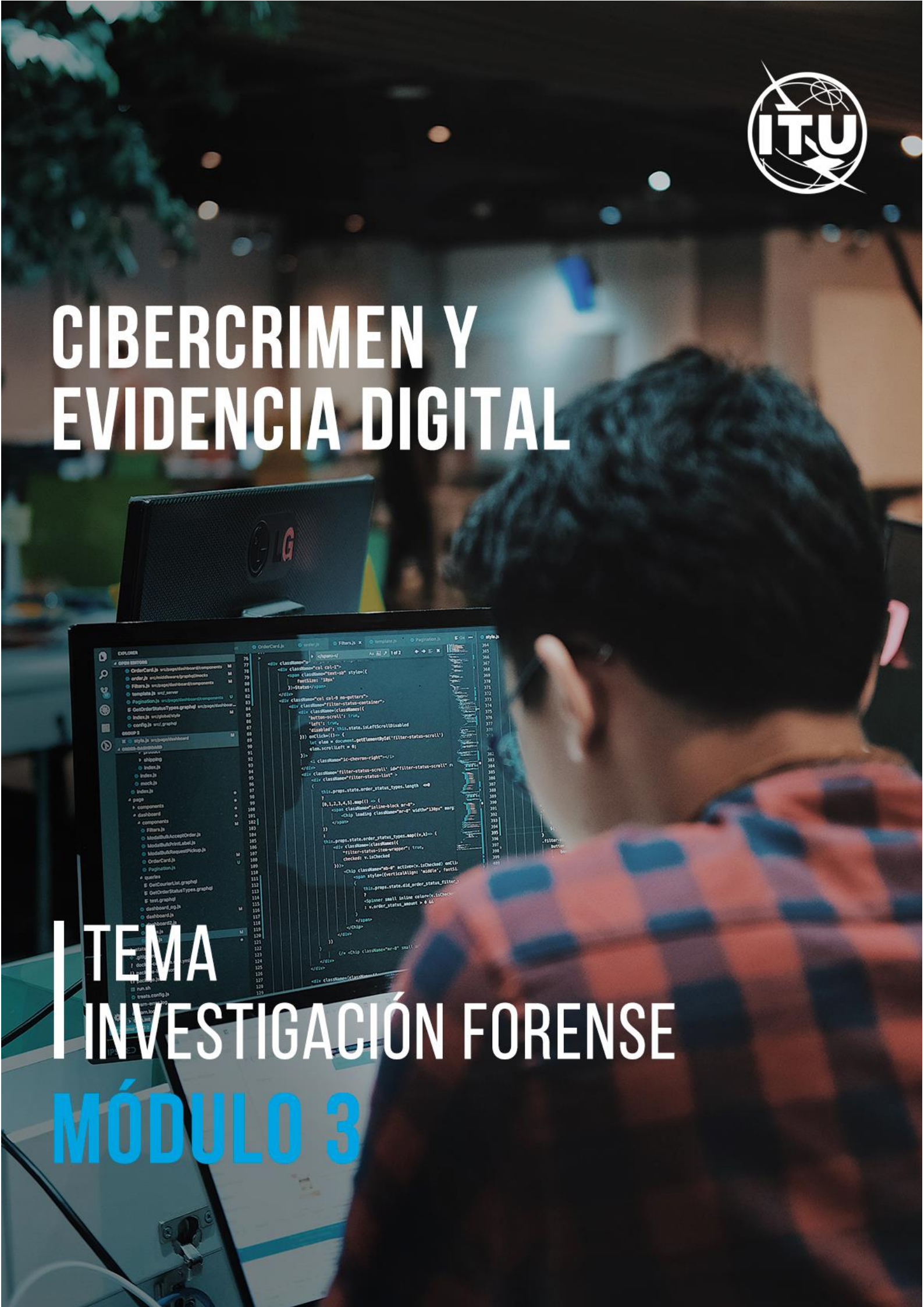


CIBERCRIMEN Y EVIDENCIA DIGITAL

TEMA
INVESTIGACIÓN FORENSE

MÓDULO 3

TABLA DE CONTENIDOS

MÓDULO 3 3

INVESTIGACIÓN FORENSE 3

1. OBJETIVO DEL MÓDULO 3

2. NOCIONES GENERALES DE INVESTIGACIÓN FORENSE EN MEDIOS DIGITALES 3

Sistema binario y operadores lógicos 3

Sistemas numéricos 4

ASCII 6

Investigación digital forense 7

3. ROLES Y PERSONAS INVOLUCRADAS EN LA INVESTIGACIÓN 9

4. TIPOS DE INVESTIGACIÓN 11

Investigaciones criminales 11

Investigaciones civiles 11

Investigaciones corporativas 12

5. DEFINICIÓN DEL PROCESO Y ETAPAS EN LA INVESTIGACIÓN 12

Identificación 12

Recolección 13

Examinación 13

Análisis 14

Presentación 14

6. BIBLIOGRAFÍA 15

MÓDULO 3

INVESTIGACIÓN FORENSE

En el presente módulo se contempla una breve introducción a los sistemas digitales (uso del binario y sistemas numéricos). Luego de ello, se hace una introducción a lo que es la investigación forense en medios digitales y los distintos elementos que lo conforman: personas y proceso.

1. OBJETIVO DEL MÓDULO

Brindar los conocimientos básicos sobre sistemas digitales, así como los conceptos generales de la investigación digital forense.

2. NOCIONES GENERALES DE INVESTIGACIÓN FORENSE EN MEDIOS DIGITALES

Parte de los avances de la era digital es la proliferación de grandes cantidades de datos de distintas personas en el planeta. La información de cada persona, grabaciones de audio y video, mensajería, etc., es transformada en valores digitales que pueden visualizarse a través de medios como computadoras, teléfonos móviles entre otros. Antes de poder ahondar en el ámbito de la investigación, es importante entender ciertos términos y conceptos asociados a los datos.

Sistema binario y operadores lógicos

La información digital puede entenderse en la actualidad como un conjunto de 1's y 0's, valores que indican Verdadero o Falso respectivamente (Boolean). Estos dos valores son usados por los diferentes sistemas digitales para la representación de información. A primera vista, una secuencia de 1's y 0's no transmite alguna información a un ser humano.

Los valores de Verdadero y Falso son analizados por sistemas digitales mediante operadores lógicos: NOT; AND, OR, XOR. Los operadores lógicos pueden entenderse como operadores matemáticos (suma, resta, multiplicación, etc.). Teniendo dos posibles argumentos, uno verdadero y uno falso, estos operadores determinan la verdad o falsedad al combinar estos dos argumentos:

