
ÍNDICE

ACERCA DEL AUTOR	17
CAPÍTULO 1. INTRODUCCIÓN A FORENSE DIGITAL.....	19
1.1 CONCEPTOS BÁSICOS	19
1.1.1 Definición de forense digital	19
1.1.2 Investigaciones corporativas e investigaciones criminales	22
1.1.3 Diferencias entre E-Discovery y forense digital	23
1.1.4 Definición de evidencia digital.....	23
1.1.5 Principios internacionales de evidencia digital	24
1.1.6 Registros generados y registros almacenados por un ordenador.....	25
1.1.7 Cadena de custodia.....	26
1.1.8 Recopilación de evidencias digitales.....	26
1.1.9 El método científico	29
1.1.10 Mejor evidencia.....	30
1.1.11 Antiforense digital.....	31
1.2 GESTIÓN DE UN CASO FORENSE DIGITAL	31
1.2.1 Introducción	31
1.2.2 Recepción de la petición	32
1.2.3 Registro de un caso	32
1.2.4 Registro de la prueba documental	34
1.2.5 Fotografiar la prueba documental.....	36
1.2.6 Análisis de la prueba documental.....	36
1.2.7 Devolución de la prueba documental	36
1.2.8 Cierre del caso.....	36
1.3 PROCEDIMIENTO DE INVESTIGACIÓN	37
1.3.1 Importancia del procedimiento investigador.....	37
1.3.2 Pasos previos a la preparación de la investigación.....	37
1.3.3 Preparación de la investigación.....	40
1.3.4 Recopilación de evidencias digitales.....	42

1.3.5	Preservación de las evidencias	44
1.3.6	Análisis de las evidencias.....	44
1.3.7	Presentación de informes de la investigación.....	45
1.3.8	Presentación de informes de la investigación ante un tribunal	46
1.3.9	Cierre del caso	46
1.4	RAMAS DE LAS INVESTIGACIONES FORENSES DIGITALES	47
1.4.1	Introducción	47
1.4.2	Forense de ordenadores	47
1.4.3	Forense de dispositivos móviles.....	48
1.4.4	Forense de red	49
1.4.5	Análisis de malware	49
1.5	EL LABORATORIO FORENSE DIGITAL	50
1.5.1	Generalidades	50
1.5.2	Emplazamiento del laboratorio	51
1.5.3	Seguridad física del laboratorio.....	52
1.5.4	Tamaño y disposición del laboratorio	53
1.5.5	Normativa aplicable a un laboratorio forense digital	55
1.5.6	Departamentos dentro del laboratorio forense digital	55
1.6	EVIDENCIAS DIGITALES	56
1.6.1	Introducción	56
1.6.2	Objeto y campo de aplicación	57
1.6.3	Términos y definiciones	57
1.6.4	Preservación de la evidencia	60
1.7	ADQUISICIÓN DE EVIDENCIAS DIGITALES	61
1.7.1	Inteligencia digital y recolección de evidencias de un escenario.....	61
1.7.2	Retos de la recogida de evidencias digitales	63
1.7.3	Triage de evidencias en un escenario	64
1.7.4	Proceso de adquisición de evidencias digitales.....	69
1.7.5	Dispositivos apagados	72
1.7.6	Dispositivos encendidos	74
1.7.7	Obtención de evidencias de activos empresariales.....	77
1.7.8	Sistemas virtualizados	78
1.7.9	Extracción de evidencias mediante manipulación hardware.....	79
CAPÍTULO 2. SOPORTES DE ALMACENAMIENTO Y SISTEMAS DE FICHEROS.....		85
2.1	INTRODUCCIÓN	85
2.2	DISCOS DUROS.....	86
2.2.1	Interfaz de conexión	86
2.2.2	Estructura física	99
2.2.3	Estructura lógica.....	107
2.2.4	Volúmenes de disco	112

