Manual de Prácticas – Apto III

Información general

- **Materia:** SEMINARIO DE ACTUALIZACION TECNOLOGICA PERMANENTE PARA INGENIERO EN TELEINFORMATICA POR OPERACION VIRTUAL III
- **Duración del curso:** Inicio 16-01-2025 Fin 01-06-2025
- **Docente:** José Guadalupe Alvarado Ornelas
- **Número de prácticas:** 3 + Proyecto Final
- **Objetivo general:** Capacitar al estudiante en el análisis, recuperación, preservación e interpretación de evidencia digital mediante herramientas especializadas.

Práctica 1: Introducción a las herramientas forenses (Uso de OSForensics)

Objetivo:

Familiarizar a los alumnos con el uso de OSForensics para realizar análisis forense en un sistema, enfocándose Crear una imagen forense, montar una imagen forense en la recuperación de archivos, búsqueda avanzada y análisis de actividad del sistema.

Instrucciones Generales

1. Descarga e instala **OSForensics** en un equipo de prueba.
2. Trabaja en un equipo que contenga datos previamente preparados, como archivos eliminados, historial de navegadores, y logs de actividad.
3. Sigue los pasos indicados a continuación y entrega los resultados requeridos.

Actividad 1: Creación de un Caso

1. Abre OSForensics y selecciona la opción **"Create New Case"**.
2. Introduce un nombre para el caso y una breve descripción. Por ejemplo, "Investigación de dispositivo sospechoso".
3. Configura el caso para que guarde los datos en una carpeta específica.
4. Toma una captura de pantalla del caso recién creado y anexa la imagen en tu reporte.

Actividad 2: Recuperación de Archivos Eliminados

1. Utiliza la herramienta **"File Recovery"** para analizar una partición o disco que contenga archivos eliminados.
2. Recupera al menos 5 archivos eliminados.
3. Registra el nombre, ubicación original, tamaño y tipo de cada archivo recuperado en un informe.

Actividad 3: Análisis de Actividad del Sistema

1. Utiliza la herramienta **"System Activity"** para analizar el historial del sistema:
    - Identifica el historial de archivos abiertos recientemente.
    - Localiza eventos relevantes, como accesos a aplicaciones o cambios en el sistema.
2. Captura al menos dos eventos importantes y documenta:
    - Fecha y hora del evento.
    - Usuario que realizó la acción.
    - Descripción del evento.

Actividad 4: Búsqueda Avanzada de Archivos

1. Usa la herramienta **"Search Indexing"** para buscar archivos relacionados con términos específicos, como "proyecto", "contraseña", o cualquier palabra clave previamente asignada.
2. Filtra los resultados por tipo de archivo (PDF, DOCX, etc.) y encuentra al menos 3 archivos relevantes.

3. Anota los nombres y ubicaciones de los archivos encontrados.

Actividad 5: Creación de la Imagen Forense

1. Selecciona la opción "Disk Imaging" en el menú principal.
2. Selecciona **"Create New Disk Image"**
3. Asigna un nombre descriptivo a la imagen y proporciona detalles como caso, investigador y una breve descripción.

Montaje de la Imagen Forense

4. Ve a la opción "Mount Disk Image" en el menú principal de OSForensics.
5. Selecciona la imagen forense creada en la Parte 1.
6. Monta la imagen y accede a los archivos como si fueran parte de una unidad real.

Actividad 6: Análisis de Hash

1. Genera el hash MD5 o SHA1 de al menos 3 archivos sospechosos utilizando la opción **"Hash Set Viewer"**.
2. Compara los hashes generados con bases de datos de hash conocidas (si están disponibles en el laboratorio).
3. Documenta:
    - Nombre del archivo.
    - Hash generado.
    - Observaciones (¿El hash coincide con algún archivo malicioso?).

Entrega

1. Un informe con los siguientes apartados:
    - Introducción: Describe brevemente los objetivos y la metodología.
    - Evidencia: Incluye capturas de pantalla y descripciones de cada actividad.
    - Conclusiones: Reflexiona sobre el uso de OSForensics y los hallazgos obtenidos.
2. Entregar el informe en formato PDF.

Nota:

- Asegúrate de realizar esta práctica en un entorno controlado.
- No trabajes con datos sensibles reales sin el consentimiento correspondiente.

