



## Módulo 1 (Curso 2020/21): Análisis forense de sistemas. Auditoría Informática II



Catálogos con una clasificación de las herramientas que hay disponibles:

<https://toolcatalog.nist.gov/taxonomy/index.php>

<https://www.dfir.training/tools-sw-hw/>

### Entornos:

Kali (bastante sencilla): <https://www.kali.org/downloads/>

CAINE 7 (Computer Aide Investigation Environment)

SIFT (SANS Investigative Forensic Toolkit)

DEFT

### SW:

#### GRUPO 1 - ADQUISICIÓN Y ANÁLISIS DE LA MEMORIA

Set de utilidades que permite la adquisición de la memoria RAM para posteriormente hacer un análisis con ella.

**pd** – Process Dumper - Convierte un proceso de la memoria a fichero.

**FTK Imager** – Permite entre otras cosas adquirir la memoria.

**Dumplt** – Realiza volcados de memoria a fichero.

**Responder CE** – Captura la memoria y permite analizarla.

**Volatility** – Analiza procesos y extrae información útil para el analista.

**RedLine** – Captura la memoria y permite analizarla. Dispone de entorno gráfico.

**Memorize** – Captura la ram (Windows y OSX).

#### GRUPO 2 - MONTAJE DE DISCOS

Utilidades para montar imágenes de disco o virtualizar unidades de forma que se tenga acceso al sistema de ficheros para posteriormente analizarla.



## Módulo 1 (Curso 2020/21): Análisis forense de sistemas. Auditoría Informática II



**ImDisk** – Controlador de disco virtual.

**OSFMount** – Permite montar imágenes de discos locales en Windows asignando una letra de unidad.

**raw2vmdk** – Utilidad en java que permite convertir raw/dd a .vmdk

**FTK Imager** – Comentada anteriormente, permite realizar montaje de discos.

**vhdtool** – Convertidor de formato raw/dd a .vhd permitiendo el montaje desde el administrador de discos de Windows .

**LiveView** – Utilidad en java que crea una máquina virtual de VMware partiendo de una imagen de disco.

**MountImagePro** – Permite montar imágenes de discos locales en Windows asignando una letra de unidad.

### GRUPO 3 - CARVING Y HERRAMIENTAS DE DISCO

Recuperación de datos perdidos, borrados, búsqueda de patrones y ficheros con contenido determinado como por ejemplo imágenes, vídeos. Recuperación de particiones y tratamiento de estructuras de discos.

**PhotoRec** – Muy útil, permite la recuperación de imágenes y vídeo.

**Scalpel** – Independiente del sistema de archivos. Se puede personalizar los ficheros o directorios a recuperar.

**RecoverRS** – Recupera urls de acceso a sitios web y ficheros. Realiza carving directamente desde una imagen de disco.

**NTFS Recovery** – Permite recuperar datos y discos aún habiendo formateado el disco.

**Recuva** – Utilidad para la recuperación de ficheros borrados.

**Raid Reconstructor** - Recuperar datos de un RAID roto, tanto en raid 5 o raid 0. Incluso si no conocemos los parámetros RAID.

**CNWrecovery** – Recupera sectores corruptos e incorpora utilidades de carving.

**Restoration** – Utilidad para la recuperación de ficheros borrados.

**Rstudio** – Recuperación de datos de cualquier sistema de disco NTFS, NTFS5, ReFS, FAT12/16/32, exFAT, HFS/HFS+ (Macintosh), Little y Big Endian en sus distintas variaciones UFS1/UFS2 (FreeBSD/OpenBSD/NetBSD/Solaris) y particiones Ext2/Ext3/Ext4 FS.

**Freerecover** – Utilidad para la recuperación de ficheros borrados.

**DMDE** – Admite FAT12/16, FAT32, NTFS, y trabaja bajo Windows 98/ME/2K/XP/Vista/7/8 (GUI y consola), DOS (consola), Linux (Terminal) e incorpora utilidades de carving.