A	B
0	0
0	1
1	0
1	1

!A	A^B	A$^{\vee}$B	A$\oplus$B
1	0	0	0
1	0	1	1
0	0	1	1
0	1	1	0

- **NOT (!A):** Indica la negación de A. Es decir, el valor opuesto de A.

- **AND (A^B):** Para que el resultado sea verdadero, ambos argumentos deben serlo.
- **OR (A˅B):** Para que el resultado sea verdadero, basta que uno de los dos argumentos lo sea.
- **XOR (A⊕B):** Arroja un valor de verdadero cuando ambos argumentos son distintos; es decir, cuando uno es verdadero y el otro es falso.

RETO: Indicar cuál es el resultado de A⊕ (A⊕B) e indicar cuál es la relación entre este resultado y la encriptación.

Sistemas numéricos

Cuando se trata de describir números, el sistema comúnmente usado es el sistema decimal (BASE10). Esto nos permite contar números del 0 al 9. Cada número está asociado a un valor. Para valores mayores a 9, se usan columnas adicionales (unidades, decenas, centenas, etc). Por ejemplo, para el número 274:

2*(10^2)	7*(10^1)	4*(10^0)	Resultado
200	70	4	**274**

Sin embargo, en el sistema binario (BASE2) solo contamos con dos símbolos (1 y 0). Cada unidad de información, que puede simbolizar un 1 o un 0, es conocida como bit. Para poder representar información, se requiere de una cadena de bits por lo que, dependiendo de la cantidad de bits usados, se pueden representar un número finito de valores:

- Con 10 bits: 2^10 = 1024 posibles valores
- Con 20 bits: 2^20 = 2^10 * 2^10 = alrededor de un millón de valores

Al representar información en binario, la información suele convertirse en cadenas largas de data. Otro problema presente es que el sistema decimal no es idóneo para la representación de binario. Por ello, se suele usar Hexadecimal (BASE16) para representar al binario en sistemas digitales. Este sistema cuenta con 16 símbolos: 0 1 2 3 4 5 6 7 8 9 A B C D E F. De querer hacer una comparación entre estos tres sistemas podemos tomar como ejemplo los siguientes valores:

DEC	203	113	33
BIN	1100 1011	0111 0001	0010 0001
HEX	0xCB	0x71	0x21

NOTA: el prefijo “0x” es una denotación usada para indicar que el número está representado en Hexadecimal. No basta con indicar un número sino también indicar qué sistema numérico se está usando.

