FORMACIÓN E-LEARNING

Curso Online de
Informática Forense para empresas

→ Para garantizar las políticas de seguridad de la empresa y la protección tanto de la información como de las aplicaciones que facilitan el acceso a esa información.

ARGENTINA
(54) 1159839543
BOLÍVIA
(591) 22427186
(591) 70695490
COLOMBIA
(57) 15085369
CHILE
(56) 225708571
COSTA RICA
(34) 932721366
EL SALVADOR
(503) 21366505
MÉXICO
(52) 5546319899
PERÚ
(51) 17007907
PANAMÁ
(507) 3888513
PUERTO RICO
(1) 7879457491
REPÚBLICA DOMINICANA
(1) 8299566921
URUGUAY
(34) 932721366
VENEZUELA
(34) 932721366

Llamada Whatsapp
(34) 601615098

Iniciativas Empresariales
estrategias de formación

MANAGER BUSINESS SCHOOL

attcliente@iniciativasempresariales.edu.es
america.iniciativasempresariales.com

ARGENTINA - BOLÍVIA - COLOMBIA - COSTA RICA - CHILE - EL SALVADOR - MÉXICO
PANAMÁ - PERÚ - PUERTO RICO - REPÚBLICA DOMINICANA - URUGUAY - VENEZUELA - ESPAÑA

Presentación

La Informática Forense, según la definición oficial adoptada en el primer DFRWS (Digital Forensics Research WorkShop o Taller de Investigación Digital Forense) del año 2001, se basa en el uso de métodos científicos comprobables para la preservación, recogida, validación, identificación, interpretación, análisis, documentación y presentación de evidencias procedentes de medios digitales con el objeto de reconstruir hechos considerados delictivos y/o ayudar a la prevención de actos no autorizados y capaces de provocar perturbaciones en operaciones planificadas de organismos y empresas.

El estudio sistemático de medios digitales y datos con efectos potencialmente probatorios, sujeto a buenas prácticas y estándares aceptados, resulta necesario para llevar a cabo investigaciones eficaces y asegurar la validez jurídica de las evidencias obtenidas, con el objeto de que las mismas puedan ser utilizadas posteriormente ante jueces, autoridades públicas o responsables de seguridad de las empresas.

El presente curso adopta un enfoque a mitad de camino entre la especialización técnica y una generalización de conceptos para información del personal directivo de las empresas.
El objetivo principal consiste en orientar a aquellas personas que dentro de las organizaciones respectivas sean responsables de tomar decisiones ejecutivas con capacidad para influir sobre procedimientos y operaciones, de manera que un mejor conocimiento de la Informática Forense, en el contexto de la problemática de la cual se deriva, los procedimientos utilizados y las posibles consecuencias de un tratamiento inadecuado de las evidencias digitales, se traduzca en mejoras de eficiencia y ahorros de costes.

La Educación On-line

Los cursos e-learning de Iniciativas Empresariales le permitirán:

- **La posibilidad de escoger el momento y lugar más adecuado.**
- **Interactuar con otros estudiantes enriqueciendo la diversidad de visiones y opiniones y su aplicación en situaciones reales.**
- **Trabajar con diversos recursos que ofrece el entorno on-line.**
- **Aumentar sus capacidades y competencias en el puesto de trabajo en base al estudio de los casos reales planteados en este curso.**

attcliente@iniciativasempresariales.edu.es - america.iniciativasempresariales.com

Método de Enseñanza

El curso se realiza on-line a través de la plataforma *e-learning* de Iniciativas Empresariales que permite, si así lo desea, descargarse los módulos didácticos junto con los ejercicios prácticos de forma que pueda servirle posteriormente como un efectivo manual de consulta.
A cada alumno se le asignará un tutor que le apoyará y dará seguimiento durante el curso, así como un consultor especializado que atenderá y resolverá todas las consultas que pueda tener sobre el material docente.
El curso incluye:

Aula Virtual | Tutor personal | Flexibilidad de horarios | Pruebas de Autoevaluación

Contenido y Duración del Curso

El curso tiene una duración de 80 horas y el material didáctico consta de:

Manual de Estudio
Corresponde a todas las materias que se imparten a lo largo de los 10 módulos de formación práctica de que consta el curso Informática Forense para empresas.

