INCIDENTES DE SEGURIDAD Y FORÉNSICA DIGITAL

CURSO TEÓRICO-PRÁCTICO

DIRIGIDO A: Estudiantes, profesionales y técnicos superiores en informática, computación, sistemas, telecomunicaciones o área afín, así como gerentes de sistemas, gerentes de seguridad (CISO), miembros de centros de respuesta CSIRT/CERT, administradores de sistemas, consultores, analistas, desarrolladores, programadores, pentesters, peritos informáticos, auditores, abogados, criminalistas, policías, fiscales y jueces que se ocupan de delitos informáticos.

REQUISITOS DESEABLES: Conocimientos en el área de telecomunicaciones, redes y protocolos, especialmente TCP/IP. Conocimientos de computación (hardware, software, programación) y de sistemas operativos (Windows, Linux, Mac, Android). Conocimientos de seguridad (vulnerabilidades, ataques, hacking, malware, criptografía, hashing). Conocimiento instrumental del idioma inglés.

MODALIDAD Y DURACIÓN: El curso se realiza a distancia o de forma semipresencial y se utiliza un DVD como material de apoyo, el cual se puede obtener en físico o descargarlo de Internet. En el DVD se encuentran las presentaciones de las clases, hiperenlaces, libros electrónicos, guías para las experiencias prácticas, así como los programas y herramientas para efectuar dichas prácticas. La metodología utilizada combina clases y lecturas con experiencias prácticas. El participante avanza a su propio ritmo, de acuerdo a su disponibilidad de tiempo. Se pueden realizar consultas en línea (Skype, WhatsApp, teléfono) y por correo electrónico. La duración del curso es de 9 semanas y se requieren unas 32 horas de dedicación (entre teoría y práctica) para completar el adiestramiento. Se entrega un certificado de aprobación.

EQUIPAMIENTO: El participante debe disponer de PC o laptop de buenas prestaciones y acceso a Internet. Las imágenes forenses que se usan para ciertas prácticas son de varios GB y se deben descargar de Internet. Para las prácticas (opcionales) de *Forénsica en Dispositivos Móviles* se requiere un teléfono celular con sistema operativo Android y que eventualmente se pueda "rootear".

DOCENTE: Ing. Vincenzo Mendillo - Profesor Titular (UCV - USB - UNIMET - UCAB)

- Ingeniero Electricista (Especialidad: Telecomunicaciones) - Universidad Central de Venezuela
- Master of Science in Electronics - University of Southampton (UK)
- Live Senior Member No. 6008791 del IEEE - Institute of Electrical and Electronics Engineers
- Miembro No. 11850 del Colegio de Ingenieros de Venezuela (CIV)
- Miembro de CriptoRed - Red de Criptografía y Seguridad de la Información
- Coordinador del Diplomado STIT en Seguridad en Tecnología Informática y Telecomunicaciones.
- Primer presidente y miembro fundador de ASOVESINFO (Asociación Venezolana de la Seguridad de la Información)

BENEFICIOS Y LOGROS PARA EL PARTICIPANTE: Este curso constituye una buena oportunidad para prepararse profesionalmente en un campo laboral en fuerte crecimiento, donde hay una alta demanda y excelente remuneración. El participante adquiere experticia técnica, operativa y legal, junto con competencias, capacidades y destrezas para:

- Preparar un plan de gestión de incidentes de seguridad e investigar ataques de denegación de servicio (DoS), penetración de intrusos, infección con malware, etc., pudiendo informar y describir los hechos ocurridos y estableciendo responsabilidades a través de la auditoría del incidente.
- Llevar a cabo investigaciones forenses mediante una metodología basada en las mejores prácticas y ateniéndose a la normativa nacional e internacional, como parte de respuesta a incidentes, investigaciones internas y litigios civiles o penales.
- Interactuar con los diferentes tipos de personas que intervienen en un caso, como abogados, fiscales, policías, jueces.
- Conocer los aspectos legales, morales y éticos de una investigación forense, respetando los códigos de ética profesional.
- Utilizar el procedimiento técnico y procedimental más apropiado para decomisar la evidencia física y digital de forma que sea aceptada en un juicio civil o penal.
- Crear la imagen forense con su código hash de discos duros, dispositivos móviles y memoria RAM, a fin que los datos puedan ser analizados posteriormente sin comprometer su integridad.

- Manejar herramientas especializadas para crear la imagen forense de equipos y dispositivos (discos duros, memoria USB, memoria RAM, teléfonos inteligentes, etc.), así como para la extracción de evidencias.
- Realizar un análisis a fondo del Registro de Windows y de los distintos logs de actividades.
- Buscar evidencia que haya sido manipulada mediante técnicas antiforenses, tales como criptografía y esteganografía.
- Recuperar datos borrados en dispositivos USB y en disco duro, ya sea por accidente o intencionalmente.
- Detectar la infección de malware mediante el análisis de la memoria RAM.
- Redactar el informe pericial basándose en buenas prácticas y normas nacionales e internacionales.
- Prepararse para obtener las certificaciones internacionales de más alta reputación, tal como CHFI (*Computer Hacking Forensic Investigator*), CCFP (*Certified Cyber Forensics Professional*), SANS (GIAC *Computer Forensics*), CSFA (*CyberSecurity Forensic Analyst),* CCFE (*Certified Computer Forensics Examiner*), CCE (*Certified Computer Examiner*).

