CURSO DE “ESPECIALIZACIÓN EN CIBERSEGURIDAD EN ENTORNOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN”

TEMA 4
Análisis forense informático

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

ÍNDICE

Análisis forense informático. 3
4.1 Introducción y conceptos 3
Evidencias 3
Memorias Volátiles 3
Memorias No Volátiles 4
Firmas de fichero 4
Delitos tecnológicos y ciberdelitos 5
4.2 Normativa y metodología para un análisis forense. 5
Cadena de Custodia 6
4.3 Análisis Forense en móviles Android/IOS 7
Android 7
WhatsApp 8
IOS 9
WhatsApp 10
4.4 Análisis Forense a PC/Servidor u otros dispositivos 11
Firmas de fichero y Metadatos 11
Sistemas Operativos Microsoft Windows 12
Memoria RAM 12
Comandos 16
Memoria No Volátil 17
Registro de Windows 17
Comandos 18
USB 19
Sysinternals 20
Sistemas Operativos Linux 21
Memoria RAM 21
Memoria No Volátil 24
Sistemas Operativos Mac OS 25
Memoria RAM 25
Ftk Imager 27
Autopsy 28
SQLite Browser 29
4.5 Informe pericial y defensa en el juicio 30
Informe pericial 30
Presentación del caso y aceptación 30
Realización del informe pericial 31
Declaración en los juzgados 31

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

Tratamiento del delito tecnológico 31
Instrucción del proceso 31
La calificación y la vista oral 31
Enlaces a recursos 31

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

Análisis forense informático.

4.1 Introducción y conceptos

Informática Forense, es aquella en la que aplicamos una serie de técnicas de examinación de datos para localizar o recuperar información. La informática forense aplica **técnicas científicas y analíticas** especializadas a **infraestructuras tecnológicas** que permiten **identificar, preservar, analizar y presentar datos válidos** dentro de un proceso legal.

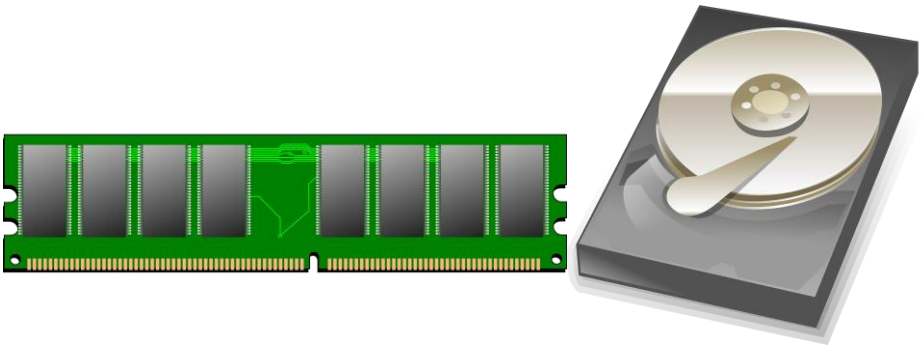

Ilustración 1 - Tipo de Evidencias, Volátiles y No Volátiles

Un análisis forense informático es fundamental que tenga al menos la siguientes fases:

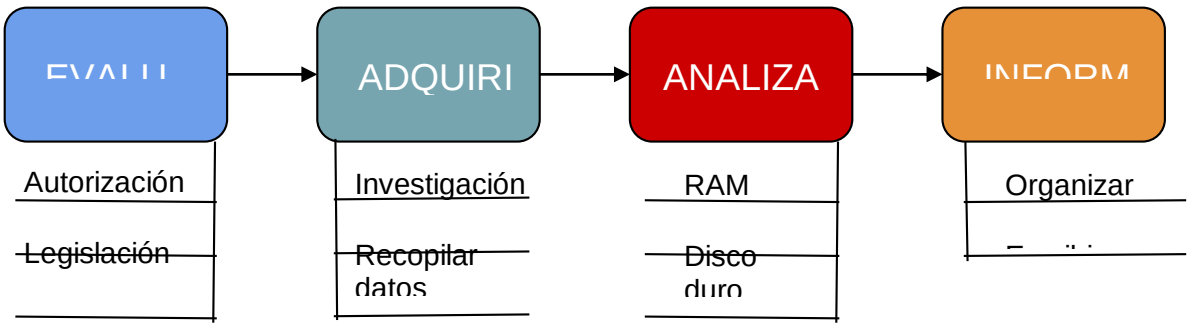

Ilustración 2 - Fases de un análisis forense

Evidencias

A la hora de realizar un análisis informático forense nos podemos encontrar **dos tipos de evidencias**:

Memorias Volátiles

La **memoria volátil** de una infraestructura tecnológica, es aquella cuya información se pierde al interrumpirse el flujo eléctrico.

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

El término “volátil” se refiere a cómo se **pierde la información** si se produce una **interrupción** del **flujo eléctrico**.

El tipo más común de memoria volátil es la RAM del sistema pero existen **diferentes tipos**:

- Memoria de acceso aleatorio o RAM del sistema.
- RAM de video.
- Procesador L1 y L2 caché.
- Caché de disco HDD y SSD.

Memorias No Volátiles

La **memoria no volátil** es un tipo de memoria que **no necesita** de un **flujo eléctrico** para mantener guardada la información en ella.

El término “no volátil” se refiere a cómo se a**lmacena la información** y **no se produce pérdida** si ocurre una **interrupción** en el **flujo eléctrico**.

El tipo más común de memoria no volátil es un disco duro pero existen **diferentes tipos**:

- Disco Duro (HDD o SSD).
- CD.
- DVD.
- Cinta magnética.
- Disquete.
- EPROM.
- EEPROM.
- MRAM.
- Memoria de tambor.
- NVRAM.
- Flash.
- PROM.
- PRAM.
- ROM.
- Bios.
- Memoria racetrack.

Firmas de fichero

Una **firma** o **file signatures**, es un identificador que nos verifica el contenido de un fichero. Estas firmas se conocen cómo **Magic Numbers** o **Magic Bytes**.

Muchos ficheros no se pueden leer cómo texto, si lo abriéramos con un editor de textos el contenido sería inteligible para nosotros.

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

Dependiendo del tipo de fichero, nos encontraremos **diferentes firmas** a las cuales en un análisis forense tendremos que **identificar** para poder analizar las evidencias obtenidas.

Delitos tecnológicos y ciberdelitos

La acción u omisión voluntaria o imprudente penada por la ley, que se realiza mediante conocimientos científicos y técnicas que hacen posible el tratamiento de la información, de forma antijurídica, por medio de ordenadores o elementos informáticos.

Según la ONU(Organización de las Naciones Unidas) se define tres tipos de delitos informáticos:

- Fraudes cometidos mediante manipulación de ordenadores.
- Manipulación de los datos de entrada.
- Daños o modificaciones de programas o datos informatizados.

Según nuestro Código Penal se contemplan ocho tipos de delitos informáticos:

- Amenazas.
- Calumnias e injurias.
- Infracciones contra la propiedad intelectual.
- Pornografía infantil.
- Fraudes y Estafas informáticas.
- Falsedades.
- Sabotajes informáticos.
- Ataques contra el derecho a la intimidad.

4.2 Normativa y metodología para un análisis forense.

Existen múltiples metodologías, protocolos de actuación y recomendaciones relativas a la recolección de evidencias forenses, el estándar y referente principal es el documento “RFC 3227”.

Según la RFC 3227 a la hora de recolectar las evidencias tenemos que tener en cuenta:

1. Principios de recolección.
2. Orden de volatilidad.
3. Cosas a evitar.
4. Privacidad de los datos.

En la RFC 3227 se establecen unos principios de recolección de Evidencias Digitales:

- Primero recolectar y segundo analizar.
- Duplicar evidencias.
- Evitar e identificar cambios en los contenidos.
- Sistema metódico adaptado al dispositivo.
- Fechar y firmar anotaciones.

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

- Obtener una copia.
- Preparar prueba testifical.
- Política de seguridad del lugar.

La RFC 3227 establece unos parámetros a seguir respecto al orden de volatilidad de la prueba.

1. Registros y caché.
2. Enrutamiento, ARP, conexiones entrantes, …
3. Discos duros.
4. Log y configuración.
5. Documentos.

Durante el proceso de recopilación de evidencias y para que el proceso no pueda ser invalidado por terceros tenemos que evitar:

- No apagar el equipo hasta recopilar todas las evidencias.
- No confiar en la información de los programas del sistema.
- Evitar programar que modifiquen la hora y/o la fecha de ficheros.
- Evitar programas que puedan eliminar de forma automática las evidencias.

Los métodos utilizados para recolectar evidencias deben ser transparentes y reproducibles.

- Listar sistemas involucrados.
- Fijar volatilidad.
- Sincronización reloj
- Documentar cada paso.
- Anotar personal involucrado.

Cadena de Custodia

La cadena de custodia es el proceso de captación, preservación y conservación de la prueba en el cual el mismo objeto de la pericia es transmitido sin modificación sustancial desde que se ocupa hasta que se analiza.

La cadena de custodia supone garantía de la mismidad de la prueba, es decir, lo ocupado es lo mismo que lo analizado. Cualquier fallo en la captación de la prueba hará que se genere esa duda sobre su autenticidad e integridad haciendo que no sea una prueba nula, sino que sea una prueba no fiable.

Lo que intenta la cadena de custodia es lograr el adecuado equilibrio entre un proceso penal eficiente y un proceso penal que le dé al imputado la oportunidad de defenderse en un marco de verdadera imparcialidad.

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

Antes de nada, no hay obligación de seguir un proceso determinado. Ante la duda, siempre elegir primero recolectar las evidencias de mayor a menor volatilidad y recolectar las evidencias ante acta notarial o con testigos para correcta conservación y verificación íntegra de las evidencias analizadas.

La cadena de custodia se divide en diferentes etapas:

1. Ocupación.
2. Conversación.
3. Manipulación.
4. Transporte y traslado.
5. Custodia y preservación.

4.3 Análisis Forense en móviles Android/IOS

Android

A la hora de realizar un análisis forense en Android para poder acceder a las evidencias tendremos que realizar un rooteo del teléfono.

Una vez que tengamos rooteado nuestro teléfono Android podremos acceder a todas las evidencias.

Para analizar una APK para comprobar si tiene malware podemos utilizar **MobSF**. Esta herramienta nos permite realizar un análisis completo del funcionamiento y código de la aplicación. Se puede descargar desde su repositorio en github:

https://github.com/MobSF/Mobile-Security-Framework-MobSF

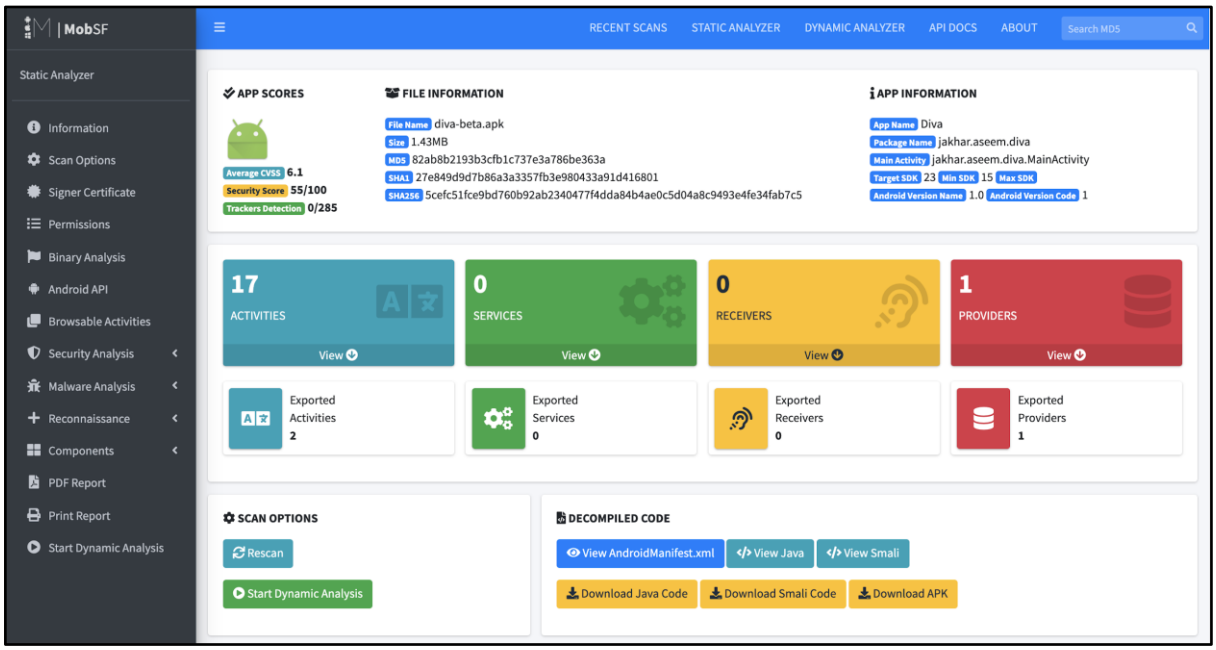

Ilustración 3 - Interfaz de MobSF

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

WhatsApp

Las bases de datos SQLite en WhatsApp se encuentran cifradas. Para poder extraer la key de cifrado tendremos que rootear el teléfono y extraer la key de cifrado y la base de datos cifrada de WhatsApp.

