos que ocurrió en el espacio de tiempo de aproximadamente 1 minuto:

1. **Usuario A** se conecta a Internet a través de su proveedor de acceso residencial (información suministrada por el proveedor de acceso);

2. **Usuario A** recibe un email privado con contenido criminal del **Usuario B** (información suministrada por el proveedor de email);

Figura 1.11: Informe generado automáticamente por el NTCCC - recogida de vídeos

3. **Usuario A** disemina el contenido criminal en un Ferrum público en Internet (información suministrada por el proveedor de hospedaje del forum);

4. **Autoridad** recibe denuncia anónima sobre la publicación del contenido en el forum (información grabada en el sistema de denuncia de la autoridad);

5. **Autoridad** recolecta contenido del forum y confirma la publicación (información grabada en el sistema de recogida de evidencias de la autoridad);

6. **Usuario A** recibe un email privado conteniendo un virus de computadora (información suministrada por el proveedor de email);

7. **Usuario A** su computadora es infectada por el virus recibido (información verificada en un procedimiento investigaciónl);

8. **Usuario A** se desconecta de su proveedor de acceso a Internet (información suministrada por el proveedor de acceso);

En este ejemplo notamos que el procedimiento de investigación se inicia solamente después del ítem 4, cuando la denuncia es registrada, a pesar de que existen 3 eventos anteriores y otros 4 posteriores a la denuncia. Estos eventos son igualmente relevantes para la reconstitución de los hechos y la presentación futura de las pruebas. No obstante, tendrán utilidad **en la medida en que puedan ser reconstituidos cronológicamente**. Verificamos que en un intervalo de tiempo de algunos minutos hubo, por lo menos, 6 computadoras con informaciones relevantes para la investigación involucradas en este episodio. Ellas son:

- La computadora que registró la conexión y desconexión del Usuario A en su proveedor de acceso a Internet (ítems 1 y 8);

- La computadora (servidor de email) que envió el email del Usuario B para la dirección de email del Usuario A (ítems 2 y 6);

- La computadora que hospedó el contenido criminal en su servicio de forum online (ítem 3);

- La computadora de la Autoridad que recibió y registró la denuncia anónima online (ítem 4);

- La computadora de la Autoridad que realizó la recogida de evidencias y confirmó la publicación del contenido criminal (ítem 5)

- La computadora del Usuario A, que publicó el contenido en el forum y posteriormente fue infectada por un virus (ítem 7)

Para que haya consistencia en la correlación de los eventos citados, es necesario que las 6 computadoras involucradas tengan sus relojes sincronizados. Es necesario entonces que haya una referencia única a ser seguida por todas ellas. Antes de entrar en los detalles técnicos de como esto funciona, vamos a imaginar algunas consecuencias negativas para la investigación en caso de falla o falta de registro de horarios en los eventos anteriores:

- Suponga que el proveedor de email del **Usuario A** suministre un horario incorrecto referente al recibimiento del email con contenido criminal del **Usuario B**. Es a partir de este horario que será formulado el pedido de informaciones de registro de este usuario en su proveedor de acceso, conforme veremos con más detalles en el capítulo **Aspectos técnicos de la investigación**. Puede ocurrir por tanto que en aquel horario (incorrecto) suministrado, otro usuario del proveedor de acceso estaba accediendo a Internet, y que este nada tenga que ver con el crimen.

- Si el proveedor de hospedaje del forum suministra un horario incorrecto referente al momento del upload del contenido criminal, muy probablemente el

proveedor de acceso no localizará ningún registro de IP en su base de datos (referente al horario incorrecto), tornándose por tanto inhabilitado para suministrar los datos para la autoridad, perjudicando por fin aquello que sería el próximo paso de la investigación.

- Un eventual argumento de que hubo publicación involuntaria del contenido criminal por parte del acusado (Usuario A) puede ganar fuerza, en caso que no sea posible comprobar que su computadora fue infectada por un virus solamente después del upload para el forum. Es bastante común la alegación de que el supuesto criminal perdió el control sobre su computadora por culpa de un virus, o incluso en virtud de otros factores menos probables [31], librándose por tanto de la responsabilidad del acto.

1.6.2 El NTP (Network Time Protocol)

El NTP es un protocolo de comunicación que permite la sincronización de los relojes de computadoras y otros equipos en una red, a partir de una referencia confiable de tiempo. El Network Time Protocol presenta una topología jerárquica, dividida en capas, donde en el nivel más alto están las computadoras directamente conectadas a dispositivos que suministran marcaciones precisas de tiempo, como receptores GPS (Sistema de Posicionamiento Global) o relojes atómicos. Estos dispositivos reciben el nombre de estrato 0 (stratum 0), mientras que las computadoras conectadas a ellos son los estrato 1 (stratum 1). Las computadoras estrato 1 suministran el tiempo para los estrato 2 y así en adelante, jerárquicamente, conforme ilustrado en la figura 1.12.

[31] http://www.independient.co.uk/life-style/gadgets-and-tech/news/man-blames-cat-for-porn-downloads-1770059.html (hombre culpa a su gato por downloads de pornografía infantil)

Figura 1.12: Estructura jerárquica en capas del NTP (fuente: NTP.br)

Se nota que en la arquitectura del NTP las computadoras poseen dos funciones básicas: la de **consultar** el tiempo y la de **suministrar** el tiempo. De esta manera - aunque un tanto simple – se da la sincronización de los relojes de los hosts conectados a Internet.

1.6.3 La Hora Legal Brasileña y el Proyecto NTP.br

Por medio de un acuerdo firmado entre el NIC.br (Núcleo de Información y Coordinación del Punto BR) y el Observatorio Nacional [32], nació el proyecto NTP.br, que tiene por objetivo ofrecer condiciones para que los servidores de Internet en Brasil estén sincronizados con la Hora Legal Brasileña.[33]

El NTP.br ofrece gratuita y públicamente 3 servidores NTP estrato 2, nombrados como:
- a.ntp.br
- b.ntp.br
- c.ntp.br

Estos servidores están conectados a tres servidores estrato 1, que a su vez están sincronizados con relojes atómicos bajo responsabilidad del Observatorio Nacional, conforme muestra la figura 1.13.

[32] El Observatorio Nacional tiene como atribución legal generar, mantener y diseminar la hora legal Brasileña. Ley 2.784 del 18 de junio de 1913, reglamentada por el decreto 10.546 del 5 de noviembre de 1913.

[33] http://www.ntp.br/estructura.html

Figura 1.13: Estructura del NTP en Brasil (fuente: NTP.br)

Vale recordar que, a pesar de que el NTP sea un protocolo bastante simple, y que el NTP.br suministre una estructura gratuita para la sincronización de los relojes de computadoras en Internet, es necesario que el administrador del sistema realice los pasos de instalación y configuración de software para la utilización de este recurso. El sitio Web del NTP.br[34] ofrece tutoriales en texto y vídeo sobre los procedimientos técnicos necesarios.

1.6.4 Entendiendo referencias y formatos de hora en Internet

Aunque el sistema de referencias de hora no sea algo específico de la red mundial de computadoras, es un hecho que la creciente onda de comunicación online entre diferentes husos horarios ha popularizado (y a veces confundido) a las personas en este tema.

[34] http://ntp.br/utilizando.html

El Greenwich Mean Time, o GMT, fue por bastante tiempo el término utilizado para referenciar el huso horario central del planeta, que guiaba a todos los otros localizados a su este y oeste. A pesar de que aun es muy utilizada, la referencia GMT fue sustituida por el término Coordinated Universal Time, o UTC, traducido como Tiempo Universal Coordinado. Con frecuencia nos deparamos con las dos siglas en conjunto: GMT/UTC, o UTC/GMT, que en realidad ofrecen la misma información que se pretende cuando son referenciadas individualmente, a saber: el huso horario 0 (cero), central, del planeta.

UTC, GMT, logs de conexión en Internet

Uno de los principales objetos de investigación de crímenes cibernéticos son los logs (registros) de conexiones. Un log de conexión en general está compuesto por los tres elementos siguientes:

1. una dirección IP de origen (o de destino) de la conexión
2. el momento relativo de la ocurrencia de la conexión (día, mes, año, hora, minuto y segundo)
3. la referencia UTC de la ocurrencia de la conexión

El primer componente, como fue visto en **Conceptos introductorios**, identifica la computadora de origen (o en casos menos usuales, la de destino) involucrada en la conexión. El segundo componente informa la fecha y horario de la conexión en relación al huso horario local **en el cual los logs son registrados en aquel sistema**. Finalmente, la referencia UTC complementa el ítem 2, suministrando un elemento que torna absoluta la información de fecha y hora de la ocurrencia del evento, a partir de una referencia universalmente adoptada.

Los ejemplos a continuación son extracciones de logs de conexión reales que ya pasaron por análisis del NTCCC/PR/SP. Las direcciones IP fueron intencionalmente modificadas para no revelar ningún dato sensible de estos eventos.

2008/12/16 10:52:47 189.34.23.19 UTC/GMT

Tenemos anteriormente el registro de una conexión de la dirección IP 189.34.23.19 realizada a las 10:52:47 el dieciséis de diciembre de 2008. Además de esto, tenemos la referencia UTC/GMT, sin indicación de suma o sustracción de horas. Esto significa que la información de fecha y hora fue suministrada en el huso-horario 0 (cero), también referenciada como "en hora universal". Es necesario por tanto que se efectúe la conversión, una vez que se desea conocer el horario local de este evento. En este caso, al sustraer tres horas de 10:52:47 tendremos 07:52:47, que es la hora local de Brasilia registrada en el momento de la ocurrencia.

13/12/08 02:33:09 201.97.231.2 BRT

En el registro anterior se ve una referencia de horario que no es UTC ni GMT. Se trata de la abreviación BRT, que significa Brazilia Time, u horario de Brasilia. La información de tiempo presente en este log se presenta por tanto ya convertida para nuestro horario oficial. Se utiliza además la sigla BRST (Brazilia Summer Time) cuando se quiere designar una ocurrencia en horario de verano, o sea, dos horas atrasadas en relación al UTC. Veamos otro ejemplo:

10/03/2007 03:34:01 am 200.21.39.29 +0100

En el registro anterior tenemos la sigla **am** después de la información de horario de la conexión. Se trata de una convención bastante popular principalmente en países de lengua inglesa, donde se dividen las 24 horas de un día en dos períodos de 12 horas: a.m.(ante meridiem) y p.m. (post meridiem). Por tanto para evitar confusión es necesario que la hora suministrada sea acompañada de una referencia que puede ser representada como AM/PM, am/pm o A.M/P.M.[35]

Aun en este ejemplo, notamos que hay una referencia de huso- -horario representado por +0100, o sea, una hora adelantada en relación al UTC/GMT. Al convertir esta información para el horario oficial de Brasilia, se debe observar que la fecha (y no solamente la hora) será también modificada. Dejamos para el lector este cálculo como ejercicio.

09/15/2009 04:12:42 pm 200.23.45.67 GMT-2

Este ejemplo es semejante al anterior, no obstante fue adoptada aquí otra notación para referencia UTC. Intuitivamente se nota que el horario suministrado anteriormente se sitúa a dos horas atrasadas en relación a la hora universal. Podría haberse utilizado también la abreviación BRST, como vimos anteriormente.

7/4/2005 7:23:01 am 65.3.25.38 PST

[35] Surge la duda acerca de la forma correcta de representar el mediodía en esta convención. ¿Sería mediodía 12 am o 12 pm? Según el Museo Marítimo Nacional en Greenwich, ninguna de las dos representaciones está correcta, una vez que al mediodía el sol está exactamente en la línea del meridiano, por tanto ni antes (ante meridiem) ni después (post meridiem). Se percibe entonces que esta convención carga una cierta ambigüedad, tornándola no recomendada para asuntos de orden técnica - a pesar de que esté siendo aun bastante utilizada.

El log ilustrado anteriormente presenta una nueva abreviación para referencia de huso-horario. El PST es una de las diversas siglas utilizadas para este fin. Se trata del Pacific Standard Time y es utilizado en los Estados Unidos y Canadá. La hora estándar del pacífico está a ocho husos negativos del UTC. Podría ser también indicado como GMT-8, -0800, UTC-0800 etc. En el apéndice A del presente guión hay una tabla conteniendo las abreviaciones más populares con sus respectivas distancias en horas en relación al UTC.

Hay además en este ejemplo un agravante técnico que puede hacer inviable la utilización de este registro de conexión en una investigación. La información de fecha aisladamente no presenta una organización que distinga claramente las informaciones de mes y de día. Al final, ¿este acceso se consumó el 7 de abril de 2005 o el 4 de julio de 2005? Veremos a continuación como evitar estas confusiones.

1.6.5 Buenas prácticas al lidiar con fecha y hora en Internet

Verificamos en el 1.6 que desgraciadamente no hay un estándar único que determina la disposición de los datos en los registros de fecha y hora en sistemas computacionales. La manera como se almacenan los datos depende exclusivamente del software que realiza el registro, el cual depende del individuo o corporación responsable de su desarrollo y manutención.

No obstante, podemos citar algunas prácticas capaces reducir los impactos negativos consecuentes de esta diversidad de estándares. A continuación aparecen nuestras recomendaciones finales para este asunto:

1. Una vez que no hay un estándar único, no habrá receta de pastel en la interpretación de los datos. Es necesario el conocimiento sólido del problema para que se desarrolle una solución adecuada para cada caso. Se recomienda disponer por tanto de al menos una persona dotada de este conocimiento durante la conducción de las investigaciones, principalmente en las etapas en que se formulan los pedidos de violación de confidencialidad telemática. En este momento se debe prestar atención a los diferentes estándares y referencias ofrecidas por cada proveedor de Internet y realizar todos los cálculos necesarios.

2. Se debe, siempre que sea posible, solicitar al proveedor de acceso o servicio de Internet un documento explicativo acerca del estándar por él utilizado para almacenar los registros que suministrarán. En el último ejemplo del tópico 1.6.4 sería posible identificar con precisión la fecha suministrada en el registro de conexión, siempre que hubiese un documento simple informando que aquellos datos cumplen el estándar **MM/DD/AAAA H:MM:SS am/pm IP Referencia UTC por abreviación**.

3. Hay casos en que el monto de datos a ser analizado demanda un procesamiento automatizado. Es necesario entonces tener un programa de computadora apto para comprender un determinado formato de datos. Como vimos, hay estándares definitivamente inadecuados para este tipo de procesamiento, que deben por tanto ser evitados. En situaciones como esta, se recomienda solicitar la colaboración del proveedor de acceso para que se implemente o para que realice la conversión de sus datos para un estándar consistente. El NTCCC/PR/SP ha adoptado el estándar ISO 8601[36] bajo la forma 2OO2-O5-3OTO9:3O:1O-O3:OO.[37]

[36] http://www.iso.org/iso/date_and_time_format
[37] La CPI de la Pedofilia (Senado Federal, 2008-2010) ilustra una situación en la cual fue necesario establecer estándares de suministro de datos de confidencialidad telemática en virtud de la inmensa cantidad de logs de conexión a ser analizados. Tal solicitud de adecuación a los estándares desarrollados era anexada a los requerimientos dirigidos a las empresas responsables del suministro. Ver detalles en http://www.senado.gov.br/sf/comissoes/documentos/SSCEPI/TextosPedofilia.pdf

4. Utilice recursos automatizados para certificar la consistencia de eventuales conversiones de huso-horario durante la investigación. Una opción online es el servicio gratuito http://www.thetimezoneconverter.com.

5. Para el desarrollo de estándares en este sentido, recomendamos consultar los frentes de trabajo del OASIS LegalXML[38] y Global Justice XML[39]. El NTCCC/PR/SP viene trabajando en conjunto con otras autoridades y proveedores en la elaboración de un estándar unificado de transferencia de datos telemáticos. Consideramos que unir esfuerzos en este sentido resulta en beneficios para todas las partes.

1.7 Conectándose a Internet

Sabemos que hay actualmente una variedad de formas de conectarse a Internet. Entre los medios de acceso más populares se destacan los aparatos móviles (ej. smartphones) y el uso de la estructura de telefonía fija (ADSL y línea discada). En regiones más distantes de los centros urbanos se ve popularizada la conexión vía satélite. Redes corporativas y académicas tienden a utilizar tecnologías más robustas para conexión (ej. estructuras de fibra ótica). El hecho es que, sea cual sea el medio físico utilizado, el internauta estará por fin inmerso en el mismo conglomerado de redes, que es Internet - gozando por tanto de los mismos beneficios y utilizando los mismos protocolos abordados en los tópicos anteriores de este Guión. Sin embargo, cada modo de conectarse a Internet carga algunas peculiaridades, influenciando por ejemplo la decisión al respecto de los caminos más adecuados a seguir en el intento de identificación de un criminal en la red.

[38] http://www.legalxml.org
[39] http://www.it.ojp.gov

Resumimos a continuación las formas comúnmente utilizadas para acceder a Internet, destacando algunos puntos que merecen atención durante un procedimiento investigativo. Más detalles son abordados en el capítulo 3, **Aspectos técnicos de la investigación.**

1.7.1 Conexión por línea discada (dial up)

Pionera como medio de acceso a Internet, la conexión por línea discada hace uso exclusivo de una línea telefónica, valiéndose de un dispositivo electrónico responsable de la modulación de señales digitales en ondas analógicas (y viceversa). Este aparato es conocido popularmente como módem.

Según investigación coordinada por el CETIC.br (septiembre a noviembre del 2009), solamente 20% de los internautas brasileños aun utilizan línea discada como medio de conexión a Internet[40]. La tendencia es que este índice disminuya en virtud de los beneficios que ofrecen las conexiones "banda ancha".

Consejo para investigación

La dirección IP suministrada por el proveedor de acceso en línea discada al cliente es generalmente dinámica y de alta volatilidad. O sea, se tiene prácticamente un nuevo IP a cada nueva conexión. Por tanto es fundamental asegurar una alta precisión referente al horario de acceso en un caso que tenga este tipo de tecnología.

[40] http://cetic.br/usuarios/tic/2009-total-brasil/rel-geral-05.htm

1.7.2 ADSL

ADSL, acrónimo para Asymmetric Digital Subscriber Line es la tecnología más común de la familia de tecnologías DSL (o xDSL). Tal como la dial up, utiliza una línea telefónica convencional para transmisión de los datos, valiéndose no obstante de las frecuencias que no son utilizadas en llamadas de voz. Tal hecho asegura el uso de la línea para transmisión de datos simultáneamente a la transferencia de señales analógicas de una llamada telefónica.

El ADSL fue proyectado para suministrar una capacidad de download mayor que de upload, lo que usualmente atiende a las demandas de los internautas domésticos. De una manera general, tenemos con el ADSL una tasa de download de hasta 24Mbits/s, capacidad muy superior a las conexiones de línea discada, las cuales normalmente operan en 56Kbits/s. Tal hecho coloca a la tecnología ADSL entre aquellas consideradas de banda ancha, en contraposición a la banda estrecha de la anterior.

El requisito para conexión ADSL es básicamente la disponibilidad de un módem conectado a una línea telefónica con el servicio activado. Al módem se conecta normalmente a una computadora con interfaz de red ethernet o un ruteador inalámbrico (WiFi).

Consejo para investigación

Al conectarse a Internet a través del servicio ADSL, el internauta normalmente recibe una dirección IP dinámica, o sea, un IP que no es exclusivo para su uso y por consecuencia otros clientes del mismo proveedor de acceso lo utilizarán posteriormente. Tal como ocurre para conexiones en línea discada, se debe prestar atención a las marcaciones de fecha y hora de acceso en este tipo de conexión. No obstante hay, servicios domésticos y corporativos que ofrecen al cliente una dirección IP fija, bajo costos más elevados. Esta información debe ser solicitada al proveedor de acceso.

1.7.3 Cable (cable módem y fibra ótica)

Mientras la conexión ADSL utiliza la infraestructura de telefonía para transmisión de datos, el acceso a Internet a través del cable normalmente ofrece conectividad a través de la estructura física de TV por cable preexistente en una residencia. Bastante popular para uso doméstico, esta tecnología suministra velocidades de acceso que pueden sobrepasar los 100Mbps (download) y 20Mbps (upload).

Es necesario disponer de un cable módem y una computadora con interfaz de red para disfrutar del servicio. Tal como ocurre en el ADSL, es común que se conecte un

ruteador en el módem para acceso inalámbrico en el ambiente doméstico. En general, el módem se conecta a un cable coaxial, que a su vez se conecta (dentro de la estructura de un edificio o en puntos externos de distribución) a una estructura de fibra ótica que transmite los datos de una vecindad en alta velocidad hasta la localización del proveedor de acceso.

Consejo para investigación

Las direcciones IP suministradas a los clientes residenciales son dinámicas, siguiendo modelo similar al aplicado en los servicios ADSL. Es posible también que proveedores de acceso por cable otorguen direcciones IPs privadas a sus clientes, valiéndose de las tecnologías de mapeo de IP, conforme vimos en 1.2 Conceptos introductorios. Tal hecho puede dificultar la identificación posterior de un cliente, en caso que el proveedor no posea los registros de mapeo necesarios y disponibles en el momento de la solicitud de la autoridad.

1.7.4 Radio (WiFi)

Proveedores de Internet a través de radio dispensan el uso de una línea telefónica y otras estructuras de cableado que son requisitos en los medios abordados hasta aquí. La conexión es realizada entre dos antenas de radio, una presente en el proveedor de acceso y otra en la localización del cliente. No debe existir cualquier barrera física entre ellas. Internet a través de radio es una opción comúnmente utilizada en condominios y en locales en que no hay infraestructura de cableado para otras tecnologías de banda ancha. La tasa de propagación de las señales digitales en el aire varía de acuerdo con las condiciones naturales y calidad de los equipos. Es común también que proveedores de Internet por radio posean estaciones repetidoras, o puntos de presencia instalados en locales estratégicos para mayor amplitud de las señales.

Consejo para investigación

En servicios de Internet por radio generalmente no se atribuye una dirección IP real a las computadoras de los usuarios. Algunos proveedores utilizan recursos de traducción de direcciones (NAT) y enmascaramiento de IP evitando costos adicionales con alquiler de bandas de IPs reales y a veces ofreciendo la no identificación del cliente en Internet como un diferencial en relación a las otras tecnologías, como expone un gran proveedor brasileño de Internet por radio en su sitio Web:

"Además de esto, los clientes poseen un IP enmascarado, o sea, las personas conectadas en la red interna no pueden ser identificadas por usuarios comunes conectados a Internet."

La práctica de la no utilización de direcciones IP reales para clientes es necesaria hoy ante la escasez de direcciones IPv4. Por otro lado, al adoptarla, es importante que el proveedor implemente internamente otros medios que identifiquen a un cliente a partir de una conexión. En caso contrario las investigaciones que lidian con usuarios de Internet por radio quedarán eventualmente perjudicadas.

1.7.5 Satélite

Otra alternativa que también dispensa infraestructura terrestre es la conexión a Internet vía satélite. Este tipo de conexión utiliza satélites y es utilizada especialmente para alcanzar locales de difícil acceso, como las zonas rurales más alejadas de centros urbanos. Servicios de Internet vía satélite son también ofrecidos para transmisión ocasional de eventos, por interferir mínimamente en la infraestructura local.

1.7.6 Redes de telefonía celular

Una breve lectura sobre el proceso evolutivo de las tecnologías de telefonía celular proporcionará al lector una familiaridad con algunos conceptos y términos relevantes en este asunto. Resumimos a continuación cada una de las generaciones de estos sistemas. Dos referencias fueron esenciales para la elaboración de este tópico: [Harte 2006] y [Newton 2009].

1.7.6.1 Primera generación (1G)

La primera generación de telefonía celular (1G) transmitía informaciones de voz utilizando una forma de modulación analógica, como por ejemplo, por medio del uso de frecuencia modulada (FM), donde los bits 0 pueden ser representado por ondas senoidales de alta frecuencia y los bits 1 por ondas senoidales de baja frecuencia, manteniendo constante su amplitud.[41] En 1974 fue implantado en los Estados Unidos el sistema de comunicación de primera generación bautizado AMPS (Advanced Mobile Phone Service). Fueron asignados solamente 666 canales de frecuencia en un espectro de 40MHz. En 1986 hubo una expansión para 832 canales con la adición de 10MHz al espectro ya asignado. El sistema AMPS dividía sus 832 canales en dos bandas, A y B, permitiendo así la operación de dos proveedores de servicio en una misma área de cobertura. Con la llegada de las generaciones siguientes los sistemas analógicos de telefonía celular como el AMPS, TACS, NMT, MCS, etc., se volvieron obsoletos.

[41] La representación binaria a través de los dígitos 1 y 0 es útil para fines didácticos. Se trata no obstante de los pulsos eléctricos positivos (1) y no positivos (0) consecuentes de la discretización de las ondas analógicas (continuas) para transmisión y procesamiento de los datos (a través de señales digitales).

1.7.6.2 Segunda generación (2G)

Los sistemas **digitales** para celular, llamados sistemas de segunda generación, difieren de los anteriores especialmente por el hecho de transmitir informaciones de voz y datos a través de señales digitales, no utilizando ondas analógicas como en la primera generación. Se añade además la capacidad de servir a varios clientes en un único canal de radio simultáneamente. Estos canales de radio son subdivididos en canales de comunicación, lo que no ocurre en las tecnologías analógicas anteriores.

Se estima que cada canal de comunicación soporta de 20 a 32 clientes (considerando que cada cliente utiliza el equipo durante algunos minutos por día). Por consecuencia, si un canal de radio posee 8 canales de comunicación, una estación de telefonía celular digital con 25 canales podría soportar de 4.000 a 6.400 clientes en una única área de cobertura (25 canales de radio x 8 usuarios por canal x 20 a 32 usuarios por canal de comunicación).

Entre los tipos de sistema de telefonía de segunda generación están el GSM, IS-136, CDMA y TDMA. Posteriormente, a partir de una **actualización** de la segunda

generación, se posibilitó la transmisión de datos en forma de **paquetes**. Este fue el gran paso para la viabilización del acceso a Internet a través de sistemas de telefonía celular. Para este upgrade de protocolos, softwares y equipos en los sistemas 2G, se dio el nombre de generación 2.5 o sistemas 2.5G, que incluyen las tecnologías **GPRS, EDGE y CDMA2OOO 1xRTT.**

En la práctica (al menos en Brasil), los sistemas 2.5G ofrecen tasas de transmisión equivalentes a las proporcionadas por conexiones dial up. El gran diferencial aquí está en la movilidad ante la posibilidad de acceso a través de aparatos portátiles e inalámbricos, como los aparatos celulares, PDAs, Netbooks etc.

Consejo para investigación

No hay restricciones técnicas en lo que se refiere a la asignación de direcciones IP para los clientes de tecnologías 2.5G. En Brasil, hemos notado que dependiendo de la operadora de acceso y de la localización geográfica, los usuarios pueden recibir direcciones IP públicas o IPs privadas traducidas a través de NAT. En ambos casos la dirección IP atribuida es dinámica, reforzando por tanto la necesidad de identificación precisa del momento de los eventos que motivaron la investigación, de manera que la operadora de acceso esté apta para localizar otras informaciones referentes al usuario investigado.

1.7.6.3 Tercera generación (3G)

Los requisitos para los sistemas de tercera generación son definidos por el proyecto Internacional Mobile Telecommunications (IMT-2OOO), coordinado por el International Telecommunications Union (ITU). Las tecnologías y protocolos implementados en esta generación posibilitan un mayor **ancho de banda** para transmisión de datos, además de técnicas más sofisticadas de compresión, ofreciendo así velocidades muy superiores a la anterior de 2.5G (GPRS, EDGE, etc.). El sistema WCDMA (Wideband Code Division Multiple Access) es el más popular actualmente para acceso a las redes 3G. Este sistema utiliza canales de radio que poseen un ancho de banda mayor, propiciando por tanto mayor velocidad de transmisión. A veces los aparatos celulares con soporte para la conexión 3G son referenciados como aparatos WCDMA, como se ve en la noticia siguiente:

Brasil con 18,9 millones de celulares 3G

Según una institución especializada en investigaciones en este tema, “Brasil terminó Dic/10 con 18,9 millones de celulares 3G, siendo 14,6 millones aparatos WCDMA y 4,3 millones módems. De las adiciones netas de 1.268 mil accesos 3G en el mes, 1.025 mil fueron a través de aparatos WCDMA y 243 mil por módems. Ya son 3G 9,3% de los celulares de Brasil.” [a]

[a] Fuente: Teleco. Teleco permite la publicación parcial de su sitio Web para publicaciones sin fines comerciales, siempre que sea citada la fuente.

En Brasil los proveedores comercializan paquetes 3G con velocidad de acceso de hasta 1Mbps, a pesar de que estos sistemas hayan sido especificados para atender demandas

de velocidades superiores. Diversos factores influencian en la calidad y velocidad de transmisión de los datos, como por ejemplo:

- cantidad de usuarios por área de cobertura
- distancia entre el usuario y la estación radio base (ERB) asociada
- si el equipo está en movimiento o en reposo
- infraestructura de la operadora y técnicas de compresión utilizadas

Tal como ocurre en la generación anterior (2.5G), las direcciones IP asignadas para los clientes 3G son dinámicas y pueden, dependiendo del proveedor, ser direccionables o no en Internet (Ver 1.2 para más detalles). Con la llegada de esta generación, se hizo bastante común la utilización de modems 3G para el acceso a través de aparatos que no son dedicados a la telefonía, como laptops, netbooks e incluso computadoras domésticas.

1.7.6.4 Cuarta generación (4G)

También referido como IMT-A (International Mobile Telecommunications Advanced) y LTE (Long Term Evolution), la tan esperada red de cuarta generación es el asunto de un esfuerzo global de estandarización que incluye a organizaciones como ITU, 3GPP, 3GPP2, IETF, industria y operadores de telecomunicaciones con el propósito de definir la próxima generación de plataforma de red para telefonía móvil.

Se busca en esta nueva tecnología la capacidad de transmisión que alcance 100Mbps en aparatos en movimiento (teléfonos móviles, PDAs, laptops) y 1Gbps en equipos fijos, como microcomputadoras domésticas. Hay previsiones para que el servicio esté disponible comercialmente a partir del 2012.

1.7.7 Red eléctrica

Conocida por el nombre de BPL (Broadband over Power Lines), o PLC (Power Line Communications), la conexión de datos a través de la estructura de redes eléctricas aun no se popularizó en Brasil. A pesar de que ya cuente con algunos casos de éxito y diversos debates en los ámbitos técnicos y normativos, el servicio aun no es masivamente ofrecido en el país.

En la Resolución número 527 del 8 de abril del 2009 la ANATEL (Agencia Nacional de Telecomunicaciones) aprobó el **Reglamento sobre Condiciones de Uso de Radiofrecuencias por Sistemas de Banda ancha por medio de Redes de Energía Eléctrica (BPL)**.[42]

Posteriormente, el 25 de agosto de 2009, la ANEEL (Agencia Nacional de Energía Eléctrica) "**aprobó las reglas para la utilización de la red eléctrica para transmisión de datos, voz e imagen y acceso a Internet en alta velocidad por medio de la tecnología Power Line Communications (PLC). La Resolución Normativa número 375/2009 que establece las condiciones de repartición de la infraestructura de las distribuidoras permitirá significativos avances al país, con un importante estímulo a la inclusión digital, pues el 95% de la población brasileña tiene acceso a la electricidad por medio de 63 concesionarias y 24 cooperativas, que llevan energía a 63,9 millones de unidades consumidoras**". La completa publicación y otras

informaciones acerca de esta tecnología pueden ser vistos en el sitio Web que la ANEEL mantiene bajo el título **Internet por la Red Eléctrica**. [43]

[42] http://legislacao.anatel.gov.br/resolucoes/24-2009/101-resolucao-527
[43] http://www.aneel.gov.br/hotsite/plc/

La figura 1.14 exhibe un módem (también referido como adaptador) PLC, necesario para la transmisión de datos a través de la red eléctrica. A pesar de que aun es escaso el ofrecimiento de este servicio para acceso a Internet, este equipo ya está a la venta en Brasil y ha sido utilizado para extensiones de redes locales domésticas o corporativas.

Figura 1.14: Módem PLC para distribución de datos a través de red eléctrica

1.7.8 WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) es el nombre dado por el WiMAX Forum[44] a la familia de estándares 802.1645, que especifica una tecnología para ofrecimiento de redes metropolitanas inalámbricas.

Recapitulando un poco de la historia, tenemos que las primeras conexiones eran realizadas por línea discada (dial up). Entonces se lanzaron las tecnologías de banda ancha, como el ADSL y las redes cableadas. Actualmente tenemos como populares las opciones de conexión a través de satélite, telefonía celular y por radio (en este caso utilizándose el estándar WiFi - definido en la IEEE 802.11). Podemos considerar que los esfuerzos del grupo por detrás del desarrollo del WiMAX está en unir los beneficios de cada una de las tecnologías existentes, con el objetivo de ofrecer en un único servicio la velocidad de conexión de las redes alámbricas y la movilidad que proporcionan las redes inalámbrico.[46]

Vimos en **1.7.4 Conceptos introductorios** que los servicios de acceso a través de radio son una opción viable una vez que haya ausencia de obstáculos entre el transmisor y el receptor (visión directa). En un ambiente metropolitano realista, 50% a 70% de los potenciales clientes no poseen visión directa y abierta al punto de acceso a la red inalámbrico, en virtud de la presencia de edificios, árboles, puentes, etc. No obstante, el protocolo utilizado en el WiMAX es capaz de comunicarse en distancias de hasta 6Km sin visión, utilizando solamente un mecanismo de reflexión [Lima Luiz Fernando Gomes Soares 2004]. De manera general, se puede afirmar que el WiMAX es un WiFi de larga distancia, donde cada antena propaga ondas en un rayo de 50Km^2 y alcanza velocidad de transmisión de hasta 70Mbps.

[44] The WiMAX Forum is an industry-led, not-for-profit organization formed to certify and promote the compatibility and interoperability of broadband wireless products based upon the harmonized IEEE 802.16/ETSI HiperMAN standard. http://www.wimaxforum.org/
[45] The IEEE 802.16 Working Group on Broadband Wireless Access Standards develops standards and recommended practices to support the development and deployment of broadband Wireless Metropolitan Area Networks. IEEE 802.16 is a unit of the IEEE 802 LAN/MAN Standards Committee. http://www.ieee802.org/16/
[46] Aun se considera que el WiMAX y el 4G son esfuerzos competidores en este sentido.

La Intel, una de las mayores patrocinadoras del Forum WiMAX, declaró públicamente que el 802.16 es la cosa más importante desde la llegada de la propia Internet.

En Brasil, el WiMAX aun no es explotado comercialmente, aunque haya expectativa de que los servicios comiencen a ser ofrecidos en breve. Contando con una concesión temporal de la Anatel, fue firmado en el 2005 un acuerdo entre la Intel y el MEC para la conexión de escuelas a Internet con tecnología inalámbrica en algunas ciudades brasileñas. La prueba de fuego fue realizada en la ciudad de Ouro Preto, que en virtud de su topografía accidentada, dificulta la comunicación por medio de antenas que necesiten de visión directa. Los resultados fueron positivos, según noticia publicada por la RNP (Red Nacional de Investigación):

> **"A pesar de que se pueda esperar de la tecnología Wi-Max una tasa de transmisión nominal de 75Mbps, durante el piloto en Ouro Preto se alcanzó una tasa efectiva en torno de 14Mbps, lo que, en muchos casos, no es poco para una conexión punto a punto".[47]**

[47] http://www.rnp.br/noticias/2005/not-050927.html

CAPÍTULO 2
UNA INTRODUCCIÓN A LA GOBERNANZA DE INTERNET

> *Actores somos todos nosotros, y ciudadano no es aquel que vive en sociedad: es aquel que la transforma.*
>
> Augusto Boal

2.1 Introducción

La terminología **Gobernanza de Internet**, o Internet Governance en inglés, pasó a ser adoptada después de algunos debates, en especial durante la World Summit on the Information Society en el año 2003. El término **gobernanza** fue considerado controvertido por algunas delegaciones en esa época, en virtud de las posibles interpretaciones que lo relacionan directamente con **gobierno**, estado y gestión pública, presentándose por tanto como un término excluyente en un contexto donde se debería incluir igualitariamente a los sectores no gubernamentales. No obstante, la definición propuesta por el WSIS resolvería (o al menos amenizaría) el impasse:

> *"Gobernanza de Internet es el desarrollo y aplicación por parte de gobiernos, el sector privado y la sociedad civil, en sus respectivos papeles, de compartir principios, normas, reglas, procedimientos de toma de decisiones, y programas que modelan la evolución y el uso de Internet".*

La traducción del término governance refuerza el argumento de su relación semántica con sectores del gobierno, como en el español (gestión pública, gestión del sector público, y función de gobierno), en el francés (gestion des affaires publiques, efficacité de l administration, qualité de l administration, y mode de gouvernement) y en el idioma portugués (gestión pública y administración pública). [Kurbalija 2010, pág. 7]

El hecho es que el entonces polémico término se popularizó con el pasar de los años, tornándose por fin referencia inmediata cuando se desea investigar por el tema. Eventos ya consolidados, compuestos por los principales actores en este proceso de evolución de la gran red también utilizan esta terminología, tal como ocurre en el propio nombre del Internet Governance Forum[1].

2.2 Una breve historia de la gobernanza de Internet

Conforme visto en la sección 1.3, Internet nació de un proyecto de gobierno, llamado Advanced Research Projects Agency Network (ARPANET). En las décadas del 60 y 70 había además otras iniciativas similares, que utilizaban protocolos diversos, como las redes Mark I (Reino Unido), CYCLADES (Francia), Merit Network, Tymnet y Telenet (Estados Unidos). El principio en común entre estas redes era el de conmutación de paquetes, un método que posibilita la transmisión de datos en medios de comunicación sin la necesidad de canales dedicados para cada conexión.[2] Diferente de lo que ocurre en los métodos de conmutación de circuitos, en la conmutación de paquetes el medio de transmisión es distribuido, trayendo por tanto una característica clave para lo que se

transformó posteriormente en Internet: la descentralización de los servicios, y consecuentemente la dificultad de implantar mecanismos de control y otros tipos de barreras políticas en esta red. Como resultado, se hizo necesaria la elaboración de un nuevo modelo de gestión igualmente distribuido para tales recursos.

[1] http://www.intgovforum.org

[2] Podemos comprender mejor este principio al comparar los modelos de cobro para servicios de voz y de datos en el mercado de telecomunicaciones. En la telefonía (voz), en general el servicio es facturado por tiempo de utilización, pues en el instante de una llamada un canal de comunicación está dedicado exclusivamente al cliente en uso. Por otro lado, servicios de acceso a Internet facturan (o limitan) por monto de datos transitados, a fin de cuentas, no hay exclusividad del medio de comunicación utilizado, que es compartido en virtud del uso de la tecnología de conmutación de paquetes.

IETF - the Internet Engineering Task Force

En medio a la evolución de Internet en la década del 80, y ante la necesidad de un nuevo modelo de gestión para esta red, una fuerza-tarea compuesta por 21 investigadores financiados por el gobierno de los Estados Unidos fue formalmente establecida, recibiendo el nombre de IETF (Internet Engineering Task Force).[3]

El objetivo del IETF era contribuir con el desarrollo de Internet por medio de un modelo de gestión cooperativa, basada en consenso, involucrando una variedad de sectores e individuos. No debería haber un gobierno que centralizase las decisiones, así como no habría una planificación central, ni un gran proyecto para la gran red [Kurbalija 2010, pág. 7].

[3] El IETF fue continuación de otro grupo de trabajo, el Gateway Algorithms and Data Structures (GADS) Task Force.

Al inicio de la década del 90, el IETF se asoció al Internet Society, tornándose una organización independiente del gobierno norteamericano. La Internet Engineering Task Force cuenta con diversos grupos de trabajos para temas específicos que influencian (o que influenciarán) de alguna manera el funcionamiento de Internet. Los espacios de discusión son abiertos en listas públicas de email y en los encuentros presenciales de la organización. Las decisiones son tomadas por medio de las listas públicas a través de consenso. El grupo de trabajo para directrices y procedimientos del IETF (Working Group Guidelines and Procedures) define que (traducción libre):

> *“Consenso en el IETF no requiere que todos los participantes concuerden con algo, aunque esto sea, claro, preferido. En general, el punto de vista dominante de un grupo de trabajo debe prevalecer. (No obstante, la dominancia no está para ser determinada basándose en el volumen o persistencia, sino en un sentido de concordancia más general)”.*

Otras citaciones del IETF ilustran bien su funcionamiento, como "**nosotros rechazamos reyes, presidentes y votantes[...]**" , de David Clark y "**Sea conservador en lo que usted somete y liberal en lo que usted acepta**" , de Jon Postel. La guía para novatos en el IETF lista una serie de principios e instrucciones acerca de su funcionamiento y está disponible en el website de la organización.[4]

[4] http://www.ietf.org/tao.html

Vale citar que las tan citadas RFCs (Requests for Comments) son en general desarrolladas por grupos de trabajos del IETF y que después de criterioso proceso de aprobación se consolidan como estándares para Internet. Tenemos por ejemplo la especificación del protocolo IPV6 y asuntos asociados. Este único tema reúne decenas de RFCs, que pueden ser consultadas directamente en el website del IETF.[5]

ICANN - the Internet Corporation for Assigned Names and Numbers

En 1993 fue firmado un acuerdo de cooperación entre la principal entidad mantenedora de la infraestructura de Internet - la US National Science Foundation (NSF) - y una empresa privada llamada Network Solutions, Inc. (NSI), para que los nombres de dominio de segundo nivel (por ejemplo, el nombre wikipedia en wikipedia.org - ver sección 1.3 para saber más sobre dominios) serían distribuidos por demanda, en el modelo "el primero en pedir es el primero en recibir", bajo gestión de la referida empresa.

En 1995 este acuerdo ya era blanco de muchas críticas, que se intensificaron después de una modificación de acuerdo con el acuerdo de cooperación que permitía a la NSI cobrar tasas para nuevos registros de nombres de dominio (U$100 por dos años, de acuerdo con el artículo publicado por Craig Simon, Overview of the DNS Controversy[6]). Un movimiento contrario surgía, con el objetivo de frenar el monopolio privado que estaba a punto de nacer con este acuerdo.