FECHA Y COSTO: El curso se abre 2 veces al año. Los estudiantes universitarios inscriben y pagan el curso en su respectiva universidad. Los demás participantes pueden pagar el curso de distintas formas. Los detalles se encuentran aquí.

EVALUACIÓN: A lo largo del curso el participante deberá realizar una serie de actividades por su cuenta. La realización con esmero, dedicación y constancia de las actividades planificadas, determinará el nivel de conocimientos, destrezas y competencias que el participante habrá adquirido al completar el curso. La evaluación del aprendizaje se realiza básicamente mediante cuestionarios y exámenes parciales (tests) sobre la teoría e informes sobre las prácticas. Para aprobar el curso se requiere que la nota final sea de al menos 50%.

- 4 cuestionarios sobre las 4 partes de teoría: 25% de la nota final
- 4 informes sobre 4 experiencias prácticas: 50% de la nota final
- 2 exámenes parciales (tests) sobre la teoría: 25% de la nota final

El examen parcial #1 (test #1) consta de 40 preguntas de opción múltiple sobre la Parte 1 y la Parte 2 del Contenido Programático. El examen parcial #2 (test #2) consta de 40 preguntas de opción múltiple sobre la Parte 3 y la Parte 4 del Contenido Programático. El tiempo disponible para cada examen es de 60 minutos. Luego de finalizar el examen, es posible ver las respuestas correctas si se ha contestado bien al menos el 50% de las preguntas. Se puede repetir el examen hasta 10 veces y saldrán nuevas preguntas. La primera vez puede resultar difícil obtener una alta calificación, por lo que hay que estudiar y volver a intentarlo. Los resultados del examen se guardan en una base de datos, siempre que se haya contestado bien al menos el 50% de las preguntas. De esta forma se puede hacer el seguimiento del desempeño a lo largo del tiempo. Para efectuar los exámenes, hay que registrarse previamente en línea con su nombre, apellido, email, login y password. Además se debe conocer la contraseña de acceso al sistema, la cual debe solicitarse al profesor.

Se otorgará la mención honorífica a los participantes que hayan aprobado los exámenes parciales con un promedio de al menos el 80% y que hayan entregado 6 o más informes.

INTRODUCCIÓN AL CURSO:
La utilización de sistemas informáticos y redes como Internet se ha incrementado espectacularmente, al grado de convertirse en un elemento indispensable para el funcionamiento de entes públicos y privados, así como para el quehacer diario de muchas personas.

Actualmente la mayor parte de la información se transmite, se procesa y se almacena en formato digital utilizando medios electrónicos. Tal situación lleva consigo la aparición de novedosas y variadas formas de ataques y delitos informáticos, afectando la confidencialidad, integridad y autenticidad de la información.

La relativa facilidad con la cual se puede manipular la información digital requiere que se implanten medidas de protección apropiadas y que se investiguen a fondo los incidentes de seguridad que ocurren (¿quién? ¿qué?, ¿cómo? ¿dónde? ¿cuándo? ¿porqué?).

Los hackers son frecuentemente los causantes de incidentes de seguridad de todo tipo. Su motivación se debe a distintas razones, por ejemplo curiosidad, saltarse las medidas de seguridad, desafío, beneficio económico. También suelen actuar por diversión, conseguir estima entre sus pares, creencias políticas, ideológicas o religiosas.

Pero en ciertos casos el causante de incidentes está dentro de la propia organización y sus actividades presentan las siguientes características resaltantes:

- Son conductas típicas de delincuentes de "cuello blanco", ya que sólo individuos con ciertos conocimientos técnicos o profesionales pueden llegar a cometerlas.
- Son acciones de oportunidad, ya que se aprovechan ciertas brechas y debilidades que aparecen en el complejo mundo de las TIC.
- Suelen ser muy sofisticados y son bastante comunes en el ámbito bancario y contra los clientes.
- Frecuentemente causan graves pérdidas económicas, ya que casi siempre producen dividendos al malhechor y a sus socios.
- Son muchos los casos y pocas las denuncias, ya que los entes afectados no se atreven a demandar a estos sujetos debido al posible daño a su reputación. A menudo sólo se conforman con su renuncia, así que el individuo queda libre para continuar con sus fechorías en otra empresa.
- Si obtiene éxito la primera vez, el malhechor usualmente vuelve a intentarlo y puede ser descubierto (aunque por lo general el descubrimiento es casual).