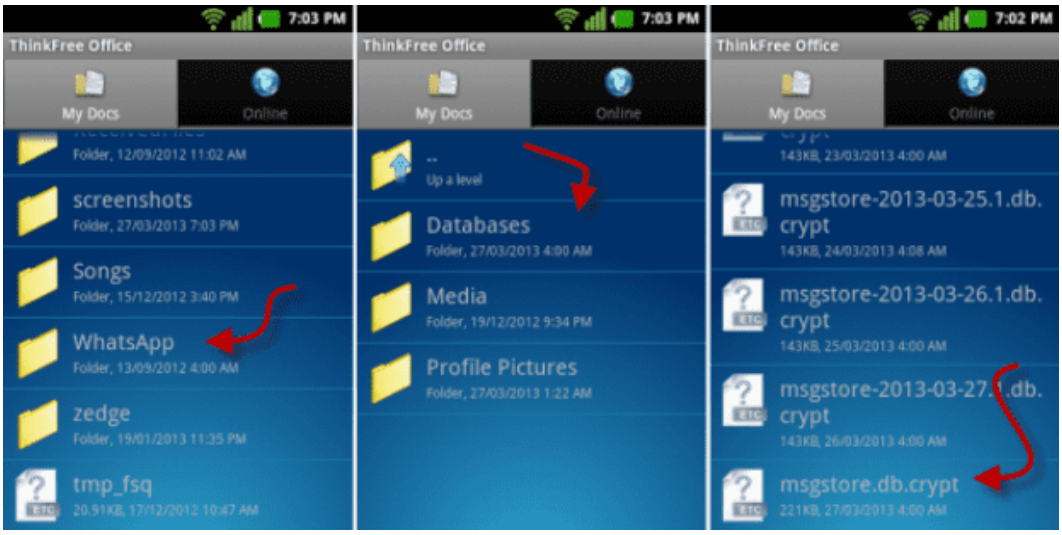

Ilustración 4 - Base de Datos de WhatsApp

Una vez extraídos los ficheros, tendremos que utilizar alguna herramienta como WhatsApp Viewer que nos permite desencriptar la base de datos con la llave de cifrado. La herramienta se puede descargar desde el siguiente enlace:

https://andreas-mausch.de/whatsapp-viewer/

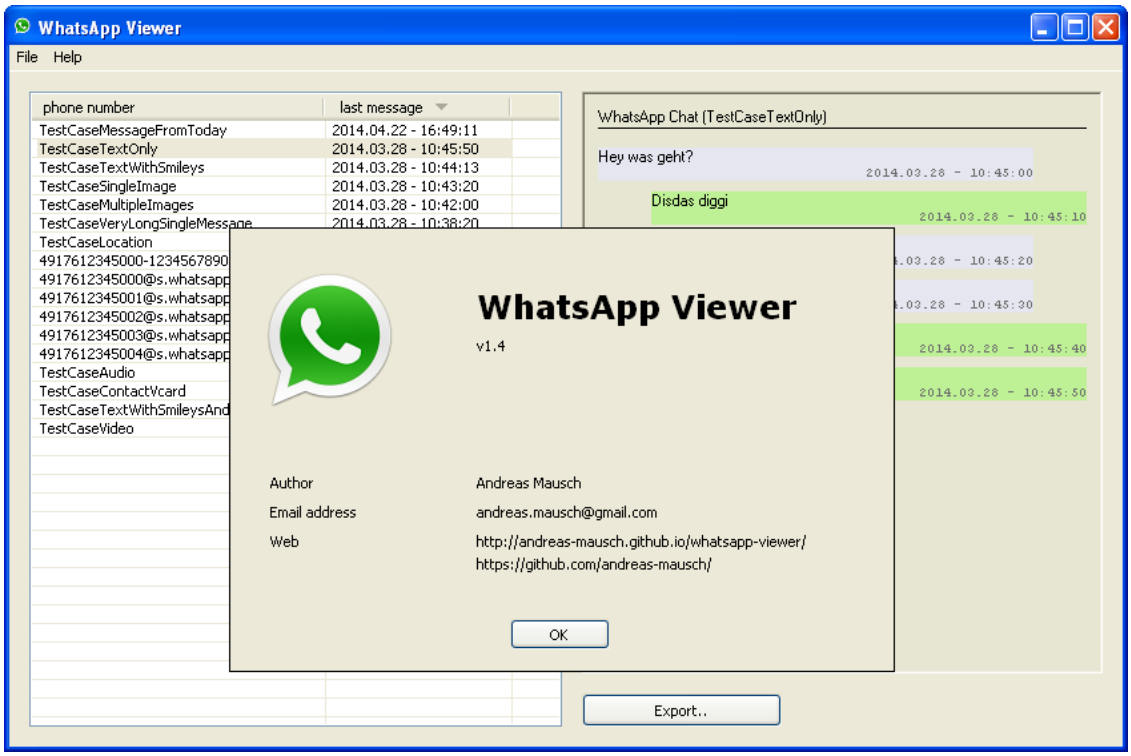

Ilustración 5 - Aplicación WhatsApp Viewer

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

IOS

A la hora de realizar un análisis forense en IOS, tendremos que realizar un clonado del dispositivo. Para ello vamos a utilizar la aplicación iTunes, esta nos permite realizar una copia de seguridad en nuestro dispositivo para así poder acceder a todas las evidencias.

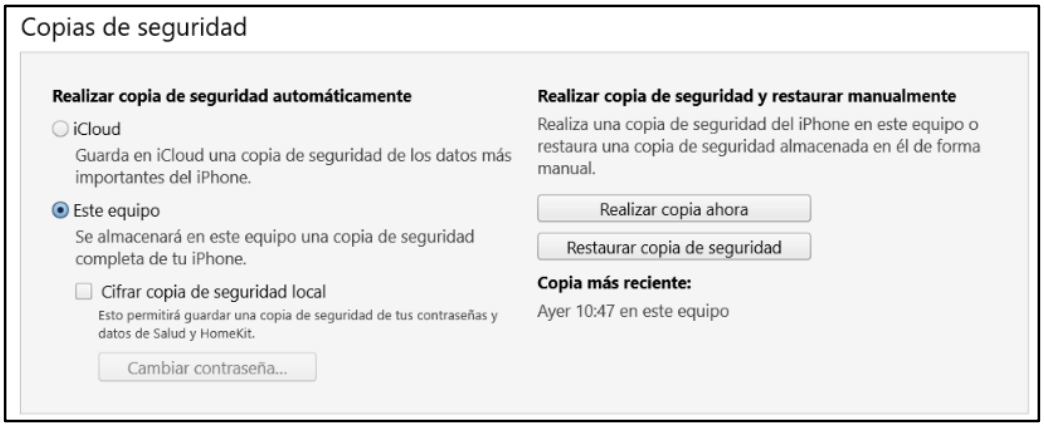

Ilustración 6 - Copias de seguridad de iPhone

Una vez realizada la copia de seguridad vamos a proceder a utilizar la herramienta iBackupBot. Esta herramienta nos permite abrir las copias de seguridad de los dispositivos móviles IOS, navegar a través de las copias y obtener y extraer evidencias.

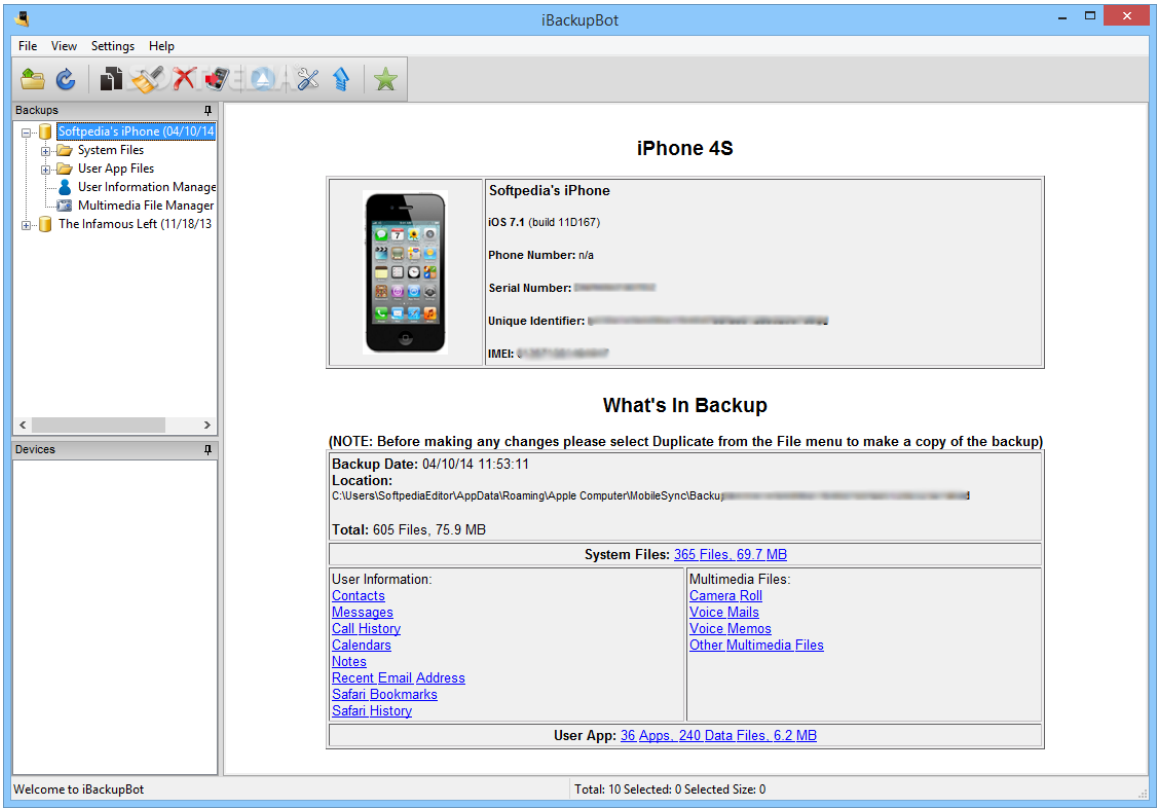

Ilustración 7 - Interfaz de iBakcupBot

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

Para analizar una aplicación IOS para comprobar si tiene malware podemos utilizar **MobSF**. Esta herramienta nos permite realizar un análisis completo del funcionamiento y código de la aplicación. Se puede descargar desde el siguiente enlace:

https://github.com/MobSF/Mobile-Security-Framework-MobSF

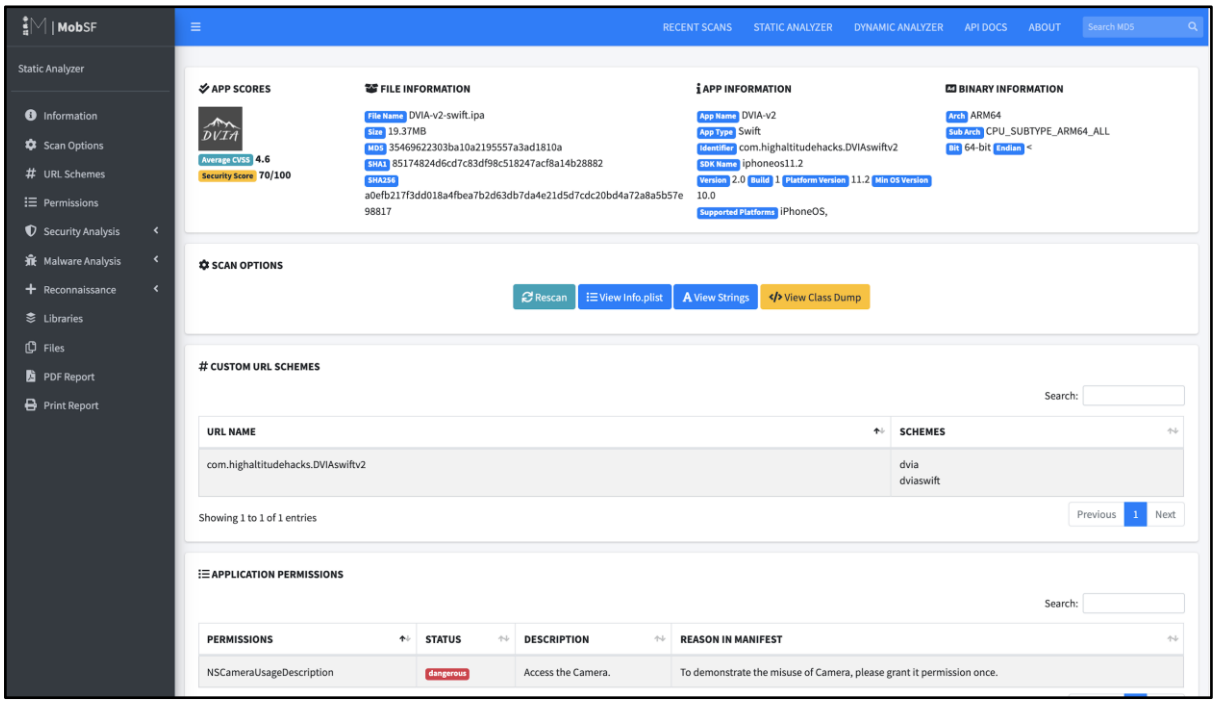

Ilustración 8 - Interfaz de MobSF

WhatsApp

Para analizar una base de datos SQLite de WhatsApp de IOS es tan simple que a partir de la copia de seguridad extraemos el fichero ChatStorage.sqlite y la carpeta Library.

El fichero ChatStorage.sqlite contiene todas las conversaciones y la carpeta Library todo el contenido multimedia como imágenes o vídeos. Estos se encuentran en la ruta “net.whatsapp.WhatsApp\Documents\”.

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

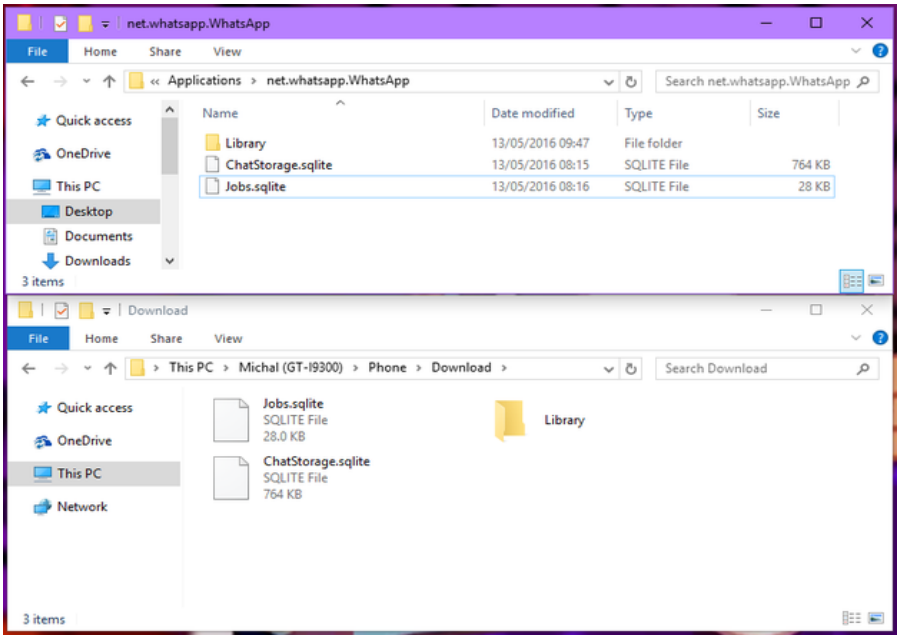

Ilustración 9 - Ficheros de Base de Datos

4.4 Análisis Forense a PC/Servidor u otros dispositivos

A la hora de realizar un análisis forense de un pc o servidor se tiene que tener en cuenta:

- Sistema Operativo
- Uso que se le daba al equipo

Dependiendo del Sistema Operativo, se tendrán que utilizar una serie de técnicas u otras para analizar el equipo.

Firmas de fichero y Metadatos

A la hora de realizar un análisis forense de un fichero tenemos que identificar que tipo de fichero es. Para identificar un fichero se observa al principio la firma del fichero.

47 49 46 38 37 61	GIF87a	0	gif
47 49 46 38 39 61	GIF89a		

Ilustración 10 - Firma de fichero de Gif

En sistemas operativos Linux podemos utilizar la herramienta File. Nos muestra información del fichero y de qué tipo es.

```
root@kali:/media/seguridad# file chall9
chall9: DOS/MBR boot sector; partition 1 : ID=0xb, start-CHS (0x0,32,33), end-CH
S (0x10,81,1), startsector 2048, 260096 sectors, extended partition table (last)
```

Ilustración 11 - Tipo de fichero

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

Podemos visualizar de forma hexadecimal el contenido de un fichero para poder visualizar o modificar la firma. Para ello podemos utilizar un editor hexadecimal HexEdit(Microsoft Windows) o HexEditor(Linux).

```
File: perro.jpg                    ASCII Offset: 0x00000510 / 0x000052DB (%06)
000003C0  A8 FD 84 79  91 F8 C3 C7   7F 4F 9D D2  5F 43 1E 19   ...y.....O.._C..
000003D0  B1 FC 8A D3  F5 7A 3F 65   47 53 86 AC  67 FC CA D7   .....z?eGS..g...
000003E0  F5 7A 3F 65  6F 99 1F 81   E3 BF A7 CF  AB D0 BE 80   .z?eo...........
000003F0  1C 35 63 F9  15 AF EA F4   7E CA 63 B8  6A CB 5F EA   .5c.....~.c.j._.
00000400  56 BF AB D1  FB 28 F2 E3   F0 CE C3 FA  70 14 97 71   V....(......p..q
00000410  A7 81 59 82  66 D2 DB F4   14 B4 FF 00  A5 57 B9 C1   ..Y.f........W..
00000420  EC C6 82 D2  D8 7F F6 29   7D 95 AB AA  8B FD 18 F0   .......)}.......
00000430  BF A7 16 49  76 27 60 B6   99 7F CD 6D  FF 00 41 4F   ...Iv'`....m..AO
00000440  EC AC FE 29  61 6E 33 06   D0 A2 35 E5  49 82 3D 41   ...)an3...5.I.=A
00000450  32 EA 17 C1  5E 36 8E 7A   92 DA 5A 59  D1 CA E2 69   2...^6.z..ZY...i
00000460  52 3E 34 D9  F5 84 FA 56   76 E4 89 A5  4B E4 33 D8   R>4....Vv...K.3.
00000470  A8 B2 5F E8  46 8C 42 4B   A0 D3 B0 B6  C8 F3 E6 A8   ..._.F.BK.......
00000480  CC 1D 7C DB  3A 75 8D 10   73 6D 48 13  F8 36 6F A7   ..|.:u..smH..6o.
00000490  61 BE C4 F6  61 96 49 6B   99 6F 47 F1  54 FE 43 7D   a...a.Ik.oG.T.C}
000004A0  89 C6 DE 8F  E2 69 7E 8D   9E C4 58 18  F4 96 BC DA   .....i~...X.....
000004B0  D3 FC 4D 3F  D1 B7 D8 A2   16 74 FF 00  17 4F 7F 88   ..M?.....t...O..
000004C0  DF 62 2C 0C  AA 4B 64 CB   4A 3F 8A A7  B7 E2 D9 EC   .b,..Kd.J?......
000004D0  50 FB 96 96  BF 83 A7 F2   1B EC 45 9B  46 4D 25 AC   P.........E.FM%.
```

Ilustración 12 - Editor Hexadecimal

Sistemas Operativos Microsoft Windows

Memoria RAM

La RAM es una memoria volátil que en el momento de producirse una interrupción en el flujo eléctrico se pierde lo que tenía almacenado. La memoria RAM es una de las principales evidencias que deben ser extraídas al principio del proceso de extracción de evidencias.

Para poder capturar la memoria RAM existen diferentes herramientas como Magnet RAM Capture. Se puede obtener y descargar de forma gratuita desde https://www.magnetforensics.com/resources/magnet-ram-capture/

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

Ilustración 13 - Proceso de Captura de RAM

Una vez tengamos la captura de la memoria RAM procederemos a su análisis. Para ello vamos a utilizar la herramienta más famosa, usada y de código abierto para análisis de las capturas de RAM.

Volatility es una herramienta que nos permite analizar capturas de RAM de diferentes sistemas operativos. En este caso, nos vamos a centrar en Microsoft Windows. Podéis descargar Volatility desde su página web https://www.volatilityfoundation.org/ o desde su repositorio de GitHub https://github.com/volatilityfoundation/volatility/

Primero de todo, para empezar a analizar una captura de RAM tenemos que identificar su perfil(versión del sistema operativo), para ello vamos a hacer uso del plugin imageinfo. Para ello ejecutamos en consola “volatility -f FICHERO_RAM imageinfo” y obtendremos el perfil específico de Windows.

```
root@kali:[redacted]# volatility -f reto1_taller.raw --profile=Win7SP1x86 imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86_24000, Win7SP1x86 (Instantiated with Win7SP1x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace ([redacted]/reto1_taller.raw)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x82977be8L
          Number of Processors : 1
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0x82978c00L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2019-11-07 12:52:54 UTC+0000
     Image local date and time : 2019-11-07 13:52:54 +0100
```

Ilustración 14 - Identificando perfil de Windows

Una vez tengamos identificado el perfil podemos proceder a analizar diferentes evidencias dentro de la captura de RAM.