[5] El proyecto IPV6.br ofrece una lista con los links de estas RFCs en http://www.ipv6.br/IPV6/ArtículoRfcIPv6
[6] disponible en http://www.rkey.com/dns/overview.html

A finales de 1996 un grupo de 10 personas llamado International Ad Hoc Committee (IAHC) fue establecido con el objetivo de formalizar un frente de acciones en favor de la administración de recursos de Internet por organizaciones sin fines lucrativos. Un manifiesto nombrado Generic Top Level Domains Memorandum of Understanding (gTLD-MoU) fue publicado por el IAHC, contando con el apoyo de otras entidades. En medio a diversas manifestaciones, esta guerra del DNS trajo nuevos actores para el escenario de la gobernanza de Internet, incluyendo organizaciones internacionales y representaciones de otros gobiernos.

Más detalles acerca de este episodio pueden ser vistos en [Kurbalija 2010] y en el artículo citado en el párrafo anterior. El hecho es que la NSI perdió el monopolio lucrativo que había conquistado con el negocio de venta de dominios en Internet, abriendo un precedente de resistencia de la sociedad civil en favor de los principios originales de descentralización de la gran red. Las principales controversias fueron finalmente superadas en 1998, con la formación de Internet Corporation for Assigned Names and Numbers (ICANN), una organización con representación mixta, supuestamente independiente del estado y sin fines lucrativos. La ICANN es aun hoy la organización responsable de la gestión de identificadores de hosts en Internet, o sea, está en la cima de la pirámide en la jerarquía de distribución de las direcciones IP y de los nombres de dominio, conforme visto en la sección 1.3. La figura 2.1 ilustra la actual estructura organizacional de Internet Corporation for Assigned Names and Numbers.

Figura 2.1: Estructura organizacional de la ICANN
(http://www.icann.org/en/about/)

WSIS - the World Summit on the Information Society

> *"La ICANN demoró algún tiempo para reconocer que el alcance de la gobernanza de Internet debía ser extendido, incorporando cuestiones más amplias de importancia crucial para el futuro de Internet."*
>
> [Afonso 2005]

El 21 de diciembre de 2001, la Asamblea General de las Naciones Unidas aprobó la resolución 58/183, endosando la Cúpula Mundial sobre la Sociedad de la Información, que contaría con dos forums de debates presenciales, programados para el 2003 en Ginebra y 2005 en Túnez. La decisión promovía la contribución de gobiernos, sectores privados y sociedad civil en los trabajos de preparación de los forums, así como recomendaba la activa participación de todos los sectores durante los dos encuentros.

En Ginebra el evento ocurrió del 10 al 12 de diciembre del 2003. El objetivo de esta primera fase fue "**elaborar y alimentar una clara declaración de voluntad política y dar pasos concretos con el objetivo de establecer los cimientos para una Sociedad de la Información para todos, reflexionando los diversos intereses en juego**". Este encuentro contó con la participación de 50 jefes de estado y vicepresidentes, 82 ministros, 26 viceministros, representantes de grandes organizaciones internacionales, sectores privados y sociedad civil. Más de 11.000 participantes de 175 países participaron del WSIS en el 2003 y eventos relacionados[8].

Esta primera etapa del WSIS resultó en la creación del Plan de Acción de Ginebra (Geneva Plan of Action)[9] y de la Declaración de Principios de Ginebra (Gineva Declaration of Principles)[10], estableciendo cuatro objetivos principales, conforme certifica el siguiente fragmento - en traducción presente en el capítulo 1 de [Afonso 2005]:

[7] http://www.itu.int/wsis/docs/background/resolutions/56_183_unga_2002.pdf
[8] http://www.itu.int/wsis/geneva/index.html
[9] http://www.itu.int/wsis/docs/geneva/official/poa.html
[10] http://www.itu.int/wsis/docs/geneva/official/dop.html

> *"Solicitamos al secretario general de las Naciones Unidas la formación de un grupo de trabajo sobre gobernanza de Internet, en un proceso abierto e inclusivo que asegure un mecanismo para la participación plena y activa de gobiernos, de la iniciativa privada y de la sociedad civil tanto de los países en desarrollo como de los desarrollados, con la participación de organizaciones y forums intergubernamentales e internacionales pertinentes, para investigar y hacer propuestas de acción sobre la gobernanza de Internet, conforme juzguen adecuado, hasta el año 2005. Entre otras cosas, el grupo debe:*

1. Desarrollar una definición funcional de gobernanza de Internet;
2. Identificar las cuestiones relativas a las políticas públicas pertinentes a la gobernanza de Internet;
3. Desarrollar una comprensión común de los papeles y responsabilidades de los gobiernos, de las organizaciones intergubernamentales e internacionales que existen y otros forums, así como de la iniciativa privada y de la sociedad civil tanto de los países en desarrollo como de los desarrollados;
4. Preparar un informe sobre los resultados de esta actividad, a ser presentado para consideración y medidas correspondientes para la segunda fase de la CMSI, en Túnez, en el 2005. "

Otro resultado expresivo de este primer evento fue la creación de un grupo de trabajo, el Working Group on Internet Governance (WGIG), que preparó el informe a ser utilizado como base para las discusiones en el encuentro siguiente, que ocurriría dos años después, en Túnez.

Los registros de las actividades en Ginebra, incluyendo lista de participantes, informes, transcripciones de los debates, vídeos y demás documentos están disponibles en el sitio web del WSIS[11].

Como previsto, la segunda fase de the World Summit on the Information Society ocurrió entre las fechas 16 y 18 de noviembre del 2005, en Túnez, y contó con un número expresivo de participantes, totalizando la presencia de aproximadamente 19.000 personas de 174 países. El objetivo de este encuentro era dar marcha a los aspectos prácticos del Plan de Acción de Ginebra, así como buscar soluciones en los diversos campos de la Gobernanza de Internet, en las formas de financiamiento e implementación de los demás documentos propuestos en la primera etapa.[12] Entre los resultados obtenidos en Túnez vale resaltar el establecimiento del Internet Governance Forum (IGF), que se consolidaría por fin como un espacio de debates manteniendo el carácter abierto y multisectorial del WSIS, siendo convocado anualmente por la Secretaría General de las Naciones Unidas.

[11] Específicamente en http://www.itu.int/wsis/geneva/index.html
[12] Los registros de este evento están disponibles en http://www.itu.int/wsis/tunis/index.html

IGF - the Internet Governance Forum

El primer the Internet Governance Forum ocurrió en Atenas, del 30 de octubre al 2 de noviembre del 2006. Cuatro macro-temas fueron propuestos en los encuentros preparatorios que lo antecedieron:

- Apertura (Openness) - Libertad de expresión, libre flujo de información, ideas y conocimiento.
- Seguridad (Securite) - Creando credibilidad y confiabilidad de forma colaborativa, particularmente protegiendo a los usuarios de los spams, phishings y virus, preservando la privacidad.

• Diversidad (Diversite) - Promoviendo el multilingüismo, incluyendo la internacionalización de nombres de dominios y contenidos locales.
• Acceso (Access) - Conectividad a Internet: política y costo, lidiando con la disponibilidad y viabilidad financiera en las cuestiones de inclusión del acceso a Internet, interoperabilidad y estándares abiertos.

La tabla 2.1 exhibe una lista con transcripciones, registros oficiales e impresiones personales sobre el IGF en Atenas.

En el 2007 el Internet Governance Forum ocurrió en Río de Janeiro entre las fechas 12 y 15 de noviembre. Los temas principales de este año fueron Acceso, Diversidad, Abertura, Seguridad y la administración de Recursos Críticos de Internet. Este último, que no constaba en la agenda del evento anterior, trata de los aspectos técnicos y políticos involucrados en el mantenimiento de la infraestructura de Internet. Este año el ICANN se enfocó en las discusiones sobre la liberación de dominios .xxx (dedicados a sitios web de contenido pornográfico), trayendo al debate cuestiones sobre el poder de decisión de esta organización, que en este caso fue acusada de exceder el ámbito técnico. Intervenciones del gobierno de los Estados Unidos en este asunto también motivaron alguna polémica acerca de la influencia de gobiernos locales en las decisiones de la ICANN que, dado el carácter transnacional de la gran red, siempre resultará en consecuencias globales.

Tabla 2.1: Algunos registros online del IGF 2006

Descripción	Dirección
Registros oficiales del IGF 2006, incluyendo transcripciones de las sesiones y una síntesis de los debates disponible en 6 idiomas	http://www.intgovforum.org/cms/athensmeeting
Sumario del evento publicado por la Internet Society (ISOC), puntuando principalmente la participación de esta institución en el IGF 2006	http://isoc.org/wp/igf/?cat=4547
Programación completa del IGF 2006	http://www.intgovforum.org/wksshop_ program3. htm
Informes de participación del Number Resource Organization en el IGF 2006	http://www.nro.net/news/igf-in-athens
Informe del representante del Ministerio de la Cultura de Brasil en el IGF 2006	http://www.cultura.gov.br/site/2006/11/06/ igf-atenas-2006-relatorio-de-viagem/
Materia periodística sobre práctica de censura en China, en debate ocurrido en el IGF 2006	http://news.cnet.com/China-We-dont-censor-the-Internet.-Really/2100-1028_3-6130970. html
Informe de la organización IP Justice sobre IGF 2006	http://ipjustice.org/2006/11/15/igf_athens_ report/

IP Justice, una organización con sede en California, que tiene por objetivo promover el equilibrio entre la propiedad intelectual y la libertad de expresión, publicó un informe

con una serie de impresiones sobre el IGF 2007, comparándolo con el encuentro anterior en Grecia y puntuando, en su visión, cuales fueron los puntos negativos y positivos de esta edición en Brasil. Según la IP Justice, el evento se destacó por el alto nivel de los workshops y sesiones de mejores prácticas, organizadas independientemente por los participantes, así como por los encuentros informales propiciados por el ambiente y localización del evento. Como punto negativo, la organización destaca la exacerbada diplomacia al tratar de asuntos controvertidos, como las prácticas de censura online por algunas naciones y cuestiones relativas a los derechos humanos.

> *"Todos recordarán que países como China e Irán, además de compañías como Cisco Systemas y Yahoo! fueron reprendidos por la comunidad debido a sus contribuciones para la censura en Internet. Desgraciadamente, este año, no fueron promovidas discusiones críticas concernientes a los derechos humanos, y los organizadores principales del evento tuvieron cuidado para evitar ofender a China y a las empresas que auxilian en la represión de la libertad y democracia de Internet."*[13]

La tercera edición del Internet Governance Forum ocurrió en Hyderabad, en la India, entre los días 3 y 6 de diciembre del 2008, con destaque para el tema Internet para todos. Esta propuesta de traer cuestiones de inclusión para el IGF no quedó solamente en el ámbito de los debates. La organización del evento ofreció una contribución práctica al crear al inicio del mismo año un grupo de trabajo responsable de viabilizar que personas y organizaciones pudiesen participar activamente por medio de recursos en Internet. El evento fue integralmente transmitido en audio y vídeo en la red. Más de 500 personas participaron remotamente, de forma independiente o por medio de Hubs oficiales, por ejemplo el grupo de la **Ciudad del Conocimiento** (USP)[14].

[13] en traducción libre de http://ipjustice.org/wp/2007/11/19/2007-igf-rio-wrap-up/
[14] IGF 2008: 32 horas de Vigilia http://www.cidade.usp.br/blog/igf-2008-32-horas-de-vigilia/

Tabla 2.2: Algunos registros online del IGF 2007

Descripción	Dirección
Registros oficiales del IGF 2007, incluyendo transcripciones de las sesiones y una síntesis de los debates disponible en 6 idiomas	http://www.intgovforum.org/cms/ secondmeeting
Programación completa del IGF 2007	http://www.intgovforum.org/Rio_Schedule_ final. html
Vídeos de las sesiones del IGF 2007	http://www.igfbrazil2007.br/videos- archive.htm
Informe de la organización IP Justice sobre IGF 2007	http://ipjustice.orgwp/2007/11/19/2007- igfrio- wrap-up/
Extensa lista con noticias relacionadas al IGF 2007, ofrecidas por el CGI.br	http://governanca.cgi.br/
"Los dos primeros años del IGF". Una publicación de la UNESCO con más de 400 páginas conteniendo	http://www.intgovforum.org/cms/hydera/ IGFBook_the_first_two_years.pdf

transcripciones, artículos, informes y otras diversas informaciones acerca de las dos primeras ediciones del Internet Governance Forum	

El IGF 2008 también estuvo marcado por los debates sobre los temas de la Neutralidade[15] de la red y la protección de datos personales. El primero apalancado por la discordancia que reina entre los grandes proveedores de servicio y de acceso a Internet, mientras que el último, tomado por el crecimiento desenfrenado de redes sociales controladas por corporaciones privadas, como Facebook.

[15] La neutralidad de la red (o neutralidad de Internet, o principio de neutralidad) significa que todas las informaciones que transitan en la red deben ser tratadas de la misma forma, navegando a la misma velocidad. Este es el principio que garantiza el libre acceso a cualquier tipo de información en la red -- http://pt.wikipedia.org/wiki/Neutralidade_da_rede

La cuarta edición del IGF ocurrió en Sharm el Sheikh, en Egipto, entre las fechas 15 y 18 de noviembre del 2009, bajo la temática principal Internet Governance - Creating Opportunities for All (Gobernanza de Internet - Creando Oportunidades para Todos). El evento contabilizó más 1.800 participantes de 112 países.

A pesar del macro-tema seleccionado, las discusiones este año tuvieron como foco el propio evento. Tal hecho ocurrió en virtud del fin del primer mandato del IGF, previsto para el 2010. Muchos participantes enfatizaron la utilidad del forum como un espacio para el diálogo libre de presiones causadas por negociaciones, defendiendo por tanto la continuidad del modelo actual para las ediciones futuras. Otros se manifestaron favorables a la toma de decisión durante el evento, de forma que el IGF pudiese incluso resultar en recomendaciones formales acerca de los temas debatidos. [16]

La programación principal del evento en el 2009 fue compuesta por las sesiones que trataron de las cuestiones de la democratización del acceso a Internet y promoción de contenido / diversidad cultural local; de la seguridad de Internet y el combate a los ciber-crímenes; de la gestión de los recursos críticos, como los servidores DNS raíz, números de direcciones IP y estándares abiertos de comunicación. Fue dedicada además una sesión para tratar de las cuestiones que emergen del crecimiento de las redes sociales en Internet. Esta colocó en pauta los temas incluyendo privacidad, protección de datos, libertad de expresión, publicación de manifestaciones criminales y demás tópicos derivados. Adicionalmente, más de 100 **workshops**, forums de buenas prácticas y otros encuentros abiertos ocurrieron paralelamente, tratando de los más diversos temas, como usualmente ocurre en todas las ediciones del evento.[17]

[16] http://www.itu.int/net/itunews/issues/2009/10/36.aspx

Tabla 2.3: Algunos registros online del IGF 2008

Descripción	Dirección
Registros oficiales del IGF 2008, incluyendo transcripciones de las principales sesiones	http://www.intgovforum.org/cms/2008- igf-hyderabad
Lista de workshops del IGF 2008	http://www.intgovforum.org/cms/ workshops_08/ wrkshplist.php

Síntesis de las sesiones del IGF 2008, por la ISOC	http://isoc.org/wp/igf/?cat=138
Informaciones sobre la participación de la NRO en el IGF 2008	http://www.nro.net/news/nro-atigf-2008-hyderabad-india
Sitio web dedicado a la participación remota del IGF 2008 (instrucciones, participantes, asuntos debatidos, etc.)	http://www.igfremote.info/
Breve informe de participación del Hub brasileño en el IGF 2008	http://www.cidade.usp.br/blog/igf2008-32-horas-de-vigilia/
Blog mantenido por el Ministerio de la Cultura de Brasil con una variedad de publicaciones redactadas por autores brasileños diversos, ofreciendo relatos e impresiones personales sobre los debates del IGF 2008	http://blogs.cultura.gov.br/igf/
Vídeos de los varios Hubs que participaron remotamente del IGF 2008	http://www.diploInternetgovernance. org/page/igf- remote-participation
Informe final del grupo de trabajo responsable de la participación remota del IGF 2008	http://www.intgovforum.org/cms/ Contributions2009/Report_RP_IGFfinal.pdf

[17] IGF Final Round Up release: http://www.intgovforum.org/cms/2009/sharm_el_Sheikh/ Stocktaking/ IGF09-Round-Up%20Release-final.pdf

Tabla 2.4: Algunos registros online del IGF 2009

Descripción	Dirección
Registros oficiales del IGF 2009, incluyendo transcripciones de las principales sesiones	http://www.intgovforum.org/cms/2009- igf-sharm- el-sheikh
Programación completa del IGF 2009	http://www.intgovforum.org/cms/2009/ sharm_el_Sheikh/WorkshopSchedule. html
Lista de workshops del IGF 2009	http://igf.wgig.org/cms/index.php/component/ chronocontact/?chronoformname= WSProposals2009ListView
Vídeos de todas las sesiones del IGF 2009	http://www.un.org/webcast/igf/ondemand.asp

La quinta edición del Internet Governance Forum ocurrió en Vilnius, en Lituania, entre los días 14 y 17 de Septiembre, trayendo para debate el macro-tema IGF 2010 - Developing the Future Together . El evento contó con la presencia de 1461 participantes, donde fueron contabilizados 113 encuentros paralelos a las sesiones principales, que este año incluyeron los siguientes tópicos y las respectivas preocupaciones [18]:

- **Gestión de los recursos críticos de Internet**: disponibilidad del IPV6 alrededor del mundo, ejemplos y casos de uso; internacionalización de los recursos de Internet; la importancia de nuevos TLDs e IDNs; y manutención de los servicios de la gran red en situaciones de crisis y desastres.

• **Acceso y Diversidad**: esta sesión se enfocó en la importancia de la disponibilidad de Internet para regiones en desarrollo, en la necesidad de internacionalización de nombres de dominio (incluyendo caracteres de variados orígenes), en los medios más baratos de suministro de acceso (como redes de banda-ancha inalámbrica) y en la preocupación con la creciente práctica de bloqueos de contenido en la red.
• **Seguridad, Apertura y Privacidad**: ante la realidad en que los datos personales se encuentran hoy en la nube de la gran red, la preocupación se vuelve para las garantías que los proveedores de hospedaje suministran al respecto de la protección de estas informaciones. Por la perspectiva de los derechos humanos, el derecho a la privacidad es algo fundamental que depende de mecanismos de seguridad para que sea plenamente ejercido. Por tanto, fue colocada en pauta la necesidad de desarrollar estos dos temas simultáneamente (seguridad y privacidad), y no tratarlos como si la ascensión de uno perjudicase al otro.

En este tópico fueron debatidos también la necesidad de creación de leyes que regulen la relación entre usuarios y empresas en posesión de sus datos, una vez que se verifica el valor comercial que estos presentan actualmente. Cuestiones de seguridad para niños y adolescentes en Internet fueron igualmente expuestas.

[18] IGF 2010 - Chairman's Summary: http://intgovforum.org/cms/2010/The.2010.Chairmans.Summary.pdf

• **Gobernanza de Internet para el desarrollo**: por primera vez el tema fue reservado para una de las sesiones principales del evento. Esta sesión exploró el papel de la gobernanza de Internet en el desarrollo de países emergentes. Fue un espacio también para que diferentes países compartieran informaciones acerca de sus modelos locales de gobernanza. El sumario oficial del evento registra especialmente las manifestaciones de Brasil y Senegal en este asunto. Por fin, el presidente de la sesión concluyó con una citación sugiriendo que "existe solamente una pequeña distancia entre dictaduras y anarquías descontroladas", mencionando que el modelo multisectorial puede ayudar a evitar estos extremos.

Tabla 2.5: Algunos registros online del IGF 2010

Descripción	Dirección
Registros oficiales del IGF 2010, incluyendo transcripciones de las principales sesiones	http://www.intgovforum.org/ cms/2010-igf-vilnius
Programación completa del IGF 2010	http://www.intgovforum.org/cms/2010/schedule/ WorkshopSchedule_Vilnius201009.htm
Informe Social del IGF 2010, iniciativa de la Diplo Foundation que reúne en un único sitio diversos canales que refieren el IGF 2010, como microblogs y redes sociales	http://igf2010.diploInternetgovernance.org
Lista de workshops del IGF 2010	http://www.intgovforum.org/ cms/2010-igf-vilnius/workshopproposal
Vídeos de todas las sesiones del IGF 2010	http://webcast.intgovforum.org/ ondemand/

Blog de la delegación brasileña en el IGF (creado en el 2010) http://igfbr.blog.br

• **Tópico emergente computación en nube**: desafíos que surgen a partir de la distribución de contenidos personales en la gran red fueron debatidos en esta sesión, incluyendo cuestiones técnicas, científicas, de costos, seguridad y privacidad. Entre varios cuestionamientos levantados, el presidente de la sesión relató los siguientes:

- ¿La nube sería dominada por algunas pocas corporaciones tal como ocurre con la distribución de electricidad?
- ¿La utilidad de la nube ayudaría o trabaría las innovaciones? ¿Y cuáles políticas serían necesarias para mitigar los efectos negativos de la nube?
- ¿Qué estructura sería necesaria, dada la complejidad de la computación en nube, para construir un modelo confiable, especialmente en términos de confidencialidad y privacidad?

• **Un balance de la Gobernanza de Internet y pasos futuros**: Como el título indica, el foco de esta sesión fue la evolución del escenario de la Gobernanza de Internet desde la primera edición del IGF en el 2006, así como los desafíos que están por venir durante el próximo mandato de 5 años, que finaliza en el 2015.

El IGF 2010 contó además con más de 600 personas que no se encontraban presencialmente en el evento, pero que de alguna manera participaron por medio de uno de los 32 Hubs registrados. Brasil estuvo presente en dos Hubs locales, uno preparado en la Universidad Federal de Bahía (UFBA) y otro en la Universidad Federal de Río de Janeiro (UFRJ).

2.3 Clasificación de los temas de Gobernanza de Internet

> *"...es casi imposible que una persona domine conocimiento suficiente para lidiar con todos los temas relacionados a la gobernanza de Internet. El GTGI listó más de 40 de estos temas y, a pesar de algunas impresiones contrarias, el grupo no está constituido por especialistas en todos ellos."*
>
> Carlos Afonso, en Gobernanza de Internet - Contexto, Impasses y Caminos

[19] Report of the Working Group on Internet Governance: http://www.wgig.org/docs/ WGIGREPORT.pdf - página 5

Desde el primer encuentro de the World Summit on the Information Society en el 2003 existe por parte de los actores involucrados la preocupación en mapear las variadas facetas de la gobernanza de Internet, compuesta por asuntos técnicos, políticos, económicos etc. En el informe del Working Group on Internet Governance (WGIG), publicado en el 2005 [19] son identificadas cuatro áreas principales:

1. Cuestiones relacionadas a la infraestructura y gestión de los recursos críticos de Internet, incluyendo la administración del sistema de nombres de dominios (DNS), direcciones de Internet (IPs), administración de los servidores raíz de DNS, estándares técnicos, interconexión, infraestructura de telecomunicaciones y multilingüismo en la

red. Estos, según el informe, son asuntos de directa relevancia para la gobernanza de Internet y acaban por incluir también a las organizaciones por ellos responsables.

2. Cuestiones relacionadas al uso de Internet, incluyendo spam, seguridad y ciber-crímenes.

3. Cuestiones que son relevantes para Internet, pero que el impacto alcanza dimensiones aun mayores fuera de Internet y que para ellas existen organizaciones responsables, como derechos de propiedad intelectual y comercio internacional.

4. Cuestiones relacionadas al propio desarrollo de la gobernanza de Internet, en particular la capacidad de desarrollo en países emergentes.

Las sesiones principales de las 5 primeras ediciones del IGF reflejan también un consenso al respecto de las divisiones temáticas, aunque presenten algunas variaciones en cada evento:

1. Acceso
2. Seguridad (que incluye privacidad y protección de datos)
3. Abertura
4. Diversidad
5. Gestión de los recursos críticos (adicionado en el IGF 2007)
6. Gobernanza de Internet para el Desarrollo (otro acrónimo creado: IG4D - adicionado en el IGF 2010)
7. Computación en nube (adicionado en el IGF 2010 como asunto emergente)

Mientras las clasificaciones temáticas varían, hay un grupo de 40 a 50 cuestiones que permanecen en las ruedas de discusiones de la gobernanza, no obstante, asumiendo nuevas prioridades con el paso del tiempo. Está por ejemplo el tema spam, que en el 2006 era tratado como el principal problema de seguridad en la gran red, mientras que en el 2010 se convirtió en uno de los temas menos debatidos en el área de seguridad. [Kurbalija 2010, pág. 28]

La Diplo Foundation[20], considerando investigaciones realizadas desde 1997, subdivide los temas de la gobernanza en 5 dominios[21] principales:

1. Infraestructura y estandarización
2. Legal
3. Económico
4. Desarrollo
5. Socio-cultural

La figura 2.2 ilustra metafóricamente el intento de consolidar los elementos que componen proceso de gobernanza. Consideramos que el enfoque de Diplo Foundation ofrece un buen recurso didáctico para la comprensión de las cuestiones de la gobernanza de Internet. Utilizaremos los capítulos 3 al 6 de la cuarta edición de la publicación An Introduction to Internet Governance [Kurbalija 2010] como base para las secciones del presente capítulo, profundizando el contenido de temas más pertinentes al propósito de este Guión y a veces suprimiendo aquello que no es tan relevante en nuestro contexto de la investigación de crímenes cibernéticos. Sin embargo, recomendamos la lectura de

este libro, que está disponible online bajo licenciamiento Creative Commons en el sitio Web de la organización. Actualmente existe solamente la versión en idioma inglés, a pesar de que la Diplo Foundation promueva las traducciones.[22]

[20] http://www.diplomacy.edu/ig/default.asp
[21] Originalmente denominados baskets. Demos preferencia al término dominio para designar esta subdivisión temática, que nada tiene que ver con el sistema de nombres de dominios - DNS.

2.3.1 Las cuestiones infraestructura y estandarización en Internet

Este dominio está compuesto principalmente por las cuestiones técnicas relacionadas al funcionamiento básico de la red mundial de computadoras y se divide en dos grupos:

- aspectos fundamentales para el funcionamiento de Internet y de la World Wide Web. Aquí están incluidas tres capas distintas, las cuales se refieren a (1) infraestructura de comunicación; (2) estándares para el funcionamiento de la red (TCP/IP, DNS, etc.) y (3) estándares de contenido y aplicaciones (HTML, XML, etc.).

- aspectos referentes a la seguridad y estabilidad de Internet, como ciber-seguridad, criptografía y spam.

[22] Conforme consta en la publicación, personas interesadas en colaborar con traducciones pueden entrar en contacto por el email diplo@diplomacy.edu

Figura 2.2: Ilustración de la gobernanza de Internet en construcción (www.diplomacy.edu/IG)

La infraestructura de telecomunicación

Esta capa se refiere a los medios físicos de comunicación de datos en Internet, como aquellos vistos en la sección **Conceptos introductorios** de este Guión. Esta infraestructura es regulada en niveles nacionales e internacionales por una serie de organizaciones públicas y privadas.

En el ámbito internacional se destacan aquí dos organizaciones:

• **International Communication Union ITU**: una agencia de las Naciones Unidas que hace "145 años viene coordinando el uso compartido del espectro de radios, promoviendo cooperaciones internacionales acerca del posicionamiento de órbitas de satélites, mejorando la infraestructura de telecomunicaciones en países en desarrollo, estableciendo estándares para incentivar la intercomunicación en la vasta gama de sistemas alrededor del mundo y buscando soluciones para los desafíos de nuestra era, como la atenuación del calentamiento global y el fortalecimiento de la ciber-seguridad."[23]

• Word Trade Organization - WTO: popular en el idioma portugués como Organización Mundial del Comercio (OMC), "lidia con las cuestiones del comercio entre las naciones, a nivel global, o casi global"[24]. La OMC actuó como pieza clave en el proceso de liberalización de los mercados de telecomunicaciones en la década del 90. Este proceso, formalizado en 1998, se caracterizó por la privatización de monopolios

estatales en acuerdo adherido en aquel instante por más de 100 naciones, promoviendo la competición y el establecimiento de agencias nacionales reguladoras.[25]

Al tiempo que a ITU establece estándares técnicos, promueve reglamentos internacionales y ofrece asistencia para países en desarrollo, la WTO trabaja en el ámbito de las reglas generales de mercado.

Las cuestiones involucradas en la capa de infraestructura de telecomunicaciones, de una manera general, incluyen: la viabilización de mayor acceso a Internet al usuario final en los países en desarrollo y en regiones de difícil acceso; la liberalización del mercado de telecomunicaciones en países que dependen de los ingresos generados por los monopolios; y el establecimiento de estándares técnicos internacionales (como por ejemplo el IEEE 802.b, el popular Wi-Fi).

[23] http://www.itu.int/net/about
[24] http://www.wto.org/english/thewto_e/whatis_e/tif_e/fact1_e.html
[25] http://www.wto.org/english/tratop_e/serv_e/4prote_e.html

El Transport Control Protocol/Internet Protocol - TCP/IP

El TCP/IP es considerado el principal estándar de comunicación de Internet. Las especificaciones de esta "pila" de protocolos es responsabilidad del Internet Engineering Task Force y cualquier propuesta de modificación requiere extensos debates y pruebas consistentes de que son soluciones eficientes. Los principios y trabajos del IETF son tratados con más detalles en este Guión en la sección 2.2.

Además de los aspectos estrictamente técnicos que componen las discusiones acerca del TCP/IP, hay una cuestión quien viene siendo tratada con prioridad en los últimos años, que se refiere a la distribución de direcciones IP en Internet. Como fue visto en la sección **1.2 - Conceptos introductorios**, los números IPs deben ser únicos en la red, lo que acarrea una potencial escasez de recursos. Se ve entonces los esfuerzos de adaptación de nuevos protocolos que sean capaces de enfrentar el problema con el menor impacto posible en la estructura actual. Un sumario de este problema y respectivas soluciones en curso son tratados en el presente Guión en la sección **1.2.1 - Conceptos introductorios**.

Modificaciones en el TCP/IP para adopción del protocolo IPv6 acarrean beneficios también en las cuestiones de seguridad, especialmente en virtud de la implementación nativa del IPSec, que ofrece la posibilidad del uso de la criptografía de manera independiente de la aplicación utilizada por el Internauta. Un sumario de este tema puede ser encontrado en el capítulo 7 del artículo " IPv6: la nueva generación de comunicación", publicado en el sitio web del proyecto IPv6.br[26].

El Sistema de Nombre de Dominios – DNS

> *“El hecho es que el proceso original de gobernanza de Internet, que llevó a la creación de la ICANN, resultó en la transformación en mercancía de un bien que debería ser de dominio público, el conjunto de nombres de dominio globales (conocidos por la sigla en inglés gTLDs). Este enfoque fue desgraciadamente seguido por varios países con relación a sus*

> *nombres de dominio de primer nivel de código de país (los ccTLDs, que caracterizan o deberían representar la identidad de un país en Internet). A veces, un ccTLD está en las manos de una empresa particular fuera del país al cual él pertenece (como es el caso del ".tv', de Tuvalu, del ".st', de São Tomé y Príncipe, y varios otros)".*
>
> [Afonso 2005]

Los aspectos técnicos y operacionales del DNS son tratados en la sección 1.3 - CONCEPTOS INTRODUCTORIOS de este Guión. Listamos a continuación algunos elementos que componen cuestiones desafiadoras en otros contextos de la gobernanza de Internet, en lo que se refiere al sistema de nombres de dominios:

[26] http://www.ipv6.br/ipv6/ArtículoNovaGeracaoComunicacaoParte07

- **Problemas en la creación de nuevos Dominios Genéricos de Primer nivel -- gTLDs (universo de los .com, .net, .org, etc.)**. Actualmente existen 22 gTLDs en operación[27]. Corporaciones de protección de marcas han dificultado este proceso, alegando que cada nuevo dominio de primer nivel creado genera dificultades para la protección de sus marcas registradas, esencialmente por la práctica de cybersquatting, que significa el registro de nombre de dominios relacionados a marcas registradas con la intención de lucrar con esto.[28]

- **Registros de nombres de dominios relacionados a contenido**. Aun un asunto pendiente, se trata de decisiones acerca de la creación de gTLDs relacionados a un determinado contenido. Un ejemplo reciente de este problema se refiere a la creación del gTLD .xxx, reservado para "entretenimiento adulto". En marzo del 2007 esta propuesta fue rechazada por la ICANN, que revertió la decisión en el 2010, aprobándolo finalmente el 18 de marzo de este año. Hubo gran presión internacional en el sentido de que la ICANN, al rechazar la propuesta en el 2007, estaba subordinándose al gobierno de los Estados Unidos, que se declaró también contrario, apoyado por diversos países, incluyendo Brasil, según [Kurbalija 2010, pág. 43].

Se ven aun indefiniciones de políticas que establezcan criterios (principalmente políticos) para ubicación de ccTLDs (nombres de dominio para países); cTLDs para idiomas específicos; y nombres de dominios multi-lingüísticos. Este último ha sido implementado en la forma de Internationalized Domain Names (IDNs) y es considerada una gran conquista del régimen actual de gobernanza de Internet.[29]. La figura 2.3 ilustra el acceso al sitio web de la ICANN dedicado a las discusiones sobre el IDN, en el idioma hindi, que utiliza el alfabeto devanagari.

[27] Una tabla descriptiva de estos TLDs está disponible en http://www.icann.org/en/registries/listing. html
[28] Es a veces referido como ciber-especulación en idioma español. Una definición detallada de esta actividad puede ser vista en http://en.wikipedia.org/wiki/Cybersquatting.

Figura 2.3: Ejemplo del Internationalized Domain Name en funcionamiento en idioma hindi. Imagen retirada de http://blog.icann.org/2010/05/idn-usability/

Los servidores DNS raíz

Resumiendo lo que fue abordado en el capítulo CONCEPTOS INTRODUCTORIOS, tenemos que el Sistema de Nombre de Dominios (DNS) está básicamente compuesto por:

[29] http://idn.icann.org/

- servidores DNS raíz (DNS root servers)
- servidores de Dominios de Primer Nivel (Top Level Domains - TLDs)
- otros servidores DNS de niveles inferiores distribuidos por el planeta

Los servidores raíz son los equipos conectados a Internet que están en la cima de la jerarquía del DNS, o sea, son los primeros a ser consultados ante una requisición de conversión de dirección IP para nombre de dominio en Internet, además de delegar autoridad para los servidores en el nivel inferior que gestionan los TLDs (o sea, los dominios de primer nivel como .org, .com, .net, .us, .br, etc.).[30]

Una cuestión polémica que fue puesta en debate en los últimos forums trata de la autoridad del gobierno de los Estados Unidos sobre la mayor parte de los servidores raíz del DNS (DNS root servers), por medio de su Departamento de Comercio. De los 13 servidores raíz existentes, 10 son originalmente asignados en territorio norteamericano. Los otros 3 están en Suecia, Holanda y Japón. Por tanto, si por ejemplo dos de los 13 servidores fallan simultáneamente, los otros 11 estarán aptos para asumir el funcionamiento del DNS sin mayores problemas.[31]

Adicionalmente, una técnica de distribución geográfica en los servidores raíz fue adoptada, de forma que los datos son constantemente replicados para diversos servidores disponibles en diferentes localidades.[32]

[30] Ver sección 1.3.3 y figura 1.4 para más detalles acerca de los conceptos de TLD, ccTLD, gTLD etc.
[31] En la práctica, millares de otros servidores DNS en Internet poseen copias de los datos de los servidores raíz, de forma que una catástrofe de consecuencias prácticas en este sistema sea algo difícil de imaginar.

Según el informe de la Packet Clearing House Report[33] actualizado el 4 de mayo de 2011, existen 69 países que hospedan servidores DNS raíz (cantidad posible en virtud de la utilización del anycast), donde 59 están en los Estados Unidos. El mapa suministrado por esta organización, presente en la figura 2.4 de este Guión, ilustra la distribución de estos servidores alrededor del mundo. Este mapa, así como el referido informe, completo y actualizado, puede ser consultado en el sitio web de la PCH.[34]

Figura 2.4: Distribución de servidores DNS raíz alrededor del mundo - imagen bajo licenciamiento Creative Commons Sampling Plus por la PCH

A pesar de la robustez técnica ofrecida por el sistema de nombre de dominios en Internet y de que el mantenimiento de los servidores es realizado por representantes de diversos sectores, se tiene que la gestión del archivo raíz (que posee los datos replicados en todos los servidores raíz) está bajo responsabilidad de Internet Assigned Numbers Authority (IANA), operada por la Internet Corporation for Assigned Names and Numbers (ICANN). Las organizaciones que mantienen los servidores raíz reciben de la IANA las actualizaciones propuestas, que a su vez deben ser autorizadas por el Departamento de Comercio de los Estados Unidos antes de ser automáticamente

replicadas para todo el sistema. Ante tal hecho, se han notado preocupaciones por parte de algunos países que consideran la posibilidad de confronto con eventuales decisiones unilaterales del gobierno americano en este asunto.

[32] Para saber más sobre esta tecnología, conocida por anycast, consulte la RFC 4786 disponible en http://tools.ietf.org/html/rfc4786
[33] http://www.pch.net/home/index.php
[34] https://prefij.pch.net/applications/ixpdir/summary/rootservers/

Hay actualmente algunas propuestas concretas en lo que se refiere al problema de la gestión centralizada de los servidores DNS raíz por los Estados Unidos, especialmente después de la firma de un Affirmation of Commitments entre la ICANN y el Departamento de Comercio de los Estados Unidos, que trajo la posibilidad de algunas reformas en el modelo actual, como la internacionalización de la ICANN y la transferencia de la palabra final en relación al archivo DNS raíz para esta organización.[35]

Neutralidad de la red

El éxito de Internet es atribuido en gran parte al carácter imparcial en el tratamiento de las informaciones transmitidas entre los pares de la red. El concepto de la neutralidad es simple, a pesar de que las consecuencias de esta característica sean bien abarcadoras. En junio del 2006, Tim Berners-Lee, el inventor de la Web, esclarece algunos puntos acerca de la neutralidad en manifestación publicada en su blog[36]. A continuación aparecen algunos fragmentos, en traducción libre:

[35] http://www.icann.org/en/announcements/announcement-30sep09-en.htm. Un análisis de este acuerdo puede ser consultado en http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1744086
[36] Net Neutrality: This is serious - http://dig.csail.mit.edu/breadcrumbs/node/144

> *"Control de información es algo poderosísimo. En los Estados Unidos, la amenaza es que empresas controlen lo que yo puedo acceder por razones comerciales. (en China, el control es en virtud de las razones políticas)..."*
>
> *"Neutralidad no es pedir Internet gratis"*
>
> *"Si, regulación para mantener la Internet abierta es regulación. Y principalmente, Internet se ha desarrollado sin regulación. Pero algunos valores básicos deben ser preservados. Por ejemplo, el mercado depende de la regla que usted no puede fotocopiar cédulas de dinero. La democracia depende de la libertad de expresión. La libertad de conexión con cualquier aplicación y para cualquier lugar es la base social fundamental de Internet, y, ahora, la sociedad está basada en ella."*

En suma, la neutralidad de la red se refiere a la manutención de un modelo en que no se aplica ninguna restricción o beneficio al flujo de datos en virtud de uno u otro contenido transmitido. Según [Kurbalija 2010, pág. 48], paradójicamente, el principio de la neutralidad nunca fue estrictamente aplicado en Internet. El argumento del autor es que los operadores de la red (empresas de telecomunicación y proveedores de acceso)

utilizan diversos artificios técnicos para priorizar ciertos tipos de tráfico. Por ejemplo, un servicio de VoIP (voz sobre IP) como el Skype no puede tolerar atrasos en la transmisión de los datos, mientras el atraso de algunos segundos en el recibimiento de un email no será notado por el remitente y destinatario.

Mientras algunos puristas en este tema defienden el tratamiento igualitario de los bits transitados, donde hay clara oposición incluso con relación a las técnicas más inofensivas de **QoS** (calidad de servicio), los operadores de red argumentan que para que los usuarios gocen igualitariamente de los servicios en Internet es necesario que ciertos tipos de tráfico sean tratados de maneras distintas. El problema está en la zona limítrofe entre el uso justificado de técnicas de control de tráfico y la manipulación fundamentada en cuestiones políticas y/o comerciales.

Un caso que se volvió bastante popular en este asunto incluye a un gran proveedor de acceso a Internet de los Estados Unidos, Comcast, que durante años redujo la capacidad de transferencia de datos de sus clientes para determinadas aplicaciones P2P (par a par)[37]. Tal hecho promovió debates aun más intensos acerca de la neutralidad de Internet a lo largo de los últimos años. En diciembre del 2010 la FCC (Federal Communications Commission) finalmente adoptó reglas que dificultarán esta práctica, al prohibir que empresas de telecomunicaciones y proveedores de acceso favorezcan o perjudiquen el tráfico de datos con base en el contenido transitado.[38]

[37] Comcast v the FCC - http://www.economist.com/node/15867976
[38] Divided FCC Adopts Rules to Protect Web Traffic - http://www.cbsnews.com/stories/2010/12/21/ tech/ main7171081.shtml

La computación en nube

El "término computación en nube" o "computación en las nubes" es utilizado para describir un modelo de utilización de computadoras que ya no depende de recursos locales para que tareas rutinarias sean ejecutadas. En la práctica, esto se refiere a la posibilidad de accesar nuestros emails de cualquier lugar, sin depender de softwares específicos (lo que no es novedad). Lo mismo de gerenciar por completo nuestros archivos personales, que pasan a ser almacenados en computadoras esparcidas por el mundo, mantenidas por empresas que ofrecen recursos de criptografía, sistemas de backups e incluso softwares Web con características semejantes de un sistema operativo completo, para que el Internauta esté apto para acceder a su ambiente de trabajo desde cualquier lugar que ofrezca acceso a Internet. Digamos que esta es la gran novedad que trae el término.

En [Kurbalija 2010, pág. 64] son listadas las siguientes preocupaciones que la computación en nube ha despertado en los forums de gobernanza de Internet, las cuales resumimos a continuación:

• La computación en nube tiende a aumentar la dependencia que ya es notoria de los individuos en relación a Internet. Si hace algunos años las personas estaban imposibilitadas de verificar email y navegar en websites de noticias cuando Internet estaba inaccesible, hoy puede ocurrir la imposibilidad de realizar cálculos y escribir artículos (ej: Google Docs). Tal dependencia, inevitable, debe ser acompañada de medidas que garanticen la estabilidad de la gran red, lo que puede demandar participación más activa de los gobiernos.