La Forénsica Digital o *Informática Forense* (en inglés Computer Forensics) es una novedosa especialidad en el entorno digital y se ocupa principalmente de investigar incidentes de seguridad, actividades sospechosas, delitos y muchos otros hechos vinculados a las tecnologías de la información y las comunicaciones (TIC), por ejemplo penetración de intrusos, hackeo de sitios web, infección por malware, ataque de ransomware, delitos financieros, fraude contable, desfalco, falsificación, malversación, lavado de dinero, robo de identidad, fuga de información, espionaje industrial, abuso de privilegios, pirateo de software, tráfico de drogas, pornografía infantil, secuestro, acoso, chantaje. En el sector de la inteligencia y contrainteligencia militar, ayuda a combatir el terrorismo y a los enemigos, al extraer información residente en teléfonos inteligentes, laptops y otros dispositivos secuestrados. En el sector tributario, ayuda a encontrar pruebas de evasión de impuestos y de cuentas bancarias en "paraisos fiscales". En casos de litigios personales y divorcios, ayuda a encontrar pruebas de infidelidad.

En la Forénsica Digital se utilizan técnicas y herramientas de punta para identificar, preservar, analizar y presentar evidencias, las cuales muchas veces son requeridas en un proceso judicial. Al extraer las evidencias, se debe resguardar su integridad mediante una función hash y una adecuada cadena de custodia. El investigador o perito forense debe poseer conocimientos de computación (hardware, software, programación), de sistemas operativos operativos y de seguridad (vulnerabilidades, ataques, hacking, malware, criptografía, hashing). Además debe saber de la legislación nacional e internacional relacionada a delitos informáticos y respetar el código de ética profesional.

El espectro de acción de la Forénsica Digital es muy amplio y abarca varias ramas más específicas. Por ejemplo, la Forénsica de Redes (Network Forensics) se ocupa de la captura y el análisis del tráfico en redes para casos de intrusiones y ataques de denegación de servicio (DoS), así como reconstruir sesiones de chat, de correo electrónico, transferencia de archivos, fuga de información, etc. Se trata de información volátil y dinámica, ya que el tráfico de red se transmite y luego se pierde. A menudo pueden quedar rastros en los logs de equipos (ej. servidor, router, firewall, IDS).

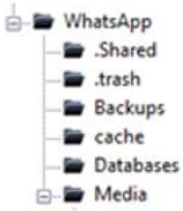
Por lo general se asume que todo equipo informático contiene potencialmente evidencia digital. Por eso, una vez que se ha decomisado o incautado un equipo, se lleva a un laboratorio para allí extraer y analizar los datos. A este procedimiento se le denomina a veces *forénsica post-mortem*, para distinguirla de la *forénsica en vivo*, que se realiza cuando el sistema se encuentra encendido o no se puede apagar por diversas razones, por ejemplo si se trata de un servidor en un data center. Pero ya sea que se vaya a apagar o no el equipo, se puede hacer un volcado de la memoria RAM para luego analizarla a fondo. Es lo que se conoce como Memory Forensics. A este respecto hay que considerar que hay dos tipos de datos: (a) datos volátiles en la memoria RAM y en archivos temporales, que se pierden si el equipo se apaga, por ejemplo la lista de los procesos en ejecución y (b) datos no volátiles en discos duros y dispositivos USB que no se pierden cuando se apaga el sistema.

Cuando se trata de casos donde están involucrados dispositivos móviles, se trata de Mobile Device Forensics, que se ocupa de extraer, recuperar y analizar las evidencias que se encuentran en este tipo de dispositivos, utilizando técnicas y herramientas especializadas.

Android Apps Security

Practical Mobile Forensics

Search Strings



Learning Android Forensics

Mediante una diversidad de técnicas y herramientas, su experiencia y la propia intuición, el investigador forense va extrayendo evidencia tras evidencia, siguiendo un hilo conductor que le permita llegar a conclusiones plausibles. Este curso ayuda a los participantes a adquirir los conocimientos, la experiencia y las destrezas para desenvolverse como investigador forense en escenarios y casos como los siguientes:

Caso 1. El administrador de sistemas de una pequeña empresa se ha dado cuenta que existe una cuenta que él no creó en el servidor principal (Windows Server 2013), por lo que sospecha que hubo una intrusión. Hacía poco tiempo que habían emigrado al uso de esta plataforma. Según el administrador, él se preocupa de mantener el sistema actualizado y no se explica cómo un intruso pudo ingresar al sistema. Sin embargo, también menciona que más de una persona tiene acceso a cuentas privilegiadas en el sistema y confiesa que utilizaban a veces estas cuentas para labores no sólo administrativas, sino también para labores personales o para aplicaciones que no requerían ningún tipo de privilegio para ejecutarse. Ahora es necesario determinar si realmente hubo una intrusión, cómo ocurrió y el alcance de los daños.

Caso 2. Un empleado penetra al sistema de nómina y extrae información sobre la remuneración y otros beneficios de la cúpula directiva. Luego envía a cada directivo un email, utilizando una cuenta de correo anónima, amenazando con hacer públicos esos datos a no ser que se despida de inmediato al presidente.