Para el valor 203, el mecanismo para poder representarlo en binario se debe considerar la posición del bit. En la siguiente tabla se puede apreciar la representación numérica en bits del número 203.

Valor	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**
BIN	1	1	0	0	1	0	1	1

- **Primera columna (128):** Dado que es menor a 203, se le considerará un valor en bit de 1 y se sustraerá el valor de 128 al número inicial. De esta forma, indicamos que 128 unidades del valor inicial ya están representadas: 203-128=75
- **Segunda columna (64):** Similar al caso anterior, es posible representar 64 unidades del restante del valor inicial con este bit: 75-64=11
- **Tercera columna (32):** En este caso, el valor representativo del bit es mayor al valor restante a representar. Por lo tanto, el valor del bit es 0
- **Cuarta columna (16):** Similar a la columna anterior, el valor será 0.
- **Quinta columna (8):** Esta vez, el valor está por debajo del valor restante (11). Se coloca el valor del bit en 1 y se resta las unidades representadas al valor restante: 11-8 =3
- **Sexta columna (4):** El valor está por encima del valor restante. Se deja al bit en 0.
- **Séptima columna (2):** El valor está por debajo del valor restante. Se deja al bit en uno y se calcula la diferencia: 3-2=1
- **Octava columna (1):** El valor es igual al valor restante. Se coloca el bit en 1 y así se logró representar el valor 203 en binario

NOTA: Es importante tener en cuenta que el ejercicio fue hecho con 8 bits, los cuales pueden representar hasta 255 valores. Para valores mayores, se requerirán más bits.

De la tabla anterior, si hacemos el ejercicio de transformar cualquier número en Decimal a Binario, vemos que la transformación no es tan sencilla. Sin embargo, si tratamos de transformar de Binario, a Hexadecimal, vemos que agrupando los valores en binario es un proceso más sencillo. Volviendo al ejemplo de representar 203:

Valor BIN	1100	1011
Valor decimal	12	11
Valor HEX	C	B

NOTA: Recordar la relación entre los valores en Hexadecimal y decimal: A=10, B=11, C=12, D=13, E=14 y F=15.

Usando 4 bits es posible representar 2^4 valores (16 en total). De ese modo, grupos de cuatro bits pueden ser representados con un único carácter en hexadecimal.

Finalmente, otro sistema numérico comúnmente usado para la representación de llaves es BASE 64

- A' a la 'Z' → 26 símbolos
- 'a' a la 'z' → 26 símbolos
- '0' al '9' → 10 símbolos
- + → 1 símbolo
- / → 1 símbolo

Si queremos ver la relación con el binario, podemos tomar la siguiente tabla como ejemplo:

BASE 64	BINARIO	DECIMAL
A	000 000	0
Z	011 101	25
a	011 010	26
z	110 011	51
0	110 100	52
9	111 101	61
+	111 110	62
/	111 111	63