Práctica 2: Análisis de Metadatos en Imágenes con FOCA y Exif Viewer

Objetivo:

Aprender a identificar y extraer metadatos ocultos en imágenes digitales utilizando herramientas especializadas, con el fin de entender cómo estos datos pueden revelar información crítica sobre un archivo y su origen.

Material necesario:

- Una imagen previamente proporcionada por el profesor.
- PC con acceso a:

- **FOCA** (solo para Windows, puede descargarse desde ElevenPaths)
- **Exif Viewer** (puede usarse online: https://exifinfo.org o instalarse como extensión de navegador)

Instrucciones:

- **Parte 1: Análisis con FOCA**
  1. Abre FOCA y crea un nuevo proyecto.
  2. Importa la imagen proporcionada (click derecho > Add File).
  3. FOCA analizará automáticamente los metadatos disponibles.
  4. Revisa los datos extraídos, como:
     - Nombre del autor o usuario del equipo
     - Software o cámara utilizada
     - Fecha de creación/modificación
     - Ruta del archivo de origen
     - Coordenadas GPS (si están presentes)

Tarea 1:

Anota y explica qué metadatos importantes se pudieron extraer. ¿Qué riesgos implica compartir esa imagen con esos datos?

- **Parte 2: Análisis con Exif Viewer**
  1. Abre el navegador y accede a https://exifinfo.org.
  2. Carga fotos que usaste en FOCA.
  3. Revisa los resultados: detalles técnicos de la imagen y posible información GPS.
  4. Si aparecen coordenadas, copia y pega en Google Maps para ubicar el sitio exacto.

Tarea 2:

Compara los resultados entre FOCA y Exif Viewer. ¿Hay diferencias? ¿Qué herramienta te pareció más completa?

Reflexión final:

Responde en un párrafo:

- ¿Por qué es importante eliminar o revisar los metadatos antes de compartir imágenes?
- ¿Qué tipo de ataque o situación real podría aprovecharse de esta información?

Entrega esperada:

- Capturas de pantalla de los resultados obtenidos en FOCA y Exif Viewer.
- Documento con las respuestas a las tareas 1 y 2, y la reflexión final.

Aprendizaje obtenido:

- El estudiante comprende que las imágenes digitales pueden contener información sensible.
- Identifica herramientas útiles para análisis forense de archivos.
- Toma conciencia sobre privacidad digital.

Práctica 3: | de Red con Wireshark

Objetivo
Familiarizarse con el uso de Wireshark para capturar y analizar paquetes de red, identificando protocolos comunes, direcciones IP, puertos, y observando patrones de comunicación entre dispositivos en una red local.

Material necesario
- PC con Wireshark instalado
- Acceso a red local (puede ser una red Wi-Fi o LAN simple entre 2 PCs)

Consideraciones éticas
- Esta práctica se realiza en una red controlada y con consentimiento de los participantes.
- No se debe analizar tráfico ajeno ni redes públicas sin autorización.
- Evitar capturar credenciales reales; usar sitios de prueba o tráfico no sensible.

Instrucciones
1. Iniciar Wireshark
- Abre Wireshark y selecciona la interfaz de red activa (Wi-Fi o Ethernet).
- Presiona el botón **"Start capturing packets"** (ícono del tiburón azul).

2. Generar tráfico de red
Mientras Wireshark está capturando:
- Abre un navegador web y visita sitios como:
  - http://example.com
  - https://www.wikipedia.org
- Haz ping a algún sitio desde la terminal:

```
ping www.google.com
```

3. Detener la captura
- Vuelve a Wireshark y presiona **Stop** (cuadro rojo).

Actividades de análisis
A. Filtrar por protocolo
- En la barra de filtros, escribe:
  - http → Para ver solo tráfico HTTP
  - dns → Para ver peticiones DNS
  - icmp → Para ver los pings

B. Identificar IPs
- Observa las columnas de Source y Destination para identificar:
  - Tu dirección IP local

- IPs de servidores externos

C. Examinar un paquete HTTP

- Haz clic sobre un paquete HTTP y observa:
  - Método utilizado (GET, POST)
  - Host solicitado
  - User-Agent del navegador

D. Analizar una solicitud DNS

- Busca una consulta DNS y revisa:
  - Nombre del dominio solicitado
  - Dirección IP resuelta

Preguntas para reflexionar

1. ¿Qué protocolos observaste con mayor frecuencia?
2. ¿Cuál es la diferencia entre una petición HTTP y HTTPS?
3. ¿Qué IPs externas aparecen más comúnmente?
4. ¿Se puede saber a qué sitios web accedió un usuario usando Wireshark?