Caso 3. La policía detiene a un joven sospechoso de vender droga y le incauta una memoria USB, donde se presume que existe información comprometedora sobre la red de distribución de drogas. Sin embargo el sujeto ya había sido alertado y había formateado el dispositivo USB. Afortunadamente por la urgencia, él aplicó el formato rápido, así que los datos no se borraron, pero se eliminó el file system y la estructura de directorios, por lo que los archivos no se pueden visualizar y habrá que utilizar técnicas de file carving. ¿Se podrá extraer suficiente evidencia para incriminarlo y ganar un posible juicio?

Caso 4. El gerente de sistemas de una organización finalmente se decidió a probar el sistema operativo Linux, dadas las buenas referencias recibidas sobre sus virtudes y funcionalidades. Así que lo instaló en un determinado equipo, pero luego de unos días abandonó las pruebas por otros trabajos que eran importantes para la organización. Un día llegó un nuevo programador y el gerente le encomendó configurar ese equipo como servidor web y colocar allí un CMS (*Content Management System*) como WordPress para el nuevo portal de la organización.. Transcurrido un tiempo, el servidor dejó de funcionar y el gerente, sospechando que se tratase

de un ataque interno por parte de un empleado descontento, decidió iniciar una investigación a fin de determinar qué actividades realizaron cada uno de los individuos que tuvieron acceso al servidor, si hubo algún tipo de intrusión o daño, qué técnicas y herramientas se utilizaron, y detallar toda la información pertinente al incidente, en base a la evidencia digital encontrada.

Caso 5. Un grave incidente de seguridad ha ocurrido en la empresa SwiftLogic, donde se han percatado que documentos confidenciales sobre un nuevo producto se fugaron a la competencia. Se sospecha de un ingeniero y se le ha solicitado que entregue su laptop y su teléfono inteligente Android para buscar allí evidencias de hurto de propiedad intelectual y luego proceder legalmente. ¿Qué hacer si el teléfono está bloqueado y el ingeniero se niega a suministrar la contraseña?

Caso 6. Oculto tras el anonimato, en su oscuro cubículo, solamente iluminado por la tenue luz del atardecer, un empleado consulta en la PC sus mensajes electrónicos privados y profesionales, y... ¿por qué no?... también los de algunos de sus compañeros de trabajo. ¿Qué clientes tiene? ¿Alguna relación amorosa inconfesable? ¿Algún problema económico? ¿Consumo o venta de drogas? ¿Algún escándalo político? En fin, algún dato que pueda ser tomado en cuenta... profesionalmente o como chisme. Sobresaltado por la aparición en la puerta del director y una comitiva, trata de cerrar los archivos que estaba consultando. Demasiado tarde... lo han pillado. Pero... ¿qué se va hacer con esa PC? ¿Se debe apagar? ¿Se debe hacer un volcado de la memoria RAM primero? ¿Cuáles son los pasos a seguir?

Caso 7. En la calle no hay ni un alma. Hace demasiado calor. Es el momento ideal. Tres individuos suben una fotocopiadora... pero los agentes, vigilantes y sigilosos, aprovechan el momento para subir tras ellos e iniciar un registro en el local. No encuentran dispositivos USB, ni DVD grabados, no hay papel, sólo una PC, cámaras fotográficas, máquinas cortadoras, impresoras de tinta, tarjetas en blanco con banda magnética, impresoras de tarjetas de crédito, y otro tipo de material. Parece que hay indicios de clonación de tarjetas bancarias. Entonces... ¿qué hacer con la PC? ¿La impresora? ¿La cámara?...

Caso 8. Durante varios años acaparó la atención pública el caso del guerrillero Raúl Reyes, luego que militares colombianos, en marzo de 2008, llevaron a cabo un ataque sorpresivo en un campamento de la FARC en Ecuador, cerca de la frontera. En la operación falleció ese guerrilleros, considerado el número 2 de las FARC. Las autoridades colombianas afirmaron haber encontrado en el campamento tres laptops, dos discos duros externos y tres dispositivos USB. Luego solicitaron la ayuda de Interpol para llevar a cabo un análisis forense de su contenido. El informe se puede leer aquí.

Caso 9. Un joven es hallado muerto en su casa con una bala en la cabeza. No está claro si se trata de un suicidio o un homicidio. La policía averigua que el individuo tenía conexión con un grupo de ciberdelicuentes llamado KRYPTIX. El iPhone y el iPad encontrados en la escena del crimen son vital para determinar con quién se comunicó antes de su muerte y quizás allí se consiga otros datos reveladores. ¿Cómo se hace el análisis forense a un iPhone y a un iPad?

Caso 10. El cadáver de una mujer se halla a un lado de la cama. Un armario, una mesa y una silla completan el mobiliario de la habitación. Mientras los investigadores indagan sobre la tormentosa vida conyugal de la víctima, los especialistas de policía científica continúan con su labor, examinando la escena, tomando fotografías y realizando un reportaje videográfico. Un arma de fuego corta asoma tras el cuerpo de la víctima, y al otro lado de la habitación, sobre una puerta, se adivina la marca dejada por un proyectil, el cual no ha sido encontrado... todavía. ¿Suicidio? ¿Asesinato? Encima de la mesa hay un laptop y un teléfono inteligente. Todas las evidencias dactiloscópicas, biológicas y balísticas se recogen aplicando las técnicas adecuadas, pero... ¿qué hacer con el laptop?... ¿Qué hacer con el teléfono?...