- ¿Cómo quedan las cuestiones de la protección de datos y privacidad, una vez que nuestros datos están en la posesión de organizaciones privadas esparcidas por el mundo, sometidas a las más diversas legislaciones (o falta de ellas) sobre este tema? ¿Cuáles son las oportunidades de que los internautas pierdan el control sobre sus propias informaciones? ¿Las empresas proveedoras de la "nube" utilizarán datos personales para que propósitos?

- Algunos vislumbran la posibilidad de la creación de "nubes" locales, ante la incomodidad que puede existir por parte de algunos gobiernos, ante la posibilidad de que datos sensibles de sus ciudadanos o del propio Estado estén en posesión de empresas localizadas en otros países. Para empeorar la situación, se tiene que los grandes operadores de "nubes" están situados en los Estados Unidos, trayendo a la luz los mismos problemas ya tan debatidos acerca de la (des)centralización de la ICANN, organización de extrema relevancia en la manutención de Internet que aun se encuentra sometida al gobierno americano.

- Cuestiones incluyendo estándares abiertos para que sea posible la interconexión entre las diversas "nubes" (ej: computadoras de Google conectándose con computadoras de Amazon) están en discusión.

Ciber-seguridad

Internet nació de un proyecto en el cual no se veían razones para preocuparse con cuestiones más críticas de seguridad. Con el pasar de los años Internet pasó a ejercer un papel fundamental en las tareas rutinarias y a veces críticas de la vida moderna. Redes eléctricas, sistemas de transportes, servicios de salud, etc., dependen hoy del buen funcionamiento de la gran red, que consecuentemente se convierte en blanco frecuente de lo que llamamos "ciber-ataques."

[Kurbalija 2010, pág. 66] sugiere una clasificación de los ataques cibernéticos de acuerdo con los siguientes criterios:

- **Tipo de acción**: son por ejemplo interceptación de datos, acceso ilegal a contenido privado, negación de servicio (DoS), robo de identidad, diseminación de virus y malwares en general, phishing scam, spam, etc.

- **Tipo de criminal**: esencialmente se refiere a la motivación del crimen. En este ítem el autor cita ciber-terroristas y equivocadamente utiliza el término hacker para designar un tipo de ciber-criminal, cuando lo mejor sería utilizar el término cracker.[39]

- **Tipo de blanco**: individuos, empresas privadas, gobiernos, infraestructuras críticas etc.

Con el objetivo de suplir las lagunas en lo que se refiere a la seguridad en la infraestructura de Internet, organizaciones de amplitud internacional como la International Telecommunication Union (ITU) y la IETF han desarrollado una serie de estándares técnicos y recomendaciones para el uso más seguro de la red.

Una referencia actual - aunque bastante controvertida - en el tema de la ciber-seguridad, es la Convention on Cybercrime, popular en el idioma español como Convención Internacional sobre Ciber-crimen, o Convención de Budapest. Esta convención es el primer tratado que aborda el asunto en el ámbito internacional, en el intento de armonizar legislaciones y promover cooperación entre naciones en el enfrentamiento de los crímenes cibernéticos. Entre los crímenes abordados en la Convención están la infracción de copyright, fraudes en Internet, violaciones de sistemas de seguridad, pornografía infantil y los crímenes de odio. Incluye además una serie de poderes a las autoridades, como procedimientos de rastreo, búsqueda y aprehensión de computadoras, e interceptación telemática.

[39] http://en.wikipedia.org/wiki/Hacker_definition_controversy#Hacker_definition_controversy

Un párrafo presente en el sitio Web de la UNESCO resume los primeros pasos de este tratado (traducción libre):

> *"El 18 de marzo del 2004, Lituania ratificó la Convención Internacional sobre Ciber-crimen, haciendo que este instrumento entre en vigor el 1 de julio de 2004. La Convención y su Informe Explicativo fueron adoptados por el Comité de Ministros del Consejo de Europa en su 109ª Sesión (8 de noviembre de 2001). Él fue abierto para firmas/ adhesiones en Budapest, el 23 de noviembre de 2001, como uno de los asuntos tratados en la Conferencia Internacional de Ciber-crimen. Fue requerido que hubiesen 5 ratificaciones, incluyendo 3 Estados miembros del consejo de Europa para que entrase en vigor".*

Actualmente la Convención Internacional sobre Ciber-crimen cuenta con 22 signatarios. Los países que firmaron el tratado son: Albania, Armenia, Bosnia y Herzegovina, Bulgaria, Chipre, Croacia, Dinamarca, Eslovaquia, Eslovenia, Estados Unidos de América, Estonia, Finlandia, Francia, Hungría, Islandia, Letonia, Lituania, Macedonia, Noruega, Países Bajos, Rumania y Ucrania.

En Brasil, los debates acerca de la adhesión aun causan cierta polémica. Por un lado, hay iniciativas en el congreso, incluyendo proyectos de ley y la explícita recomendación de la Comisión Parlamentaria de Indagación para investigación de pedofilia en Internet (CPI de la Pedofilia, Senado Federal). De manera general, la adhesión recibe apoyo de autoridades brasileñas, conforme ilustran los siguientes fragmentos extraídos del informe final de actividades de la CPI de la Pedofilia del Senado, publicado en el 2010[40]:

> *"La Policía Federal ha participado de encuentros internacionales, pero el Ministerio de las Relaciones Exteriores no. Ya yo, por más de una vez, ya provoqué al Ministerio de las Relaciones Exteriores en este sentido, en el sentido de que Brasil haga adhesión a la Convención de Budapest, que trata de este asunto cibernético como un todo, como ellos llaman, los países de Europa todos ya firmaron, los Estados Unidos, Canadá,*

> *Japón; en América Latina, México y Costa Rica también ya se pronunciaron y Brasil, no". - pág. 15, pronunciamiento del Senador Eduardo Azeredo, en sesión de apertura de la CPI.*
>
> *"De una forma general, la Policía Federal apuntó el texto de la Convención Europea, referido en el ítem 3.2.2 de este Informe, como uno de los caminos para resolver los obstáculos a las investigaciones a los crímenes cibernéticos en Brasil." - pág. 152*

[40] http://www.senado.gov.br/noticias/agencia/pdfs/RELATORIOFinalCPIPEDOFILIA.pdf

El Informe apunta consideraciones acerca de una posible adhesión de Brasil al tratado:

> *"Sobre la posibilidad de que Brasil se vincule a la Convención, recordamos lo siguiente: (i) Brasil no es miembro del Consejo de Europa, no participó de la producción del texto convencional y no goza del status de observador ante el Consejo; (ii) la Convención está abierta a la firma de los Estados-miembros del Consejo, así como de los no miembros que participaron de su elaboración (Sudáfrica, Canadá, Japón, Montenegro y Estados Unidos de América); y (iii) la Convención dispone sobre la posibilidad de que el Comité de Ministros del Consejo de Europa (órgano de decisión política más elevado que congrega a los cancilleres de los países miembros) invite a cualquier otro Estado para vincularse al tratado, después de la obtención del consentimiento unánime de los Estados contratantes de la Convención (art. 37) 157." - pág. 306*

No obstante, la posición del Ministerio de las Relaciones Exteriores, al menos hasta la fecha de publicación del Informe de la CPI, no comparte del mismo entusiasmo expresado por los miembros de la Comisión al respecto de la adhesión de Brasil a la convención europea, conforme expresado en el fragmento siguiente:

> *"La respuesta fue enviada por el Oficio número 16 AFEPA/SGAPI/PARL, subscrito por el entonces Ministro de las Relaciones Exteriores Interino Samuel Pinheiro Guimarães. En suma, fue informado que, a pesar de haber estudios sobre el tema en varias unidades del MRE, este no manifestó, hasta aquel momento, "intención de proponer la adhesión del país a aquella Convención". Según el MRE, "las reservas previstas en algunos de los artículos de la Convención fragilizarían y comprometerían la eficacia de la cooperación internacional en la prevención y combate a los crímenes cibernéticos, a la luz de su característica transnacional". Desde el ángulo político, además, como Brasil no participó de las negociaciones de la Convención, no habría sido posible "incluir las percepciones brasileñas en el tratado, que, por otra parte, fue elaborado para permitir casi total compatibilidad con las leyes vigentes en*

> *algunos de los países que participaron de las negociaciones, para disminuir la necesidad de ser efectuadas adaptaciones de los respectivos derechos internos". Esta Comisión comprende, de todos modos, ser relevante para el País la adhesión a los términos de la Convención de Budapest sobre Ciber-crimen, razón por la cual envía recomendación en este sentido al final de este Informe." - págs. 315 y 316*

Es oportuno destacar que el Informe Final de la CPI de la Pedofilia, compuesto por 1696 páginas, es un valioso recurso para la comprensión del problema en Brasil, una vez que comprende una serie de transcripciones de audiencias públicas y sesiones oficiales de la Comisión, reuniendo datos estadísticos, opiniones, desafíos, avances y propuestas en curso manifestados por diversas instituciones públicas y privadas en Brasil acerca del tema de la seguridad en Internet y otros aspectos de la gobernanza.

Como ya fue mencionado anteriormente, la adhesión de Brasil a la Convención sobre Ciber-crímenes, propuesta que caminó lado a lado con algunos proyectos de ley aun en tramitación en el Congreso, despertó fuerte oposición de la sociedad civil, simbolizado por diversos actos públicos, manifestaciones en la blogósfera y finalmente por las más de 160 mil firmas presentes en una petición online, donde se destacan los siguiente fragmentos:

> *"Un proyecto de Ley del Senado brasileño quiere bloquear las prácticas creativas y atacar a la Internet, haciendo más rígidas todas las convenciones del derecho autoral. El Sustitutivo del Senador Eduardo Azeredo quiere bloquear el uso de redes P2P, quiere liquidar con el avance de las redes de conexión abiertas (Wi-Fi) y quiere exigir que todos los proveedores de acceso a Internet se conviertan en delatores de sus usuarios, colocando a cada uno como un probable criminal."*
>
> *"Por estas razones nosotros, que firmamos a continuación, investigadores y profesores universitarios apelamos a los congresistas brasileños para que rechacen el proyecto Sustitutivo del Senador Eduardo Azeredo al proyecto de Ley de la Cámara 89/2003, y Proyectos de Ley del Senado 137/200O, y n. 76/200O, pues atenta contra la libertad, la creatividad, la privacidad y la diseminación de conocimiento en la Internet brasileña." 41*

Hasta la presente fecha los debates continúan pendientes, los proyectos de ley aun tramitan en el Congreso y Brasil no es signatario de la Convención de Budapest.

Spam

En pocas palabras, se puede definir el spam como un mensaje de email no solicitado, de carácter impersonal, enviado a un gran número de destinatarios. De una manera general, spams son objetos de promoción comercial, pero frecuentemente son usados como un medio eficiente para difusión de campañas políticas, activismos, o incluso para fines ofensivos y prácticas criminales como los phishing scams.

Según la organización SpamHaus[42], aproximadamente 90% de los emails que circulan en Internet son spams (información suministrada por proveedores de acceso de América del Norte, Europa y Australia). En el ámbito técnico, este hecho demanda de los administradores de sistema la habilidad de implementar filtros anti-spam sin perjuicio de recibir emails legítimos, así como mantener los servicios en buen funcionamiento, evitando eventuales atrasos en la entrega de los mensajes en virtud del alto procesamiento requerido por los mecanismos de filtrado. Para los gestores y ejecutivos, el desafío está en mantener esta estructura sin gastar demasiados recursos de su organización.[43]

[41] Por el veto al proyecto de ciber-crímenes. En defensa de la libertad y del progreso del conocimiento en la Internet Brasileña: http://www.petitiononline.com/veto2008/petition.html
[42] http://www.spamhaus.org/

Otro frente de combate al spam emerge también en el ámbito legal. Algunos países ya poseen leyes anti-spam. En los Estados Unidos, desde diciembre del 2003 está en vigor el Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003, también conocido como "acto CAN-SPAM". La Oficina de Protección al Consumidor en los Estados Unidos alerta que cada email enviado que incumpla esta ley puede incurrir en multas de hasta 16 mil dólares. La misma oficina ofrece una guía para que las empresas utilicen sistemas de correo directo con los cuidados necesarios para que no haya ninguna infracción de acuerdo con el CAN-SPAM.[44]

Según [Kurbalija 2010, pág. 71], no hay evidencias de que hubo ninguna reducción en el número de mensajes indeseados desde la implantación de esta ley en los Estados Unidos.

La Unión Europea también posee una ley anti-spam como parte de su Directiva sobre Privacidad y Comunicaciones Electrónicas [45]. Esta ley promueve la auto-regulación e iniciativas del sector privado para el enfrentamiento del problema. [46]

[43] La SpamHaus suministra una breve guía para implementar una solución utilizando softwares libres en http://www.spamhaus.org/whitepapers/effective_filtering.html
[44] http://business.9c.gov/documents/bus61-can-spam-act-compliance-guide-business
[45] http://en.wikipedia.org/wiki/Directive_on_Privacy_and_Electronic_Communications
[46]http://ec.europa.eu/information_society/policy/ecomm/todays_framework/privacy_protection/spam/index_en.htm

En Brasil no existen leyes específicas para el combate al spam, a pesar de que haya por parte de algunos, el entendimiento de que hay como encuadrar esta actividad en otros dispositivos legales.[47] Una búsqueda por palabras clave acerca del tema en el sitio Web del Senado Federal[48] informa la existencia de 3 proyectos de ley en este sentido, todos en la situación "11/01/2011 - ARCHIVADA AL FINAL DE LA LEGISLATURA":

- PLS 21/2004 del 02/03/2004: "Disciplina el envío de mensajes electrónicos comerciales."
- PLS 36/2004 del 10/03/2004: "Dispone sobre mensajes no solicitados en el ámbito de la red mundial de computadoras (Internet)."
- PLS 367/2003 del 28/08/2003: "Cohíbe la utilización de mensajes electrónicos comerciales no solicitados por medio de red electrónica."

En la Cámara de los Diputados hay 10 ocurrencias de proyectos de ley que tratan del problema del spam, siendo que 1 fue archivado y 9 aun tramitan en la casa (6 anexados). Más detalles pueden ser verificados en el sistema Web de investigación de la Cámara.[49]

Aun en el nivel nacional, Brasil cuenta con iniciativas de la Comisión de Trabajo Anti-spam del CGI.br[50], que tiene como objetivos "**Recomendar procedimientos tecnológicos para el combate al Spam; disponer informaciones sobre spam para los diferentes actores; recomendar códigos de conducta para empresas, usuarios y administradores de red; recomendar proyectos de ley para el poder legislativo; y promover articulación internacional sobre el tema**". Esta comisión mantiene un sitio Web informativo sobre spam, el AntiSpam. br[51], que aborda de manera bastante didáctica el asunto, posibilitando al lector una fácil comprensión del problema y los actuales medios de enfrentamiento, además de curiosidades, como la interesante historia del surgimiento del término spam, en la década del 70, influenciada por una de las escenas del programa Monty Python's Flying Circus TV Show.[52]

[47] Por ejemplo, el artículo "Spam: Violaciones, Ilicitudes, Contravenciones y Crímenes", disponible en http://www.conteudojuridico.com.br/?artículos&ver=2.23643 trata del asunto, refiriendo otros diversos argumentos en este tema.
[48] http://www.senado.gov.br/atividade/materia/
[49] http://www.camara.gov.br/sileg/default.asp
[50] http://www.cgi.br/acoes/antispam.htm

A pesar de que el spam aun sea considerado una de las mayores plagas de Internet, el tema dejó de ser el centro de las atenciones en los debates sobre seguridad en los forums de gobernanza. Cuestiones como fraudes financieros, "ciber-terrorismo", crímenes de odio, pornografía infantil, privacidad y protección de datos son preocupaciones en mayor evidencia últimamente.

Aspectos legales de la gobernanza de Internet

Los aspectos legales están presentes en casi todos los asuntos de la gobernanza de Internet, lo que no significa que el asunto no sea abordado, por si sólo, como un macro-tema independiente y dotado de peculiaridades, controversias y acalorados debates a lo largo de los años.

Por un lado, hay quien defiende la hipótesis de que Internet, considerada una evolución natural de los métodos tradicionales de comunicación, no trae novedades significativas en el ámbito de las relaciones humanas (al menos en lo que se refiere a las reglas de comportamiento sociales), de manera que la legislación que trata de los asuntos habituales debe abarcar igualmente los derechos y deberes en el ámbito de la gran red. O sea, si hay una falla en este sentido, esta no está en la carencia de legislación específica, sino en la inconsistencia de las leyes que tratan de instrumentos legales ya consolidados como contratos, términos de responsabilidad, etc.

[51] http://antispam.br/
[52] http://antispam.br/historia/

El juez norteamericano Frank H. Easterbrook[53] publicó un artículo durante el University of Chicago Legal Forum, datado de 1996, denominado "Cyberspace and the Law of the Horse" (Ciberespacio y la Ley del Caballo), en el cual defiende la tesis de que tal como no tiene sentido establecer una ley específica para cuidar de cuestiones de caballos, no

se debe perder tiempo con leyes para el ciberespacio, sino enfocarse en otros frentes más genéricos, de forma que por fin el ciberespacio pueda beneficiarse de estos esfuerzos.[54]

La siguiente citación es utilizada por Easterbrook para basar su pensamiento, siendo de autoría de otro reconocido académico en el área del derecho en los Estados Unidos, Gerhard Casper[55]: (traducción libre):

> *"...la mejor manera de comprender la ley aplicable a la conductas específicas es estudiar las reglas generales. Varios casos lidian con venta de caballos; otros lidian con personas pateadas por caballos; hay además más casos que lidian con licenciamiento y carrera de caballos, o con los cuidados dados a los caballos por los veterinarios, o con los premios ofrecidos en shows con caballos. Cualquier esfuerzo para reunir estas vertientes en una única dirección tal como una "Ley del Caballo" estará condenado a ser superficial y carecer de los principios unificadores."*

[53] http://en.wikipedia.org/wiki/Frank_H._Easterbrook
[54] http://www.law.upenn.edu/fac/pwagner/law619/f2001/week15/easterbrook.pdf
[55] http://en.wikipedia.org/wiki/Gerhard_Casper

Por otro lado, esta teoría es desafiada por otros diversos autores, como Lawrence Lessig que, en un artículo de 46 páginas denominado "The Law of the Horse: What Cyberlaw Might Teach" ("La ley del caballo: lo que una ley del ciberespacio puede enseñar"), propone una reflexión acerca de los límites del poder y los eventuales beneficios en leyes específicas para el ciberespacio.[56]

En [Kurbalija 2010, págs. 81 a 86] son citados una serie de instrumentos legales ya existentes que son - o pueden venir a ser - aplicados en la gobernanza de Internet, clasificados de la siguiente manera:

• Nacionales:
- Legislación
- Normas sociales
- Auto-regulación
- Jurisprudencia

• Internacionales:
- Derecho internacional público
- Derecho internacional privado
- Convenciones internacionales
- Derecho internacional consuetudinario
- Soft law o instrumentos "casi-legales"
- Jus cogens

[56] http://www.lessig.org/content/articles/works/finalhls.pdf

Copyright y derechos de la propiedad inmaterial

Es evidente que Internet modificó la forma y la aplicación de los derechos de copia tradicionales. Las leyes que protegen la expresión de una idea materializada (CD, libro, etc.) no suministran - de una manera general - una clara distinción entre la propia idea y su expresión, algo fundamental para abordar lo que sería elegible para las restricciones de acceso en el mundo intangible de los bits.

El gran desafío en este tópico está en la búsqueda de la justa medida entre los derechos del autor y el interés público. Se ve claramente una asimetría de poderes al analizar la proactividad de representantes de las dos partes. Por un lado, la gran industria del entretenimiento y producción de contenido actúa en los más variados frentes en defensa de sus intereses económicos. En el otro lado se notan, de forma aun tímida, sin embargo constante en ascendencia, iniciativas globales en busca del libre acceso al conocimiento y a la información, representadas por la propia sociedad civil y eventualmente por los gobiernos.

Un marco histórico en este tema fue la creación del Digital Millennium Copyright Act (DMCA)57, una ley de los Estados Unidos que implementa dos tratados de la World Intellectual Property Organization (WIPO) y que "criminaliza no sólo la infracción del derecho autoral en si, sino también la producción y la distribución de tecnología que permita evitar medidas de protección de los derechos de autor. Además de esto aumenta las penas por infracciones de derechos autorales en Internet. "[58]

[57] http://thomas.loc.gov/cgi-bin/query/z?c105:H.R.2281

Un artículo publicado por el grupo de trabajo sobre derechos de propiedad intelectual de la oficina de marcas y patentes de los Estados Unidos sugiere que son suficientes solamente pequeños ajustes en las leyes de copyright para llenar las lagunas que surgieron con la llegada de Internet.[59] Según los autores, se debe dedicar esfuerzos para "desmaterializar" los conceptos actuales de fijación, distribución, transmisión y publicación de las obras, dado el carácter no escaso de la información en medio digital. El fragmento siguiente ilustra un poco las preocupaciones encontradas (traducción libre):

> *"Una transmisión, por si sola, no es una fijación. Mientras que una transmisión puede resultar en una fijación, una obra no es fijada como consecuencia de una transmisión. Por tanto, transmisiones "en vivo" por medio de la Infraestructura Nacional de Información (NII) no atenderán las exigencias de fijación, y estarán desprotegidas por la ley de derechos autorales (Copyright Act), al menos que la obra sea fijada (grabada) en el mismo instante en que está siendo transmitida. La ley de derechos autorales dice que una obra "consistiendo de sonidos, imágenes o ambos, siendo transmitidos" atienden los requisitos de fijación solamente "si una fijación de la obra está siendo realizada simultáneamente con su transmisión." [...]"*

[58] http://pt.wikipedia.org/wiki/Digital_Millennium_Copyright_Act
[59] Intellectual Property and the National Information Infrastructure: http://www.uspto.gov/web/ offices/ com/doc/ipnii/

Este documento ha influenciado los principales tratados internacionales concernientes a cuestiones de derechos autorales, incluyendo el Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)[60] de la Organización Mundial del Comercio y convenciones de la World Intellectual Property Organization (WIPO)[61].

Además en el ámbito de la protección de los "bienes inmateriales" se ven debates acalorados acerca de temas no tan recientes, como los límites del uso justo (fair use) de una obra protegida, registro de marcas (principalmente cuando involucra nombres de dominios en Internet) y razonabilidad de criterios para la concesión de patentes.

2.3.3 Internet y derechos humanos

Dentro del dominio que [Kurbalija 2010] designa como cuestiones socio-culturales de la gobernanza de Internet, se encuentra mayoritariamente el tema de los derechos humanos - y como estos han sido resguardados (o violados) en la gran red.

Tal como visto en el tópico anterior, que aborda el impacto de Internet en los sistemas legales, es de imaginar que la discusión en el tema de los derechos humanos siga un camino semejante. Y de hecho es lo que ocurre. Reflexiones acerca de los "derechos reales" versus "derechos virtuales" han emergido con notorio destaque en los últimos forums de gobernanza de Internet.

[60] http://www.wto.org/english/tratop_e/trips_e/trips_e.htm
[61] http://www.wipo.int/treaties/en/

Listamos a continuación algunas iniciativas y organizaciones comprometidas en este debate:

- La **Coligación Dinámica de Derechos y Principios de Internet (IRP)**, "que es una red abierta de individuos y organizaciones que trabajan para defender los derechos humanos en el mundo de Internet", compiló en un documento los **10 Derechos y Principios de Internet**. Según la organización, "estos principios están enraizados en las normas internacionales de derechos humanos, y se derivan de la Carta de Derechos Humanos y Principios Para Internet en elaboración por la Coligación."[62]

- La **Asociación para el Progreso de las Comunicaciones (APC)** es "una red global de redes cuya misión es empoderar y apoyar organizaciones, movimientos sociales e individuos en el uso de la información y de las tecnologías de la comunicación (TIC)."[63] Aun en elaboración, la **Carta de los Derechos Humanos y Principios para Internet** de la IPR está inspirada en la Carta de los Derechos de Internet de la APC, disponible actualmente en 20 idiomas.[64]

- La **Global Network Initiative (GNI)** es una iniciativa que cuenta con la representación de grandes corporaciones privadas en su cuerpo director, como Google, Microsoft y Yahoo, además de organizaciones sin fines lucrativos, inversionistas y académicos. El objetivo de la GNI es promover internacionalmente algunos principios en el ámbito de los derechos humanos, como libertad de expresión y privacidad.[65]

[62] http://Internetrightsandprinciples.org/node/402
[63] http://www.apc.org/pt-br
[64] http://www.apc.org/en/pubs/about-apc/apc-Internet-rights-charter-download

• Por ser la organización mantenedora de la **Convención para la protección de los Derechos humanos y de las libertades fundamentales** [66] de 1950, el **Consejo de Europa** está ejerciendo un papel importante en lo que se refiere al tema cuando es tratado en el ámbito en Internet. Como ejemplos podemos destacar la **Declaración sobre la libertad de comunicación en Internet** del 2003 [67] y la **Declaración sobre Derechos Humanos y el Estado de Derecho en la Sociedad de la Información** del 2005.[68]

Regulación de contenido en Internet

Los intentos de regular la publicación de contenido en la gran red es un asunto que implica directamente en debates acerca de los derechos de libertad de expresión y de comunicación. Por tanto, se reflejan en los forums de gobernanza los mismos conflictos aun no resueltos al respecto de los límites de lo que debe ser cohibido, y cuales son los medios a ser adoptados para tal práctica.

Según [Kurbalija 2010, pág. 136], las discusiones se concentran generalmente en tres grupos de contenido:

1. Contenido que presenta un consenso global acerca de la necesidad de ser controlado, como la pornografía infantil, justificaciones para genocidios, incitación a actos terroristas etc.

[65] http://www.globalnetworkinitiative.org
[66] http://conventions.coe.int/Treaty/en/Summaries/Html/005.htm
[67] https://wcd.coe.int/wcd/ViewDoc.jsp?id=37031
[68] https://wcd.coe.int/wcd/ViewDoc.jsp?id=849061

2. Contenido sensible para algunas naciones, regiones o grupos étnicos en particular, debido a valores peculiares - culturales y religiosos, por ejemplo. Se cita aquí el acceso a la pornografía adulta y juegos de azar online.

3. Censura política en Internet. La organización Reporteros sin Fronteras mantienen en su sitio Web una sección que trata exclusivamente de lo que consideran como "Los enemigos de Internet."[69] En la presente fecha están listados 10 países considerados "enemigos" y otros 16 en "vigilancia". Los criterios utilizados por la ONG y las razones por las que colocaron a cada país en estas listas son expuestas en detalles en un informe accesible en la misma dirección. El siguiente fragmento resume un poco la situación actual (traducción libre):

> *"El año 2010 consolidó el papel de las redes sociales y de Internet como herramientas de movilización y transmisión de noticias, especialmente durante la primavera Árabe. Los nuevos y los tradicionales medios de comunicación se muestran cada vez más complementarios. No obstante, los regímenes represivos han intensificado la censura, la propaganda y la represión, manteniendo a 119 internautas en la prisión. Cuestiones tales como seguridad nacional - relacionadas a las publicaciones de Wikileaks - y la propiedad intelectual están desafiando a países democráticos a apoyar la libertad de expresión online".*

[69] http://march12.rsf.org/en/#ccenemies

Los medios de control

Los medios utilizados para controlar el acceso a determinados contenidos en la red son variados y pueden combinar métodos estrictamente técnicos con dispositivos legales ya existentes en cada país. A continuación aparecen ejemplos de las prácticas más populares actualmente, aunque algunas sean consideradas exageradas por muchos:

• **Filtros de contenido de responsabilidad del gobierno**: utilizando recursos tecnológicos (firewalls, proxies, re-direccionamientos DNS, etc.) algunos gobiernos niegan el acceso a determinados contenidos para sus ciudadanos. A pesar de que el contenido permanezca disponible en Internet, las conexiones originadas en estos países son localmente bloqueadas cuando intentan realizar el acceso a los destinos prohibidos (que pueden estar localizados fuera o dentro del país que realiza el bloqueo).

Recientemente una decisión del Reino Unido, que adopta (por medio de la ONG Internet Watch Foundation - IWF) esta práctica para el bloqueo de material online conteniendo pornografía infantil, motivó la ira de millares de internautas que notaron el bloqueo de un artículo [70] de Wikipedia sobre un antiguo disco de la banda alemana Scorpions, que en su capa presenta la imagen de una adolescente desnuda. Se cuestionó por ejemplo la prohibición del acceso al texto del artículo, y no solamente a la imagen supuestamente delictiva. Y por qué el sitio web de la empresa Amazon[71] no fue igualmente bloqueado, una vez que esta comercializa el mismo disco exponiendo, tal como se ve en Wikipedia, la imagen de su portada.72

[70] http://en.wikipedia.org/wiki/Virgin_Killer

Tal práctica mantenida por la organización IWF en conjunto con los proveedores de Internet del Reino Unido presenta criterios razonablemente transparentes para efectuar bloqueos, como por ejemplo, la supuesta desconformidad de imágenes con el Protection of Children Act 1978. No obstante, organizaciones que actúan en la defensa de la libertad de expresión están denunciando una serie de países que estarían utilizando esta misma práctica para asegurar bloqueos de orden político.

• Clasificaciones y filtrados particulares

En septiembre del 2009 la World Wide Web Consortium (W3C) pasó a recomendar el uso del Protocol for Web Description Resources (POWDER)[73], una tecnología que tiene por objetivo posibilitar la inserción de metadatos en recursos en la Web, de forma que un software pueda interpretar de lo que se trata aquel contenido y tomar decisiones predefinidas por un usuario u organización (ej: continuar el acceso o no).

[71] http://www.amazon.com/gp/costomer-media/product-gallery/B000V7JCXS/ref=cm_ciu_pdp_images_0?ie=UTF8&index=0
[72] Wikipedia child image censored: http://news.bbc.co.uk/2/hi/7770456.stm
[73] http://www.w3.org/TR/powder-dr/

Esta tecnología sustituye a la anterior, también desarrollada dentro de la W3C, denominada Platform for Internet Content Selection (PICS).[74]

El siguiente fragmento, que resme bien esta propuesta, fue extraído del documento oficial que registra los casos de uso y requerimientos del POWDER75 (traducción libre):

> *"El desarrollo del Protocol for Web Description Resources ha sido motivado en atención a cuestiones sociales y comerciales. Por el lado social, existe la demanda de un sistema que identifique si un contenido está de acuerdo con ciertos criterios que se aplicarían a determinado público. Comercialmente, existe la demanda de personalizar el contenido para un usuario o contexto en particular."*

El mismo documento ofrece ejemplos de como el POWDER puede ser utilizado para evitar la exposición de niños a sitios Web considerados inadecuados. Adaptamos uno de ellos, como se ve a continuación:

1. João, que tiene solamente 12 años, recibió un mensaje SMS en su teléfono celular, de un remitente desconocido. En este mensaje hay un URL http://adulto.ejemplo.com, que es una de las secciones del portal Web http://ejemplo.com.

[74] http://www.w3.org/PICS/
[75] http://www.w3.org/TR/2007/NOTE-powder-use-cases-20071031/

2. La operadora de celular posee una política de protección de acceso para niños que permite que los padres establezcan criterios acerca de lo que puede ser accedido. Uno de los métodos que la operadora utiliza es la verificación de los metadatos suministrados por el portal Web antes de responder al usuario si él tiene permiso para acceder a aquel sitio específico.

3. http://ejemplo.com retorna un mensaje para la operadora de João informando que todo URL dentro de su portal que posea la palabra **adulto** presenta desnudez explícita. La operadora entonces compara esta respuesta con los criterios previamente definidos por los padres de João y concluye que ellos determinaron que este tipo de contenido debe ser bloqueado para su hijo. (todo el proceso es automatizado)

4. A operadora exhibe entonces, en lugar del contenido del sitio http:// adulto.ejemplo.com, un mensaje explicando a João que la página no está accesible en virtud de la política de protección al niño utilizada por la empresa.

• Filtrado por el destino basado en la localización del origen

En este método es el proveedor del contenido (por determinación del gobierno, de la justicia o incluso por cuenta propia) que determina quien posee las credenciales para accederlo, utilizando como criterio la localización geográfica del internauta. Los sistemas capaces de detectar la localización de un internauta a partir de su dirección IP han evolucionado a lo largo de los años, alcanzando actualmente algo cerca del 100% de exactitud en la determinación del país de origen e índices un poco menores de acierto en referencia a regiones, estados, ciudades e incluso barrios.[76]

• Control de contenido por medio de sistemas de búsqueda

Mecanismos de búsqueda en Internet son considerados el medio más natural a ser explorado por el internauta en el intento de encontrar los sitios Web de su interés, dispensando el previo conocimiento de sus direcciones (URLs). Consecuentemente, los buscadores, que generalmente funcionan como servicios mantenidos por grandes corporaciones (ej: Google, Yahoo, Microsoft), se convierten en víctimas (o cómplices) de políticas de control de acceso impuestas por los gobiernos.

El ejemplo más emblemático en este tema implicó a China y al más popular buscador en la gran red, ofrecido por la empresa Google. La empresa pasó a operar como un proveedor de Internet en China en el 2006, cuando lanzó su servicio de búsquedas en aquel país, Google.cn. La empresa, que siempre cargó el lema Don't be Evil (no sea malo), ganó la confianza de millones de internautas al destacarse por un buen tiempo como una empresa dotada de principios éticos diferenciados. Sin embargo, al rendirse a las oportunidades de negocio que el mercado chino propiciaría, Google concordó en cumplir las órdenes de auto-censura determinadas por el gobierno, generando enormes críticas de millares de organizaciones e individuos alrededor del mundo.[77]

[76] Una empresa destacada en este asunto es Maxmind, que ofrece gratuitamente versiones simplificadas de sus bases de datos de geo-referenciamiento en http://www.maxmind.com/app/ ip-location, que pueden ser consultadas directamente en el sitio de la empresa o por medio de aplicaciones locales.
[77] Una fuente didáctica sobre el caso puede ser es el artículo Google in China -- The Great Firewall: http:// www.duke.edu/web/kenanethics/CaseStudies/GoogleInChina.pdf. Hay además innumerables fuentes de noticias y artículos en diversos idiomas en Internet sobre el asunto.

Cuatro años después de la presencia en China, el buscador de Google aun permanecía muy atrás de su principal competidor chino, Baidu, que concentraba cerca del 75% del mercado, contra aproximadamente 25% de la empresa norteamericana, en constante caída.[78]. Tal hecho es considerado por algunos analistas la principal razón de que la empresa haya anunciado en diciembre del 2010 una drástica revisión de sus operaciones en el país.[79] Entretanto, Google alega oficialmente que la motivación partió de los ataques a cuentas de Google Mail (Gmail) supuestamente apoyados por el gobierno chino (donde entre los blancos estaban diversos activistas de derechos humanos), entre otras dificultades de orden técnico y político que emergieron en virtud de las imposiciones locales.[80]

Este episodio, aun no completamente resuelto, impulsó los debates acerca de la concentración del poder de empresas que poseen monopolios de servicios en Internet y como los principios de neutralidad de la red pueden ser afectados/evitados en tales circunstancias.

Privacidad y protección de datos

El término **protección de datos** se refiere al instrumento legal que garantice el derecho del ciudadano de controlar y decidir sobre sus informaciones personales, o sea, a la privacidad - derecho reconocido en la Declaración Universal de Derechos Humanos y en otras convenciones internacionales.

[78] http://www.6.com/cms/s/2/d14f6800-db87-11df-ae99-00144feabdc0. html#axzz1NUATW2J3
[79] http://techcrunch.com/2010/01/12/google%E2%80%99s-china-stance-more-about-businessthan
[80] http://googleblog.blogspot.com/2010/01/new-approach-to-china.html

En [Kurbalija 2010, págs. 140 y 141] las cuestiones involucrando privacidad y protección de datos son clasificadas de la siguiente manera:

• Entre **individuos y gobiernos**, donde el principal desafío está en establecer un equilibrio entre la necesidad de modernización del Estado y la garantía de los derechos a la privacidad de los ciudadanos.

• Entre **individuos y empresas**, dado que informaciones que revelan el perfil de un cliente pasaron a ser pieza fundamental en el modelo de negocio de las empresas de Internet, principalmente en servicios de redes sociales como Facebook y Orkut.

• Entre **gobiernos y empresas**. Ambos poseen datos sensibles de individuos alrededor del mundo. Hay casos en que estos datos son compartidos a nivel internacional con el objetivo de evitar actos criminales, como acciones terroristas. La cuestión está en los límites de esta relación de cooperación transnacional.

• Entre **individuos**. Esta preocupación se refiere a lo que algunos autores designan como "democratización de los medios de vigilancia." O sea, actualmente los individuos pueden adquirir herramientas poderosas para la práctica de vigilancia, desde softwares sofisticados hasta aparatos físicos específicos (mini-cámaras, etc.). Es una novedad que demanda a veces la elaboración de nuevas leyes, como fue hecho en los Estados Unidos con el Video Voyeurism Prevention Act del 2004.[81]

[81] http://www.govtrack.us/congress/bill.xpd?bill=s108-1301

Tabla 2.6: Taxonomía de los tipos de pornografía infantil, según [Taylor 2003]

Nivel	Nombre	Descripción del contenido del material publicado
1	Indicativo	Imágenes de niños con pocas vestimentas, trajes de baño, etc., sin contenido sexual, retiradas de álbumes de familia o bases de imágenes comerciales, organizadas en un contexto que indique alguna sospecha.
2	Nudismo	Imágenes de niños desnudos o parcialmente desnudos, expuestas fuera de contexto sexual, en un ambiente legítimo de nudismo, publicadas por fuentes legítimas.
3	Erotismo	Imágenes de niños desnudos o parcialmente desnudos, registradas solapadamente.
4	Pose	Niños deliberadamente posando para fotos, desnudos o parcialmente desnudos, en las que el contexto sugiere algún interés sexual.
5	Pose erótica	Niños deliberadamente posando para fotos, desnudos o parcialmente desnudos, en exposición explícitamente sexual o provocativa.
6	Pose erótica explícita	Niños deliberadamente posando para fotos, exhibiendo las áreas genitales.
7	Actividad sexual explícita	Implica algún contacto físico, masturbación, sexo oral o relación sexual entre niños, sin la presencia de adultos.
8	Violación	Niños sometidos a un escenario de abuso sexual, con algún contacto manual con adultos.

9	Violación grotesca	Niños sometidos a un escenario de abuso sexual, con penetración, masturbación o sexo oral con uno o más adultos.
10	Sadismo/ Bestialidad	Imágenes exhibiendo niños siendo inmovilizados, golpeados, azotadas o sufriendo cualquier agresión de ese género; o imágenes con animales puestos en situación sexual con niños.

Seguridad para niños y adolescentes en Internet

Los últimos Forums de Gobernanza de Internet (IGF) dedicaron sesiones enfocadas en este tema en sus programaciones principales.

• **Cyberbullying**. El National Crime Prevention Council [82] define cyberbullying "como cuando la Internet, teléfonos celulares u otros dispositivos son utilizados para enviar textos o imágenes con la intención de herir o avergonzar a otra persona".

• **Abuso y explotación sexual infantil-juvenil**. Este tipo de crimen implica una serie de conductas, demandando por tanto variados (y a veces complejos) medios de enfrentamiento y prevención, donde los resultados dependen de la cooperación entre sectores de la sociedad civil, industria y gobiernos. En [Taylor 2003] los autores sugieren una clasificación de los "tipos de pornografía infantil", partiendo del grado de severidad del contenido publicado en la red. Reproducimos esta clasificación en la tabla 2.6, con pequeñas adaptaciones, para ofrecer al lector una idea del problema en cuestión.[83]

[82] http://www.ncpc.org/cyberbullying

• **Juegos con contenido inadecuado**. Según [Kurbalija 2010, pág. 151], la lista de los 10 juegos de video-game más populares en las principales consolas ha sido dominada por temas de violencia. Se nota de hecho la popularidad de tales juegos al consultar fuentes especializadas en Internet, como la CNET, que lista los 10 mejores / más populares juegos en los últimos 10 años, donde 8 tienen violencia [84]. Surgen además nuevos temas en la industria de juegos, explotando el terrorismo, uso de drogas, sexo, robos, asesinatos en escenas cada vez más realistas. El impacto de estos juegos en el comportamiento de niños y adolescentes ha sido largamente debatido.

2.4 Marco Civil de Internet

El “Marco Civil de Internet” merece este título porque representa un intento de traer de forma pionera para la tutela judicial los derechos fundamentales como la intimidad y la libertad de expresión.

Por eso también se llama “Constitución de Internet”, ya que pretende establecer las reglas del juego para la utilización de Internet. Denotando que Internet será un espacio neutro, se prohíbe que prestadoras de servicio restrinjan el acceso a servicios de la competencia por parte de los usuarios. Garantiza que solamente los IPs serán almacenados, y no los datos personales, cuya divulgación depende - conforme veremos - de una única autorización judicial. Protege la libertad de expresión al decir que las prestadoras de servicio de Internet no pueden realizar censura previa sobre el contenido publicado, reservadas materias que afronten dispositivos penales (p.ej., crímenes relacionados a la pornografía infantil-juvenil) o después de determinación judicial.

[83] El término "imagen" presente en esta tabla se refiere a fotografías, vídeos o montajes que identifiquen a un niño real.
[84] http://www.cnet.com/1990-11136_1-6310088-1.html

Es común que se diga que la cultura de Internet es algo nuevo, no susceptible de reglamentación por la forma tradicional. No obstante, el tiempo demostró lo contrario, hasta con una aguda obviedad. Las relaciones en el cyberspace gozan de los mismos defectos y virtudes de cualquier relación humana.

El espacio y el tiempo, aunque aparentemente diluidos, no tienen la fuerza suficiente para alejar estándares culturales de respeto a lo que consideramos el sentido de moral y jurídico.

Es así que el Proyecto de Ley número 2126/2011 (Marco Civil de Internet - MCI) está compuesto por cinco capítulos, siendo el último destinado a las disposiciones finales, donde se refuerza la posibilidad de tutela individual y colectiva en consideración a los derechos establecidos en el diploma.