Material Complementario
Incluye ejemplos y modelos de soporte sobre la materia con el objetivo de ejemplificar y ofrecer recursos para la resolución de las problemáticas específicas en la prevención, detección y obtención de pruebas del fraude cometido a través de los dispositivos electrónicos de la empresa.

Ejercicios de Seguimiento
Corresponden a ejercicios y prácticas del tipo “hágalo usted mismo” donde se plantean y solucionan determinados casos referentes a la Informática Forense. El objetivo de estos ejercicios consiste en familiarizar al alumno con la vertiente práctica de la materia y animarlo a desplegar su iniciativa personal en el campo de la investigación de soportes digitales.

Pruebas de Autoevaluación
Para la comprobación práctica de los conocimientos que Ud. va adquiriendo.

attcliente@iniciativasempresariales.edu.es - america.iniciativasempresariales.com

Este curso le permitirá saber y conocer:

- Cuál es el estado actual de la Informática Forense en un contexto de cambio estructural y rápidos avances tecnológicos.
- Cuáles son las implicaciones jurídicas del uso, la investigación y el análisis de medios digitales, tanto en el ámbito de la empresa como en cualquier otro aspecto de la vida social.
- Cómo se lleva a cabo el análisis forense de los dispositivos digitales.
- Qué dispositivos son susceptibles de análisis forense.
- Cuál es la probabilidad de que se produzca un robo de datos o una intrusión en el sistema de una empresa.
- Cómo debe prevenirse la fuga de información confidencial en la empresa.
- Cuáles son las bases legales que en España regulan la recogida, interpretación y valoración de evidencias digitales.
- Cuáles son los componentes relevantes de una red corporativa.
- Qué dificultades plantea al investigador y a la defensa legal el análisis de teléfonos móviles y smartphones.
- Cómo evaluar la conveniencia de emprender actuaciones legales que pueden suponer un coste importante para la empresa.
- Cómo elaborar políticas de uso de Internet y de medios digitales por parte del personal de la empresa.
- Cómo detectar y corregir vulnerabilidades en el sistema de seguridad de la empresa.

Una eficaz herramienta para la prevención, detección y obtención de pruebas de un fraude cometido a través de los dispositivos electrónicos en la empresa.

Dirigido a:

Profesionales del mundo de la Informática que quieran actualizar sus conocimientos para resolver problemas relacionados con la seguridad de la información de sus empresas, así como a todos aquellos profesionales que quieran aplicar de forma práctica la Informática Forense para realizar valoraciones, dictámenes y peritaciones informáticas en la empresa.

attcliente@iniciativasempresariales.edu.es - america.iniciativasempresariales.com

Contenido del curso

→ MÓDULO 1. Principios metodológicos: investigación forense de delitos digitales

6 horas

Este primer módulo del curso logra que el alumno establezca un contacto inicial con la materia: problemática de base, definiciones y principios generales.

1.1. Amenazas digitales:
1.1.1. Delitos informáticos.
1.1.2. Evaluación de riesgos.
1.1.3. Motivaciones de un ciberdelincuente.
1.1.4. Amenazas internas y externas.

1.2. Estrategia del atacante:
1.2.1. Footprinting.
1.2.2. Escaneo de puertos y protocolos.
1.2.3. Enumeración.
1.2.4. Penetración.
1.2.5. Puertas traseras.
1.2.6. Borrado de huellas.

1.3. Investigación informática forense:
1.3.1. "First responder" o primer interviniente.
1.3.2. Apagado brusco del sistema.
1.3.3. Objetos recogidos.
1.3.4. Etapas de una investigación digital forense:
1.3.4.1. Adquisición forense (Imaging).
1.3.4.2. Análisis de los datos.
1.3.4.3. Presentación de informes.
1.3.5. Requisitos de una investigación forense:
1.3.5.1. Aceptabilidad.
1.3.5.2. Integridad.
1.3.5.3. Credibilidad.
1.3.5.4. Relación causa-efecto.
1.3.5.5. Carácter repetible.
1.3.5.6. Documentación.
1.3.6. Línea de tiempo.

1.4. Finalmente, las decisiones de rigor.

attcliente@iniciativasempresariales.edu.es - america.iniciativasempresariales.com

Contenido del curso

→ MÓDULO 2. Soportes de datos

10 horas

El objetivo de este módulo es que el alumno entienda conceptos clave como volúmenes, particiones, sistemas de archivos, journaling, etc., así como procedimientos de adquisición forense y las características de los principales tipos de archivos informáticos.