2.3	ALMACENAMIENTO FLASH.....	114
2.3.1	Tipos de dispositivos.....	114
2.3.2	Peculiaridades de los dispositivos de almacenamiento SSD.....	115
2.4	ALMACENAMIENTO EN SOPORTE ÓPTICO.....	123
2.5	ALMACENAMIENTO EN RED.....	123
2.6	ALMACENAMIENTO RAID.....	125
2.6.1	Generalidades.....	125
2.6.2	RAID 0.....	126
2.6.3	RAID 1.....	127
2.6.4	RAID 1E.....	127
2.6.5	RAID 2.....	128
2.6.6	RAID 3.....	129
2.6.7	RAID 4.....	129
2.6.8	RAID 5.....	130
2.6.9	RAID 6.....	130
2.6.10	RAID 01.....	131
2.6.11	RAID 10.....	132
2.6.12	RAID 30.....	133
2.6.13	RAID 100.....	134
2.6.14	RAID 50.....	135
2.6.15	Comparativa entre diferentes niveles de RAID.....	136
2.6.16	Otras configuraciones posibles.....	136
2.7	ARQUITECTURAS DE ALMACENAMIENTO NON-RAID.....	137
2.8	OBTENCIÓN DE EVIDENCIAS DE UN NAS.....	138
2.9	SISTEMAS DE FICHEROS.....	141
2.9.1	Introducción.....	141
2.9.2	Sistemas de ficheros en Microsoft Windows.....	142
2.9.3	Sistemas de ficheros en macOS.....	148
2.9.4	Sistemas de ficheros en Linux.....	154
2.10	PROCESO DE INICIO DE UN ORDENADOR.....	156
2.10.1	Arranque de un sistema operativo Microsoft Windows.....	157
2.10.2	Arranque de un sistema operativo Linux.....	158
2.10.3	Arranque de un sistema operativo macOS.....	159
CAPÍTULO 3. VIRTUALIZACIÓN Y SANDBOXING.....		161
3.1	VIRTUALIZACIÓN.....	161
3.1.1	Generalidades.....	161
3.1.2	Tipos de VM.....	161
3.1.3	Tipos de hipervisor.....	163
3.1.4	Contenedores.....	164
3.1.5	FUSE.....	166
3.1.6	Discos y unidades virtuales.....	167

3.2	FORENSE DE VM	177
3.2.1	Forense de hipervisores Tipo 2.....	177
3.2.2	Forense de hipervisores Tipo 1.....	180
3.3	SANDBOXING	180

CAPÍTULO 4. INTRODUCCIÓN A FORENSE DE MICROSOFT WINDOWS 185

4.1	INTRODUCCIÓN	185
4.1.1	Programa, proceso e hilo de control.....	186
4.1.2	Volatilidad de los artefactos forenses	186
4.1.3	Empleo de la consola del sistema y de <i>PowerShell</i> como herramientas de recopilación de artefactos forenses.....	188
4.1.4	Empleo de herramientas de terceros para la recopilación y análisis de artefactos forenses	192
4.2	ADQUISICIÓN DE SOPORTES DE ALMACENAMIENTO MASIVO	196
4.2.1	Obtención de imágenes de volúmenes de disco con AccessData FTK Imager.....	197
4.2.2	Obtención de imágenes de volúmenes de disco desde una distribución Live.....	197
4.3	ADQUISICIÓN DE EVIDENCIAS VOLÁTILES EN ENTORNOS WINDOWS	199
4.3.1	Variables de entorno del sistema	200
4.3.2	Fecha y hora del sistema	202
4.3.3	Información relativa al sistema	202
4.3.4	Histórico de comandos de la consola del sistema	203
4.3.5	Usuarios registrados en el sistema local.....	204
4.3.6	Información del dominio	207
4.3.7	Archivos abiertos.....	209
4.3.8	Programas, procesos y servicios.....	210
4.3.9	Conexiones de red	216
4.3.10	Tabla de enrutamiento interna	220
4.4	ANÁLISIS POST MORTEM DE EVIDENCIAS DIGITALES	221
4.4.1	Análisis “en muerto” y “en vivo”.....	221
4.4.2	Análisis de evidencias con OpenText EnCase Forensic.....	222
4.4.3	Análisis de evidencias con AccessData FTK	223
4.4.4	Nuix Workstation.....	224
4.4.5	Otras suites de análisis forense digital	224