Los capítulos I y II del MCI tienen como contenido la fijación de los principios generales, de las definiciones de los términos utilizados en los capítulos siguientes de la ley, así como el esclarecimiento de los derechos y garantías básicos de los usuarios de Internet.

Como paño de fondo a las directrices generales en discusión, está la disciplina del uso de Internet y el respeto a la intimidad y a la libertad de expresión. Es así que en los capítulos III y IV se cuida de regular la provisión de conexión y de aplicaciones de Internet - artículos 9º al 23 de la ley.

Cabe un análisis más riguroso según el aspecto criminal del MCI. Las dificultades investigativas para aclarar los crímenes cometidos por Internet son inmensas, una vez que el domicilio digital es fácil de ser modificado y depende de una serie de complejidades técnicas que exigen cooperación y repartición de informaciones.

Toca al MCI permitir que el Ministerio Público pueda solicitar datos de registro y que las prestadoras de servicio en Internet tengan la obligación de guardar datos de conexión por un período razonable para facilitar el rastreo del domicilio digital sospechoso.

Por supuesto, esta apertura de informaciones particulares exigirá una postura vigilante al respecto de la responsabilidad civil en la liberación de los datos.

Aparece, por tanto, una necesidad de cambio en el estado actual del proyecto de ley del MCI, que perfiló la doctrina norteamericana de que la expectativa de privacidad sólo merece ser restringida mediante orden judicial. No obstante, es necesario recordar que la recogida de pruebas en los Estados Unidos es mucho más liberal que en Brasil. Por ejemplo, con base en estudios sociológicos, los cuales tienen como objetivo trazar el perfil del criminal, se acepta que un agente estatal infiltrado se haga pasar por víctima y tenga acceso al perfil de los usuarios de redes virtuales de relación [Jaishankar 1998]. Aquí, en Brasil, esta postura sufriría intransigente contestación ante una semántica garantizadora del derecho de intimidad.[85]

De esta forma, el MCI debe incorporar y resolver, en lo posible, los problemas investigativos de los crímenes cibernéticos. Lo contrario causaría un Marco que no protegería suficientemente los derechos fundamentales.

Es saludable tener en mente que el derecho a la intimidad sólo es posible cuando es conciliado con las diversas dimensiones de la libertad de expresión: a) la libertad de expresión como derecho personalísimo (aspecto individual); b) libertad como derecho de tener el acceso más amplio posible a informaciones divulgadas (aspecto social); y c) libertad comercial, consistente en la prestación de servicio de acceso o de aplicaciones de Internet.

La Convención del cybercrime, firmada en Budapest, en el 2001, por iniciativa del Consejo Europeo, trató de dar un ropaje jurídico a estas preocupaciones, recomendando, por ejemplo, la sanción para el acceso no autorizado a datos o el uso de Internet en la divulgación de imágenes pedo-pornográficas, etc.:

[85] Dentro de esta corriente garantizadora, basta recordar el antiguo informe en el 145 del STF: no hay crimen cuando la preparación del flagrante por parte de la policía hace imposible su consumación.

> *Article 2 - Illegal access.*
>
> *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.*
>
> *Article 9 - related to child pornography.*
>
> *1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:*
> *a) producing child pornography for the purpose of its distribution through a computer system;*
> *b) offering or making available child pornography through a computer system;*
> *c) distributing or transmitting child pornography through a computer system;*
> *d) procuring child pornography through a computer system for oneself or for another person;*
> *e) possessing child pornography in a computer system or on a computer-data storage medium.*[86]

Más tarde, en el 2004, no es excesivo recordar el protocolo adicional a la referida Convención, con el objetivo de cohibir los crímenes de racismo y xenofobia cometidos por Internet, como contrapunto al liberalismo capitaneado por la Suprema Corte norteamericana.[87]

Por otro lado, la Comisión Parlamentaria de Investigación (CPI) de la pedofilia, instaurada en el 2008, en el Senado Federal, al tratar de la "pedofilia", verificó que el tema requiere el enfrentamiento de mecanismos de cooperación que faciliten la investigación de identificar el domicilio digital (IPs etc.)[88].

En este contexto, uno de los trabajos más elogiados en el combate al crimen cibernético fue el acuerdo entre el MPF y las prestadoras de servicio en Internet para garantizar la preservación y accesibilidad de datos que posean de las conexiones efectuadas por usuarios a partir de Brasil; email de acceso, número de IP de creación, logs de acceso, hora y referencia GMT de las conexiones, etc.[89]

Obsérvese que la mirada crítica delineada ya está reflejada en un conjunto de preceptos legales que podrían muy bien ser confirmados por el MCI. Menciónese el art. 8º, 42º [90], Ley Complementaria (LC) número 75/93, c/c el art. 26, 2º, c/c el art. 80 [91], Ley número 8.625/93; indicados como elementos imprescindibles en la confección del MCI. La confidencialidad de datos de registro no pueden ser impuestos al Ministerio Público por la conformación legal, incluso de estatuto superior (LC) a la ley ordinaria por la cual será publicado el MCI.

[86] http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm, el 16.10.2012
[87] http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm, el 16.10.2012.
[88]http://www.senado.gov.br/noticias/agencia/pdfs/RELATORIOFinalCPIPEDOFILIA.pdf, el 16.10.2012
[89] http://www.prsp.mpf.gov.br/crimes-ciberneticos/TACgoogle.pdf, el 16.10.2012

Es una tendencia que se corrobora con la reciente modificación en la Ley de lavado de dinero (Ley número 9.613/98): "Art. 17-B. **La autoridad policial y el Ministerio Público tienen acceso**, exclusivamente, **a los datos de registro del investigado** que informan calificación personal, filiación y dirección, independientemente de autorización judicial, mantenidos por la Justicia Electoral, por las empresas telefónicas, por las instituciones financieras, por los proveedores de Internet y por las administradoras de tarjeta de crédito. (Incluido por la Ley número 12.683, del 2012)."

[90] Art. 8º Para el ejercicio de sus atribuciones, el Ministerio Público de la Unión podrá, en los procedimientos de su competencia: (. . .) § 2º Ninguna autoridad podrá imponer al Ministerio Público, bajo ningún pretexto, la excepción de confidencialidad, sin perjuicio de la subsistencia del carácter confidencial de la información, del registro, del dato o del documento que le sea suministrado.
[91] Art. 26. En el ejercicio de sus funciones, el Ministerio Público podrá: I (. . .) § 2º El miembro del Ministerio Público será responsable del uso indebido de las informaciones y documentos que solicite, incluso en las hipótesis legales de confidencialidad. Art. 80. Se aplican a los Ministerios Públicos de los Estados, subsidiariamente, las normas de la Ley Orgánica del Ministerio Público de la Unión.

CAPÍTULO 3
ASPECTOS TÉCNICOS DE LA INVESTIGACIÓN

If you can't change yourself, change at least your watch.

SPAM anónimo

3.1 Visión general del procedimiento de investigación

Los métodos consolidados en la ciencia forense son igualmente adoptados en la investigación de crímenes en Internet. Tales métodos consisten básicamente en la **adquisición, preservación, análisis y presentación** de evidencias. Estos cuatro pasos incluyen una serie de actores y actividades criteriosas y en la práctica acostumbran a ser cíclicos. Raramente se ven casos en que la presentación de evidencias es única y definitiva. El ejercicio del contradictorio posibilita que la defensa conteste la legitimidad de los procedimientos de investigación o incluso la consistencia de un laudo investigación, tornando usual la necesidad de nuevas adquisiciones, análisis y presentación de las informaciones durante la marcha del proceso.

Es necesario cumplir con algunos requisitos para que las evidencias digitales de una investigación sean jurídicamente válidas. Según la RFC 3227 [1], que ofrece una serie de recomendaciones para procedimientos de recogida y preservación de pruebas en medio digital, la evidencia electrónica debe ser (traducción libre):

[1] Guidelines for Evidence Collection and Archiving - http://www.faqs.org/rfcs/rfc3227.html

1. Admisible: o sea, estar en plena conformidad con la ley para que pueda ser presentada a la justicia.

2. Auténtica: las pruebas deben ser comprobadamente relacionadas al incidente/crimen investigado. El trabajo de una documentación de calidad es esencial para el cumplimento de este ítem.

3. Completa: el conjunto de evidencias debe suministrar una presentación completa acerca del evento investigado. Nunca debe depender de elementos faltantes o dudosos. Debe "contar la historia" completa, y no solamente suministrar perspectivas particulares.

4. Confiable: no debe haber incertidumbre acerca de la autenticidad y veracidad de las evidencias, así como sobre las formas como fueron recolectadas y posteriormente manipuladas durante la investigación.

5. Convincente: además de todas las características anteriores, debe ser documentada y presentada de forma clara y organizada.

3.1.1 Vestigios, indicios y evidencias

Los términos mencionados anteriormente a veces son utilizados como sinónimos, a pesar de que carguen semánticas formales distintas. Cabe al investigador la clara

comprensión de estas diferencias. Comencemos nuestra reflexión sobre este tema analizando la siguiente proposición:

> *"Mientras el vestigio abarca, la evidencia restringe y el indicio circunstancia."*
>
> [Filho 2009]

Según el autor, el vestigio abarca en el sentido que, en términos investigacionales, este concepto "**mantiene la característica abarcadora del vocablo que le dio origen, pudiendo ser definido como toda y cualquier señal, marca, objeto, situación fáctica o ente concreto sensible, potencialmente relacionado a una persona o a un evento de relevancia penal, y/o presente en un local de crimen, sea este último mediato o inmediato, interno o externo, directa o indirectamente relacionado al hecho delictivo**".

En el contexto de la investigación de crímenes computacionales, donde notadamente el objeto **sensible** es casi siempre representado por lo **intangible**, se tiene que el vestigio es mayoritariamente presentado como un registro **digital** que existe como consecuencia de una previa intervención humana, tratada aquí como agente motivador directo o indirecto de aquel evento. Estos vestigios pueden ser, por ejemplo, los logs almacenados por un software, o un mensaje recuperado en la Web. Una vez que el investigador extraiga - por medio de determinaciones analíticas - las informaciones presentes en estos vestigios, podrá verse autorizado a inferir objetivamente sobre el vínculo de estos con el delito en cuestión, presentando así **evidencias** de que, por ejemplo, aquel mensaje publicado en la Web partió indudablemente de aquella computadora investigada. Cabe resaltar que la amplitud de los vestigios debe ser podada en la medida de lo que se considere necesario y suficiente para la construcción lógica de la evidencia, la que debe presentarse por tanto **restringida** a su utilidad en el proceso.

En el Código de Proceso Penal, el **indicio** es presentado como "**la circunstancia conocida y probada, que, teniendo relación con el hecho, autorice, por inducción, a concluirse sobre la existencia de otras circunstancias**." Concordamos por tanto con [Filho 2009], cuando este deduce que "**la evidencia es el vestigio que, mediante pormenorizados exámenes, análisis e interpretaciones pertinentes, se encuadra inequívoca y objetivamente en la circunscripción del hecho delictivo. Al mismo tiempo, se infiere que toda evidencia es un indicio, sin embargo lo contrario no siempre es verdadero, pues el segundo incorpora, además del primero, otros elementos de orden subjetivo**."

O sea (siguiendo la línea del ejemplo anterior), se constata que la evidencia presentada por medio de análisis de los vestigios recolectados es igualmente interpretada como un indicio de que el mensaje fue publicado por medio de la computadora ya identificada en la investigación. Se suman a este indicio otros de orden subjetivo, como el hecho de que la computadora analizada estaría físicamente localizada en la residencia habitada por un único individuo. Se ve por fin, como está ilustrado en el Código Procesal Penal, un proceso inductivo, dotado de elementos objetivos y subjetivos, alimentados por diligencias diversas y procedimientos investigacionales que, sumados, posibilitan conclusiones acerca de la existencia de nuevas circunstancias - que son también indicios

- y que, después del convencimiento de las autoridades competentes, son presentadas como prueba material en el proceso.

Es oportuno citar otro fragmento del referido artículo, este compone un desenlace didáctico importante para nuestra reflexión de carácter analógico:

> **"La presentación de una prueba material, en una corte judicial criminal, es el momento clímax de todo un proceso, que se extiende desde la preservación del local del crimen al tránsito en juzgado de un proceso penal. Antes de esto, la prueba material ya fue un vestigio, una evidencia, un indicio; estuvo expuesta a las condiciones de un local de crimen y almacenada hasta los envíos debidos; pasó por las manos de peritos criminales, autoridades policiales, estafetas, funcionarios del forum y del Ministerio Público. "**

3.1.2 Procedimientos de seguridad lógica en el ambiente de investigación

La protección de las informaciones recolectadas es esencial para que sean cumplidos los requisitos que posteriormente implican en la confiabilidad de las pruebas. Es necesario por tanto mantenerlas fuera del alcance de virus, worms, spywares y otras plagas virtuales.

Sistemas basados en Unix como GNU/Linux y Mac OS son recomendados para investigaciones por ser menos vulnerables a ataques [Jones 2006, 1.6.1 - Viruses, Worms and Other Threats]. Sistemas de código abierto traen además el beneficio de ser integralmente auditables factor especialmente relevante en la etapa de **presentación** de las evidencias. En caso que el investigador opte por utilizar la plataforma Windows en los procedimientos de investigación, serán necesarios una serie de cuidados adicionales, con el objetivo de reducir las oportunidades de contaminación de las informaciones. Es recomendado en este caso la utilización de softwares actualizados de antivirus, anti-spywares, etc. Otras precauciones pueden además minimizar la posibilidad de comprometimiento, como la utilización de navegadores alternativos a Internet Explorer y al conjunto de herramientas para oficina Microsoft Ofice[2]. Recomendamos la sustitución de estas por los softwares libres y gratuitos correspondientes Mozilla Firefox y LibreOfice.org.

Otras técnicas adoptadas para reducir las oportunidades de comprometimiento del material recolectado (como la utilización de máquinas virtuales) son abordadas en 3.4 **Aspectos técnicos de la investigación**.

3.1.3 Preservando el anonimato del investigador

Comunicaciones de cualquier naturaleza en Internet dejan rastros. Por tanto, de la misma manera que un criminal habilidoso está atento para no dejar pistas sobre sus acciones, el investigador debe también dedicar atención para que el sospechoso no desconfíe que está bajo investigación.

El dueño de un website, por ejemplo, puede fácilmente visualizar informaciones acerca de su público visitante. En general todos los accesos a un website son registrados. Constan en este registro al menos la dirección IP de origen y el horario de los accesos realizados. A partir de la dirección IP es posible determinar una serie de informaciones acerca del origen del acceso, como por ejemplo la localización geográfica, proveedor de acceso, institución responsable de la red, etc. Es posible además inferir sobre lo que motivó al internauta a acceder a su website por medio del registro de términos buscados por él o por el mecanismo de redireccionamiento que lo llevó hasta allá, como ilustra la figura 3.1.3.

[2] En virtud del extenso histórico de fallas de seguridad de estas herramientas

Figura 3.1: awstats: ejemplo de sistema que registra datos de acceso en sitios Web

Búsqueda por Frases (Primeros 10)
Lista completa

12 frases(s) diferente(s)	Búsqueda	Por ciento
site web perso	3	17.6 %
laurent destailleur	2	11.7 %
site web personnel	2	11.7 %
destailleur.fr	2	11.7 %
prestashop	1	5.8 %
chiensderace	1	5.8 %
infos almirida crte	1	5.8 °.(0
coordonnAce	1	5.8 %
destailleur	1	5.8 %
laurent detailleur	1	5.8 9(0
Otras frases	2	11.7 °I-0

Rastros similares pueden ser dejados también por otros servicios de Internet, como email y peer to peer. Es por tanto fundamental que el ambiente en que ocurrirá el procedimiento de adquisición de evidencias esté configurado de tal forma que no deje para el sospechoso ningún indicio de que está siendo investigado.

Existen diversas técnicas para reducir la exposición del internauta y los rastros de navegación. Estos métodos son legítimos y a veces son igualmente explotados para la práctica del crimen. La utilización de proxies ha sido el medio más efectivo para asegurar un nivel razonable de anonimato en la red. En la sección 3.8.3 **Aspectos técnicos de la investigación** describimos detalles sobre el funcionamiento de esta estructura de proxies anónimos. Describimos además un paso a paso para la utilización de esta tecnología en ambientes GNU/Linux y Microsoft Windows. Por ahora vale registrar esta preocupación y enumerar algunas buenas prácticas para el bien del anonimato en la investigación.

Cuatro consejos para el bien del anonimato

• Utilizar una red externa a la de la institución responsable de la investigación. Esto puede ser hecho a partir de la contratación de un link doméstico exclusivo para los procedimientos;

• Utilizar servicios de proxies anónimos en Internet, de preferencia tecnologías más avanzadas, como se ve en la red TOR;

• No utilizar email institucional para registros online en servicios cuando es necesario algún tipo de registro para recogida de informaciones;

• No utilizar palabras clave que indiquen la motivación de la investigación en buscadores online para llegar al servicio investigado.

3.2 Las evidencias digitales

Una definición para lo que normalmente asumimos como **evidencia digital** es propuesta en [Casey 2004, 1.1], la cual exponemos a continuación en libre adaptación:

> *Una evidencia digital puede ser entendida como cualquier dato almacenado o transmitido utilizándose una computadora, de manera que con este dato sea posible demostrar o refutar una hipótesis acerca de un evento; o también que este suministre elementos críticos determinantes en un caso investigado, tal como premeditación, dolo, coartada, etc.*

Una **evidencia digital** no deja de ser una abstracción de un evento del mundo físico. De hecho, los elementos involucrados en la publicación de un contenido en la red nunca son integralmente recuperables. La manipulación del teclado, los clicks del mouse, la presencia de personas en el acto, las operaciones de escritura en disco y los detalles de la transmisión del contenido son reducidos a lo que el investigador esté apto a inferir por medio de registros disponibles después del evento.

Se nota, sin embargo, que tal situación no difiere de aquellas observadas en escenarios más tradicionales de investigación de crímenes, donde no todas las piezas del rompecabezas están inmediatamente disponibles para el investigador.

Veremos en este tópico que las evidencias digitales presentan peculiaridades que, si son bien comprendidas, podrán emerger como piezas fundamentales en el desdoblamiento de un caso. Al paso que, si son subestimadas o mal comprendidas, inevitablemente surgirán como un estorbo en el ambiente de investigación. Listamos a continuación algunas de sus características para justificar esta aserción:

• en virtud de su alto grado de volatilidad, evidencias digitales son fácilmente manipulables. Es posible que haya modificaciones por el propio criminal en el intento de ocultar rastros, o incluso por el investigador, durante las etapas de adquisición y análisis.

• pueden ser fácilmente duplicadas, de manera que el examinador utilice una copia para su análisis, evitando el riesgo de comprometer la "original." De cierta forma, tal característica anula lo que hay de negativo en la anterior.

• pueden ser fácilmente comparadas con la "original," para certificar su integridad o detectar eventual modificación.

- en virtud de su intangibilidad, son menos propensas a la total destrucción.

- en general cargan metadatos relevantes para la investigación. Tal como se pueden extraer huellas digitales de un documento impreso, es posible con mucho menos esfuerzo recolectar informaciones de autoría en documentos digitales.

- por ser más abundantes, demandan metodologías más sofisticadas de filtrado, de manera que se extraiga solamente lo que interesa al caso investigado. La manipulación incorrecta puede acarrear una considerable confusión de informaciones, consecuentemente **contaminando** aquello que sería de interés para el caso.

Al utilizar los métodos presentados en este Guión para recolectar, analizar, reconstruir el escenario de un crimen y por fin probar las hipótesis enunciadas, el investigador, en posesión de las evidencias digitales, podrá presentar posibilidades bastante consistentes acerca de lo ocurrido.

3.2.1 Adquisición de evidencias

Una vez que se conoce el objeto primario de la investigación [3], se debe explotar al máximo las informaciones sobre él disponibles públicamente en la red. En muchas ocasiones las fuentes públicas suministran información suficiente para alcanzar el blanco (humano) de la investigación.

[3] El objeto primario de una investigación puede ser por ejemplo una dirección de email denunciada, un website, un perfil de usuario en red social, el nombre o hash de un archivo en redes P2P, etc.

No obstante existen casos en que es necesario utilizar técnicas adicionales, con el objetivo de recolectar aquello que no fue posible a partir de fuentes públicas. Entran aquí las demás posibilidades que demandan autorización judicial. Estas incluyen actividades de ingeniería social, inoculación, infiltración, interceptación telemática etc.

Veremos más adelante en este Guión algunas formas de recolectar evidencias en los tipos de servicios más comunes en Internet.

3.2.2 Garantizando la preservación e integridad de las evidencias digitales

Preservar una evidencia digital significa sobre todo garantizar que ella no sufrió modificaciones desde del momento en que fue recolectada de una fuente externa hasta la fase final de presentación de las pruebas. Esta práctica es usual en los procedimientos de investigación en dispositivos de almacenamiento (discos duros, llaveros USB, dispositivos móviles, etc). No obstante hay ocasiones en que esta tarea es también esencial durante la fase de adquisición de evidencias en Internet, incluso cuando tratamos de fuentes públicas. Podemos citar como ejemplo la replicación de un website criminal, donde el investigador realiza el download de todos los archivos que componen un sitio en la web para que pueda efectuar su posterior análisis. Al final de la recogida (o incluso durante la misma, dependiendo de la herramienta utilizada) él debe, antes de cualquier otra acción, generar las "impresiones digitales" de cada archivo bajado, para que sea posible evaluar su integridad (o sea, si sufrieron alguna modificación) en cualquier instante futuro.

Figura 3.2: Extracción de firmas (hashes) de archivos

También es común la utilización del término "firma" para designar lo que de hecho es la **suma criptográfica** del contenido de un archivo. Una suma criptográfica (o firma, o hash, o huella digital) de un archivo es el resultado de una función matemática aplicada directamente en la secuencia de bits que lo compone. O sea, en caso que un único bit sea modificado en un archivo, aunque visualmente sea imposible identificar tal modificación, el resultado de la aplicación de la misma función será diferente del anterior, quedando comprobado que su integridad fue comprometida. Para este fin, generalmente son utilizados métodos matemáticamente consistentes y de dominio público, como los populares algoritmos **MD5 y SHA-1**. La figura 3.2 ilustra esta operación de extracción de hashes de archivos.

Se nota en la figura 3.2 la existencia de 4 archivos de texto (1.txt, 2.txt, 3.txt y 4.txt), cuyo contenido está expuesto en los bloques de color azul. Los archivos son sometidos a funciones MD5 y SHA-1, que resultan en hashes tales como exhibidos en los bloques de color rosado, en representación alfanumérica. Hay algunos puntos importantes a considerar en esta ilustración. El primero es representado al someter el archivo 2.txt a dos diferentes algoritmos, lo que resultará en dos hashes distintos. La segunda observación vale para los archivos 3.txt y 4.txt que, a pesar de ser aparentemente idénticos, poseen diferentes hashes, incluso cuando son sometidos a una misma función (en este caso, la sha-1). Veremos eso con detalles al analizar las líneas a continuación, que exhiben estas acciones en la práctica, en un sistema GNU/Linux, utilizando los softwares md5sum y sha1sum.

1	ntccc@ntccc:—/archivos$ grep " *
2	1.txt:Fox
3	2.txt:The red fox jumps over the blue dog
4	3.txt:The red fox jumps over the blue dog
5	4.txt:The red fox jumps over the blue dog
6	ntccc@ntccc:—/archivos$ md5sum 1.txt 2.txt
7	2e 1efc59375746270b4f5cc98ce31cc4 1.txt
8	ee15c78637efbb850745b06dc75130cc 2.txt
9	ntccc@ntccc:—/archivos$ md5deep 1.txt 2.txt
10	2e1efc59375746270b4f5cc98ce31cc4 /home/ntccc/archivos/l.txt
11	eel 5c78637efbb850745b06dc75130cc home/ntccc/archivos/2.txt
12	ntccc@ntccc:—/archivos$ shal sum 2.txt 3.txt 4.txt
13	0504e140d01c8c8cad73ac18873fd7944e236f90 2.txt
14	6f548495066f017b7254108b42a210d6be3fd11b 3.txt
15	4f4c60548c3ca082585e7949e20846122eabb4aa 4.txt
16	ntccc@ntccc:—/archivos$ shal deep 2.txt 3.txt 4.txt
17	0504e140d01c8c8cad73ac18873fd7944e236f90 /home/ntccc/archivos/2.txt
18	6f548495066f017b7254108b42a210d6be3fd11b /home/ntccc/archivos/3.txt
19	4f4c60548c3ca082585e7949e20846122eabb4aa /home/ntccc/archivos/4.txt
20	ntccc@ntccc:—/archivos$ we -m 3.txt 4.txt
21	36 3.txt
22	37 4.txt

Las líneas 2 a 5 exhiben los archivos y sus respectivos contenidos en el presente directorio. Las líneas 7 y 8 exhiben el hash MD5 de los archivos 1.txt y 2.txt, presentados después de la ejecución del programa md5sum (línea 6). En la línea 9 ejecutamos otra aplicación que aplica la misma función, el md5deep, solamente para demostrar que la función es completamente independiente del software utilizado, como se puede observar en los resultados (líneas 10 y 11). Realizamos el mismo procedimiento para la función sha-1 en los archivos 2.txt, 3.txt y 4.txt (líneas 12 a 19). La cuestión que aún no fue aclarada es: ¿por qué los archivos 3.txt y 4.txt poseen un hash sha-1 diferentes si presentan el mismo contenido? La respuesta es un tanto obvia: ellos no presentan el mismo contenido. A pesar de no ser posible verificar visualmente la diferencia entre el contenido de los dos archivos, hay un carácter de espacio al final del archivo 4.txt, lo que ya es suficiente para que su hash tenga un valor diferente. Tal diferencia puede ser verificada de otras maneras, por ejemplo, utilizando un editor de textos o por medio del programa wc, que cuenta la cantidad de caracteres presentes en cada archivo, conforme ilustrado en las líneas 20 a 22.

Existen infinitas posibilidades de verificar la integral equivalencia de contenido entre dos o más archivos. Sin duda, el uso de los métodos consolidados de suma criptográfica (hashes) es el más adecuado para nuestro caso. El investigador encontrará la funcionalidad de generación de hashes en cualquier producto dirigido para preservación y análisis de evidencias. Se debe consultar su manual y optar por las funciones que considere adecuadas (teniendo en cuenta cuestiones de desempeño y confiabilidad). En sistemas GNU/Linux y derivados Unix existen diversas opciones, como el md5deep (también disponible para plataforma Windows), desarrollado por Jesse Kornblum en la época en que era un agente del United States Air Force Office of Special Investigations. Por tratarse de un trabajo del gobierno americano, no es protegido por copyright, según consta en su website[4]. El md5deep implementa los algoritmos MD5, SHA-1, SHA-256, Tiger y Whirlpool. Hay también una serie de opciones con interfaces visuales, como el MD5Summer5.

Estas aplicaciones facilitan el proceso de generación y verificación de hashes en lote. La figura 3.3 ilustra el MD5Summer en funcionamiento.

Figura 3.3: Generación de hashes con MD5Summer

Adicionalmente a los procedimientos de generación de firmas de las evidencias digitales, el investigador debe siempre mantener preservado los archivos tal como originalmente recolectados, en conjunto con sus respectivos hashes. Toda actividad posterior de análisis debe ser realizada en una copia exclusiva, evitando así perjudicar la integridad de las pruebas.

[4] http://md5deep.sourceforge.net/
[5] http://www.md5summer.org

3.2.3 Análisis de las evidencias

El análisis de las evidencias consiste en organizar y clasificar las informaciones recolectadas en la etapa anterior, de manera que sea posible extraer de ellas lo que es de interés para la investigación. En este proceso se debe también asegurar la preservación de la integridad de los datos examinados. Debe además ser reproducible, auditable y

libre de contaminación. Vale resaltar otra vez que todo el proceso debe ser realizado en una copia integral de los datos, conforme visto en 3.2.2.

Un paso importante para el proceso de análisis es lo que llamamos **reducción**, que nada más es que un filtrado inicial con el objetivo de reducir este monto al que de hecho será útil para un posterior (e inevitable) análisis humano. El desafío está en mantener un equilibrio, para que ninguna información potencialmente útil sea dispensada de verificación.

En las investigaciones realizadas en discos duros con sistemas instalados, se puede en la mayoría de los casos dispensar de inmediato el análisis de archivos comunes y necesarios al funcionamiento del sistema operativo, conocidos como **archivos de sistema**. Retirar duplicidades y enfocarse en el contenido directamente relacionado con la ocurrencia investigada [6] son también buenas prácticas a adoptar en esta fase.

[6] Por ejemplo, en un website destinado a la propagación de manifestaciones nazis es mucho más común encontrar vestigios de autoría en textos que, por ejemplo, en un website que divulgue imágenes de pornografía infantil, donde el enfoque está en el contenido multimedia.

Figura 3.4: Exhibición de metadatos de una fotografía en la Web

Acciones simples y poco metódicas de búsqueda por estándares y palabras clave son bastante eficientes en determinadas situaciones. Por ejemplo, la extracción de imágenes anexadas en una caja de email interceptada o la investigación por URLs compartidas en un forum destinado al intercambio de links de material ilícito pueden revelar rápidamente los elementos de principal interés de la investigación. En casos más genéricos se pueden clasificar los archivos por tipos, fechas creación, de acceso, tamaño, dueño etc. Casos específicos pueden aun recurrir a bases de datos compartidas entre autoridades, como por ejemplo ocurre con la Interpol y Europol, capaces de confrontar imágenes de pornografía infantil con una base de datos de casos previamente investigados buscando la identificación de víctimas y criminales por medio de algoritmos sofisticados. [Casey 2004]

Otra característica del mundo digital que debe ser explotada durante la etapa de análisis son los metadatos y encabezamientos de archivos. Como el nombre lo indica, un metadato carga información acerca del propio archivo. Un ejemplo bastante popular son los datos EXIF (Exchangeable Image File format), que revelan informaciones sobre las condiciones técnicas de captura de fotografías digitales. La figura 3.4 exhibe la pantalla de un servicio de hospedaje de fotos Web donde datos EXIF son expuestos públicamente. La misma fotografía, al ser analizada por medio del programa exifprobe[7], revela otras informaciones importantes, como es ilustrado a continuación (diversos campos fueron omitidos intencionalmente):

1	FileName = /home/ntccd6057979741_e348341672_o.jpg	
2	FileType = JPEG	
3	FileSize = 2916618	
4	JPEG.APP1.1fdO.Make	= 'NIKON CORPORATION'
5	JPEG.APP1.1fdO.Model	= 'NIKON D50'
6	JPEG.APP1.1fdO.Software	= 'Ver.1.00 '
7	JPEG.APP1.1fdO.DateTime	= '2011:08:09 10:01:26'

8	JPEG.APP1.1fdO.Exif.DateTimeOriginal	= '2011:08:09 10:01:26'
9	JPEG.APP1.1fd0.Exif.DateTimeDigitized = '2011:08:09 10:01:26'	
10	JPEG.APP1.1fdO.Exif. Flash	= 0 = 'no flash'
11	JPEG.APP1.1fd0 .Exif.FocalLength	= 26 mm
12	JPEG.APP1.1fd0[...].Length = '18 mm'	
13	JPEG.APP1.1fd0[...].MaxFocalLength = '55 mm'	
14	JPEG.APP1.1fd0[..1.MaxApertureAtMinFocalLength = 3.50 APEX =13.4'	
15	JPEG.APP1.1fd0[..1.MaxApertureAtMaxFocalLength = 5.60 APEX = 'f7.0'	
16	FileFormat = JPEG/APP1/TIFF/EXIF [...] (Nikon Corporation [2])	

Anteriormente aparece el fabricante y modelos de la cámara utilizada para registrar la foto, la versión del software instalado en la cámara, la fecha del registro, la distancia focal del lente en el momento del registro, las características focales del lente utilizada y la información de que no fue utilizado el flash. Otros diversos datos fueron retirados de este ejemplo para fines didácticos, sin embargo representarían informaciones igualmente relevantes en una investigación.

[7] http://www.virtual-cafe.com/~dhh/tools.d/exifprobe.d/exifprobe.html

No son solo las fotografías digitales las que cargan informaciones sobre ellas mismas. Archivos resultantes de suites de oficina como Microsoft Office y LibreOflice, archivos PDF, MP3, etc., también pueden revelar datos importantes por medio del análisis de sus metadatos. El ejemplo a continuación lista las informaciones de un archivo PDF utilizándose la herramienta pdfinfo, que es parte del software xpdf [8]:

1	ntccc@ntccc:—/ciberneticos/manual/libro$ pdfinfo manual-libro.pdf	
2	Title:	Crímenes en Internet: Manual Práctico de Investigación
3	Subject:	
4	Keywords:	
5	Author:	Procuraduría de la República en el Estado de São Paulo
6	Creator:	LaTeX with hyperref package
7	Producer:	pdfTeX-1.40.10
8	CreationDate:	Wed Aug 31 02:49:37 2011
9	ModDate:	Wed Aug 31 02:49:37 2011
10	Tagged:	en el
11	Pages:	218
12	Encrypted:	no
13	Page size:	612 x 792 pts (letter)
14	File size:	8291961 bytes
15	Optimized:	en el
16	PDF version:	1.4

A continuación aparece un comando que integra algunas herramientas disponibles en sistemas GNU/Linux, de manera que revela el directorio en el cual el archivo originalmente se localizaba en el sistema del supuesto autor. Enseguida utilizamos la herramienta wvSummary para exhibir de manera organizada los metadatos del archivo que revelan incluso el usuario del sistema que salvó el documento por última vez, así como la fecha de creación, última modificación y última impresión.

[8] http://foolabs.com/xpdf/

1	$ cat /tmp/E-igf2006.doc I tr -d 110 I strings I grep D:
2	kummerPD:WyDocuments\SynthesisTackground[...]Meeting_1st_sept..docZ
3	
4	$ wvSummary /home/ntccc/Downloads/manual/E-igf2006.doc
5	Metadata for /home/ntccc/Downloads/manual/E-igf2006.doc:
6	Creator = "IGF"
7	Last Modified = 2006-09-02T08:37:00Z
8	Description = ""
9	Keywords = ""
10	Subject = ""
11	Title = "Introduction"
12	Number of Characters = 44716
13	Last Printed = 2006-08-30T13:09:00Z
14	Last Saved by = "kummer"
15	Number of Pages = 1
16	Security Level = 0
17	Number of Words = 7844
18	Created = 2006-09-02T08:37:00Z
19	Revision = "2"
20	Editing Duration = 2009-04-22T19:27:48Z
21	Generator = "Microsoft Word 9.0"
22	Template = "Normal.dot"
23	msole:codepage = 1252
24	Company = "IGF"
25	Category = ""
26	Document Parts = [(0, "Introduction")]
27	Document Pairs = [(0, "Title"), (1, 1)]
28	Number of Lines = 372
29	Links Dirty = FALSE
30	Manager = ""
31	Number of Paragraphs = 89
32	Scale = FALSE
33	msole:codepage = 1252
34	Unknownl = 54914
35	Unknown3 = FALSE
36	Unknown6 = FALSE
37	Unknown? = 594226

3.2.4 Presentación de las evidencias

La última etapa de esta fase de examen de las evidencias digitales es la preparación de un documento que integre de manera clara y precisa las informaciones (útiles) para apreciación de la justicia. Es necesario construir argumentos sólidos y dejar de lado las suposiciones.

Compilamos a continuación algunas orientaciones que pueden contribuir con la calidad de un informe de presentación de evidencias:

- Suministrar informaciones que identifiquen el caso (número del proceso, investigación, piezas informativas, etc.), quien lo solicitó, si fue requerida alguna(s) respuesta(s) en especial, quien lo elaboró, cuando y donde, protocolo único del núcleo/laboratorio responsable del análisis.

- Suministrar un sumario acerca de las evidencias examinadas. Se debe apuntar el origen de los datos, como fueron recolectados, garantía de integridad con respectivos resúmenes criptográficos. Se debe apuntar precisamente casos de sospechosa de modificación de los datos en medio al proceso.

- Dedicar al menos un párrafo para la exposición del ambiente utilizado en los procedimientos de análisis, incluyendo indicación de las tecnologías y métodos adoptados, si es posible con citación de referencias externas que los validan.

- Indicar con más detalles como los archivos más relevantes para la investigación fueron encontrados, así como notificar cualquier ausencia de archivos que en principio deberían estar presentes en el material analizado.

- Suministrar un inventario con metadatos de los archivos relevantes encontrados.

- Para cada hipótesis enunciada, ofrecer el máximo de evidencias posibles, interpretando la correlación entre ellas y exponiendo como reducen el grado de incertidumbre acerca de las inferencias.

- Suministrar un glosario de términos técnicos utilizados a lo largo del documento.

- Suministrar en medio digital no regrabable los datos relevantes referenciados en el documento de manera organizada e indexada en el informe. Si es posible incluir los softwares necesarios para accederlos en cualquier sistema operativo.

- Finalizar con una conclusión clara y objetiva, resumiendo los ítems de mayor relevancia, evitando "contaminar" el documento con informaciones extras de poca o ninguna utilidad.

Se debe por fin siempre estar atento a la naturaleza del documento, tal como requerido por la autoridad. A veces es requerida una simple **nota técnica**, o una explicación objetiva para una cuestión técnica específica. Para un laudo técnico, se debe enfocar casi que únicamente en la exposición de las evidencias encontradas, mientras que la solicitud de un **parecer técnico** demanda un documento conclusivo y por tanto compuesto por eventuales interpretaciones en diferentes niveles de certidumbre. [Casey 2011] sugiere la utilización de una Certainty Scale, donde se atribuye un valor (C-value) para cada conclusión basándose en una o más piezas de evidencia digital, conforme la tabla 3.1 (en traducción libre).

3.3 La investigación de websites

Un sitio web (o website) está compuesto por una o más páginas web (o webpages), generalmente organizadas jerárquicamente para simplificar al máximo la navegación por parte del internauta. No hay límites para la cantidad de páginas dentro de un sitio web.

Además de archivos de texto, audio, vídeo y otros binarios en general (pdf, doc, swf, etc.), un website puede cargar componentes de otros websites, o hacer solamente referencia a ellos (links). Es muy común que los websites "embutan" vídeos que están localizados en otros websites, recurso que se volvió popular principalmente después de la popularización del servicio YouTube y otros similares. Al analizar un website es necesario por tanto tener en consideración todos estos factores, lo que puede tornar la tarea de investigación dispendiosa y a veces imposible, en caso de que no sean utilizadas herramientas y metodologías adecuadas.

Tabla 3.1: Escala propuesta para categorización de niveles de certidumbre en evidencias digitales

Nivel de certidumbre	Descripción	Calificación
C0	Evidencia contradice hechos conocidos	Erróneo/Incorrecto
C1	Evidencia es altamente cuestionable	Incertidumbre alta
C2	Solamente una de las fuentes de evidencia no está libre de adulteración	Un tanto incierto
C3	Las fuentes de evidencia son difíciles de adulterar pero no hay evidencia suficiente para sustentar una conclusión firme; o hay inconsistencias sin explicación en la evidencia disponible	Posible
C4	(a) Evidencia es protegida contra adulteración o (b) no es protegida contra adulteración, pero múltiples e independientes fuentes de evidencias convergen para una misma acción	Probable
C5	Hay una convergencia de múltiples e independientes fuentes de evidencias, todas protegidas contra adulteración. No obstante, existen pequeñas incertidumbres (por ejemplo, inconsistencias cronológicas o pérdida de datos)	Casi certidumbre
C6	Las evidencias son consideradas no adulterables y/o poseen un alto grado estadístico de confiabilidad sobre la hipótesis enunciada	Certidumbre

3.3.1 Uniform Resource Locator (URL)

Un website es accedido en Internet a través de una URL[9], sigla que puede ser traducida para el español como Localizador de Recursos Universal. Una URL posee la siguiente estructura:

protocolo://dirección/camino/recurso

[9] Algunas fuentes se refieren al URL en masculino: "el URL".

URLs son utilizadas para el acceso a diversos servicios en una red de computadoras. La URL de una impresora en una red local puede ser por ejemplo:

ipp://red.local/gabinete/impresora_01
En el ejemplo anterior, tenemos el protocolo "ipp", la dirección "red.local", el camino "gabinete" y el recurso impresora_01. Para la URL de un website, tomamos el siguiente ejemplo:

https://pt.wikipedia.org/wiki/Http

Tenemos entonces el ejemplo de una URL real, del website Wikipedia, donde el protocolo es "http", la dirección es el nombre de dominio "pt. wikipedia.org", el camino es "wiki" y el recurso es la página web "Http". Utilizamos a propósito esta URL para animar al lector a consultar la Wikipedia y conocer más detalles sobre el HyperText TransferProtocol.

3.3.2 Iniciando el proceso de investigación

Al investigar un website buscamos conocer la materialidad reportada, la localización geográfica del contenido hospedado y finalmente el responsable de su publicación.

Ante estas cuestiones es necesario partir para los procedimientos mencionados anteriormente en **3.2 Aspectos técnicos de la investigación**. La investigación de websites generalmente se inicia a partir de la denuncia de una URL, a veces acompañada de un screenshot y/o descripción acerca del contenido reportado. Como vimos en **3.3.1 Aspectos técnicos de la investigación**, entre los componentes de una URL está la **dirección**, que en el caso de un website es un **nombre de dominio**. Fue visto también en **1.3 Conceptos introductorios** que un nombre de dominio debe ser resuelto en una **dirección IP** en Internet. Además del nombre de dominio y de la dirección IP, debemos considerar obviamente el **contenido** del website que la URL denunciada apunta.

Podemos listar entonces 3 frentes de trabajo independientes, no obstante complementarios, para el inicio de la investigación de un website. Ellos son (1) la recogida del **contenido** del website, (2) la recogida de informaciones referentes al **nombre de dominio** del website y (3) la recogida de informaciones referentes a la **dirección IP** del servidor que hospeda el website. A partir de ahí tendremos una serie de pasos que nos suministrarán las evidencias necesarias, conforme ilustra la figura 3.5. En este tópico detallaremos como proceder para la recogida y preservación del contenido de un website, una vez que la adquisición de informaciones acerca del nombre de dominio y dirección IP son tratadas detalladamente en **1.5 Conceptos introductorios**.