2.1. El modelo de niveles:
2.1.1. Nivel 1: dispositivos físicos.
2.1.2. Nivel 2: volúmenes y participaciones.
2.1.3. Nivel 3: sistema de archivos.
2.1.4. Nivel 4: bloque de datos.
2.1.5. Nivel 5: metadatos.
2.1.6. Nivel 6: nombres de los archivos.
2.1.7. Nivel 7: Journaling.

2.2. Participaciones y sistemas d archivos:
2.2.1. Microsoft NTFS.
2.2.2. Microsoft FAT.
2.2.3. Sistemas de archivos Linux ext2, ext3 y ext4.
2.2.4. HFS, HFS+, JFS, ReiserFS, Btrfs y otros.

2.3. Procedimientos de adquisición forense:
2.3.1. Dinámica general de la adquisición forense.
2.3.2. Herramientas de adquisición forense:
2.3.2.1. dd.
2.3.2.2. EnCase/Linen.
2.3.2.3. dcfldd, dc3dd y ddrescue.
2.3.2.4. AIR.
2.3.2.5. Adquisición forense vía hardware.
2.3.2.6. Sumas de verificación (hash).
2.3.2.7. Cálculo de MD5 y SHA1 con Linux y Windows.

2.4. Recuperación de archivos borrados:
2.4.1. Borrado de archivos por el sistema operativo.
2.4.2. ¿Qué es el slack de archivo, cluster y sector?
2.4.3. Tecnologías de recuperación de archivos borrados.
2.4.4. Data Carving.

2.5. Análisis de archivos:
2.5.1. Firmas características.
2.5.2. Documentos ofimáticos:
2.5.2.1. Documentos Open Office.

attcliente@iniciativasempresariales.edu.es - america.iniciativasempresariales.com

Contenido del curso

2.5.2.2. Archivos MS-Office antiguos.
2.5.2.3. Documentos RTF.
2.5.2.4. OpenDocument.
2.5.2.5. Documentos PDF.
2.5.3. Archivos gráficos:
2.5.3.1. Archivos JPG.
2.5.3.2. GIF.
2.5.3.3. PNG.
2.5.3.4. TIFF.
2.5.3.5. RAW.
2.5.4. Archivos de medios: video y audio
2.5.4.1. MPEG-1, MPEG-2 y MPEG-4.
2.5.4.2. WMV (Windows Media Video).
2.5.4.3. QuickTime.
2.5.4.4. MKV.
2.5.5. Archivos de medios: solo audio
2.5.5.1. WAV (Waveform Audio Format).
2.5.5.2. MPEG-3.
2.5.5.3. ASF/WMA.
2.5.5.4. AAC/M4A.

2.6. Código ejecutable.

2.7. Exclusión de archivos conocidos.

→ MÓDULO 3. Análisis forense de sistemas MS-Windows

22 horas

Este módulo es el más importante y se plantea como una guía ordenada para el alumno de aproximación y estudio a los problemas de análisis forense de plataformas Microsoft Windows en sus diferentes versiones históricas.

3.1. Generalidades:
3.1.1. Versiones diferentes.
3.1.2. Interfaces gráficos vs línea de comando.

3.2. Información volátil:
3.2.1. Orden de volatilidad.
3.2.2. Tipos de información volátil:
3.2.2.1. Fecha y hora del sistema.

attcliente@iniciativasempresariales.edu.es - america.iniciativasempresariales.com

Contenido del curso

3.2.2.2. Conexiones de red.
3.2.2.3. Puertos abiertos.
3.2.2.4. Ejecutables conectados a puertos TCP y UDP.
3.2.2.5. Usuarios conectados.
3.2.2.6. Tabla de enrutamiento.
3.2.2.7. Procesos en ejecución.
3.2.2.8. Archivos abiertos.

3.3. Análisis forense de la memoria RAM:
3.3.1. Información no estructurada.
3.3.2. Captura de RAM mediante dd.exe.
3.3.3. Otras herramientas para captura de RAM.
3.3.4. Análisis de RAM con Volatility.

