

Creando una Trayectoria Profesional en Seguridad Digital: Análisis Forense Digital

Agosto, 2021

Tabla de contenidos

Capacitación en Ciberseguridad OEA

Introducción a Análisis Forense Digital

Breve introducción a los sistemas de archivos

Análisis de bitácoras

Análisis de binarios

El registro de Windows

Proceso y linea de tiempo del análisis forense digital

Capacitación en Ciberseguridad OEA

Introducción al Análisis Forense Digital

Se presentarán técnicas y procedimientos prácticos para recopilar y analizar evidencia de información digital en el marco de la informática forense. **El módulo contiene una práctica y un examen en línea.**

Introducción a Análisis Forense Digital (1/2)

En esta sesión se abordaran los siguientes temas:

- ▶ Introducción al análisis forense digital
- ▶ Breve introducción a los sistemas de archivos
- ▶ Bitácoras (*Logs*) y registro de eventos
- ▶ Análisis de binarios: Virus Total
- ▶ El registro de Windows y artefactos forenses
- ▶ La línea de tiempo forense

A continuación se listan algunos de los principios que conducen la base del análisis forense digital:

- ▶ **Principio de intercambio de Locard's:** *Siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto.* E.j. Pintura de dos autos que chocan

Introducción a Análisis Forense Digital (2/2)

- ▶ **Principio de la navaja de Ockham:** *En igualdad de condiciones, la explicación más sencilla suele ser la correcta.*
E.j. KISS (*Keep it simple, stupid!*)
- ▶ **El principio de Alexiou:** *¿Qué pregunta quiero contestar?*
¿Qué datos necesito para responder? E.j. No especular. Dejar que los datos cuenten la historia.

Breve introducción a los sistemas de archivos (1/2)

¿Qué es un sistema de archivos

- ▶ Un sistema de archivos establece un sistema de organización lógico para almacenamiento de datos en un medio físico
- ▶ Facilita a usuarios (y programas) crear, alterar, copiar y borrar archivos



XFS
FAT



HFS
FAT



NTFS
FAT

Figura 1: Formatos de disco, para diferentes sistemas operativos.

Breve introducción a los sistemas de archivos (2/2)

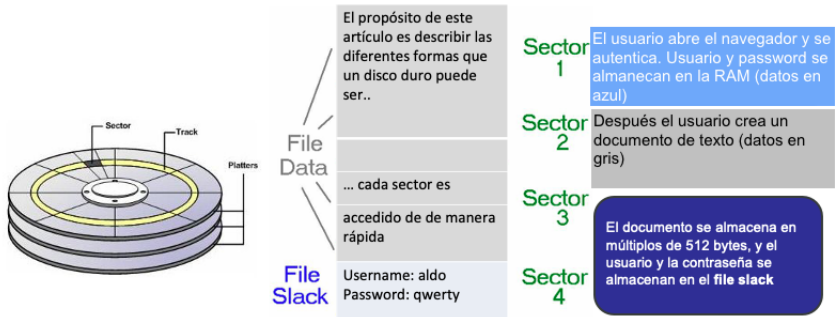


Figura 2: Diagrama de escritura de disco, con sus componentes y sectores.

Análisis de bitácoras (1/5)

Bitácoras (*Logs*) y registro de eventos

- ▶ El detalle de las bitácoras depende de la funcionalidad del dispositivo y de su configuración
- ▶ Los dispositivos de red que pueden ser útiles en en análisis de bitácoras son:
 - ▶ Routers
 - ▶ Switches
 - ▶ Firewalls
 - ▶ IDS/IPS
 - ▶ Web application firewalls (WAFS) y firewalls físicos
 - ▶ Servidores Proxy
 - ▶ Aplicativos anti-malware

Análisis de bitácoras (2/5)

- ▶ Es común analizar **bitácoras de firewalls**, ya que estos son dispositivos muy comunes en la mayoría de las redes empresariales
- ▶ Los registros de bitácora recolectados de forma adecuada deben ser convertidos en un formatos fáciles de leer e interpretar:
 - ▶ Delimitados por coma (CSV)
 - ▶ Delimitados por tabuladores
 - ▶ Syslog (búsqueda por patrones o *expresiones regulares*)
 - ▶ SNMP (Simple Network Management Protocol)
- ▶ Una vez convertidos, hay múltiples herramientas disponibles para la **visualización de datos**

Análisis de bitácoras (3/5)

¿Qué son las expresiones regulares?