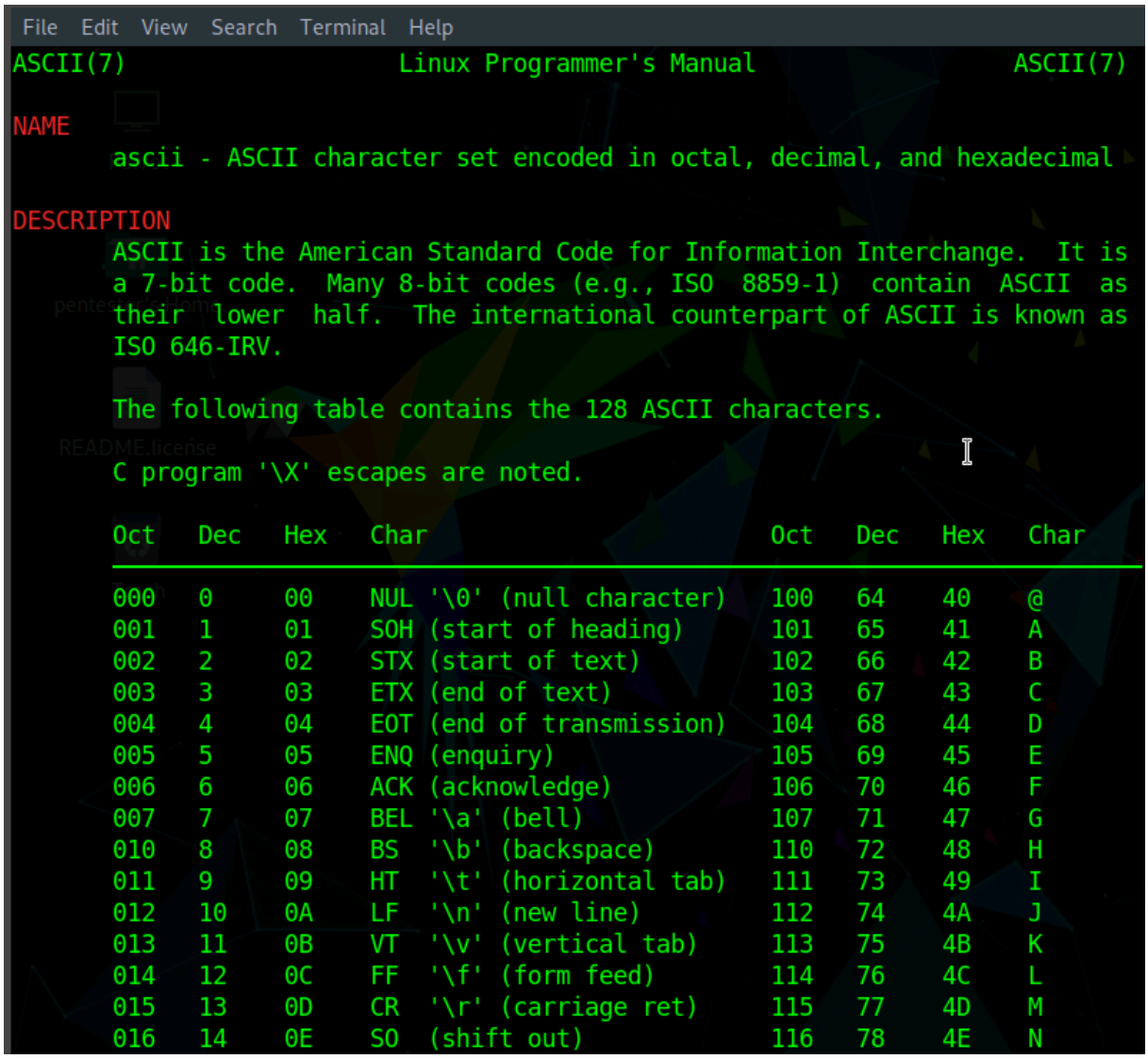
Es así que cobra mayor importancia saber el sistema numérico en el cual se está trabajando. Tomando la siguiente tabla como ejemplo:

BASE 2	001 100	000 000
BASE 64	M	A
HEX	C	0

El valor C en hexadecimal es igual al valor de M en BASE 64.

ASCII

Conjunto de caracteres de impresión y caracteres de control, los cuales no guardan una relación directa con el valor en binario. Un ejemplo de esto es, estando en una PC trabajando con Linux, podemos colocar el comando "man ascii" para ver lo que los desarrolladores indican respecto a la representación.



Fuente propia

De la imagen podemos apreciar que el valor A en Char (ASCII) es igual a 41 en Hexadecimal. A la hora de analizar información digital, algunos programas traducen el binario en ASCII a fin de poder distinguir si es que existe información visible en texto plano.

Investigación digital forense

Más conocido como “digital forensics”, es una ciencia que no solo investiga evidencia digital en computadoras, sino en diferentes tecnologías digitales (Reith, et al., 2002). Esta ciencia se basa en el uso de diversos métodos para la recuperación y presentación de evidencias. Para este fin, dicha evidencia solo puede ser considerada como tal siempre que esta sea admisible.