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

Con el plugin **netscan** se pueden visualizar las **conexiones entrantes y salientes** que había en el equipo en el momento de realizar la captura de RAM y desde que proceso se están realizando dichas conexiones.

```
root@kali:/media/seguridad# volatility -f capturashs2k19.raw --profile=Win7SP1x64 netscan
Volatility Foundation Volatility Framework 2.6
Offset(P)          Proto    Local Address                  Foreign Address      State            Pid      Owner          Created
0x7db99590         UDPv4    0.0.0.0:0                      *:*                                   656      VBoxService.ex 2019-01-28 23:45:58 UTC+0000
0x7dc76690         UDPv4    10.0.2.11:1900                 *:*                                   1260     svchost.exe    2019-01-28 23:40:19 UTC+0000
0x7dc84c80         UDPv4    127.0.0.1:1900                 *:*                                   1260     svchost.exe    2019-01-28 23:40:19 UTC+0000
0x7dc850d0         UDPv6    ::1:59748                      *:*                                   1260     svchost.exe    2019-01-28 23:40:19 UTC+0000
0x7dc877f0         UDPv6    fe80::9508:aaeb:24b3:2217:59747 *:*                                  1260     svchost.exe    2019-01-28 23:40:19 UTC+0000
0x7dcb0a00         UDPv4    10.0.2.11:59749                *:*                                   1260     svchost.exe    2019-01-28 23:40:19 UTC+0000
0x7dcc8c30         UDPv6    ::1:1900                       *:*                                   1260     svchost.exe    2019-01-28 23:40:19 UTC+0000
0x7dce4ec0         UDPv4    0.0.0.0:3702                   *:*                                   236      svchost.exe    2019-01-28 23:40:15 UTC+0000
0x7dce4ec0         UDPv6    :::3702                        *:*                                   236      svchost.exe    2019-01-28 23:40:15 UTC+0000
0x7dce6140         UDPv4    0.0.0.0:3702                   *:*                                   236      svchost.exe    2019-01-28 23:40:15 UTC+0000
0x7dce6140         UDPv6    :::3702                        *:*                                   236      svchost.exe    2019-01-28 23:40:15 UTC+0000
0x7dceab60         UDPv4    0.0.0.0:3702                   *:*                                   236      svchost.exe    2019-01-28 23:40:15 UTC+0000
0x7dceb560         UDPv4    0.0.0.0:59746                  *:*                                   236      svchost.exe    2019-01-28 23:40:15 UTC+0000
0x7dceb560         UDPv6    :::59746                       *:*                                   236      svchost.exe    2019-01-28 23:40:15 UTC+0000
0x7dceba60         UDPv4    0.0.0.0:59745                  *:*                                   236      svchost.exe    2019-01-28 23:40:15 UTC+0000
0x7dcebd70         UDPv4    0.0.0.0:3702                   *:*                                   236      svchost.exe    2019-01-28 23:40:15 UTC+0000
0x7dd0bec0         UDPv4    0.0.0.0:0                      *:*                                   2160     svchost.exe    2019-01-28 23:40:15 UTC+0000
0x7dd0bec0         UDPv6    :::0                           *:*                                   2160     svchost.exe    2019-01-28 23:40:15 UTC+0000
0x7dd24cc0         UDPv4    0.0.0.0:0                      *:*                                   2160     svchost.exe    2019-01-28 23:40:16 UTC+0000
0x7dd24cc0         UDPv6    :::0                           *:*                                   2160     svchost.exe    2019-01-28 23:40:16 UTC+0000
0x7dd5e530         UDPv4    127.0.0.1:59750                *:*                                   1260     svchost.exe    2019-01-28 23:40:19 UTC+0000
0x7dde85b0         UDPv4    0.0.0.0:3540                   *:*                                   2160     svchost.exe    2019-01-28 23:40:26 UTC+0000
0x7dde85b0         UDPv6    :::3540                        *:*                                   2160     svchost.exe    2019-01-28 23:40:26 UTC+0000
0x7dded7d0         UDPv4    0.0.0.0:0                      *:*                                   2160     svchost.exe    2019-01-28 23:40:26 UTC+0000
0x7dded7d0         UDPv6    :::0                           *:*                                   2160     svchost.exe    2019-01-28 23:40:26 UTC+0000
0x7de94200         UDPv4    0.0.0.0:0                      *:*                                   656      VBoxService.ex 2019-01-28 23:44:18 UTC+0000
```

Ilustración 15 - Identificando Conexiones entrantes

Con el plugin **pstree** podemos visualizar el **árbol de procesos** que había en ese momento en el Sistema Operativo. Esto es bastante importante, ya que nos permite ver que programas o que se estaba ejecutando en ese momento en el equipo. Cada proceso tiene un identificador único que se le conoce como Pid. A la hora de realizar una pericial con Malware nos tendremos que centrar en los procesos y conexiones entrantes y salientes del equipo.

```
root@kali:/media/seguridad# volatility -f capturashs2k19.raw --profile=Win7SP1x64 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0xfffffa80018fb2f0:wininit.exe                       392    336      3     74 2019-01-28 23:39:23 UTC+0000
. 0xfffffa8002a13b30:services.exe                     488    392      9    200 2019-01-28 23:39:26 UTC+0000
.. 0xfffffa8001aba580:svchost.exe                    2732    488      9    301 2019-01-28 23:42:01 UTC+0000
.. 0xfffffa800372c9e0:svchost.exe                    1260    488     22    301 2019-01-28 23:39:39 UTC+0000
.. 0xfffffa8003b0a670:svchost.exe                    2160    488     10    348 2019-01-28 23:40:15 UTC+0000
.. 0xfffffa800389aa80:taskhost.exe                   1700    488      9    200 2019-01-28 23:39:45 UTC+0000
.. 0xfffffa8003c4b720:mscorsvw.exe                   2496    488      6     79 2019-01-28 23:41:48 UTC+0000
.. 0xfffffa8003517060:svchost.exe                     812    488     21    549 2019-01-28 23:39:31 UTC+0000
... 0xfffffa80035b83a0:audiodg.exe                    952    812      4    128 2019-01-28 23:39:33 UTC+0000
.. 0xfffffa80039e8b30:wmpnetwk.exe                   1800    488      9    208 2019-01-28 23:40:13 UTC+0000
... 0xfffffa80037aab30:explorer.exe                  1840   1800     26    859 2019-01-28 23:39:47 UTC+0000
.... 0xfffffa80039cba30:VBoxTray.exe                 1252   1840     12    149 2019-01-28 23:39:59 UTC+0000
.... 0xfffffa8001b02850:MagnetRAMCaptu               1064   1840      6    282 2019-01-28 23:43:59 UTC+0000
.. 0xfffffa800193c870:spoolsv.exe                    1088    488     14    307 2019-01-28 23:39:38 UTC+0000
.. 0xfffffa8003623060:svchost.exe                     328    488     14    453 2019-01-28 23:39:35 UTC+0000
.. 0xfffffa80035883f0:svchost.exe                     844    488     27    487 2019-01-28 23:39:32 UTC+0000
... 0xfffffa800387bb30:dwm.exe                       1812    844      3     68 2019-01-28 23:39:47 UTC+0000
.. 0xfffffa8003539b30:svchost.exe                     720    488      7    262 2019-01-28 23:39:30 UTC+0000
.. 0xfffffa80029fb740:SearchIndexer.                 1196    488     11    605 2019-01-28 23:40:11 UTC+0000
.. 0xfffffa8003504970:svchost.exe                     596    488      9    350 2019-01-28 23:39:29 UTC+0000
... 0xfffffa8003d94060:WmiPrvSE.exe                  3008    596      6    113 2019-01-28 23:41:05 UTC+0000
.. 0xfffffa800359a890:svchost.exe                     868    488     36   1009 2019-01-28 23:39:32 UTC+0000
... 0xfffffa80019f5b30:WMIADAP.exe                   2984    868      6     84 2019-01-28 23:43:48 UTC+0000
.. 0xfffffa8003520060:VBoxService.ex                  656    488     12    117 2019-01-28 23:39:30 UTC+0000
.. 0xfffffa80036b7560:svchost.exe                    1124    488     18    300 2019-01-28 23:39:38 UTC+0000
```

Ilustración 16 - Árbol de procesos

Con el plugin **memdump** podemos extraer el minidump o crash dump de un proceso. Para ello primero tendremos que indicarle el PID del proceso.

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

```
root@kali:/media/seguridad/Taller_Mundo_Hacker_Academy# volatility -f reto1_taller.raw --profile=Win7SP1x86_23418 memdump -p 3112 -D .
Volatility Foundation Volatility Framework 2.6
**********************************************************************
Writing notepad.exe [  3112] to 3112.dmp
```

```
Writing notepad.exe [  3112] to 3112.dmp
```

Ilustración 17 - Extrayendo proceso de la RAM

Con el plugin **filescan** podemos **visualizar** los **diferentes ficheros cargados en memoria**. Cada fichero tiene una dirección de memoria.

Con el plugin **dumpfiles** podemos **extraer** un **fichero que haya cargado en memoria**. Para ello tenemos que indicarle con la opción -Q la dirección en memoria obtenida en filescan.

```
root@kali:/media/seguridad/[redacted]# volatility -f dump --profile=Win7SP0x8
6 filescan | grep findme
Volatility Foundation Volatility Framework 2.6
0x000000001ee20110      3      0 R--rwd \Device\HarddiskVolume2\Users\info\Desktop\findme
root@kali:/media/seguridad/[redacted]# volatility -f dump --profile=Win7SP0x8
6 dumpfiles -Q 0x000000001ee20110 -D . -u -n
```

Ilustración 18 - Resultados de volatility

Con el plugin **hashdump** podemos dumpear los **hashes NTLM** de las **contraseñas** de los **usuarios** del Sistema Operativo. Para ello lo primero de todo es importante que en el árbol de procesos esté activo el proceso lsass.exe, que es el encargado en Windows de la autenticación de usuarios.

```
root@kali:/media/seguridad# volatility -f capturashs2k19.raw --profile=Win7SP1x64 hashdump
Volatility Foundation Volatility Framework 2.6
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
edusatoe:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:7c451a2b1f306d11783f884326b67790:::
root@kali:/media/seguridad#
```

Ilustración 19 - Hashes de las contraseñas de usuario

Para poder crackear el hash de una cuenta de usuario podemos hacer uso de herramientas como HashCat u online como CrackStation https://crackstation.net/

Con el plugin **driverscan** podemos visualizar los **diferentes drivers** que hay instalados en el equipo. Esto nos permite comprobar si el usuario ha enchufado algún dispositivo específico.

```
root@kali:[redacted] volatility -f reto2_taller.raw --profile=Win7SP1x86_23418 driverscan
Volatility Foundation Volatility Framework 2.6
Offset(P)          #Ptr     #Hnd Start           Size Service Key          Name         Driver Name
------------------ -------- -------- ---------- ---------- -------------------- ------------ -----------
0x0000000005c5e8a0        3        0 0x91358000    0x51000 srv                  srv          \FileSystem\srv
0x00000000077da3f8        5        0 0x913cc000    0x2a000 fastfat              fastfat      \FileSystem\fastfat
0x000000000825e510        4        0 0x913a9000    0x21000 vmhgfs               vmhgfs       \FileSystem\vmhgfs
0x000000000a22f538        3        0 0x913ca000     0x1080 IefRamDump           IefRamDump   \Driver\IefRamDump
0x000000000ce9f728        3        0 0x91309000    0x4f000 srv2                 srv2         \FileSystem\srv2
0x000000000e810780        4        0 0x86e00000     0xb000 mouhid               mouhid       \Driver\mouhid
0x000000000e811688        3        0 0x86ff8000     0x8000 vmusbmouse           vmusbmouse   \Driver\vmusbmouse
```

Ilustración 20 - Drivers de los diferentes componentes

Se pueden visualizar todos los plugins de volatility en la siguiente URL:
https://github.com/volatilityfoundation/volatility/wiki/Command-Reference

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

Comandos

Podemos ejecutar comandos en el terminal para obtener información del ordenador como conexiones activas, procesos, conexión de la red local.