CAPÍTULO 5. FORENSE DE LA MEMORIA RAM EN SISTEMAS WINDOWS . 229

5.1	INTRODUCCIÓN	229
5.1.1	Generalidades	229
5.1.2	Forense de memoria	230
5.1.3	Artefactos forenses presentes en la memoria RAM	231
5.1.4	Memoria física y memoria virtual	232
5.1.5	Archivos de volcado de memoria RAM.....	234
5.1.6	Archivos de hibernación.....	237

5.2	ADQUISICIÓN DE MEMORIA RAM.....	240
5.2.1	Introducción	240
5.2.2	Volcado del contenido completo de la RAM.....	241
5.2.3	Volcado de memoria utilizando pmem.....	244
5.2.4	Archivos de paginación e hibernación	246
5.2.5	Volcado de la memoria RAM tras un fallo del sistema operativo.....	247
5.2.6	Adquisición de memoria de máquinas virtuales.....	249
5.2.7	Adquisición de memoria de contenedores.....	250
5.2.8	Recolección de memoria de sistemas remotos	251
CAPÍTULO 6. ANÁLISIS DE LÍNEAS TEMPORALES		257
6.1	INTRODUCCIÓN	257
6.1.1	Importancia de la elaboración de una línea temporal.....	257
6.1.2	Dificultades en la generación de líneas temporales.....	258
6.1.3	Punto de partida de una investigación.....	258
6.1.4	Proceso de análisis de una línea temporal.....	260
6.1.5	Predicción en el análisis de líneas temporales.....	261
6.1.6	Herramientas para la confección de líneas temporales	264
6.2	ANÁLISIS DE ARTEFACTOS FORENSES EN WINDOWS	267
6.2.1	Evidencias de descarga de archivos	267
6.2.2	Evidencias de ejecución de programas.....	270
6.2.3	Evidencias de archivo eliminado o conocimiento de archivo	275
6.2.4	Evidencias de actividad de red y de ubicación física	279
6.2.5	Evidencia de apertura de archivos/carpetas.....	282
6.2.6	Evidencias de utilización de cuentas de usuario	286
6.2.7	Evidencias de conexión de dispositivos USB	289
6.2.8	Evidencias de utilización del navegador	293
6.3	CREACIÓN Y ANÁLISIS DE LÍNEAS TEMPORALES	296
6.3.1	Triaje de la línea temporal del sistema de ficheros.....	296
6.3.2	Creación y análisis de una línea temporal del sistema de ficheros.....	301
6.3.3	Creación y análisis de una línea temporal a partir de un volcado de memoria RAM.....	306
6.3.4	Creación de una Super Timeline	307
6.3.5	Creación de una Super Timeline dedicada	311
6.3.6	Triaje rápido de artefactos forenses.....	312
6.3.7	Filtrado de una Super Timeline	314
6.3.8	Análisis de una Super Timeline.....	317
CAPÍTULO 7. ARCHIVOS DE LOG.....		323
7.1	INTRODUCCIÓN	323
7.1.1	Archivo de log de eventos	323
7.1.2	Agregación de logs.....	324
7.1.3	Monitorización de archivos de log.....	325
7.1.4	Importancia de los archivos de log de eventos de seguridad	326