Figura 3.5: Sumario del procedimiento de investigación de un website

Note además en la figura 3.5 que las líneas en color negro y no punteadas indican los procedimientos que implican orden judicial para la adquisición de las evidencias. Como podemos ver, la investigación de un website puede resultar en una serie de otras medidas a ser ejecutadas, como análisis de contenido de emails, interceptación telemática, análisis de equipos aprehendidos etc.

3.3.2.1 Recolectando el contenido de un website

El análisis de contenido de un website que posee extensa cantidad de material puede llevar días, o incluso meses de trabajo dedicado. No es recomendado que se ignore contenido aparentemente inofensivo con el objetivo de acelerar los trabajos. Vea algunos ejemplos que ilustran la necesidad del análisis completo del contenido recolectado:

- dentro de un documento pdf referenciado en el website se pueden encontrar emails que identifiquen el(los) blanco(s) de la investigación;

- un vídeo embutido en un website internacional puede estar hospedado en el datacenter de un proveedor nacional, de acceso más fácil para la justicia brasileña;

- una imagen aparentemente inofensiva puede contener mensajes implícitos dirigidas para fines criminales a través de técnicas de esteganografía

Sabemos no obstante que una investigación con este nivel de exigencia puede demandar mucho tiempo para ser concluida, mientras que el website investigado puede sufrir actualizaciones o incluso ser retirado del aire en este período, dificultando bastante el proceso.

Entonces es necesario la gestión local del contenido investigado, a partir de fotografías (snapshots) completas e incrementales del website investigado. Esta metodología consiste en mantener localmente todas las informaciones posibles de un website, incluso su histórico de actualizaciones. Utilizando este enfoque, el investigador puede obtener las siguientes informaciones:

- Almacenamiento de todo el contenido del website localizado en su servidor (host) principal, aquel que la URL denunciada apunta;

- Fecha y hora en que fueron recolectadas las informaciones anteriores;

- Informaciones sobre actualizaciones del website de forma organizada, donde es posible conocer exactamente lo que fue modificado en el website y en que fecha/hora aproximadas ocurrieron las actualizaciones.

- Listado de todas las referencias (links) del website, con posibilidad de obtener el contenido hospedado en estos websites referenciados.

- Reorganización de los datos para mayor eficiencia en el análisis del contenido. (ej: organizar todas las imágenes en un único directorio para visualización o incluso para automatizar tareas de quiebra esteganográfica)

- Obtener archivos que fueron publicados por equivocación y rápidamente retirados del website investigado.

- Garantía del almacenamiento de las pruebas, sin depender del proveedor responsable del hospedaje, incluso cuando el contenido es retirado.

• Automatización de tareas en general. (ej: análisis automático de imágenes o texto a partir de softwares inteligentes)

Un software bastante popular para la captura y replicación de websites es Httrack Website Copier [10], disponible libremente para plataformas Unix y Windows. En Debian GNU/Linux y sus distribuciones derivadas, el httrack puede ser instalado por el administrador de paquetes nativo (APT), conforme ilustrado a continuación:

```
root@ntccc:/home/ntccc# aptitude install httrack
```

[10] http://httrack.com

A continuación aparece un ejemplo de uso del Httrack, donde el website http://www.ejemplo.com es clonado para el sistema local del usuario a partir del siguiente comando:

```
httrack http://www.ejemplo.com/ -O /tmp/ejemplo.com +* -r6 -v
```

Los parámetros +* -r6 anteriores limitan el nivel de profundidad de URLs linkadas en este website en como máximo 6, sin restricción de dominio. El -v hace que el programa ofrezca detalles de la operación en tiempo real para el usuario. Para actualizar un clon ya existente, utilice el comando siguiente:

```
root@ntccc:/ejemplo.com# trac --update
```

Estos y otros diversos comandos del Httrack pueden ser consultados directamente en la documentación disponible en el website del programa. Para utilizar el software por medio de una interfaz gráfica más simple, el investigador puede optar por las versiones WinHttrack para Windows o WebHttrack para GNU/Linux. Las figuras siguientes ilustran la utilización del WebHttrack, que puede ser fácilmente instalado y ejecutado en un sistema Debian por medio de los comandos:

```
root@ntccc:~# aptitude install webhttrack
root@ntccc:~# webhttrack
```

Basta seguir los pasos, exhibidos de manera auto-explicativa, para realizar la captura o actualización de los websites deseados.

3.3.3 Recuperando contenido ya retirado de un website

Cuando un website reportado ya fue retirado de Internet, ya sea por su dueño o por el proveedor de hospedaje, la recogida de evidencias a partir de su contenido puede ser considerablemente dificultada. En este caso no será posible capturar su contenido, como vimos en **3.3.2.1 Aspectos técnicos de la investigación**. Restan entonces las siguientes alternativas:

Figura 3.6: Httrack - Entrada de URLs para recogida de contenido

Figura 3.7: Httrack - Download del website en ejecución

Figura 3.8: Httrack - Navegando después de finalización del download del website

1. Solicitar del denunciante este contenido. No siempre el denunciante es identificado, casi nunca guarda el contenido, como máximo posee un screenshot;

2. Solicitar del proveedor de hospedaje el contenido ya removido. En general necesita orden judicial, proceso dificultado cuando el proveedor se localiza fuera del país;

3. Intentar recuperar parte del contenido a través de servicios de cache en Internet. Difícil conseguir el contenido integral originalmente hospedado, sin embargo muy útil para recuperar textos publicados en HTML puro.

Note que los tres ítems anteriores no son mutuamente exclusivos. De hecho, mientras más correlaciones existan entre las informaciones suministradas por el denunciante, proveedor y servicios de cache, más consistentes serán las evidencias posteriormente presentadas a la justicia. Trataremos a continuación de algunos métodos de recuperación de contenido en fuentes públicas en la Web.

3.3.3.1 Cache de buscadores

Para la recuperación de contenido recién retirado de websites se pueden utilizar recursos de buscadores en Internet. El más popular de ellos es el buscador de Google, que ofrece una opción para visualización de snapshots recientes. Este servicio puede ser accedido a partir de los resultados de búsquedas realizados en el website http://www.google.com, haciendo clic en el link *En cache* conforme ilustrado en la figura 3.3.3.1. Alternativamente, se puede realizar una búsquedadirecta por el cache de un website con el formato cache:www.site-ejemplo.com.

Otros buscadores como http://www.yahoo.com o http:// www.bing.com ofrecen el mismo servicio gratuitamente y de forma semejante al anterior.

Figura 3.9: Opción de acceder cache a partir de un buscador de páginas

3.3.3.2 Cache del archive.org

El Internet Archive es una organización sin fines lucrativos fundada en 1996, en California, con el propósito de ofrecer acceso permanente a las colecciones históricas que existen en formato digital en Internet. El sitio hace público textos, audios, vídeos, softwares y páginas web archivadas. A través de la dirección http://www.archive.org/web/web.php es posible acceder a un website con el mismo contenido que era dispuesto en un instante del pasado. Este servicio fue nombrado como Wayback Machine (figura 3.10). La figura 3.11 exhibe un snapshot del website de la Procuraduría General de la República el 09 de octubre de 1997, recuperado a través de cache de la Wayback Machine.

Figura 3.10: Wayback Machine, servicio de Archive.org

Figura 3.11: website de la PGR en 1997, recuperado a través de cache

3.3.4 Como funciona el email

El email, a veces referido como "mensaje electrónico" o "correo electrónico", es un archivo digital usualmente compuesto por un remitente; uno o más destinatarios; un asunto; y un "cuerpo". El cuerpo del email es el propio mensaje a ser leído por el remitente y puede contener no solamente texto, sino archivos diversos (imágenes, vídeos, otros mensajes de email, etc.). Un mensaje de email contiene además una serie de meta-informaciones que instruyen a los softwares para que la entrega y el procesamiento del mensaje sean realizadas correctamente y con la mínima intervención humana. Veremos aquí cuales son estos softwares y como ellos interactúan desde la computadora doméstica hasta los servidores en Internet.

Atención: es necesario comprender el funcionamiento del Sistema de Nombres de Dominios (DNS) para acompañar esta sección. Este asunto es tratado en 1.3 Conceptos introductorios.

Para explicar el funcionamiento del email en Internet vamos a considerar el flujo del envío de un mensaje, conforme ilustrado en la figura 3.12:

Figura 3.12: Ejemplo de funcionamiento básico del email

1. Alice redacta un mensaje de email para Bob utilizando su "cliente de email" (o "software de email" como es popularmente conocido). Mozilla Thunderbird, Microsoft Outlook y los Webmails son ejemplos de softwares (o clientes) de email. En el lenguaje técnico este tipo de software es referido como MUA (Mail User Agent). Al recibir el comando para enviar el mensaje, el software se conectará al servidor SMTP configurado previamente por el usuario para intentar efectuar el envío. Un software que ofrece el servicio SMTP es también denominado MTA (Mail Transport Agent).

2. El servidor mx.a.org, en posesión del mensaje, necesita saber cual es el otro servidor SMTP en Internet que está autorizado para recibir los mensajes destinadas a Bob. Esto es hecho a partir de una consulta en el servidor DNS responsable del dominio del email de Bob [11].

[11] Recordando que, en una dirección de email, el dominio es aquello que viene después de la @ (arroba)

3. El servidor ns.b.org, responsable de los nombres del dominio b.org, responde a la mx.a.org que mx.b.org es el servidor autorizado para recibir los mensajes destinados a Bob (y a todos los usuarios de email @b.org).

4. El servidor mx.a.org envía entonces el mensaje para el servidor SMTP mx.b.org. Observe que mx.b.org también ofrece el servicio POP3 para que sus usuarios accedan a los emails.

5. A partir de su computadora personal, Bob utiliza su cliente de email (o MUA) para conectar en el servidor de entrega de emails a través del protocolo POP3 y realiza el download del email enviado por Alice para su computadora personal.

La figura 3.12 resume el funcionamiento del email en Internet. Veremos no obstante que en la práctica es común encontrar escenarios un poco más complejos que, sin

embargo, no intimidarán al investigador que comprendió bien la estructura básica ilustrada en nuestro ejemplo.

3.3.5 "Disecando" un mensaje de un email legítimo

A partir de un mensaje de email, se pueden obtener inmediatamente las siguientes informaciones:

- El contenido del mensaje (incluyendo los archivos anexados)
- La dirección de email del remitente del mensaje
- Las direcciones de email de los destinatarios del mensaje
- La dirección IP de la computadora que envió el mensaje
- Las direcciones IP de las computadoras en las cuales el mensaje transitó hasta llegar al destino

Vimos que un mensaje de email está formado básicamente por su contenido explícito (aquel que el remitente quiere que el destinatario lea) y por un encabezamiento (header) de texto con informaciones que instruyen a las computadoras a procesarlos correctamente. Estas informaciones dicen por ejemplo para donde el mensaje debe ser entregado y como el software lector de email debe exhibirlo para el usuario. De una manera general, el encabezamiento de un mensaje de email nos posibilita reconstituir el camino que el mensaje recorrió desde su envío hasta su recibimiento [12].

De la manera como fue especificado y funciona hasta los días de hoy, un encabezamiento de email puede ser forjado. Esta característica (o falla) permite la aplicación de diversos golpes en la red, como phishing scans y diseminación de virus, como veremos con más detalles a continuación.

En un primer análisis, identificaremos lo que cada campo significa en el siguiente mensaje de email legítimo enviado de contato@ joaobrito.info para alice@eumx.net [13]:

1	From joao@gmail.com Wed Jan 06 01:46:08 2010
2	Return-path: <joao@gmail.com>
3	Envelope-to: alice@eumx.net
4	Delivery-date: Wed, 06 Jan 2010 01:46:08 +0000
5	Received: from Debian-exim by eumx.net with spam-scanned (Exim 4.69)
6	(envelope-from <joao@gmail.com>)
7	id 1NSKy0-0007Ys-Mv
8	for alice@eumx.net; Wed, 06 Jan 2010 01:46:08 +0000
9	X-Spam-Checker-Version: SpamAssassin 3.2.5 (2008-06-10) on eumx.net
10	X-Spam-Level: *
11	X-Spam-Status: No, score=1.3 required=5.0 tests=AWL,SPF_PASS
12	autoleam=unavailable version=3.2.5
13	Received: from dspam by eumx.net with local (Exim 4.69)
14	(envelope-from <joao@gmail.com>)
15	id 1NSKy0-0007Yp-JV
16	for alice@eumx.net; Wed, 06 Jan 2010 01:46:08 +0000
17	Received: from Debian-exim by eumx.net with spam-scanned (Exim 4.69)
18	(envelope-from <joao@gmail.com>)
19	id 1NSKyM-0007Yg-2L

20	for alice@eumx.net; Wed, 06 Jan 2010 01:46:08 +0000
21	Received: from ey-out-2122.google.com ([74.125.78.24]:32995)
22	by eumx.net with esmtp (Exim 4.69)
23	(envelope-from <joao@gmail.com>)
24	id 1NSKyM-0007Yc-OA
25	for alice@eumx.net; Wed, 06 Jan 2010 01:46:06 +0000
26	Received: by ey-out-2122.google.com with SMTP id 9so481800eyd.29
27	for <alice@eumx.net>; Tue, 05 Jai 201017:46:05 -0800 (PST,
28	MIME-Version: 1.0
29	Sender: joao@gmail.com
30	Received: by 10.216.90.9 with SMTP
31	id d9mr1249245wef.201.1262742363580;
32	Tue, 05 Jan 2010 17:46:03 -0800 (PST)
33	Date: Tue, 5 Jan 2010 22:46:03 -0300
34	Message-ID:
35	<d470605b1001051746)651d06k8830793631c7€062@yriail.g-nail.com>
36	Subject: Saudades
37	From: Joao <contato@joaobrito.info>
38	To: Alice <alice@eumx.net>
39	Content-Type: text/plain; charset=ISO-8859-1
40	Content-Transfer-Encoding: quoted-printable
41	X-EUMX-Dspam: scanned by eumx.net, Wed, 06 Jan 2010 01:46:08 +0000
42	X-DSPAM-Result: Innocent
43	X-DSPAM-Processed: Wed Jan 6 01:46:08 2010
44	X-DSPAM-Confidence: 1.0000
45	X-DSPAM-Probability: 0.0023
46	X-DSPAM-Signature: 4b43eb60290645329814613
47	X-UID: 973
48	Status: RO
49	X-Status: A
50	
51	Hola, ¿cómo estás?
52	

[12] la RFC 2076 (Common Internet Header Messsages) especifica con detalles el formato de un encabezamiento, a pesar de que sea común encontrar algunas modificaciones en el día a día
[13] el mensaje es real. Las direcciones fueron modificadas para proteger la privacidad de los usuarios. Algunos campos específicos del servicio Gmail fueron también retirados

Hay 7 campos que estarán siempre presentes en un mensaje de email. Ellos son:

- From: identifica el remitente
- To: identifica el destinatario
- Subject: asunto del mensaje
- Received: camino detallado recorrido por el mensaje
- Content-: informaciones sobre el contenido del mensaje
- Date: fecha de envío del mensaje por el remitente
- Message-ID: identificador único del mensaje

En el ejemplo anterior, notamos que las líneas 37 y 38 indican el remitente y destinatario del mensaje, respectivamente [14]. En la línea 36 está el asunto del mensaje: "Saudades". Las líneas 39 y 40 contienen informaciones sobre el contenido (cuerpo) del mensaje, que en este caso es un mensaje en texto puro plain text con codificación de caracteres en el estándar ISO-8859-1. La línea 33 exhibe el momento en que el mensaje fue enviado por el usuario remitente. En las líneas 34 y 35 tenemos el identificador único del mensaje, generado en el momento del envío por el software del remitente.

Para las finalidades de la investigación, uno de los campos más importantes es el Received: En general el análisis de los campos Received posibilita al investigador conocer todo el camino recorrido por el mensaje. Un mensaje de email puede pasar por diversos servidores hasta llegar a la computadora de destino. Toda vez que el mensaje pasa por un servidor, este adiciona un nuevo Received: con informaciones sobre el origen, fecha y próximo destino del mensaje. A pesar de que pueda contener modificaciones, el campo Received: usualmente posee el siguiente estándar (generalmente no respeta los saltos de línea siguientes, forzados aquí para mejor comprensión):

Received: from <servidor de origen>by <servidor que recibió este mensaje> with <protocolo usado en la transferencia> id <identificador único del mensaje>for <dirección de email del destinatario>;<fecha/hora en que fue recibida por el servidor>

[14] Note que para el destinatario, la dirección del remitente será contato@joaobrito.info. No obstante, el análisis del encabezamiento del mensaje, en especial el campo Sender: nos muestra que la dirección real de envío es joao@gmail.com. La modificación en el campo From: es posible a través del propio software de lectura de email y es un artificio utilizado para definir identidades diferentes utilizando el mismo servidor SMTP para envío de los mensajes.

Los campos Received: deben ser analizados de abajo para arriba, manteniendo así la consistencia cronológica del camino recorrido por el mensaje. Observando entonces las líneas 30 y 31 de nuestro primer ejemplo, podemos inferir que:

- El servidor MTA que recibió inicialmente el mensaje posee dirección IP 10.216.90.9;
- El protocolo utilizado para el envío fue el SMTP;
- El identificador de este mensaje en este servidor MTA es d9mr1 249245wef.2O1.126274236358O[15];
- El mensaje fue recibido por este servidor el 05 de enero de 2010 a las 17:46:03 -0800 (PST)[16];

Las líneas 21 a 25 ilustran el momento en que el mensaje deja los servidores de Google (Gmail) y llegan a las máquinas del proveedor eumx.net, responsable del servicio de email del destinatario (alice@eumx.net). Tenemos entonces las siguientes informaciones:

[15] Este identificador es importante ante la necesidad de confirmar la veracidad del envío, a partir de los logs generados por el servidor.
[16] Nunca olvide observar la referencia UTC!. Consulte 1.6 Conceptos introductorios para más detalles.

- El servidor MTA de origen es ey-out-2122.google.com, de dirección IP 74.125.78.24 y puerta de origen de la conexión 32995;

- El servidor que recibió el mensaje es eumx.net, a través de protocolo ESMTP. Tenemos además una información extra: el software y la versión del servidor de email utilizado en este servidor (Exim 4.69). Es posible también confirmar el email de origen (envelop-from <joao@gmail.com>).
- El identificador del mensaje en este servidor es 1NSKyM- -OOO7Yc-OA
- El destinatario es alice@eumx.net
- A mensaje llegó a este servidor el 06 de enero de 2010 a las 01:46:06 +0000 (¡atención a la referencia UTC!)

Como ejercicio, sugerimos que el lector "reconstruya" todo el trayecto del mensaje hasta su destino final.

Profundizando un poco más el análisis, estaremos aptos para extraer otras informaciones que pueden ser útiles en la investigación:

- En un encabezamiento de email, los campos que comienzan con una X - son campos que generalmente no están especificados por ningún organismo de estandarización, sin embargo son utilizados para instruir algunos softwares involucrados en el intercambio de mensajes en Internet. En nuestro ejemplo podemos verificar entre las líneas 9-11 y 39-44 informaciones sobre una herramienta anti-spam llamada DSPAM. Por los valores de estos campos, podemos constatar que el servidor al lado del eumx.net posee esta herramienta instalada, que hizo la verificación en este mensaje e indicó en un alto nivel de confianza que **no** se trata de un SPAM. Estas marcaciones en el encabezamiento pueden instruir por ejemplo un software lector de email a realizar filtrados automáticos de spam a partir de los valores en los campos X-DSPAM.

- Hay tres timezones diferentes durante el curso del mensaje hasta su destino. Del lado del remitente, podemos verificar que la marcación de fecha (campo Date:) está tres horas atrasadas en relación al UTC (Tue, 5 Jan 2010 22:46:03 -0300). Notamos posteriormente que al llegar a los servidores de Google, la referencia cambia para la hora del Pacífico (-0800 (PST)). Enseguida, tenemos los registros en referencia UTC +0000 en los servidores del proveedor EUMX, o sea, posiblemente localizados en una región próxima del meridiano de Greenwich.

- Es posible notar también que la fecha de envío del mensaje y la fecha del recibimiento en el primer servidor de Google corresponden a un instante muy próximo (menos de un segundo de diferencia). Basta convertir las dos fechas para una misma referencia UTC: Tue, 5 Jan 2O1O 22:46:O3 -O3OO (línea 32) y Tue, O5 Jan 2O1O 17:46:O3 -O8OO (PST) (línea 31). Ambas corresponden al día 06 de enero de 2010, 01:46:03 +0000 (UTC). Esta información nos permite desconfiar de la posibilidad de que el mensaje haya sido enviado a partir de un software presente dentro de la estructura de Google, debido al cortísimo intervalo de tiempo entre el envío y el recibimiento en el servidor de la empresa. O sea, hay una gran posibilidad de que este mensaje haya sido enviado a través del Webmail que el servicio que Gmail ofrece a sus usuarios. Otra evidencia es la dirección IP del primer servidor en que el mensaje llega (10.216.90.9). Esta dirección pertenece a una banda reservada de direcciones para redes internas y no es ruteable en Internet (consulte 1.2 **Conceptos introductorios** para más detalles). Una solicitación de logs de conexión a Google y una posterior confrontación con los registros y cookies del navegador en la computadora del investigado pueden reforzar las

evidencias para que aun tengan valor jurídico incluso en la situación en que el mensaje no esté más disponible para confirmación de la autoría.

• La verificación del estándar de codificación de caracteres del mensaje, sumándose la información de huso-horario en la fecha del envío, puede suministrar una indicación de la localización geográfica del remitente. En este caso tenemos la codificación ISO-8859-1, estándar también conocido como Latin1, utilizado en alfabetos latinos (que demandan acentuación), muy utilizado en Brasil. El huso-horario de envío es el UTC -3, que cubre la mayor parte del país, durante casi todo el año.

• El mensaje llevó solamente 5 segundos para ser entregado al destino final. La posibilidad de que el encabezamiento del mensaje no haya sido forjado durante su curso es grande. **Generalmente mensajes modificados a lo largo del camino sufren un atraso mayor en la entrega**. Es importante recordar que todos los servidores por los cuales el mensaje pasó deben tener sus relojes sincronizados para que la información de tiempo tenga algún valor. Vea más sobre la importancia de utilizar el NTP para este propósito en **1.6 Conceptos introductorios**.

3.3.6 Disecando un mensaje de email forjado

Figura 3.13: email forjado en nombre de la Policía Federal

En la figura 3.13, que exhibe el encabezamiento simple y el cuerpo de un mensaje supuestamente enviado por la Policía Federal, podemos extraer algunas características que son comunes en emails forjados para objetivos ilícitos:

• Texto mal escrito, generalmente con errores groseros de la lengua española y falta de acentuación. Se nota en el propio asunto la escritura de la palabra “ACESO”.
• Letras mayúsculas con el objetivo de llamar la atención. Toda organización que posee un departamento autorizado para enviar emails para sus clientes o usuarios está consciente de las reglas básicas de etiqueta y evita utilizar este recurso.
• Email disponible **solamente** en formato HTML.
• El contenido del mensaje generalmente implica una obligación que, si no es cumplida, traerá algún perjuicio para la víctima. El cumplimento de tal obligación puede ser realizada a través del suministro de informaciones sensibles o acceso a un link ofrecido por el criminal, que llevará a la víctima a un website o código malicioso.
• Fecha y hora incorrectas e/o inconsistentes. Es común observar fechas futuras y horarios fuera del expediente usual de trabajo. En este caso tenemos que el email fue recibido por el MTA de la víctima a las 00:05. Esto significa que el mensaje fue supuestamente enviado en un horario bastante próximo a este.
• Impersonalidad: como el mensaje es destinado a millares (a veces millones) de usuarios, la víctima es tratada con impersonalidad. En este caso fue utilizado el “Señor/Señora”.

Además de las claras evidencias que denuncian el mensaje a partir de su contenido explícito, es posible identificar una serie de informaciones en el encabezamiento que confirman que el email es forjado y pueden suministrar pistas sobre la autoría:

1	Return-Path: <aline@juno.com>
2	X-Originating-IP: [194.90.6.38]

3	Received: from 127.0.0.1 (EHLO mxout10.netvision.net.i1)(194.90.6.38)
4	by mta114.mail.ac4.yahoo.com with SMTP;
5	Fri, 22 Jan 2010 20:06:35 -0800
6	MIME-version: 1.0
7	Content-type: multipart/mixed;
8	boundary="Boundary_(ID_P3iKx3U1pYx1tr9TsQ)"
9	Received: from bvzu.net ([201.14.123.152])
10	by mxoutl0.netvision.net.il
11	(Sun Java(tm) System Messaging Server 6.3-9.01
12	with ESMTPAid 4JKVV000E5EM1ZPU10@mxout10.netvision.neti›;
13	Sat, 23 Jan 2010 06:06:34 +0200 (1ST)
14	Message-id: <OKW000E5WM2SPU10@mxout10.netvision.net.il>
15	From: POLICIA FEDERAL <policiafederal@pf.gov.br>
16	To: xxxxxxxxxxxxx <xxx>000000000(gyahoo.com.br>
17	Subject: POLICÍA FEDERAL, ESCLARECIMIENTO DE ACESO ILEGAL.
18	Date: Sat, 23 Jan 2010 02:05:04 +0000 (Hors)
19	X-Priority: 3
20	X-MSMail-priority: Normal
21	X-Mailer: Microsoft Outlook Express 6.00.2462.0000
22	X-MIMEOLE: Produced By Microsoft MimeOLE V6.00.2462.0000
23	Content-Length: 2246

En la línea 9 verificamos que el MTA que inicialmente disparó el mensaje se presenta como bvzu.net. Es importante saber que esta identificación es suministrada por el software MTA del remitente y es uno de los campos preferidos para forjar. No obstante existe dentro de los paréntesis una información valiosa que desmentirá la información suministrada por el remitente.

Además en la línea 9, dentro de los paréntesis observamos la dirección IP 201.14.123.152. Esta dirección, al contrario de lo que ocurre en relación a la información presente fuera de los paréntesis, es suministrado por el MTA que recibió el mensaje, en este caso el mxout1O.netvision.net.il. En circunstancias normales, el dominio bvzu.net debería corresponder a la dirección IP 201.14.123.152, pero al realizar una consulta de DNS para el dominio bvzu.net, observamos que este dominio no posee ninguna dirección IP asociada a él:

```
1 $ dig +noall +answer bvzu.net
2 $
```

Confirmamos también que el referido dominio ni siquiera está registrado:

1	$ whois bvzu.net
2	
3	Whois Server Version 2.0
4	
5	Domain names in the .com and .net domains can now be registered
6	with many different competing registrars. Go to http://www.internic.net
7	for detailed information.
8	

9	No match for "BVZU.NET'.
10	>>> Last update of whds database: Tue, 02 Feb 2010 16:18:32 UTC <<<

Reforzando las evidencias, una consulta de DNS para la dirección IP 201.14.123.152 indica que esta está asignada para Brasil, bajo responsabilidad del proveedor Brasil Telecom, conforme el resultado del comando siguiente:

1	$ dig +noall -Fanswer -x 201.14.123.152
2	152.123.14.201.in-addr.arpa. 77860 IN PTR
3	201-14-123-152.gnace703.dsl.brasiltelecom.net.br.

Note además que el FQDN para la dirección IP consultada sugiere que esta es asignada para el servicio de Internet banda ancha de Brasil Telecom a través de tecnología DSL: 2O1-14-123- 153.gnace7O3.dsl.brasiltelecom. net.br. Todo indica que se trata de una computadora doméstica, conectada a Internet a través del servicio DSL de Brasil Telecom y que fue utilizada para disparar el email malicioso en nombre de la Policía Federal.

Podemos además localizar la región en Brasil en que esta dirección IP está asignada. El servicio gratuito de la empresa Maxmind puede suministrar con cierta precisión datos georreferenciales de un dado IP. En este caso, una consulta a través de la URL http://www.maxmind. con/app/locate_ip?ips=201.14.123.152 certifica que esta dirección está asignada para Brasilia, conforme podemos verificar en la figura 3.14.

Una información precisa sobre la entidad responsable sobre esta dirección debe ser obtenida a través de Registro.br. Al realizar la investigación a través de la URL http://whois.registro.br constatamos que de hecho Brasil Telecom S/A, a través de su Filial en el Distrito Federal, es el proveedor que responde por la dirección:

inetnum:	201.14/16
asn:	AS8167
ID abusos:	BTA17
entidad:	Brasil Telecom S/A - Filial Distrito Federal
documento:	076.535.764/0326-90
responsable:	Brasil Telecom S. A. - CNBRT
dirección:	SEPS 702/092 Cj. B - BI B 3 andar Gen. Alencastro, S/N,
dirección:	70390-025 - Brasilia - DF
país	BR
teléfono:	(61)4154201 [ ]

Figura 3.14: Consulta por localización geográfica de una dirección IP

El campo Received: anterior suministra solamente las informaciones del recibimiento del mensaje posteriormente por el MTA de yahoo. con. Verificamos por tanto que desde el envío del mensaje hasta el recibimiento no hubo ninguna participación de servidores de la Policía Federal, que deberían estar debajo de los dominios .dpf.gov.br. Hasta el momento, podemos inferir que el mensaje partió de una máquina localizada en Brasilia, posteriormente enviada para un MTA de un proveedor localizado en Israel, que

finalmente entregó en el MTA del destinatario, perteneciente al servicio de email de Yahoo Inc.

Buscando confirmar al menos los datos referentes al proveedor Brasileño, será necesario solicitar a la empresa Brasil Telecom S/A las informaciones de registro referentes al terminal telefónico utilizado para realizar la conexión que originó el envío del email malicioso en aquel instante.

Se recomienda también que sea solicitado informalmente al proveedor localizado en Israel, netvision.net.il, los registros (logs) referentes al envío del referido mensaje. Se debe enviar al proveedor por lo menos el identificador único presente en el encabezamiento: <OKWOOOE5WM2SPU1O@mxout1O.netvision.net.il>. La información suministrada por el Netvision puede fortalecer las pruebas y certificar con precisión el momento del envío y fortalecer el material probatorio al final del análisis.

Vale resaltar que en la solicitud enviada a Brasil Telecom S/A, es necesario que sean especificados la dirección IP investigada, el horario y referencia UTC en que el mensaje fue enviado. Para el caso en cuestión, la dirección IP es 201.14.123.152, el horario de envío es Sat, 23 Jan 2010 06.06.34 y la referencia UTC es +0200 (IST).

¿Por qué no confiar en el campo Date:?

El caso que analizamos es un buen ejemplo para responder esta pregunta. Debemos primeramente recordar que las direcciones IP suministradas para usuarios domésticos generalmente son dinámicas y por eso el horario de la conexión en los pedidos de violación de confidencialidad debe ser preciso. Vimos también que el campo Date: en el encabezamiento de email es insertado por el cliente de email del remitente, que a su vez utiliza el horario del sistema operativo del usuario, este que usualmente no está sincronizado con referencias confiables de tiempo. Por otro lado, servidores en Internet, en especial aquellos que ofrecen servicios a muchos usuarios, generalmente utilizan el NTP para sincronizar sus relojes. En nuestro ejemplo podemos notar que el horario marcado en el campo Date: del mensaje es el Sat, 23 Jan 2O1O O2:O5:O4 +OOOO, mientras que el servidor MTA del proveedor NetVision.net.il certifica que recibió el mensaje en el horario 23 Jan 2010 06:06:34 +0200 (IST). Convirtiendo para UTC, tenemos una diferencia de aproximadamente dos horas entre el envío y el recibimiento del mensaje por el MTA de NetVision. net.il, lo que es un atraso fuera del estándar. Para reforzar que el horario definido en el campo Date: está incorrecto, podemos recurrir al último MTA que recibió el mensaje antes de ser entregado al usuario, que en este caso es el MTA del servidor mta114.mail.ac4.yahoo.com, de Yahoo Inc.. Este servidor marcó el recibimiento del mensaje en el horario Fri, 22 Jan 2O1O 2O:O6:35-O8OO, que corresponde a solamente 1 segundo de diferencia del horario en que el MTA anterior recibió, lo que es un tiempo bastante razonable para este tipo de tráfico. Es por tanto mucho más prudente confiar en los relojes de dos grandes proveedores de Internet que parecen estar debidamente sincronizados que utilizar precipitadamente el horario marcado por la computadora personal del remitente. Sería muy probable recibir los datos de registro de otro suscriptor que no sea aquel dueño de la máquina utilizada para el envío del email, en caso que utilizásemos el horario del campo Date: para la solicitud enviada a Brasil Telecom S/A.

Por fin, cabe resaltar que desgraciadamente estamos lejos de conocer los detalles sobre la autoría del crimen. Al suministrar los datos del suscriptor, el procedimiento de investigación puede por ejemplo concluir que el sistema utilizado para enviar el mensaje en nombre de la PF estaba comprometido. O sea, el suscriptor no fue responsable directo por el envío del mensaje, pero su sistema era mal administrado, había sufrido una intrusión y estaba siendo utilizado por criminales para diseminar emails maliciosos en Internet.

3.4 Phishing Scam

Phishing, o phishing scam son términos creados para describir el tipo de fraude por Internet donde un mensaje electrónico no solicitado es enviado masivamente con el objetivo de inducir el acceso a sitios falsificados capaces de capturar informaciones confidenciales de los destinatarios. Es también común que los phishings instalen silenciosamente códigos maliciosos en la computadora de la víctima.[17]

La palabra "phishing" es una variación de fishing (“pesquería”) y su uso fue registrado por primera vez en 1996, probablemente influenciado por el término “phreaking”.[18] En este tipo acción, son enviadas “carnadas” (e-mails), que intentan hacerse pasar por instituciones conocidas con la intención de “pescar” contraseñas u otras informaciones sensibles de Internautas. El caso abordado en la sección anterior e ilustrado en la figura 3.13 es un ejemplo de phishing scam que intenta pasarse por un email legítimo de la Policía Federal.

[17] Cartilla de Seguridad para Internet Versión 4.0 del CERT.br http://cartilha.cert.br/golpes/#2.3
[18] http://en.wikipedia.org/wiki/Phishing

Nota sobre phishing Scam

Veremos que el phishing scam demanda del investigador la habilidad de rastrear un mensaje de email, recolectar informaciones de un sitio Web y a veces realizar análisis minucioso en códigos de alta complejidad. A pesar de que algunos tópicos sean abordados en otras secciones de este Guión, consideramos importante apuntar aquí algunos conceptos y medios de investigación enfocados en las peculiaridades de este tipo de crimen, que es tan aplicado en Brasil. Para elaboración de este tópico, utilizamos principalmente [Ligh et al. 2010] y [Malin Eoghan Casey 2008], en conjunto con la experiencia práctica del NTCCC de la PR/SP.

De una manera general, en el cuerpo del email phishing hay un link que al ser accionado solicitará de la víctima una de las siguientes acciones:

1. El llenado de formularios con datos privados, como contraseñas bancarias e informaciones personales. En este caso es exhibido al usuario un sitio Web fraudulento, comúnmente constituido como copia visual fiel de otro sitio legítimo. Puede haber dificultad en apuntar diferencias entre los dos, a depender del nivel de sofisticación del golpe. La figura 3.15 ilustra un ejemplo.

2. El download de un software malicioso (“malware”) que, al instalarse en el sistema de la víctima, podrá ejecutar innumerables actividades con el objetivo de recolectar informaciones privadas necesarias para la aplicación del golpe planificado. Las figuras 3.16 y 3.17 ilustran dos bases de datos criminales conteniendo informaciones bancarias

de las víctimas de phishing, respectivamente almacenadas en archivo de texto y SGBD SQL.

Las próximas secciones presentan algunas técnicas utilizadas para investigar el phishing. El principal objetivo será la obtención de informaciones que puedan revelar detalles de la autoría. Cabe resaltar que muchas veces las técnicas abordadas en la literatura disponible en este asunto, incluyendo el presente Guión, no siempre presentarán resultados satisfactorios. La actividad de phishing está en constante evolución técnica y casi siempre cuenta con un factor sorpresa a ser desvendado por el investigador más atento. Trataremos por tanto de algunos fundamentos básicos para comprender y combatir estos golpes, listando también las herramientas que consideramos más interesantes para los propósitos de su investigación.

Figura 3.15: Ejemplo de sitio Web forjado para captura de datos bancarios

Figura 3.16: Datos bancarios de víctimas de phishing almacenados en archivo de texto

3.4.1 Preparación del ambiente de investigación

Para mayor seguridad y practicidad es recomendado el uso de una máquina virtual (Virtual Machine) para la realización de los procedimientos de investigación del phishing scam. Una máquina virtual, popularmente referenciada como VM, es un software que permite la instalación de un sistema operativo "dentro" de otro, funcionando de forma independiente.

Figura 3.17: Datos bancarios de víctimas de phishing almacenados en SQL

Algunos beneficios en la utilización de VMs son listados a continuación:

- La computadora hospedera (o sea, el sistema principal que hospeda una o más VMs) permanece aislada, evitando así posibles daños que los procedimientos puedan causar al sistema operativo;

- La VM permite que sean tirados snapshots, que son “fotografías” del estado del sistema. Es posible por tanto almacenar un snapshot antes de iniciar la investigación y, después de finalizarla, traer el sistema para su estado inicial, "limpio";

- Pueden ser creadas diversas VMs en el mismo hospedero, simulando así un ambiente de red para comprender mejor el funcionamiento de un malware;

- Todo lo que está en la VM queda almacenado solamente en un archivo en el disco duro del hospedero, hecho que simplifica rutinas de backups, duplicaciones y transporte.

Hay una variedad de softwares para virtualización disponibles, incluyendo programas libres y/o gratuitos. Recomendamos el uso de VirtualBox [19], un software libre que puede ser instalado en sistemas operativos GNU/Linux, MacOS, Solaris y Windows.[20]

3.4.2 Investigación de sitios Web "falsificados"

La investigación de un sitio Web fraudulento, generalmente referido en los emails de phishing, consiste en navegar por su ambiente con el objetivo de comprender su funcionamiento, obteniendo así el mayor número de informaciones posibles acerca del golpe.

A partir de una máquina virtual preparada para este fin, el investigador seguirá algunos pasos para alcanzar su objetivo:

• Abrir el email phishing y hacer clic en el link que esté en el cuerpo del mensaje, simulando el comportamiento de la víctima. Al hacer clic en este link verificar el comportamiento del navegador y para cual sitio el internauta es conducido. Esto puede también ser hecho por medio de un análisis directo en el código HTML del mensaje.

• Confirmar si realmente se trata de un sitio engañoso, falso. Esto es posible verificando la URL exhibida en la barra de direcciones del navegador o informaciones del certificado de seguridad que el sitio original generalmente presenta. Más informaciones pueden ser consultadas en la Cartilla de Seguridad para Internet Versión 4.0 del CERT.br;[21]

[19] http://www.virtualbox.org/
[20] Es importante resaltar que algunos códigos logran detectar que están siendo ejecutados en máquinas virtuales, y con esto ejecutan acciones específicas para dificultar la investigación.

• Al constatar que se trata de un golpe, se inicia entonces el estudio del funcionamiento de las páginas de este sitio Web. Podemos por ejemplo insertar informaciones bancarias falsas en los campos del formulario para verificar su funcionamiento;

• Exhibir el código fuente de las páginas para verificar posibles URLs utilizadas por el sitio fraudulento; [22]

• Intentar acceder a directorios y archivos del sitio directamente por la barra de direcciones del navegador. Muchas veces el autor se olvida de insertar una página estándar (en general el index.html) para ocultar el contenido de los directorios, posibilitando que el investigador tenga acceso a la lista con todos los archivos allí presentes, incluyendo fechas de modificaciones y otras informaciones útiles. La figura 3.18 ilustra una situación en la cual fue posible tener acceso a toda la lógica del golpe por descuido del criminal;

• Intentar localizar la consola (shell) utilizada por el autor del fraude. Generalmente, en conjunto con los archivos del sitio falsificado hay uno que es utilizado para manipular archivos e interactuar con el servidor de hospedaje. Por medio de este archivo, que normalmente es una página Web dinámica escrita en PHP, será posible retirar, modificar, hacer upload y download de otros archivos en el servidor. Consecuentemente, el investigador que logra localizarlo puede obtener una copia local de todos esos archivos, que revela toda la lógica del golpe, incluyendo el destino dado a los datos de las víctimas.

[21] http://cartilha.cert.br/golpes/
[22] Esto puede ser hecho haciendo clic con el botón derecho del mouse en la página y escogiendo la opción “código-fuente” o “exhibir código-fuente”

Después de las etapas listadas anteriormente, se debe realizar un análisis de todas las informaciones y archivos encontrados con el objetivo de descubrir posibles direcciones de email, URLs y servidores de base de datos que puedan revelar la autoría del crimen. Consulte otras buenas prácticas y softwares de apoyo para investigación de sitios Web en general en la sección **3.3 Aspectos técnicos de la investigación**.

Figura 3.18: Archivos de sitio Web fraudulento expuestos

3.4.3 Investigación en software malicioso

La investigación en programas maliciosos, o malwares, es más compleja y muchas veces exige del investigador habilidades en diferentes áreas de la computación, como por ejemplo lenguaje de montaje (Assembly, APIs del sistema operativo, encabezamientos de archivos binarios, análisis de tráfico de red, sistemas de archivos, compiladores, lenguajes de programación, depuradores (debuggers), etc.

En la investigación de malwares se utiliza básicamente dos tipos de análisis, los cuales chamamos **estático** y **dinámico** (o comportamental). En el análisis estático son empleadas técnicas de ingeniería reversa de software, o sea, se intenta comprender el funcionamiento del malware por medio del análisis de los códigos - al revertirlos para una forma legible - dispensando la ejecución. Ya en el análisis dinámico, se ejecuta el malware (en una máquina virtual) y a través de softwares específicos se monitorea su comportamiento, por medio de las modificaciones e interacciones que él realiza con el sistema operativo, con el usuario y con el ambiente de red. Los dos tipos de análisis son abordados a continuación.

