Autopsy revelado

Software de análisis de evidencia Open Source

Ing María Andrea Vignau

Perito Forense Penal

Poder Judicial del Chaco

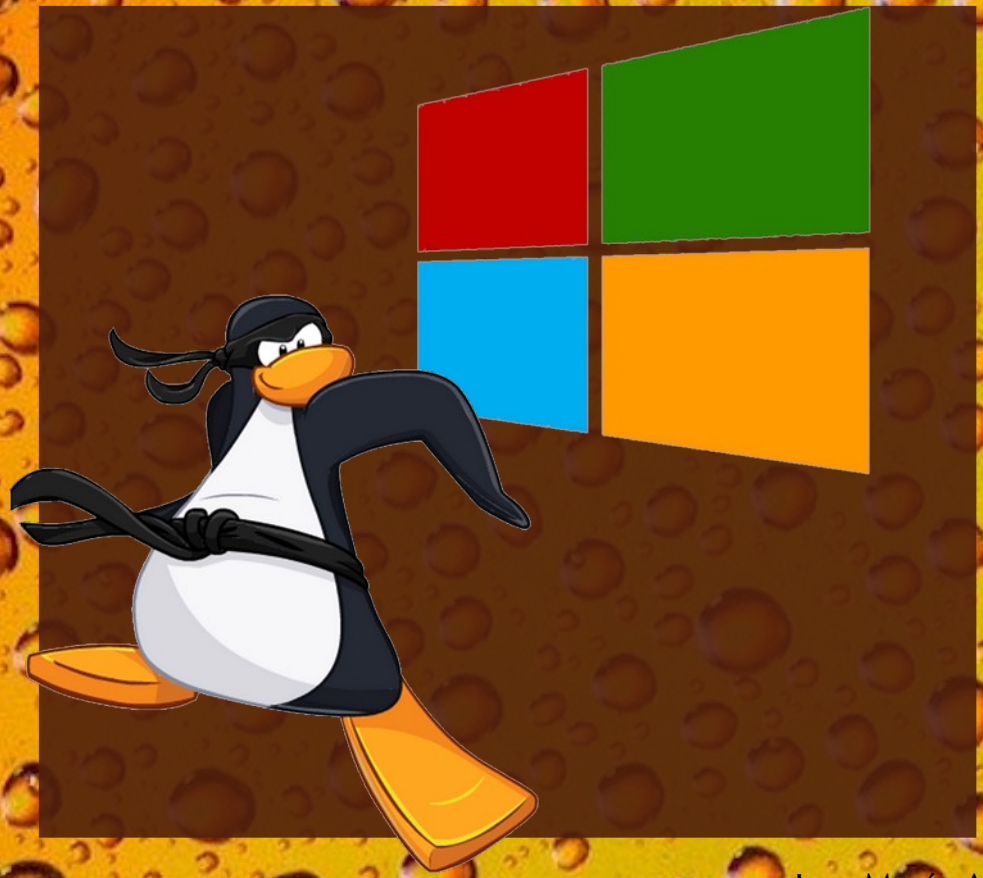
Autopsy revelado

- Instalación
- Presentación y conceptos
- Módulos automáticos
- Interfaces especiales
- Etiquetado y reportes

1

Instalación

Instalación



- **Mono usuario**
- Cada investigador en su propio caso
- En Windows y Linux

Instalación

Multiusuario

- Varios investigadores analizan un caso
- Servidores compartidos

2

Presentación

Presentación

- Crear caso
- Agregar fuentes de datos
- Correr módulos automáticos
- Analizar manualmente
- Etiquetar y reportar

Flujo de trabajo

Presentación

- **Árbol**
  - Fuentes de datos
  - Vistas
  - Resultados
  - Etiquetas
  - Reportes
- **Grilla**
- **Vista detalle**

Interfaz gráfica

Presentación

- Recupera archivos borrados
- Usa la estructura de los archivos.
- En espacio no utilizado
- No usa la información en el sistema de archivos.

Carving

Presentación

- No están vinculados a un directorio que los contenga.

Archivos huérfanos

Orphan

Presentación

- Guarda información entre diferentes casos.
- Al volver a encontrar el archivo etiquetado se lo marca como “notable”

Motor de correlación

Presentación

- Autopsy.db

Directorios

- Exportación
- Reportes
- Salida de módulos

Estructura de un caso

3

Fuentes de datos

Fuentes de datos

Tipos

- Imágenes de disco
- Unidades y directorios
- Imager de Autopsy
- Archivos
- Volcados de memoria

Fuentes de datos

Imágenes de disco

- imágenes crudas “raw” (.bin, .raw, etc)
- encase images .E01 etc
- virtual machines
  - vmdk
  - vhd

Fuentes de datos

Sistemas de particionado

- DOS, GPT, MAC, BSD SOLARIS

Sistemas de archivos

- NTFS, FAT, exFAT
- HFS+ ISO9660
- Ext2/3/4
- YAFFS2 UFS

Fuentes de datos

Escanea

fuente de datos

Almacena

- Nombre de archivos
- Fechas y horas
- Tamaño
- MD5
- Esquema de particionado

Módulos de procesamiento

Pizarra

Artefactos

- Estructura de datos
- Atributos
  - Par tipo y valor

4

Módulos de procesamiento

Módulos de procesamiento

- Navegación:
  - Bookmarks
  - Cookies
  - Downloads
  - Formularios
- Se agrupan juntos

Actividad reciente

Módulos de procesamiento

- Análisis del registro
  - USB
  - Cuentas de usuario
  - ShellBags
  - Programas instalados
- Papelera
  - Recupera archivos

Actividad reciente

(RegRipper)

Módulos de procesamiento

- Usa la file signature
  - No la extensión
- El tipo desconocido es:

application/octet-stream

- No concordancia podría ser ocultamiento.