3.4. Adquisición de soportes de datos:
3.4.1. Adquisición forense con FTK Imager.
3.4.2. Adquisición con EnCase.
3.4.3. Otros procedimientos de adquisición.

3.5. Análisis de una adquisición forense:
3.5.1. Análisis con EnCase.
3.5.2. Access Data FTK.
3.5.3. Soluciones de bajo coste:
3.5.3.1. Captain Nemo.
3.5.3.2. FileDisk.
3.5.3.3. Mount Image Pro.
3.5.3.4. ProDiscover Basic.

3.6. Análisis de participaciones NTFS y FAT:
3.6.1. RunTime Disk Explorer.
3.6.2. Recuperación de archivos borrados:
3.6.2.1. No existe el borrado seguro al 100%...al menos en la práctica.
3.6.2.2. Runtime GetDataBack.
3.6.2.3. Easy Recovery Professional.
3.6.2.4. R-Studio.

3.7. La papelera de reciclaje:
3.7.1. Funcionamiento de la papelera de Windows.
3.7.2. Análisis de la papelera de Windows con Rifiuti.
3.7.3. La papelera en Windows Vista y 7.
3.7.4. La papelera en Windows 8/10.

3.8. El historial de navegación en Internet:
3.8.1. El factor humano.

Contenido del curso

3.8.2. Microsoft Internet Explorer.
3.8.3. Análisis con Pasco.
3.8.4. X-Ways Trace.
3.8.5. iehist.
3.8.6. Mozilla Firefox:
3.8.6.1. Ubicación de archivos.
3.8.6.2. Análisis con Sqliteman.
3.8.7. Google Chrome.

3.9. Cookies:
3.9.1. El problema con las cookies.
3.9.2. Funcionamiento.
3.9.3. Investigación de cookies con Galleta.

3.10. Metadatos:
3.10.1. Pero, ¿qué son exactamente?
3.10.2. Cómo podemos verlos.
3.10.3. F.O.C.A.
3.10.4. Metadata Assistant.
3.10.5. Metadatos EXIF.

3.11. Cadenas de caracteres:
3.11.1. Disk Investigator y Evidor.
3.11.2. Win-Hex.

3.12. Clientes de correo electrónico:
3.12.1. PST y DBX Folders.
3.12.2. Paraben´s E-Mail Examiner.

3.13. El registro de Windows:
3.13.1. Dónde está y qué es el Registro de Windows.
3.13.2. Estructura del Registro de Windows.
3.13.3. Análisis off-line con Windows Registry Recovery.
3.13.4. RegRipper.

3.14. Artefactos forenses en Windows 8/8.1/10.

3.15. Otros artefactos de relevancia forense en Windows:
3.15.1. Archivos prefetch.
3.15.2. Carpetas temporales.
3.15.3. Eventos de Windows.
3.15.4. Archivo de paginación.
3.15.5. Registro de conexiones WiFi.

Contenido del curso

→ MÓDULO 4. Investigación forense en el entorno Linux

6 horas

El éxito de las plataformas de código libre – especialmente Linux/Ubuntu – obliga al investigador a tenerlas en cuenta, no solo como objeto de análisis, sino también como herramienta para la investigación forense.

4.1. Importancia y limitaciones de Linux.

4.2. Código libre:
4.2.1. Definición y características del software libre.
4.2.2. Ventajas de la apertura del código.

4.3. Linux como herramienta de investigación forense:
4.3.1. Ventajas operativas y económicas.
4.3.2. Comenzando a trabajar.
4.3.3. La línea de comando.
4.3.4. Descarga, compilación e instalación de herramientas.
4.3.5. Peligro: montaje automático de participaciones.
4.3.6. HAL, udev, d-messagebus.
4.3.7. Soluciones al problema del montaje automático.

4.4. Estructura y organización de Linux:
4.4.1. Aprendizaje de Linux.
4.4.2. Arquitectura del sistema.
4.4.3. Designación de unidades y sistemas de archivos.
4.4.4. Jerarquía de directorios.
4.4.5. Algunos directorios de interés.
4.4.6. Diferentes tipos de usuario.
4.4.7. Archivos, permisos y privilegios de acceso.
4.4.8. Marcas de tiempo en Linux:
4.4.8.1. Utilidad de las marcas de tiempo.
4.4.8.2. Peligros.

