Universidad Nacional de Córdoba

Facultad de Matemática, Astronomía y Física

Especialización en Criminalística y Actividades Periciales

Trabajo Final Integrador "Técnicas Anti-Forenses Informáticas"

Autor: Lic. Miguel Darío Vasquez

Director: MCs. Ing. Eduardo Casanovas

Córdoba - Marzo 2016

Agradecimientos

- A *Fernando Comuñez*, docente del módulo de Marco Jurídico, quién facilitó parte de la bibliografía para dar el contexto legal con respecto a los delitos informáticos.
- A la empresa *Intel*, que permitió tener horarios laborales flexibles para cursar la especialización en tiempo y forma durante estos dos últimos años.
- A *Eduardo Casanovas*, quien acepto dirigir el trabajo, revisarlo y sugerir mejoras.
- A los miembros del *Tribunal Evaluador*, quienes accedieron participar de la evaluación del Trabajo Final Integrador.

Prefacio

El Trabajo Final Integrador fue concebido como una monografía con el estado del arte de las técnicas anti-forenses informáticas más utilizadas en la actualidad. Se han abordado conceptos de los siguientes módulos:

- *Informática Forense:* estudiando las diferentes técnicas anti-forenses que pueden dificultar la investigación de un perito forense informático.
- *Análisis de Imágenes:* analizando los formatos de imágenes y videos para uso de esteganografía.
- *Metodología de la Investigación:* resaltando que los procedimientos y metodologías forenses no son infalibles y también pueden ser atacados.
- *Marco Jurídico:* comparando la legislación argentina con la internacional, respecto a los delitos informáticos.
- *Ética y Deontología:* tratando de justificar la importancia del "hacker ético" como impulsor de nuevas técnicas anti-forenses y mencionado los principios éticos que debería adoptar un profesional informático.

El objetivo general es entender cómo piensa y actúa un delincuente informático para dificultar la investigación de un perito forense informático. El conocimiento de las técnicas anti-forenses resulta de utilidad al *perito oficial* que lleva adelante la investigación, para pensar en formas alternativas de buscar la evidencia digital. Por otro lado también le resulta útil al *perito de control*, para defender a su parte y cuestionar los procedimientos forenses.

Notar que este conocimiento también podría ser mal utilizado por un "hacker anti-forense". En ese sentido este trabajo no realiza apología de delitos informáticos, sino que tiene fines educativos y profesionales. Se pretende concientizar que estas prácticas existen y hay que saber lidiar con ellas.

Índice General

Índice de Abreviaturas

ACM Association for Computing Machinery. 51
AES Advanced Encryption Standard. 5, 7
AIFF Audio Interchange File Format. 12
ATA Advanced Technology Attachment. 16
BPCS Bit-Plane Complexity Segmentation. 14
CEI Computer Ethics Institute. 52
DBAN Darik's Boot and Nuke. 20
DCO Device Configuration Overlay. 16
DCT Discrete Cosine Transform. 14, 15, 25
DFT Discrete Fourier Transform. 13, 14
DNS Domain Name Server. 32
DoS Denial of Service. 30, 37
DWT Discrete Wavelet Transform. 14
EBE Edges Based Embedding. 14
FDE Full Disk Encryption. 5
HDD Hard Disk Drive. 5, 19
HPA Host Protected Area. 16, 19
ICMP Internet Control Message Protocol. 15
IEEE Institute of Electrical and Electronic Engineers. 8, 51
IMEI International Mobile Equipment Identity. 47
IMSI International Mobile Suscriber Identity. 47
IP Internet Protocol. 7, 9, 15, 32, 47
JPEG Joint Photographic Experts Group. 25
LSB Least Significative Bit. 13
MD5 Message Digest Algorithm 5. 7
MP3 MPEG Audio Layer 3. 12
NSA National Security Agency. 17
OSI Open System Interconnection. 15
PVD Pixel Value Differencing. 14
RC4 Rivest Cipher 4. 7
RGB Red Green Blue. 25
RPE Random Pixel Embedding. 14
SED Self Encrypting Drive. 5

SHA Secure Hash Algorithm. 7

SMART Self-Monitoring Analysis and Reporting Technology. 32

SOCKS Socket Secure. 10

SSD Solid State Drive. 5, 20, 54

SSL Secure Socket Layer. 7

TCP Transmission Control Protocol. 7, 10, 15

TKIP Temporal Key Integrity Protocol. 8

TLS Transport Layer Security. 7

TPVD Tri-way Pixel Value Differencing. 15

UDP User Datagram Protocol. 15

USB Universal Serial Bus. 5, 20, 24, 54

US-CERT United States Computer Emergency Readiness Team. 1

VPN Virtual Private Network. 7

WAV Waveform Audio File Format. 12

WEP Wired Equivalent Privacy. 8

WPA Wi-Fi Protected Access. 8

Índice de Figuras

Índice de Tablas

Resumen

Palabras claves: *perito, forense, anti-forense, evidencia digital, hacking, delito informático.*

Las técnicas anti-forenses buscan frustrar a los peritos, pericias y herramientas forenses.

Por ejemplo, las técnicas de ocultamiento de datos esconden la evidencia digital. En particular, la criptografía asegura la protección de datos y brinda un canal de comunicación seguro ante un potencial análisis forense. La esteganografía oculta la información de tal modo que el perito forense no advierte el envío de los datos secretos en archivos o protocolos de red. Otros procedimientos encapsulan software maliciosos para evitar su detección. Por último, los datos pueden ocultarse en espacios no convencionales del sistema de archivos o medio de almacenamiento.

Algunos métodos eliminan datos para destruir la evidencia digital. La sanitización de un disco puede ser: lógica, analógica, digital o criptográfica. Existen métodos más drásticos como la destrucción física del medio de almacenamiento.

Técnicas como la anti-concepción de datos evita la creación de datos. Normalmente se realizan llamadas al sistema de un proceso remoto o se ejecutan los procesos completamente en memoria para no dejar rastros en el disco.

Ciertos métodos de ofuscación buscan confundir o desviar la investigación. Se sobrescriben metadatos de los archivos o se aplican artilugios en el envío de e-mails para dificultar la detección del emisor o receptor.

Una nueva tendencia es atacar al software forense, en especial la validación de datos, integridad del hash, heurísticas frágiles o incluso provocando denegación de servicio. También se pueden cuestionar las diferentes etapas de los procedimientos forenses utilizados para recolectar o analizar la evidencia digital.

Existe una estrecha relación entre técnicas anti-forenses, delitos informáticos y *hacking*. La tecnología avanza mucho más rápido que la legislación, dejando ciertos vacíos legales que pueden ser explotados. Al tratarse de una actividad que trasciende las fronteras, es difícil juzgar y capturar a un delincuente informático. La legislación argentina presenta algunas carencias con respecto al Convenio sobre Ciberdelincuencia, pero está relativamente actualizada en comparación a los países de la región.

Como reflexión final, un *hacker ético* puede desarrollar técnicas anti-forenses con la finalidad de mejorar el software y los procedimientos forenses, sin que ello represente un delito informático.

Summary

Title: Computer Anti-forensics
Key words: *forensic expert, anti-forensic, digital evidence, hacking, cybercrime.*

Anti-forensic techniques are designed to frustrate the forensic expert, investigation and tools.

For instance, data hiding techniques conceal the digital evidence. In particular, encryption ensures data protection and provides a secured communication channel against potential forensic analysis. Steganography hides information so that the forensic expert does not detect data being sent through files or network protocols. Another procedures encapsulates malicious software to avoid detection. Finally, the data can be hidden in non-conventional locations of file system or disk.

Some methods delete data to destroy digital evidence. Disk sanitization can be: logic, analog, digital or cryptographic. There exist more drastic methods, such as physical destruction of storage media.

Techniques like anti-conception techniques avoid data creation. The most common are the system calls to a remote process or execute processes completely in memory without leaving any traces on disk.

Obfuscation methods confuse or divert the investigation. File metadata is overwritten or hacks are applied in e-mail transmission in order to avoid detection of sender or receiver.

A new trend is to attack the forensic software; especially data validation, integrity hash, fragile heuristics or even generating a denial of service. Another strategy is to question the forensic procedures used to collect and analyze the digital evidence.

There is a tight relationship between anti-forensic, cybercrime and hacking. Information technology is moving much faster than legislation, leaving some loopholes that can be exploited. Being an international activity, it is difficult to judge and capture a cyber-criminal. Argentine legislation has some deficiencies in comparison to the Cybercrime Convention, but is relatively updated in comparison to neighbor countries.

As a final thought, an ethical hacker can develop anti-forensic techniques in order to improve the software and forensic procedures, without that represents a cybercrime.

Capítulo 1

Introducción

En tiempos donde las telecomunicaciones y el manejo de la información se encuentran globalizados y al alcance de cada vez más personas, los delitos informáticos han proliferado y en formas más sofisticadas. Es acá donde toma importancia mantener actualizadas las metodologías y herramientas que analizan la evidencia digital.

La US-CERT es una organización que combate los delitos informáticos en EE.UU. y define *informática forense* como [1]:

> *"La disciplina que combina elementos legales y de la ciencia de la computación para colectar y analizar datos desde sistemas computacionales, redes, comunicaciones inalámbricas y dispositivos de almacenamiento; en una manera que es admisible como evidencia ante una corte."*

Si consideramos todos los métodos disruptivos que puedan interferir en el correcto análisis de la evidencia digital, llegamos al concepto de anti-forense. Más formalmente, se define como *anti-forense* [15]:

> *"Conjunto creciente de herramientas y técnicas que frustran las investigaciones, investigadores y herramientas forenses."*

Teniendo como objetivos principales:

- Evitar la detección de algún tipo de evento que ya ocurrió.
- Interferir en la recolección de la información.
- Aumentar el tiempo que demanda una pericia.
- Sembrar duda sobre el informe de la pericia.

Este trabajo se enfoca en presentar varias técnicas anti-forenses que pueden dificultar el trabajo del investigador forense. Más formalmente se define como *perito* [24]:

> *"Sujeto al cual el juez debe ineludiblemente recurrir cuando se ha verificado que para descubrir o valorar un elemento de prueba son necesarios determinados conocimientos artísticos, científicos o técnicos."*

En particular, el *perito oficial* es aquel que presta servicios en relación de dependencia en cualquiera de los poderes del Estado (principalmente el Judicial) y en organismos como universidades nacionales. Por otro lado se considera *perito de oficio* a aquel particular que es designado por el órgano judicial, por ejemplo aquellos que están anotados en las listas de peritos judiciales. Por simplicidad, en el resto del trabajo nos referiremos al perito oficial con conocimientos informáticos simplemente como *perito informático forense*.

A su vez, cada parte puede proponer otro perito legalmente habilitado a su costa. Es el llamado *perito de parte*, también llamado perito contralor o perito de control.

El principal propósito del trabajo es informar y alertar sobre las deficiencias de las herramientas y procedimientos informáticos forenses actuales. Luego se dará el contexto legal, definiendo qué es un delito informático y estudiando las legislaciones vigentes en diferentes países para dimensionar el alcance y consecuencias de las técnicas anti-forenses. También se analizarán aspectos éticos, en relación a los profesionales informáticos, para discutir en qué contexto puede ser positivo innovar sobre técnicas anti-forenses.

Al final del trabajo se incluye un anexo con varias herramientas anti-forenses que implementan las técnicas estudiadas.

Parte I

Técnicas Anti-forenses

Capítulo 2

Ocultamiento de Datos

Estas técnicas apuntan principalmente a ocultar la evidencia digital. El perito forense informático puede encontrarla pero sin poder interpretarla; o peor aún no encontrarla por la manera que fue ocultada.

2.1 Criptografía

Del griego *kryptos* (secreto) y *graphein* (escritura), es un conjunto de técnicas para proteger datos y tener una comunicación segura en presencia de terceros, llamados adversarios. Paradójicamente, el adversario en este caso sería el perito forense informático, de quién se desea proteger la comunicación.

La criptografía está basada en matemática avanzada, complejidad computacional, probabilidad y estadística. Sin embargo, como no es necesario comprender la matemática subyacente para poder utilizarla, se convierte en una herramienta potente y peligrosa en manos de delincuentes informáticos.

En primer lugar se dan algunos conceptos básicos de criptografía [19], que se utilizarán para explicar las técnicas anti-forenses mencionadas en esta sección.

- *Cifrado*: es el proceso de codificar un mensaje de tal manera que su significado no es obvio.
- *Descifrado*: es el proceso inverso, transformando un mensaje cifrado a su forma original.
- *Criptosistema*: un sistema que permite cifrado y decifrado.
- *Texto plano*: la forma original del mensaje.
- *Texto cifrado*: la forma cifrada del mensaje.

2.1.1 Cifrado de Discos

La empresa de seguridad Symantec publicó un artículo detallando como funciona el cifrado de un disco [9]. Esta estrategia se utiliza en general para proteger la información en caso de robo o pérdida accidental; o en este caso para resistir un análisis forense. Se cifra el disco completo incluyendo los archivos regulares, archivos de swap/paginación, archivos de sistema

y los generados por hibernación[1]. Sólo el usuario autorizado puede acceder a sus contenidos. Sin embargo, no existe protección cuando el usuario ya inició sesión en el sistema operativo y deja desatendida la computadora, permitiendo que usuarios no autorizados abran cualquier archivo del disco.

Uno de los mayores desafíos es cómo se modifica el sector de arranque del disco para habilitar el cifrado. El sistema de arranque es el conjunto de operaciones que se ejecutan cuando se enciende la computadora. El cargador de arranque (*boot loader*) es un pequeño programa que carga el sistema operativo principal y que se aloja en el punto de arranque del disco. En el momento que se inicia la computadora, se lanza una pantalla requiriendo un passphrase[2] y luego de autenticar al usuario continua cargándose el sistema operativo normalmente.

Varios de estos software, también pueden cifrar medios de almacenamiento externos como discos HDD, SSD y USB flash. Del mismo modo, cuando se monta el medio de almacenamiento externo, se requiere un passphrase para autenticar el usuario antes de utilizar el disco.

El software opera en conjunto con la arquitectura del sistema de archivos, capturando la mayoría de las operaciones de entrada/salida (I/O). Es por ello que existe alguna degradación del desempeño, pero el mecanismo de cifrar/descifrar es totalmente transparente para el usuario. Cuando se cifra el disco por primera vez se cifran los bloques del disco uno por uno.

Los datos descifrados nunca están disponibles en el disco. Cuando un usuario accede un archivo, los datos se descifran en memoria antes que sean presentados para ver. Cuando se modifica un archivo, los datos son cifrados en memoria y son escritos en los correspondientes bloques del disco.

2.1.2 Cifrado de Discos por Hardware

El cifrado completo del disco por hardware, o Full Disk Encryption (FDE), es totalmente transparente para el usuario. Salvo la autenticación inicial, opera como cualquier otro disco. No existe degradación del desempeño como ocurre en el cifrado por software, ya que todas las operaciones criptográficas son invisibles al sistema operativo y al CPU.

El disco protege todos los datos, aún el sistema operativo está cifrado con un algoritmo robusto como el AES. El disco requiere un código de autenticación, el cual debe tener al menos 32 bytes (256 bits) para desbloquear el disco.

La clave simétrica de cifrado es mantenida independiente del CPU, esto es para evitar ataques criptográficos sobre la memoria RAM de la computadora. En relación a los discos HDD, se usa más comúnmente el término Self Encrypting Drive (SED).

[1] Apagar una computadora guardando el estado de la memoria de ese momento.

[2] Secuencia de palabras utilizada como una contraseña, pero más larga.

2.1.3 Cifrado de Discos Virtuales

Una de las herramientas más conocidas de este tipo es TrueCrypt[6]. Es capaz de mantener sobre la marcha (*on-the-fly*) un volumen cifrado. Esto quiere decir que los datos son automáticamente cifrados justo antes que se almacenen y son descifrados justo antes de ser leídos, sin intervención alguna del usuario. Para leer datos del volumen cifrado, se debe utilizar una clave criptográfica. Este tipo de herramientas cifran por completo su sistema de archivos: nombres de archivos, directorios, contenidos, espacio libre y metadatos.

2.1.4 Sistemas de Archivos Criptográficos

Una de las maneras más sencillas para cifrar datos en un disco es utilizar un sistema de archivos criptográfico, mediante el cual se provee una capa adicional de seguridad.

Son especialmente diseñados con la idea de cifrado y seguridad en mente. Se cifran todos los datos, incluyendo los metadatos del sistema de archivos como: estructura de directorios, nombres de archivos, tamaños o fechas. Usualmente se implementan alojándose en un directorio sobre un sistema de archivos existente.

2.1.5 Sistemas de Archivos con Cifrado

A diferencia de los sistemas de archivos criptográficos o discos cifrados, este tipo de sistemas de archivos cifran archivos específicos, pero típicamente no cifran los metadatos. Esto puede ser un problema si esa información es confidencial. Dicho de otra manera, utilizando herramientas forenses se podría saber que documentos están almacenados en el disco, aunque no sus contenidos.

Cuando el usuario inicia sesión en un sistema operativo, los contenidos del archivo permanecen cifrados. Puede operar a nivel de archivos como el Encrypted File System de Microsoft, o a nivel de bloques como es el caso del PGP Virtual Disk.

Se requiere acción por parte del usuario. Los nuevos archivos creados o los archivos temporales generados por las aplicaciones de software como los navegadores web, no se cifran automáticamente.