Tipo de archivo

Extensiones que no concuerdan

Módulos de procesamiento

- Tipo de dispositivo
- Extrae
  - Cámara
  - Hora y fecha
  -

Extracción de EXIF

Módulos de procesamiento

- Abre archivos comprimidos
  - ZIP; RAR; etc
- Extrae imágenes de
  - PDF, DOCX, etc
  - Marca si está protegido por clave

Extracción de Archivos embebidos

Módulos de procesamiento

- Abre archivos de email.
  - MBOX, PST, EML
  - Agrega a pizarra
  - Agrupo por hilos
  - Agrego adjuntos como dependientes.

Extracción de emails

Módulos de procesamiento

- Reglas que permitan identificar archivos especiales:
  - Billeteras, máq. Virtuales, etc.
- Por tipo, nombre, path, tamaño, fechas, etc

Filtros para

Archivos interesantes

Módulos de procesamiento

- Identifica archivos que podrían estar encriptados
  - Alta entropía
  - Sin tipo conocido
- Detecta contraseñas en documentos de Ofice

Detección de archivos encriptados

Módulos de procesamiento

- Crear indices de texto
- Usa Apache Solr
- Contiene nombre de archivo, contenido y artefactos.
- Listas de palabras claves

Palabras clave

Módulos de procesamiento

- **Normaliza**
  - Upper/lower case
  - Unicode
- **Busca**
  - Coincidencia exacta
  - Subcadenas
  - Expresiones regulares

Palabras clave

Módulos de procesamiento

- Extrae fechas y horas
  - Usa PLASO
- Puede duplicar los extraído por Autopsy
- Tarda bastante tiempo
  - Winreg y PE

PLASO

Eventos temporales

Módulos de procesamiento

- Detecta discos virtuales como VMDK y VHDI
- Los agrega como fuentes de datos.

Extracción de máquinas virtuales.

Módulos de procesamiento

- Calcula los hash MD5
- Los almacena en BBDD
- Los busca y marca
- Evitar analizar archivos conocidos por NSRL
- Identifica archivos conocidos
- Mantiene un repositorio central

Búsqueda por hash

Módulos de procesamiento

El estado de conocimiento del hash

- Conocido como malo o notable
- Conocido
  - Se evita procesarlo y se lo esconde (optativo)
- Desconocido

Búsqueda por hash

Módulos de procesamiento

- Analiza BD SQLite y archivos
- Agrega a la pizarra
- Extracciones físicas o lógicas

Analizador para Android

Módulos de procesamiento

- Logs de llamadas
- Contactos
- Mensajes
  - SMS, Whastapp, Messenger
- Browsers: cookies, bookmaks
- Geolocalización
- Aplicaciones

Analizador para Android

5

Interfaces especiales

Interfaces especiales

Línea de tiempo

Vistas

- **Cuentas**
  - Gráfico de barras
- **Detalles**
  - Eventos específicos, agrupados
- **Lista**
  - Tabla de los eventos

Interfaces especiales

Línea de tiempo

Vistas de detalle

- **Pin**
  - Fijar un evento y no perderlo
- **Hide**
  - Ocultar elementos comunes
- **Place marker**
  - Marcar un momento

Interfaces especiales

Galería de imágenes

Interfaces especiales

Mapa geográfico

- Puntos geolocalizados
- Artefactos

Interfaces especiales

Comunicaciones

Cuentas relacionadas

- Por llamada o mensajes
- En los contactos

Cuenta de dispositivo

- Representa un dispositivo físico

5

Etiquetar, y comentar

Reportes

Etiquetar y Reportar

- Etiquetas
  - referencia futura
  - reportes
- Se pueden editar, crear o agregar
- Se agregan comentarios
- Se asocian al usuario

Características

Etiquetar y Reportar

- Archivos
- Resultados (Artefactos)
- Regiones de imágenes
- Si se agregan comentarios

Qué puedo etiquetar

Etiquetar y Reportar

Qué se puede incluir

- Todo
- Todo los etiquetado
- Parte de lo etiquetado

Reportes

Etiquetar y Reportar

- HTML, Excel
- Archivo de texto
- KML de Google Earth
  - GPS + EXIF
- Genera hash set
- Caso portable

Tipos de reporte

Etiquetar y Reportar

- Base de datos parcial
- Se comprime en volúmenes
- Se abre en Autopsy
- Se usa como otro caso.

Caso portable

Autopsy revelado

por María Andrea Vignau

Ing en Sistemas de Información
Perito Informático Forense
Poder Judicial Chaco

Twitter: @mavignau
Telegram: @mavignau
GitHub: marian-vignau