7.2	GESTIÓN DE ARCHIVOS DE LOG	326
7.2.1	Gestión de archivos de log de seguridad	327
7.2.2	Sistema centralizado de archivos de log.....	328
7.3	ESTIMACIÓN DE GENERACIÓN DE ARCHIVOS DE LOG	328
7.3.1	Eventos por segundo	329
7.3.2	Generación normal y picos de EPS.....	329
7.3.3	Volumen de los archivos de log.....	330
7.4	TIPOS DE ARCHIVOS DE LOG	330
7.5	ARCHIVOS DE LOG GENERADOS EN ENDPOINTS EN CIBERSEGURIDAD.....	332
7.5.1	Archivos de log de Eventos de Windows.....	332
7.5.2	Archivos de log de Linux.....	332
7.5.3	Archivos de eventos de dispositivos iOS.....	333
7.5.4	Archivos de eventos de dispositivos <i>Android</i>	334
7.5.5	Archivos de log de interés para incorporar al SIEM.....	334
7.6	GESTIÓN DE ARCHIVOS DE LOG DE EDR	335
7.7	GESTIÓN DE ARCHIVOS DE LOG DE FIREWALLS	335
7.8	RECOLECCIÓN DE ARCHIVOS DE LOG CON SYSLOG	336
7.9	TÉCNICAS DE ANÁLISIS DE ARCHIVOS DE LOG.....	341
7.10	PROCESADO DE ARCHIVOS DE LOG.....	341
7.10.1	Flujo de procesado de los archivos de log.....	342
7.11	ANÁLISIS DE ARCHIVOS DE LOG EMPLEANDO UN SIEM	343
7.12	SINCRONIZACIÓN HORARIA ENTRE DISPOSITIVOS.....	343
7.13	LOS ARCHIVOS DE LOG DESDE UN PUNTO DE VISTA LEGAL.....	345
7.13.1	Procesado de archivos de log conforme a la legislación estadounidense... 345	
7.13.2	Archivos de log conforme a la legislación española	346
CAPÍTULO 8. FORENSE DE RED.....		347
8.1	DEFINICIÓN DE FORENSE DE RED	347
8.2	HERRAMIENTAS DE MONITORIZACIÓN DE RED.....	348
8.2.1	Capturador de paquetes	348
8.2.2	Analizador de paquetes	348
8.2.3	Monitorización del flujo de paquetes	349
8.2.4	Monitor de interfaz.....	350
8.2.5	Monitor de rendimiento.....	351
8.2.6	Registros de eventos del sistema y su gestión.....	351
8.3	ANÁLISIS DE TRÁFICO DE RED.....	352
8.3.1	Cabecera del paquete.....	352
8.3.2	Payload.....	353
8.3.3	Trailer	354
8.4	INVESTIGANDO EL TRÁFICO DE RED	354
8.4.1	Ventajas de investigar el tráfico de red.....	354

8.4.2	Acceso ilícito a la red objetivo	355
8.4.3	Fuentes de evidencias para forense de red	356
8.4.4	Origen del ataque	356
8.4.5	Atribución a partir de evidencias forenses de red	357
8.4.6	Forense en redes inalámbricas.....	358
8.5	HERRAMIENTAS FORENSES DE RED	361
8.5.1	Herramientas más habituales en forense de red	361
8.5.2	Recopilación y análisis de artefactos forenses empleando la consola del sistema	364
8.6	FORENSE DE PÁGINAS WEB Y URL.....	366
8.6.1	Copia forense de sitios web.....	366
8.6.2	Servicios recortadores de URL.....	366
8.6.3	Resolución estática de servidores C2	366
8.6.4	Domain Generation Algorithm.....	366
8.6.5	Fast-Flux Service Networks	368
8.7	CORREO ELECTRÓNICO.....	369
8.7.1	Protocolos y servicios de correo electrónico	369
8.7.2	Cabecera de un correo electrónico	373
8.7.3	Cuerpo de un correo electrónico	376
8.7.4	Importancia de la gestión de registros electrónicos.....	377
8.7.5	Delitos cometidos empleando el correo electrónico.....	377
8.7.6	Delitos cometidos en salas de chat.....	379
8.7.7	Procedimiento para investigar delitos cometidos utilizando el correo electrónico y las salas de chat.....	379
8.7.8	Análisis de correos electrónicos	387
CAPÍTULO 9. FORENSE DE BASE DE DATOS.....		391
9.1	INTRODUCCIÓN	391
9.2	BREVES NOCIONES DE BASES DE DATOS Y SQL.....	391
9.3	IMPORTANCIA DEL FORENSE DE BASES DE DATOS	395
CAPÍTULO 10. FORENSE EN LA NUBE.....		397
10.1	INTRODUCCIÓN A LA COMPUTACIÓN EN LA NUBE	397
10.2	TIPOS DE SERVICIOS DE COMPUTACIÓN EN LA NUBE	399
10.2.1	IaaS.....	400
10.2.2	PaaS.....	400
10.2.3	SaaS.....	401
10.2.4	Separación de responsabilidades en la nube.....	401
10.3	MODELOS DE DESPLIEGUE EN LA NUBE	403
10.3.1	Nube privada	404
10.3.2	Nube híbrida	405
10.3.3	Nube comunitaria	406
10.3.4	Nube pública	407