2.1.6 Protocolos de Comunicación

Las comunicaciones de Internet cifradas hacen que el análisis del tráfico de red se vuelva muy difícil. Eventualmente un analista forense podría utilizar herramientas como Wireshark (Windows y Linux) o TCPDump (Linux) para analizar los paquetes de la red, pero al estar cifrados difícilmente se pueda examinar su contenido.

Los paquetes de datos que se transportan a través de Internet tienen dos partes, un cuerpo de datos (*payload*) y un encabezado (*header*) utilizado para el ruteo del paquete. El

payload puede contener datos de un email, una página web o un archivo de audio. Aunque el payload se encuentre cifrado, un analista forense a partir de los headers podría inferir orígen, destino, tamaño, hora de envío, etc.

El mayor problema se da en los intermediarios, ya sean los autorizados como por ejemplo los proveedores de Internet, o también los atacantes utilizando técnicas estadísticas para identificar patrones en las comunicaciones. Para todos estos casos el cifrado podría no ser suficiente y esto motivó a la creación de proyectos como Tor que se discute en el final de esta sección.

A continuación se discuten los principales protocolos de comunicación que utilizan el cifrado.

SSL/TLS El protocolo Secure Socket Layer (SSL) fue diseñado originalmente por Netscape para proteger la comunicación entre el navegador web y el servidor web (ver Figura 2.1). Luego evolucionó como Transport Layer Security (TLS). Es una interfaz entre aplicaciones y los protocolos de red TCP/IP para proveer autenticación del servidor y cliente; y un canal de comunicación cifrado entre ambos. El servidor y cliente negocian una suite para cifrado y hashing durante la sesión; por ejemplo AES con SHA1, o RC4 (clave de 128 bits) con MD5.

Inicialmente el cliente requiere una sesión SSL. El servidor responde con su certificado que incluye la clave pública, tal que el cliente pueda determinar la autenticidad del servidor. El cliente retorna parte de una clave simétrica de sesión que es cifrada usando la clave pública del servidor. Ambos calculan la clave de sesión compartida y a partir de ese momento mantienen un canal de comunicación cifrado.

El protocolo es simple pero efectivo y es el más utilizado de los protocolos de red seguros en Internet. Sin embargo hay que remarcar que el protocolo sólo protege los datos entre el navegador y el punto de descifrado en el servidor. Los datos están expuestos entre el teclado y el navegador, como así también en el servidor receptor. Para solucionar esto existen algunos software como LocalSSL, que protegen los datos localmente de potenciales keyloggers o troyanos.

VPN En una Virtual Private Network (VPN) se extiende una red privada a través de una red pública como Internet (ver Figura 2.2). Le permite a los usuarios enviar y recibir datos a través de redes públicas como si sus dispositivos estuvieran conectados directamente a la red privada, dando los beneficios de funcionalidad y gestión de políticas de seguridad para la red privada.

Se pueden usar varios firewalls para implementar una VPN. Cuando un usuario establece una comunicación con el firewall, puede requerir una clave de cifrado para la sesión, y subsecuentemente ambos la utilizan para cifrar todo el tráfico entre ambos. De esta manera, se restringe la red sólo a aquellos usuarios que la VPN le dio accesos especiales a través de

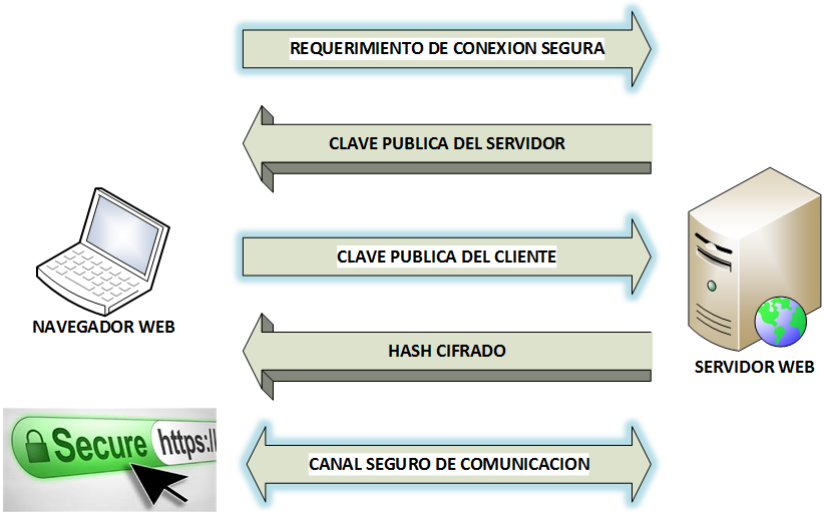

Figura 2.1: SSL durante la navegación web

sus políticas de seguridad. Es por ello que al usuario le da la impresión que está en una red privada aún cuando no es así.

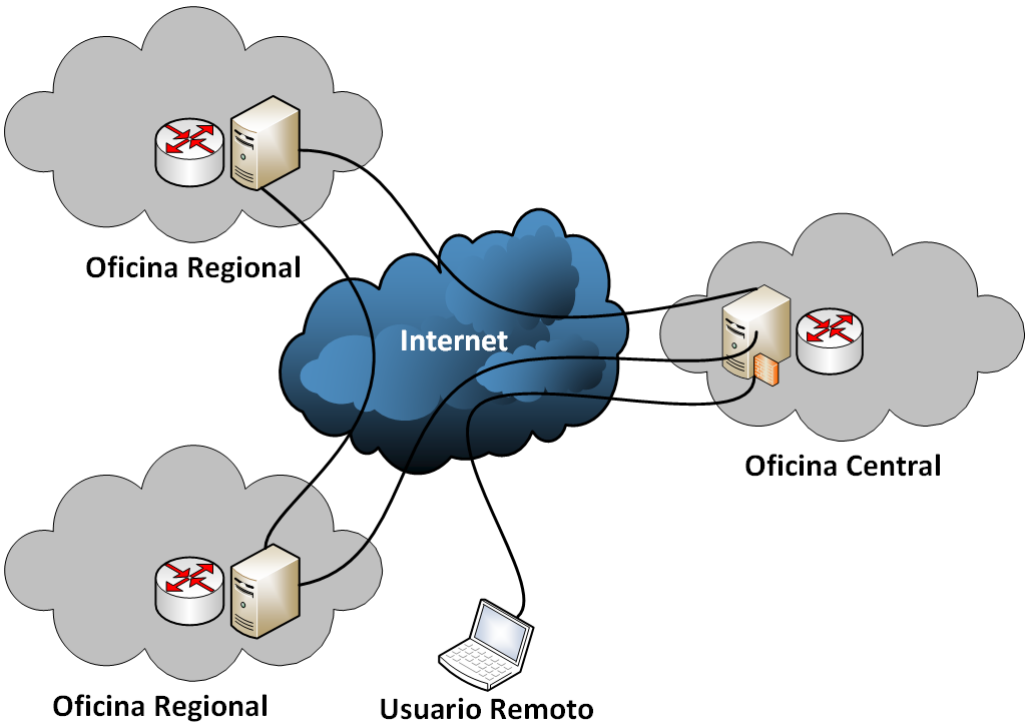

Figura 2.2: Red privada virtual

WPA2 El protocolo criptográfico para comunicaciones inalámbricas Wi-Fi Protected Access (WPA), fue creado para mejorar todas las fallas de seguridad que tenía su predecesor Wired Equivalent Privacy (WEP). El estándard IEEE 802.11i fue aprobado en 2004 y es conocido ahora como WPA2, el cual es una extensión de WPA. Las mejoras introducidas son:

- Se cambia la clave de cifrado automáticamente en cada paquete del tráfico, estrategia llamada TKIP.
- La autenticación puede ser hecha por: password, token, certificado u otro mecanismo.
- WPA2 usa un algoritmo de cifrado mas robusto como AES.
- Se utiliza un chequeo de integridad de 64 bits que esta cifrado.
- El protocolo de inicio tiene tres pasos: autenticación, handshake de 4 pasos y un handshake opcional para comunicación multicast (ver Figura 2.3).

Luego del intercambio regular para lograr la autenticación, se genera una clave secreta compartida (PMK). El intercambio de mensajes que se ejecuta durante el handshake de 4 pasos se resume de la siguiente manera.

1. El punto de acceso envía al cliente un mensaje ANonce, con todos los atributos para construir la clave de cifrado (PTK).
2. El cliente envía al punto de acceso un mensaje CNonce, incluyendo autenticación (MAC) y un código de integridad.
3. El punto de acceso envía una clave de cifrado temporal para descifrar el tráfico (GTK) y un número de secuencia junto a otro MAC.
4. El cliente envía la confirmación al punto de acceso.

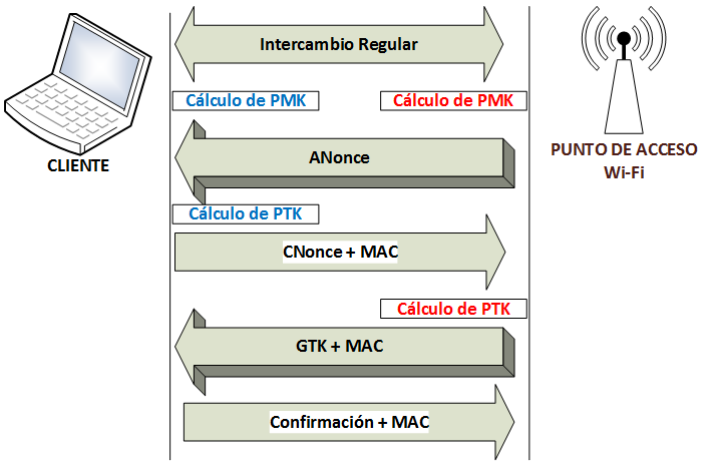

Figura 2.3: Handshake del protocolo WPA2

TOR Según el sitio web oficial [11], se define el proyecto como:

> *"Un software libre y red de comunicación abierta para defenderse contra el análisis de tráfico, una forma de vigilancia que atenta contra la libertad personal, la privacidad, confidencialidad en los negocios y relaciones."*

Tor protege las comunicaciones utilizando una red distribuida de repetidores voluntarios de todo el mundo. Evita que alguien que pueda ver la conexión a Internet, determine qué sitios

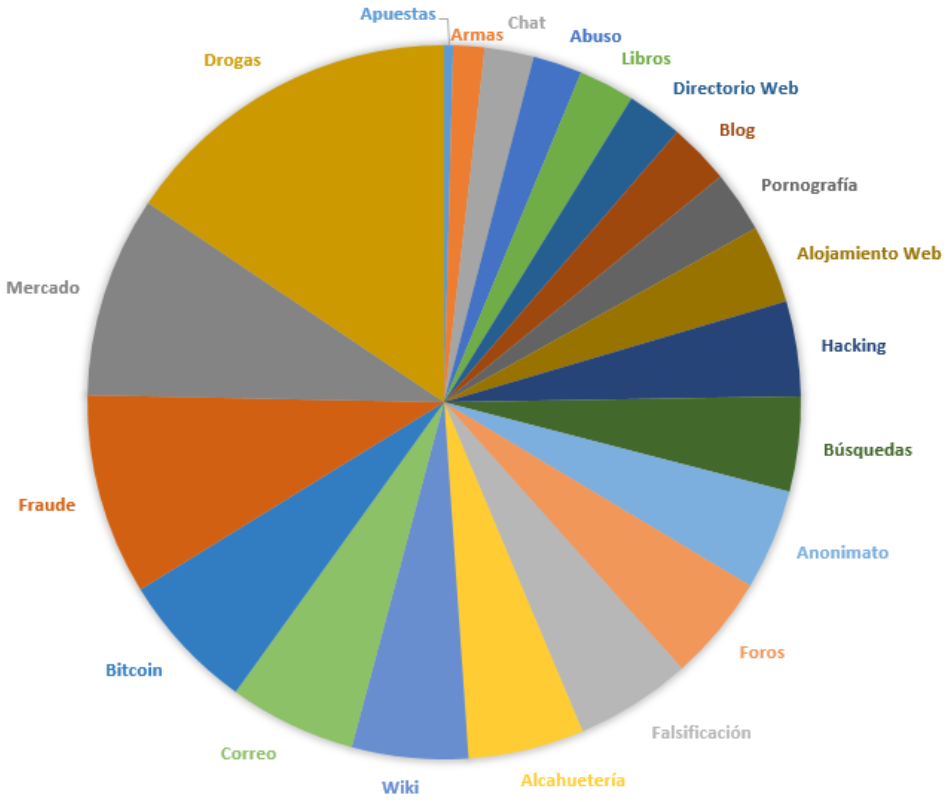

Figura 2.4: Usos reales de Tor

web se visitan. También previene que los sitios web que se visiten determinen la dirección IP de quien se conecta a ellos.

Es interesante comparar los usos promocionados del proyecto como: familia y amigos, negocios, activismo político, periodismo, fuerza militar y policial; con los que ocurren efectivamente en la *dark web*[3] (ver Figura 2.4).

Tor reduce los riesgos de análisis del tráfico de la red, distribuyendo las transacciones en diferentes lugares de Internet. En lugar de tomar una ruta directa del origen al destino, los datos de los paquetes de Tor toman rutas aleatorias a través de varios relevos ocultando de donde vienen los datos y hacia adonde van.

Como se puede apreciar en la Figura 2.5, se crea una ruta de red privada, construyendo de forma incremental un circuito de conexiones cifradas a través de los relevos de la red. El circuito se extiende un tramo a la vez, cada relevo sólo conoce que relevo le transmitió los datos y a qué relevo le debe transmitir. Ningún relevo conoce la ruta completa del paquete de datos. El cliente negocia un conjunto de claves de cifrado diferente para cada tramo a lo largo del circuito para asegurar que ningún tramo pueda rastrear estas conexiones.

Una vez establecido el circuito, se pueden intercambiar datos e implementar varios tipos de aplicaciones de software. Dado que cada relevo no ve más de un tramo, ningún

[3]Parte de la *deep web*, son redes públicas y privadas que requieren software o autorización especial para acceder usualmente a contenidos ilícitos.

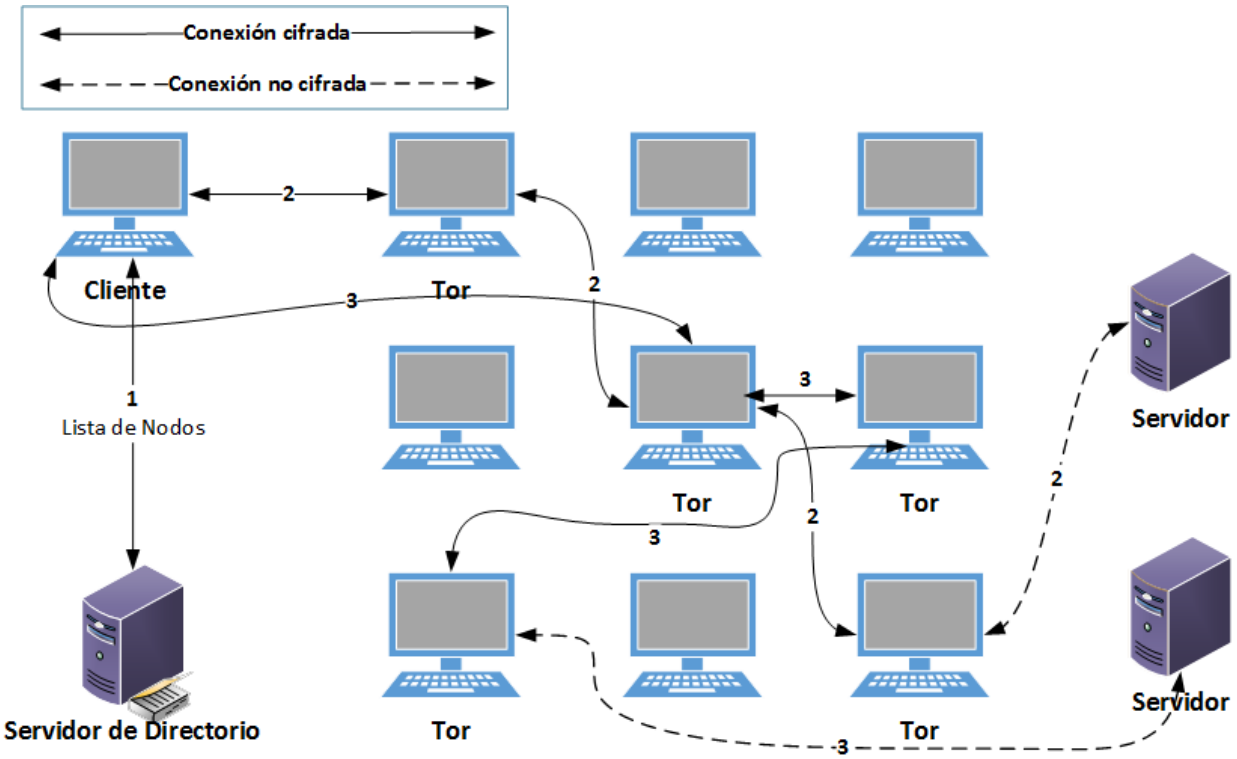

Figura 2.5: Esquema de una conexión en Tor

espía, analista forense o incluso un relevo comprometido pueden analizar el tráfico para relacionar el origen y el destino de la conexión. Tor sólo funciona con el protocolo TCP y puede ser usado por cualquier aplicación con soporte de SOCKS.

Por eficiencia, se utiliza el mismo circuito para las conexiones que se producen dentro de un período de diez minutos. Luego se asigna un nuevo circuito para evitar que un analista forense vincule comportamientos pasados con nuevas acciones.