4.5. Información volátil:
4.5.1. Fecha y hora del sistema.
4.5.2. Puertos utilizados y conexiones abiertas.
4.5.3. Procesos en ejecución.
4.5.4. Otras informaciones de interés.

4.6. Adquisición forense de Sistemas Linux:
4.6.1. Copia a bajo nivel con dd.
4.6.2. Adepto.

attcliente@iniciativasempresariales.edu.es - america.iniciativasempresariales.com

Contenido del curso

4.7. Fase de análisis:
4.7.1. Líneas de tiempo.
4.7.2. Obtención de datos en bruto para una línea de tiempo.
4.7.3. Recuperación de archivos borrados.

4.8. Otras herramientas:
4.8.1. ¿Qué es un rootkit?
4.8.2. Chkrootkit y RKhunter.
4.8.3. Md5deep.

→ MÓDULO 5. Investigación forense en redes e internet

8 horas

Los ordenadores ya no son entornos aislados sino que forman parte de redes empresariales y domésticas. Un estudio de los conceptos básicos de la arquitectura de redes TCP/IP es condición imprescindible para la ejecución de tareas de investigación forense en cualquier entorno distribuido de tipo empresarial o particular.

5.1. Elementos característicos de una red local:
5.1.1. Esquema general de una red corporativa.
5.1.2. Archivos de registro.
5.1.3. Ejemplo: log de un servidor DHCP.
5.1.4. Datos en reposo y en tránsito.
5.1.5. Datos estacionarios de carácter volátil.
5.1.6. Dando saltos de aquí para allá.
5.1.7. ¿Quién dijo fácil?

5.2. Protocolos:
5.2.1. Funcionamiento general de los protocolos.
5.2.2. Pilas de protocolos.
5.2.3. Capa de aplicación.
5.2.4. Protocolos de nivel superior: HTTP y SMB.
5.2.5. Capa de transporte: TCP.
5.2.6. Puertos.
5.2.7. Capa de red: IP.
5.2.8. Red pública y redes privadas (locales).
5.2.9. El protocolo IPv6.
5.2.10. Enrutamiento.
5.2.11. Capa de enlace de datos: el interfaz Ethernet.
5.2.12. Conmutador (switch) y concentrador (hub).

Contenido del curso

5.3. Análisis y comprobación de direcciones IP:
5.3.1. Herramientas de traza de red.
5.3.2. Ping/fping.
5.3.3. Traceroute/Tracert.
5.3.4. Whois, o quién es quién en Internet.

5.4. Correo electrónico:
5.4.1. Procedimiento de análisis.
5.4.2. Estructura típica de un encabezado.

5.5. Análisis del tráfico de red:
5.5.1. Wireshark.
5.5.2. Captura de tráfico de red:
5.5.2.1. Conexión mediante hub.
5.5.2.2. Port mirroring.
5.5.2.3. Otros procedimientos.
5.5.3. Manejo de Wireshark.

→ MÓDULO 6. Investigación forense de sistemas Apple OS X

2 horas

Aunque los Mac siguen siendo poco utilizados, la complejidad, capacidades técnicas y relevancia de los entornos Apple para diversas aplicaciones obligan a incluirlos en este módulo adicional que tiene un carácter meramente introductorio y descriptivo.

6.1. Carácter exclusivo y particularidades:
6.1.1. Observaciones preliminares.
6.1.2. Apple y el delito de guante blanco.
6.1.3. Breve historia del Mac.

6.2. Acceso a la máquina:
6.2.1. Examen en vivo.
6.2.2. Modo de usuario único.
6.2.3. Arranque desde CD/DVD.
6.2.4. Arranque en modo “Target Disk”.

6.3. Cómo organiza Apple la información:
6.3.1. Sistemas de archivos.
6.3.2. Estructura de disco:
6.3.2.1. Apple Partition Map.

attcliente@iniciativasempresariales.edu.es - america.iniciativasempresariales.com

Contenido del curso

6.3.2.2. Tabla de particiones GUID.
6.3.3. El sistema de archivos HFS+.

6.4. Adquisición forense.

6.5. Elementos de evidencia en memoria virtual.

6.6. Elementos de evidencia específicos de las aplicaciones:
6.6.1. Correo electrónico.
6.6.2. Mensajería instantánea.
6.6.3. Internet.
6.6.4. Historial de comandos del terminal.

