GUIA EJECUCION AUDITORIA

Metodología

- La Informática Forense es una disciplina criminalística que tiene como objeto la investigación en sistemas informáticos de hechos con relevancia jurídica.
- Conjunto multidisciplinario de teorías, técnicas y métodos de análisis que brindan soporte conceptual y procedimental a la investigación de la prueba informática.

Objetivos

- Ayuda a recuperar, analizar y preservar el ordenador y los materiales relacionados de tal manera que ayuda a la agencia de investigación a presentarlos como evidencia en un tribunal de justicia.
- Ayuda a postular el motivo detrás del crimen y la identidad del principal culpable.
- Diseñar procedimientos en una presunta escena del crimen que ayudan a garantizar que la evidencia digital obtenida no esté corrupta.
- Adquisición y duplicación de datos: recuperación de archivos eliminados y particiones eliminadas de medios digitales para extraer la evidencia y validarlos.
- Ayuda a identificar la evidencia rápidamente y también permite estimar el impacto potencial de la actividad maliciosa en la víctima
- Producir un informe forense informático que ofrece un informe completo sobre el proceso de investigación.
- Preservar la evidencia siguiendo la cadena de custodia.

Metodología

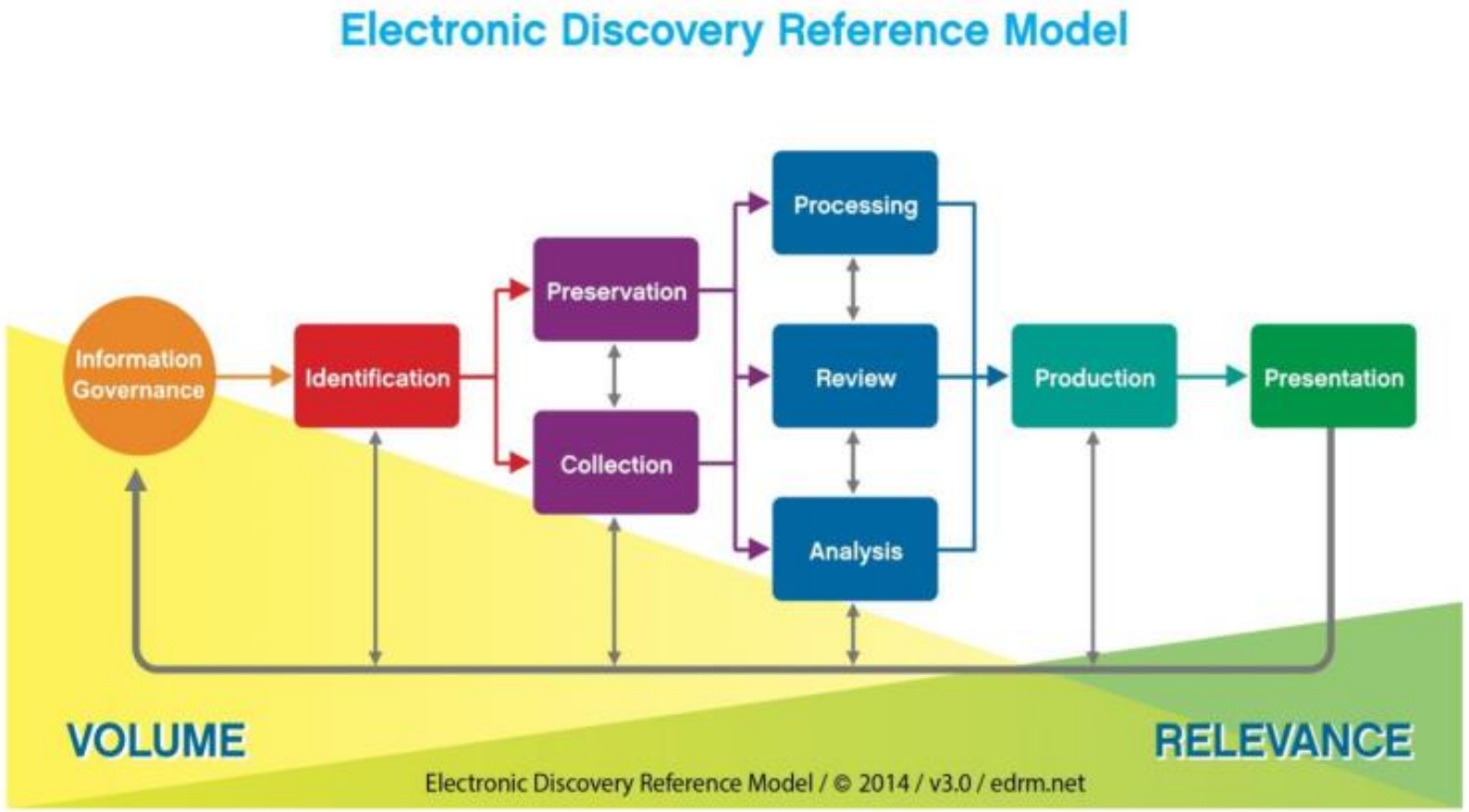
- Fases:
  - Identificación
  - Preservación
  - Recolección
  - Procesamiento
  - Revisión / Análisis
  - Producción
  - Presentación