Tor no soluciona todos los problemas de anonimato, sólo se focaliza en el transporte de los datos. Se puede utilizar por ejemplo Tor Browser mientras se navega para ocultar información sobre la configuración de la computadora.

2.2 Esteganografía

Del griego *steganos* (cubierto u oculto) y *graphos* (escritura), evita que alguien no autorizado detecte la presencia de datos. Hoy en día la esteganografía es uno de los métodos más populares para ocultar la información, dado que la trasmisión de datos en sistemas de comunicación pública no es segura.

En la Figura 2.6 se muestra el esquema general de un sistema esteganográfico. El *mensaje secreto* se embebe en el *archivo portador*, generando un *archivo estego* que oculta la información secreta y está expuesto en un canal inseguro. Luego el *extractor* aplica un proceso inverso y recupera idealmente el *mensaje secreto* original.

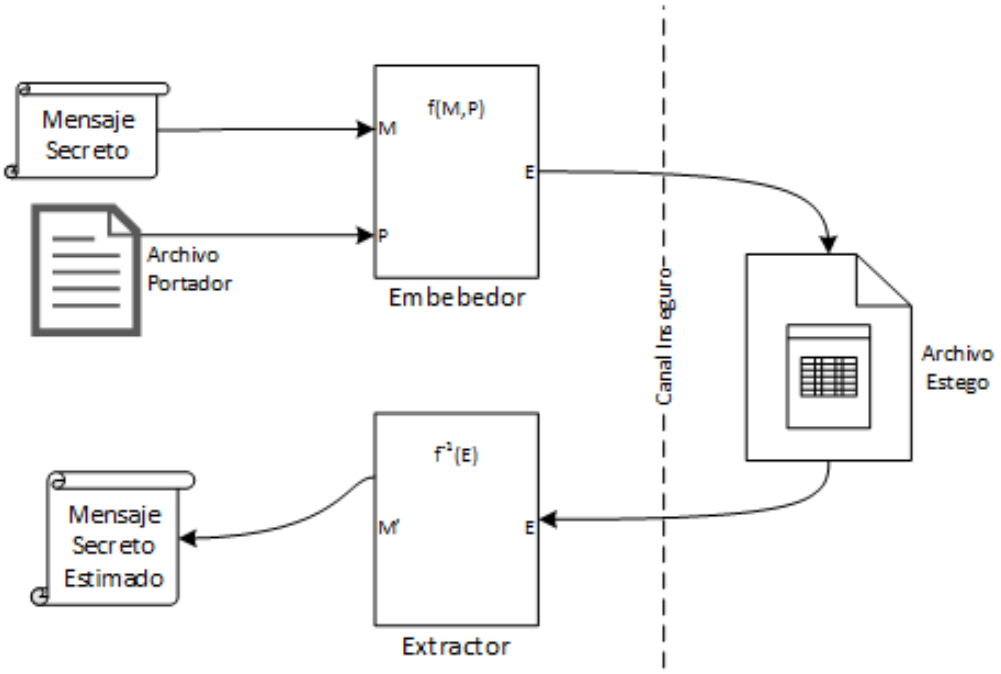

Figura 2.6: Esquema general de un sistema esteganográfico

Los medios digitales usualmente incluyen datos redundantes o innecesarios que pueden ser manipulados para ocultar datos. Los datos o archivos secretos pueden ser ocultados dentro de otros archivos de texto, imagen, audio, video o incluso protocolos de red [3] [17].

2.2.1 Texto

Se oculta información dentro de los archivos de texto. Los datos secretos se pueden ocultar por ejemplo detrás de cada n-ésima letra de cada palabra del mensaje de texto. Se utilizan varios métodos para codificar datos secretos, basados en:

- *Formato:* i.e. uso de letras mayúsculas o minúsculas.
- *Aleatoriedad y estadística:* i.e. número de tabulaciones o espacios.
- *Lingüística:* i.e. transformaciones léxicas, sintácticas o semánticas.

2.2.2 Audio

Un archivo de audio puede ser modificado para que pueda incluir datos ocultos. Esta modificación debe ser hecha de tal manera que la información secreta este segura sin alterar la señal original. Se pueden utilizar formatos de audio como: WAV, AIFF, AU o MP3.

Cuando se oculta la información en un archivo de audio, se crea un archivo de audio denominado *estego* y se envía al receptor; el cual puede recuperar la información usando diferentes algoritmos que se detallan a continuación.

Codificación de fase Los bits son codificados como un cambio de fase en el espectro de fase de una señal digital siguiendo estos pasos:

1. Se divide la codificación del sonido original en segmentos mas pequeños del mismo tamaño que el mensaje a ser codificado.
2. Se aplican trasformadas de Fourier (DFT) a cada segmento y se crea una matriz de las fases y sus respectivas magnitudes.
3. Se calculan las diferencias entre las fases de segmentos adyacentes.
4. Utilizando la nueva matriz de fases y la matriz original de magnitudes, la señal del sonido es reconstruida aplicando la función inversa de DFT y luego concatenando los segmentos de sonido.

Finalmente, si el receptor desea extraer la información secreta, debe conocer la longitud del segmento; luego aplica DFT para obtener las fases y extraer la información.

Codificación del bit menos significativo (LSB) Considerando la representación de un byte, se reemplaza el bit menos significativo para ocultar datos. Alterándolo, se cambia en la menor medida posible el valor total del número representado. Entonces cada 8 bytes se puede ocultar 1 byte. Aquí la tasa de transmisión ideal será de 1 kbps por cada 1 KHz. Luego, si el receptor tiene que extraer los datos secretos de un archivo de audio codificado con LSB, necesita acceder a la secuencia de índices utilizados en el proceso.

Ocultamiento en el eco Se utiliza el eco de una señal discreta y se agrega sonido extra. El eco tiene tres parámetros que se varían en la señal original para ocultar información: amplitud, velocidad de desintegración y tiempo de retardo. Estas variaciones se aplican siempre por debajo del umbral del oído humano. Lo notable es que a diferencia de los otros métodos se puede mejorar el audio original.

Dispersión del espectro Los datos secretos se dispersan en el espectro de la frecuencia al azar, tanto como sea posible. Los datos son modulados y como resultado la señal resultante ocupa un ancho de banda mayor con respecto al realmente requerido. La principal desventaja de este método es que introduce ruido en el archivo de audio original.

2.2.3 Imagen

Se utilizan las intensidades de los píxeles para ocultar datos. En la esteganografía digital, las imágenes se utilizan mucho porque hay un número importante de bits presentes.

Dominio espacial Los datos secretos están embebidos en la intensidad de los píxeles. Esto significa que algunos valores de los píxeles de la imagen se cambian durante el ocultamiento de datos. Esta técnica se divide en varias categorías, las principales son:

- *Bit menos significativo (LSB).* Se reemplazan los bits menos significativos de los píxeles de la imagen con los bits de datos secretos. La imagen obtenida luego del reemplazo es casi similar a la imagen original, porque los cambios en los píxeles de la imagen no introducen diferencias notorias.
- *Diferenciación del valor del pixel (PVD).* Se seleccionan dos píxeles consecutivos para embeber los datos. El payload se determina chequeando la diferencia entre dos píxeles consecutivos y sirve como base para identificar si los dos píxeles pertenecen a una región del borde o a una región lisa.
- *Segmentación de la complejidad en el plano de bits (BPCS).* Se segmenta la imagen mediante la medición de su complejidad. Se utiliza la complejidad para determinar el bloque ruidoso. Los bloques ruidosos del plano de bits se reemplazan por los patrones binarios asignados de los datos secretos.
- *Embebido de datos basado en los bordes (EBE).*
- *Embebido de píxeles aleatorios (RPE).*
- *Mapeo de píxeles a datos secretos.*

Distorsión El mensaje secreto es almacenado distorsionando la señal. Una secuencia de modificaciones es aplicada a la imagen original por el codificador. El decodificador calcula las diferencias entre la imagen original y la distorsionada para recuperar el mensaje secreto.

El mensaje es codificado seleccionando bits pseudo-aleatorios. Si el valor de los píxeles es idéntico se codificó un "0", caso contrario un "1".

Dominio de Transformaciones Es una manera más compleja de esconder datos en una imagen, se utilizan varios algoritmos y transformaciones. La mayoría de los sistemas esteganográficos actuales operan de esta forma. Tienen como ventaja sobre las técnicas del dominio espacial, que la información se esconde en áreas de la imagen que son menos expuestas a compresión, recorte y procesamiento de la imagen. Algunas de las técnicas no dependen del formato de la imagen y pueden generar conversiones de formato con y sin pérdida. El detalle de cada una de las transformaciones excede el objetivo del trabajo, pero las principales son:

- Transformada de Fourier Discreta (DFT)
- Transformada de Coseno Discreta (DCT)
- Transformada Wavelet Discreta (DWT)
- Método reversible o sin pérdida (DCT)
- Embebido de bits en coeficientes

Enmascaramiento y Filtrado Se oculta información marcando una imagen, de la misma forma que las marcas de agua en el papel. Se embebe la información secreta en áreas significativas de la imagen. Las técnicas de marcas de agua se pueden aplicar sin riesgo

de destrucción de la imagen; debido a que existe una menor compresión con pérdida, ya que están más integradas en la imagen.

2.2.4 Video

Se ocultan datos en formatos de vídeo digital como: H.264, MP4, MPEG y AVI. Un archivo de video *stego* es creado para ocultar los datos secretos. Generalmente se utiliza la Transformada Discreta del Coseno (DCT), para alterar los valores y ocultar datos en cada una de las imágenes en el vídeo. Esta modificación resulta imperceptible para el ojo humano. A continuación se describen los principales métodos empleados.

Partición rectangular no uniforme. Se aplica sobre formatos de video sin comprimir. Se puede ocultar un video secreto dentro de otro video principal de casi el mismo tamaño. Se toma cada cuadro o *frame* de ambos videos y se aplica esteganografía de imágenes.

Video comprimido. Las operaciones para ocultar datos son ejecutadas enteramente sobre el formato de compresión que se explicará de manera muy breve para dar el contexto necesario. El formato de compresión es básicamente una secuencia de tres tipos de cuadros:

- *I-frame*: un cuadro de imagen completamente especificado.
- *P-frame*: usa las diferencias del cuadro anterior.
- *B-frame*: usa las diferencias del cuadro anterior y siguiente.

A su vez cada uno de estos cuadros son segmentados en bloques o *macroblocks*, que se clasifican de la misma manera. Los datos secretos son embebidos, tanto en los macroblocks de I-frames con máximo cambio de escena, como en los P-frames y B-frames con máxima magnitud de vector de movimiento. Lo más importante es que el proceso no degrade la calidad del video y que los cambios introducidos sean imperceptibles a la visión humana. Los detalles del algoritmo TPVD empleado para tal fin pueden encontrarse en [4].

2.2.5 Protocolos de Red

Se oculta la información mediante la adopción de protocolos de red como: TCP, UDP, ICMP o IP como objeto portador. En el modelo de capas de red OSI existen canales encubiertos en los que se puede utilizar la esteganografía.

A través de los *headers* de los protocolos se pueden enviar datos secretos entre dos partes que acuerden un protocolo encubierto. Usando esta estrategia es posible embeber datos por ejemplo en las conexiones iniciales, conexiones ya establecidas u otros pasos intermedios.

2.3 Empaquetadores de Programas

Un empaquetador de programas es un software que comprime y/o cifra un segundo software y lo empaqueta junto con su respectivo extractor. Por lo general son utilizados por atacantes para que el software malicioso no sea sometido a ingeniería inversa[4] o detectado por algún anti-virus o herramienta forense.

También suelen incorporar protección contra debugging, por ejemplo si otro programa intenta trazar al proceso malicioso en ejecución, este último se cierra automáticamente. Si el proceso no está siendo trazado, se crea otro proceso para que se tracen mutuamente; de esta manera se logra que ningún otro programa pueda trazarlo, ya que en varios sistemas operativos sólo puede haber uno al mismo tiempo.

Los empaquetadores que requieren una contraseña para ejecutarse son tan seguros como su cifrado o contraseña. Aquellos que no requieren una contraseña son vulnerables a un análisis estático de código[5].

Sin embargo son vulnerables en tiempo de ejecución, una herramienta como Burndump espera que el proceso sea descifrado y luego copia el programa desprotegido a otro lugar para su posterior análisis.

Otro tipo de empaquetadores encapsulan múltiples archivos en un solo ejecutable. La estrategia es mezclar archivos regulares con otros maliciosos, dificultando su detección por parte de los anti-virus.

2.4 Otras Formas de Ocultamiento

Los datos pueden ser ocultados en espacios sin asignar o inaccesibles por las herramientas forenses actuales, como por ejemplo:

- Espacio slack de los sistemas de archivos FAT o NTFS de Windows
- Bloques defectuosos del disco.
- Espacio de directorios.
- Espacio reservado para los i-nodos en sistemas de archivos Unix.
- Páginas no asignadas de archivos Microsoft Office.
- Host Protected Area (HPA) y Device Configuration Overlay (DCO) de los discos ATA.

[4]Proceso para obtener el código fuente o diseño de un programa a partir de su archivo ejecutable.
[5]Proceso para analizar el código fuente del software.

Capítulo 3

Eliminación de Datos

El objetivo de estas técnicas es lograr la eliminación de la evidencia digital. Al perito forense informático se le dificulta mucho recuperar datos que fueron destruidos.

3.1 Sanitización

Se define como *sanitización* al proceso de borrar total o parcialmente los datos de un dispositivo de almacenamiento digital, de tal manera que no se puedan recuperar. Los motivos para hacerlo pueden ser tan variados como privacidad, seguridad o eliminar algún tipo evidencia.

3.1.1 Tipos

Lógica. También llamada *clearing*. Los datos no se pueden recuperar usando los comandos integrados de sanitización de las interfaces ATA o SCSI del hardware estándar. El usuario puede sobrescribir un archivo o el disco entero.

Digital. También llamada *wiping*. No es posible recuperar los datos utilizando cualquier medio digital, incluyendo comandos del disco sin documentar, o subversiones del controlador o firmware. En los discos duros, sobrescribir y luego borrar el archivo por software es suficiente para lograr la sanitización lógica y digital; salvo los bloques dañados del disco que son retirados del uso. Esto se logra utilizando las operaciones primitivas del sistema operativo.

Analógica. También llamada *purging* o *degaussing*. Se degrada la señal analógica que codifica los bits que representan los datos, tal que recuperar la señal es imposible aún con el equipo de sensores más avanzados. El proceso es muy costoso y suele ser utilizado por organismos como la NSA con fines de seguridad nacional. Sólo se aplica a los discos magnéticos.

Criptográfica. La criptografía provee una de las más simples y posiblemente mejor manera de sanitizar. Si los datos se cifran cuando se escriben en el disco y se descifran antes de leerse,

entonces un disco entero puede ser sanitizado simplemente desechando la clave criptográfica. Esto es mucho mas rápido que los costosos procesos de sobrescritura por software que pueden demandar horas de sanitización; tiempo que aumenta mientras más grande es el disco.

Cuando se ejecuta un comando de sanitización en un disco cifrado, con la apropiada autenticación primero, el disco genera una nueva clave de cifrado. Sin la clave anterior, los datos viejos se convierten en irrecuperables.

La eficacia reside en la seguridad del algoritmo de cifrado utilizado y de la habilidad del diseñador para eliminar la clave criptográfica, lo cual en la práctica puede ser difícil de implementar. Por otro lado el diseño debe ser lo suficientemente robusto como para evitar los ataques para extraer la clave, lo cual podría vulnerar la criptografía.

En la sección 2.1 se trata con mas detalle esta técnica.

3.1.2 Taxonomía de los Datos

Para identificar mejor los datos de interés forense, en [8] se propone una clasificación de los datos que pueden estar presentes en un disco.

Nivel 0 - Archivos regulares

- Información contenida dentro del sistema de archivos.
- Nombres, atributos y contenidos de los archivos.
- No se requiere ninguna herramienta especial para leer este tipo de datos.

Nivel 1 - Archivos temporales

- Archivos generados por una impresión.
- Archivos de la cache del navegador web.
- Archivos auxiliares de aplicaciones.
- El usuario promedio supone que estos archivos son eliminados automáticamente, o peor aún, no sabe que existen.
- No se requiere ninguna herramienta especial para leer este tipo de datos, pero se necesita un mínimo conocimiento técnico para buscarlos.

Nivel 2 - Archivos borrados

- Cuando se borra un archivo del sistema de archivos, la mayoría de los sistemas operativos no sobrescribe los correspondientes bloques en el disco. Sólo se elimina la referencia al archivo, del directorio que lo contiene.
- Los bloques del archivo borrado se colocan en la lista de bloques libres.
- Existen ciertas herramientas tradicionales como Norton Utilities (disponible para Windows, Linux y Mac OS X) que permiten recuperar esos archivos.

Nivel 3 - Bloques de datos retenidos

- Datos que pueden ser recuperados de un disco, pero no es obvio de que pertenezcan a un archivo.
- Información en un espacio de un disco fragmentado.
- Espacio swap del disco usado para la memoria virtual.
- Datos del Nivel 2 que fueron parcialmente sobrescritos, de tal manera que el archivo completo no se puede recuperar.
- Datos de un disco que fue formateado con el comando `format` de Windows o `newfs` de Linux.
- Existe la creencia popular que el formateo sobrescribe el disco entero.
- Hay datos que pueden ser recuperados con herramientas forenses.

