FORENSIC EXPLORER

Advanced Forensics Software

GetData FORENSICS

Forensic Explorer (FEX), es un software avanzado para la conservación, el análisis y la presentación de evidencia electrónica. Los principales usuarios de este software son las fuerzas de procuración de justicia y los departamentos de investigación gubernamentales, militares y empresariales. Este curso de capacitación certificado de cuatro días se desarrolló para formar investigadores forenses digitales de todos los niveles sobre cómo utilizar FEX de la mejor manera. Al finalizar el curso, los participantes obtendrán la valiosa certificación profesional de Examinador Certificado de Forensic Explorer, FEXCE.

Nivel Uno

Descripción general e introducción de Forensic Explorer

- Instalación y configuración de la estación de trabajo
- Gestión del caso
- Activación y mantenimiento del dispositivo de seguridad (Dongle)
- Configuración avanzada de red y clave WiBu

Adquisición forense

- Bloqueo de escritura vs. Protección contra escritura
- Examinación y análisis de redes
- FEX Triage, FEX Memory Imager y FEX Imager

Crear un caso digital

- Agregar y eliminar evidencia en FEX
- Evaluación y vista previa de la evidencia
- Crear, convertir vistas previas y guardar un caso
- Crear y gestionar perfiles de investigadores
- Comprender el procesamiento de la evidencia

Nivel Dos

Interfaz del Forensic Explorer

- Interpretación de datos de los módulos
- Personalización de formatos
- Registro y establecimiento de prioridades en los procesos
- Verificación de fecha y hora
- Análisis forense digital de fecha y hora
- Sistemas de archivos FAT, NTFS, HFS, HFS+, APFS, CDFS
- Manejo de dispositivos cifrados con Bitlocker y File Vault
- Información de fecha y hora en el registro de Windows

Investigación y análisis del caso

- Estructura y descripción de los módulos
- Estructura del árbol de carpetas
- Filtros de categorías
- Vistas de datos
  - Lista de archivos, Galería, Disco, Gráfica de categorías
- Vistas de archivos
  - Hexadecimal y texto
  - Marcadores
  - Esquema de bytes y distribución de caracteres
  - Pantalla- (Interpretación nativa)
  - Registro del sistema de archivos
  - Metadatos
  - Extensión de archivos
  - Visor de propiedades (Módulo de correo electrónico)

Gestión de datos

- Filtros
- Búsqueda interna de datos y vistas de archivos

Búsqueda por palabras clave e índices

- Búsqueda por palabra clave - Gestión
  - Texto, hexadecimal y expresiones regulares (PCRE)
- Técnicas de análisis y búsqueda dtSearch

Marcadores - Notas y observaciones del investigador

- Relación entre marcadores e informes
- Marcadores manuales y automáticos
- Modificación de marcadores

Nivel Tres

Examinación de la Copia en Sombra

- Identificación de la Copia en sombra
- Restauración de archivos de la Copia en sombra
- Análisis forense de la Copia en sombra
- Recreación de puntos de restauración históricos

Live Boot / Mount Image Pro / Máquina virtual

- Virtualización Live Boot de la evidencia del sujeto
- Bypass de contraseñas / recuperación de cuentas de usuario
- Live Boot desplegable para VirtualBox

Análisis de valores Hash

- Valores hash y algoritmos
- Creación y uso de conjuntos hash

Análisis de firmas de restauración de archivos

- Análisis de firma de archivos
- Identificación de firma / encabezado y pie de página de archivos
- Recuperación de particiones eliminadas

Módulo de correo electrónico

- Gestión de correo electrónico y compatibilidad
- Identificación y análisis de correos electrónicos y sus archivos adjuntos

Módulo del Registro

- Análisis automatizado del registro
- Claves de registro eliminadas

Introducción a la funcionalidad de Scripting (archivo de comandos) de FEX

- Funcionalidad de scripts en la interfaz FEX
- Uso de scripts automatizados
- Análisis gráfico y reconocimiento facial

Nivel Cuatro

Redacción y gestión de informes

- Creación rápida de informes en MS Word
- Uso de plantillas de informes de manera predeterminada
- Personalización de plantillas de informes
- Presentación de informes

Visor FEX / Portátil

- Revisión del caso con el Dongle free viewer / portátil

Práctica final

- Evaluación práctica que abarca todos los aspectos de las actividades de los cuatro días anteriores
- Otorgar la certificación de “Examinador Certificado de Forensic Explorer (FEXCE)”»