10.4	INTRODUCCIÓN AL FORENSE EN LA NUBE	409
10.4.1	Definición	409
10.4.2	Ámbito de aplicación	410
10.4.3	Delitos en la nube	412
10.4.4	Agentes implicados en una investigación de forense en la nube	413
10.4.5	Procedimiento forense en la nube	414
10.5	RETOS QUE SE PRESENTAN EN LAS INVESTIGACIONES DE FORENSE EN LA NUBE	416
10.5.1	Arquitectura e identificación	416
10.5.2	Recolección de datos	418
10.5.3	Archivos de log	420
10.5.4	Legales	420
10.5.5	Análisis	422
10.5.6	Gestión de roles	422
10.5.7	Estándares	423
10.5.8	Adiestramiento	423
10.5.9	Empleo de técnicas antiforenses	423
10.5.10	Respuesta a incidentes	423
10.6	INVESTIGACIÓN FORENSE DE SERVICIOS DE ALMACENAMIENTO EN LA NUBE	424
10.6.1	Introducción	424
10.6.2	Dropbox	425
10.6.3	Google Drive	430

CAPÍTULO 11. FORENSE DE DISPOSITIVOS

MÓVILES E IOT	435	
11.1	INTRODUCCIÓN	435
11.1.1	Forense de dispositivos móviles	435
11.1.2	Forense de teléfonos móviles	435
11.1.3	Ciberdelitos y ciberamenazas en dispositivos móviles	436
11.1.4	Actividades delictivas que pueden realizarse desde un dispositivo móvil. 437	
11.2	TIPOS DE DISPOSITIVOS MÓVILES	438
11.2.1	Generalidades	438
11.2.2	Teléfonos móviles estándar	438
11.2.3	PDA	439
11.2.4	Reproductores multimedia	440
11.2.5	Smartphones	441
11.2.6	Tabletas y phablets	442
11.3	IOT	443
11.3.1	Introducción	443
11.3.2	Forense de dispositivos IoT	444

11.4	REDES DE ACCESO CELULAR.....	446
11.4.1	Elementos de una red celular.....	446
11.4.2	Redes celulares de datos.....	447
11.4.3	Telefonía 2G.....	448
11.4.4	Telefonía 3G.....	448
11.4.5	Telefonía 4G.....	449
11.4.6	Telefonía 5G.....	449
11.5	EL DISPOSITIVO MÓVIL.....	451
11.5.1	Hardware, sistema operativo y aplicaciones de un dispositivo móvil..	451
11.5.2	ME.....	453
11.5.3	UICC.....	454
11.5.4	Medidas de seguridad en la UICC.....	455
11.5.5	Codificación de la UICC.....	456
11.5.6	Autenticación Ki.....	456
11.5.7	Estructura de ficheros de la UICC.....	457
11.6	INTERVENCIÓN DE UN DISPOSITIVO MÓVIL.....	458
11.6.1	Aislamiento de redes.....	458
11.6.2	Anulación de códigos de protección.....	459
11.6.3	Cables de alimentación y datos.....	459
11.6.4	Dispositivos desconectados.....	459
11.7	ARTEFACTOS FORENSES DE INTERÉS EN UN TELÉFONO MÓVIL.....	460
11.7.1	Información proporcionada por la UICC.....	460
11.7.2	Información almacenada en el smartphone.....	460
11.7.3	Información almacenada por el operador de telefonía.....	462