Las expresiones regulares, a veces abreviadas *regex*, son cadenas de texto que permiten **crear patrones** que ayudan a localizar y gestionar el texto.

Análisis de bitácoras (4/5)

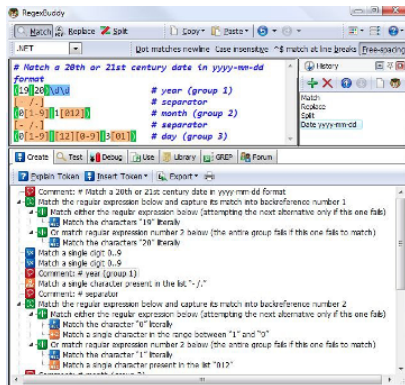


Figura 3: Una herramienta para construir expresiones regulares es [RegexBuddy](#).

Análisis de bitácoras (5/5)

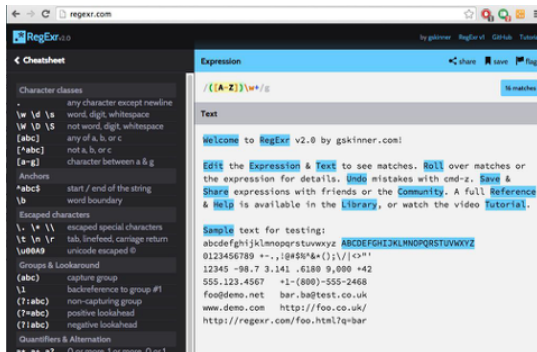


Figura 4: Múltiples sitios web permiten evaluar expresiones regulares. Uno de los más utilizados es regexr.com.

Análisis de binarios (1/7)

¿Qué es el análisis de binarios?

El análisis de binarios o de código de binarios, es un **procedimiento de evaluación** de amenazas y vulnerabilidades, probando un binario (ejecutable) a nivel de código. Existen dos tipos de implementaciones:

- ▶ **Estático:** es realizado en un **ambiente fuera de línea**. Su fortaleza radica en examinar el código fuente, código en bits o binarios de la aplicación
- ▶ **Dinámico:** se encarga de examinar los **patrones de comportamiento** durante la ejecución del programa

Análisis de binarios (2/7)

¿Qué es una APT?

Una APT (Advanced Persistent Threat) es una técnica continua y sofisticada para gaanar acceso a un sistema y permanecer dentro de manera prolongada y potencialmente destructiva.

- ▶ Existen herramientas en línea que permiten analizar un archivo o binario con **múltiples motores de diferentes vendedores de antivirus**
- ▶ Identifican propiedades estáticas del binario: *componentes, cabeceras, instrucciones, empaquetado, firmas, etc.*

Análisis de binarios (3/7)

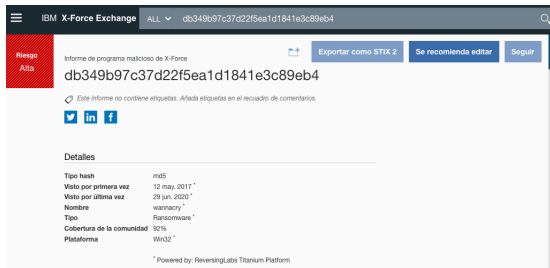


Figura 5: **IBM X-Force Exchange** es una plataforma de inteligencia de amenazas que permite investigar incidentes de seguridad, agregación de inteligencia y colaboración con pares.