Nivel 4 - Datos ocultos del fabricante

- Bloques de datos donde reside al controlador del disco.
- Bloques utilizados para la administración de los bloques dañados del disco.
- Host Protected Area (HPA) de los discos.
- Solo se pueden acceder usando comandos específicos del fabricante.

Nivel 5 - Datos sobrescritos

- Información que puede ser recuperada de un disco, aun después que fue sobrescrito.
- Esto ocurre principalmente en los antiguos discos magnéticos (HDD), que no han sido correctamente sanitizados. Se puede inspeccionar con avanzadas técnicas el residuo de la señal analógica de los datos originales.

3.1.3 Sanitización por Software

Lamentablemente los sistemas operativos en general tienen un diseño limitado para dar soporte de sanitización. Ello se debe mayormente a que pueden sufrir una degradación del desempeño, si cada vez que se eliminan datos se hace una sobrescritura.

Usar un software de sanitización, tiene ciertos riesgos si no está correctamente implementado. Por ejemplo, si el programa lee y escribe en el disco sin hacerlo a través del sistema operativo, existe el riesgo de corromper el disco. Si por el contrario, lo hace a través del sistema operativo, existe el riesgo de que no coincidan las funciones primitivas que ofrece el sistema operativo y la manera que esas abstracciones fueron implementadas en el firmware del disco. Otro riesgo es que los programas podrían no brindar la funcionalidad de sanitización de la manera que lo publican.

Archivos existentes (Niveles 0 y 1) Programas como Norton Disk Doctor, PGP Disk y el comando `shred` de Linux borran archivos individualmente de forma segura.

Bloques libres del disco (Niveles 2 y 3) El comando `chiper.exe` de Windows crea un nuevo archivo y escribe en el mismo hasta que se ocupa todo el espacio libre del disco. Esto puede impactar en el uso normal del disco. Otro problema que tiene es que podría no sobrescribir archivos que son lo suficientemente pequeños como para almacenarse en el sistema de archivos.

Datos residuales (Nivel 3) Los sistemas operativos típicamente asignan varios bloques de espacio libre para un archivo, aún cuando sólo se escriban unos pocos bytes en el primer bloque. En los bloques restantes pueden existir datos residuales de archivos anteriores que han sido borrados hace mucho tiempo. A estos bloques sin usar se los denomina *slack*.

Disco entero (Niveles 1, 2 y 3) Algunos programas simplemente sobrescriben los contenidos del disco entero. Típicamente son ejecutados desde un CD o USB booteable y son tipificados por Darik's Boot and Nuke (DBAN).

En la práctica, muchos usuarios particulares y empresas utilizan software basado en técnicas de sobrescritura para destruir los datos almacenados en discos HDD y funcionan razonablemente bien. Pero como se demuestra en [7], debido a que los dispositivos SSD y USB tienen otra arquitectura, las técnicas tradicionales de sanitización no son efectivas en todos los casos. Las conclusiones principales del estudio son:

- Los comandos integrados de los discos (firmware) suelen ser efectivos para sanitizar el disco entero, pero los fabricantes a veces los implementan incorrectamente.
- Sobrescribir dos veces el espacio entero de direcciones visibles de un SSD es generalmente suficiente para sanitizar el disco, pero no siempre. Esto se logra a través de las operaciones que brinda el sistema operativo.
- Ninguna de las técnicas para sanitización individual de un archivo son efectivas en un medio SSD.

En la Tabla 3.1 se comparan los diferentes tipos de sanitización aplicadas a distintos medios de almacenamiento (* indica la mayoría de los casos).

3.2 Destrucción Física

En [12] se mencionan técnicas más extremas que apuntan a la destrucción física del medio de almacenamiento. El beneficio es que se asegura que los datos son imposibles de recuperar usando las técnicas de laboratorios disponibles en la actualidad.

Tabla 3.1: Sanitización en diferentes medios de almacenamiento

Tipo de Sanitización	**HDD**		**SSD**		**USB**	
	Disco	Archivo	Disco	Archivo	Disco	Archivo
Lógica (software)	SI	SI	SI	NO	NO	NO
Digital (software)	SI	SI	SI*	NO	SI*	NO
Criptográfica (software/hardware)	SI	NO	SI	NO	SI	NO
Analógica (física)	SI	NO	NO	NO	NO	NO

- *Incineración*: se quema hasta reducir a cenizas.
- *Cortado*: se corta o razga en partículas minúsculas.
- *Desintegración*: se separan las partes que componen un disco.
- *Desmagnetización o degaussing*: se degrada la señal analógica de los discos magnéticos.
- *Pulverizado*: se muele hasta reducirlo a polvo.

Sin embargo doblar, cortar u otros procedimientos de emergencia como usar un arma de fuego para perforar el medio de almacenamiento, solo lo daña parcialmente; dejando algunas porciones accesibles para ser analizadas usando técnicas avanzadas.

Capítulo 4

Anticoncepción de Datos

A diferencia de la sobrescritura y borrado de datos, las técnicas de anticoncepción directamente previenen la creación de datos. Datos que nunca existieron obviamente no pueden ser recuperados utilizando ninguna herramienta forense.

4.1 Syscall Proxying

Con esta técnica se intermedian las llamadas al sistema de un proceso a un servidor remoto, simulando una ejecución remota [10].

Durante un ataque en una organización el atacante intenta escalar privilegios. Es decir que luego de un ataque exitoso, gana acceso a una computadora intermedia o una aplicación en el sistema. El acceso a esta computadora intermedia le permite realizar ataques más eficaces contra el sistema, tomando ventaja de la confianza y una posición más privilegiada en la red interna. A este tipo de práctica se le llama *pivoting*.

Pivotar sobre una computadora comprometida puede ser una tarea costosa, requiriendo instalar herramientas o atacar a una plataforma diferente. Esto puede incluir instalar librerías y paquetes requeridos; o a veces hasta un compilador del lenguaje C en el siguiente sistema que se desea atacar.

Syscall Proxying es una técnica para simplificar la fase de escalación de privilegios. Se provee una interfaz en el sistema operativo destino, que permite que el código y las herramientas de ataque estén en control de los recursos remotos (ver Figura 4.1).

4.2 Compiladores/Emsambladores en Memoria

En este escenario el atacante envía fragmentos de código remoto al compilador o ensamblador residente en la memoria del dispositivo comprometido. Esta técnica permite que las herramientas sean compiladas para la plataforma comprometida completamente en memoria, dentro de un proceso alterado (hijacking). Nuevamente, el objeto principal es no dejar rastros en el disco local.

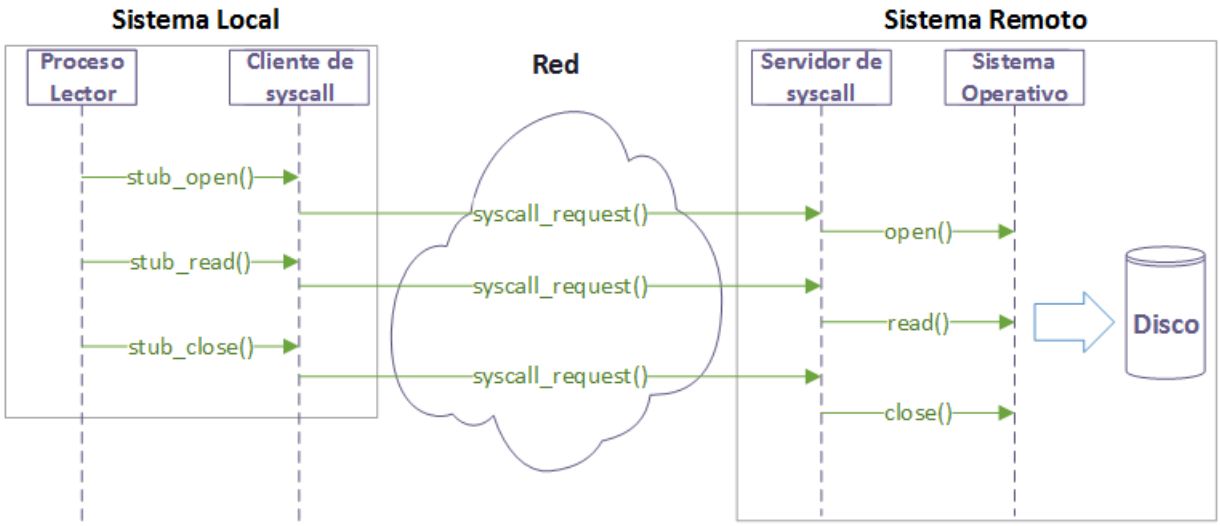

Figura 4.1: Diagrama de secuencia de Syscall Proxying

4.3 Inyección de Código en Memoria

En esta técnica se carga una librería remota en memoria; es decir que se inyecta código en memoria sin tenerlo en el disco.

La forma tradicional de hacerlo es utilizando exploits del tipo buffer overflow. Esto ocurre cuando un programa escribe datos más allá de los límites asignados, sobrescribiendo bloques de memoria adyacentes. De esta manera se logra que código malicioso sea ejecutado dentro de otro proceso que ya está en ejecución.

4.4 Manipulación del Kernel

El *kernel* es el componente central del sistema operativo. Este método le permite a un atacante utilizar drivers para modificar objetos asociados al kernel. Microsoft y otros vendedores de sistemas operativos típicamente sólo usan dos de los cuatro niveles de privilegios disponibles en una arquitectura Intel. No existe separación entre el kernel y los drivers, con lo cual el driver tiene acceso a la memoria del kernel permitiéndole ejecutar con altos privilegios varias actividades anti-forenses.

4.5 Live Distros

La mayoría de la información forense es dejada en el sistema de archivos de la computadora. El software portable es capaz de ejecutarse sin la necesidad de instalar archivos en el sistema de archivos.

El término *live* viene del hecho que son distribuciones capaces de ejecutarse en vivo, diferenciándose de los típicos sistemas operativos que primero necesitan instalar varios

paquetes de software antes de poder ser utilizados.

Los *live distros* son sistemas operativos almacenados en un medio extraíble (como CD, DVD o memoria USB) que se ejecuta en el arranque sin instalarse en el disco. Típicamente todos los archivos del sistema residen en la memoria. Sin embargo, un *live USB* se diferencia de un *live CD* en que tiene la capacidad de persisitir configuraciones del sistema operativo e instalar de forma permanente paquetes de software en el dispositivo USB.

Los *live distros* que pueden resultar de más utilidad son aquellos que brindan un arsenal de herramientas forenses y otras para realizar test de penetración como por ejemplo BackTrack o Kali.

4.6 Máquinas Virtuales

Una *máquina virtual* es un software que emula a una computadora y puede ejecutar programas como si fuera una real.

Una técnica anti-forense es instalar un sistema operativo en una máquina virtual, donde la mayoría de la información de interés forense queda en el archivo único donde se aloja la misma y que posteriormente puede ser más fácilmente eliminado.

Capítulo 5

Ofuscación

El propósito de las técnicas de ofuscación es confundir, desorientar y desviar la investigación forense.

5.1 Sobrescritura de Metadatos

Alterando los metadatos de los archivos se puede distorsionar las propiedades de los archivos de interés forense. A continuación se muestran algunos ejemplos.

5.1.1 Atributos de Archivos

Un perito forense informático podría determinar qué archivos accedió el atacante examinando la fecha de acceso de cada archivo del sistema. Se puede construir una línea de tiempo de todas las acciones del atacante ordenando todas las fechas y horas de acceso en orden cronológico.

Aunque el atacante podría directamente sobrescribir el disco, esto podría llamar la atención del perito forense informático. Entonces es más inteligente sobrescribir las fechas de acceso para distorsionar la construcción de la línea de tiempo. Esto se puede lograr utilizando alguna herramienta anti-forense como Timestomp (Windows) o The Defiler's Toolkit (Linux).

5.1.2 Imágenes JPEG

JPEG es un formato de compresión de imágenes con pérdida, es decir que puede resultar en la distorsión de la imagen original. Los software de edición de imágenes permiten manipularlas sin dejar rastros visuales, por lo cual el análisis forense toma suma importancia. Decidiendo si una imagen fue previamente comprimida, los peritos forenses informáticos pueden hacer un juicio preliminar sobre su autenticidad.

El proceso de compresión JPEG se divide básicamente en estas etapas:

1. Conversión del modo de color de RGB a YUV.
2. Submuestreo de crominancia.
3. Transformación DCT.
4. Cuantificación.

5. Codificación Huffman.

La compresión JPEG comienza con la transformación del sistema de color y la reducción de la información del color; ya que el ojo humano capta mejor los cambios de brillo que de color. Seguidamente, se segmenta la imagen digital en bloques de 8x8 pixeles y luego se aplica DCT-2 para transformar cada bloque en 64 coeficientes DCT. En la etapa de cuantificación, cada valor de coeficiente es cuantificado. Este procedimiento se convierte en la huella dacticar (*fingerprint*) de la cuantificación de coeficientes DCT y al mismo tiempo en los artefactos que pueden sufrir manipulación anti-forense.

Las técnicas forenses hacen uso de los *fingerprints* de la compresión de una imagen JPEG para verificar si fue alterada. Una técnica anti-forense típica es modificar los coeficientes DCT y borrar el efecto de bloques aplicando un blur en los límites de los bloques. De esta manera se elimina la historia de compresión de la imagen. El proceso completo puede verse en la Figura 5.1.

Actualmente, hay investigaciones en curso que analizan el ruido añadido en el proceso de borrar el efecto de bloques para detectar estas alteraciones [2].

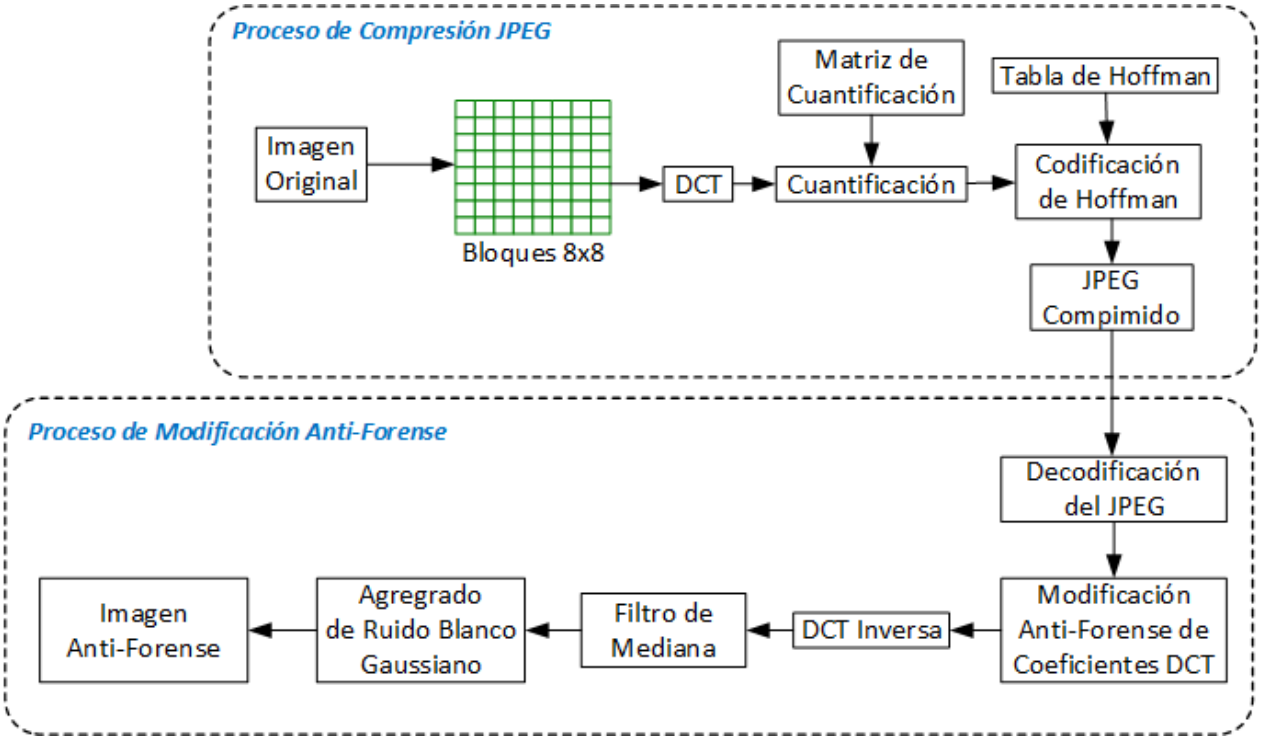

Figura 5.1: Proceso de compresión JPEG y proceso de modificación anti-forense

5.2 E-mails

Existen varias técnicas anti-forenses destinadas a evitar la detección del empleo del e-mail como medio de comunicación [5].

5.2.1 Sistema de Punto Muerto

Recientemente se identificó que los ciber-criminales usan el e-mail para comunicarse de una manera no convencional. Para evitar ser detectados por los peritos forenses informáticos, se comunican con un sistema de e-mail de punto muerto (*dead drop*). Suponiendo que A y B son dos ciber-criminales, siguen el siguiente procedimiento (ver Figura 5.2).

1. A abre la cuenta de e-mail y escribe el mensaje requerido.
2. A no envía el e-mail, lo guarda en una carpeta borrador.
3. A cierra la sesión de la cuenta.
4. B abre la misma cuenta de e-mail, pero desde otra locación.
5. B lee el contenido de la carpeta borrador.
6. B elimina el documento de la carpeta borrador.

Claramente es un método de ocultamiento de evidencia (guardando en la carpeta borrador) y de destrucción de la evidencia (borrando el documento).