Para obtener las conexiones activas podemos usar el comando “netstat -a” para listar las conexiones entrantes y salientes.

```
C:\Users [redacted]>netstat -a

Conexiones activas

  Proto  Dirección local        Dirección remota       Estado
  TCP    0.0.0.0:135            [redacted]:0           LISTENING
  TCP    0.0.0.0:443            [redacted]:0           LISTENING
  TCP    0.0.0.0:445            [redacted]:0           LISTENING
  TCP    0.0.0.0:903            [redacted]:0           LISTENING
  TCP    0.0.0.0:913            [redacted]:0           LISTENING
  TCP    0.0.0.0:1521           [redacted]:0           LISTENING
  TCP    0.0.0.0:1536           [redacted]:0           LISTENING
  TCP    0.0.0.0:1537           [redacted]:0           LISTENING
  TCP    0.0.0.0:1538           [redacted]:0           LISTENING
  TCP    0.0.0.0:1539           [redacted]:0           LISTENING
  TCP    0.0.0.0:1542           [redacted]:0           LISTENING
  TCP    0.0.0.0:1546           [redacted]:0           LISTENING
  TCP    0.0.0.0:1548           [redacted]:0           LISTENING
```

Ilustración 21 - Conexiones entrantes y salientes

Con el comando “ipconfig /all” podemos obtener la información completa de las tarjetas de red y que dirección IP tienen asignadas.

```
C:\Windows\system32>ipconfig /all

Configuración IP de Windows

   Nombre de host. . . . . . . . . . : AYERIM-PC
   Sufijo DNS principal  . . . . . . :
   Tipo de nodo. . . . . . . . . . . : híbrido
   Enrutamiento IP habilitado. . . . : no
   Proxy WINS habilitado . . . . . . : no

Adaptador PPP sj:

   Sufijo DNS específico para la conexión. . :
   Descripción . . . . . . . . . . . . . . . : sj
   Dirección física. . . . . . . . . . . . . :
   DHCP habilitado . . . . . . . . . . . . . : no
   Configuración automática habilitada . . . : sí
   Dirección IPv4. . . . . . . . . . . . . . : 190.6.74.115(Preferido)
   Máscara de subred . . . . . . . . . . . . : 255.255.255.255
   Puerta de enlace predeterminada . . . . . : 0.0.0.0
   Servidores DNS. . . . . . . . . . . . . . : 200.55.128.3
                                               200.55.128.4
   NetBIOS sobre TCP/IP. . . . . . . . . . . : deshabilitado
```

Dirección IP equipo

Servidores DNS

Ilustración 22 - Configuración e información de las tarjetas de red

Con el comando “route print” podemos obtener todas las rutas de conexiones que hay en el sistema.

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

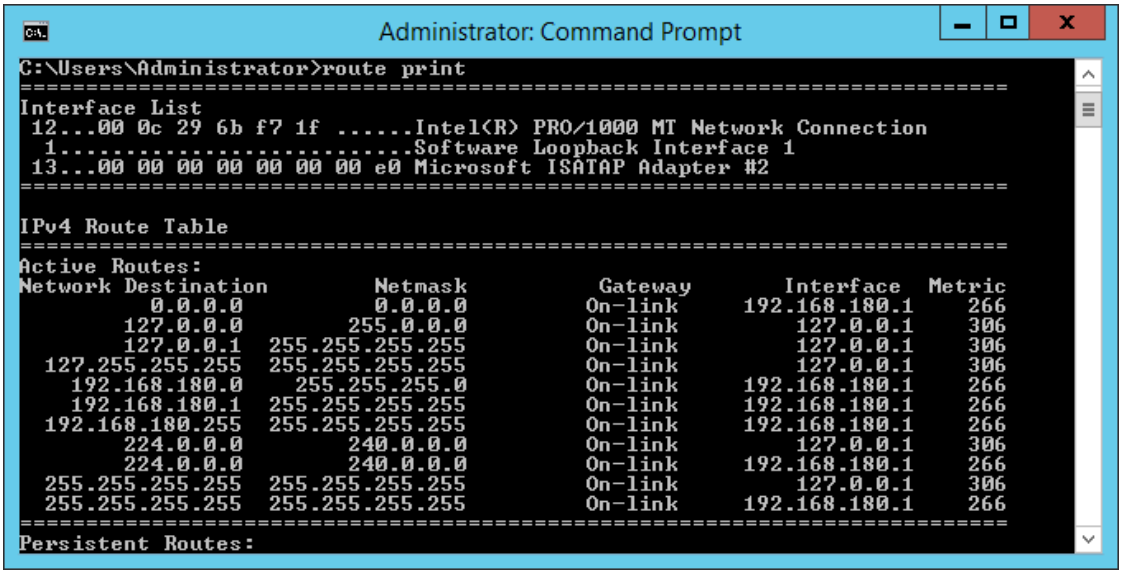

Ilustración 23 - Ruta de conexiones

Memoria No Volátil

Cómo explicamos anteriormente, una evidencia no volátil puede ser desde un HDD a un USB. En los sistemas operativos Windows encontramos evidencias como registro de Windows , los eventos, ficheros del sistema…

Registro de Windows

En el registro de Windows podemos encontrar todas las claves y configuración del sistema.

Si queremos obtener información del sistema instalado, cómo fecha de instalación, versión exacta, id del producto podemos consultarlo en la siguiente ruta:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\

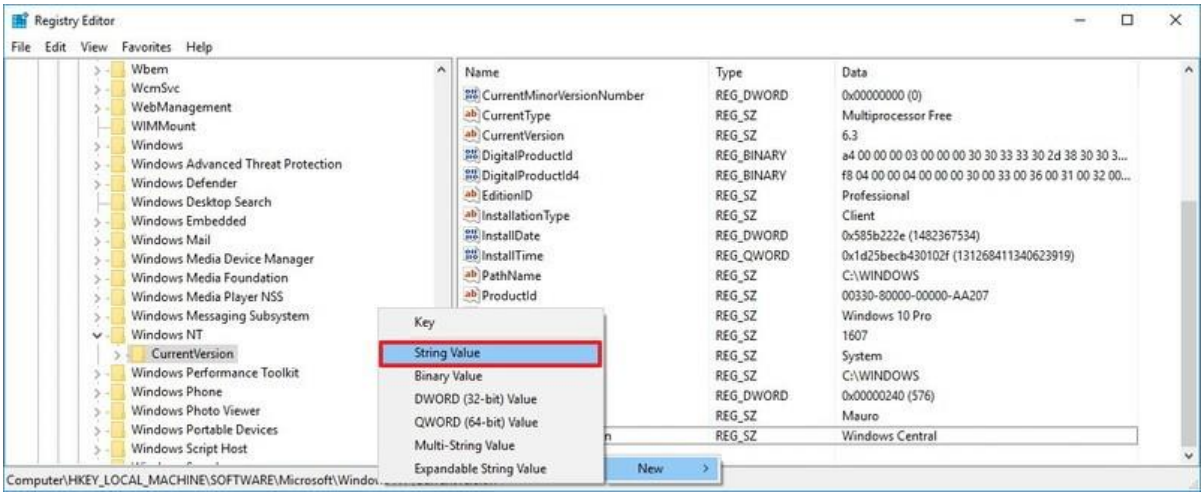

Ilustración 24 - Editor de registro de Windows

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

Para identificar la fecha de instalación nos vamos a la key “InstallDate” y copiamos su valor. Una vez que tengamos el valor a través de EpochConverter nos permitirá convertir el valor del tiempo en hexadecimal a legible y podremos saber en qué fecha se instaló el sistema operativo. Se puede acceder desde el siguiente enlace:

https://www.epochconverter.com/hex

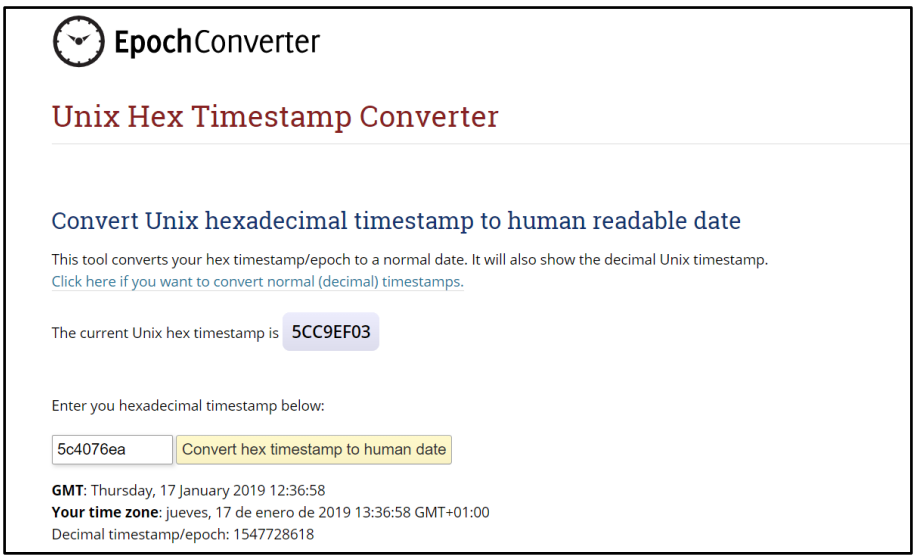

Ilustración 25 - Web de EpochConverter

Comandos

A su vez, también podemos obtener la fecha de instalación del sistema a través de la terminal de Windows. Con el comando systeminfo nos proporcionará directamente la fecha de instalación del sistema.

```
C:\Users [redacted] systeminfo | find /i "original"
Fecha de instalación original:            17/01/2019, 14:36:58
```

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

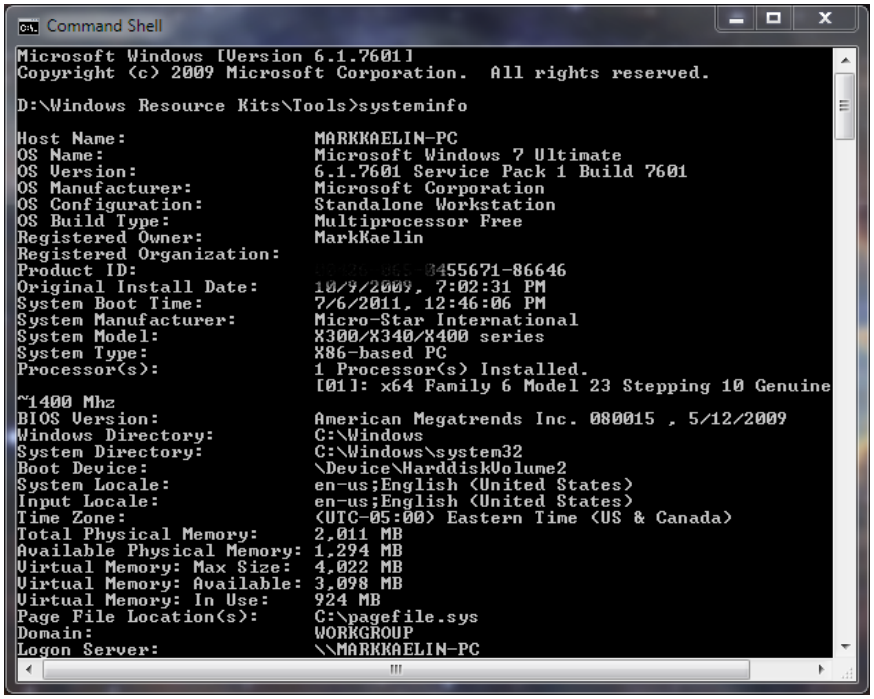

Ilustración 26 - Información del sistema con systeminfo

USB

Para obtener todos los dispositivos USB que han sido conectados a lo largo del tiempo en un equipo podemos usar la herramienta USBDeview. Se puede descargar desde https://www.nirsoft.net/utils/usb_devices_view.html