6.7. Conclusiones.

→ MÓDULO 7. Investigación forense de dispositivos móviles

8 horas

La movilidad merece capítulo aparte no solo por su presencia cada vez más extendida en los entornos empresariales, sino también por las dificultades a la hora de evitar incidentes de seguridad, ataques desde Internet y perturbaciones originadas en ámbitos particulares o ajenos a la organización.

7.1. Generalidades:
7.1.1. Dos grandes protagonistas: Apple y Android.
7.1.2. A ningún lado sin mi Smartphone.
7.1.3. Hardware.
7.1.4. Software:
7.1.4.1. Apple.
7.1.4.2. Android.
7.1.5. ¿Qué tipo de información se puede extraer?
7.1.5.1. Grandes capacidades de almacenamiento.
7.1.5.2. Elementos de evidencia.
7.1.5.3. Aislamiento de redes.

7.2. Apple iPhone:
7.2.1. Consideraciones generales:
7.2.1.1. Visualización directa.
7.2.1.2. Adquisición lógica con un ordenador.
7.2.1.3. Recuperación de backups.
7.2.1.4. Extracción física.

attcliente@iniciativasempresariales.edu.es - america.iniciativasempresariales.com

Contenido del curso

7.2.1.5. Técnicas avanzadas.
7.2.1.6. Encriptación por hardware.
7.2.2. Procedimientos de adquisición:
7.2.2.1. Adquisición a través de iTunes.
7.2.2.2. iPhone Backup Extractor.
7.2.2.3. Backup encriptado.
7.2.2.4. Wondershare Dr. Fone.
7.2.3. Otros dispositivos Apple.

7.3. Android:
7.3.1. Google y la Open Handset Alliance.
7.3.2. Características fundamentales.
7.3.3. Acceso inmediato al dispositivo:
7.3.3.1. Tarjeta de memoria.
7.3.3.2. Acceso a un teléfono móvil Android.
7.3.3.3. Sincronización con el propio software.
7.3.4. Acceso a través de SDK:
7.3.4.1. Modo de empleo.
7.3.4.2. Ajustes imprescindibles.
7.3.5. Empleo de ADB:
7.3.5.1. Exploración del terminal.
7.3.5.2. Ejemplos de extracción de datos.
7.3.6. Rooting:
7.3.6.1. Significado del Rooting.
7.3.6.2. Rooting temporal.
7.3.6.3. Particiones Recovery.
7.3.6.4. Rooting permanente.
7.3.6.5. XDA-Developers.

7.4. Plataformas comerciales:
7.4.1. Ventajas de los productos comerciales.
7.4.2. Oxygen Forensic Suite 2015.
7.4.3. Cellebrite UFED/Touch.

Contenido del curso

→ MÓDULO 8. Imagen digital forense

4 horas

Los archivos de imágenes digitales constituyen una parte importante de la investigación forense, tanto por la información gráfica que aportan como por los problemas de tratamiento jurídico a los que dan lugar.
Este módulo incluye un repaso de los diferentes sistemas de metadatos gráficos.

8.1. Fundamentos técnicos:
8.1.1. Consideraciones preliminares.
8.1.2. Cómo funciona una cámara digital.
8.1.3. ¿Y el color?

8.2. Imágenes manipuladas:
8.2.1. Interpolación y consistencia estadística.
8.2.2. Artefactos.
8.2.3. Áreas clonadas.
8.2.4. Inconsistencias en la iluminación.
8.2.5. E.L.A. (Error Level Analysis).

8.3. La imagen digital como herramienta de investigación:
8.3.1. La imagen digital como prueba.
8.3.2. Recomendaciones.
8.3.3. Buenas prácticas.
8.3.4. Imágenes RAW.

8.4. Metadatos de archivos gráficos:
8.4.1. Exif.
8.4.2. IPTC-IIM.
8.4.3. Adobe XMP.
8.4.4. Limitaciones de los metadatos gráficos.

→ MÓDULO 9. Otras herramientas software para la investigación forense

8 horas

A través de este módulo el alumno conocerá las principales soluciones de tipo comercial y de código libre utilizadas durante la investigación forense de dispositivos digitales.