Análisis de binarios (4/7)

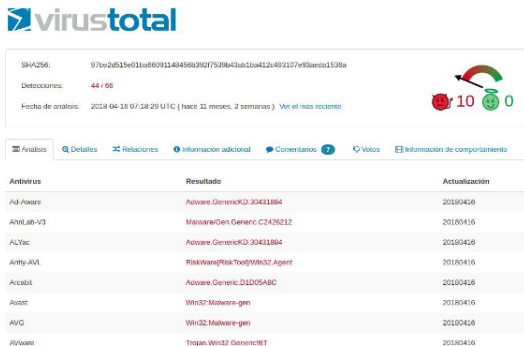


Figura 6: **Virus Total** es un servicio en línea que analiza archivos, binarios y URLs para la detección de patrones de comportamiento malicioso.

Análisis de binarios (5/7)

¿Qué es una *sandbox*?

Una sandbox en términos de **análisis de binarios**, es un sistema controlado que analiza la ejecución y comportamiento dinámico de un binario (*solicitudes hacia Internet, acciones sobre el sistema, llamados al kernel y bibliotecas, etc.*).

Análisis de binarios (6/7)

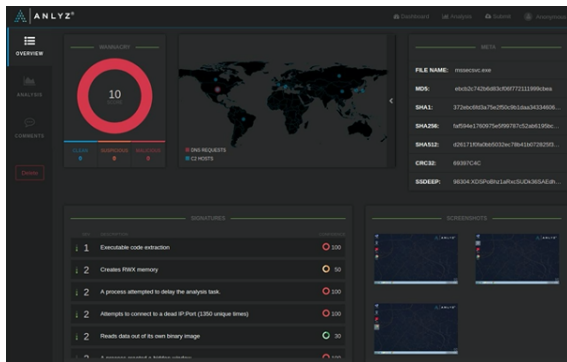


Figura 7: **Anlyz** provee *sanboxes* en línea para analizar patrones de comportamiento de diferentes archivos/binarios.

Análisis de binarios (7/7)

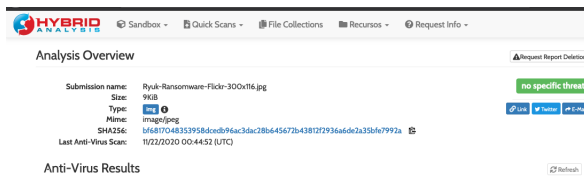


Figura 8: [Hybrid Analysis](#) es un servicio gratuito de análisis de malware.

El registro de Windows (1/9)

¿Qué es el Registry Hive?

Windows mantiene una base de datos de soporte al sistema operativo, la cual se almacena en archivos denominados **Registry Hives**. Los tipos de registros (hives) son:

- ▶ *System*
 - ▶ *Software*
 - ▶ *Security*
 - ▶ *SAM*
 - ▶ *NTUSER*, para cada usuario
-
- ▶ Los *hives* están almacenados en C:\Windows\system32\config

El registro de Windows (2/9)

- ▶ Cada *hive* se descompone en secciones llamadas llaves y sub-llaves denominadas *keys*
- ▶ Cada llave *key* contiene información específica almacenada en valores o *values*
- ▶ Las llaves registran su último cambio en el valor de la variable **LastWriteTime**
- ▶ El **System hive** contiene la configuración particular de un sistema. Algunas de las llaves presentes en este contenedor son:
 - ▶ *Hostname*
 - ▶ *Time Zone*
 - ▶ *Crash Dump Settings*
 - ▶ *Mounted Devices*
 - ▶ *Network Adapters*
 - ▶ *Firewall Settings*
 - ▶ *Remote Administration Settings*

El registro de Windows (3/9)

- ▶ *Loaded Drivers*
- ▶ *Running Services*
- ▶ *USB Storage*
- ▶ El **System Hive** contiene información sobre el software instalado en el sistema. Algunas de las llaves presentes en este contenedor son:
 - ▶ *Operating System and Version*
 - ▶ *Applications executed from the Run prompt*
 - ▶ *Default Browser Settings*
 - ▶ *Profile List*
 - ▶ *User List*
 - ▶ *Installed Components*
 - ▶ *Application Full Paths*

El registro de Windows (4/9)

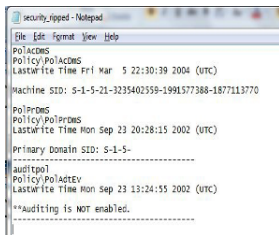


Figura 9: El **Security Hive** contiene información específica sobre las opciones de auditoría habilitadas en el sistema.