ACERCA DEL AUTOR

Mario Guerra Soto es Ingeniero de Telecomunicación por la Universidad de Cantabria (UC). Durante siete años trabajó en el Mando Conjunto de Ciberdefensa como DFIR, *threat hunter*, analista de ciberinteligencia, y analista de *malware*. Es Máster en Seguridad de Tecnologías de Información y Comunicación por la Universitat Oberta de Catalunya (UOC), y Máster en Análisis de Evidencias Digitales y Lucha contra el Cibercrimen por la Universidad Autónoma de Madrid (UAM). Dispone de las certificaciones en ciberseguridad GCFA, GCTI, GREM, CEH, CHFI, CND, CCPA, CASA y KAPE. Además, ha realizado otros cursos relacionados con la ciberseguridad, como el de Cyber Security Professional por la NATO School of Oberammergau, y el Curso de Especialidades Criptológicas por el Centro Criptológico Nacional (CCN). Ha colaborado como ponente en diferentes CON nacionales como RootedCON, Cybercamp, C1b3rwall, IntelCon, Hackron y TACS. Colabora como docente en el programa de postgrado de la UAM y de la Universidad de Salamanca (USAL).

1

INTRODUCCIÓN A FORENSE DIGITAL

1.1 CONCEPTOS BÁSICOS

1.1.1 Definición de forense digital

La Ciencia Forense juega un papel fundamental en las investigaciones criminales. Debe entenderse como una aproximación multidisciplinar que permite juntar todo tipo de evidencias en una investigación. Normalmente, durante el transcurso de una investigación, deberán aplicarse los principios y metodologías de diferentes disciplinas científicas para la presentación de evidencias ante un tribunal.

En 1910, el francés Edmond Locard establece el primer laboratorio forense policial en Lyon. Pasa además a la historia de la ciencia forense por enunciar el denominado **Principio de Locard** “*Todo contacto deja una huella*”. Es decir, que la presencia del autor de los hechos en la escena del crimen conlleva una transferencia de evidencias, pues el criminal deja rastros en la escena del crimen, pero también lleva consigo evidencias que demuestran su presencia en dicho lugar. Dicho de otra forma, las acciones físicas dejan evidencias físicas en el mundo físico; las acciones digitales dejan evidencias digitales en el mundo digital.

Actualmente, entre las diferentes ramas de la Ciencia Forense destacan: Toxicología, Psicología, Podología, Patología, Odontología, Lingüística, Geología, Entomología, Ingeniería, Análisis de ADN, Botánica, Arqueología, Antropología, Balística y Digital.

Podría definirse Forense Digital como la disciplina que combina elementos legales, informáticos y de telecomunicaciones para obtener y analizar evidencias

digitales (Ej. Ordenadores, tráfico de red, dispositivos de almacenamiento, teléfonos móviles, *smartphones*, *wearables*) de modo que sean admisibles ante un tribunal. Si bien a primera vista su principal aplicación sería la investigación de cibercrímenes, el nivel de digitalización de la sociedad moderna provoca que, en la mayoría de los casos, sea necesario el análisis de una o más evidencias digitales.

A su vez, Forense Digital puede subdividirse en diferentes ramas: forense de ordenadores, análisis forense de información, forense de bases de datos, forense de red, forense de dispositivos móviles y forense de vídeo/audio.

Uno de los aspectos más complejos de las investigaciones forenses digitales consiste en determinar el papel que desempeña el dispositivo en el incidente objeto de estudio. En general, los dos roles que puede adoptar el dispositivo son:

- La herramienta empleada para realizar la acción objeto de estudio, es decir, el *arma del crimen*.
- El objetivo de la acción objeto de estudio, es decir, el *cadáver*.

Un ejemplo que permite ilustrar la clasificación anterior sería un escenario en el que un agente malicioso consigue tomar el control del equipo de un usuario de una organización. El atacante podría utilizar ese equipo bajo su control para intentar acceder a un servidor de ficheros dentro de dicha organización y exfiltrar información (entiéndase por exfiltrar la extracción ilícita de información sin conocimiento de su legítimo propietario). En este escenario, el equipo controlado por el atacante es la herramienta, mientras que el servidor es el objetivo. No obstante, si el atacante hubiese exfiltrado información del equipo corporativo bajo su control, este equipo sería a la vez la herramienta y el objetivo del ataque.