9.1. Virtualización:
9.1.1. Ventajas de la virtualización.
9.1.2. Fundamentos técnicos de la virtualización.

attcliente@iniciativasempresariales.edu.es - america.iniciativasempresariales.com

Contenido del curso

9.1.3. VMware Workstation.
9.1.4. VirtualBox.

9.2. Distribuciones Linux:
9.2.1. Linux DEFT.
9.2.2. CAINE.

9.3. Lista de herramientas forenses.

→ MÓDULO 10. Conclusiones: escenarios prácticos y perspectivas de futuro

6 horas

Módulo final a modo de resumen del curso donde se añaden consideraciones puntuales para facilitar el paso de la teoría a los usos prácticos de la materia, y donde se habla de nuevas tendencias y retos de futuro y se facilitan consejos para la práctica procesal y el ahorro de costes en las empresas.

10.1. Escenarios de investigación:
10.1.1. Ante la autoridad judicial.
10.1.2. Casos civiles y compañías de seguros.
10.1.3. Empresas y organizaciones.
10.1.4. Seguridad nacional y sector público.

10.2. Obstáculos:
10.2.1. Destrucción intencionada de datos.
10.2.2. Antiforensics.

10.3. Retos y tendencias de futuro:
10.3.1. Clusters.
10.3.2. Computación en la Nube.
10.3.3. Internet de las Cosas.
10.3.4. Redes Sociales.
10.3.5. Blockchain: cadenas de consenso distribuidas.

10.4. Investigación convencional:
10.4.1. El problema.
10.4.2. Mundo virtual y mundo real.
10.4.3. Tomas de declaración e interrogatorios:
10.4.3.1. Cuestionario para víctimas de delitos digitales.
10.4.3.2. Preguntas para administradores de sistemas.
10.4.3.3. Cuestionario para el sospechoso.

attcliente@iniciativasempresariales.edu.es - america.iniciativasempresariales.com

Contenido del curso

10.4.3.4. Preguntas para casos de pederastia y pornografía infantil.
10.4.4. Finalidad de los procedimientos convencionales.
10.4.5. Misión del investigador.

10.5. Rematando el trabajo:
10.5.1. Elaboración de informes.
10.5.2. Implicaciones jurídicas.

attcliente@iniciativasempresariales.edu.es - america.iniciativasempresariales.com

Autor

El contenido y las herramientas pedagógicas del curso Informática Forense para empresas han sido elaboradas por:

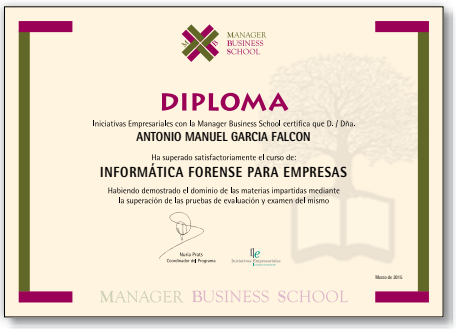
Francisco Lázaro

Perito Informático Judicial con amplia experiencia en la consultoría informática en el asesoramiento en seguridad de datos y redes de ordenadores e investigación de soportes digitales.
Experto en Protección de Datos, Informática Forense y recuperación de archivos borrados, así como en el análisis de soportes (discos duros, llaves USB, tarjetas de memoria, etc.).

El autor y sus colaboradores estarán a disposición de los alumnos para resolver sus dudas y ayudarles en el seguimiento del curso y el logro de objetivos.

Titulación

Una vez realizado el curso el alumno recibirá el diploma que le acredita como **experto en Informática Forense para empresas.** Para ello, deberá haber cumplimentado la totalidad de las pruebas de evaluación que constan en los diferentes apartados. Este sistema permite que los diplomas entregados por Iniciativas Empresariales y Manager Business School gocen de garantía y seriedad dentro del mundo empresarial.


MANAGER BUSINESS SCHOOL

DIPLOMA

Iniciativas Empresariales con la Manager Business School certifica que D./ Dña.

ANTONIO MANUEL GARCIA FALCON

Ha superado satisfactoriamente el curso de:

INFORMÁTICA FORENSE PARA EMPRESAS

Habiendo demostrado el dominio de las materias impartidas mediante la superación de las pruebas de evaluación y examen del mismo

MANAGER BUSINESS SCHOOL