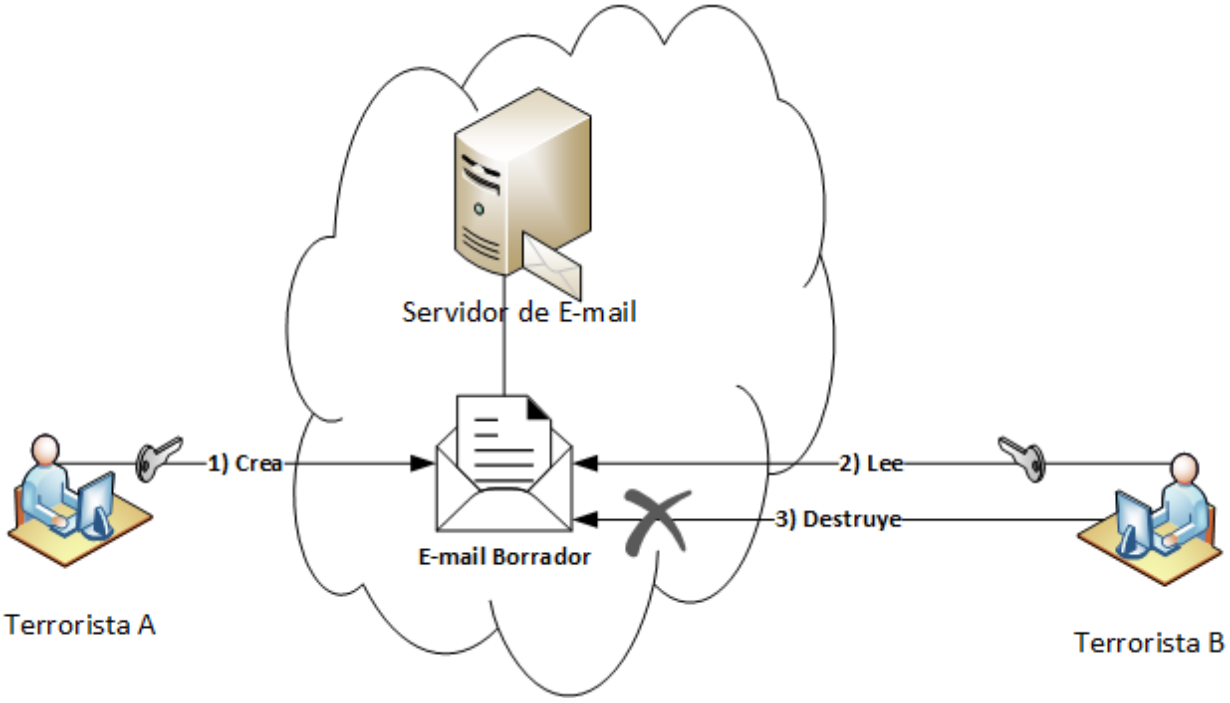

Figura 5.2: Sistema de e-mail dead drop

5.2.2 Spam combinado con Esteganografía

Otra arma de los ciber-criminales es el correo basura. Utilizando técnicas de esteganografía, se crea un mensaje oculto en un e-mail de spam y se lo envía a miles de usuarios, incluyendo a otros ciber-criminales. Los que no son terroristas, no comprenden el e-mail y probablemente lo borren. Pero los terroristas filtran el e-mail deseado y leen el mensaje oculto. De esta

forma se dificulta aun mas la investigación porque los terroristas se camuflan entre todos los receptores (ver Figura 5.3).

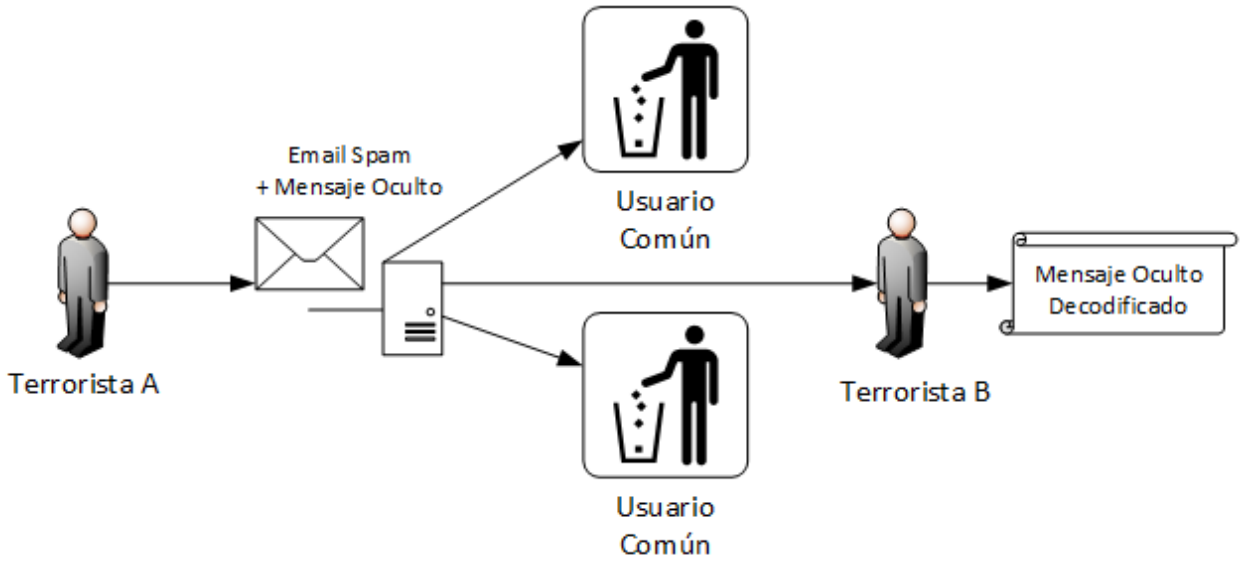

Figura 5.3: Spam combinado con esteganografía

5.2.3 Falsificación de Encabezados

Existen simples técnicas explotadas por los que envían e-mails no deseados (*spam*), agregando falsos encabezados (*headers*) al e-mail o alterando encabezados existentes introduciendo información falsa para confundir el verdadero origen. Por ejemplo los delincuentes informáticos pueden ocultar su identidad falsificando la dirección de origen del e-mail.

Esta práctica se conoce como *e-mail spoofing*. Generalmente consiste en colocar un falso emisor en los encabezados *From* y *Reply-to*. De esta manera el usuario final ve al e-mail como si hubiera sido enviado por la dirección que figura en esos encabezados. Cuando responde el e-mail ninguno de ellos resulta auténtico generando respuestas automáticas con mensajes rebotados. En la Figura 5.4 se muestra una captura de pantalla donde se utiliza SquirrelMail para falsificar los encabezados del e-mail.

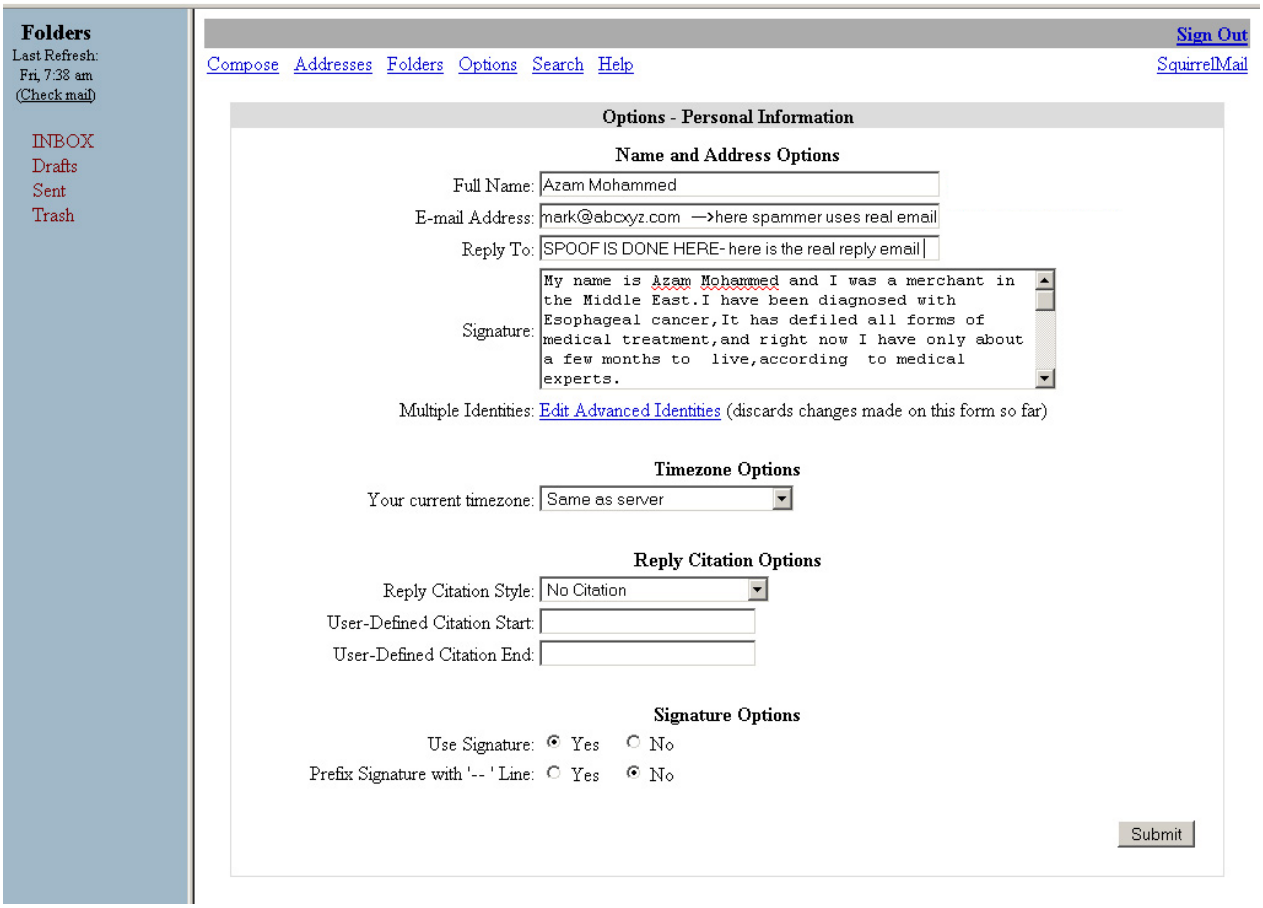

Figura 5.4: Falsificación de encabezados utilizando SquirrelMail

Capítulo 6

Ataques al Software Forense

Entre las nuevas tendencias anti-forenses se destacan los ataques contra las herramientas forenses. Estos métodos se han beneficiado principalmente de:

- Metodologías forenses bien documentadas.
- Difusión de las vulnerabilidades del software forense.
- Fuerte dependencia de los peritos forenses informáticos por el software forense.

Por otro lado, estos ataques permiten:

- Ejecutar código en el dispositivo desde el cual se ejecuta el software forense.
- Borrar la evidencia recolectada.
- Hacer que el software forense deje de funcionar.
- Filtrar información confidencial sobre el perito forense informático o la investigación.
- Implicar al perito forense informático.

En [16] se mencionan varias técnicas que atacan al software forense y se describen a continuación.

6.1 Fallas en la Validación de Datos

Como cualquier otro software, las herramientas forenses que no validan correctamente los datos de entrada pueden ser subvertidas a través de un ataque de tipo buffer overflow. Sobre todo las herramientas forenses usadas para el análisis del tráfico de red, están potencialmente expuestas a una cantidad ilimitada de información. Buscando las últimas vulnerabilidades encontradas en herramientas como tcpdump, snort o Ethereal, se pueden crear exploits apropiados para vulnerar el software forense.

6.2 Denegación de Servicio

Los recursos computacionales como la memoria y el procesamiento que utiliza la herramienta forense, son determinados en función de los datos de entrada y potencialmente son susceptibles a los ataques de denegación de servicio (DoS).

Ciertas herramientas forenses que analizan los archivos de logs, ejecutan expresiones regulares que encuentran dentro de esos archivos. Entonces expresiones regulares cuidadosamente creadas, pueden hacer que esas herramientas dejen de funcionar. Como se demuestra en [18], una expresión regular de este tipo:

```
t@t.t.t.t.t.t.t.t.t.t.t.t.t.t.t%20
```

puede hacer colapsar un software que utiliza la técnica de *backtracking* cuando busca coincidencias con respecto a la expresión regular. El *backtracking* se basa sobre un autómata finito no determinístico (NFA), el cual es diseñado para validar todos los estados de entrada. En este caso el software atacado busca e-mails y cuando encuentra esa expresión consume el 99% del procesador, produciéndose una condición de DoS.

Otro tipo de ataques DoS son las *bombas de compresión*; las cuales son pequeños archivos de datos que consumen una enorme cantidad de espacio en el disco cuando son descomprimidos. Un ejemplo es el archivo **42.zip**, aún disponible en varios sitios web; el mismo es un archivo ZIP con tamaño de 42 kilobytes, conteniendo 5 niveles de archivos comprimidos anidados, con cada archivo del último nivel con tamaño de 4 gibabytes, sumarizando un total de 4 petabytes (4000 terabytes) de datos descomprimidos (ver Figura 6.1).

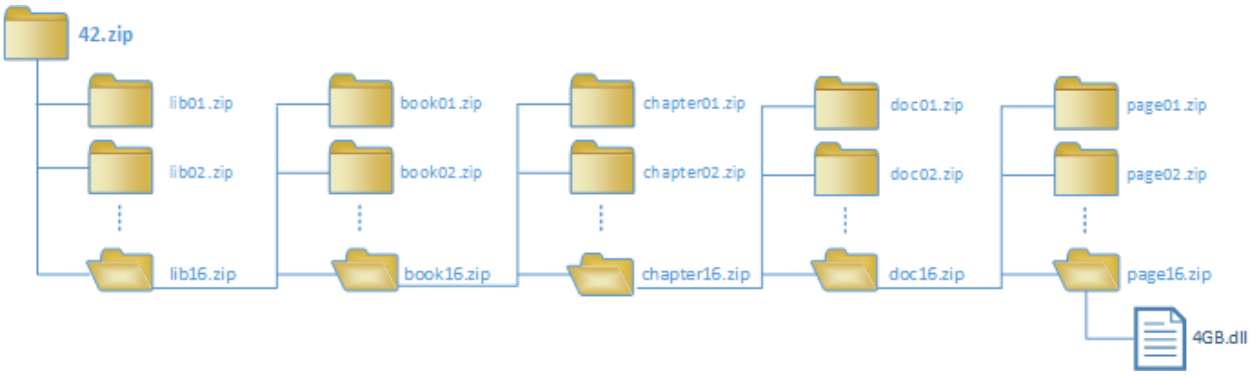

Figura 6.1: Estructura del archivo 42.zip

6.3 Heurísticas Frágiles

Las herramientas forenses necesitan determinar el tipo de archivo para hacer un procesamiento eficiente. Por ejemplo un perito forense informático podría tratar de ahorrar tiempo omitiendo los archivos ejecutables de las búsquedas. Muchas herramientas determinan el tipo de archivo, simplemente consultando la extensión del mismo o analizando los primeros bytes del archivo (el *número mágico*).

Un atacante que conoce estas heurísticas, puede enmascarar un archivo de texto haciéndolo pasar por uno ejecutable. Utilizando el proyecto Metasploit se convierte un

archivo de texto en un ejecutable, cambiando la extensión del archivo a ".exe" y escribiendo los caracteres "MZ" al principio del archivo. Entonces una herramienta forense como EnCase asumirá que el archivo es binario y no lo procesará.

6.4 Integridad del Hash

Normalmente un perito forense informático crea una imagen del disco y de la memoria del dispositivo analizado, para preservar la evidencia en su estado original. De esta manera se evita que un posterior procesamiento por parte de la herramienta forense afecte la evidencia.

Para verificar la integridad de las imágenes creadas, las herramientas forenses computan un hash. La técnica anti-forense en este caso, consiste en alterar la integridad del hash, para que cualquier evidencia digital recolectada posteriormente pueda ser anulada.

6.5 Contrarrestar el Análisis Forense

Un software anti-forense podría cambiar su comportamiento si detecta que una herramienta forense se está ejecutando.

Los contadores Self-Monitoring Analysis and Reporting Technology (SMART), integrados en la mayoría de los discos, reportan una serie de métricas que incluyen: energía utilizada, tiempo de uso y un historial de las altas temperaturas alcanzadas entre otras cosas. Por ejemplo, si un perito forense informático está creando una imagen del disco, el contador de energía utilizada registrará un gran incremento; detectándose de esta manera cierta actividad forense y cambiando el comportamiento según sea necesario.

6.6 Detectar el Monitoreo de Red

Las herramientas forenses que analizan el trafico de red, capturan los paquetes utilizando una interfaz Ethernet que está configurada en modo promiscuo. Esto quiere decir que se capturan todos los paquetes de la red local en lugar de sólo los propios. Los sistemas configurados de esta forma pueden ser detectados por la forma que responden a los paquetes IP mal formados.

Otra forma que un atacante puede detectar el monitoreo de la red, es enviando paquetes a través de la red con los encabezados alterados. Más precisamente, con una dirección IP de destino no utilizada que este en la sub-red y una dirección de origen de una red poco utilizada. En este escenario una herramienta de monitoreo inicia una petición de Domain Name Server (DNS) para resolver el nombre de la red desconocida. De esta manera, si el atacante puede monitorear el servidor de DNS, puede inferir que existe actividad forense en la red.