Tipos

- **De sistemas operativos**
- **De redes**
- **En dispositivos móviles**
- **En la nube o Cloud**

Metodología

- Modelo EDRM: www.edrm.net



Metodología

- Fases:
  - Identificación: Hardware, software, responsables, dónde, cómo, credenciales, storage
  - Preservación: Aislarlos para que sean legalmente defendibles, razonables, amplios, pero a medida, auditables y repetibles. Cadena de Custodia.

Metodología

- Fases:
  - Recolección:
    - Validar las herramientas, licenciamiento válido, hash del ejecutable
    - Preparar la estación de trabajo forense
    - Preparar los dispositivos de almacenamiento mediante wipeado
  - Dead Collection.
    - Imagen forense, clonado bit a bit. Bloqueo contra escritura por hard o soft.
  - Live Collection
    - Verificar la imagen mediante un hash.

Herramientas para el análisis forense digital

- **Creación de imágenes (Clonado)**
  - Guymager.
  - **FTK Imager 4.7**
  - Magnet Aquire.
  - dc3dd.
  - dcfldd.

Herramientas para el análisis forense digital

- **Cálculo de Hash**
  - **HashCalc**
    - Se utiliza para calcular HMAC, resúmenes de mensajes y sumas de comprobación para archivos. También se puede usar para calcular cadenas hexadecimales y cadenas de texto. El programa proporciona 13 de los algoritmos de suma de comprobación y hash más comunes.
  - QuickHash
  - Karen hasher

Herramientas para el análisis forense digital

- **Análisis de memoria volátil**
- **Volatility**:
  - Se utiliza para la respuesta a incidentes y el análisis de malware. Con esta herramienta, puedes extraer información de procesos en ejecución, tomas de red, conexión de red, archivos DLL y colmenas de registro. También tiene soporte para extraer información de archivos de volcado por caída de Windows y archivos de hibernación. Esta herramienta está disponible de forma gratuita bajo licencia GPL.
- **Belkasoft Live RAM capturer**:
  - es una pequeña herramienta forense gratuita para extraer de forma confiable todo el contenido de la memoria volátil del ordenador, incluso si está protegido por un sistema activo de antidepurado o antidumping. Se encuentran disponibles versiones separadas de 32 y 64 bits para minimizar la huella de la herramienta tanto como sea posible. Los volcados de memoria capturados con Belkasoft Live RAM Capturer se pueden analizar con cualquier herramienta forense.

Herramientas para el análisis forense digital

- **Análisis de registros**
- descubrimiento y la extracción de información recopilada en la etapa de recopilación. El tipo de análisis depende de las necesidades de cada caso. Puede ir desde extraer un solo correo electrónico hasta unir las complejidades de un caso de fraude o terrorismo.
- **Ej: AccessData Registry Viewer**.