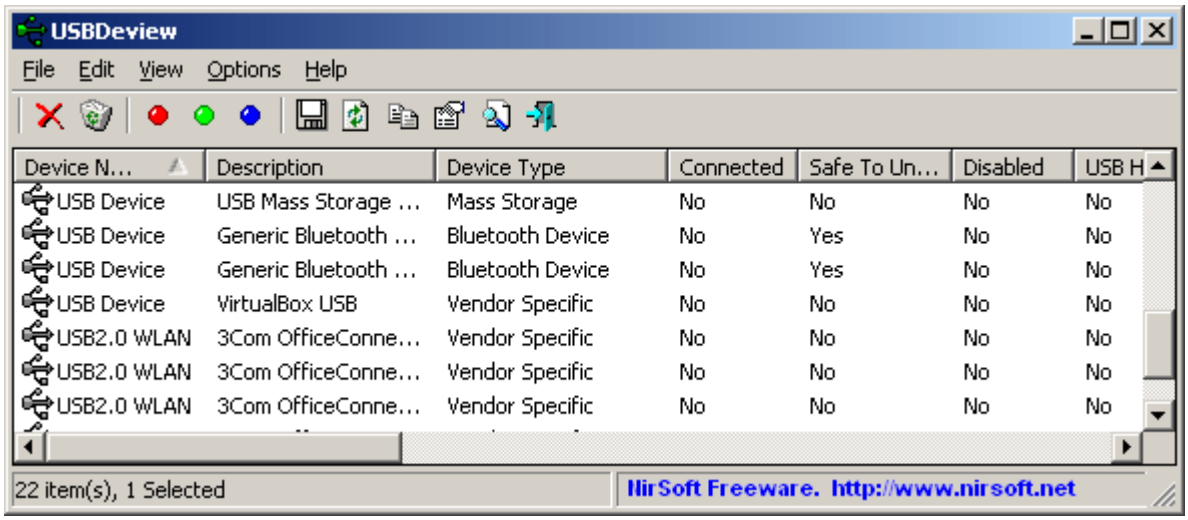

Ilustración 27 - Historial de dispositivos USB

Cada dispositivo USB tiene dos identificadores, VendorID, que indica el ID de la marca del dispositivo y ProductID, que indica el ID del producto dentro de la marca. Si necesitamos identificar si un dispositivo ha sido conectado a un equipo podemos consultar a través de USBDeview el listado de USB conectados y buscar a través del VendorID y ProductoID en una base de datos de ID de USB. Podemos acceder a esta base de datos desde https://www.the-sz.com/products/usbid/ .

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

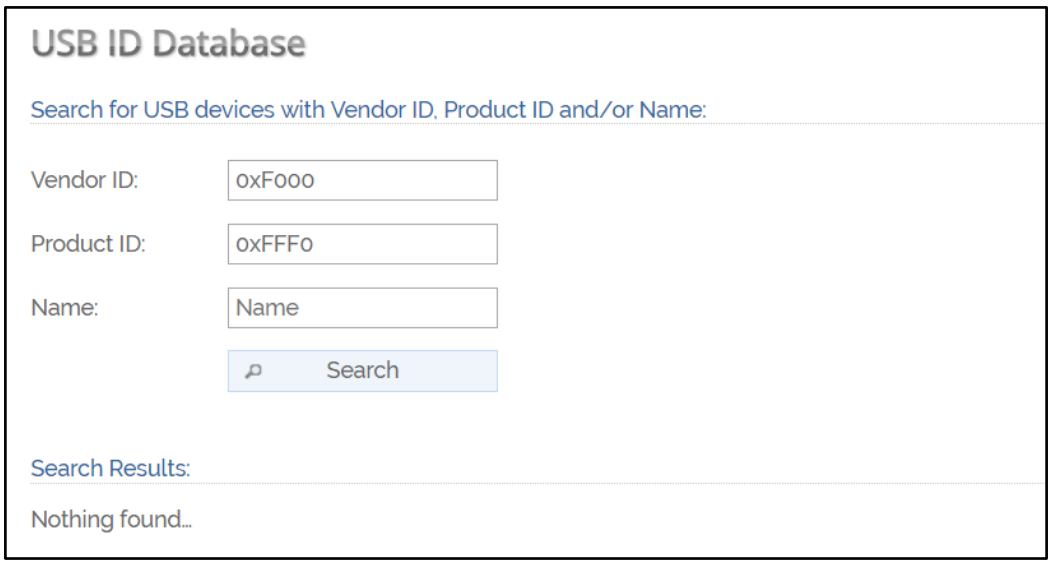

Ilustración 28 - Base de Datos USB

Sysinternals

Las Windows Sysinternals son una serie de herramientas externas que nos permiten obtener información de los sistemas operativos Windows. Se pueden obtener en https://docs.microsoft.com/en-us/sysinternals/

Ilustración 29 - Windows Sysinternals

Con la utilidad pslist podemos listar todos los procesos en memoria.

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

```
C:\Users\wesleywh\Desktop\data\sysinternals>pslist

pslist v1.3 - Sysinternals PsList
Copyright (C) 2000-2012 Mark Russinovich
Sysinternals - www.sysinternals.com

Process information for IT385-08:

Name                 Pid Pri Thd  Hnd   Priv        CPU Time    Elapsed Time
Idle                   0   0   4    0      0    5:33:51.015     1:30:48.553
System                 4   8 113 1021    196    0:01:04.265     1:30:48.553
smss                 364  11   2   44    276    0:00:01.937     1:30:48.475
csrss                464  13  10  381   2356    0:00:01.875     1:30:36.443
csrss                544  13  12  335   2636    0:00:08.593     1:30:32.227
wininit              552  13   1   76    792    0:00:00.500     1:30:32.227
winlogon             600  13   2  176   1532    0:00:00.562     1:30:31.587
services             640   9   4  290   4356    0:00:05.890     1:30:24.504
lsass                648   9   8 1100   5676    0:00:03.875     1:30:24.423
svchost              724   8   9  510   5852    0:00:01.265     1:30:20.006
svchost              768   8   9  487   4472    0:00:01.312     1:30:19.896
dwm                  880  13   6  196  18236    0:00:56.234     1:30:19.709
MsMpEng              892   8  36  641 113148    0:02:59.156     1:30:19.631
atiesrxx             964   8   5  109    876    0:00:00.000     1:30:17.365
svchost              988   8  23  752  16448    0:00:03.625     1:30:17.318
svchost               80   8  39 2738  31668    0:00:16.593     1:30:17.146
svchost              444   8  20  582   8568    0:00:00.640     1:30:16.974
svchost              420   8  11  424  97992    0:02:16.984     1:30:16.568
svchost             1044   8  39  906  10400    0:00:01.312     1:30:16.240
spoolsv             1224   8  13  448   5600    0:00:00.734     1:30:16.084
svchost             1248   8  22  473  21572    0:00:01.796     1:30:16.068
AgentManager        1400   8  60  408  26100    0:00:00.250     1:30:14.519
svchost             1468   8  10  363   4464    0:00:00.203     1:30:11.666
mgsvc               1512   8  21  290   4128    0:00:00.031     1:30:11.541
```

Ilustración 30 - Procesos del sistema

Con la utilidad logonsessions podemos listar el historial de acceso de los usuarios.

```
C:\WINDOWS\system32\cmd.exe
Logonsesions v1.1
Copyright (C) 2004 Bryce Cogswell and Mark Russinovich
Sysinternals - www.sysinternals.com


[0] Logon session 00000000:000003e7:
    User name:    CTSAMBA\TEST-382-XP$
    Auth package: NTLM
    Logon type:   (none)
    Session:      0
    Sid:          S-1-5-18
    Logon time:   22.11.2007 12:35:59
    Logon server:
    DNS Domain:
    UPN:
      592: \SystemRoot\System32\smss.exe
      664: \??\C:\WINDOWS\system32\csrss.exe
      688: \??\C:\WINDOWS\system32\winlogon.exe
      732: C:\WINDOWS\system32\services.exe
      744: C:\WINDOWS\system32\lsass.exe
      900: C:\WINDOWS\system32\svchost.exe
     1056: C:\WINDOWS\System32\svchost.exe
     1440: C:\WINDOWS\system32\spoolsv.exe
     1596: C:\Programme\G DATA\AVKClient\AVKCl.exe
     1608: C:\Programme\Gemeinsame Dateien\G DATA\AVKProxy\AVKProxy.exe
```

Ilustración 31 - Historial de acceso de usuarios

Sistemas Operativos Linux

Memoria RAM

Volatility es una herramienta que nos permite analizar capturas de RAM de diferentes sistemas operativos. En este caso, nos vamos a centrar en Microsoft Windows. Podeis descargar Volatility desde su página web https://www.volatilityfoundation.org/ o desde su repositorio de GitHub https://github.com/volatilityfoundation/volatility/

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

Primero de todo, para empezar a analizar una captura de RAM tenemos que identificar su perfil(versión del sistema operativo), para ello vamos a hacer uso de la herramienta strings. Volatility no cuenta con un plugin que identifique el tipo de perfil y versión de kernel que se va a utilizar para analizar la RAM. Con el comando strings seguido de la palabra GNU/Linux o Welcome nos aparecerá.

```
root@kali:/[redacted]# strings memory.raw | grep GNU/Linux
GNU/Linux
 (GNU/Linux)
elcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-72-lowlatency x86_64)
 Google Earth is available for GNU/Linux from their web site, but is
HWelcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-72-lowlatency x86_64)
```

```
GNU/Linux 4.4.0-72-lowlatency x86_64
```

Ilustración 32 - Salida comando strings

Una vez que sepamos la versión correcta del kernel tendremos que instalarnos esa versión en nuestro sistema operativo linux o máquina virtual (más recomendable). Vamos a proceder a crear el módulo de volatility. Para ello usaremos las herramientas de volatility.

```
taller@osboxes:/usr/share/volatility/tools/linux$ sudo make -C /lib/modules/4.4.
0-72-lowlatency/build CONFIG_DEBUG_INFO=y M=$PWD modules
make: se entra en el directorio '/usr/src/linux-headers-4.4.0-72-lowlatency'
  CC [M]  /usr/share/volatility/tools/linux/module.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /usr/share/volatility/tools/linux/module.mod.o
  LD [M]  /usr/share/volatility/tools/linux/module.ko
make: se sale del directorio '/usr/src/linux-headers-4.4.0-72-lowlatency'
taller@osboxes:/usr/share/volatility/tools/linux$ sudo sudo dwarfdump -di ./modu
le.o > /home/taller/module.dwarf
```

Ilustración 33 - Creación módulo volatility

Cuando generemos el módulo podemos importar el perfil creado con la opción --plugins y usar el --info para comprobar si se ha importado correctamente.

```
taller@osboxes:/usr/share/volatility/tools/linux$ sudo zip /home/taller/Ubuntu16
04-4.4.0-72-lowlatency.zip /home/taller/module.dwarf /boot/System.map-4.4.0-72-l
owlatency
  adding: home/taller/module.dwarf (deflated 91%)
  adding: boot/System.map-4.4.0-72-lowlatency (deflated 79%)
taller@osboxes:/usr/share/volatility/tools/linux$ volatility --plugins=/home/tal
ler/x32 --info | grep Ubuntu
Volatility Foundation Volatility Framework 2.6
LinuxUbuntu1604-4_4_0-72-lowlatencyx64 - A Profile for Linux Ubuntu1604-4.4.0-72
-lowlatency x64
```

Ilustración 34 - Creación del perfil de volatility

Con el plugin **linux_pslist** podemos listar los procesos en el sistema. Con el plugin **linux_pstree** sería de forma similar pero se mostrarían en forma de árbol.