Capítulo 7

Ataques a Procedimientos Forenses

Otras de las nuevas tendencias anti-forenses son aquellas que atacan a las diferentes etapas de los procedimientos forenses [13]. Un juez puede admitir una evidencia científica basándose en estos factores del procedimiento:

Testeo: ¿Puede y ha sido probado?
Tasa de Error: ¿Existe una tasa de error?
Publicación: ¿Ha sido publicado y revisado por otros pares científicos?
Aceptación: ¿Es generalmente aceptado en la comunidad científica?

Este tipo de estrategias son especialmente útiles para los peritos de parte, ya que se basan en destacar los errores cometidos en los procedimientos forenses. En particular se define como *cadena de custodia*:

> *"El registro cronológico y minucioso de la manipulación adecuada de los elementos de prueba encontrados en el lugar de hecho, durante todo el proceso judicial."*

En la Tabla 7.1 se resumen los ataques que se podrían hacer en cada una de las etapas de un procedimiento forense informático.

Tabla 7.1: Ataques contra los procedimientos forenses

Etapa	**Descripción**	**Ataques**
Identificación	Método por el cual el perito identifica que hay un incidente para investigar.	Oscurecer el incidente o esconder el nexo entre el dispositivo digital y el hecho bajo investigación.
Preservación	Pasos por los cuales se preserva la integridad de la evidencia.	Interrumpir la cadena de custodia o poner en duda la integridad de la evidencia misma.
Recolección	Proceso por el cual los datos son extraídos de la evidencia.	Evitar que se complete la recolección de datos o poner en duda el software, hardware, políticas y procedimientos utilizados para recolectar la evidencia.
Examinación	Proceso que se ocupa de cómo se revisa la evidencia.	Mostrar que las herramientas son inadecuadas, incompletas o que no están certificadas.
Análisis	Etapa en la cual el perito saca las conclusiones a partir de la evidencia. Se basa en las herramientas, la habilidad del perito y el resto de la evidencia no digital que fue encontrada.	Si el caso se basa solamente en la evidencia digital, la interpretación será la más propensa a ser atacada.
Presentación	Métodos por los cuales los resultados de la investigación digital son presentados al jurado u otros investigadores.	Si la evidencia es sólida, herramientas y métodos anti-forenses serán usados para atacar la fiabilidad y el rigor de los informes o el examinador.

Parte II

Marco Legal y Ético

Capítulo 8

Marco Legal

En este capítulo y el próximo se tratan aspectos no técnicos de las actividades anti-forenses. Las técnicas estudiadas pueden estar encubriendo un delito informático. Es importante entender la dimensión de las mismas, porque la tecnología avanza más rápido que la correspondiente legislación.

Asimismo, se analizaron las leyes de diferentes países para tener una perspectiva legal integral, ya que estas actividades anti-forenses se encuentran globalizadas. En [19] se da un enfoque bastante abarcativo sobre diferentes aspectos legales.

8.1 Delitos Informáticos

A los fines del análisis de las diferentes legislaciones, se define como *delito informático* a:

> *"Cualquier actividad ilegal que encuadra en figuras tradicionales ya conocidas como: robo, hurto, fraude, falsificación, perjuicio, estafa y sabotaje; pero siempre que involucre la informática de por medio para cometer la ilegalidad."*

A continuación se clasifican los perfiles más comunes de las personas que cometen este tipo de ilícitos.

8.1.1 Perfiles de Delincuentes

Amateur: la mayoría de los delitos informáticos reportados suelen ser cometidos por profesionales que trabajan con algún medio informático ordinario, o usuarios que mientras hacen su trabajo descubren que tienen acceso a algo valioso. La mayoría no son hackers; sino que son gente común que han observado alguna debilidad en algún sistema que les permitió acceso a dinero o información valiosa.

Cracker: usualmente son personas con estudios de nivel secundario o estudiantes universitarios, que intentan acceder a recursos de algún sistema en el cual no han sido autorizados. Romper las defensas de una computadora es percibido como el máximo logro; disfrutan del solo hecho de ingresar a un sistema y ver qué cosas se pueden hacer. Una red de hackers puede trabajar de forma colaborativa, intercambiando información y secretos para

producir un efecto importante. Otros ataques son por curiosidad, ganancia personal o puro narcisismo. Por último, existen otros tantos que disfrutan causando caos, pérdidas y daños.

Cibercriminal profesional: entiende perfectamente el alcance y objetivos del cibercrimen. Muy difícilmente lo cambiarían por incendiar campos, robar un auto o realizar un asesinato. Comúnmente comienzan como profesionales de informática, hallando la perspectiva y una buena remuneración. Por ejemplo, el espionaje electrónico se ha hecho más común para infiltrarse dentro de alguna empresa para vender algún secreto.

Mientras un hacker alardea y desea recibir reconocimiento, un cibercriminal quiere recursos y obtener el máximo beneficio del sistema informático a lo largo del tiempo. Estos diferentes objetivos se refleja en la estrategia que usan. El hacker realiza un ataque rápido y sucio, en el sentido que puede dejar rastros. El cibercriminal quiere un ataque ordenado, robusto y que no sea detectado.

Terrorista/Hacktivista: usa un medio informático para causar denegación de servicio (DoS) en sitios web y servidores, por alguna razón política para atraer atención a la causa que defienden y desprestigiar al objetivo que están atacando. Otro tipo de uso es usar sitios web y listas de e-mails como una forma económica de llevar un mensaje a mucha gente.

8.1.2 Legislación Retrasada

La comunidad legal no se mueve a la velocidad de los avances tecnológicos (ni aquí ni en el primer mundo). Para que los delitos informáticos tengan un tratamiento apropiado es necesario capacitar a todos los actores que participan del proceso legal. Legislar para crear o modificar leyes es un proceso lento y siempre está varios pasos atrás con respecto a los progresos tecnológicos.

Otro problema es que un dispositivo informático puede representar varias cosas al mismo tiempo en un delito informático, ya que puede ser:

Sujeto: atacado (e.g. intento de acceso no autorizado).
Medio: usado para atacar otro sistema (e.g. suplantando un nodo de la red del sistema).
Objeto: utilizado para cometer el delito (e.g. con un troyano).

8.1.3 Dificultad para Juzgar

Aún cuando pueda haber consenso que un delito informático ha sido cometido, es difícil de juzgar por las razones que se mencionan a continuación.

Falta de entendimiento: los jueces, abogados, fiscales, policías no necesariamente tienen conocimientos tecnológicos.

Falta de evidencia física: muchos de los delitos informáticos no tienen una evidencia tangible o rastros físicos como otros delitos.

Desconocimiento de los activos: es difícil de cuantificar el valor de los datos perdidos o tiempo computacional de un sistema que deja de funcionar.

Poco impacto político: poner en prisión a un delincuente informático por un delito oscuro y de alto nivel tecnológico, puede tener menos atención de la prensa que por ejemplo meter preso a un violador.

Complejidad del caso: delitos básicos como un asesinato, robo, violación pueden ser entendidos por cualquier persona. Un caso de lavado de dinero puede ser un poco más complicado de juzgar. Pero es mucho más complejo explicar: una escalación de privilegios lograda por un buffer overflow, que luego fue usada para ejecutar código, que luego fue eliminado para no dejar rastros.

Edad del acusado: la sociedad minimiza delitos serios que fueron cometidos por adolescentes, porque los considera como propios de la inmadurez de la edad.

Publicidad negativa: la víctima prefiere no iniciar acciones legales para no generar un impacto negativo. Por ejemplo en el caso de bancos, compañías de seguro, financieras, gobierno o instituciones médicas.

Aún con las definiciones en las leyes, los jueces deben interpretar qué es una computadora. Los legisladores no pueden definir qué es una computadora porque la tecnología se usa también en otros dispositivos como robots, calculadoras, relojes, automóviles, microondas, instrumental médico, etc. Además no se puede predecir que tipo de dispositivos pueden ser inventados en la próxima década.

Otro problema que se observa es que los juzgados no pueden diferenciar el valor de un objeto de su valor para producirlo. Por ejemplo, es claro que un cuadro de arte famoso es más valioso que el lienzo utilizado para pintarlo, pero es más difícil cuantificar el valor de las horas necesarias para recolectar los datos o tiempo de procesamiento consumido para producir esos datos.

8.1.4 Dificultad para Capturar

Resulta difícil para los organismos que investigan los delitos informáticos capturar a un delincuente informático.

En primer lugar se debe a que es una actividad multinacional pero que usualmente se persigue a nivel local o nacional. No existen leyes internacionales, mas allá que los países desarrollados suelen colaborar para rastrear a los delincuentes informáticos. De todos modos existen refugios seguros desde los cuales pueden operar sin ser atrapados.

Otro factor que dificulta la investigación es la complejidad tecnológica. Por ejemplo un atacante astuto podría realizar un ataque a una red pasando por varios lugares. Cada paso

intermedio representa para el perito forense informático más pasos legales. Sin mencionar que tiene que identificar los servidores correctos y sus correspondientes administradores.

8.2 Legislación Internacional

Es importante entender las leyes de otros países porque Internet es una entidad internacional. Personas de un país son afectadas por usuarios de otros países y ciudadanos de un país pueden estar sujetos a las leyes de otros países. La naturaleza internacional de los delitos informáticos hacen más complicado el análisis.

Por ejemplo una persona del país A, puede estar situada en el país B, usar un proveedor de Internet del país C, utilizar una computadora comprometida en el país D y atacar sistemas que están en el país E; sin mencionar que las comunicaciones atraviesan otros tantos países. Para encausar este delito se requiere cooperación de los cinco países involucrados. Puede ser requerido que el atacante sea extraditado de B a E para que sea juzgado allí. Por otro lado, la evidencia digital obtenida en D puede ser considerada inadmisible en E por la manera que fue obtenida o almacenada. Entonces las fuerzas del orden aún cuando cooperen entre sí, podrían ser incapaces de actuar en ciertos casos.

8.2.1 Legislación en Sudamérica

A fin de tomar una mejor perspectiva de como está la legislación argentina en materia de delitos informáticos, se analizaron los principales países que componen el Mercosur y/o la UNASUR [23].

Bolivia No tiene una ley específica, los delitos informáticos son tratados como delitos comunes en el Código Penal.

Brasil Ley 10.764 (2003). Se modifica el *Estatuto del Menor y Adolescente* que pune la prestación de imágenes por Internet, con escenas de sexo explícito que involucren a menores.

Ley 12.737 (2012). Se incluyen penas por robo de información personal, reproducción de programas informáticos, accesos no autorizados a dispositivos y la interrupción de servicios telemáticos o de informática de utilidad pública. La acción penal contra ese tipo de crímenes sólo podrá ser iniciada por la víctima, salvo cuando se trate de delitos contra la administración pública, cualquiera de los poderes de la República o empresas concesionarias de servicios públicos.

Colombia Ley 1.273 (2009). Se tipifican delitos de acceso abusivo u obstaculización ilegítima a un sistema informático o red de telecomunicaciones; interrupción de datos

informáticos, daño informático, uso de software malicioso, violación de datos personales, hurto por medios informáticos y transferencia no consentida de activos.

Chile Ley 19.223 (1993). Se contempla únicamente daños, hurto y la revelación maliciosa de datos contenidos en un sistema informático. Posteriormente se dicto un decreto que regula el uso de la firma digital y los documentos electrónicos del estado.

Paraguay Ley 1.160 (1997). Se reformó el Código Procesal Penal Nacional. Se tipifican la lesión de derechos a la comunicación; violación del secreto de la comunicación; alteración de datos; sabotaje de computadoras; operaciones fraudulentas por computadora; aprovechamiento clandestino de una prestación; perturbación a las instalaciones de telecomunicaciones; asociación criminal; alteración de datos relevantes para la prueba; equiparación para el procesamiento de datos.

Ley 1.328 (1998). Se tipifican las acciones que violan los derechos de autor y otros derechos intelectuales.

Ley 2.861 (2006). Se reprime el consumo, posesión, comercio y la difusión comercial o no comercial de material pornográfico, utilizando la imagen u otra representación de menores o incapaces.

Uruguay No tiene una ley específica sobre delitos informáticos, pero en su Código Penal se han tipificado las publicaciones de contenido pornográfico y el conocimiento fraudulento de los secretos.

Venezuela Ley 27.313 (2001). Llamada *Ley Especial Contra los Delitos Informáticos*. Es una de las legislaciones mas completas porque tipifica las conductas delictivas y también da definiciones para que los artículos puedan ser aplicados eficazmente. La ley se encuentra dividida en cinco títulos:

i Contra los sistemas que utilizan tecnologías de información.
ii Contra la propiedad.
iii Contra la privacidad de las personas y de las comunicaciones.
iv Contra niños y adolescentes.
v Contra el orden económico.

8.2.2 Legislación de EE.UU.

Sin dudas EE.UU. ha sido pionero en materia tecnológica, delitos informáticos y también en legislación. Se propone explorar varias leyes del país, descritas en [19], para tener una referencia sobre que temas es importante legislar.

Fraude Electrónico y Abuso El estatuto 18 USC 1030 se promulgó en 1984 y recibió varias actualizaciones desde entonces. Se prohibe:

- Acceso no autorizado a una computadora:
  - que contenga información protegida para defensa nacional o asuntos de relaciones internacionales.
  - que contenga información bancaria o financiera.
  - operada por el gobierno de los EE.UU. para uso, modificación, destrucción o revelación de información.
  - *protegida*, la cual para los juzgados es considerada cualquier computadora conectada a Internet.
- Fraude de computadora.
- Transmitir código que cause daño a un sistema o red.
- Capturar tráfico con contraseñas.

Las penalidades pueden duplicar el valor económico de la ofensa, ir de 1 a 20 años de prisión o ambas.

Espionaje Económico Uso de una computadora para espionaje extranjero, negocio o secretos comerciales.

Transferencia Electrónica de Fondos Se prohibe el uso, transporte, venta, recepción o suministro de instrumentos de débito obtenidos fraudulentamente del comercio entre estados o del extranjero.

Privacidad La ley de privacidad de 1974, protege la privacidad de datos personales recolectados por el gobierno. A un individuo se le permite determinar que información ha sido recolectada sobre él, para qué propósito y a quién se le brindó tal información. Otro uso de la ley es evitar que una agencia del gobierno acceda a información recolectada por otra agencia para otro propósito.

Privacidad en Comunicaciones Electrónicas Esta ley promulgada en 1986, protege contra la intervención de la línea telefónica. Las agencias del gobierno siempre pueden obtener una orden judicial para acceder a las comunicaciones o grabarlas. Una actualización de la ley requiere que los proveedores de Internet instalen equipamiento especial para permitir las intervenciones de las comunicaciones. La ley también permite a los proveedores de Internet leer el contenido de las comunicaciones para mantener el propio servicio o para protegerse de cualquier daño, como por ejemplo virus y gusanos.

Gramm-Leach-Billey Ley pública 106-102 de 1999, cubre privacidad de datos para clientes de instituciones financieras. Cada institución debe tener políticas de privacidad, informarlas a los clientes y estos tienen el derecho de rechazar cualquier uso de la información que vaya más allá del negocio. También se requiere que las instituciones se sometan a una evaluación rigurosa de seguridad para evitar acceso no autorizado a la información privada de los clientes.

Portabilidad del Seguro Médico y Responsabilidad Le ley pública 104-191, *Health Insurance Portability and Accountability (HIPAA)*, fue promulgada en 1996. La primera parte de la ley se ocupa de los derechos de los trabajadores para mantener la cobertura médica luego que termina el empleo. La segunda parte exige protección de la privacidad de las historias clínicas de los pacientes.

Acta Patriótica Luego de los atentados de 2001 ocurridos en EE.UU., se promulgó una ley que permite al gobierno acceder a las comunicaciones electrónicas. Bajo esta ley las agencias de seguridad sólo necesitan una orden judicial para intervenir las comunicaciones si sospecha que existe un agente de una potencia extranjera.

E-mail no solicitado Los e-mails no solicitados son un gran problema, se estima que más de la mitad del tráfico de correo electrónico es de este tipo. En 2003 los legisladores de EE.UU. promulgaron la ley *Controlling the Assault of Non-Solicited Pornography and Marketing (CAN SPAM)*. Los puntos claves de la ley son:

- Prohíbe información falsa en los encabezados de los e-mails.
- Prohíbe lineas engañosas del asunto.
- Requiere que los e-mails comerciales le provean a los receptores un método para desuscribirse.
- Prohíbe venta o transferencia de la lista de direcciones de e-mails de personas que ya se desuscribieron.
- Requiere que los e-mails comerciales sean identificados como publicidad.

Las mayores críticas que recibió esta ley es que no hace mucho con respecto al correo no deseado que viene de otros países. Desafortunadamente el correo no solicitado en EE.UU. no ha declinado desde la promulgación de esta ley.

8.2.3 Convenio sobre Ciberdelincuencia de Budapest

El 23 de Noviembre de 2001, EE.UU., Canadá, Japón y 22 países europeos firmaron en Budapest (Hungría), el convenio sobre ciberdelincuencia [20]. El objetivo principal fue definir las actividades de los delitos informáticos y soportar su investigación y persecución

internacionalmente. La importancia de este tratado no radica solamente en que esas actividades son ilegales, sino que los países las reconocen como crímenes más allá de sus fronteras. Esto permite que los organismos dedicados a hacer cumplir la ley y extraditar a los delincuentes informáticos en caso de ser necesario.