Herramientas para el análisis forense digital

- **Programas de análisis**
- **Sleuthkit**
  - Es una colección de herramientas de línea de comandos y una biblioteca C que permite analizar imágenes de disco y recuperar archivos de ellas. Se utiliza detrás de escena en Autopsia y en muchas otras herramientas forenses comerciales y de código abierto.
- **Encase Forensics**
  - Permite buscar, identificar y priorizar rápidamente evidencia potencial, en ordenadores y dispositivos móviles, para determinar si se justifica una investigación adicional. Esto dará como resultado una disminución de la cartera de pedidos para que los investigadores puedan concentrarse en cerrar el caso.

Herramientas para el análisis forense digital

- **Programas de análisis**
- **SIFT Workstation 3**
  - Es un grupo de herramientas forenses y de respuesta libre a incidentes de código abierto diseñadas para realizar exámenes forenses digitales detallados en una variedad de entornos. Puede coincidir con cualquier respuesta actual a incidentes y conjunto de herramientas forenses.
  - SIFT demuestra que las capacidades avanzadas de respuesta a incidentes y las técnicas forenses digitales de inmersión profunda para intrusiones se pueden lograr utilizando herramientas de código abierto de vanguardia que están disponibles gratuitamente y se actualizan con frecuencia.
- **OsForensics v6**
  - Proporciona una de las formas más rápidas y potentes de localizar archivos en un ordenador con Windows. Puede buscar por nombre de archivo, tamaño, fechas de creación y modificación, y otros criterios.
  - Los resultados se devuelven y están disponibles en varias vistas útiles diferentes. Esto incluye la Vista de línea de tiempo que le permite examinar las coincidencias en una línea de tiempo, lo que evidencia el patrón de actividad del usuario en la máquina.
  - OSForensics también puede buscar el contenido de los archivos y devolver resultados casi instantáneamente después de la indexación. Es capaz de buscar dentro de los formatos de archivo más comunes y funciona con el motor de búsqueda Zoom de gran precisión de Wrensoft .

Más Herramientas para el análisis forense digital OPEN SOURCE

- Adquisición y Análisis:
  - Forensic Exchange EDB Viewer v5.0
  - Free Gmail Forensics Software v4.0
  - Forensic PST Viewer v5.0
  - Forensic SQLite Viewer v2.0
  - Kernel for Exchange EDB to PST Converter
  - MFCMapi: Archivos PT
- Video: Video Cleaner.
- Metadata: MediaInfo
- Análisis de registros del sistema: Registry manager
- Análisis Hexadecimal:
  - Winhex
  - Zeroview

Más Herramientas para el análisis forense digital OPEN SOURCE

- Data Carving:
  - Foremost
  - Scalpel
- Recuperación de archivos borrados
  - NTFS Recovery
  - Recuva
  - RecoverRS
- Cifrado:
  - Truecrypt
  - Bitlocker
  - Zeroview
- Análisis de tráfico de red:
  - Wireshark
  - NetworkMiner
  - Snort

Más Herramientas para el análisis forense digital OPEN SOURCE

- RAM:
  - RedLine
  - DumpIt
  - Memorize

Hardware y Software propietario

HARDWARE

Bloqueadores Forenses

- Tableau T8u Forensic USB 3.0 Bridge
- Tableau T6u Forensic SAS Bridge
- Tableau T35u-RW Forensic SATA / IDE Bloqueador de lectura-escritura
- Tableau T35u Forensic SATA/IDE Bridge
- Tableau T7u Forensic PCIe Bridge
- Tableau T9 Forensic FireWire Bridge

Duplicadores/Clonadores Forenses

- Tableau TX1
- Tableau TD2u
- OSForensics Colección Rainbow Table & Hash Set
- Logicube SuperSonix®-NG PCIe
- Logicube Talon Ultimate

Computadores Forenses

- HTCI EDAS FOX Ultimate Investigator 2023
- HTCI EDAS FOX Data Crusher 2023
- Digital Intelligence FRED SR
- Digital Intelligence FRED Workstations
- EDAS FOX Oxygenator
- HTCI EDAS FOX Laptops
- Digital Intelligence FRED L

Accesorios

SOFTWARE

Análisis de Datos Extraídos

- Passware Kit Forensic
- Oxygen Forensic® Extractor
- Oxygen Forensic® Detective Network
- OSForensics V8
- MSAB XAMN pro
- Magnet Axiom
- Magnet Axiom Cyber
- EnCase® Forensic