Tomando como base los casos anteriores, es evidente que hoy día existe una gran necesidad de personal capacitado en el campo de la Forénsica Digital, es decir de investigadores y peritos forenses. Las organizaciones modernas deberían tener alguna capacidad interna para manejar incidentes de seguridad y realizar una investigación a fin de mitigar, contener y prevenir en el futuro situaciones semejantes o acometer acciones legales contra un intruso o un empleado deshonesto. Para reducir los gastos, se puede recurrir a peritos externos en ciertos casos (ej. recuperación y reconstrucción de datos en un disco duro dañado, extracción de datos de un teléfono inteligente), ya que de otra manera se requeriría equipos e instrumentos especializados, instalaciones físicas y experticia técnica que no podrían justificar debido a los altos costos de adquisición y mantenimiento.

CONTENIDO PROGRAMÁTICO DEL CURSO

Parte 1: Incidentes de Seguridad

El contexto de la seguridad de la información. Introducción a la Forénsica Digital. Incidentes de seguridad y su clasificación. Ataques DoS/DDoS. Malware, botnets y ransomware. Intrusiones internas y externas. Indicadores de compromiso (IOC). Búsqueda de amenazas (*threat hunting*). Sistemas de detección y prevención de intrusos (IDS/IPS). Centro de Operaciones de Seguridad (SOC).

Security Information and Event Management (SIEM). Plan de respuesta a incidentes. Gestión de incidentes (preparación, identificación, clasificación, análisis, contención, erradicación, recuperación, investigación, resolución, lecciones aprendidas, documentación). Operación de un centro de respuesta CSIRT/CERT. Proyecto AMPARO de LACNIC. Normas ISO/IEC 27035 y 27043. Guías 800-61 y 800-184 del NIST. Cibercrimen y delitos informáticos (fraude, estafa, scam, extorsión, lavado de dinero, pornografía infantil). Triángulo del fraude. Fraude bancario y falsificación de datos. Robo en telecajeros. Delitos utilizando las redes. Scam y estafa nigeriana. A la caza de datos personales (redes sociales, Google, Pipl, Maltego, i2). Robo de identidad. Ingeniería social. Phreakers y fraude telefónico. Fraude en telefonía móvil celular. Robo de teléfonos inteligentes, alteración y liberación del código IMEI. Piratería en audio, video y televisión por suscripción. Piratería de software. Prevención, detección y respuesta contra fraudes informáticos, bancarios y telefónicos. Defensa contra fallas, accidentes y desastres.

Parte 2: Fundamentos de Forénsica Digital

La forénsica digital y su campo de acción. Ejemplos de casos de investigación y escenarios. Las distintas áreas de la Forénsica Digital. Técnicas antiforense: eliminación/falsificación de evidencias, ocultación de evidencias mediante criptografía, ofuscación de evidencias mediante esteganografía. El investigador y el perito forense. El *expert witness* y el *first responder*. El estándar Daubert. Certificaciones profesionales (CHFI, SANS GIAC, CCFP, CCFE, CSFA, CCE, CFE). Normas internacionales ISO/IEC 27037 y 27042. Normas españolas UNE 71505 y UNE 71506. RFC 3227. Metodología para la investigación forense. Las etapas principales. El método científico en forénsica. El principio de intercambio de Lockard. El paradigma Inman-Rudin. Aspectos legales y éticos. Orden judicial (*warrant*) y orden de registro (*search*). Decomiso de las pruebas (*seizure*). Documentación inicial de la escena del crimen. Fotografía y video. Búsqueda, recolección, resguardo y preservación de las evidencias. Cadena de custodia. Evidencia física y digital. Manejo de las evidencias. Las mejores prácticas según SWGDE (*Scientific Working Group on Digital Evidence*). Adquisición de datos. Equipos encendidos y equipos apagados. Orden de volatilidad. Duplicación de datos. Creación de imagen bit-a-bit. Uso de dd y netcat. Verificación de integridad mediante MD5 y SHA. Máquinas virtuales. Dispositivos de almacenamiento de datos. Estructura de un disco duro. Sectores y clusters. *Slack space*. Particiones. MBR. Sistemas de archivos (FAT, NTFS, Ext2, Ext3, Ext4, HFS). Extracción de evidencias. Extracción física y lógica. E-discovery. Análisis de archivos y de imágenes gráficas. Recuperación de datos borrados. Técnicas de *carving.* Análisis de metadatos. Logs de actividades y de eventos. Syslog. Correlación de eventos. Cronología de los hechos (*timeline*). Marcas de tiempo (*time stamp*). Forénsica en ambiente Windows y Linux. Documentación de la evidencia. Redacción del informe final.