De lo visto previamente, la información digital es representada en un esquema de bits. Fuera del elemento de almacenamiento usado, las tramas de información están representadas con valores

binarios. Conociendo la estructura en la que se almacenan los bits, es posible interpretar la información.

Elementos como computadoras portátiles, videocámaras, teléfonos celulares, suelen contar con algún elemento interno de almacenamiento de datos, donde la información puede estar guardada en un dispositivo con formato volátil o permanente.

Ejemplos de equipos de almacenamiento:

- Computadoras (Computer forensics)
- Computadoras portátiles (laptops)
- Teléfonos y tablets (Mobile forensics)
- Memorias USB
- Sistemas de videovigilancia
- Sistemas de navegación
- Entre otros

Ejemplos de datos de donde se puede extraer la evidencia:

- Documentos digitales
- Bases de datos
- Programas y aplicaciones
- Archivos de imagen, audio y video
- Grabaciones de llamadas
- Tráfico de red (Network forensics)

Por ejemplo, cuando una persona sube una foto a una red social, la data de donde se puede extraer la evidencia es el archivo de imagen (información de la imagen misma, lugar donde se tomó la imagen, fecha y hora en la que se tomó la imagen, etc), mientras que el dispositivo que guarda la información es tanto el teléfono como los servidores donde se guarda la imagen en la red social.

Por otra parte, como se indicó previamente, no toda la data presente en un medio digital es relevante para la investigación. Lo que se busca obtener de la investigación es Evidencia Digital.

- **Evidencia digital**

Puede ser definida como cualquier información digital que contiene información confiable que puede afirmar o refutar una hipótesis en un incidente o crimen (Årnes, 2017, p. 7). Esta información, almacenada, transmitida o recibida en forma de bits, puede encontrarse en cualquier tipo de equipo electrónico. Lo más importante es que la evidencia recolectada debe tener el suficiente peso para poder demostrar un argumento.

El trabajo del investigador es en primer lugar el obtener la evidencia de forma confiable. Esto implica el poder obtener la evidencia sin alterar el elemento de prueba; en este caso, la unidad de almacenamiento. Sea cual sea el equipo electrónico, el investigador no puede alterar la información dentro del sistema de almacenamiento ya que así estaría contaminando la evidencia, haciéndola inadmisible.

En segundo lugar, el investigador debe buscar la forma adecuada de presentar la evidencia. Esto implica que, una vez obtenida la evidencia, presentarla de forma adecuada para que el público objetivo pueda entenderla. Esto debido a que un jurado o juez no necesariamente tiene la experiencia suficiente para entender las técnicas y métodos usados, así como el proceso de obtención de la evidencia.
La obtención de la evidencia no es un trabajo sencillo, dado que no todos los equipos han sido diseñados para ser investigados. Cuando la información no es considerada evidencia (no corrobora o niega la hipótesis dada), esta es considerada un artefacto.

- **Estado actual de la investigación digital forense**

La investigación digital forense (Digital Forensics) es una ciencia relativamente nueva que está creciendo considerablemente dado su importante uso tanto en el entorno privado como en lo penal. Investigaciones dentro de este ámbito pueden ayudar en investigaciones criminales referidas a crimen organizado, terrorismo, entre otros (Årnes, 2017, p. 1).

Sin embargo, el investigador debe estar preparado para cualquier tipo de información que pueda encontrar durante su investigación. El investigador puede estar expuesto a imágenes impactantes o indecentes (pornografía infantil, asesinatos, decapitaciones, etc). Esto puede darse incluso cuando la investigación no cubre estos temas. Es por ello que la terapia sicológica es importante.

3. ROLES Y PERSONAS INVOLUCRADAS EN LA INVESTIGACIÓN

Dentro de una investigación, diversas personas forman parte del proceso. Fuera del entorno en que se esté dando la investigación (dentro de una compañía privada o dentro de una investigación policial), hay ciertos personajes que son importantes de mencionar:

- Oficial del caso (Case Manager / Case Officer)
- Examinador/Analista del caso (Case Examiner/Analyst)
- Investigador de la escena del crimen (Crime Scene Investigator): Persona encargada de asegurar la escena del crimen y recolectar la evidencia.
- Testigo Experto (Expert witness): Experto llamado a juicio para explicar evidencia en caso sea necesario.