- ▶ El **SAM Hive** contiene información sobre los usuarios y grupos del sistema. Algunas de las llaves presentes en este contenedor son:
 - ▶ *Usernames*
 - ▶ *Group Memberships*

El registro de Windows (5/9)

- ▶ *User ID Creation Date*
- ▶ *Last Accessed Time*
- ▶ *Password Reset Date*
- ▶ *Interactive Login Count*

El NTUSER.DAT Hive

- ▶ **NTUSER.DAT** es una base de datos que contiene información sobre cada usuario del sistema
- ▶ Cada usuario que inicia una sesión interactiva con el sistema (por ejemplo un shell de Windows) tiene su propio archivo **NTUSER.DAT**
- ▶ Como los otros sub-árboles, **NTUSER.DAT** está compuesto por llaves y fecha del último cambio, que se registra en la llave **LastWriteTime**

El registro de Windows (6/9)

- ▶ **NTUSER.DAT** está localizado en:
 - ▶ **C:\Documents and Settings \<username>** (Windows NT, 2000 y 2003)
 - ▶ **C:\Users\<username>** (Windows 7, 8 y 10)
- ▶ **NTUSER.DAT hive** contiene información de la actividad de un usuario que ha iniciado una sesión interactiva en el sistema. Algunas de las llaves presentes en este contenedor son:
 - ▶ *Last Items Searched*
 - ▶ *Last Visited Location (within the Windows OS)*
 - ▶ *The Last Files Saved*
 - ▶ *Visited Computer Descriptions*
 - ▶ *Recent Files List*
 - ▶ *Recent Documents*
 - ▶ *Last Commands Issued at the Run Prompt*
 - ▶ *Typed Uniform Resource Locators (URLs)*
 - ▶ *User Assistance Information*

El registro de Windows (7/9)

¿Qué es la carpeta **PREFETCH**?

- ▶ Es una carpeta del sistema operativo Windows, que fue diseñada para **acelerar el lanzamiento de aplicaciones** durante el proceso de inicio del sistema
- ▶ Contiene el nombre de los ejecutables, una lista en *Unicode* de los DLL utilizados, un contador de veces que el ejecutable ha sido lanzado y una marca de tiempo de la última vez que se lanzó el ejecutable
- ▶ Se introdujo en Windows XP

El registro de Windows (8/9)