Análisis Discos Duros y Computadores

- OSForensics Unidad Flash USB Arranque
- Magnet Axiom Cyber
- Intella Pro
- AccessData Summation
- Exterro FTK

Análisis Datos y Evidencia Masiva

- Exterro FTK Central

Análisis DVR

- DME Forensics DVR Examiner

Extracción Información

- X1 Social Discovery
- Oxygen Forensic® Extractor
- Oxygen Forensic® Detective Network
- MSAB XRY
- Magnet Axiom
- Intella Pro
- DiskInternals Uneraser™
- DiskInternals RAID Recovery™
- DiskInternals Partition Recovery™
- Compelson MOBILedit Forensic Express

Dispositivos Móviles (Drones, celulares, tarjetas de memoria, USB)

- MSAB XRY
- Magnet Axiom
- Magnet Axiom Cyber

Nube

- Magnet Axiom
- Magnet Axiom Cyber
- Compelson MOBILedit Forensic Express

Discos Duros y Computadores

- Magnet Axiom
- Magnet Axiom Cyber
- Intella Pro
- Exterro FTK

Hardware y Software propietario

- Hardware

–Bloqueador de escritura:

- Tableau Forensic Universal Bridge: U$ 1139.33 + imp (env incl)

Hardware y Software propietario

- Hardware

–Imágenes Forenses:

- Tableau Forensic Duplicator: U$ 1654.66 + imp (env incl)
- CRU Ditto DX: U$ 2249 + imp + env
- Falcon Neo

Hardware y Software propietario

- Software

–EnCaseForensic:

  –https://www.guidancesoftware.com/encase-forensic

–GriffEye Analyze:

  –https://www.griffeye.com/

–F-Response v8:

  –https://www.f-response.com/

–BCWIPE: https://www.jetico.com/data-wiping/wipe-files-bcwipe

–Nuix: https://www.nuix.com/

–Relativity: https://www.relativity.com/

–OSForensics: https://www.osforensics.com/

INFORME

Elaborar informe: Formato informe Auditoria

- Introducción
- Controles de Seguridad realizados
- Conclusiones
- Recomendaciones
- Apéndice 1. Metodología aplicada
- Apéndice 2. Situación observada de los controles
- Acrónimos y glosario de términos

Metodología

- Presentación.
  - Exponer de forma clara y precisa.
  - Público no-técnico.
  - Mínimo necesario.

Metodología: Para poder elaborar controles y conclusiones

- Procesamiento
  - Visualizar, filtrar, indexar, normalizar y reducir datos.
  - Categorización de archivos, eliminar duplicados, recuperar archivos borrados
- Revisión / Análisis:
  - Comprender la información. Agrupando subconjuntos lógicos de información. Búsqueda mediante patrones, conceptos, palabras clave.
- Producción:
  - Preparar y producir los resultados de la investigación. Respetando los plazos.