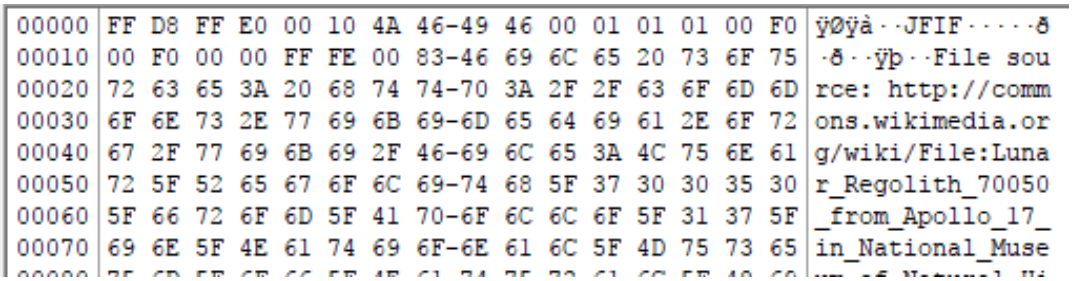
Cuando se asegura la escena del crimen, dentro de la recolección de evidencia una de las tareas a realizar es acceder al medio digital y recuperar la evidencia en físico. La persona encargada debe ser una persona competente a fin de poder obtener la data del medio digital sin modificarla. El reto del investigador empieza al entrar a la escena del crimen y determinar las circunstancias en las que se recibe la evidencia:

- **Energía:** ¿El equipo está prendido o apagado? ¿Está conectado a una fuente de energía?
- **Estado del equipo:** ¿El equipo está en óptimas condiciones? ¿La unidad de almacenamiento fue dañada por el investigado?
- **Acceso:** ¿Es posible acceder al contenido digital? ¿Se requiere de contraseñas para poder acceder? ¿El sistema está cifrado?

Para poder realizar su trabajo, el investigador cuenta con diversas herramientas de hardware y software para poder obtener la información sin alterar el medio digital. Las herramientas buscan ayudar a acceder al equipo sin producir cambios en el sistema de almacenamiento, al mismo tiempo que ayudan a realizar una copia digital del sistema**. Esta copia digital es la que será usada por el experto para realizar sus labores**, mientras que el equipo físico quedará en custodia a fin de que no sea accedido ni modificado por otras personas.

Una vez obtenida la información del sistema digital, uno o más examinadores se encargan de la búsqueda de evidencia digital. Ellos son los encargados de producir el reporte, infografía o testimonio que explique lo encontrado y cómo interpretarlo.

Para realizar su trabajo, el examinador cuenta con la copia digital obtenida de la escena del crimen, sobre la cual puede buscar y recabar información del sistema de archivos. Si bien la copia digital es idéntica a su contraparte original, el software de investigación forense se orienta a ver a gran detalle cada uno de los archivos:



00000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	F0	ÿØÿà··JFIF·····ð
00010	00	F0	00	00	FF	FE	00	83	46	69	6C	65	20	73	6F	75	·ð··ÿþ··File sou
00020	72	63	65	3A	20	68	74	74	70	3A	2F	2F	63	6F	6D	6D	rce: http://comm
00030	6F	6E	73	2E	77	69	6B	69	6D	65	64	69	61	2E	6F	72	ons.wikimedia.or
00040	67	2F	77	69	6B	69	2F	46	69	6C	65	3A	4C	75	6E	61	g/wiki/File:Luna
00050	72	5F	52	65	67	6F	6C	69	74	68	5F	37	30	30	35	30	r_Regolith_70050
00060	5F	66	72	6F	6D	5F	41	70	6F	6C	6C	6F	5F	31	37	5F	_from_Apollo_17_
00070	69	6E	5F	4E	61	74	69	6F	6E	61	6C	5F	4D	75	73	65	in_National_Muse

Fragmento de la representación hexadecimal de una imagen (Lallie, 2017)

La figura mostrada en la parte superior fue obtenida del programa Autopsy. Al analizar un archivo, podemos ver la información tanto en Hexadecimal (columna del medio) como una traducción en ASCII (columna derecha). La información en Hexadecimal es importante ya que permite ver con veracidad la

composición del archivo. La traducción en ASCII nos permite poder ver información presente en texto plano. Para la investigación, es necesario recurrir a la búsqueda de elementos clave a fin de poder distinguir la evidencia de los miles de artefactos que puedan estar presentes en la copia digital.