El dispositivo debe ser considerado la escena del crimen digital, pues contiene las evidencias digitales que permitirán al investigador forense digital determinar cuándo (*When*) y cómo (*How*) el ataque tuvo lugar. Adicionalmente, podrían obtenerse evidencias que demostraran quién (*Who*), qué (*What*), dónde (*Where*) y por qué (*Why*) realizó el ataque. Las famosas 5WH a obtener en toda investigación forense.

En forense digital, separar la parte legal de la parte técnica puede ser en ocasiones complicado. Los avances técnicos alteran los tipos de evidencia que pueden ser obtenidos; las modificaciones en las leyes afectan el modo en el que las evidencias pueden ser obtenidas y si esas evidencias serán admisibles ante un tribunal.

El reconocimiento de la importancia de las investigaciones forenses digitales tiene su primer hito con la creación en 1984 por el FBI del CART (*Computer Analysis and Response Team*).

La capacidad de determinar con prontitud el impacto de un ataque, la identidad del atacante y sus posibles objetivos son una muestra de los beneficios aportados a una organización por la disciplina de forense digital. Otros beneficios adicionales serían el mantenimiento del estado operacional de sistemas informáticos y redes, además de poder facilitar a las FCSE (Fuerzas y Cuerpos de Seguridad del Estado) la información necesaria de las actividades maliciosas llevadas a cabo por empleados maliciosos haciendo uso de los equipos y redes corporativas.

Existe cierta controversia a la hora de determinar qué es un ciberdelito. En general, suele considerarse que una actividad delictiva es un ciberdelito cuando solo pueda cometerse empleando ordenadores o comunicaciones digitales. Es decir, acceso ilegal a sistemas informáticos, distribución de *malware*, manipulación de aplicaciones informáticas, fraude en apuestas ilegales, ataques DoS (*Denial of Service*), *webjacking*, contrabando de identidades digitales y uso ilegal de equipos de telecomunicaciones contra dispositivos en red (Ej. *Eavesdropping*, creación de identidades digitales fraudulentas).

Por un lado, el atacante podría haber utilizado el dispositivo como herramienta para la comisión del delito (Ej. Acceder a un sistema remoto, envío de mensajería digital, videoconferencia). Por otro, el dispositivo pudiera ser el objetivo del ataque (exfiltración, modificación o borrado de información). Por tanto, el dispositivo será la escena del delito en la cual hay que preservar las evidencias (Ej. Archivos de *log*, aplicaciones instaladas, línea temporal de actividades). Algunas de estas evidencias (Ej. Memoria RAM, tablas ARP, conexiones de red) tendrán un elevado grado de volatilidad (es decir, que su grado de permanencia con respecto del tiempo es limitada), debiendo ser por tanto obtenidas con la mayor presteza posible o desaparecerían. En cambio, otras evidencias (Ej. Archivos en disco duro, soporte óptico) tendrán un grado de volatilidad menor o, dicho de otro modo, su grado de persistencia será mayor.

Resulta por tanto necesario dentro de una organización que exista un equipo con las capacidades técnicas y recursos necesarios para poder hacer frente a un incidente concreto. La seguridad informática puede ser vista como un triángulo donde uno de sus lados lo constituye la detección y respuesta a intrusiones, siendo sus otros dos lados el análisis de vulnerabilidades y las investigaciones informáticas.

La detección de intrusiones, el análisis de vulnerabilidades y las investigaciones informáticas están directamente relacionadas con diferentes controles de seguridad que pueden ser implementados en una organización. El análisis de vulnerabilidades identifica los fallos a corregir o mitigar; la detección y respuesta a intrusiones representan controles de investigación y compensación; y las investigaciones intentan analizar el origen y establecer los pertinentes controles preventivos.