Figura 3.19: Phishing en nombre de la Recaudación Federal enviado por correo tradicional

Alguien ya puede haber hecho el trabajo

Antes de iniciar cualquier análisis, recomendamos que sea utilizado un software para identificación de malwares, o algún servicio (hay diversos gratuitos) online, como en http://virusscan.jotti.org y http://www.virustotal.com. La oportunidad de que un programa malicioso ya haya sido identificado anteriormente por otras personas es grande y, en este caso, alguien puede haber efectuado y publicado en Internet detalles acerca del comportamiento del ejecutable, lo que evitaría trabajo duplicado en algunas fases de la investigación. La figura 3.21 ilustra el resultado de uno de estos servicios.

3.4.3.1 Análisis estático

Antes de conocer los softwares utilizados en la ingeniería reversa es importante entender un poco acerca del formato de archivo ejecutable del sistema operativo Windows, ya que esta plataforma ha sido la más utilizada para diseminar malwares. Es también interesante saber un poco sobre los compactadores de ejecutables, muy utilizados en los malwares para dificultar la investigación.

Figura 3.20: Phishing con nombre del destinatario en el cuerpo del mensaje

Figura 3.21: Análisis online de malware a través de http://virusscan.jotti.org

El formato *Portable Executable*

Los sistemas operativos Windows de 32 y 64 bits utilizan un formato único para archivos ejecutables, especificado como Portable Executable (o PE). El término "portable" se debe a la portabilidad en el sistema de 32 bits (y, por extensión, al de 64 bits) para sus diversas versiones. Básicamente, el formato PE es una estructura de datos que mantiene encapsuladas las informaciones que Windows necesita para administrar el código ejecutable. Esto incluye referencias a bibliotecas dinámicas, tablas de exportación e importación de la API y a los datos de gestión de recursos. El formato PE incluye, entre otros tipos, los archivos EXE (ejecutables), DLL (bibliotecas) y OBI (objetos). Por consecuencia, los malwares del tipo ejecutable en Windows serán siempre archivos PE.

Compactadores de PE

Compactadores PE, conocidos también como packers, funcionan como "zipadores" de ejecutables con una diferencia: archivos "zip", en su forma compactada quedan inaccesibles, mientras que ejecutables compactados, a pesar de estar "encogidos", continúan trabajando normalmente. [23]

Adicionalmente, cuando un archivo PE es compactado, su código es "mezclado". El compactador realiza una serie de operaciones en el archivo, suprimiendo espacios vacíos, modificando las secciones de posición, reorganizando el código y por fin inserta sus propias rutinas de descompactación. De esta manera, el tamaño del archivo es reducido y su código fuente original permanece escondido. En otras palabras, el uso de los packers en malwares dificulta la investigación por análisis estático, demandando etapas extras al procedimiento de investigación, que incluyen la identificación del tipo de compactación y al menos un medio eficiente para descompactación.

[23] http://www.numaboa.com/informatica/taller/181-reversa/488-compactadores

Herramientas para identificación de compactadores PE

Figura 3.22: PEiD detectando compactador de archivo PE

Hemos verificado en la práctica que en la mayoría de los casos los malwares están compactados con algún packer. Sin la debida identificación y eliminación de la compactación no será posible obtener informaciones relevantes por medio del análisis estático. Es necesario por tanto suprimir la rutina de compactación para proseguir con la investigación. Sin embargo, a depender del grado de complejidad y novedad del método utilizado, no será tan simple realizar el procedimiento de descompactación ("unpack").

Dos softwares utilizados para identificación de packers son el PEiD [24] y el ExEinfoPE[25]. El PEiD ofrece diversas funcionalidades, entre ellas la de identificar el packer utilizado en el archivo ejecutable. Posee además un "unpacker" genérico bastante útil, un analizador de criptografía para identificar el uso de la misma en el ejecutable y otras funciones relacionadas, además de permitir la instalación de complementos (plugins)

con funciones adicionales. El ExEinfoPE posee las mismas funciones del PEiD, sin embargo ha retornado más resultados que el primero. Adicionalmente, el ExEinfoPE exhibe consejos sobre donde encontrar la herramienta de “unpacking” adecuada para cada caso. Las figuras 3.22 y 3.23 ilustran screenshots de estos dos softwares en funcionamiento, que en ambos casos detectaron con éxito los compactadores utilizados.

[24] http://www.peid.info/
[25] http://www.exeinfo.xwp.pl/

Figura 3.23: ExEinfoPE detectando compactador de archivo PE

Búsqueda por estándares de textos (strings matching)

Superada la fase de eliminación de la compactación del ejecutable, la próxima etapa debe enfocarse en la búsqueda dentro del archivo por términos que suministren informaciones relevantes para la investigación. Existen diversos softwares que auxilian en este procedimiento. Algunos de los más populares son:

• **strings**: presente activamente en gran parte de las distribuciones GNU/Linux. En Debian este programa forma parte del paquete binutils. A través del es posible extraer todo el contenido textual de un determinado archivo.[26] A continuación aparece un ejemplo del uso de esta herramienta en conjunto con otra (grep) buscando la palabra complete dentro de un binario capaz de capturar datos bancarios del usuario, imprimiendo las 5 líneas anteriores y las 5 posteriores a la ocurrencia encontrada:

1	ntccc©ntccc:—$strings Bradesco.dcu Igrep -i "complete " -A 5 -B 5
2	ZYYd
3	n[yyi
4	jOhp
5	ZYYd
6	Bradesco
7	Complete el campo siguiente con la clave en un
8	rica indicada en el reverso de su cart
9	o, conforme posi
10	o solicitada.
11	ZYYd
12	n[yyi

• **Analogx TextScan**: software de búsqueda textual con interfaz gráfica para plataforma Windows [27]. La figura 3.24 exhibe un screenshot de este software en funcionamiento.

[26] Hay una versión gratuita para Windows en http://technet.microso0.com/en-us/sysinternals/ bb897439. Otra opción para utilizar comandos nativos del Unix en plataforma Windows es la utilización de emulación del ambiente operacional, tal como ofrecida por los softwares Cygwin y WinAVR
[27] http://www.analogx.com/contents/download/Programming/textscan/Freeware.htm

Como fue visto anteriormente, el comando strings puede ser utilizado en conjunto con otras aplicaciones, para suministrar innumerables posibilidades de consulta para el investigador. Hay diversas fuentes online ofreciendo consejos sobre búsquedas textuales y otras acciones más complejas utilizando comandos Unix, siempre muy útiles para la

investigación. En idioma portugués, recomendamos [Neves 2010]. Se deben concentrar las investigaciones en estándares de texto que vengan a revelar direcciones de email, URLs, nombres de dominio, direcciones IP, canales IRC y otras informaciones que el investigador considere relevantes.

Figura 3.24: Búsqueda textual por medio del software Analogx TextScan

Búsqueda por recursos: íconos, imágenes y cajas de diálogo (dialogs)

Es posible encontrar dentro de un archivo ejecutable algunos elementos que no son representados textualmente, como imágenes, íconos y cajas de diálogos, igualmente útiles para la comprensión del funcionamiento del malware. Un software recomendado para esta tarea es el PEBrowsePro. Esta aplicación posee diversas funcionalidades, entre ellas la de exhibir íconos, imágenes, DLLs y otras informaciones en formato binario presentes en el archivo analizado.[28]

Descompiladores

La propuesta de un descompilador es intentar convertir un archivo binario en su código fuente original, en un lenguaje de programación de alto nivel, o sea humanamente legible. Generalmente un descompilador es capaz de identificar solamente algunas funciones, recursos, formularios, strings, procedimientos y variables que fueron originalmente utilizadas, sin suministrar una reconstrucción completa del código original. No obstante, en la mayoría de los casos estas informaciones son suficientes para la comprensión de la lógica del programa investigado.

Parte del código generado por los compiladores aun permanece en lenguaje de montaje (Assembly), sin embargo de una forma más organizada y estructurada, facilitando bastante el entendimiento del programa analizado. Cabe resaltar que para cada lenguaje de programación es necesaria la utilización de un descompilador específico. Se nota que la mayoría de los softwares maliciosos diseminados en Brasil son escritos en los lenguajes de programación Delphi y Visual Basic. Listamos a continuación dos descompiladores que funcionan para estos lenguajes:

[28] http://www.smidgeonso&.prohosting.com/pebrowse-pro-file-viewer.html

- **DeDe**: descompilador para el lenguaje Delphi. A veces logra buenos resultados, recreando formularios, imágenes y procedimientos del código fuente original. Permite también que el resultado sea salvado como un “Delphi project”, pudiendo por tanto ser posteriormente analizado en la herramienta de compilación utilizada originalmente (Borland Delphi).[29] La figura 3.25 muestra la interfaz de ejecución del DeDe, mientras que la 3.26 exhibe el código descompilado siendo abierto como un proyecto en el Borland Delphi.

- **VB Decompiler Pro**: descompilador para el lenguaje Visual Basic. Identifica formularios, funciones, variables y strings. Genera código híbrido de Visual Basic y Assembly. Permite salvar el proyecto y posteriormente abrirlo en el propio Microsoft Visual Basic. [30]

Desmontadores (disassemblers) y Depuradores (debuggers)

Desmontadores son softwares que permiten convertir el contenido de un archivo ejecutable en el lenguaje de montaje (Assembly). Este es una lenguaje un poco más complejo de los que lamamos de "alto nivel", justamente porque se asemeja más con el lenguaje de máquina, interpretado por la computadora. Todavía, con un poco de conocimiento del lenguaje de montaje es posible comprender diversas funciones internas del malware, descubrir por ejemplo lo que él hace con las informaciones capturadas de los usuarios, cuales modificaciones realiza en la computadora, como hace para mantenerse oculto para dificultar la investigación, etc.

[29] http://www.softpedia.com/get/Programming/Debuggers-Decompilers-Dissasemblers/DeDe.shtml
[30] http://www.vb-decompiler.org/products/pt.htm

Figura 3.25: Descompilador DeDe en acción

Depuradores permiten la ejecución paso a paso, línea a línea, de un programa. Con ellos es posible observar los resultados de cada operación del malware y descubrir la función de cada línea del código Assembly. Estos son de gran utilidad para revelar fragmentos cifrados dentro del malware. Es común que strings y recursos importantes del código se encuentren cifrados. Ante un análisis más detallado, y contando con la ayuda de los debuggers, puede localizarse la función responsable de la desencriptación de las strings dentro del propio código. Posteriormente al descubrimiento de tal función, será posible insertar en aquel instante un breakpoint y ejecutar el malware hasta alcanzar este punto crítico del código. A partir de este momento, se ejecuta secuencialmente cada línea del código hasta obtener el retorno de la función con la string en texto simple. [31]

Listamos a continuación algunos disassemblers/debuggers:

• **OllyDbg**: ofrece función de disassembler/debugger para ambiente Windows. Posee interfaz gráfica con diversas opciones de análisis de código binario. Reconoce automáticamente strings y DLLs. Permite además la edición del código Assembly analizado [32]. La figura 3.27 exhibe una pantalla del OllyDbg.

• **Immunity Debugger**: programa basado en el OllyDbg, fue desarrollado por la empresa Immunity, ofreciendo como diferencial una API para el lenguaje Python. A través de esta API es posible escribir scripts en Python para manipular todo el proceso de depuración, tornando la herramienta bastante poderosa y flexible en el análisis de malwares.[33]

[31] Descriptografía de Strings en Malwares, Ronaldo Pinheiro de Lima, 17ª Reunión del Grupo de Trabajo en Seguridad de Redes, CGI.br: ftp://ftp.registro.br/pub/gts/gts17/01-DescriptografíaMalwares.pdf
[32] http://www.ollydbg.de/
[33] http://www.immunitysec.com/products-immdbg.shtml

Figura 3.26: Malware descompilado en el DeDe y abierto en Borland Delphi

Figura 3.27: Software depurador/desmontador OllyDbg en utilización en el análisis de un malware

• **IDA Pro**: un disassembler que posee versión para Windows, GNU/Linux y Mac OS X. También ofrece la funcionalidad de debugger. Para cada binario analizado, el

programa crea un archivo con todas sus informaciones, así la manipulación del código es realizada en este archivo externo.[34]

3.4.3.2 Análisis Dinámico (o comportamental)

El análisis dinámico tiene como objetivo ejecutar el malware en la máquina virtual en un ambiente preconfigurado y monitoreado, para permitir la verificación de las modificaciones e interacciones que son realizadas en el sistema operativo y en la red. Este enfoque a veces suministra una opción más simple de comprender el funcionamiento del programa malicioso.

[34] http://www.hex-rays.com/idapro/

Figura 3.28: “Keylogger of Banker”: kit criminal para captura de datos bancarios

Monitores de procesos y sistema de archivos

Durante la ejecución del malware, estos softwares de monitoreo posibilitan el "rastreo" del proceso generado por el ejecutable, sus llamadas a las APIs, DLLs, modificaciones efectuadas en el sistema de archivos y en el registro de Windows.

Vea a continuación dos softwares recomendados para este tipo de acción:

Figura 3.29: “Ladrón of Bank”: kit criminal para captura de datos bancarios.

• Process Explorer: una herramienta de Microsoft similar al administrador de tareas de Windows, sin embargo con muchas más funcionalidades. Permite visualizar los procesos en ejecución de manera bastante detallada.[35]

• Process Monitor: software de Microsoft que permite monitorear procesos en tiempo real y verificar todas las modificaciones que ellos realizan en el sistema de archivos, DLLs y registro. Una verdadera navaja suiza para desvendar cada paso del malware en el sistema operativo.[36] La figura 3.30 exhibe el funcionamiento del Process Monitor.

[35] http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx
[36] http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx

Monitores de registro

Softwares en esta categoría permiten verificar cuales modificaciones el malware realiza en el registro de Windows por medio de su ejecución. Recomendamos el uso del Regshot [37]. Esta aplicación permite que se tire un snapshot del registro de Windows antes de la ejecución del malware y otro después de su ejecución. Posteriormente él mismo compara las dos versiones y produce un informe con las modificaciones detectadas.

Monitores de tráfico de red

Popularmente conocidos como sniffers de red, estos monitores permiten descubrir origen y destino de los paquetes transitados en la red, además del contenido transmitido.

Esta actividad es importante en el análisis dinámico, dado que en la mayoría de los casos el malware efectuará alguna interacción con la red, ya sea para hacer download de otros softwares maliciosos o para enviar un email con las informaciones capturadas de la víctima. Sin duda, la herramienta más popular para este propósito es Wireshark, un software multi-plataforma, robusto, que realiza la captura de tráfico en tiempo real y posibilita análisis offline. Permite además configurar filtros y visualizar de forma organizada los datos de los paquetes capturados.[38]

[37] http://regshot.sourceforge.net/
[38] http://www.wireshark.org/

Figura 3.30: Software Process Monitor en utilización para análisis de malware

Figura 3.31: Análisis de tráfico de red con el software Wireshark

Las etapas anteriores revelarán nombres de dominio, direcciones IP, direcciones de email y otras informaciones que podrán ser investigadas por medio de las técnicas presentadas en los tópicos correspondientes a cada uno de estos temas en el presente Guión, dejando de ser asunto específico del phishing.

3.5 A investigación de comunicadores instantáneos

Softwares de comunicación instantánea, conocidos como IM (Instant Messaging) permiten, como el nombre sugiere, la comunicación directa e instantánea entre dos o más usuarios en una red de computadoras. En Internet la popularización de este tipo de comunicación se dio en la década del 90, a través del ICQ (www.icq.com).

Hay actualmente una diversidad de protocolos, servicios y softwares de comunicación instantánea en Internet. Entre los más populares, se destaca el Windows Live Messenger, sucesor del MSN Messenger, ambos de Microsoft Corporation, que ofrece el software en la instalación estándar del sistema operativo Windows. Otros con gran popularidad en la red son el AOL Instant Messenger, Yahoo! Messenger y Skype.

En el ámbito de la investigación, podemos afirmar que la principal característica de la comunicación a través de IM es el hecho de que el contenido transmitido entre los interlocutores no es almacenado en un host central antes de ser entregado al destinatario, como ocurre por ejemplo en los servicios de email. Esta peculiaridad refuerza la sensación de anonimato, una vez que parece no haber intermediarios en la comunicación. Consecuentemente, este pasa a ser uno de los canales más utilizados para la práctica de algunos tipos de crímenes, como el de reclutamiento online de menores.

Es importante resaltar que no solamente mensajes de texto son intercambiadas a través de IM. La mayoría de los protocolos permite además la transmisión de cualquier tipo de archivo, además de la exhibición de vídeo por medio de webcams de los interlocutores.

Considerando que el investigador posee la identificación de un usuario de IM[39], pueden ser seguidos los siguientes caminos:

- Pedido de suministro de los logs de conexión del usuario para el proveedor del servicio de comunicación instantánea. A pesar de que el contenido de la comunicación intercambiado entre usuarios en este servicio no camine por los servidores de la

empresa que lo suministra, esta ciertamente almacena los logs de conexión de sus usuarios, pues estos realizan la autenticación a partir de sus servidores. Además de los logs de conexión, muchas veces la empresa está apta para suministrar otras informaciones, como por ejemplo, la lista de contactos de un usuario.

• Interceptación telemática. Una vez que la autoridad ya conoce la localización geográfica en la cual el sospechoso se conecta a Internet, es posible solicitar al proveedor responsable del acceso la interceptación telemática de los datos transitados. En este caso existe la necesidad de posterior análisis de los datos capturados, a través de softwares específicos, como veremos más adelante. De una manera general, la interceptación es realizada completamente en el ámbito de la infraestructura del proveedor de acceso. Los datos capturados son enviados posteriormente a la justicia para que los técnicos responsables realicen los filtrados y análisis.

[39] A depender del servicio, puede ser una dirección de email (MSN), un número (ICQ) u otra identificación, generalmente suministrada por el denunciante.

• Investigación del (de los) email(s) utilizados para registro del usuario en el servicio de IM. Generalmente el email utilizado para autenticación en el servicio de comunicación instantánea es también utilizado por el usuario en su día a día como un correo electrónico simple. Para detalles de como proceder en la investigación de emails, vea **3.3.5 Aspectos técnicos de la investigación**.

3.6 Investigación en redes de repartición de archivos

En pocas palabras, podemos decir que **Repartición de archivos** es un término utilizado para designar la actividad de suministro de archivos para download entre internautas, utilizando la Internet como medio de transmisión. En general se comparten canciones, vídeos, juegos, aplicaciones, libros etc. Este tipo de comunicación par a par (peer to peer, p2p), donde una estructura intermedia es dispensable, pasó a motivar una serie de actividades ilícitas en la gran red. El usuario ofrece archivos almacenados en su propia computadora para otros usuarios de la red, lo que le garantiza igualmente acceso a los archivos de estos otros pares. En general no hay ningún tipo de autenticación, contrato, términos de uso, o sea, ninguna obligación formal para la publicación de estos archivos, a no ser la propia legislación local, muchas veces desconsiderada en virtud de la peculiar sensación de anonimato que la red ofrece.

La primera gran red de repartición de archivos emergió con el programa Napster, introducido en 1999, limitado al intercambio de archivos mp3 en Internet. El protocolo utilizado por Napster dependía de un servidor central, lo que posibilitó que procesos judiciales apalancados por representantes de la industria fonográfica anulasen su funcionamiento aproximadamente 2 años después de la popularización.

Con el cierre de Napster, que pasó a ofrecer tímidamente servicios pagados, nuevas redes de repartición surgieron, de esta vez apoyadas por hackers independientes capaces de ofrecer tecnologías aun más sofisticadas y de código abierto, como se ve hoy en las redes Gnutella y en el protocolo Bittorrent. Algunas empresas aun apuestan en un modelo de negocio de repartición de archivos "legalizado", como Kazaa y LimeWire.

Notamos que en el ámbito de los investigados del GCCC/PR/SP, una red de repartición en especial es predominante para la práctica de crímenes. Se trata de la red eDonkey,

popularizada por el software eMule y derivados, como el aMule y DreamMule. Daremos a continuación la debida atención a esta red, donde los pasos aquí sugeridos para investigación pueden ser útiles también para casos involucrando otras redes, una vez que cargan principios y tecnologías semejantes.

3.6.1 Red Edonkey

La red eDonkey, también conocida como eD2k (sigla para eDonkey 2000) fue creada por una empresa alemana, MetaMachine Corporation, en el año 2000 y tenía como objetivo suministrar una estructura adecuada para transferencia de archivos grandes en Internet. Hasta los días de hoy es muy utilizada para repartición de vídeos, discografías y softwares en general.

La red eD2k se basa en los principios Peer to Peer; los archivos no son almacenados en un servidor central sino en las máquinas de los usuarios de la red que utilizan uno de los softwares disponibles que implementan su protocolo. Actualmente no hay una organización formal responsable del mantenimiento de la red, que es mantenida enteramente por usuarios voluntarios.

Podemos considerar que la red eDonkey es parcialmente centralizada. A pesar de que los archivos sean transmitidos de punto a punto - caracterizando así el modelo P2P - hay aun algunos servidores responsables de indexar informaciones sobre la disponibilidad de los archivos y sus respectivos usuarios que los ofrecen.

Un software bastante popular para acceder a la red eD2k es el eMule, desarrollado para plataforma Windows y disponible libremente en el website del proyecto.[40]

De manera general, la actividad de repartición de archivos en la red eD2k se da por medio de algunos pasos simples, conforme detallados a continuación:

[40] http://www.emule-project.net

1. El internauta instala unos de los softwares disponibles para acceder a la red eDonkey en su computadora, por ejemplo el eMule. Durante la instalación, es generada una cadena de caracteres alfanuméricos que identificará a este usuario únicamente en la red.

2. La primera vez que el usuario ejecute el software, será necesario hacer el download de una lista de servidores, lo que es realizado generalmente por el propio software, automáticamente. Conforme vimos anteriormente, los servidores de la red eD2k almacenan índices relacionando los archivos disponibles en la red y los usuarios que los poseen. El software escoge arbitrariamente uno de los servidores de la lista y se conecta a él.

3. En el momento en que el usuario busca un archivo en la red a través de su programa instalado, el software "pregunta" al servidor eD2k cuales usuarios poseen aquel archivo. El servidor ofrece entonces una respuesta bastante completa, suministrando no solo cuales usuarios poseen tal archivo, sino la última vez en que ellos fueron vistos online, cuales "pedazos" del archivo cada uno posee, cuales son sus direcciones IP, entre otras informaciones.

4. El software, ahora dotado de una lista de posibles usuarios compartiendo aquel archivo, se conecta **directamente** a las computadoras de aquellos que están compartiendo en el momento, sin ninguna interferencia del servidor eD2k. Se inicia entonces el download de los pedazos del archivo, par a par, que puede ocurrir simultáneamente (bajando un pedazo diferente del archivo de cada usuario) para reducir el tiempo de conclusión.

5. En este momento, el usuario que hace el download está automáticamente enviando informaciones para el servidor, certificando que ahora él posee aquel archivo, y consecuentemente estará publicando en la red para que otros usuarios puedan bajarlo.

Es importante comprender bien algunas características de la red eD2k:

- Todo usuario de la red eD2k posee un identificador único.

También referido como Hash de usuario, este identificador alfanumérico es creado en el momento de la instalación del software en su máquina personal. La generación es realizada a través de un algoritmo de hash MD4[41] implementado en el software. Además de su identificación en la red, un usuario eD2k puede definir un username, que por estándar es el nombre del software, conteniendo su versión instalada.

- Todo archivo en la red eD2k posee un identificador único.

La forma utilizada para diferenciar archivos en la red eD2k es una identificación única, conocida como hash eD2k, generada también por medio de un algoritmo de hash MD4 a partir del contenido del archivo, y nada tiene que ver con su nombre.

- Archivos en la red eD2k pueden ser presentados con nombres diferentes.

Dada la información del ítem anterior, podemos verificar que un archivo en la red puede poseer tantos nombres como suministren los usuarios. No hay impedimento para que un vídeo de nombre pthc.avi conteniendo escenas de abuso sexual infantil sea renombrado para show-en-vivo- jazz.avi y así sea distribuido. De esta manera, un usuario que busca un concierto de jazz en la red eD2k puede ser sorprendido por un contenido criminal después de efectuar el download. Ante esta situación, los softwares eD2k generalmente exhiben para el usuario el bestname del archivo, o "mejor nombre", que significa el nombre más popular del archivo dado por los usuarios que lo comparten en la red. Es posible también visualizar el contenido parcial de algunos tipos de archivos (por ejemplo, vídeos) localmente antes de completar el download.

[41] La RFC 1320 describe este algoritmo.

- Usuarios que comparten más, ganan más reputación en la red.

El sistema de créditos del software eMule, como es descrito en el sitio oficial del proyecto [42], puntúa al usuario que suministra más archivos. Tales puntos son utilizados en el sistema de reputación de la herramienta, de forma que cuanto más uploads un usuario X ofrece para un usuario Y, más rápido el usuario X avanza en la fila para hacer downloads de archivos del usuario Y. Este sistema sirve para promover la repartición.[43]

- Usuarios de la red eD2k pueden compartir solamente "pedazos" de archivos.

Vimos que la red Edonkey fue concebida para suministrar estructura adecuada para el intercambio de archivos grandes en Internet. Una de las principales facetas para alcanzar este objetivo es el hecho de que el protocolo permita que usuarios de la red

compartan chunks, o pedazos de archivos incluso antes de poseerlos integralmente almacenado. De esta manera, es posible realizar el download de un vídeo de 100MB a partir de 100 pares (usuarios) distintos, donde cada par suministrará por ejemplo un pedazo de 1MB del archivo total, lo que puede ser hecho simultáneamente, posibilitando mayor eficiencia en el download. Digamos que después de algunos minutos el usuario que baja este vídeo posee los pedazos de número 1, 45 y 58 del vídeo. En este momento él ya está apto a ofrecer estos pedazos para otros pares de la red.

[42] (http://www.emule-project.net/home/perl/help.cgi?l=1&rm=show_topic&topic_id=134)
[43] Este es un recurso que no está implementado en el protocolo original de la red eD2k. Es una de las extensiones del protocolo implementado en el software eMule, que también fue adoptada por otros softwares posteriormente.

• Al bajar archivos, el usuario de la red eD2k automáticamente lo hace disponible en la red para otros usuarios.

Como consecuencia de lo que fue expuesto en los ítems anteriores, podemos observar que el download de archivos en la red Ed2k posee una peculiaridad que demanda cautela en la investigación: un usuario puede compartir un archivo (o mejor, pedazos de un archivo) criminal sin tener conciencia de esto, pues antes de finalizar el download completo, él ya está compartiéndolo en la red. Las autoridades pueden valerse de algunas métricas simples al analizar estos casos. Por ejemplo, la presencia de una decena de vídeos con situación sexual con niños en una computadora investigada, habiendo sido estos compartidos por varios días en la red, sumándose además algunos términos de búsqueda encontrados en la misma computadora indicando la investigación intencional por tal contenido, difícilmente será aceptado como un "download accidental" por la justicia.

3.7 Posibles escenarios después de identificación del IP

Una vez conocidos las direcciones IP y horarios exactos referentes a los accesos que originaron un crimen en Internet, el investigador debe estar apto para identificar la infraestructura tecnológica utilizada en la práctica del delito, así como reconocer los actores involucrados (ej: proveedores de acceso). Esta etapa es fundamental para definir los próximos pasos de la investigación.

En los tópicos siguientes identificaremos los escenarios con mayor probabilidad de aparecer en la investigación de crímenes cibernéticos una vez que el investigador ya tiene posesión de una o más direcciones IP sospechosas y/o reportadas por el denunciante. En la práctica, la etapa que tratamos aquí es exactamente aquella que se da después de las investigaciones de WHOIS, DNS, enrutamiento, etc. vistas en **1.5 Conceptos introductorios**. Normalmente el resultado de estas investigaciones ya apunta para uno de los escenarios siguientes. O sea, ellas son capaces de suministrar información suficiente para que el investigador sepa si la conexión se originó, por ejemplo, de una residencia, de una empresa privada o de un órgano público.

Escenario 1: acceso doméstico a Internet

Figura 3.32: Escenario simple de conexión residencial a Internet

El acceso a Internet a través de cable o servicio ADSL es predominante en Brasil. Los grandes proveedores de acceso son responsables de la mayor parte de los usuarios de la red, que generalmente utilizan una computadora doméstica y se conectan utilizando direcciones IP reservadas (ver **1.2 Conceptos introductorios**). Estos son los casos más simples y demandan colaboración de los proveedores de acceso, principalmente en lo que se refiere al almacenamiento de registro de acceso de sus clientes. A pesar de que no haya legislación específica que obligue esta guarda de logs, los grandes proveedores de acceso a Internet del país se han comprometido en este sentido por medio de términos de cooperación y TACs con las autoridades brasileñas. La figura 3.32 ilustra como se da este tipo de conexión. Se ve en este caso la necesidad de solicitud de informaciones del suscriptor responsable de la dirección IP investigada.

Esta solicitud debe ser dirigida al proveedor de acceso a Internet verificado en la investigación de WHOIS previamente realizada.

Se ve además en la figura 3.32 que Registro.br es la organización que asigna un bloque de direcciones IP para el proveedor de acceso, conforme ya explicado en **1.2 Conceptos introductorios**. No obstante, la posesión de los datos del suscriptor final del IP está con el proveedor de acceso, y no con el Registro.br. Esta reserva vale para todos los escenarios aquí descritos.

Escenario 2: proveedor de acceso intermedio

Consta en el website del **Registro.br** que "**según la Ley General de Telecomunicación, acceso a Internet es un servicio de valor adicionado, y por tanto no reglamentado. No existe actualmente ningún órgano con competencia para conceder otorgamientos a proveedores. Por tanto, no hay necesidad de licencia para el funcionamiento de los mismos**."

Sobre todo en ciudades más distantes de las capitales, es común encontrar proveedores de acceso a Internet de pequeño y mediano porte, legalmente registrados, sin embargo carentes de una infraestructura adecuada para garantizar el correcto almacenamiento de logs de los clientes. Estos en general ofrecen acceso a través de línea discada o inalámbrico (Wireless). Algunos ya ofrecen tecnología ADSL y cable. Los proveedores representados por el **Proveedor de acceso** 2 en la figura 3.33 alquilan un bloque de direcciones IP de otro proveedor mayor, por eso son considerados proveedores "intermedios" entre el proveedor mayor y el usuario final.

Figura 3.33: Acceso a Internet por medio de un proveedor intermedio

Cuando el investigador se depara con direcciones IP asignadas en proveedores intermedios de acceso, es recomendado que sean consideradas las siguientes acciones:

1. Confirmar con el proveedor de acceso principal (aquel que suministra el bloque de direcciones para este menor) se en la fecha en que el crimen fue cometido aquella dirección IP ya estaba asignada para el proveedor menor, o si estaba en posesión de otra organización.

2. Solicitar al proveedor intermedio las informaciones de registro de los usuarios que utilizaban la dirección IP en el momento de la ocurrencia investigada, en caso que este

proveedor no sea también considerado sospechoso. Si es considerado sospechoso, todas las informaciones deben ser solicitadas directamente al proveedor principal. En este caso es más común optar por la interceptación telemática, pues el proveedor principal no estará apto para suministrar datos del cliente del proveedor intermedio.

Escenario 3: acceso corporativo o público

Podemos interpretar que si una dirección IP pertenece a una persona jurídica (empresa privada o pública) que no sea proveedor de acceso a Internet, ella será entonces responsable directa por los accesos originados por esta dirección. Esta interpretación, al contrario de lo que pueda parecer, no simplifica la investigación. Organizaciones públicas y privadas pueden poseer centenas o millares de funcionarios, departamentos, filiales o incluso ofrecer acceso a personas físicas externas dispensando registro (ej.: lanhouses, telecentros, cafés, librerías, etc.).

Figura 3.34: Escenario común de acceso corporativo a Internet

Ante este escenario, es necesario dedicar tiempo a un trabajo de inteligencia más abarcador. Identificar si la organización en cuestión está apta para colaborar de forma exenta es el primer paso.[44]

Adicionalmente, un trabajo eficiente de interceptación telemática puede suministrar informaciones que identifican la autoría, sin comprometer el funcionamiento de la organización. Los procedimientos de recogida de evidencias de los sospechosos a través de interceptación pueden ser ejecutados con la colaboración de la empresa involucrada o directamente en el proveedor de acceso responsable. Esta última opción dispensa que la empresa involucrada tenga conciencia del hecho, lo que es fundamental en algunos casos.

Escenario 4: acceso a través de proxies anónimos

Podemos imaginar el escenario en que la autoridad recibe la denuncia de que un blog en idioma portugués ha publicado manifestaciones discriminatorias dirigidas a comunidades brasileñas. En un primer análisis, por medio de la verificación preliminar del contenido, se infiere que el autor del blog denunciado es brasileño. La empresa responsable del blog suministra las direcciones IP solicitadas por la justicia, que se refieren a las conexiones que originaron las publicaciones. Al analizar estas IPs, el investigador se sorprende con el hecho de que las IPs pertenecen a rangos de direcciones asignadas fuera de Brasil. Algunas posibilidades surgen de este hecho. El autor del referido blog puede residir en el exterior, o podría estar de viaje en el momento de las publicaciones ofensivas. No obstante, al realizar las debidas investigaciones de WHOIS, el investigador nota que las IPs suministradas por la empresa pertenecen a decenas de países diferentes. Y lo más intrigante: las conexiones partieron de diversos países en un intervalo de tiempo muy pequeño, en cuestión de minutos.

[44] Por ejemplo, si por lo menos una de las conexiones partieron de una lanhouse en el momento en que estaba cerrada para el público externo, evidentemente surge la sospechosa de la participación de sus propietarios en la autoría de la acción investigada

Figura 3.35: Acceso a Internet a través de Proxy

Este es el típico escenario de utilización de una red de proxies anónimos esparcidos por el mundo para acceder a Internet, representados en rojo en la figura 3.35. Vimos que la red más popular para este fin es la red TOR (**3.8.3 Aspectos técnicos de la investigación**). Es sabido también que las direcciones IP de los nodos de salida de esta red son públicos y pueden ser consultados online.[45] O sea, el investigador estará apto para realizar consultas en la red y eventualmente constatar la utilización de proxies por parte del investigado. Incluso redes de proxies menos populares, o incluso redes zombis a veces poseen sus IPs listadas públicamente. Queda por tanto la recomendación de utilizar servicios de búsqueda en Internet en estos casos. Los resultados pueden revelar la estrategia de anonimato utilizada por el sospechoso. **¿Cómo proseguir la investigación en casos como este?**

[45] Por ejemplo en http://torstatus.blutmagie.de

Para intentar responder la pregunta, es importante primeramente considerar la realidad brasileña en la utilización de esta tecnología. De hecho, redes de proxies anónimos son muy eficientes desde el punto de vista técnico para garantizar el anonimato, en especial la red TOR. Sin embargo, algunos factores aun inhiben su utilización: la lentitud que generalmente es provocada por la utilización de los proxies extranjeros; la necesidad de alguna habilidad técnica para su utilización y; la necesidad de software propio para configuración de los servicios, lo que dificulta la instalación en centros públicos de acceso.

Algunas investigaciones apuntan bajísima utilización de proxies por internautas brasileños y el NTCCC/PR/SP confirma esta información. A lo largo de los años de existencia de este núcleo fueron verificados poquísimos casos con la utilización de proxies de la red TOR. Cabe no obstante listar algunas recomendaciones para estos casos:

• Intentar identificar, en la lista suministrada por el proveedor, cuales direcciones IP pertenecen a redes de proxies anónimos, siguiendo la sugerencia expuesta anteriormente. Esto puede revelar el uso de proxies localizados en Brasil o en otros países, quedando a cargo de la autoridad decidir los próximos pasos de la investigación para cada situación.

• Al analizar los logs, tentar localizar al menos una dirección IP brasileño que no esté ligado a una red pública de proxies. Debido a los factores que eventualmente dificultan su utilización, el investigado puede haber realizado algunas pocas conexiones directas (sin uso de proxy) y un único descuido en este sentido podrá ser suficiente para que su identidad sea revelada.

• Siempre solicitar al proveedor de servicios, además de los logs de conexión, los datos de registro del cliente. En muchos casos es posible conseguir una dirección de email válida u otras informaciones que sean útiles para otros frentes de investigación. Por ejemplo, la empresa responsable del blog investigado muy probablemente estará apta para informar la dirección de email del investigado. A partir de esta dirección de email, el investigador puede solicitar de su proveedor de email los IPs de conexiones de este usuario que ocurrieron en un período próximo al de las publicaciones ofensivas, o incluso una **cuenta espejo** para monitoreo en tiempo real. Puede ocurrir que el

investigado no utilice proxies para acceder emails - diferentemente de lo que hace al acceder al blog - lo que facilitará bastante los próximos pasos de la investigación, pues en este caso el investigador tendrá en manos direcciones IP que reflejan el local real de los orígenes de las conexiones.

Escenario 5: proveedor de acceso extranjero

Figura 3.36: Acceso a Internet a través de proveedor extranjero

En este caso, conforme representado en la figura 3.36, solamente el proveedor de acceso (localizado fuera del país) será capaz de suministrar informaciones del terminal telefónico utilizado en la conexión. El alto costo y la baja calidad del link es ciertamente un factor que minimiza las posibilidades de popularización de utilización de empresas extranjeras para acceso a Internet, incluso por aquellos dedicados a la práctica de crímenes en la red. Aquí se aplican las mismas recomendaciones del ítem anterior.

Escenario 6: el internauta nómada

Los escenarios vistos hasta aquí no son mutuamente exclusivos en una investigación. El internauta dispuesto a cometer crímenes puede utilizar diferentes métodos de acceso con la finalidad de dificultar un eventual rastreo. En este caso la interceptación telemática de datos a través de proveedor de acceso puede no ofrecer los resultados deseados, considerando que el comportamiento del investigado es imprevisible - o sea, no hay un punto de acceso único que él probablemente utilizará para conectarse en las fechas subsiguientes.

Figura 3.37: Escenario de acceso a Internet por diversos medios, lo que dificulta la investigación

Ante un escenario complejo como el ilustrado en la figura 3.37, la correlación de informaciones (de registro y logs de conexión) suministradas por los proveedores de servicio y acceso involucrados es fundamental. Se puede identificar algunos estándares de comportamiento que auxiliarán en las investigaciones (ej. Se puede inferir que los fines de semana el usuario investigado acostumbra utilizar lanhouses en los alrededores de un determinado barrio identificado por algunas IPs suministradas, y así se puede accionar un trabajo de investigación en campo). También se recomienda la interceptación de email u otros servicios de comunicación (a partir de la creación de cuenta-espejo u otros métodos).[46]

[46] Es común que los proveedores de servicio, principalmente aquellos con matriz en el exterior, dificulten al máximo el procedimiento de interceptación, alegando conflictos de legislación, ofreciendo sugerencias para que este procedimiento sea realizado por el proveedor de acceso. Es importante que las autoridades comprendan que son dos mecanismos diferentes de interceptación, y que, a depender del caso, solamente uno de ellos será útil para la investigación. En el ejemplo del escenario 6, observamos que la interceptación a través de proveedor de acceso es prácticamente inviable.

Tabla 3.2: Criptografía y Esteganografía

Criptografía	Esteganografía
En el instante en que se tiene conciencia de la existencia del mensaje	El mensaje se oculta en otro completamente desasociado, no genera

se puede tomar la acción de interceptarla y evitar que esta alcance el destino pretendido por el remitente. Incluso ante la imposibilidad de conocer su contenido se consuma con relativa facilidad el perjuicio de la comunicación entre las partes.	sospecha y por tanto no hay interceptación.
Existen leyes o proyectos de leyes en tramitación que limitan o incluso desautorizan el uso de la criptografía en diversos países.	No hay leyes asociadas a la Esteganografía

3.8 Principales técnicas utilizadas para la ocultación del crimen y de su autor

3.8.1 Esteganografía

La Esteganografía es un tipo de comunicación escondida que significa literalmente "escritura oculta", término originado del griego graphia (escritura) y stegano (oculto). Vimos en **3.8.4.1 Aspectos técnicos de la investigación** y **3.8.4.2 Aspectos técnicos de la investigación** que la criptografía se preocupa en ocultar el **significado** del mensaje a partir de técnicas variadas. En este tópico veremos que la esteganografía esconde la propia **existencia** del mensaje, también utilizando las más variadas técnicas y tecnologías.

De una manera general, un mensaje encriptado no deja de exponerse en el medio de comunicación en el cual es transmitido. No obstante, su contenido se encuentra "mezclado" de tal forma que un humano o incluso una computadora de alta capacidad de procesamiento no logran ordenar y conocer su contenido semántico. Podemos identificar dos limitaciones de carácter práctico en este enfoque, que no ocurren en la esteganografía, conforme ilustrado en la tabla 3.2.

Control de la criptografía en el mundo

En http://rechten.uvt.nl/koops/cryptolaw/cls-sum.htm (actualizado en julio del 2010) es posible visualizar un mapa que ilustra los controles de importación, exportación y uso doméstico de la criptografía en el mundo. La referencia para estos mapas son el Crypto Law Survey, disponible en http://rechten.uvt.nl/koops/cryptolaw/, iniciativa del investigador Bert-Jaap Koops, también autor de la tesis de doctorado A Key Conflict in the Information Society , disponible en http:// rechten.uvt.nl/koops/files/page.asp?page_id=21

3.8.1.1 Técnicas clásicas de Esteganografía

Ciertamente las limitaciones de la criptografía pueden comprometer la acción de criminales, y es exactamente por este el motivo que algunos optan por la esteganografía. Veremos a continuación los métodos más comunes de esta técnica de ocultación de mensajes, independientemente de las tecnologías disponibles. Enseguida mostraremos la realidad de la esteganografía en el mundo digital, así como algunos casos que se hicieron populares. Listamos también algunos softwares destinados tanto a la ocultación como a la detección de las técnicas de ocultación existentes.

Los métodos siguientes fueron bastante utilizados en el pasado e ilustran bien cuan efectiva puede ser la aplicación de la esteganografía, incluso antes de contar con las tecnologías disponibles actualmente:

• Micro-puntos

El micro-punto es una imagen o texto reducido al tamaño de aproximadamente 1 milímetro de diámetro. Esta técnica se hizo popular durante la Segunda Guerra Mundial. Mensajes estratégicos eran escondidos en puntos finales de frases y puntos de la letra 'i' , dentro de otros mensajes fuera de sospecha.[47]

El contenido de los micro-puntos era posteriormente visualizado con el auxilio de equipos específicos o incluso por microscopios comunes. Un proceso para generación de micro-puntos en ambiente doméstico utilizándose técnicas fotográficas es descrito en http://www.wonko.net/ microdot2results.html.