Finalmente, el examinador puede estar orientado a un campo en particular (equipos móviles, computadoras, transmisión sobre redes, etc.) por lo que en casos complejos esto puede convertirse en un trabajo multipartidario de personas. A su vez, debido a los sistemas actuales de almacenamiento que permiten salvar cantidades inmensas de data, el trabajo de investigación llega a tomar tiempos considerables.

RETO: Investigar lo que es el efecto CSI y cómo afecta la visión que se tiene de la investigación forense.

4. TIPOS DE INVESTIGACIÓN

Incluso trabajando en el ámbito civil, es posible que la compañía tenga información que pueda estar involucrada en delitos criminales. Siendo un investigador digital dentro de una empresa privada, cualquiera de los siguientes tipos de investigación puede presentarse:

Investigaciones criminales

Este tipo de investigaciones requieren de la presencia policial. Crímenes el día de hoy comprenden también el uso de dispositivos digitales para su ejecución: fraude, secuestro, asesinato, tráfico de drogas, corrupción, etc. Si bien estos casos son generalmente manejados por la policía, en ocasiones se requiere el apoyo de terceros expertos.

El trabajo del investigador en este tipo de casos suele ser de apoyo al fiscal, brindando tanto la evidencia como su testimonio de la evidencia encontrada. La investigación busca demostrar la actividad ilegal por lo que la fiscalía depende del experto.

Un ejemplo son las conversaciones telefónicas: no solo se trata de presentar la grabación digital, sino corroborar la identidad de las personas en el audio, como fue obtenida la evidencia, y confirmar que esta se encuentra de forma íntegra (sin modificar o recortar).

Investigaciones civiles

Si bien no es usual tener investigadores dentro de una empresa, algunas empresas suelen contratar investigadores independientes. A diferencia de la investigación criminal, la empresa hace un reclamo sobre un contrato.

En el caso de empresas, las disputas pueden darse por los contratos celebrados por ambas partes. Las causas para requerir investigadores en estos casos pueden ser muchas, pero cobran fuerza cuando los incidentes pueden terminar evidenciando actividades criminales. Por otro lado, estos contratos pueden haber sido celebrados con un Estado o Nación, o pueden formar parte de actividades de interés nacional. Por ejemplo: accidente aéreo, que requiere del análisis de la caja negra y las comunicaciones con la torre de control.

Investigaciones corporativas

En el ámbito interno de la empresa, las investigaciones van orientadas a los equipos electrónicos que la empresa provee a un empleado. El mal uso de los equipos suele estar ligado a conductas inapropiadas (visualización de contenido ajeno a las labores del empleado) o incluso a espionaje corporativo (venta de información a empresas rivales). Ante la sospecha de alguno de los indicios, es posible la incautación de los elementos electrónicos como parte de la investigación.

En compañías medianas y/o grandes, se suele tener un grupo de ciberseguridad (distinto al de Tecnologías de la Información o TI) que se encarga de ver Incidentes de Seguridad. Como parte de su trabajo se puede tener el monitoreo y análisis de equipos provistos por la compañía, así como también realizar investigaciones como parte de una orden judicial o investigación interna.

5. DEFINICIÓN DEL PROCESO Y ETAPAS EN LA INVESTIGACIÓN

El proceso de investigación puede verse de la siguiente forma (Årnes, 2017, p. 6):

Identificación	Recolección	Examinación	Análisis	Presentación

Esta estructura puede variar, sin embargo, estos cinco puntos engloban en esencia la investigación en general.

Identificación

En este paso se debe identificar la naturaleza y objetivo de la investigación: El argumento que se desea corroborar. Es posible que para tener claro el objetivo específico se tengan preguntas adicionales que ayuden a detallar lo que se busca finalmente. En este punto se deben considerar toda la información que pueda ser relevante para la investigación:

- Nombres e información de los sospechosos
- Palabras claves relacionadas al objetivo (dinero, fraude, algún lugar en particular)
- Posibles fuentes de evidencia (fotografías, videos, documentos, etc)

Esto también puede ser conocido como “Case Statement”, donde toda la información mencionada previamente se encuentra descrita en un documento. Este documento es distinto al de una orden expedida por un juez, en la que este da autoridad a las fuerzas del orden a arrestar a un sospechoso, como a requisar elementos que puedan ser evidencia potencial.