WinPrefetchView							
File Edit View Options Help							
X [Icons] [Details] [Compare] [Filter]							
Filename	Created Time	Modified Time	File Size	Process DCL	Process Path	Run Count	
77FM.FXF 56D4FPA.pf	9/8/2015 10:17:10 PM	9/8/2015 10:17:10 PM	45,164	77FM.FXF	C:\PROGRAM FILES\7 Zip\7zFM.exe	1	
77C.FXF F40B048.pf	9/8/2015 5:40:40 PM	9/8/2015 1:15:47 AM	78,656	77C.FXF	C:\PROGRAM FILES\7 Zip\7zC.exe	4	
AIIPNWARFOR...SCRFENDISPLAY.F...	9/9/2015 1:03:39 AM	9/9/2015 1:03:39 AM	14,486	AIIPNWARFOR...	C:\PROGRAM FILES (X86)\AIIPNWAR...	1	
APPUPDATER.FXF 1360B64C.pf	9/8/2015 11:38:27 PM	9/8/2015 10:14:31 AM	142,394	APPUPDATER.F...	C:\PROGRAM FILES\AIIPNWARFVS...	4	
AUTODIG.FXF AR22P9A5.pf	5/14/2015 8:04:18 PM	9/9/2015 1:34:27 AM	28,492	AUTODIG.FXF	C:\WINDOWS\System32\audodig.exe	957	
AUTOPSYS4.FXF D313FD23.pf	9/8/2015 11:36:35 PM	9/8/2015 11:36:35 PM	201,126	AUTOPSYS4.FXF	C:\PROGRAM FILES\AUTOPSYS 3.1.2\...	1	
AWCCAPPLICATIONWATCHRR32.F...	9/9/2015 1:03:43 AM	9/9/2015 1:03:43 AM	38,032	AWCCAPPLICA...	C:\PROGRAM FILES\AIIPNWARFVS...	1	
AWCCAPPLICATIONWATCHRR64.F...	9/9/2015 1:03:43 AM	9/9/2015 1:03:43 AM	15,310	AWCCAPPLICA...	C:\PROGRAM FILES\AIIPNWARFVS...	1	
BACIDIPPI.C.FXF 5F04117C.pf	9/8/2015 5:14:17 PM	9/8/2015 5:56:57 PM	58,412			6	
BCDFDIT.FXF FF2142B.pf	9/8/2015 5:14:17 PM	9/8/2015 5:56:56 PM	6,308	BCDFDIT.FXF	C:\WINDOWS\System32\bcdedit.exe	5	
BINGSVCT.FXF 4B0888FD.pf	9/9/2015 1:02:57 AM	9/9/2015 1:02:57 AM	21,648	BINGSVCT.FXF	C:\Users\FORPASCATOR\AppData\l...	1	
BSPATCH.FXF D67CCDFE.pf	8/20/2015 9:27:24 AM	9/8/2015 10:14:16 AM	53,086	BSPATCH.FXF	C:\PROGRAM FILES (X86)\PAIDA SE...	20	
RTPLAYRECTIL.FXF 9AF3015C.pf	9/9/2015 1:03:14 AM	9/9/2015 1:03:14 AM	27,104	RTPLAYRECTIL...	C:\PROGRAM FILES (X86)\Jinn\BLUF...	1	
CAT.EVE 60894715.pf	9/8/2015 11:48:19 AM	9/8/2015 11:55:07 AM	11,644	CAT.EVE	C:\Users\FORPASCATOR\COMMO...	9	
Filename	Full Path	Device Path	Index				
7-ZIP.DLL	C:\PROGRAM FILES\7 Zip\7-zip.dll	\\DEVICE\\HARDISK\\VOLUME3\\PROGRAM FILES\7-ZIP\7-ZIP.DLL	59				
7Z.DLL	C:\PROGRAM FILES\7 Zip\7z.dll	\\DEVICE\\HARDISK\\VOLUME3\\PROGRAM FILES\7-ZIP\7Z.DLL	63				
7ZFM.EXE	C:\PROGRAM FILES\7 Zip\7zFM.exe	\\DEVICE\\HARDISK\\VOLUME3\\PROGRAM FILES\7-ZIP\7ZFM.EXE	5				
ADVAPI32.DLL	C:\WINDOWS\System32\advapi32.dll	\\DEVICE\\HARDISK\\VOLUME3\\WINDOWS\\SYSTEM32\\ADVAPI32.DLL	19				
APISchema.DLL	C:\WINDOWS\System32\APISchema.dll	\\DEVICE\\HARDISK\\VOLUME3\\WINDOWS\\SYSTEM32\\APISchema.DLL	2				
APPHELP.DLL	C:\WINDOWS\System32\apphelp.dll	\\DEVICE\\HARDISK\\VOLUME3\\WINDOWS\\SYSTEM32\\APPHELP.DLL	39				
ATL100.DLL	C:\PROGRAM FILES\MICROSOFT OFFICE 15\...	\\DEVICE\\HARDISK\\VOLUME3\\PROGRAM FILES\MICROSOFT OFFICE 15\ROOT\15\PROG...	44				
CFGMGRI2.DLL	C:\WINDOWS\System32\cfgmgr2.dll	\\DEVICE\\HARDISK\\VOLUME3\\WINDOWS\\SYSTEM32\\CFGMGRI2.DLL	29				
CLBCATQ.DLL	C:\WINDOWS\System32\clbcatq.dll	\\DEVICE\\HARDISK\\VOLUME3\\WINDOWS\\SYSTEM32\\CLBCATQ.DLL	40				
COMCTL32.DLL	C:\WINDOWS\WinSxS\x-wwww-microsoft...	\\DEVICE\\HARDISK\\VOLUME3\\WINDOWS\\WINRES\\AMDS4_Microsoft...\\WINDOWS.CO...	5				
COMDLG32.DLL	C:\WINDOWS\System32\comdlg32.dll	\\DEVICE\\HARDISK\\VOLUME3\\WINDOWS\\SYSTEM32\\COMDLG32.DLL	13				
CRYPTBASE.DLL	C:\WINDOWS\System32\CRYPTBASE.DLL	\\DEVICE\\HARDISK\\VOLUME3\\WINDOWS\\SYSTEM32\\CRYPTBASE.DLL	38				
CYLSHONS.LIB	C:\Users\FORPASCATOR\AppData\Local\MICROSOFT\\	\\DEVICE\\HARDISK\\VOLUME3\\USERS\FORPASCATOR\\APPDATA\\LOCAL\\MICROSOFT\\WIL...	35				
DESKTOP.INI	C:\Users\desktop.ini	\\DEVICE\\HARDISK\\VOLUME3\\USERS\\DESKTOP.INI	37				
329 Files, 1 Selected							
My Soft FreeWare: http://www.mrsoft.net							