Parte 3: Técnicas Forenses

Equipamiento para forénsica digital. Herramientas en software (TSK, Autopsy, PALADIN, CAINE, DEFT, SIFT, HELIX, FTK, EnCase, OSForensics, X-Ways Forensics). Volcado de la memoria RAM (FTK Imager, Magnet RAM Capture, Belkasoft RAM Capturer). Prácticas de investigación de casos en computadoras y en dispositivos USB. Análisis de la memoria RAM y búsqueda de malware mediante Volatility. Identificación y verificación de hablantes. *Speaker recognition*. Autenticación de grabaciones de audio. Fonemas. Espectro de frecuencias. Análisis por Fourier. Uso de Audacity. Decodificación de tonos de discado DTMF (*Dual-Tone Multi-Frequency*). Análisis forense de dispositivos móviles. Actividades ilícitas por medio de teléfonos celulares. Procedimiento forense en dispositivos móviles. Identificación del equipo (serial, IMEI, SIM, IMSI, ICCID). Acceso al equipo (PIN, PUK, biometría). Jailbreak y rooting. Extracción de datos. Adquisición manual, lógica y física. Técnicas avanzadas (JTAG, chip-off). Desbloqueo de dispositivos móviles. Extracción lógica mediante MTP y mediante ADB (*Android Debug Bridge*). Rootear Android. Extracción física mediante DD. Uso de Netcat. Análisis de datos extraídos mediante FTK Imager Lite, Autopsy, PhotoRec, strings. Herramientas forenses (Santoku, Cellebrite, MobilEdit, MicroSystemation XRY, Oxygen Forensics, NowSecure, Magnet Axiom, Paraben, Andriller). Práctica de análisis forense de Android. Libros, revistas, videos, cursos y retos sobre Forénsica Digital.

Parte 4: Ley y Ética

Sistemas jurídicos en el mundo. Derecho penal y derecho civil. Leyes contra el lavado de dinero y contra el financiamiento al terrorismo. AML (*Anti Money Laundering*) y KYC (*Know Your Client/Know Your Customer*). Normativa de SUDEBAN. Legislación venezolana: Ley contra delitos informáticos, Ley de telecomunicaciones, Código penal, Código orgánico procesal penal (COPP), Ley de Infogobierno. Legislación internacional: GDPR, Sarbanas-Oxley, HIPAA. La propiedad intelectual y la protección del software. Digital Millennium Copyright Act (DMCA). Aspectos éticos y morales. Deodontología y teleología. Ética e Internet. RFC 1087. Códigos de ética (IEEE, CIV, ISACA, CISSP, EC-COUNCIL, SANS). Ética en el sector bancario y financiero.

PRÁCTICAS DE ADIESTRAMIENTO

Las prácticas pueden seleccionarse según los tópicos que más interesan.

1. Gestión de fallas en redes y sistemas informáticos
2. Respaldo y restauración de datos

3. Recuperación de datos borrados o dañados
4. Introducción a la forénsica digital
5. Forénsica digital y marcas de tiempo
6. Análisis forense mediante el Registro de Windows
7. Investigación de casos de forénsica digital
8. Análisis forense de un servidor web vulnerable
9. Análisis forense de la memoria RAM
10. Análisis forense de dispositivos móviles
11. Identificación de hablantes y de tonos DTMF en telefonía
12. Captura y análisis de tráfico en redes
13. Captura y análisis de tráfico en WLAN (Wi-Fi)
14. Captura de teclado y programas espía
15. Criptografía clásica y moderna
16. Marcas de agua, esteganografía e información oculta
17. Protección de datos en laptops y medios extraíbles
18. Gestión de contraseñas
19. Configuración y operación de Windows
20. Configuración y operación de Linux
21. Ataques a las contraseñas de Windows
22. Máquinas y redes virtuales
23. Servicios básicos de Internet con TELNET, SSH, FTP, TFTP
24. Correo electrónico mediante SMTP, POP3 y MIME
25. Navegación en Internet con HTTP y autenticación de usuarios
26. Servidores proxy y navegación anónima

BIBLIOGRAFÍA

Los libros sobre Forénsica en Dispositivos Móviles se encuentran al final de esta lista.