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

```
root@kali:[redacted]/backup# volatility
--plugins=../profile -f memory.raw --profile=LinuxUbuntu1604-4_4_0-72-lowlatencyx64 linux_
pslist
Volatility Foundation Volatility Framework 2.6
Offset             Name                 Pid             PPid            Uid             Gi
d    DTB                 Start Time
------------------ -------------------- --------------- --------------- --------------- --
---- ------------------ ----------
0xffff88000c9c0000 systemd              1               0               0               0
     0x000000000cbde000 2017-05-05 12:04:06 UTC+0000
0xffff88000c9c0e40 kthreadd             2               0               0               0
     ------------------ 2017-05-05 12:04:06 UTC+0000
0xffff88000c9c1c80 ksoftirqd/0          3               2               0               0
     ------------------ 2017-05-05 12:04:06 UTC+0000
```

```
.[irq/20-vboxgues]   493
.[ttm_swap]          534
.[irq/18-vboxvide]   535
.[kdmflush]          625
.[bioset]            628
.[kcryptd_io]        629
.[kcryptd]           630
.[dmcrypt_write]     631
.[bioset]            632
.[jbd2/dm-0-8]       652
.[ext4-rsv-conver]   653
.[irq/19-enp0s3]     784
```

Ilustración 35 - Listado de procesos con volatility

Con el plugin **linux_bash** podremos obtener los comandos que se han ejecutado y siguen cargados en memoria.

```
Command
-------
history
apt-get install linux-image-4.4.0-72-lowlatency linux-headers-lowlatency
reboot
apt-get insta
history
apt-get install lynx gnupg
nano /etc/fstab
nano /etc/crypttab
cd /mnt/
cp -R /media/sf_DUMP/dir* .
ping 8.8.8.8
```

Ilustración 36 - Comandos ejecutados

Puedes visualizar la lista completa de plugins de volatility para linux en el siguiente recurso:

https://github.com/volatilityfoundation/volatility/wiki/Linux

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

Memoria No Volátil

A la hora de analizar una evidencia con un sistema operativo linux podemos encontrar las siguientes evidencias importantes.

El historial de comandos. En la carpeta de cada usuario del sistema podemos encontrar el fichero **.bash_history** que nos mostrará el historial completo de comandos que ha ejecutado el usuario.

```
Enter Your Command:$ cat /home/hendadel/.bash_history | grep 'kill'
sudo killall apt
sudo killall apt-get
sudo kill -9 735
sudo apt install xorg-xkill
xkill
```

Ilustración 37 - Historial de comandos

En el directorio /var/log nos encontramos los logs del sistema y sus diferentes servicios como Apache.

```
root@OPNsense:~ # cd /var/log/
root@OPNsense:/var/log # ls
bsdinstaller            lighttpd.log            setuid.yesterday
configd.log             mount.today             squid
dhcpd.log               ntp                     squid.log
dmesg.today             ntpd.log                suricata
dmesg.yesterday         openvpn.log             suricata.log
dnsmasq.log             pkg.log                 system.log
elasticsearch           portalauth.log          userlog
filter.log              ppps.log                utx.lastlogin
gateways.log            resolver.log            utx.log
ipsec.log               routing.log             vpn.log
lighttpd                setuid.today            wireless.log
root@OPNsense:/var/log #
```

Ilustración 38 - Directorio /var/log

El fichero passwd y shadow nos muestran el listado de usuarios del sistema y los hashes de sus contraseñas.

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

```
rui@rui-VirtualBox: ~
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:116::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false
saned:x:119:127::/var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
rui:x:1000:1000:Rui,,,:/home/rui:/bin/bash
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
test1:x:1001:1001:,,,:/home/test1:/bin/bash
test2:x:1002:1002:,,,:/home/test2:/bin/bash
test3:x:1003:1003:,,,:/home/test3:/bin/bash
test4:x:1004:1004:,,,:/home/test4:/bin/bash
test5:x:1005:1005:,,,:/home/test5:/bin/bash
```

Ilustración 39 - Fichero passwd

Sistemas Operativos Mac OS

Memoria RAM

Volatility es una herramienta que nos permite analizar capturas de RAM de diferentes sistemas operativos. En este caso, nos vamos a centrar en Microsoft Windows. Podéis descargar Volatility desde su página web https://www.volatilityfoundation.org/ o desde su repositorio de GitHub https://github.com/volatilityfoundation/volatility/

Para poder analizar la RAM necesitamos el perfil de MAC OS específico. En el siguiente repositorio podréis encontrar perfiles para todas las versiones de MAC OS y perfiles de algunas versiones de kernel de Linux. Podeis descargar los perfiles desde https://github.com/volatilityfoundation/profiles

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

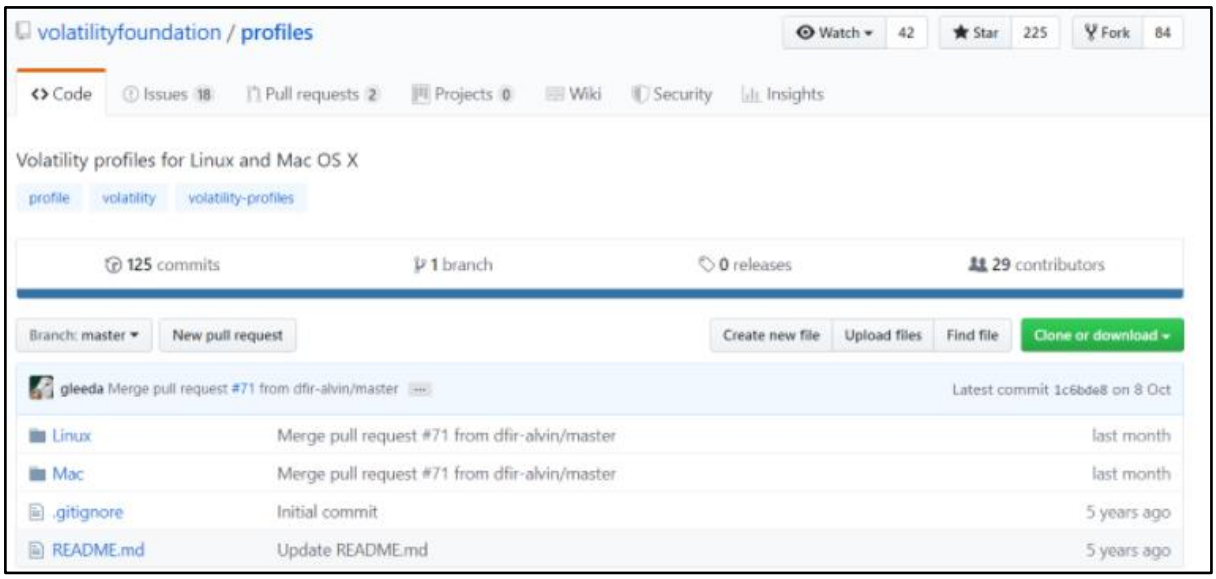

Ilustración 40 - Perfiles de volatility

Una vez descargados probamos a importarlos con la opción --plugins y comprobamos con el plugin **mac_get_profile** que es capaz de identificar el perfil para nuestra captura de RAM.

```
root@kali:/[redacted]# volatility --plugins=/media/seguridad/profiles_vo
latility/Mac/10.8/ -f findmeback.dmp mac_get_profile
Volatility Foundation Volatility Framework 2.6
Profile                                             Shift Address
--------------------------------------------------- -------------
MacMountainLion_10_8_1_AMDx64                       0x00006000000
```

Ilustración 41 - Perfil de volatility

Con el plugin **mac_mount** podemos visualizar cuales son las particiones y dispositivos montados en el sistema operativo.

```
[redacted] volatility --plugins=/media/seguridad/profiles_volatility/Mac/10.8/ -f findmeback.dmp --
profile=MacMountainLion_10_8_1_AMDx64 mac_mount
Volatility Foundation Volatility Framework 2.6
Device                          Mount Point                                                  Type
------------------------------- ------------------------------------------------------------ ----
/                               /dev/disk0s2                                                 hfs
/dev                            devfs                                                        devfs
/net                            map -hosts                                                   autofs
/home                           map auto_home                                                autofs
/Volumes/VMware Shared Folders .host:/VMware Shared Folders                                  vmhgfs
```

Ilustración 42 - Perfil de volatility

Con el plugin **mac_notesapp** podemos visualizar las notas del programa de notas por defecto de MAC OS.

```
[redacted] volatility --plugins=/media/seguridad/profiles_volatility/Mac/10.8/ -f findmeback.dmp
profile=MacMountainLion_10_8_1_AMDx64 mac_notesapp -D notes
Volatility Foundation Volatility Framework 2.6
Pid      Name                 Start              Size     Path
-------- -------------------- ------------------ -------- ----
248      Notes                0x0000000110dba504     2623 notes/Notes.248.110dba504.txt
248      Notes                0x0000000110dbaf51       75 notes/Notes.248.110dbaf51.txt
248      Notes                0x0000000110dbafaa       62 notes/Notes.248.110dbafaa.txt
248      Notes                0x0000000110dbaff6       61 notes/Notes.248.110dbaff6.txt
248      Notes                0x0000000110dbb040       72 notes/Notes.248.110dbb040.txt
248      Notes                0x00000001112a2f78       72 notes/Notes.248.1112a2f78.txt
248      Notes                0x00000001112b5700      391 notes/Notes.248.1112b5700.txt
248      Notes                0x00007fd0a14e00f0      391 notes/Notes.248.7fd0a14e00f0.txt
248      Notes                0x00007fd0a18bc018     2623 notes/Notes.248.7fd0a18bc018.txt
248      Notes                0x00007fd0a214ad20       72 notes/Notes.248.7fd0a214ad20.txt
248      Notes                0x00007fd0a2196c21       62 notes/Notes.248.7fd0a2196c21.txt
248      Notes                0x00007fd0a219ade1       61 notes/Notes.248.7fd0a219ade1.txt
248      Notes                0x00007fd0a219baf1       72 notes/Notes.248.7fd0a219baf1.txt
```

Ilustración 43 - Perfil de volatility

Con el plugin **mac_contacts** podemos obtener los contactos de la agenda del sistema.

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

```
ck# volatility --plugins=/media/seguridad/profiles_volatility/Mac/10.8/ -f findmeback.dmp --
profile=MacMountainLion_10_8_1_AMDx64 mac_contacts
Volatility Foundation Volatility Framework 2.6
KyeongsikLeekyeongsik lee Kyeongsik Lee lee kyeongsik Lee Kyeongsik
HyungjoonLeehyungjoon lee Hyungjoon Lee lee hyungjoon Lee Hyungjoon
F?lixGrobertf?lix grobert F?lix Grobert grobert f?lix Grobert F?lix
JoachimMetzjoachim metz Joachim Metz metz joachim Metz Joachim
OmarChoudaryomar choudary Omar Choudary choudary omar Choudary Omar
Georgeabitbolgeorge abitbol George abitbol abitbol george abitbol George
rootmerootme rootme rootme rootme ?0
Appleapple Apple apple Apple _
P???
KyeongsikLeekyeongsik lee Kyeongsik Lee lee kyeongsik Lee Kyeongsik
HyungjoonLeehyungjoon lee Hyungjoon Lee lee hyungjoon Lee Hyungjoon
F?lixGrobertf?lix grobert F?lix Grobert grobert f?lix Grobert F?lix
JoachimMetzjoachim metz Joachim Metz metz joachim Metz Joachim
OmarChoudaryomar choudary Omar Choudary choudary omar Choudary Omar
Georgeabitbolgeorge abitbol George abitbol abitbol george abitbol George
rootmerootme rootme rootme rootme ?0
Appleapple Apple apple Apple _
```