¿Tu impresora te está espiando?

Algunas impresoras modernas implementan la técnica esteganográfica de micro-puntos para que sea posible identificar el origen de una impresión, revelando incluso el número de serie del equipo.

La EFF (Electronic Frontier Foundation) publicó en el 2005 un artículo con el título "Investigating Machine Identification Code Technology in Color Laser Printers"[a]. En este documento están disponibles diversas fotografías que identifican la utilización de micro-puntos por diferentes modelos de impresoras, así como los estándares en formato texto para simple comparación. El artículo de la EFF fue escrito motivado por la publicación de la materia "Government Uses Color Laser Printer Technology to Track Documents" en la revista especializada PCWorld.[b] En ambos artículos son enunciadas cuestiones éticas y conflictivas entre el beneficio en las investigaciones de crímenes y el derecho de privacidad de los clientes ante tal postura de las fabricantes de impresoras.

[47] Algunas referencias sobre este tema fueron retiradas de "Historia, Técnicas y Clasificación de Algoritmos Esteganográficos", Nichols Aron Jasper, monografía para grado de tecnólogo, FATEC/ SP, 2009

[a] http://www.eff.org/wp/

[b] http://www.pcworld.com

- **Semagramas**

Semagramas son símbolos que cargan un significado específico para el destinatario. Literalmente hablando son "símbolos semánticos". En la práctica, son eficientes para breves mensajes, como por ejemplo la confirmación o desistencia de una determinada acción a partir del contenido de una tarjeta postal. Algo como: si la foto de la tarjeta postal que te envíe fue tirada por la noche, ejecute nuestro plan en 5 días. Si la foto de la postal es diurna, abandone el plan.

- **Cifras nulas**

También conocida como "código abierto", esta técnica "camufla" un mensaje de texto dentro de otro mayor, con significado irrelevante, muchas veces volviéndose confuso y levantando sospechas. Vea un ejemplo simple de esta técnica:

*"***Y***o* **o***lvido* **t***engo.* **E***s* **a***mor,* **m***ero* **o***dio."*

Extrayéndose la primera letra de cada una de las palabra anteriores tenemos la frase "Yo te amo" [48]

En las entrelíneas de un spam. . .

Un ejemplo actual del uso de la cifra nula es el servicio spam mimic. La descripción, retirada del propio website (http://www.spammimic.com) es la siguiente:

"**Existen excelentes herramientas para cifrar su email. Si las personas en el medio del camino ven su email no entenderán nada. Pero ellos ciertamente sabrán que usted está enviando un email encriptado... La respuesta: codifique su email dentro de algo aparentemente inocente**". La propuesta entonces es esconder su mensaje dentro de otro que aparente ser un spam, considerando que no levantará sospechas, ya que hay "toneladas de spam volando en Internet", como afirma el autor. El servicio es gratuito y la única cosa que el usuario necesita hacer es llenar un formulario con el mensaje que desea, que este será transformado en algo parecido con un spam común. Entonces él envía este nuevo mensaje para el destino que desee. El destinatario a su vez entra al mismo website y pega el "spam" en un formulario para extraer su contenido oculto.

• Anamorfosis

La Anamorfosis es una técnica en que una imagen es distorsionada al nivel que su apreciación sólo es posible a partir de un ángulo específico, o a través de un instrumento apropiado.

El cerebro humano es capaz de identificar imágenes distorsionadas con cierta facilidad. Por este motivo esta técnica no es muy utilizada para ocultar mensajes importantes. En compensación, podemos identificar la utilización de la anamorfosis en nuestro día a día de navegación en Internet cuando somos conducidos a un CAPTCHA para confirmación del envío de informaciones a través de un formulario en la web.

[48] http://www.gta.ufrj.br/grad/07_2/thiago_castello/TcnicasModernas.html

C.A.P.T.C.H.A ?
CAPTCHA significa Completely Automated Public Turing test to tell Computers and Humans Apart (prueba pública de Turing completamente automatizada para diferenciación entre computadoras y humanos). Esta técnica es la aplicación de la prueba propuesto por Alan Turing en 1950 para la identificación de inteligencia en un programa de computadora. En la práctica es usado para diferenciar un humano de un software. [a]

[a] http://pt.wikipedia.org/wiki/Teste_de_Turing

En los sistemas más comunes de CAPTCHA en Internet son expuestas imágenes con caracteres del alfabeto para que el usuario los identifique y envíe para validación. En razón de que algunos robots [49] son sofisticados al punto de comprender el significado de las letras, estas son distorsionadas de manera que solamente los humanos son capaces identificarlas semánticamente. O sea, se usa la técnica de anamorfosis para ocultar de los robots el significado de los mensajes. La figura 3.3 8 ilustra algunos ejemplos.[50]

Figura 3.38: Ejemplos de CAPTCHA que utilizan anamorfosis contra robots

[49] Se entiende aquí como programas de computadora que navegan en Internet automáticamente para realizar acciones específicas, como por ejemplo adicionar publicidad en los espacios de comentarios en blogs.
[50] Fuente: http://networksecurity-research.blogspot.com

• Acrósticos

Acrósticos son textos con varias líneas, donde se identifica un mensaje oculto a partir de una secuencia no usual de lectura, por ejemplo, tomándose la primera letra de cada frase verticalmente, de arriba para abajo, como en el ejemplo a continuación:

Verdes
Iguales
Deseamos
Amar

• Espaciamiento de texto

Como el nombre ya dice, esta técnica utiliza espaciamientos en un texto para enviar un mensaje en secreto. En el medio digital, el caso más común es considerar un bit 0 para cada espaciamiento simple, y el bit 1 para cada espaciamiento doble. Veamos el ejemplo siguiente:

Yo aun no se donde será el próximo encuentro de nuestro grupo amigo, ¿usted tiene alguna idea?
Se que ocurrirá este mes, la fecha es incierta.

En el texto anterior tenemos una secuencia de espaciamientos entre las palabras, lo que en general no levanta ninguna sospecha. Ocurre que los primeros 24 espacios (simples o dobles) en la frase sobre el local del encuentro, convertidos en representación binaria (un espacio = 0; dos espacios = 1) expresan un significado después de la conversión para ASCII [51]:

01010011 01010000 – S P

Mientras que los 8 bits siguientes en la frase referente a la indefinición de la fecha del encuentro representa la cifra 9 después de conversión para ASCII:

00111001 – 9

El investigador más atento podría entonces imaginar que el encuentro del grupo en este mes será en São Paulo, y la fecha está marcada para el día 9.

Hay otras diversas técnicas de esteganografía. Muchas fueron utilizadas durante períodos de guerra en que las tecnologías digitales no eran tan sofisticadas ni populares como son actualmente. Hay además el uso de radiofrecuencia, "pinturas invisibles", jergas preacordadas, tarjetas perforadas para sobreposición en textos, etc. Intentamos detallar aquí aquellas que de alguna manera influenciaron o son base para lo que tenemos hoy a través de softwares. Veremos a continuación algunos ejemplos prácticos utilizados actualmente.

[51] (Acrónimo para American Standard Code for Information Interchange, que en español significa "Código Estándar Americano para el Intercambio de Información: http://pt.wikipedia.org/ wiki/ASCII)"

3.8.1.2 Técnicas modernas de Esteganografía

En el mundo digital es posible utilizar técnicas de esteganografía para esconder textos dentro de imágenes, imágenes dentro de imágenes, imágenes dentro de vídeos, etc. En fin, cualquier información en formato binario puede ser insertada sutilmente en archivos de cualquier naturaleza. En esencia, los métodos son los mismos que aquellos vistos hasta ahora, a los cuales nos referimos por "métodos clásicos". No obstante, los mecanismos difieren de aquellos en virtud de las tecnologías que están a nuestro alcance actualmente. En una visión general, observamos que hay tres formas de esconder mensajes digitalmente, que pueden ser a través de:

- **Inyección**

El mensaje secreto es insertado en el mensaje "hospedero" mayor. El problema en este enfoque es que el tamaño del mensaje hospedero es perceptiblemente aumentado, facilitando su detección.

- Sustitución

Aquí los datos del mensaje "normal" son sustituidos por datos secretos. En este caso, la modificación en el tamaño del archivo es mínima. Existe no obstante una degradación en la calidad del archivo original, a depender de su tipo.

Las herramientas más populares que utilizan este método aplican modificaciones en los bits menos significativos del archivo hospedero con el objetivo de minimizar la degradación de su calidad.

- **Generación**

Un nuevo archivo es generado exclusivamente para la transmisión del mensaje secreto. Ya vimos un buen ejemplo de este método al citar el servicio spam Mimic anteriormente, que utiliza la técnica de la cifra nula para camuflar un mensaje dentro de otro mensaje generado exclusivamente para este propósito aparentando un SPAM.

3.8.1.3 Softwares para Esteganografía

Algunos softwares mencionados en libros y artículos sobre el tema ya no están disponibles en las direcciones referidas. De todas formas los citaremos aquí, pues es posible encontrarlos a partir de otras fuentes y son en general un precioso material para

análisis e investigación. Aquellos que fueron lanzados bajo una licencia que autorice la distribución estarán disponibles en el LiveCD anexo a este Guión.

• BackYard

Este software es capaz de esconder archivos y dispositivos (drives) dentro del sistema de archivos en un ambiente Windows. Se incluyen entre las características del Backyard la protección de los atributos de archivos y directorios escondidos.

Website: http://www.talyasoft.com/backyard.zip
Plataforma: Windows
Licencia: propietaria específica (U$25.00)

• Blindside

El Blindside esconde uno o más archivos dentro de una imagen bitmap (extensión BMP). La imagen original y aquella conteniendo los datos escondidos aparentan ser idénticas para el ojo humano. A través del software es posible insertar y posteriormente extraer los datos escondidos. Para suministrar una capa adicional de seguridad, Blindside permite la utilización de criptografía en conjunto con la esteganografía.

Diferente de los softwares que trabajan con imágenes para esconder datos, Blindside no utiliza la técnica del LSB (modificación de los bits menos significantes). Según el autor, esta técnica genera algunas imperfecciones que pueden comprometer el carácter secreto del mensaje. Blindside analiza las diferenciaciones de colores en la imagen y solamente modifica los pixeles que no serán notados por el ojo humano.

Website: http://www.blindside.co.uk
Plataforma: Windows, DOS, GNU/Linux, BSD y Unixes en general.
Licencia: Freeware, libre distribución. El autor pide que sea contactado en caso de uso comercial o por gobiernos.

• bProtected

bProtected es un software comercial para protección y ocultación de datos personales en una computadora. Permite que se escondan archivos, directorios o simplemente evita que ellos sean modificados o retirados. Él es capaz de esconder su propia instalación.

Website: http://www.clasys.com/b_protected.html
Plataforma: Windows
Licencia: propietaria (U$19.95)

• Camera/Shy

Camera/Shy es un software para uso de la esteganografía en la Web, desarrollado voluntariamente por el grupo Hacktivismo [52]. Es en realidad un navegador Web basado en Internet Explorer, capaz de reconocer y someter contenido cifrado y escondido en imágenes (solamente GIF) en websites.

La última actualización de este software ocurrió en el 2002, no obstante continúa funcional en los sistemas operativos más recientes. El mismo grupo, que es considerado un brazo del más influyente grupo de hackers en el planeta [53] posee otros proyectos que tienen como objetivo la garantía de los derechos humanos a través del uso de las tecnologías. Camera/Shy es un software muy simple de utilizar. Un ejemplo paso a paso puede ser encontrado en http://www.svrops.com/svrops/articles/camera.htm (en inglés).

La imagen 3.39 exhibe un screenshot de Camera/Shy. En este ejemplo visitamos un website que exhibía la foto de una orca conteniendo internamente un texto con los cinco primeros artículos de la declaración universal de los derechos humanos. Sólo fue posible verificar la existencia del texto porque teníamos conocimiento previo de la clave utilizada para esconderlo en la imagen. Una red de criminales puede por ejemplo utilizar esta técnica para que los miembros se comuniquen a través de websites mantenidos por ellos mismos, aparentemente inofensivos.

[52] http://www.hacktivismo.com
[53] http://cultdeadcow.com

Figura 3.39: CameraShy - navegador Web con soporte nativo para esteganografía

Website: http://sourceforge.net/projects/camerashy/
Plataforma: Windows
Licencia: libre (GPL)

- **Camouflage**

Camouflage permite insertar el contenido de un archivo cualquiera dentro de otro de cualquier naturaleza. Es una herramienta simple y también ofrece la posibilidad de cifrar los datos utilizando una clave simétrica. La manera por la cual él inyecta los datos de un archivo en su hospedero es fácilmente detectable a través de un análisis más cuidadoso. Visualmente no perjudica la imagen, cuando es utilizada, lo que lo hace eficaz en la mayoría de los casos.

Website: http://camouflage.unfiction.com/
Plataforma: Windows
Licencia: Freeware, código propietario con permiso para libre distribución del binario.

- **Cloak**

Cloak es un software comercial que soporta criptografía y técnicas de esteganografía, además de opciones de privacidad. Sin muchas novedades con relación a otros analizados, él ofrece una interfaz gráfica para ambiente Windows para que el usuario esconda archivos, escoja entre diferentes algoritmos criptográficos y digite una clave simétrica a ser usada en la posterior decodificación.

Website: http://insight-concepts.com
Plataforma: Windows
Licencia: propietaria

- **Courier**

Otro software para esconder textos dentro de archivos de imagen (solamente archivos BMP).
Website: http://pages.prodigy.net/robyn.wilson/
Plataforma: Windows
Licencia: freeware, libre distribución para uso no profesional

- **Digital Picture Envelope / Qtech Hide & View**

Desde 1997 un software llamado Digital Picture Envelope es distribuido como prueba de concepto para una técnica esteganográfica llamada BPCS54 (Bit-Plane Complexity Segmentation Based Embedding). Posteriormente este software fue reescrito y renombrado como Qtech Hide& View. Los autores creen que este es el software de esteganografía más poderoso actualmente:

> *"Qtech Hide & View was implemented by Visual C++ environment. It took several years to finalize the deliverable version. We believe this program is the best of all steganographic software currently available on a commercial / non-commercial basis."*
> *http://www.datahide.com/ BPCSe/QtechHV-program-e.html*

[54] http://www.datahide.com/BPCSe/principle-y.html

Tabla 3.3: Otros softwares para esteganografía

Nombre	URL
Contraband (Hell Edition)	http://come.to/us
Crypto 123	http://www.kellysoftware.com/software/ Crypto123.asp
Dark Files	http://www.mybestsoft.com/protect_files.html
Data Stash	http://www.skyjuicesoftware.com/software/ ds_info.html
Dound's Stegnagropher	http://download.cnet.com/Dound-s- Steganography/3640-2092_4- 8880146.html
GhostHost	http://pages.prodigy.net/robyn.wilson/
Gifshuffle	http://www.darkside.com.au/gifshuffle/
Gzsteg	http://www.nic.funet.fi/pub/crypt/ steganography/
Hide and Seek	ftp://ftp.funet.fi/pub/crypt/steganography/ hdsk41.zip
MP3Stego	http://www.petitcolas.net/fabien/ steganography/mp3stego/index.html
MP3Stegz	http://achmadz.blogspot.com/2008/05/hideany- file- inside- mp3- file.html
PGE -- Pretty Good Envelope	http://www.afn.org/^,afn21533/pge20.zip
S-Tools	ftp://ftp.spez.com.ua/bbs/public/s-tools4.zip
Stego	http://www.fourmilab.ch/stego/
Texto	ftp://ftp.funet.fi/pub/crypt/steganography
OutGuess	http://www.outguess.org/
StegHide	http://steghide.sourceforge.net
isteg	http://zooid.orgig-,,paul/crypto/jsteg/
Hydan	http://crazyboy.com/hydan/

3.8.1.4 Detección de mensajes escondidos por esteganografía

Detectar si un mensaje está escondido en otro aparentemente inofensivo no implica en el éxito de una investigación. Generalmente es necesario extraer y conocer el contenido del mensaje oculto. Hay casos en que es necesario actuar activamente, destruyendo el contenido escondido para que no sea leído por el destinatario, o incluso modificándolo para alcanzar objetivos de una investigación en curso contra, por ejemplo, ataques de grupos terroristas.[55]

El área de estudio dedicada a las técnicas para detección de la esteganografía es llamada "esteganoanálisis". En la literatura sobre el tema estas técnicas son clasificadas de la siguiente manera:

• Steganography-only attack

Cuando se tiene en manos el medio de transmisión del mensaje (archivo hospedero + mensaje oculto en él) y se desea detectar y extraer la información escondida.

[55] An Overview of Steganography for the Computer Forensics Examiner - disponible en http://www.garykessler.net/library/fsc_stego.html

- **Known-cover attack**

En este caso el atacante [56] posee también el archivo hospedero original utilizado para esconder el mensaje, de forma que puede compararlo con aquel modificado.

- **Known-message attack**

Poco común en la práctica, se refiere a la situación en que se conoce el mensaje escondido y el stego-medium [57], y se quiere entonces descubrir el método utilizado para esconderlo.

- **Chosen-steganography attack**

Cuando se posee el stego-medium y la herramienta y/o algoritmo utilizado originalmente para esconder el mensaje.

- **Chosen-message attack**

En este caso el atacante genera el stego-medium a partir de un mensaje, utilizando una herramienta en particular. De este modo él consigue una firma (hash) del stego-medium generado que puede auxiliar en la detección de otros generados por la misma herramienta.

- Known-steganography attack

Semejante al Chosen-steganography attack, sin embargo se conoce además el archivo hospedero original.
Podemos imaginar que si fuese simple detectar el uso de la esteganografía, ella no sería considerada una manera eficiente de transmitir mensajes secretos. Pues bien, una vez

que hay sospechas de uso de la esteganografía en un proceso de investigación [58], nos deparamos con una serie de desafíos técnicos a ser superados, dado que hay centenas de softwares de esteganografía disponibles en Internet y que utilizan las más variadas técnicas. Como consecuencia, es ingenuo pensar que sea posible reunir en un único producto la solución contra la esteganografía digital. Por tanto, es más prudente que el investigador posea un conocimiento general sobre las técnicas y herramientas más comunes, de forma que tenga habilidad para lidiar de manera inteligente en cada caso específico.[59]

[56] "atacante" aquí es un término de carácter puramente técnico. El atacante es la persona que desea violar el secreto de quien usó la esteganografía para esconder un mensaje. En nuestro caso, es el investigador, o el perito.
[57] Término utilizado para designar el medio en el cual la información está escondida.

En una visión general, hay dos enfoques a considerar. Estos pueden ser complementarios en un proceso de investigación. El primero utiliza métodos estadísticos para detección de modificaciones en archivos que supuestamente hayan sido modificados para abrigar mensajes secretos. Notamos que la mayor parte de las herramientas utiliza técnicas populares que pueden acusar los mismos indicios de modificación.

Por ejemplo, algunas herramientas modifican un archivo de imagen que, a depender del tamaño del mensaje, pueden perjudicar su calidad a punto de levantar sospechosas a través de una simple verificación visual.

Softwares que usan la técnica de manipulación de los bits menos significativos de una imagen generalmente generan colores excesivamente duplicados o bastante próximos, donde hay diversos pixeles con colores que obviamente difieren solamente en el valor del último bit en la paleta de colores. Por otro lado, herramientas que esconden informaciones en bits aleatorios pueden generar modificaciones en la estructura del archivo que pueden también ser explotadas. Además, algunas herramientas generan "firmas" fijas fáciles de ser verificadas.

[58] En general no encontramos evidencias que levanten esta sospecha, diferentemente de cuando se intercepta un mensaje explícitamente cifrado.
[59] Un ejemplo que refuerza nuestra afirmación es dado por el famoso libro Investigators Guide to Steganography, que en 220 páginas dedica solamente 12 para el capítulo sobre detección, Detection and Attacks.

El segundo enfoque utiliza exactamente la detección basada en esas firmas. Es un método consolidado para detección de virus y muy utilizado en sistemas de detección de intrusión. Algunas pocas herramientas que utilizan este enfoque están disponibles online. Listamos a continuación las dos más populares:

- **Stegdetect**

Stegdetect es una herramienta que automatiza el proceso de detección del uso de la esteganografía en archivos de imagen. Actualmente este software es capaz de encontrar informaciones escondidas originadas por el Jsteg, Jphide, Invisible Secrets, Outguess 01.3b, F5, AppendX y Camouflage. Un utilitario extra es suministrado, el Stegbreak, que ejecuta ataques de diccionario para violar contraseñas utilizadas por los softwares JSteg-Shell JPHide y OutGuess 0.13b.

La versión más actual utiliza la técnica de análisis discriminante lineal, que a partir de un grupo de imágenes normales y otro de imágenes con mensajes escondidos, es capaz de determinar una función de detección lineal que puede ser aplicada para inferencia en imágenes aun no clasificadas. Las funciones aprendidas pueden ser almacenadas para utilización posterior en nuevas imágenes.

El Stegdetect es un software libre, sin fines comercias. Su código fuente está disponible para distribución.[60]

• Stego Suite

Considerado por muchos el más avanzado en este propósito, esta suite incluye cuatro softwares que actúan de forma complementaria para auxiliar en la detección del uso de la esteganografía en archivos de imagen, audio y vídeo. Stego Hunter es capaz de identificar más de 500 softwares conocidos de esteganografía, volviéndolo bastante útil para los primeros pasos de una investigación forense. Stego Watch utiliza el enfoque de análisis estadístico para identificar anomalías y probables archivos hospederos de mensajes secretos. Stego Analyst está enfocado para la identificación avanzada de mensajes ocultos en imágenes y vídeos, suministrando al usuario una interfaz con importantes atributos de estos archivos. Por fin, Stego Break auxilia en la violación de claves eventualmente utilizadas para cifrar las informaciones escondidas.

Stego Suite es un software comercial y una licencia de utilización cuesta U$1.495,00 en el website oficial de la empresa, WetStone Technologies.[61]

Esteganografía desafiada

En http://www.guillermito2.net/stegano/ está el análisis de doce herramientas de esteganografía. El autor logró invalidar casi todas y demuestra paso a paso como procedió. Es sin duda un excelente recurso para el aprendizaje y comprensión de los límites de esta técnica.

[60] http://www.outguess.org/download.php
[61] http://www.wetstonetech.com/cgi-bin/shop.cgi?view,1

A pesar de que casos de uso de esteganografía no sean tan comunes en Brasil, ciertamente son medios utilizados por grupos criminales que actúan más allá de las fronteras. Tenemos dos ejemplos bastante difundidos en este tema. Uno trata del extenso uso de la esteganografía para la preparación de los atentados del 11 de septiembre del 2001 en los Estados Unidos. Otro aborda los métodos utilizados por el traficante Juan Carlos Abadia, hecho prisionero en agosto del 2007 en territorio brasileño. En las computadoras aprehendidas de este último, fueron encontradas más de 200 imágenes de Hello Kitty conteniendo mensajes de texto y audio con órdenes para movimiento de drogas entre países y asesinatos en Colombia.

3.8.2 Proxy

Un proxy es una computadora que sirve como intermediario en la conexión entre otras dos computadoras. La computadora de origen se conecta a un proxy. El proxy a su vez se conecta al servicio deseado por el origen y recibe las informaciones de este servicio.

Por fin, el proxy pasa estas informaciones para la computadora de origen. Se nota en este escenario que no hay un contacto directo entre el origen y el destino. El origen puede ser una computadora personal utilizando un link de ADSL doméstico. El destino puede ser un servicio de galería de fotos en Internet. El origen puede publicar una foto en este servicio utilizando un proxy. Una eventual investigación en los logs (registros) de acceso del destino revelaría la dirección IP del proxy, y no de la computadora de origen. O sea, en este escenario el proxy "se lleva la culpa" por la publicación de las fotos. Por otro lado, los logs almacenados en el proxy podrían revelar la dirección IP del origen, donde se encuentra el real responsable de la publicación. Diferente de lo que pueda parecer, tal hecho no ayuda al investigador, una vez que (generalmente) este proxy está localizado en países de difícil acceso para que la justicia brasileña solicite informaciones. De hecho, cualquier Internauta dotado de una dirección IP pública puede transformar su computadora en un proxy abierto para cualquier usuario de Internet, lo que dificulta aun más el rastreo.

Cabe resaltar que un proxy puede ser utilizado para diversas finalidades. En una red corporativa un proxy puede ser implementado para realizar el cache (almacenamiento temporal de contenido) con el objetivo de acelerar la navegación, establecer límites de acceso a Internet o incluso para generar indicadores acerca del material accedido. O sea, el proxy es una tecnología de carácter neutro, sin ninguna implicación directa en la práctica del crimen.

Un ejemplo curioso del uso de proxies

La copa del mundo del 2006 fue transmitida en Internet por la BBC de Londres. No obstante, solamente computadoras localizadas en la Inglaterra tenían permiso para acceder a los vídeos de los juegos. Muchos internautas brasileños utilizaron entonces proxies anónimos localizados en Inglaterra para tener acceso. Sus computadoras de origen en Brasil se conectaban a las computadoras en Inglaterra, que se conectaban al sitio de la BBC y retornaban la información (los vídeos) para las computadoras brasileños.

Proxy anónimo

Un proxy anónimo es una computadora conectada a Internet lista para hacer el papel de intermediario entre conexiones originadas de cualquier otra computadora. O sea, posee la misma definición de un proxy regular. La única diferencia es que un proxy anónimo es intencionalmente configurado con el objetivo de asegurar un nivel razonable de anonimato en la red para sus usuarios. Este anonimato es garantizado por medio de tecnologías más sofisticadas o simplemente por el hecho de que el proxy reside en una región de difícil acceso para cualquier autoridad local. Esta dificultad se presenta en diferentes niveles, pasando por la localización geográfica del proxy, por la garantía del no almacenamiento de logs, o incluso por la falta de una legislación local específica en este tema.

Utilizar un proxy anónimo no requiere ningún software adicional. Generalmente la misma computadora que suministra el servicio anónimo, ofrece también una página Web con un formulario donde el usuario digita la dirección (URL) que desea acceder y recibe el contenido "embutido" en la página del proxy. Existen softwares y componentes para navegadores que hacen más eficiente la utilización de proxies

anónimos, incluso ofreciendo al usuario listas con diversos proxies en diferentes países e incluso optimizando la búsqueda por proxies con conexiones de mayor calidad.

Algunos proxies envían informaciones a la computadora de destino (ej: encabezamientos HTTP) que posibilitan identificar la computadora de origen por medio de un análisis más juicioso. Por otro lado, algunos websites (principalmente aquellos relacionados a transacciones financieras) utilizan técnicas para detectar si un internauta está utilizando un proxy anónimo al acceder a sus servicios, bloqueando entonces este acceso con el objetivo de evitar fraudes.

3.8.3 Anonimato con la red de proxies TOR

TOR significa The Onion Router. TOR es un software libre que implementa un protocolo de comunicación capaz de asegurar en gran parte de los casos el anonimato en las transmisiones de los datos en una red de computadoras, en general en Internet. La técnica utilizada por el TOR para garantizar el anonimato es denominada Onion Routing. Este “Enrutamiento Cebolla” permite que un mensaje enviado por la red sea previamente cifrado y transite aleatoriamente por una serie de nodos (computadoras con el TOR instalado) antes de llegar a su destino final. De esta manera la tarea de interceptación de datos es considerablemente dificultada, además de prácticamente imposibilitar la identificación del origen real de la conexión.[62]

Funcionamiento del TOR

Las tres figuras siguientes 3.40, 3.41 y 3.42, extraídas del website del proyecto resumen las tres principales etapas del funcionamiento de la red TOR. En la 3.40 la usuaria Alice, que posee el TOR instalado en su máquina, realiza automáticamente el download de la lista de nodos de la red TOR disponibles en aquel instante. Esta lista puede ser encontrada en diversas fuentes y el software sabrá donde buscar.

[62] http://www.torproject.org

Figura 3.40: Funcionamiento de la red de proxies TOR - paso 1

En posesión de la lista de nodos de la red TOR, el software de Alice escoge aleatoriamente un camino para que los datos de conexión transiten hasta su destino. La figura 3.41 deja claro una característica importante para cualquier intento de investigación nwwa red TOR, que es el hecho de que el tráfico entre el último nodo del camino hasta el destino final (Bob) no es cifrado (línea en rojo). Este último nodo es conocido como "nodo de salida" (exit node). Nodos de salida son configurados voluntariamente por los usuarios y representan aproximadamente un tercio del total de nodos de la red TOR en Internet, según [Suess 2008].

La figura 3.42 solamente ilustra que para una próxima conexión realizada por Alice, esta vez buscando el destino Jane, un nuevo camino aleatoriamente definido será utilizado, pasando por nuevos nodos. De hecho esta frecuente modificación de caminos ocurre incluso en conexiones para un mismo destino. Por esto sería posible por ejemplo encontrar en los logs de conexión de Bob una serie de direcciones IP originarias de varios países diferentes, en un corto espacio de tiempo, sin embargo con un único origen real (y desconocido para el investigador): Alice.

Figura 3.41: Funcionamiento de la red de proxies TOR - paso 2

Figura 3.42: Funcionamiento de la red de proxies TOR - paso 3

La capacidad que la red TOR posee en garantizar un alto grado de anonimato generalmente es referida cuando se debate la necesidad de la guarda de logs por los proveedores de acceso y otras medidas regulatorias para el combate a crímenes en Internet. Es común la argumentación de que se es posible navegar anónimamente, de nada servirá la guarda los logs de acceso. No obstante, el monto de usuarios que utilizan esta tecnología para practicar crímenes en Brasil aun está en el campo de la especulación.

Curiosidades y limitaciones de la red TOR

Un problema serio de seguridad involucrando a la red TOR se hizo popular en el 2007, cuando un usuario responsable de un nodo de salida, por medio de interceptación de tráfico en su computadora, detectó y divulgó 100 cuentas de email con sus respectivas contraseñas en Internet, informando también que podría publicar otras 900 si quisiese [a]. Las cuentas de email eran de funcionarios de embajadas en diferentes países. Conforme vimos anteriormente, el TOR no garantiza la criptografía del tráfico entre el nodo de salida y el destino, lo que viabiliza procedimientos simples de interceptación como este. Según [Fu 2009], en un universo de 9% de nodos maliciosos en la red TOR, 60% de las conexiones pueden ser comprometidas. En [Suess 2008] el autor concluye que identificar la dirección IP de origen de una conexión en la red TOR es algo razonablemente trivial, una vez que el tráfico entre el nodo de salida y el destino está mayoritariamente compuesto por HTTP no encriptado. Esta posibilidad es también consecuencia de la utilización de una serie de plugins y configuraciones presentes en el navegador del usuario, como Windows Media, Javascript activado, Shockwave, Real Media y Quicktime Media y el uso de applets Java. Investigaciones recientes revelan que usuarios de la tecnología de peer to peer BitTorrent utilizan extensivamente la red TOR. En [Manils et al. 2010] es posible verificar algunas técnicas para eliminar el anonimato en la identificación de los usuarios, esencialmente explotando fallas en el uso de la red TOR por falta de conocimiento de los propios usuarios.

[a] http://www.wired.com/threatlevel/2007/08/embassy-e-mail/

Considerando también que es necesario tener cierto conocimiento del asunto antes de optar por la utilización del TOR; que la red TOR hace la navegación bastante lenta o inviable en diversas situaciones; y que una gran parte de los crímenes son practicados en computadoras de terceros (lan-houses, telecentros, etc.) en los cuales el usuario no está apto para instalar softwares o complementos que dan acceso a la red TOR, se nota que su utilización por criminales no es un argumento fuerte para que se dispense la guarda de logs de acceso y otras medidas que auxilien en el combate a los crímenes practicados en Internet.

Utilización del TOR

Instalando el TOR en ambiente Windows

Un usuario de Internet no necesita ser dotado de gran habilidad técnica para utilizar la red anónima TOR. El acceso puede ser realizado directamente por el navegador Web, como el Firefox, por medio de complementos (o extensiones). En este caso hay un componente que se acopla al navegador de forma que toda conexión realizada por él pasa a ser a través de la red TOR. Existen otros softwares que utilizan o interactúan con el TOR para suministrar anonimato, como el Privoxy [63] y el Vidalia.[64]

[63] http://www.privoxy.org
[64] https://www.torproject.org/projects/vidalia.html

Figura 3.43: Configuración del Firefox para utilización del TOR a través de Privoxy

Figura 3.44: Instalación del TOR en ambiente Windows

El TOR funciona de modo que cualquier software que utilice Internet como medio de comunicación pueda ser beneficiado con su tecnología. Así, no solamente navegadores pueden utilizar la red TOR, sino también mensajeros instantáneos, clientes de email, softwares para repartición de archivos, etc.

Cualquier persona o institución puede voluntariamente ofrecer una computadora con acceso a Internet para ser un nodo de la red TOR. Sin embargo, es necesario que esta computadora sea ruteable en la gran red, o sea, posea una dirección IP pública. La navegación a través de la red TOR es mucho más lenta que una navegación directa [65]. Ciertamente la demanda de usuarios es mayor que la capacidad disponible por la oferta de nodos TOR en Internet.

Figura 3.45: Instalación del TOR en ambiente Windows

[65] Pues depende de la capacidad de upload de los nodos, que en general es mucho menor que la de download.

Figura 3.46: Instalación del TOR en ambiente Windows

Figura 3.47: Instalación del TOR en ambiente Windows

Instalando el TOR en el Debian GNU/Linux

Para utilizar el TOR en el sistema operativo Debian y derivados del Debian (ej: Ubuntu) instalamos los paquetes tor y privoxy, conforme ejemplo a continuación:

root@ntccc:/home/ntccc# aptitude install tor privoxy

El próximo paso es configurar el Privoxy para conectarse en la red TOR, adicionando la siguiente línea en el archivo de configuración /etc/ privoxy/config:

forward-socks4 / 127.0.0.1:9050 .

Reinicie el privoxy:

root@ntccc:/home/ntccc# service privoxy restart

Y por fin configure su navegador Web para conectarse a Internet por medio del Privoxy. El concepto por detrás de esta secuencia de comandos es simple: su navegador se conecta en el proxy privoxy (puerta 8118), que se conecta en su cliente TOR (puerta 9050), que por fin dirige sus conexiones a la red TOR antes de que ellas lleguen a los destinos deseados. La figura 3.43 ilustra la configuración necesaria para que el navegador Firefox utilice esta estructura. La pantalla exhibida es alcanzada por los menús "Editar", "Preferencias", "Avanzado" y Configurar Conexiones, en este orden.

El software Vidalia ofrece un instalador simple y en idioma portugués para Windows, Apple OS, GNU/Linux y otros sistemas. En conjunto con el complemento del Firefox llamado torbutton [66] un usuario con poca habilidad técnica puede beneficiarse de la red TOR. Las figuras 3.44, 3.45 y 3.46 exhiben algunas etapas de la instalación, que es bastante intuitiva. La figura 3.47 ilustra el botón para activación del TOR en la parte inferior derecha del navegador, presente después de la instalación.

[66] https://www.torproject.org/torbutton/index.html

Figura 3.48: Distribución de nodos de la red TOR en el mundo.
Fuente: NTCCC

Para finalizar esta sección, ilustramos en la figura 3.48 la disposición de nodos TOR en el año 2009, mapeado en la época por el NTCCC/PR/SP. La figura 3.49 exhibe un gráfico más reciente, apuntando la distribución de nodos de salida en los diversos países en los cuales están hospedados.

Figura 3.49: Distribución de nodos de salida de la red TOR, por país de hospedaje.
Fuente: http://torstatus.blutmagie.de

3.8.4 Criptografía

La utilización de la computadora para cifrar un mensaje es bastante similar a los métodos tradicionales de cifrado, presentes desde Egipto antiguo, pasando por el Enigma de la segunda gran guerra [Singh 2005]. Hay todavía tres diferencias significativas al utilizar la computadora para este fin. La primera se refiere a la posibilidad de construir máquinas de cifrado hipotéticas a través de softwares, por ejemplo mezclando y ampliando la capacidad de millares de codificadores mecánicos simultáneamente, generando por fin un cifrado mucho más seguro. Las máquinas de cifras mecánicas obviamente se limitan a lo que es posible realizar en la práctica.

La segunda diferencia está en la velocidad de procesamiento, que es mucho mayor actualmente en virtud de que la electrónica opera más rápidamente que los mezcladores mecánicos. La tercera diferencia es que las computadoras mezclan números en lugar de letras del alfabeto. O mejor, trabajan exclusivamente con pulsos eléctricos representados por los dígitos uno y cero.

A pesar de las diferencias listadas anteriormente, el cifrado en la computadora ocurre por medio de los viejos principios de la transposición y sustitución, donde los elementos del mensaje cambian de posición o son sustituidos por otros, respectivamente. Por ejemplo, vamos a realizar un cifrado por sobreposición simple al correspondiente binario de la palabra **casa**. Aplicando un método de transposición que cambia el primer

dígito por el segundo, el tercero por el cuarto y así en adelante, tenemos el siguiente resultado:

casa –01100011011000010111001101100001 - 10010011100100101011001110010010

Se nota que el destinatario del mensaje no sería capaz de interpretar su contenido, a no ser que haya sido previamente comunicado sobre el método de cifrado utilizado, que en este caso fue una simple transposición de los dígitos vecinos. Este método revelado - de forma un poco grosera - es lo que llamamos **clave** [67]. O sea, el destinatario necesita conocer la **clave** para que, una vez aplicada al mensaje cifrado, esta revierta el proceso original de transposición (o sustitución) y revele su contenido original. Esta clave es generalmente comunicada previamente entre los pares, eventualmente utilizándose un medio de comunicación inseguro, dando márgenes a la interceptación. En caso que la clave del cifrado no sea conocida, será necesario utilizar técnicas robustas y creativas para su descifrado, aplicando métodos del área de estudio a la que se le da el nombre de criptoanálisis. Este ejemplo simple resume el funcionamiento de la criptografía simétrica, que veremos con más detalles a continuación.

[67] En la práctica tenemos que el método es una función matemática y la clave es una secuencia de caracteres. La función aplicada en esta secuencia de caracteres y en el mensaje original resulta en el mensaje cifrado. La misma función, al recibir la misma clave, será capaz de descifrar este mensaje. Tal hecho resulta en la necesidad de guardar secretamente la clave, dispensando la confidencialidad de la función matemática utilizada.

3.8.4.1 Criptografía simétrica

Técnicas de criptografía simétrica [68], permiten que un mensaje (en la práctica, cualquier archivo de computadora) sea encriptado a partir de una clave secreta, que en general es una frase-contraseña - o passphrase en inglés. A pesar de que haya diversas técnicas y softwares para este fin, el concepto de la criptografía simétrica está esencialmente basado en el hecho de que una clave secreta que es utilizada para cifrar un mensaje es también la misma utilizada para descifrarlo. Esto significa que necesariamente debe haber una comunicación entre los usuarios de origen y destino del mensaje para que se dé la repartición de esta clave. A no ser que esta comunicación sea realizada en canal seguro encriptado, ella podrá ser fácilmente interceptada por un tercero, que tendrá a partir de entonces el poder de descifrar todos los mensajes cifrados con esta clave.[69]

Es común encontrar archivos cifrados en Internet. En gran parte de los casos el usuario que suministra un archivo cifrado en la red solicita que los interesados por su contenido entren en contacto por un canal que él considera más seguro, como email, mensajeros instantáneos, teléfono o incluso personalmente. En algunos casos el usuario utiliza el beneficio de la criptografía como moneda de cambio para contenido ilícito, al ofrecer las claves necesarias para descifrar archivos a cambio de otros archivos ilícitos, como datos de tarjeta de crédito, imágenes y vídeos conteniendo pornografía infantil.

[68] También conocida por criptografía de clave secreta, de clave única, de clave compartida, o de una clave.

[69] En la lengua portuguesa se utiliza tanto cifrar/descifrar como encriptar/desencriptar para designar "traducir" para y "traducir" de lenguaje secreto.

Existen muchos algoritmos públicos capaces de ofrecer criptografía simétrica fuerte. Adicionalmente, existen millares de softwares para este propósito, los cuales utilizan

diferentes algoritmos, variaciones de estos, otros de carácter privado o varios de ellos en cascada para garantizar medios cada vez menos vulnerables a ataques. Tal hecho deja claro que no hay por tanto un método único o simple para la violación de la criptografía. Recomendamos que el enfoque de la investigación en Internet sea en la captura de las claves por medio de las técnicas abordadas en este Guión (interceptación, violación de confidencialidad telemática, etc.). El uso de la **fuerza bruta**, de la elección de herramientas para intentos de violaciones de criptografía y otros métodos más sofisticados en el ámbito del criptoanálisis serán inevitablemente menos efectivos y de mayor complejidad.

3.8.4.2 Criptografía asimétrica (o de clave pública)

Al tiempo que en la criptografía simétrica la misma clave es utilizada para cifrar y descifrar un archivo cualquiera, en el método de criptografía asimétrica solamente el destinatario posee la clave capaz de efectuar el descifrado. La encriptación es realizada por medio de un software específico, que recibe básicamente dos archivos: el archivo a ser cifrado y otro, que es la clave pública del destinatario. Como se ve, este tipo de criptografía dispensa el envío previo de una clave secreta para el destinatario. No obstante, es necesario que el destinatario suministre previamente su clave pública en algún local para que el remitente la utilice para cifrar el archivo a ser remetido.

Figura 3.50: Software para criptografía asimétrica GnuPG

El estándar de criptografía asimétrica más popular es el OpenPGP (Open Pretty Good Privace), definido en la RFC 244O. El software libre GnuPG implementa este estándar y es ampliamente utilizado en diferentes sistemas operativos. La figura 3.50 ilustra una pantalla del software asistente (GPA) del GnuPG para Windows.

Prácticamente no hay comercialización de softwares para violar criptografía, porque en este caso la criptografía se vuelve inútil. Existe no obstante una serie de programas - generalmente gratuitos - que ofrecen auxilio para violación de criptografía por medio de fuerza bruta y otras técnicas poco sofisticadas, normalmente enfocadas en herramientas específicas, como las decenas de herramientas que dicen que violan la contraseña de compactadores como Winzip y Winrar.