- Joakim Kävrestad, Fundamentals of Digital Forensics, Springer Nature, 2020.
- Nihad A. Hassan, Digital Forensics Basics - A Practical Guide Using Windows OS, Pearson Education, Inc., 2019.
- Nipun Jaswal, Hands-on Network Forensics, Packt Publishing, 2019.
- Xiaolu Zhang (ed.), Digital Forensic Education - An Experiential Learning Approach, Springer Nature, 2020.
- Aniket Roy et al., Digital Image Forensics - Theory and Implementation, Springer Nature, 2020.
- Suneeta Satpathy and Sachi Mohanty, Big Data Analytics and Computing for Digital Forensic Investigations, CRC Press, 2020.
- Lei Chen (ed.), Security, Privacy, and Digital Forensics in the Cloud, John Wiley & Sons, 2019.
- Xiaodong Lin, Introductory Computer Forensics - A Hands-on Practical Approach, Springer, 2018.
- André Årnes (ed.), Digital Forensics, John Wiley & Sons Ltd., 2018.
- Thomas J. Holt et al., Cybercrime and Digital Forensics - An Introduction, Routledge, 2018.
- Wilson Bautista, Practical Cyber Intelligence, Packt Publishing, 2018.
- Gerard Johansen, Digital Forensics and Incident Response, Packt Publishing, 2017.
- Ric Messier, Network Forensics: Hand-on Training, John Wiley & Sons, 2017.
- Ayman Shaaban and Konstantin Sapronov, Practical Windows Forensics, Packt Publishing, 2016.
- Bruce Nikkel, Practical Forensic imaging with Linux Tools. No Starch Press, 2016.
- Harlan Carvey, Windows Registry Forensics, Elsevier, Inc., 2016.
- Samir Datt, Learning Network Forensics, Packt Publishing, 2016.
- Anthony T. S. Ho (Ed.), Handbook of Digital Forensics of Multimedia Data and Devices, John Wiley & Sons, Ltd., 2015.
- Darren R. Hayes, A Practical Guide to Computer Forensics Investigations, Pearson Education, Inc., 2015.
- Irfan Shakeel, Introduction to Computer Forensics & Digital Investigations, INFOSEC Institute, 2015.
- Mohamed Chawki et al., Cybercrime, Digital Forensics and Jurisdiction, Springer International Publishing, 2015.
- Michael Spreitzenbarth and Johann Uhrmann, Mastering Python Forensics, Packt Publishing, 2015.
- Larry E. Daniel and Lars E. Daniel, Digital Forensics for Legal Professionals, Elsevier Inc., 2012.
- Jorge Navarro Clérigues, Guía para Peritos Informáticos, Universitat Politècnica de València, 2015
- José Luis García Gómez, Peritaje Informático, Tesis de Grado, España, 2015.
- Carles Gervilla Rivas, Metodología para un Análisis Forense, Tesis de Maestría, Universitat Oberta de Catalunya, España, 2014.