El tratado no define *cibercrimen*, sino que enumera varios tipos de ofensas y exhorta a los estados a contemplarlas como infracciones penales. Las sistematiza en cuatro grupos [21]:

1. Infracciones contra la confidencialidad y disponibilidad de datos y sistemas
2. Infracciones relativas al contenido
3. Infracciones contra la propiedad intelectual y derechos afines
4. Infracciones informáticas

Los países que ratifican el tratado deben adoptar leyes similares para los siguientes delitos informáticos:

- Hacking
- Fraude
- Falsificación
- Acceso no autorizado
- Infracción a derechos de autor
- Intrusión de red
- Pornografía infantil
- Propaganda sobre racismo o xenofobia

El tratado también tiene previsiones sobre facultades para investigar y procedimientos; tales como la búsqueda de computadoras de red y la intercepción de comunicaciones. Se requiere cooperación internacional para la búsqueda detención y extradición.

Hasta el día de hoy lo han firmado y ratificado 47 países:

- Albania
- Alemania
- Armenia
- Australia
- Austria
- Azerbaiyán
- Bélgica
- Bosnia-Herzegovina
- Bulgaria
- Canadá
- Croacia
- Rep. Checa
- Chipre
- Dinamarca
- Rep. Dominicana
- EE.UU.
- Eslovaquia
- Eslovenia
- España
- Estonia
- Finlandia
- Francia
- Georgia
- Hungría
- Islandia
- Italia
- Japón
- Letonia
- Lituania
- Luxemburgo
- ex Macedonia
- Malta
- Mauritania
- Moldavia
- Montenegro
- Noruega
- Países Bajos
- Panamá
- Polonia
- Portugal
- Reino Unido
- Rumania
- Rusia
- San Marino
- Serbia
- Sri Lanka
- Suiza
- Turquía
- Ucrania

Mientras que otros 7 países han firmado sin ratificar:

- Andorra
- Grecia
- Irlanda
- Liechtenstein
- Mónaco
- Sudáfrica
- Suecia

8.2.4 Ley de Protección de Datos de la Unión Europea

La ley data de 1994 y está basada en la *Directiva de Privacidad Europea*. Es una legislación modelo para todos los países de la Unión Europea. Establece derechos de privacidad y responsabilidades de protección para todos los ciudadanos. La Ley controla la recolección y almacenamiento de datos personales de los individuos: nombre, dirección, número de identificación. Se requiere un propósito de negocio para la recolección de datos y pone controles sobre el revelado de los mismos.

Lo más significativo es que ley requiere protección equivalente en países que no pertenecen a la Unión Europea, si las organizaciones de la Unión Europea pasan datos protegidos fuera de la misma.

8.2.5 Contenido Restringido

Algunos países tiene leyes que controlan el contenido de Internet. Singapur requiere que los proveedores del servicio filtren el contenido permitido. China prohíbe material que altere el orden social. Túnez tiene una ley que aplica los mismos controles sobre los discursos críticos como para otras formas de medios.

Se han propuesto leyes adicionales para que sea ilegal transmitir contenido fuera de la ley a través de un país; sin importar si el origen o destino del contenido está situado en ese país. Pero dada la compleja infraestructura de Internet, hacer cumplir efectivamente esas leyes es imposible.

8.2.6 Criptografía

Como ya se discutió en las técnicas anti-forenses, la criptografía es una herramienta muy potente y puede ser utilizada en varios escenarios.

- Los usuarios promedio desean privacidad en las comunicaciones con otros.
- La gente de negocio desea proteger sus estrategias de mercado.
- Los criminales quieren mantener en privado sus planes.
- El gobierno quiere controlar las actividades ilegales, para prevenir crímenes o para enjuiciar luego de ocurrido el hecho.
- Las naciones quieren conocer los planes militares y diplomáticos de otros países.

Entonces claramente le conviene a un gobierno que los demás no puedan utilizar criptografía avanzada, o sea que no pueda ser descifrada por el propio gobierno.

Es por ello que varios gobiernos controlan la criptografía. En China los individuos requieren un permiso especial para utilizarla. Pakistán requiere que el gobierno inspeccione todo el hardware y software que utilicen cifrado. En Irak existen serias penas para las personas que utilicen cifrado sin autorización. El caso de Francia es más complejo, el cifrado para autenticación no está restringido; el cifrado que usa una clave de hasta 128 bits sólo requiere el registro del fabricante; y para los productos que utilizan claves de más de 128 bits que sea garantizada por una tercera parte de confianza.

Estas leyes son muy difíciles de hacer cumplir a nivel individual, porque el gobierno no puede evitar que dos personas se pongan de acuerdo para tener su comunicación segura. Sin embargo sí puede imponer un control en el inicio de la cadena, es decir en los fabricantes y vendedores de software o hardware.

Hasta 1998, EE.UU. fue pionero en controlar la exportación de criptografía poniéndola en la misma categoría de municiones, tales como bombas o misiles atómicos. Aunque la ley se aplicaba a todos, en la práctica sólo se pudo forzar para los fabricantes de software masivo. Estas políticas fueron fundamentales para darle ventaja competitiva, ya que la mayoría de los grandes productores de software estaban localizados en el Silicon Valley.

La criptografía no sólo involucra productos, sino también ideas. Una decisión polémica fue cuando un juzgado de EE.UU. ordenó que el código binario[1] del software estuviera sujeto a las restricciones de exportación, pero no así una versión impresa del código fuente [2]. Un caso célebre fue el del inventor del PGP Email Encryption; en 1997 Zimmermann "exportó" libros con el código fuente del producto. Muchos voluntarios de Europa invirtieron unas 1000 horas escaneando las páginas los libros y dejándolo disponible en Internet. Luego de lo cual se imprimieron muchas remeras con la sarcástica leyenda: *"Cuidado, esta remera puede ser una munición controlada"*.

8.3 Legislación Argentina

En [21] se da una breve reseña histórica de cómo fueron evolucionando las leyes argentinas en materia de delitos informáticos y cómo se encuentran en relación al *Convenio sobre Ciberdelincuencia* de Budapest.

8.3.1 Evolución

Ley 24.766 (1997) Confidencialidad sobre información y productos que estén legítimamente bajo control de una persona y se divulgue indebidamente de manera contraria a los usos comerciales honestos. Hace referencia a la violación de secreto de una empresa.

[1] Código que resulta de la compilación del código fuente.

[2] Conjunto de líneas de texto, que son las instrucciones que debe seguir una computadora para ejecutar el programa de software.

Ley 24.769 (1997) Estableció el vigente régimen penal tributario y previsional, en el que incorporó la figura de alteración dolosa de registros fiscales incluyendo los de tipo informático.

Ley 25.036 (1998) Se modificó la vieja Ley de Propiedad Intelectual 11.723. El objetivo era proteger a los programas de computación.

Ley 25.286 (2000) Se modificó el Código Penal para incluir la protección de datos personales.

Ley 25.506 (2001) Se modificó el Código Penal para incluir los documentos y firmas digitales.

Ley 25.891 (2004) Se regula el servicio de comunicaciones móviles.

Ley 25.930 (2004) Se modificó el Código Penal para incluir el fraude mediante el uso de tarjeta débito o crédito.

Ley 26.388 (2008) Se reformó el código penal, fue el producto de la conjugación de 16 proyectos que estaban en estudio en el Congreso, se concreta la derogación de dos artículos y la modificación, sustitución o incorporación de doce.

8.3.2 Ley 26.388

Previo a esta Ley existían ciertos vacíos legales porque no estaban tipificados correctamente los delitos informáticos en el Código Penal y los fallos de los jueces resultaban caóticos porque no tenían en qué basarse.

La Ley 26.388 [22] contempla los siguientes delitos:

- Distribución de pornografía infantil.
- Interrupción, obstrucción, entorpecimiento o desvío de comunicaciones electrónicas (e-mail, navegación, mensajería instantánea, etc).
- Acceso indebido a bases de datos privadas o restringidas.
- Acceso o apertura indebida de comunicaciones electrónicas (e-mail, mensajería instantánea, e incluso SMS si se argumenta que pasan por un sistema informático central).
- Alteración del normal funcionamiento de los sistemas.
- Alteración, destrucción o inutilización de documentos, programas y sistemas informáticos.
- Venta, distribución o introducción de programas destinados a hacer daño en un sistema informático.

Por otro lado, la Ley plantea las siguientes limitaciones de alcance:

- Los delitos afectan a las personas responsables y no a la empresa donde trabajan.
- Las intercepciones de comunicaciones a nivel de servidores no son contempladas.
- Sólo se penará las comunicaciones indebidas o no autorizadas.
- No se contempla la educación del usuario. Es decir que no se protege a un usuario desprevenido que ha publicado datos personales o número de tarjeta de crédito en Internet, sin saber que podrían ser accedidos por otros.

8.3.3 Comparación con el Convenio de Budapest

Existen ciertas concordancias y carencias de la normativa nacional. El Convenio de Budapest prevee reglas relacionadas a:

- Ambito de aplicación (art. 14)
- Condiciones y garantías (art. 15)
- Competencia, conservación inmediata de datos, incluidos los de tráfico (art. 16)
- Registro y decomiso de datos almacenados (Título 4 de la sección 2)
- Recolección en tiempo real de datos (art. 20)
- Interceptación de datos (art. 21)
- Cooperación (art. 23)
- Colaboración internacional en la investigación (art. 31)
- Medidas cautelares (art. 29)
- Red de contactos 24x7 [3] (art. 35)
- Extradición (art. 24)

A todas estas reglas la normativa argentina resulta insuficiente; se omiten referencias a la adquisición, preservación y validación en juicio de la evidencia digital. Por ejemplo para las comunicaciones por Internet, no especifica cómo intervenirlas, por quién o con qué límites; dejando librado a la inspiración del juez de turno.

En varias jurisdicciones se producen discusiones si es necesario o no pedir una autorización judicial para el pedido de informe del tráfico de datos, validación del registro de llamadas de un teléfono móvil o la agenda de contactos por un fiscal. La dirección IP de una computadora que accede a la red, permite en muchos casos conocer la identificación personal a través del proveedor de Internet. A través del IMEI e IMSI, se puede obtener información del usuario y ubicación del teléfono móvil en un momento determinado; lo cual puede servir para corroborar o descartar una coartada durante una investigación.

Existen reglas genéricas pero no se regulan: por quién, cuándo, con qué límites y cómo requerir este tipo de datos. Las reglas de juego no son claras para la intervención de las

[3] 24 horas al día, los 7 días de la semana.

comunicaciones electrónicas. Esto trae ciertas controversias en el ámbito laboral, donde las empresas pueden controlar el e-mail o navegación de los empleados aprovechando los déficits legales mencionados.

Capítulo 9

Marco Ético

En la Tabla 9.1 se comparan ley y ética, para entender mejor el término de *hacker ético* que a primera vista puede resultar contradictorio.

Tabla 9.1: Contraste de ley vs. ética

	Ley	**Ética**
Descrita por:	documentos formales	principios no escritos
Interpretada por:	juzgados	cada individuo
Presentada por:	legislaturas	filósofos, religión, profesionales
Aplicable a:	todos	elección personal
Prioridad determinada por:	juzgado	individuos
Arbitrada por:	juzgado	nadie externo
Cumplimiento:	por policías y juzgados	limitado

Luego de explorar las técnicas anti-forenses más utilizadas, queda el interrogante de como se han desarrollado. Lo primero que se viene a la mente es que fueron *hackers* con intenciones de distorsionar las pericias forenses. Sin embargo, existen muchas personas que por intereses académicos o forenses tratan de alertar sobre las fallas de herramientas y procedimientos forenses.

9.1 Concepto de Hacker

Tradicionalmente el término *hackear* se refiere a:

> *"La exploración de la tecnología; tratando de entenderla a un nivel avanzado para ser capaz de manipularla en hacer algo para lo cual no fue diseñada."*

Los primeros *hackers* de este tipo lo hacían por hobby o con fines académicos, con el objetivo de usar la tecnología de formas interesantes e innovadoras. Pero el término significa diferentes cosas para distintas personas. Mucha gente afirma que el hacking es una práctica aceptable porque la falta de protección significa que los dueños de los sistemas o datos no los valoran realmente.

En [19] se cuestiona este pensamiento haciendo una analogía con entrar a una casa. Se puede considerar el argumento de que un intruso que no causa daño y no realiza cambios, está simplemente aprendiendo cómo funciona el sistema. Esto equivale a ir caminando por la calle e intentar abrir cada puerta hasta encontrar una sin llave y luego revisar en los cajones de los muebles. ¿Cómo se puede sentir el dueño si su casa ha sido invadida, aún si ningún daño fue hecho?

Ambas situaciones son una invasión a la privacidad. Decir que se hace para hacer las vulnerabilidades más visibles es presuntuoso y reprochable. Entrar en una casa o computadora sin autorización, aún con buenas intenciones, puede llevar a consecuencias no deseadas. Muchos sistemas pueden resultar dañados accidentalmente por intrusos ignorantes o descuidados.

No es aceptable el argumento que ser hacker equivale a ser experto en seguridad. Un buen profesional tiene dos cualidades: conocimiento y credibilidad. Investigadores que exploran y experimentan en un entorno o laboratorio aislado pueden aprender como encontrar y explotar vulnerabilidades tanto cómo un hacker. La principal diferencia es la confianza. Si se contrata un hacker siempre se tendrá el temor o duda si está recolectando información para atacar al dueño del sistema o alguien más. Al momento de pedir asesoramiento de seguridad, se optará por el menor riesgo; y el historial de un hacker por lo general se construye sobre un comportamiento no ético.

9.2 El Hacker Ético

Hoy en día se piensa del *hacking* en términos siniestros: irrumpir en los sistemas informáticos y cuentas de usuarios sin la autorización del dueño, para hacer dinero ilegalmente o causar algún daño.

Más recientemente se comenzó a utilizar el término de *hacker ético* para referirse a individuos que irrumpen en los sistemas informáticos, pero con el propósito de encontrar vulnerabilidades tal que puedan ser arregladas. Se supone que el adjetivo *ético* anula las connotaciones negativas de hacking. Los hackers éticos usan algunas de las técnicas y procesos de los "chicos malos", pero de una manera profesional con el adecuado consentimiento de los dueños de los sistemas, para tratar de mejorar la seguridad de los mismos.

En el curso preparatorio para la certificación internacional de seguridad de SANS [25], se da la siguiente definición de *hacking ético*:

> *"Es el proceso de usar técnicas de ataques a sistemas informáticos con el permiso del dueño, para encontrar fallas de seguridad y el objetivo de mejorar los sistemas."*

En particular, el objetivo del hacker anti-forense es encontrar fallas en las herramientas y procedimientos forenses informáticos para eliminar, ocultar o alterar la evidencia digital.

Es una realidad que las técnicas anti-forenses han hecho que las herramientas forenses evolucionen continuamente, volviéndose cada día más sofisticadas.

El filósofo e investigador Pekka Himannen propone en [26] un interesante punto de vista sobre la ética hacker. Teniendo como referente a Linus Torvalds[1], menciona los tres factores que lo convirtieron en uno de los hackers más icónicos:

- **supervicenvia:** prerrequisito para satisfacer las otras dos.
- **pasión:** motivación por algo interesante, atractivo y placentero.
- **vida social:** pertenencia y reconocimiento.

Notar que estos valores se contraponen con los ideales del capitalismo moderno donde la principal motivación es el dinero. Estas motivaciones son reflejadas en la filosofía de código abierto; cuyos principales fines son compartir lo aprendido, colaborar y lograr la máxima calidad de un producto en función de la inteligencia colectiva.

Otro de los conceptos mencionados es la *nética* o ética de la red. Es la relación que el hacker mantiene con las redes de la sociedad actual, mucho más allá de su comportamiento en la Internet. Fundamentalmente facilitando el acceso a la información y a los recursos informáticos. Esto promueve el desarrollo personal que es fundamental considerando que el conocimiento informático queda rápidamente obsoleto con los avances tecnológicos.

9.3 Test de Penetración

Otro concepto muy relacionado es el *Test de Penetración*:

> *"Es el proceso de encontrar fallas en un entorno particular con el objetivo de penetrar en los sistemas informáticos, tomando control de los mismos."*

El test de penetración, como su nombre lo indica, está enfocado en penetrar las defensas de la organización, comprometiendo sistemas y obteniendo acceso a la información.

Para resumir, hacking ético es un término en expansión abarcando todas las técnicas de hacking usadas para el bien; mientras que el test de penetración está más enfocado en el proceso de encontrar vulnerabilidades en un entorno específico. Desde este punto de vista, el test de penetración sería un caso particular del hacking ético.

9.4 Códigos de Ética

Debido a las cuestiones éticas mencionadas, muchos grupos de computación han buscado desarrollar códigos de ética para sus miembros. La mayoría de las organizaciones relacionadas a la computación, como la ACM o la IEEE son voluntarias. Ser miembro no certifica un nivel

[1] Creador del sistema operativo Linux en 1991, cuando estudiaba en la Universidad de Helsinki.

de competencia, responsabilidad o experiencia en computación. Por estas razones los códigos de ética son mayormente orientadores; pero sin dudas es un buen punto de partida para analizar los problemas de ética.

La IEEE es una organización de ingenieros, no limitada a la computación. Entonces su código de ética abarca aspectos más allá de la seguridad informática. Por otro lado, el código de ética de la ACM reconoce tres cosas de sus miembros: imperativos morales generales, profesionalismo y liderazgo tanto dentro como fuera de la asociación.