## Módulo 1 (Curso 2020/21): Análisis forense de sistemas. Auditoría Informática II



**IEF** – Internet Evidence Finder Realiza carving sobre una imagen de disco buscando mas de 230 aplicaciones como chat de google, Facebook, IOS, memoria ram, memoria virtual,etc.

**Bulk\_extractor** – Permite extraer datos desde una imagen, carpeta o ficheros.

### GRUPO 4 - UTILIDADES PARA EL SISTEMA DE FICHEROS

Conjunto de herramientas para el análisis de datos y ficheros esenciales en la búsqueda de un incidente.

**analyzeMFT** – David Kovar's utilidad en python que permite extraer la MFT

**MFT Extractor**- Otra utilidad para la extracción de la MFT

**INDXParse** – Herramienta para los indices y fichero \$I30.

**MFT Tools** (mft2csv, LogFileParser, etc.) Conjunto de utilidades para el acceso a la MFT

**MFT\_Parser** – Extrae y analiza la MFT

**Prefetch Parser** – Extrae y analiza el directorio prefetch

**Winprefetchview** – Extrae y analiza el directorio prefetch

**Fileassassin** – Desbloquea ficheros bloqueados por los programas

### GRUPO 5 - ANÁLISIS DE MALWARE

PDF Tools de Didier Stevens.

**PDFStreamDumper** – Esta es una herramienta gratuita para el análisis PDFs maliciosos.

**SWF Mastah** – Programa en Python que extrae stream SWF de ficheros PDF.

**Process explorer** – Muestra información de los procesos.

**Captura BAT** – Permite la monitorización de la actividad del sistema o de un ejecutable.

**Regshot** – Crea snapshots del registro pudiendo comparar los cambios entre ellos

**Bintext** – Extrae el formato ASCII de un ejecutable o fichero.

**LordPE** – Herramienta para editar ciertas partes de los ejecutables y volcado de memoria de los procesos ejecutados.

**Firebug** – Analisis de aplicaciones web.

**IDA Pro** – Depurador de aplicaciones.

**OllyDbg** – Desensamblador y depurador de aplicaciones o procesos.

**Jsunpack-n** – Emula la funcionalidad del navegador al visitar una URL. Su propósito es la detección de exploits.



## Módulo 1 (Curso 2020/21): Análisis forense de sistemas. Auditoría Informática II



**OfficeMalScanner** – Es una herramienta forense cuyo objeto es buscar programas o ficheros maliciosos en Office.

**Radare** – Framework para el uso de ingeniería inversa.

**FileInsight** – Framework para el uso de ingeniería inversa.

**Volatility** – Framework con los plugins malfind2 y apihooks.

**shellcode2exe** – Conversor de shellcodes en binarios.

### GRUPO 6 – FRAMEWORKS

Conjunto estandarizado de conceptos, prácticas y criterios en base a el análisis forense de un caso.

**PTK** – Busca ficheros, genera hash, dispone de rainbow tables. Analiza datos de un disco ya montado.

**Log2timeline** – Es un marco para la creación automática de un super línea de tiempo.

**Plaso** – Evolución de Log2timeline. Framework para la creación automática de un super línea de tiempo.

**OSForensics** – Busca ficheros, genera hash, dispone de rainbow tables. Analiza datos de un disco ya montado.

**DFF** – Framework con entorno gráfico para el análisis.

**SANS SIFT Workstation** – Magnifico Appliance de SANS. Lo utilizo muy a menudo.

**Autopsy** – Muy completo. Reescrito en java totalmente para Windows. Muy útil.

### GRUPO 7 - ANÁLISIS DEL REGISTRO DE WINDOWS

Permite obtener datos del registro como usuarios, permisos, ficheros ejecutados, información del sistema, direcciones IP, información de aplicaciones.