APÉNDICE E

EJEMPLOS DE PIEZAS PROCESALES

E.1 Pedido de búsqueda y aprehensión de computadoras. Crimen de racismo practicado por la red

EXCELENTÍSIMO SEÑOR JUEZ FEDERAL DEL Xº TRIBUNAL FEDERAL CRIMINAL DE LA SUBSECCIÓN JUDICIAL DE XXXXXX – SP

XXº Tribunal Federal Criminal de São Paulo
Autos número xxxxxxxxxxxxx - Investigación Policial
(IPL xxxxxxxxx)

MM Juez Federal:

1. La presente investigación policial tiene por objeto investigar la práctica del delito previsto en el artículo 20, encabezamiento, y párrafo segundo de la Ley 7716/89, por los usuarios denominados “xxx', “xxx', xxx', “xxx', “xxx' y “xxx', en CHAT del proveedor XXXX, que publicaron mensajes con contenido discriminatorio con relación a los negros y blancos, conforme fls. xx/xx.

Realizadas las diligencias necesarias, la empresa XXX informó que no es posible informar los datos del usuario denominado “xxx', que utilizó el IP xxx.xxx.xxx.xxx, en el período indicado (fls. xx), motivo por el cual las investigaciones con relación a él deben ser terminadas.

Por otro lado, se verificó que los accesos a Internet de los usuarios denominados “xxx', “xxx', xxx', “xxx' y “xxx', que utilizaron el IP xxx.xxx.xxx.xxx, en los períodos indicados, partieron de la misma dirección, o sea xxxxxxxxxx, São Paulo/SP, en nombre de xxxxxxxxx, conforme informaciones de la empresa xxxxxx (fls. xx).

2. Por medio de la representación en fls. xxx, el delegado de Policía Federal propone la realización de búsqueda y aprehensión en la referida dirección situada en la dirección xxxxxxxxxxx, São Paulo/SP, teniendo en cuenta que ese es el local de instalación de la línea telefónica por medio de la cual el usuario aquí investigado entró a Internet, así como publicó mensajes de contenido racista en el CHAT del proveedor xxxx.

3. En diligencias realizadas por la Policía Federal, fue constatado que xxxxxxxxxx reside en aquella dirección (casa de los fondos), junto con xxxxx y xxxx, según informó su xxxxxx (fls. xxx).

De esta forma, en razón de los elementos de convicción traídos a los autos, que resultan en fundados indicios de materialidad y autoría delictiva, se evidencia la necesidad de búsqueda y aprehensión en la dirección identificada, a fin de aprehender la (las) computadora(s) existente(s) en el inmueble, para examinar su contenido y comprobar la materialidad y autoría delictiva, de acuerdo con el art. 240, e y h, del Código de Proceso Penal.

4. Así siendo, el Ministerio Público Federal solicita:

4.1. archivar las investigaciones en relación al usuario denominado “xxx”, teniendo en cuenta la imposibilidad de identificar al usuario;

4.2. que sea determinada la emisión de mandato de búsqueda domiciliar, para cumplimento, con la necesaria discreción, en la dirección xxxxxxxxxxxxxxx, xxxxx, con el objetivo de:

a) aprehensión de todas las computadoras y material de informática (CDs, disquetes, pen drives, etc.) encontrados en el local;

b) aprehensión de otros elementos instrumentales al delito del artículo 20 de la Ley número 7.716/89.

En la oportunidad, la autoridad policial deberá, además, identificar realizar el interrogatorio de estas personas, especialmente de xxxxxxxx, para esclarecer la autoría delictiva.

Solicita, desde luego, autorización judicial para el acceso a los datos contenidos en el material que venga a ser aprehendido en la citada dirección.

São Paulo, xx de xxxx de xxxx

Xxxxxxxxxxxxxxx

Procurador de la República

E.2 Pedido de búsqueda y aprehensión de computadoras
Pornografía infantil

EXCELENTÍSIMO SEÑOR JUEZ FEDERAL DEL Xº TRIBUNAL FEDERAL CRIMINAL DE LA SUBSECCIÓN JUDICIAL DE XXXXXX – xxxx

Autos número xxxx.xxxx.xxxxxxxx

MM. Juez Federal:

1. La presente investigación policial tiene por objetivo la investigación del usuario que divulgó copia integral de los archivos xxx y xxx por intermedio de la red xxx, identificado como siendo de corte pedófilo.

Por medio de la representación en fls. xxx, el delegado de Policía Federal propone la realización de búsqueda y aprehensión en el inmueble situado en la dirección xxxxxxxxx, xxxx, CP xxxxxxxxx, teniendo en cuenta que ese es el local de instalación de la línea telefónica por medio de la cual el usuario aquí investigado entró a Internet, así como divulgó material de corte pedófilo, como se ve en fls. xxx/xxx.

2. Cabe notar, de inicio, que estos autos investigan hechos levantados por la policía xxxxx, en el ámbito de lo que se denominó la Operación XXXXXX.

Conforme se extrae en fls. xxx/xxx, el GECOP/DDH/CGDI/ DIREX/DPF recibió de la oficina de la Policía Criminal Estatal de xxxxx, notitia criminis referente a la divulgación, por parte de personas domiciliadas en Brasil, de los archivos ilícitos citados.

3. La materialidad delictiva queda clara por las imágenes que aparecen en fls. xxx/xxx, xxx/xxx y xxx, donde se verifica el ofrecimiento, intercambio, suministro, transmisión, distribución, publicación o divulgación, por medio de sistema de informática o telemático, de vídeo u otro registro conteniendo escena de sexo explícito o pornográfica con la participación de niño o adolescente.

En fls. xxx/xxx y xxx/xxx consta decisión redactada en los Autos número xxx. xxx.xxx.xxxxxxx-xx, que tramitó ante el xxo Tribunal Federal de la Sección Judicial del xxxxx, determinando la Violación de Confidencialidad de Datos Telemáticos para que las proveedoras de acceso envíen los datos de registro y logs de acceso de los usuarios brasileños cuyas IPs fueron identificadas por la policía xxxxx.

Fueron entonces suministrados, por la empresa xxx, los datos de registro de los usuarios de las IPs a ella vinculadas, lo que posibilitó la instauración de varias investigaciones policiales, en diferentes unidades de la Federación, para la determinación de la autoría.

4. Se investiga, en los presentes autos, el blanco xxxx de la operación, usuario de las IPs números xxx.xxx.xxx.xxx; xxx.xxx.xxx.xxx; xxx.xxx.xxx.xxx; xxx.xxx.xxx.xxx y xxx.xxx.xxx.xxx, de acuerdo con el extracto siguiente.

Según la información de la empresa xxx (fls. xxx/xxx), el blanco xxx sería xxxxxxxxx, portador del CPF número xxxxxxxxx, residente y domiciliado en la dirección xxxxxxxxxx, xxxxxxxx (fls. xxxx).

Así, ante los elementos de convicción traídos a los autos, que resultan en prueba de la materialidad y fundados indicios de autoría, se evidencia que es imprescindible la realización de búsqueda y aprehensión en la dirección identificada, para aprehender la computadora existente en el inmueble, viabilizándose el examen de su contenido y la obtención de otros elementos reveladores de la materialidad y autoría delictivas, de acuerdo con el art. 240, d, e y h, del Código de Proceso Penal.

5. Por todo lo expuesto, el Ministerio Público Federal solicita que sea determinada la emisión de mandato de búsqueda domiciliar, para cumplimiento, con la necesaria discreción, en la dirección xxxxxxxxx, xxxx, con el objetivo de:

a) aprehensión de todas las computadoras y material de informática (CDs, disquetes, pen drives, etc.) encontrados en el local;

b) aprehensión de cualesquiera materiales conteniendo imágenes de corte pedófilo (tales como libros, DVDs, CDs, impresos, vídeos, entre otros); y

c) aprehensión de otros elementos instrumentales del delito tipificado en el art. 241 y siguientes del ECA.

Solicita, desde luego, autorización judicial para el acceso a los datos contenidos en el material que venga a ser aprehendido en aquella dirección.

São Paulo, xxx de xxxx de xxxx

Xxxxxxxxxxxxxxxx

Procurador de la República

E.3 Pedido de interceptación del flujo de datos telemáticos
Pornografía infantil

Xº Tribunal Criminal Federal de la Sección Judicial de xxxxxxxxxxxxxxx

Autos número XXXX.XX.XX.XXXXXX-X

Se trata de procedimiento criminal instaurado para investigar el crimen previsto en el artículo 241 del Estatuto del Niño y del Adolescente.

El monitoreo de la cuenta del email xxxxxxxx ha sido muy productivo en el sentido de identificar individuos publicando pedofilia en la Red Mundial de Computadoras. Se pueden identificar una serie de usuarios publicando contenido con imágenes pornográficas con la participación de niños, entre los cuales están los usuarios de los emails xxxxxxxxx y xxxxxxxxxxxx.

Con respecto al email xxxxxxxxxxxxxxxxx fue autorizada la interceptación por este Juicio en los fls. xxx. No obstante, en contacto telefónico mantenido con xxxxxxxxxxxxx de la empresa xxxxxxxxxxxxxx, fue informado que la dirección mencionada no existe, tratándose, probablemente, de un artificio del usuario para no ser identificado.

Todavía, en el email enviado por el investigado está el número del protocolo generado en ocasión del envío de correspondencia electrónica, o sea xxxxxxxxxxxxxxxxxxx.

Ocurre, Excelencia, que en mensaje publicado por el mismo usuario en el sitio xxxxxxxxxxxxxxxxxxxxxxx, existe el relato de los crímenes de xxxxxxxxxxxxx, supuestamente practicados por él contra un niño de xxxxxxxx años, identificado como "xxxxxxxxxxxxxxxxxxxxxx" (relato y mensaje aquí anexados).

Ante lo expuesto, solicito sea oficiada la empresa xxxxxxxxxxxxxxxx, para que suministre, en el plazo de 24 horas, el número de teléfono y los datos de registro completos del usuario que entró a Internet el día xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx por medio del IP xxxxxxxxxxxxxxxxxxxxxxxxxxxxx (conforme encabezamiento de mensaje enviado al email xxxxxxxxxxxxxxxxxxxxxxx).

Con respecto al usuario de la cuenta xxxxxxxxxxxxxxxxxxxxxxxxxxx, se verificó que el mismo envió xxxxxxxxxxxxxxxx mensajes conteniendo imágenes pornográficas con la participación de niños.

Se trata, Excelencia, de gran cantidad de fotos de niños aparentando poquísima edad.

Presentes los indicios razonables de la materialidad y de la autoría del delito tipificado en el artículo 241 de la Ley 8.069/90 y, siendo la interceptación del flujo telemático y la Violación de la confidencialidad de los datos telemáticos los únicos medios posibles por el cual puede ser hecha la prueba, solicito en relación al usuario de la cuenta xxxxxxxxxxxxxx:

(i) la inmediata INTERCEPTACIÓN DEL FLUJO DE DATOS TELEMÁTICOS, de acuerdo con el artículo 1º, párrafo único, de la Ley 9.296/96, por el plazo de quince días, debiendo el proveedor de acceso xxxxxxxxxxxxxxxxxx ser oficiado en la persona de xxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx. Para la interceptación debe ser creada "cuenta-espejo" (cuenta-gancho creada por el proveedor, réplica de la cuenta original) cuyos datos, usuario y contraseña, deben ser rápidamente enviados a través de xxxxxxxxxxxxxxxxxxxxxxxxx al Ministerio Público Federal.

Al final de la interceptación el proveedor debe enviar a este Juicio, en multimedia y en papel, copia de todos los emails recibidos y enviados por el usuario, así como de los archivos en ellos anexados, debiendo, además, almacenar todos estos datos antes del final de la presente investigación;

(ii) la VIOLACIÓN DE LA CONFIDENCIALIDAD DE DATOS TELEMÁTICOS, debiendo la empresa xxxxxxxxxxxxxxxxxxxxxxxxx presentar, en el plazo de cinco días, todos los datos del suscriptor de las mencionadas cuentas de email, incluso las fechas de acceso y respectivos IPs y emails eventualmente almacenados.

Solicito, igualmente, ante la enorme cantidad de elementos probatorios que esta interceptación viene proporcionando, la prorrogación del plazo de la interceptación de los datos telemáticos del usuario de la cuenta xxxxxxxxxxxxxxxxxxxxxxxxxxxx, por otros 15 (quince) días, de acuerdo con el artículo 5º de la Ley 9.296/96.

Solicito, por fin, sea apreciado el pedido en fls. xxxxxxxxxxxxx, referente a la prorrogación de interceptación del flujo de datos telemáticos del usuario de la cuenta xxxxxxxxxxxxxxxxxxxxx, por otros 15 (quince) días, de acuerdo con el artículo 5º de la Ley 9.296/96.

São Paulo, xx de xxxxx de xxxxx.

Xxxxxxxxxxxxxxx

Procurador de la República

E.4 Pedido de violación de confidencialidad de datos telemáticos para proveedor que hospeda páginas web. Pornografía Infantil

EXCELENTÍSIMO(A) SEÑOR(A) JUEZ(A) FEDERAL DEL XXXXXº TRIBUNAL FEDERAL CRIMINAL DE LA SUBSECCIÓN JUDICIAL DE SÃO PAULO.

Piezas Informativas número 1.34.xxx.xxxxxxxxxxxx

El Ministerio Público Federal, por medio de la procuradora de la República signataria, solicita la VIOLACIÓN DE LA CONFIDENCIALIDAD DE DATOS TELEMÁTICOS, por los fundamentos fácticos y jurídicos expuestos a continuación:

I - DE LOS HECHOS

Las presentes piezas informativas fueron instauradas a partir de noticias anónimas, para determinación del crimen previsto en el artículo 241-A de la Ley 8.069/901 (Art. 241-A. "Ofrecer, intercambiar, suministrar, transmitir, distribuir, publicar o divulgar por cualquier medio, incluso por medio de sistema de informática o telemático, fotografía, vídeo u otro registro que contenga escena de sexo explícito o pornográfica con la participación de niño o adolescente "(Incluido por la Ley número 11.829, del 2008)), practicado por medio de la comunidad XXXXXXXXXXXXXXXXXX denominada "xxxxxxxxxxxxxxxxxx xxxxxx"(xxxxxxxxxxxxxxx) - (fls. xx/xx).

Consta en la noticia en fls. 04, que en la referida comunidad además de la divulgación de material conteniendo pornografía infantil, hay también indicación de sitios de tal contenido como www.xxxxxxxx.com.

Con relación a la página www.xxxxxxxxx.com, en investigación pública realizada en el sitio xxxxxxxxxxxxxxxxxx, fue constatado que está hospedado en servidor localizado en XXX,XXXXXX (investigación anexa).

Así, una vez que el proveedor no está situado en Brasil, y ante la inexistencia de noticia de participación de brasileños en el crimen noticiado, no hay que aplicar la ley patria en esta situación.

En razón de esto, fue enviada noticia acerca del referido sitio al Delegado de Policía Federal Representante de la INTERPOL en São Paulo, para tomar las medidas correspondientes.

Por otro lado, con respecto al servicio XXXXXXXXXXXXXXX, este es administrado por la empresa XXXXXXXXXXXXXXXXX.

El Sector de Informática de esta Procuraduría buscó e imprimió los documentos en fls. xx/xx, los cuales demuestran que los responsables por la comunidad publicaron imágenes conteniendo pornografía infantil.

Comprobada la materialidad, resta investigar la responsabilidad por la divulgación de las imágenes con contenido ilícito, una vez que tal conducta es tipificada como crimen de acuerdo con el artículo 241-A, de la Ley 8.069/90.

II- DE LOS FUNDAMENTOS

La violación de la confidencialidad de datos telemáticos es el único medio posible por el cual pueden ser recolectados los datos relativos a la autoría, indispensables para el proseguimiento de las investigaciones. Los usuarios de Internet se benefician de las dificultades encontradas en la investigación de crímenes de esta naturaleza para, contando con la impunidad, continuar en la actitud delictiva.

Es indispensable, para el proseguimiento de las investigaciones, la llegada del contenido de la página y la identificación de los responsables de la comunidad en referencia.

La competencia para la autorización de la violación de la confidencialidad de datos telemáticos, posteriormente solicitada, es hecha a la Justicia Federal, de acuerdo con lo dispuesto en el art. 109, inciso V, de la Constitución de la República (in verbis: "a los jueces federales compete procesar y juzgar los crímenes previstos en tratado o convención internacional, cuando iniciada la ejecución en el País, el resultado haya o debiese haber ocurrido en el extranjero, o recíprocamente").

Cualquier persona, en cualquier lugar del mundo, siempre que esté conectada a la red puede acceder a las fotos publicadas en el sitio. Se verifica, por tanto, cumplido el requisito de la transnacionalidad, exigido por el inciso V, art. 109, de la Constitución de la República, para justificar la competencia de esta Justicia Federal.

Además de esto, Brasil firmó el 24/09/1990 la Convención sobre los Derechos del Niño, adoptada por la Resolución L.44 (XLIV) de la Asamblea General de las Naciones Unidas el 20/11/1989.

III- DEL PEDIDO

Por todo lo expuesto, el Ministerio Público Federal, solicita la VIOLACIÓN DE LA CONFIDENCIALIDAD DE DATOS TELEMÁTICOS del responsable de la comunidad xxxxxxxxxxxxxx, debiendo la empresa xxxxxxxxxxxxxx. (con sede en la xxxxxxxxxxxxxxxxxxx) ser intimada en la persona de su Directora xxxxxxxxxxxxxxxx, para que:

1) envíe copia impresa y en medio magnético de todo el contenido de la comunidad xxxxxxxxxxxxxxxx;

2) logs de acceso (conteniendo los números de IP con fecha, hora y horarios GMT), direcciones electrónicas y otros datos eventualmente almacenados de la comunidad, su creador y también de sus responsables (tales como moderadores) xxxxxxxxxxxxxxx;

3) sin prejuicio de los ítems 1 y 2, retire la comunidad xxxxxxxxxxxxxx.

Con el objetivo de asegurar el proseguimiento de las investigaciones, solicita el Ministerio Público Federal el DECRETO DE CONFIDENCIALIDAD ABSOLUTA DE LOS PRESENTES AUTOS.

Para el mismo fin, solicita que del oficio a ser expedido a la empresa Google Brasil Internet Ltda., conste orden expresa para la preservación de la confidencialidad de la orden judicial aquí requerida.

São Paulo, xx de xxxxx de xxxxx.

xxxxxxxxxxxxxxx

PROCURADOR DE LA REPÚBLICA

E.5 Pedido para examen de investigación en computadoras aprehendidas. Pornografía Infantil

EXCELENTÍSIMO SEÑOR JUEZ FEDERAL DEL Xº TRIBUNAL FEDERAL CRIMINAL DE LA SUBSECCIÓN JUDICIAL DE XXX – XXX

Autos número XXXXXXXX –

Investigación Policial (IPL XXXXXX)

Consta en fls. xx y siguientes.

Se trata de investigación policial que tiene como objetivo identificar al usuario del sistema XXXX responsable del perfil de "XXXXXXX" (xxxxxxxxxxxxx) el cual habría utilizado la herramienta de privacidad ofrecida por el XXXXX para divulgar, en su álbum, fotos de contenido pornográfico con la participación de niños y adolescentes (fls. xxx y xx/xx).

Realizadas las diligencias necesarias, se localizó la dirección del referido usuario, habiendo sido emitido el respectivo mandato de búsqueda y aprehensión, el cual fue cumplido el xx/xx/xxxx, en la dirección xxxxxxxxx, xxx/xx, conforme Auto Circunstanciado de Búsqueda y Aprehensión y Auto de Aprehensión, cuyas copias están anexadas a los fls. xx/xx.

En la dirección, fueron aprehendidos: 1) un HD (disco duro) xxxx Gbytes, model "xxxx, s/n "xxxxx", extraído de la computadora localizada en el cuarto de xxxxxxxx; 2) un MP3 player digital, xxxx, color xxxx, con número de serie xxxx, de propiedad de xxxxxxxxxxxx; y 3) un HD (disco duro) xxxxx, model "xxxxxx", número de serie "xxxxxx", extraído de la computadora localizada en el cuarto de xxxxxxxx. Todos los objetos fueron acondicionados y lacrados con el lacre número "DPF xxxxx".

Consta en el Auto Circunstanciado de Búsqueda y Aprehensión (fls. xxx), que en el primer HD, fueron localizados registros de archivos de Internet con el nombre: "xxxxxxxx", entre otros archivos semejantes; y, en el segundo HD aprehendido, registro con el nombre: "xxxxxx", entre otros, los cuales justificaron la aprehensión. Con respecto al pendrive, el análisis de su contenido sólo sería posible en laboratorio.

Los objetos fueron enviados para la realización de investigación por medio del Memorando número xxxxx/xxxxx (fls. xxxx/xxxx).

De este modo, fueron los autos para formulación de requisitos por el Ministerio Público Federal (fls. xxxx), los cuales están relacionados a continuación y deberán ser respondidos por la investigación:

1) ¿Es posible identificar los usuarios del material aprehendido?

2) ¿Hay alguna información que vincule a los usuarios de las computadoras con el nick (apodo) "xxxxxxxxx" (xxxxxxxxxxxxxxx)? En caso positivo, es posible identificar al respectivo usuario, así como logins y contraseñas utilizados.

3) ¿Hay fotografías o imágenes con pornografía o escenas de sexo explícito con la participación de niños o adolescentes almacenadas en el material aprehendido? ¿Cuál es su naturaleza (películas, fotos, etc.)? ¿Entre las imágenes están aquellas que constan en los fls. xx?

4) ¿Es posible afirmar que hubo divulgación de fotografías o imágenes con pornografía o escenas de sexo explícito con la participación de niño o adolescente de esta computadora para otros usuarios de la red mundial? En caso positivo, ¿cuál es la fecha y el medio utilizado? ¿Cuál es el material enviado? ¿Para quién este material fue enviado?

5) ¿Hay mensajes recibidos de otros usuarios de Internet que contengan fotografías o imágenes con pornografía o escenas de sexo explícito con la participación de niño o adolescente? ¿Cuáles son las direcciones electrónicas de los remitentes? ¿Cuál es la fecha y el material recibido?

6) ¿Cuáles páginas de Internet fueron accedidas por los usuarios del material aprehendido?

7) ¿Es posible afirmar que los usuarios accedían al servicio xxxxx en Internet? En caso positivo, ¿cuáles eran las páginas (perfiles/comunidades) accedidas?

8) ¿Es posible afirmar que los usuarios participaban de grupos de discusión y/o comunidades en que divulgaban o publicaban fotografías o imágenes con pornografía o escenas de sexo explícito con la participación de niño o adolescente? ¿Cuáles son?

9) ¿Los usuarios poseen cuentas de email registradas? ¿Cuáles son?

10) ¿Es posible recuperar archivos o mensajes electrónicos borrados de la computadora? En caso afirmativo, ¿hay archivos o mensajes recuperados en que haya publicación o divulgación de fotografías o imágenes con pornografía o escenas de sexo explícito con la participación de niño o adolescente? ¿Cuál es la fecha y el medio utilizado? ¿Cuál es el material enviado? ¿Para quién fue enviado este material?

11) ¿Hay elementos que permitan concluir que fotografías o imágenes con pornografía o escenas de sexo explícito con la participación de niño o adolescente fueron producidas o editadas a través del conmutador aprehendido?

12) ¿Existen aplicaciones de edición y vídeos instalados en la computadora?

13) ¿Es posible afirmar que los usuarios obtuvieron para si o para otras ventajas patrimoniales con la divulgación o publicación de fotografías o imágenes con pornografía o escenas de sexo explícito con la participación de niño o adolescente?

14) ¿Hubo compras/ventas de fotografías o imágenes con pornografía o escenas de sexo explícito con la participación de niño o adolescente?

15) ¿Hay otras informaciones útiles para la elucidación del caso?

Por fin, teniendo en cuenta que de la búsqueda y aprehensión realizada en la mencionada dirección fue localizado material conteniendo pornografía infantil, y ante la

necesidad de identificar al respectivo responsable por el material, solicita que la Autoridad Policial proceda al interrogatorio de xxxxxx.

São Paulo, xxx de xxx de xxxxx.

xxxxxxxxxx

PROCURADOR DE LA REPÚBLICA

E.6 Denuncia. Artículo 241 del ECA

EXCELENTÍSIMO SEÑOR JUEZ FEDERAL DEL xxº TRIBUNAL CRIMINAL DE LA xxª SUBSECCIÓN JUDICIAL DEL ESTADO DE xxx xxxxxx

Autos número OOOxxxxxx

El Ministerio Público Federal, por medio del Procurador de la República que esta subscribe, viene ante la presencia de Su Excelencia para efectuar DENUNCIA en contra de xxxxxxxx, brasileño xxxx, xxxxx, xxxxxxx, portador de la cédula de identidad RG número xxxxx xxx/xxx e inscrito en el CPF/MF con el número xxxxxx, residente en la dirección xxxxxxxxx, xxxx, xxxxxx/xx;

por los hechos narrados a continuación:

1. En los Autos número xxxxxx, anexados a estos, se investigan hechos encontrados por la policía xxxxx, en el ámbito de lo que se denominó Operación xxxxx.

Conforme se extrae en fls. xx/xx de aquellos autos, el GECOP/ DDH/ CGDI/ DIREX/ DPF recibió, de la oficina de la Policía Criminal xxxxxx, notitia criminis referente a la divulgación, por parte de personas domiciliadas en Brasil, de archivos de vídeo conteniendo pornografía infantil.

El CD en fls. xxx contiene el archivo xxxxx, con diversas escenas pornográficas con la participación de niños. Este archivo fue bajado por el usuario de los IPs xxx.xxx.xxx.xxx y xxx.xxx.xxx.xxx, entre los días XX y XX de XXXX de XXXX, por medio de xxxxx.

Conforme esclarecimiento que aparece en el oficio copiando en fls. xx/xxx, “al "bajar" los archivos, aquí grabados en medio digital e integrantes de la presente "notítia criminis" , y salvarlos en carpeta compartida de la unidad de procesamiento utilizada, el internauta permite, de forma consciente y libre, que otras personas hagan el download del archivo a partir de su máquina, divulgando, de esta forma, las imágenes a través de la red mundial.”(fls. xxx)

2. Pues bien, a partir de los datos referentes a los IPs utilizados, suministrados por la policía xxxx, fueron obtenidos, con la empresa xxxx, los datos de registro del respectivo usuario, hasta aquel momento identificado solamente como blanco xx de la Operación xxxxx.

Tales datos apuntaron para el suscriptor xxxxx, residente y domiciliado en la dirección xxxxxxxxx, xxxx, xxxx (fls. xxx/xxx).

Determinada la búsqueda y aprehensión en la referida dirección (fls. xxx/ xxx), el cumplimento del respectivo mandato (fls. xxx) resultó en la prisión en flagrante de xxxxxxx.

3. De hecho, al dar cumplimento a la orden judicial, la Policía Federal constató que, en las computadoras utilizadas por xxxxxxxx, así como en un pen drive también de su propiedad, existían innumerables vídeos y fotos de contenido pornográfico, con la

participación de niños y adolescentes, conforme se ve en la información técnica en fls. xx/xx de los Autos número xxxxxxxxxxxxx, originados de la captura en flagrante.

Tal constatación, además de constituir crimen en si mismo, refuerza la evidencia derivada de la asociación entre los datos suministrados por la policía xxx y la información prestada por la empresa xxxx, lo que permite concluir que xxxxxxxxxx, usuario de la conexión mantenida por el suscriptor xxxxx, efectivamente bajó el vídeo de pornografía infantil que aparece en el CD en fls. xxxx de los Autos número xxxxxxxxxx, publicándolo, por consecuencia, en la red xxx por él utilizada.

Así, a partir de los elementos anexados a estos autos, se concluye que el Denunciado no solamente publicó, en idos de xxx de xxxx, el archivo xxxxx, conteniendo pornografía infantil, como consecuencia automática de su download por intermedio de xxxxx, como actualmente también almacenaba, en su computadora personal y en su pen drive, gran cantidad de material de tal especie.

4. Ante lo expuesto, el Ministerio Público Federal denuncia xxxxxxxxxx por infracción a lo dispuesto en el artículo 241 de la Ley número 8.069/90, en su redacción anterior a la Ley número 11.829/08, así como al actual artículo 241-B del mismo estatuto, en concurso material.

Recibida y actuada esta, solicita sea promovida la citación del Denunciado para responder a la acusación, de acuerdo con el art. 396 del Código de Proceso Penal, indicando para oportuno interrogatorio a los testigos listados a continuación.

São Paulo, xxx de xxxx de xxxxx

xxxxxxxxxxxxx

Procurador de la República

Lista de Testigos:

1.- xxxxxxx, APF, ubicado en el NO/DELINST/SR/DPF/SP; y

2.- xxxxxxx, EPF, ubicado en la DELEFIN/SR/DPF/SP.

E.7 Denuncia. Racismo

EXCELENTÍSIMO SEÑOR JUEZ FEDERAL DEL xxxxº TRIBUNAL CRIMINAL DE LA SUBSECCIÓN JUDICIAL DE xxx.

Autos número xxxxxxxxx

Denuncia número xxxxx/xxxxx

El MINISTERIO PÚBLICO FEDERAL, por medio del Procurador de la República que firmado, viene respetuosamente ante la presencia de Su Excelencia para ofrecer la presente

DENUNCIA

en contra de xxxxxxxxx, brasileño xxxx, xxxxxx, portador de la cédula de identidad RG xxxxxxxxxx, nacido el xxx de xxxx de xxxxx, residente y domiciliado en la dirección xxxxxxxxxxxx, xxxxx, xx; por la práctica de los siguientes hechos criminales:

Consta en los incluidos autos de investigación policial que el denunciado xxxxxxxxxx, el día xx de xxxx de xxxx, practicó, indujo e incitó la discriminación y el prejuicio de raza, color, etnia, religión y procedencia nacional, por intermedio del website xxxxxxxxxx,

La investigación que dio origen a la presente denuncia fue instaurada el xx de xxx de xxxxx, a partir de requisición formulada por la Procuraduría de la República en el Estado de São Paulo.

Según se determinó, el denunciado era miembro de una comunidad hospedada en el sitio de Internet xxxxxxxxxxxxxx, denominada "xxxxxxxxxxxxxxxxxxx", compuesta por xxxxx miembros, cuyo objetivo era la publicación de mensajes discriminatorios, incitando el odio y el exterminio de la raza negra. La referida comunidad fue objeto de denuncia anónima, enviada a esta Procuraduría de la República (fls. xx/xx).

Ya en la descripción de la comunidad, salta a los ojos el siguiente texto: "xxxxxxxxxxxxxxxxxxxxx" (fl. xxx).

Las discusiones trabadas en la referida comunidad no dejan duda acerca de su propósito, que era diseminar el odio y la discriminación contra los afrodescendientes. No obstante el gran número de miembros que ingresaron en la comunidad para manifestar repudio a la misma, expresivo era el número de miembros que insistía en la predicación de las ideologías racista y nazi.

En este contexto, en discusión sobre cuál sería el supuesto "regalo" concedido a los que siguiesen el propósito de la comunidad, el denunciado xxxxxxxxxxx afirmó lo siguiente (fl. xxx):

"xxxxxxxxxxxxxxxxxxxxxxxxxxx" (sic)

De esta forma, en posesión de las direcciones IP utilizadas por el usuario para efectuar su conexión a Internet, suministradas por la empresa xxxxx mediante determinación judicial (fls. xxxx), con la intención de identificar el autor del mensaje racista, se solicitó a la prestadora de servicios de telefonía los datos de registro del usuario de los referidos IPs. En respuesta, la empresa xxxxxxxxxxxxxxxx informó la dirección del denunciado, conforme información en fls. xx/xx.

En el proseguimiento de las investigaciones, se solicitó la emisión del mandato de búsqueda y aprehensión en la dirección identificada. Cumplido el mandato, conforme Auto Circunstanciado en fls. xxxx, fue aprehendida una serie de materiales de corte nazi, incluso dibujos remitiendo a la suástica, hojas impresas con imágenes de xxxx y relacionadas, de aplique de paño en formato de xxx, de DVD con el título "xxxxxx", de libro denominado "xxxxxx", de CDs de música "xxxxx", entre otros (fls. xxx/xxx).

Fue aprehendido, además, un HD de xxx GB, que también contenía material de corte racista y nazi, conforme Laudo de Examen de Dispositivo de Almacenamiento Computacional número xxx/xxxx, elaborado por el Núcleo de Criminalística de la Superintendencia Regional del Departamento de Policía Federal.

La materialidad del crimen es evidente. La autoría, a su vez, fue comprobada al conjugarse los hechos de haber sido el mensaje racista mencionado publicado en computadora localizada en la dirección residencial del denunciado, y haber este mismo cooperado con la Policía Federal para aprehensión del material de corte nazi y racista que se encontraba en su residencia, admitiendo, así, su participación en esta especie de movimiento. Se resalta que no fue encontrado ningún indicio de material racista entre las pertenencias de los demás residentes en el domicilio de xxxxxxxx. Este sería el único en la dirección a militar en favor del nazismo, expresando manifiesta aversión a los negros.

Practicando los hechos anteriormente descritos, se encuentra el acusado incurso en el artículo 20, encabezamiento y párrafo 2º, de la Ley número 7.716/89, delito este imprescriptible (artículo 5º, inciso XLII, de la Constitución Federal) y de competencia, en este caso, de la Justicia Federal, de acuerdo con el artículo 109, inciso V, de la Constitución Federal, en razón: a) de haber un tratado internacional en que Brasil se comprometió a combatir el racismo, más precisamente la Convención Internacional sobre la Eliminación de Todas las Formas de Discriminación Racial, que ingresó en el ordenamiento brasileño por medio del Decreto Presidencial número 65.810/1969; b) del hecho de que el uso de Internet para la propagación del racismo importa en inicio de ejecución en Brasil y producción de resultados en cualquier parte del mundo en que Internet pueda ser accedida.

Por todo lo expuesto, el MINISTERIO PÚBLICO FEDERAL denuncia xxxxxxxx como incurso en la pena prevista en el art. 20, encabezamiento, c.c. el § 2º, de la Ley 7.716/89, y con el art. 29 del Código Penal brasileño (incitación a la discriminación y al prejuicio a través de medio de comunicación social);

Solicita que, recibida y actuada esta, sea instaurado el proceso penal, competente citando e intimando al denunciado para todos sus actos, hasta la final condena, de acuerdo con los artículos 394 al 405 y 498 al 502 del Código de Proceso Penal, interrogándose, oportunamente, a los testigos listados a continuación.

São Paulo, xx de xxxx de xxxxx.

xxxxxxxxxxxxxxxxxx

Procurador de la República

LISTA DE TESTIGOS

1. xxxxxxxx (Delegado de Policía Federal);

2. xxxxxxxx (Delegado de Policía Federal - fls. 246)

E.8 MLAT - Mutual Legal Assistance Treaty

E.8.1 Pedido de Cooperación Internacional

Oficio número xxxxxxxxxxxxxxxxxxx

Ref.: Pedido de Cooperación Internacional número x.xx.xxx. xxxxxxxxx (Favor mencionar el número de referencia en la respuesta o en otras correspondencias).

São Paulo, xx de xxxx de xxxx.

Excelentísimo Subprocurador-General,

Por medio del presente, habiendo cumplido lo solicitado en el Pedido de Cooperación Internacional XXXXXXX - Brasil, envío el presente hecho conteniendo los documentos y las informaciones obtenidas para el debido envío (Pedido de Cooperación Internacional número x.xx.xxx. xxxxxxxx y el Expediente número xxxxxxxxxxxxx).

Atentamente,

xxxxxxxxxxxxxxxx

Procurador de la República

Al Excelentísimo Señor

XXXXXXXXXXXXXXXXXXXXXXXXXXXX

Subprocurador-General de la República

Coordinador del Centro de Cooperación Jurídica Internacional

SAF XX Cuadra X Conjunto X Bloque X Gab XX

CP XXXXX-XXX - Brasilia - DF

E.8.2 Formulario MLAT

Para: Departamento de Justicia de los Estados Unidos de América.

De: Departamento de Recuperación de Activos y Cooperación Jurídica Internacional de la Secretaría Nacional de Justicia.

Asunto: Pedido de Asistencia Jurídica en Materia Penal en razón de la producción, venta y divulgación, por medio de la red mundial de computadoras o Internet, de imágenes pornográficas, con la participación de niños y adolescentes brasileños, cuya dirección física del productor y distribuidor supuestamente se encuentra en California, Estados Unidos de América.

Referencia: Piezas Informativas número x.xx.xxx.xxxxxx/xxxx-xx.

Sumario: Piezas Informativas número x.xx.xxx.xxxxxx/xxxx-xx.

Hechos: Se cuida de Piezas Informativas, de número x.xx.xxx.xxxxxx/ xxxx-xx, iniciada a través de noticia de xxxxxxxxxxxxxxx.

Fue constatada la existencia del dominio electrónico www.xxxxxxx.com que comercializa vídeos pornográficos de niños y adolescentes, entre ellos, de nacionalidad brasileña, por copias físicas o descarga. Se encuentran divulgadas, además, fotografías con la participación de pornografía infantil-juvenil.

Se transcribe, a continuación, algunas descripciones de vídeos ofrecidos a la venta en el sitio mencionado:

1. Title: xxxxxxxxxxxxxxxxxxxxx - fls. xx;
2. Title: xxxxxxxxxxxxxxxxxxxxx - fls. xx.

De acuerdo con la página de Internet, xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Conforme la página xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Además, la página de dominio www.xxxxxxx.com, utiliza el proveedor host de IP xxx.xxx.xxx.xxx de la empresa “xxxxxxxx” (fls. xxx), supuestamente localizada en xxxxx. Esto significa que los logs de acceso al sitio www.xxxxxxxx.com están localizados en los servidores de propiedad de esta empresa, que presta el servicio de hospedaje para el mencionado sitio.

La empresa “xxxxxxxxxxxxxxx”, a su vez, supuestamente localizada en xxxxxxxxxxxxxxxxxxxxxx, ofrece el servicio de dirección electrónica para el propietario del dominio www.xxxxxxx.com. Según búsqueda en las bases de datos WHOIS y DNS, el email utilizado para el contacto administrativo del sitio en cuestión es xxxxx@xxx. xxx.xxxx.

Se subraya, por fin, que no solo las fotografías divulgadas al lado de los vídeos a ser comercializados, sino las propias informaciones de la página (xxxxx xxxxxxxx xxxxxxxx xxxxxx) demuestran que se trata de imágenes con la participación de

pornografía infantil-juvenil, lo que configura el crimen previsto en el artículo 241, de la Ley número 8.069, del 13/07/1990.

Delitos: Ley número 8.069, del 13/07/1990

Artículo 241 - Presentar, producir, vender, suministrar, divulgar o publicar, por cualquier medio de comunicación, incluso red mundial de computadoras o Internet, fotografías o imágenes con pornografía o escenas de sexo explícito con la participación de niño o adolescente:

Pena - reclusión de 2 (dos) a 6 (seis) años, y multa.

§ 1º Incurre en la misma pena quien:

I - agenciar, autorizar, facilitar o, de algún modo, intermediar la participación de niño o adolescente en la producción referida en este artículo;

II - asegurar los medios o servicios para el almacenamiento de las fotografías, escenas o imágenes producidas de acuerdo con el encabezamiento de este artículo;

III - asegura, por cualquier medio, el acceso, en la red mundial de computadoras o Internet, de las fotografías, escenas o imágenes producidas de acuerdo con el encabezamiento de este artículo.

§ 2º La pena es de reclusión de 3 (tres) a 8 (ocho) años:

I - si el agente comete el crimen valiéndose del ejercicio de cargo o función;

II - si el agente comete el crimen con el fin de obtener para si o para otros una ventaja patrimonial.

Descripción de la Asistencia Solicitada:

1. Sea determinado que la empresa “xxxxxxxxxxxxxxxx”, situada en xxxxxxxxxxx, suministre: los datos de registro del usuario responsable de la página www.xxxxxxx.com, incluyendo nombre y dirección completos, teléfono(s) y email(s) de registro; todos los logs de acceso remoto al sitio en cuestión, hospedado en el servidor de esta empresa, con fechas, horario GMT y respectiva IPs; todo el contenido hospedado en el servidor de dirección IP xxx.xxx.xxx.xxx, incluyendo fotos, vídeos y archivos de texto que hayan sido enviados por el usuario que mantiene el sitio www.xxxxxxx.com.

2. Sea determinado que la empresa “xxxxxxxxxxxxxxxx”, situada en xxxxxxxxxxxxxxx, suministre: los datos de registro, incluyendo nombre y dirección completos, teléfono(s) y email(s) de registro del usuario xxxxx@xxx.xxx.xxx; todos los logs de acceso realizados por el usuario xxxxxx@xxx.xxx.xxx, con fechas, horario GMT y respectiva IPs; todo el contenido presente en los servidores de propiedad de la empresa de los emails emitidos y recibidos por el usuario xxxxxx@xxx.xxx.xxx.

3. Sea determinado que la empresa “xxxxxxxxxxxxxxxx”, situada en xxxxxxxxxxxx, suministre: informaciones con respecto al contrato de servicio de tarjeta de crédito realizado con el responsable de la página www.xxxxxxx.com, en especial, todos los datos de ese último contratante;

Objetivo de la Solicitud: obtener todos los logs de acceso y datos de registro del usuario de Internet responsable del sitio www.xxxxxxx.com, con base en los cuáles será posible descubrir los responsables por la producción, alimentación de la página con los vídeos, así como por su comercialización.

Procedimientos a ser observados: confidencialidad de los datos telemáticos obtenidos y urgencia en la respuesta.

E.8.3 Oficio - Secretaria Nacional de Justicia

Oficio número xxxxxxxxxxxxxxxx x, xx de xxxx de xxxx.

Sr. Secretario

Envío a Su Excelencia el pedido de cooperación judicial penal internacional con los Estados Unidos de América, efectuado por medio del formulario MLAT, anexado al presente.

Me coloco, desde ya, a disposición de Su Excelencia para eventuales esclarecimientos sobre los hechos, subrayando que puedo ser contactada por medio del teléfono (xx) xxxx-xxxx y por el email xxxxx@ xxxx.mpf.gov.br.

Aprovecho la oportunidad para presentar a Su Excelencia votos de estima y consideración.

xxxxxxxxxxxxxxxxxxxxx

Procurador de la República

Exma. Sr.

Dr. xxxxxxxxxxxxxxxxxxx

DD. Secretaria Nacional de Justicia Ministerio de la Justicia -
Brasilia/DF