Anexo ¿que debemos poner?: :Live Collection

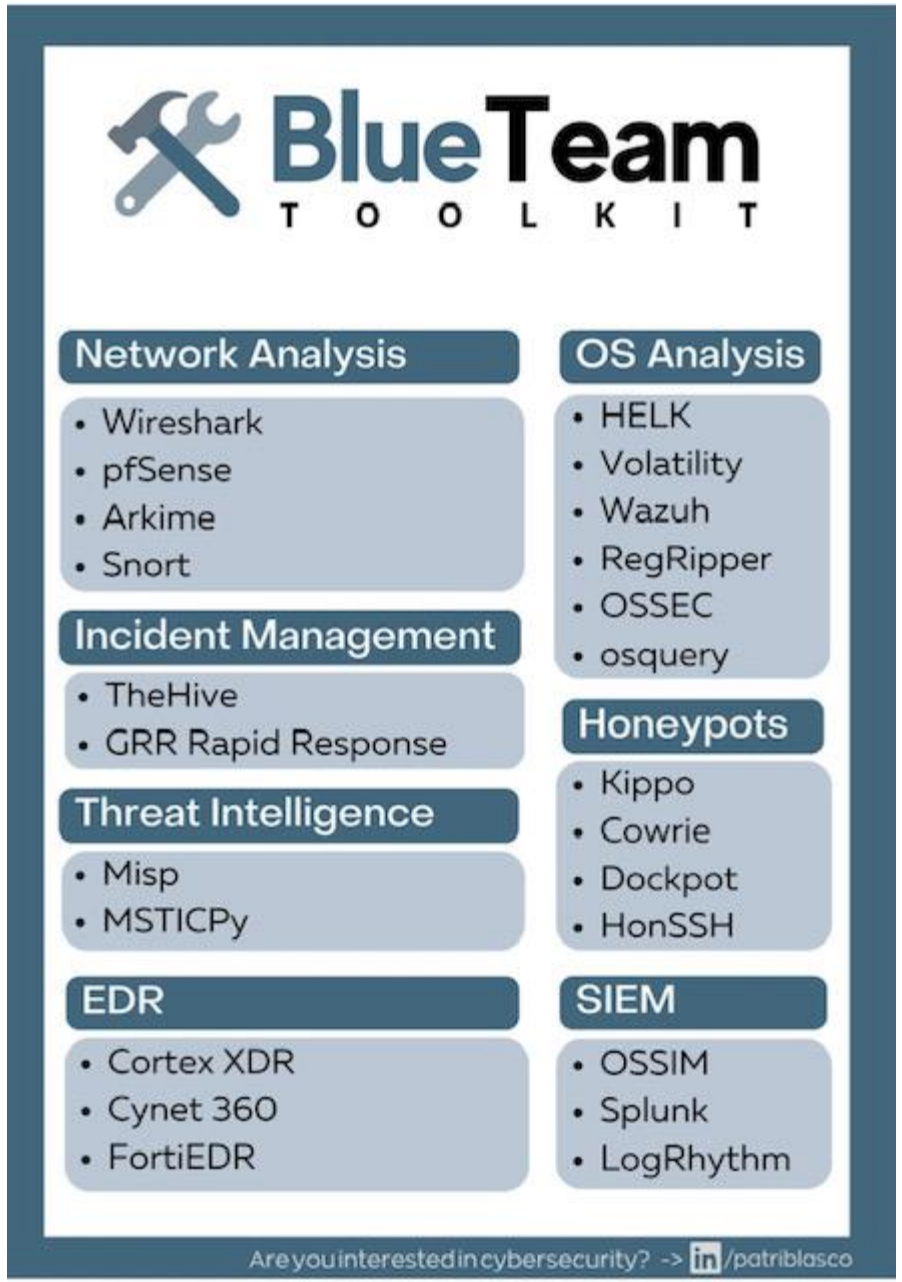
- Registros y contenidos de la caché
- Contenidos de la memoria
- Estado de las conexiones de red, tablas de rutas
- Estado de los procesos en ejecución
- Contenido del sistema de archivos y de los HD
- Contenido de otros dispositivos de almacenamiento

¿que debemos poner?: Live Collection

- Fecha y Hora
- Procesos activos
- Conexiones de red
- Puertos TCP/UDP abiertos y aplicaciones asociadas “a la escucha”
- Usuarios conectados local y remotamente

¿que debemos poner?: Live Collection

- Memoria RAM.
- Ejecución de comandos.
- Artefactos del SO: registro, prefetch, eventos, setupapi, etc.
- Artefactos de usuario: registro, shellbags, MRU, papelera de reciclaje, navegación, UserAssist, etc.
- Artefactos del sistema de archivos: Logs, $MFT, $UsnJrnl:$J.


BlueTeam
TOOLKIT
Network Analysis
• Wireshark
• pfSense
• Arkime
• Snort
Incident Management
• TheHive
• GRR Rapid Response
Threat Intelligence
• Misp
• MSTICPy
EDR
• Cortex XDR
• Cynet 360
• FortiEDR
OS Analysis
• HELK
• Volatility
• Wazuh
• RegRipper
• OSSEC
• osquery
Honeypots
• Kippo
• Cowrie
• Dockpot
• HonSSH
SIEM
• OSSIM
• Splunk
• LogRhythm
Are you interested in cybersecurity? -> in/patriblasco