Sin importar el tipo de investigación (criminal, civil, o corporativa), este paso debe realizarse. La persona a cargo de la elaboración del Case Statement es la persona a cargo de la investigación. Este paso marca el desarrollo de toda la investigación. Es aquí donde se define la información relevante a buscar.

Recolección

Ya en la escena del crimen, se identifican los elementos que puedan contener evidencia digital (información relevante al caso): computadores, memorias, etc. Se deben seguir ciertos procedimientos para la obtención de estos elementos, los cuales serán requisados y puestos bajo lo que se conoce como **Cadena de Custodia**.

La Cadena de Custodia se establece una vez se decomisa un elemento digital. En ese punto, se designa a una persona responsable de la custodia del elemento digital a fin de registre y/o niegue el acceso de personas a la evidencia. A fin de no contaminar la evidencia, es preciso que el elemento digital no sea alterado por lo que la persona designada se hace responsable de que esto no ocurra hasta el juicio.

A fin de permitir la investigación de la data, es necesario realizar una copia forense de todo el software digital dentro de la unidad de almacenamiento requisado. Una copia forense es una copia completamente idéntica a la unidad original a nivel digital (bit por bit), y puede llegar a tomar bastante tiempo en realizarse. Las investigaciones son siempre realizadas sobre la copia y nunca sobre el elemento digital, salvo casos muy excepcionales.

RETO: Brindar un ejemplo en el que la investigación no puede realizarse con una copia forense necesariamente.

Finalmente, a fin de corroborar que la copia forense es idéntica a la información guardada en el medio digital, se suelen usar valores HASH tanto de la copia como de la unidad de almacenamiento y compararlas. Dado que ambas son copias idénticas, el valor HASH debe ser el mismo de igual modo.

RETO: Explicar qué significa HASH y cómo ayuda a distinguir que dos elementos digitales son iguales

Examinación

Búsqueda constante en cada una de las imágenes forenses de evidencia digital para el caso. Este proceso es el más arduo, donde el Case Statement juega un rol importante ya que da las pautas de qué es lo que se requiere buscar.

Los distintos softwares para la búsqueda en copias forenses ofrecen diversos mecanismos para facilitar este proceso: búsqueda por tipo de archivo, búsqueda sobre data borrada, búsqueda rápida de términos, etc. Al encontrar información potencialmente beneficiosa para la investigación, se les puede etiquetar con Marcadores.

Análisis

Tras haber colocado Marcadores sobre datos que pudieran ser evidencia digital, uno o más investigadores se encargarán de examinar más a fondo lo encontrado para poder distinguir la evidencia de simples artefactos. El distinguir evidencia va de la mano con el criterio del investigador: él o ella deberá indicar si un artefacto es relevante o no.

Si bien el proceso hasta este punto se muestra secuencial, puede darse el caso que alguno de los pasos descritos requiera de un segundo análisis o iteración. Por ejemplo: Volver a realizar la examinación a fin de encontrar más artefactos que puedan convertirse en evidencia.

Presentación

Es el punto clave de la investigación, donde se apela a las habilidades para comunicarse del investigador. El reporte a brindar debe ser entendible para el público objetivo, y debe responder las preguntas y objetivo planteados al inicio del proceso.

Se debe tener bastante cuidado de ser imparcial respecto a la información a declarar. Sin importar lo impactante que pueda ser la evidencia u otros artefactos encontrados, el profesionalismo debe primar a la hora de brindar la declaración. Lo que se debe buscar evitar tras presentar el reporte (sea cual sea el formato que se utilice) es la necesidad de llamar a un testigo experto, ya que implicaría de que el reporte no es capaz de transmitir la información por sí solo. El reporte debe ser capaz de sostenerse por sí mismo.

6. BIBLIOGRAFÍA

Årnes, A., 2017. *Digital Forensics.* Primera ed. s.l.:John Wiley & Sons.

Lallie, H., 2017. *Course: Digital Forensics.* Coventry: s.n.

Reith, M., Carr, C. & Gregg, G., 2002. An Examination of Digital Forensic Models. *International Journal of Digital Evidence,* 1(3), pp. 1-12.


ITU