El Computer Ethics Institute (CEI) es una organización sin fines de lucro, destinado a la investigación y educación, que anima a la gente a considerar aspectos éticos de sus actividades informáticas. Se enfoca en los problemas, dilemas y desafíos del avance de la tecnología de la información dentro de los marcos éticos. El instituto tiene su sede en Washington D.C. (EE.UU.). A continuación se muestran los *Diez Mandamientos de Ética Informática* publicados por la organización:

I *No usarás una computadora para dañar a otras personas.*

II *No interferirás con el trabajo de la computadora de los demás.*

III *No has de husmear en los archivos de otras personas.*

IV *No usarás una computadora para robar.*

V *No usarás una computadora para dar falso testimonio.*

VI *No has de copiar o utilizar software propietario por el que no has pagado.*

VII *No usarás los recursos informáticos de otras personas sin autorización o compensación adecuada.*

VIII *No has de adueñarte de la propiedad intelectual de otras personas.*

IX *Piensa en las consecuencias sociales del programa que estas escribiendo o el sistema que estás diseñando.*

X *Usarás siempre una computadora de manera que asegure consideración y respeto por tu prójimo.*

Como se puede ver, estos mandamientos intentan evitar mayormente delitos informáticos de fraude, robo o intrusión.

Parte III

Discusión

Capítulo 10

Conclusiones

Los mayores avances tecnológicos han sido impulsados por asuntos militares o de defensa de estado. Esto también se ve reflejado en la evolución de las técnicas anti-forenses. Políticos, militares o terroristas que necesitan comunicarse de forma segura, destruir datos secretos de forma definitiva o interceptar comunicaciones electrónicas para lograr una ventaja estratégica.

Por otro lado, existen muchos entusiastas que por hobby o fines académicos diseñan técnicas e incluso software anti-forense. Todo este contexto ha permitido que se desarrollen muchos métodos que dificultan el trabajo del perito forense informático.

10.1 Aspectos Técnicos

Las técnicas de sobrescritura y ocultamiento de datos son más fáciles de detectar para un perito forense informático. Más allá que los datos mismos no sean recuperados, se puede dejar algún rastro que puede ser detectado analizando ciertas estadísticas del sistema de archivos. En ese sentido las técnicas de anti-concepción son más seguras, porque minimizan los rastros que se dejan para un posterior análisis forense.

Los medios de almacenamiento SSD y USB son menos sensibles a los golpes, más silenciosos y acceden a los datos más rápido que los tradicionales discos magnéticos. Sin embargo, para eliminar la evidencia conviene sanitizar la unidad completa, lo cual insume más tiempo. Es acá donde se puede considerar utilizar un disco con cifrado por hardware, porque se puede sanitizar la unidad simplemente desechando la clave criptográfica.

Con respecto a técnicas de ofuscación, implican un mayor esfuerzo del perito forense informático, ya que requerirá más tiempo para trazar la ruta del envío de e-mails modificados o con contenido esteganográfico.

Las herramientas forenses sin duda representan el "caballo de batalla" del perito forense informático. Pero el mismo no debería confiar ciegamente en ellas, ya que como todo software tiene vulnerabilidades y limitaciones. Hay que estar atento a las últimas técnicas que atacan al software forense, para sacar mayor provecho de la herramienta y orientar mejor la búsqueda y análisis de la evidencia digital.

10.2 Aspectos Metodológicos

Las técnicas anti-forenses que atacan los procedimientos forenses, toman mucha importancia sobretodo para un perito de control que debe defender a su parte. Normalmente desacreditando la herramienta forense utilizada, en caso que no esté certificada, o cuestionando el procedimiento para tratar la evidencia digital si no se aplicaron ciertos estándares esperados.

Asimismo, el personal judicial involucrado debería ser capacitado para estar al tanto de las últimas tendencias tecnológicas para respetar los procedimientos forenses a fin de no arruinar la evidencia digital.

10.3 Aspectos Legales

Existen ciertas dificultades para juzgar delitos informáticos. En general los juzgados no le han dado a los dispositivos tecnológicos, software y datos digitales la importancia adecuada, considerando el verdadero valor que tienen y la seriedad del delito informático. Aunque en los últimos años se ha legislado más, las leyes siguen estando atrasadas con respecto a los constantes cambios tecnológicos.

Las principales consecuencias de esta situación, son que las penas aplicadas por los magistrados podrían no ser las adecuadas considerando los daños económicos, pérdida de información o violación de la privacidad que ocurren. Si las leyes no avanzan a la misma velocidad que la tecnología, quedarán vacíos legales que los delincuentes informáticos sin escrúpulos explotarán para cometer ilícitos.

Es fundamental estudiar las legislaciones sobre delitos informáticos de los diferentes países de manera integral, ya que este tipo de delitos no reconoce fronteras. Incluso desde el punto del delincuente informático, es importante conocer las diferentes legislaciones para saber desde donde le conviene operar y aplicar las técnicas anti-forenses adecuadas para llevar adelante el delito informático.

Por el lado de los jueces, también deberían informarse de las últimas tecnologías para saber interpretar adecuadamente las leyes vigentes o jurisprudencia. Como los delitos informáticos generalmente no implican cosas tangibles, no se toma una correcta dimensión de su gravedad. En muchos casos la información almacenada que se pierde es mucho más costosa que el medio de almacenamiento que la contiene.

10.4 Aspectos Éticos

Existe una estrecha relación entre técnicas anti-forenses y técnicas de hacking. Las herramientas forenses como cualquier software presentan vulnerabilidades o fallas de diseño y necesitan ser mejoradas. En este escenario es donde toman importancia los aportes de los *hackers éticos*. Los mismos pueden desarrollar técnicas anti-forenses o destacar las deficiencias del software forense.

Existen algunos códigos de ética informática que pueden tomarse como referencia para los profesionales informáticos. Estos principios apuntan a evitar delitos informáticos de fraude, robo o intrusión, desde lo moral y no aplicando la fuerza de la ley.

Desde el punto de vista del perito forense informático, el mismo debería tratar la evidencia digital con responsabilidad, accediendo a datos privados con la debida autorización.

10.5 Reflexión Final

Para saber cómo resistir o evadir un análisis forense, el delincuente informático tiene que ponerse en el lugar del perito forense y conocer cómo funcionan las herramientas y procedimientos forenses. Recíprocamente, el perito forense debería estudiar las últimas técnicas anti-forenses, para determinar si la pericia informática dará frutos y el esfuerzo que podría demandar.

Por lo tanto el perito forense y el delincuente informático son dos perfiles que están enfrentados pero que históricamente se han retroalimentado mutuamente para mejorar sus respectivas técnicas, ya sean forenses o anti-forenses.

Anexo I: Herramientas Anti-Forenses

En este anexo se presenta un compilado de herramientas que implementan varias de las técnicas estudiadas. Como todo software, estas herramientas pueden evolucionar, cambiar de nombre, soportar nuevos sistemas operativos o incluso estar discontinuadas.

Al momento de utilizar cualquiera de estas herramientas, se recomienda chequear las últimas funcionalidades y que sistemas operativos soporta.

Ocultamiento de Datos

Cifrado de Discos

- beCrypt
- BestCrypt
- BitArmor DataControl
- BitLocker
- CGD
- Checkpoint Full Disk Encryption
- DiskCryptor
- dm-crypt
- FreeOTFE
- GBDE
- GELI
- FileVault Disk Encryption
- loop-AES
- Linux Unified Key Setup
- McAfee Drive Encryption
- PGPDisk
- SafeGuard Easy
- SECUDE
- Securstar DriveCrypt
- TrueCrypt
- vnconfig

Cifrado de Discos por Hardware

Integrado

- Hitachi Bulk Data Encryption
- Seagate Full Disk Encryption
- Toshiba Self-Encrypting Drives

Chasis Externo

- Addonics
- Apricorn
- DigiSafe
- Eracom Technology DiskProtect
- iStorage DiskCrypt Mobile
- Network Appliance (Decru)

Cifrado de Discos Virtuales

- BestCrypt
- BitLocker
- CipherShed
- CrossCrypt
- FileVault Disk Encryption
- FreeOTFE
- TrueCrypt
- VeraCrypt

Sistemas de Archivos Criptográficos

- eCryptfs
- EncFS
- MagicFS
- Rubberhose
- StegFS

Sistemas de Archivos con Cifrado

- AdvFS
- Ext4
- F2FS
- Novell Storage Services
- NTFS con EFS
- PGP Virtual Disk
- ZFS

Protocolos de Comunicación

- LocalSSL
- Orbot
- Tor Browser

Esteganografía

- Anubis
- BMPSecrets
- DarkCryptTC
- ImageSpyer G2
- MP3Stego
- OpenPuff
- OpenStego
- Outguess-rebirth
- PHP-Class Stream Steganography
- Red JPEG
- S-Tools
- Steg
- StegaMail
- Steganographic Laboratory (VSL)
- Steganography Studio
- StegFS
- Steghide
- StegoShare

Empaquetadores de Programas

- Burneye
- DocWrap
- EXEStealth
- EXEWrapper
- FileJoiner
- Morphine
- PECompact
- PEBundle
- TrojanWrap
- UPXPack

Otras Formas de Ocultamiento

- Data Mule FS
- FragFS
- KY FS
- RuneFS
- Slacker (Metasploit Framework)
- Waffen FS

Eliminación de Datos

Sanitización

- BCWipe
- Blancco Erasure Solutions
- CBL Data Shredder
- Darik's Boot and Nuke (DBAN)
- ErAce
- Eraser
- HDShredder
- HDDErase
- Norton Disk Doctor
- PGP Wipe
- R-wipe and clean
- Secure delete
- Secure Empty Trash
- comando `shred` (Linux)
- Tracks Eraser Pro
- uniShred
- WinPT wipe file
- Wipe

Anticoncepción de Datos

- portableapps.com
- U3

Live Distros

- ArchAssault
- BackBox
- BackTrack
- BlackArch
- Bugtraq
- CAINE
- Cyborg
- DEFT
- Fedora Security Spin
- Kali
- Knoppix STD
- Matriux Krypton
- NodeZero
- Parrot
- Pentoo
- Samurai Web Testing Framework
- WEAKERTH4N

Máquinas Virtuales

- Parallels
- Qemu
- Virtual Box
- VMware
- Windows Virtual PC

Ofuscación

- SquirrelMail
- The Defiler's Toolkit
- Timestomp (Metasploit Framework)

Ataques al Software Forense

- Archivo `42.zip`
- Sistema de monitoreo SMART
- Transmogrify (Metasploit Framework)

Glosario

Blur Efecto gráfico para suavizado de una imágen, también llamado desenfoque. 26

Buffer overflow Error de software que se produce cuando no se controla adecuadamente la cantidad de datos que se copian sobre un área de memoria reservada. 23, 30, 38

Cache Componente que almacena datos para futuras peticiones. 18

Debugging Proceso para encontrar y resolver los defectos de un software. 16

Exploit Pieza de software o secuencia de comandos que toman ventaja de una vulnerabilidad de seguridad de otro software. 23, 30

Expresiones regulares Secuencias de caracteres que forman un patrón de búsqueda. 30

Firewall Es un dispositivo de control de acceso que se sitúa entre dos redes o segmentos de una misma red. 7

Firmware Software que maneja físicamente un hardware. 19

Handshake Proceso automatizado de negociación que establece de forma dinámica los parámetros de un canal de comunicaciones entre dos entidades. 9

Hash Representación compacta de una cadena de entrada más grande. 32

Hijacking Técnica ilegal para robar información. 22

Keylogger Software malicioso que almacena las teclas pulsadas para robar datos como por ejemplo contraseñas. 7

Multicast Envío de información a múltiples destinos o redes simultáneamente. 9

Swap Espacio asignado en el disco para almacenar memoria virtual del sistema operativo. 4, 19

Telemático Disciplina científica originada por la convergencia entre las tecnologías de las Telecomunicaciones e Informática. 39

Trazar Imprimir las sentencias que indican el flujo de ejecución de un proceso o programa. 16

Troyano Software malicioso que no aparenta ser peligroso, para persuadir a la víctima a instalarlo. 7, 37

YUV Espacio de color típicamente usado como parte de un sistema de procesamiento de imagen en color. 25

Bibliografía

[1] US-CERT. "Computer Forensics". 2008. Disponible en Web: `https://www.us-cert.gov/sites/default/files/publications/forensics.pdf` (Consultada el 29/02/2016).

[2] JIANG Yunwen, HUI Zeng, KANG Xiangui, LIU Li. "The Game of Countering JPEG Anti-forensics Based on the Noise Level Estimation". En: *Proc. of Asian-Pacific Signal and Information Processing Association Annual Submit Conference (APSIPA ASC) 2013*, Taiwan, 2013.

[3] SARANGPURE V, TALMALE R B, DOMKE M. "Audio-Video Steganography Using Anti Forensics Technique". En: *International Journal of Research (IJR)* Volume 1, Issue 9, 2014. ISSN 2348-6848.

[4] SHERLY A P, AMRITHA P P. "A Compressed Video Steganography using TPVD". En: *International Journal of Database Management Systems (IJDMS)* Volume 2, No 3, 2010.

[5] NERALLA S, BHASKARI D L, AVADHANI P S. "Combating Against Anti-Forensics Aligned with E-mail Forensics". En: *International Journal of Computer Applications (0975 – 8887)* Volume 79, No 15, 2013.

[6] TrueCrypt Fundation. *TrueCrypt User's Guide.* version 7.1a. 7/02/2012. Disponible en Web: `https://www.grc.com/misc/truecrypt/TrueCrypt%20User%20Guide.pdf` (Consultada el 29/02/2016).

[7] WEI Michael, GRUPP Laura, FREDERICK Spada, STEVEN Swanson. "Reliably Erasing Data From Flash-Based Solid State Drives". University of California, San Diego, 2011.

[8] GARFINKEL Simson. "Sanitizaction and Usability". En: CRANOR Lorrie, GARFINKEL Simson. *Security and Usability.* Edición 1. Sebastopol: O'Reilly Media, 2005. p.293-317. ISBN 0-596-00827-9.

[9] SYMANTEC. *How Whole Disk Encryption Works* Disponible en Web: `https://www.symantec.com/content/en/us/enterprise/white_papers/b-pgp_how_wholedisk_encryption_works_WP_21158817.en-us.pdf` (Consultada el 29/02/2016).

[10] CACERES Maximiliano. "Syscall Proxying - Simulating remote execution". Core Security Technologies, 2002.

[11] TOR. "Anonymity Online". Disponible en Web: `https://www.torproject.org` (Consultada el 29/02/2016).

[12] KISSEL R, SCHOLL M., SKOLOCHENKO, S, LI X. "Guidelines for Media Sanitization". Gaithersburg: Computer Security Division, National Institute of Standards and Technology, 2014.

[13] KESSLER, Gary C. "Anti-forensics and The Digital Investigator". En: VALLI, C. *Proceedings of the 5th Australian Digital Forensics Conference.* Mt. Lawley, Western Australia: Edith Cowan University, 2007.

[14] (DFRWS) Technical Report (DTR). *A Road Map for Digital Forensics Research.* T001-01 Final: PALMER, Gary, 2001. Disponible en Web: `http://www.dfrws.org/2001/dfrws-rm-final.pdf` (Consultada el 29/02/2016).

[15] SIMSON Garfinkel. "Anti-Forensics: Techniques, Detection and Countermeasures". En: *2nd International Conference on i-Warfare and Security.* 2007.

[16] PIPPER Scott, MARK Davis, SHENOI Sujeet. "Countering Hostile Forensic Techniques". En: OLIVIER Martin S., SHENOI Sujeet *Advances in Digital Forensics II* Springer, 2006. p.80-90. ISBN 978-0-387-36891-7.

[17] KOHUR Jasleen, DEEPANKAR Verma. "Steganography Techniques". En: *International Journal of Emerging Research in Management and Technology.* 2004. ISSN 2278-9359, Volume 3, Issue 5.

[18] LIVERANI Roberto. *.NET MVC ReDoS (Denial of Service) Vulnerability - CVE-2015-2526 (MS15-101)* Disponible en Web: `http://blog.malerisch.net/2015/09/net-mvc-redos-denial-of-service-vulnerability-cve-2015-2526.html` (Consultada el 29/02/2016).

[19] PFLEEGER Charles, PFLEEGER Shari. *Security in Computing* Willis H. Ware (ed. lit.). Edición 4. Prentice Hall, Westford, 2007. ISBN 0-13-239077-9.

[20] COUNCIL OF EUROPE. "Convenio Sobre La Ciberdelincuencia". Serie de Tratados Europeos n°185. Budapest, 23/11/2001.

[21] CHERÑAVSKY Nora, TERRAGNI Marco A. "Informática y derecho penal: ¿entre el control social y el delito?". En: *XI Encuentro de la AAPDP.* Facultad de Derecho, Universidad Nacional de Rosario, 2/6/2011.

[22] Argentina. *Ley 26.388*, modificación del Código Penal. Sancionada: 4/6/2008 y promulgada de hecho: 24/6/2008.

[23] REINA PILMAYQUEN Inés. "Delitos Informáticos en Latinoamérica. Estudio de sus Legislaciones". Director: Horacio Daniel Obligado. Universidad de Buenos Aires, Facultad de Derecho, 2013.

[24] CAFFERATA NORES José, HAIRABEDIÁN Maximiliano. *La prueba en el Proceso Penal.* Edición 6. LexisNexis, Buenos Aires, 2008.

[25] SANS Institute. "Planning, Scoping and Recon". En: *SEC560 - Network Penetration Testing and Ethical Hacking.* 2010.

[26] HIMANEN Pekka. "The Hacker Ethic and the Spirit of the Information Age". Random House Inc. New York, NY, USA. 2001. ISBN 978-0-375-50566-9.