Figura 10: Vista de la carpeta **PREFETCH**.

El registro de Windows (9/9)

¿Por qué es importante la carpeta **PREFETCH**?

- ▶ Porque puede **acelerar el proceso de inicio de Windows** y reducir la cantidad de tiempo que se tarda en iniciar los programas
- ▶ Porque **almacena en caché los archivos** que necesita una aplicación para la RAM a medida que se inicia la aplicación, lo que consolida las lecturas del disco y reduce las búsquedas

Proceso y línea de tiempo del análisis forense digital (1/3)

En la siguiente Figura se muestran los cinco elementos clave en el análisis de forense digital:

Identificación

- Identificar el propósito de la investigación
- Identificar los recursos requeridos

Presección

- Los datos deben de ser aislados, asegurados y preservados

Análisis

- Identificar las herramientas y técnicas a utilizar
- Procesar los datos
- Interpretar el análisis de los resultados

Documentación

- Documentación del contexto y mapeo de la evidencia

Presentación

- Procesar el resumen y la explicación de resultados

Figura 11: Pasos del proceso del análisis forense digital.

Proceso y línea de tiempo del análisis forense digital (2/3)

¿Qué es una línea de tiempo forense digital?

- ▶ Una línea de tiempo forense es una **representación cronológica** de un sistema
- ▶ Las líneas de tiempo incluyen los tiempos MAC (*modification, access, change*) de los archivos, la bitácora de eventos del sistema operativo y registros de aplicaciones, las últimas fechas de modificación del registro y las entradas del MFT (*Master File Table*)

Proceso y línea de tiempo del análisis forense digital (3/3)

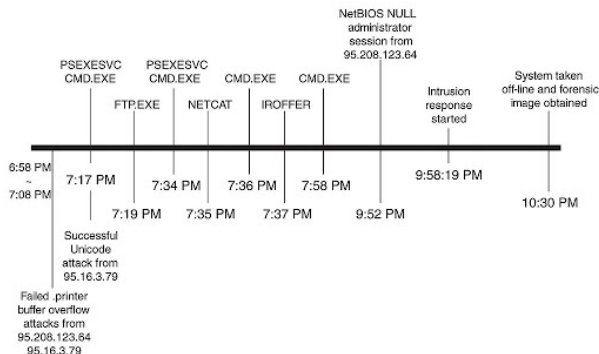


Figura 12: Ejemplo de una línea de tiempo forense digital.