**RegRipper** – Es una aplicación para la extracción, la correlación, y mostrar la información del registro.

**WRR** – Permite obtener de forma gráfica datos del sistema, usuarios y aplicaciones partiendo del registro.

**Shellbag Forensics** – Análisis de los shellbag de windows.

**Registry Decoder** – Extrae y realiza correlación aun estando encendida la máquina datos del registro.



## Módulo 1 (Curso 2020/21): Análisis forense de sistemas. Auditoría Informática II



### GRUPO 8 - HERRAMIENTAS DE RED

Todo lo relacionado con el tráfico de red, en busca de patrones anómalos, malware, conexiones sospechosas, identificación de ataques, etc.

**WireShark** – Herramienta para la captura y análisis de paquetes de red.

**NetworkMiner** – Herramienta forense para el descubrimiento de información de red.

**Netwitness Investigator** – Herramienta forense. La versión 'free edition' está limitado a 1GB de tráfico.

**Network Appliance Forensic Toolkit** – Conjunto de utilidades para la adquisición y análisis de la red.

**Xplico** – Extrae todo el contenido de datos de red (archivo pcap o adquisición en tiempo real). Es capaz de extraer todos los correos electrónicos que llevan los protocolos POP y SMTP, y todo el contenido realizado por el protocolo HTTP.

**Snort** – Detector de intrusos. Permite la captura de paquetes y su análisis.

**Splunk** – Es el motor para los datos y logs que generan los dispositivos, puestos y servidores. Indexa y aprovecha los datos de las generados por todos los sistemas e infraestructura de IT: ya sea física, virtual o en la nube.

**AlientVault** – Al igual que Splunk recolecta los datos y logs aplicándoles una capa de inteligencia para la detección de anomalías, intrusiones o fallos en la política de seguridad.

### GRUPO 9 - RECUPERACIÓN DE CONTRASEÑAS

Todo lo relacionado con la recuperación de contraseñas en Windows, por fuerza bruta, en formularios, en navegadores.

**Ntpwedit** – Es un editor de contraseña para los sistemas basados en Windows NT (como Windows 2000, XP, Vista, 7 y 8), se puede cambiar o eliminar las contraseñas de cuentas de sistema local. No valido para Active Directory.

**Ntpasswd** – Es un editor de contraseña para los sistemas basados en Windows, permite iniciar la utilidad desde un CD-LIVE

**pwdump7** – Vuelca los hash. Se ejecuta mediante la extracción de los binarios SAM.

**SAMInside / OphCrack / L0phtcrack** – Hacen un volcado de los hash. Incluyen diccionarios para ataques por fuerza bruta.

### GRUPO 10 - DISPOSITIVOS MÓVILES

Esta sección dispone de un set de utilidades y herramientas para la recuperación de datos y análisis forense de dispositivos móviles. He incluido herramientas comerciales dado que utilizo algunas de ellas y considero que son muy interesantes e importantes.

#### iPhone

**iPhoneBrowser** – Accede al sistema de ficheros del iphone desde entorno gráfico.

**iPhone Analyzer** – Explora la estructura de archivos interna del iphone.

**iPhoneBackupExtractor** – Extrae ficheros de una copia de seguridad realizada anteriormente.

**iPhone Backup Browser** – Extrae ficheros de una copia de seguridad realizada anteriormente.

**iPhone-Dataprotection** – Contiene herramientas para crear un disco RAM forense, realizar fuerza bruta con contraseñas simples (4 dígitos) y descifrar copias de seguridad.

**iPBA2** – Accede al sistema de ficheros del iphone desde entorno gráfico.

**sPyphone** – Explora la estructura de archivos interna.

#### Android

**android-locdump** – Permite obtener la geolocalización.

**androguard** – Permite obtener, modificar y desensamblar formatos DEX/ODEX/APK/AXML/ARSC

**viaforensics** – Framework de utilidades para el análisis forense.

**Osaf** – Framework de utilidades para el análisis forense.

**MOBILedit Forensic** – Herramienta que extrae y analizar en profundidad el contenido de un teléfono móvil.