- Gary Kessler, Steganography for the Computer Forensics Examiner, 2015.
- Victor Marak, Windows Malware Analysis Essentials, Packt Publishing, 2015.
- Chuck Eastom, CCFP - Certified Cyber Forensics Professional Certification Exam Guide, McGraw-Hill, 2015.
- Jason T. Luttgens, Matthew Pepe and Kevin Mandia, Incident Response & Computer Forensics, McGraw-Hill, 2014.
- Michael Hale Ligh, Andrew Case et al, The Art of Memory Forensics, Detecting Malware and Threats in Windows, Linux, and Mac Memory, John Wiley & Sons, Inc., 2014.
- Harlan Carvey, Windows Forensic Analysis Toolkit, Elsevier, Inc., 2014.
- Chris Sanders, Applied Network Security Monitoring, Syngress, 2014.
- Richard Bejtlich, The Practice of Network Security Monitoring, No Starch Press, Inc., 2013.
- Anton Chuvakin et al, Logging and Log Management, Elsevier, 2013.
- John Sammons, The Basics of Digital Forensics, Elsevier, Inc., 2013.
- Marjie T. Britz, Computer Forensics and Cyber Crime: An Introduction, Pearson Education, Inc., 2013.
- Best Forensics Tutorials, eForensics Magazine, 2013.
- Real Life Computer Forensics, eForensics Magazine, 2013.
- Erik Laykin, Investigative Computer Forensics: The Practical Guide for Lawyers, Accountants, Investigators and Business Executives, John Wiley & Sons, Inc., 2013.
- Sherri Davidoff and Jonathan Ham, Network Forensics: Tracking Hackers through Cyberspace, Prentice Hall, 2012.
- Cameron H. Malin, Eoghan Casey et al. Malware Forensics Field Guide for Windows Systems, Elsevier Inc., 2012.
- Cameron H. Malin, Eoghan Casey et al. Malware Forensics Field Guide for Linux Systems, Elsevier Inc., 2012.
- Juan Luis García Rambla, Un Forense Llevado a Juicio, Creative Commons, 2012.
- Joaquim Anguas, Peritaje en Informática: Escenarios, Conceptos y Técnicas Básicas, CPEIG, 2011.
- Cory Altheide and Harlan Carvey, Digital Forensics with Open Source Tools, Elsevier Inc., 2011.
- Michael Hale Ligh et al., Malware Analyst's Cookbook, Wiley Publishing inc., 2011.
- Michael Krausz, Managing Information Security Breaches - Studies from Real Life, IT Governance Publishing, 2010.
- Good Practice Guide for Incident Management, European Network and information Security Agency (ENISA), 2010.
- Computer Forensics: Evidence Collection and Preservation, EC-Council Press, 2010.
- Computer Forensics: Investigating Network Intrusions and Cybercrime, EC-Council Press, 2010.
- Computer Forensics: Investigating Data and Image Files, EC-Council Press, 2010.
- Computer Forensics: Investigating Hard Disks, File and Operating Systems, EC-Council Press, 2010.
- Computer Forensics: Investigating Wireless Networks and Devices, EC-Council Press, 2010.
- Bill Nelson, Amelia Phillips and Christopher Steuart, Guide to Computer Forensics and Investigations, Course Technology, 2010.
- Eoghan Casey, Handbook of Digital Forensics and Investigation, Elsevier Academic Press, 2010.
- Aaron Philipp, David Cowen, Chris Davis, Hacking Exposed - Computer Forensics, McGraw-Hill, 2010.
- Michael Davis, Sean Bodemer, Aaron Lemaster, Hacking Exposed – Malware & Rookits, McGraw-Hill, 2010.
- Terrence V. Lillard, Digital Forensics for Network, Internet, and Cloud Computing, Elsevier Inc., 2010.
- Ewa Huebner and Stefano Zanero, Open Source Software for Digital Forensics, Springer Science+Business Media, 2010.
- Helena Rifà Pous et al., Análisis Forense de Sistemas Informáticos, Universitat Oberta de Catalunya, 2009.
- Jeffe Varsalone, Cisco Router and Switch Forensics, Syngress Publishing, 2009.
- Angus M. Marshall, Digital Forensics: Digital Evidence in Criminal Investigation, John Wiley & Sons, 2008.
- James M. Aquilina, Eoghan Casey et al., Malware Forensics - Investigating and Analyzing Malicious Code, Elsevier Inc., 2008.
- Leonard W. Vona, Fraud Risk Assessment - Building a Fraud Audit Program, John Wiley & Sons, Inc., 2008.
- Rohas Nagpal, Evolution of Cyber Crimes , Asian School of Cyber Laws, 2008.
- Linda Volonino and Reynaldo Anzaldua, Computer Forensics For Dummies, Wiley Publishing, Inc., 2008.
- Dave Kleiman, The Official Study Guide for Computer Hacking Forensic Investigators (CHFI), Elsevier Inc, 2007.
- Miguel López Delgado, Análisis Forense Digital, GNU Free Documentation License, 2007.
- José Arquillo Cruz, Herramienta de Apoyo para el Análisis Forense de Computadoras, Tesis de grado, España, 2007.
- Chad Steel, Windows Forensics: The Field Guide for Corporate Computer Investigations, John Wiley & Sons, 2006.
- Robert Jones, Internet Forensics, O'Reilly, 2005.
- Brian Carrier, File System Forensic Analysis, Addison Wesley, 2005.
- Richard Nolan, Colin O'Sullivan, Jake Branson and Cal Waits, First Responders Guide to Computer Forensics, CERT, 2005.
- Richard Bejtlich, The Tao of Network Security Monitoring Beyond Intrusion Detection, Addison Wesley, 2004.
- Michael A. Caloyannides, Privacy Protection and Computer Forensics, Artech House, 2004.
- Barry J. Grundy, The Law Enforcement and Forensic Examiner Introduction to Linux, NASA Computer Crimes Division, 2004.
- Douglas Schweitzer, Incident Response: Computer Forensics Toolkit, John Wiley & Sons, 2003.
- John R. Vacca, Computer Forensics: Computer Crime Scene Investigation, Charles River Media, 2002.

- Debra Littlejohn Shinder, Cybercrime: Scene of the Computer Forensics Handbook, Syngress Publishing, 2002.
- Albert J. Marcella and Robert S. Greenfield, Cyber Forensics – A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, Auerbach Publications, 2002.
- Mike Schiffman, Hacker's Challenge: Test your Incident Response Skills, Osborne/McGraw-Hill, 2001.

Forénsica en Dispositivos Móviles

- Oleg Skulkin, Donnie Tindall and Rohit Tamma and, Learning Android Forensics, Packt Publishing, 2018.
- Rohit Tamma, Oleg Skulkin, Heather Mahalik and Satish Bommisetty, Practical Mobile Forensics, Packt Publishing, 2018.
- John Bair, Seeking the Truth from Mobile Evidence, Elsevier Inc., 2018.
- Lee Reiber, Mobile Forensic Investigations, McGraw-Hill, 2019.
- Mobile Incident Response for Android and iOS, NowSecure, 2016.
- Mattia Epifani and Pasquale Stirparo, Learning iOS Forensics, Packt Publishing, 2016.
- Iosif I. Androulidakis, Mobile Phone Security and Forensics: A Practical Approach, Springer, 2012.
- Andrew Hoog, Android Forensics - Investigation, Analysis, and Mobile Security, Elsevier, Inc., 2011.
- Sean Morrissey, IOS Forensic Analysis for iPhone, iPad, and iPod Touch, APress, 2010.
- Jonathan Zdziarski, iPhone Forensics, O'Reilly Media, Inc., 2008.
- Gregory Kipper, Wireless Crime and Forensic Investigation, Auerbach Publications, 2007.
- Sakka Vasileios, Android Forensics, Tesis de grado, Grecia, 2014.
- Maximiliano Bendinelli, Análisis forense de dispositivos móviles con sistema operativo Android, Tesis de grado, Argentina, 2013.