Opcional: Reto adicional

- Filtra solo tráfico TCP del puerto 80:

```
tcp.port == 80
```

- Intenta encontrar una cookie o encabezado HTTP en texto plano.

Aprendizaje obtenido:
Con esta práctica, los estudiantes habrán experimentado una introducción práctica a la captura y análisis de paquetes, comprendiendo cómo fluye la información a través de una red y la importancia de cifrar las comunicaciones.

Proyecto Final Apto III **Investigación Forense sobre el Caso Jimmy Wilson**

Recurso Central:
Imagen Forense: 2020JimmyWilson.E01
Formato: EnCase (E01)
Contenido: Disco duro de un sospechoso ficticio llamado Jimmy Wilson, involucrado en posibles actividades sospechosas.

Objetivo del Proyecto:
Realizar una investigación forense completa sobre la imagen de disco proporcionada, aplicando los conocimientos teóricos y prácticos adquiridos durante el curso, con el fin de:

- Preservar, analizar e interpretar evidencia digital.
- Recuperar archivos borrados u ocultos.
- Realizar análisis de metadatos y documentos.
- Buscar posibles indicios de actividad delictiva (hacking, fuga de información, acceso no autorizado, etc.).
- Presentar un informe profesional con conclusiones basadas en evidencia digital.

Herramientas para utilizar:
El proyecto debe incluir el uso **mínimo de 5 herramientas**, incluyendo obligatoriamente al menos:

- **OSForensics**
- **Autopsy**
- **Easy Professional Recovery**
- **Nmap**
- **Shodan**
- **La Foca**.

Actividades obligatorias:

1. **Montaje y verificación de la imagen**
   - Verifica la integridad de la imagen mediante hash MD5/SHA1.
   - Justifica los pasos de preservación de la evidencia.
2. **Análisis general del sistema**
   - Identifica el sistema operativo, nombre del usuario principal y estructura general de carpetas.
   - Registra el software instalado, actividad reciente y usuarios registrados.
3. **Recuperación de archivos**
   - Recupera al menos 3 archivos eliminados o escondidos e interpreta su contenido.
   - Verifica su relevancia en la investigación.
4. **Análisis de navegación y correos**
   - Extrae el historial de navegación, cookies, descargas y correos electrónicos (si los hay).
   - Investiga conexiones sospechosas o visitas a sitios no usuales.
5. **Análisis de metadatos**
   - Extrae metadatos de documentos, imágenes o PDFs encontrados.
   - Identifica autores, fechas de modificación o pistas relevantes.
6. **Investigación OSINT**
   - Utiliza La Foca, Nmap y Shodan para investigar correos, dominios, IPs o nombres encontrados en la imagen.
   - Incluye capturas y resultados del análisis.
7. **Informe final**
   - Presenta un informe técnico-profesional incluyendo:
     - Introducción y objetivos
     - Metodología
     - Herramientas utilizadas
     - Evidencias encontradas
     - Análisis e interpretación
     - Conclusiones y recomendaciones
     - Anexos con capturas y hashes

Entrega:

- **Fecha límite:** 18- mayo-2025
- **Formato:** PDF (informe), archivo comprimido con evidencias digitales relevantes
- **Evaluación:** Según rúbrica oficial del curso (puedo incluirla si la deseas nuevamente).

Criterios importantes:

- Todo hallazgo debe estar respaldado por evidencia técnica (capturas, rutas, hashes, logs, etc.).
- El trabajo debe ser original. Se penalizará cualquier plagio o copia directa.
- Se espera un análisis técnico riguroso, así como capacidad crítica para emitir recomendaciones finales.

Link de descarga de la imagen Forense:

https://drive.google.com/file/d/1aghBsw90jSL03sbVsnaQJ2QWByH30aYc/view?usp=sharing