Ilustración 44 - Perfil de volatility

Con el plugin **mac_list_files** podemos listar los ficheros del sistema operativo cargados en memoria.

```
0xffffff800f737550 /Users/rootme/Library/Mail/V2/MailData/BackingStoreUpdateJournal
0xffffff800fa58838 /Users/rootme/Library/Mail/V2/IMAP-find.me.again.and.again@imap.gmail.com/INBOX.mbox/9C9B05D3-B08B-4144-AF4C-DAAAD5E478AD
0xffffff800f8f51f0 /Users/rootme/Library/Mail/V2/IMAP-find.me.again.and.again@imap.gmail.com/[Gmail].mbox/Tous les messages.mbox
0xffffff800f8ad5d0 /Users/rootme/Library/Mail/V2/MailData
0xffffff800f23e0f8 /Users/rootme/Library/Mail/V2/MailData/Accounts.plist
0xffffff800f8ec5d0 /Users/rootme/Library/Mail/V2/Mailboxes/Outbox.mbox/Info.plist
0xffffff800fafa648 /Users/rootme/Library/Mail/V2/IMAP-find.me.again.and.again@imap.gmail.com/[Gmail].mbox/Corbeille.mbox/9C9B05D3-B08B-4144-AF4C-DA
0xffffff800f91e7c0 /Users/rootme/Library/Mail/V2/IMAP-find.me.again.and.again@imap.gmail.com/Sent Messages.mbox/9C9B05D3-B08B-4144-AF4C-DAAAD5E478A
0xffffff800f8ba550 /Users/rootme/Library/Mail/V2/MailData/Envelope Index-shm
0xffffff800f5ab2e8 /Users/rootme/Library/Mail/V2/MailData/BackupTOC.plist
0xffffff800fdbe5d0 /Users/rootme/Library/Mail/V2/IMAP-find.me.again.and.again@imap.gmail.com/[Gmail].mbox/Suivis.mbox
0xffffff8010151930 /Users/rootme/Library/Mail/V2/IMAP-find.me.again.and.again@imap.gmail.com/INBOX.mbox/9C9B05D3-B08B-4144-AF4C-DAAAD5E478AD/Data/M
0xffffff800f20e4d8 /Users/rootme/Library/Mail/V2/IMAP-find.me.again.and.again@imap.gmail.com/[Gmail].mbox/Brouillons.mbox
0xffffff800fab0458 /Users/rootme/Library/Mail/V2/IMAP-find.me.again.and.again@imap.gmail.com/.mboxCache.plist
```

Ilustración 45 - Perfil de volatility

Con el plugin **mac_pstree** podemos visualizar el árbol de procesos del sistema operativo. Con el plugin **mac_pslist** es de forma similar pero no es en forma de árbol.

```
..Finder          155          501
..SystemUIServer  154          501
..Dock            153          501
..talagent        152          501
..Calendar        151          501
..Console         150          501
..Mail            148          501
..Terminal        147          501
...login          522          0
....bash          523          501
```

Ilustración 46 - Perfil de volatility

Puedes visualizar la lista completa de plugins de volatility para MAC OS en el siguiente recurso: https://github.com/volatilityfoundation/volatility/wiki/Mac

Ftk Imager

Es una herramienta que te permite abrir en modo lectura imágenes de disco y discos duros para poder extraer las evidencias no volátiles sin modificar el sistema de forma segura.

Se puede obtener desde el siguiente enlace:

https://accessdata.com/product-download/ftk-imager-version-4-2-1

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

FTK Imager te permite también crear imágenes de disco y capturar la memoria RAM. Nosotros después de varias pruebas y de integridad recomendamos más Magnet RAM Capture para realizar las capturas de RAM.

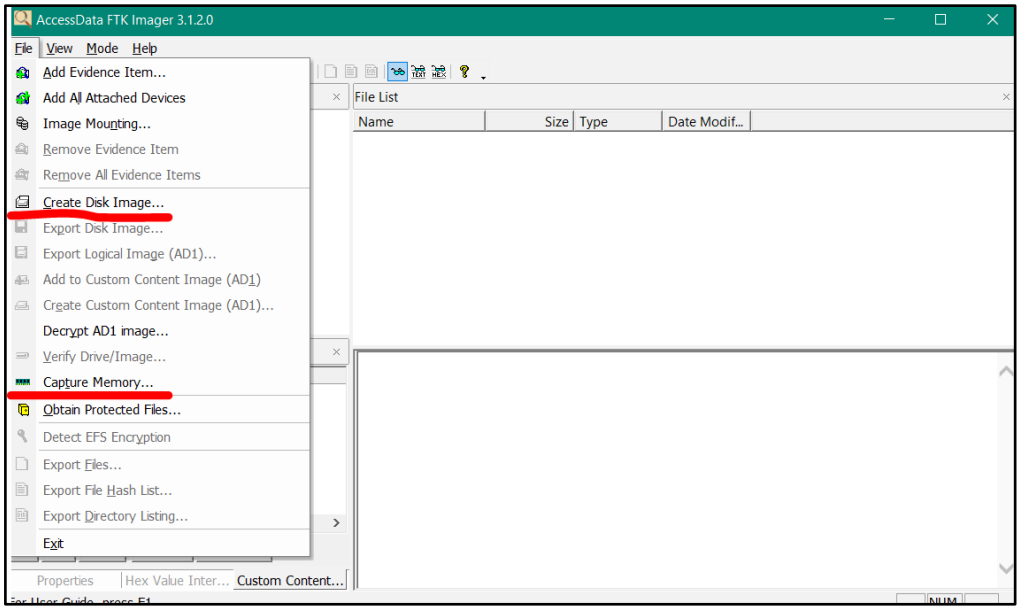

Ilustración 47 - AccessData Ftk Imager

Autopsy

Es una herramienta automática de análisis de memoria no volátil. La puedes descargar desde https://www.sleuthkit.org/autopsy/ .

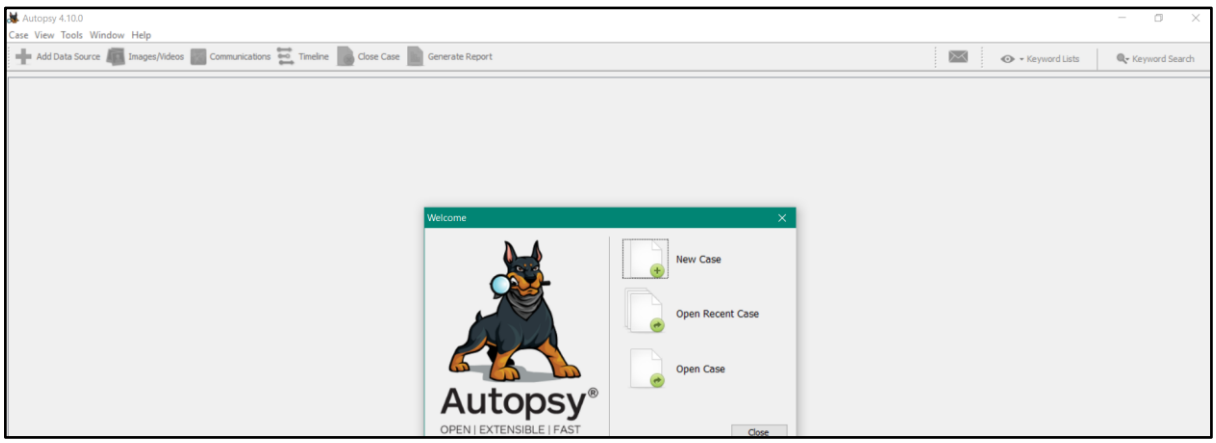

Ilustración 48 - Autopsy

Autopsy te automatiza la búsqueda de información y evidencias dividiendo por historial de navegación, cookies, descargar, programas instalados, documentos e imágenes recientes, correos electrónicos.

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

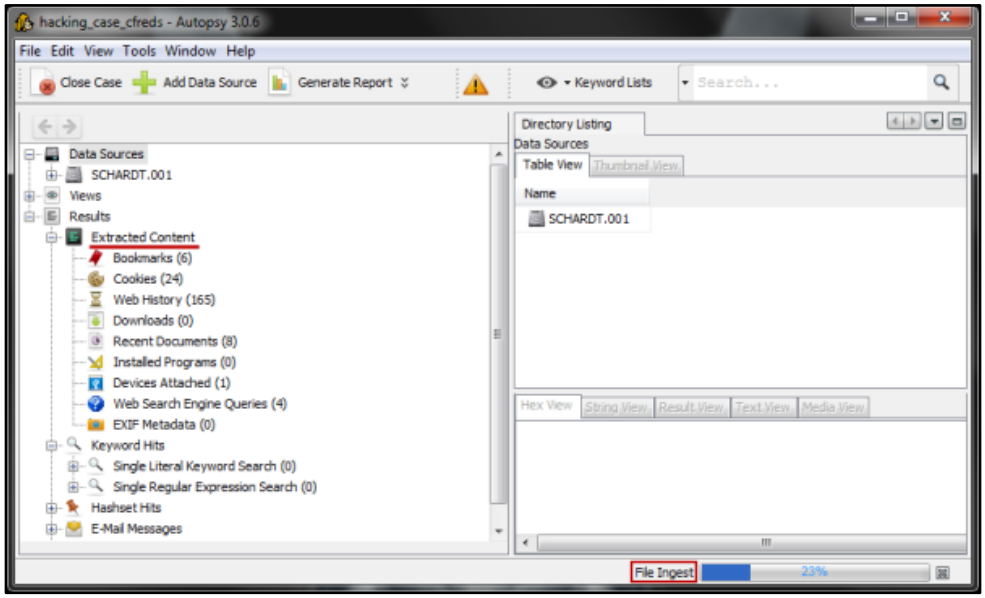

Ilustración 49 - Autopsy

También nos permite navegar por la evidencia en modo lectura sin modificarla y extraer las evidencias correctamente.

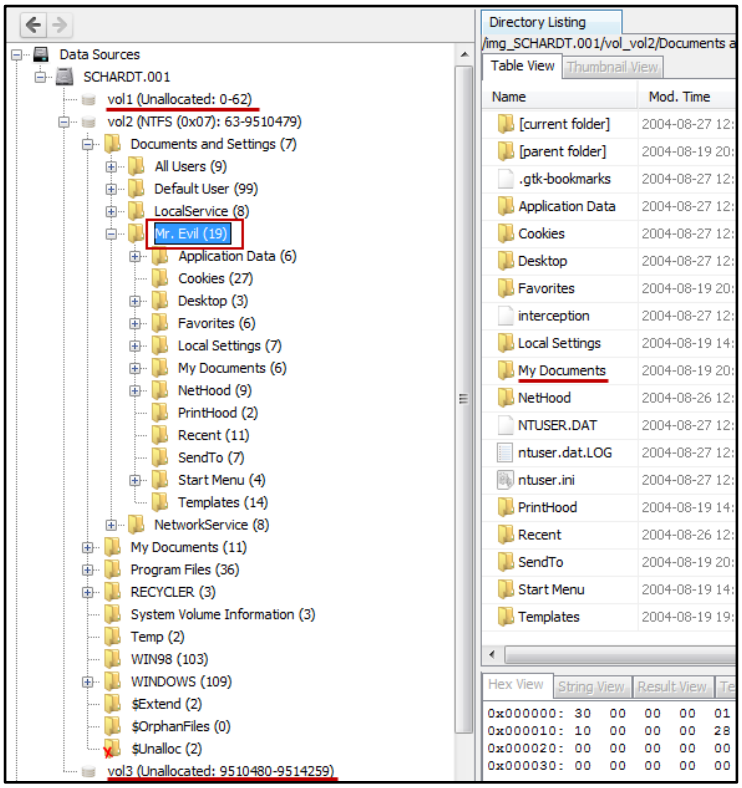

Ilustración 50 - Autopsy

SQLite Browser

Es una herramienta que nos permite navegar y abrir base de datos tipo SQLite. La mayoría de aplicaciones Android e IOS se utilizan para almacenar la información en ficheros de base de datos SQLite.

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

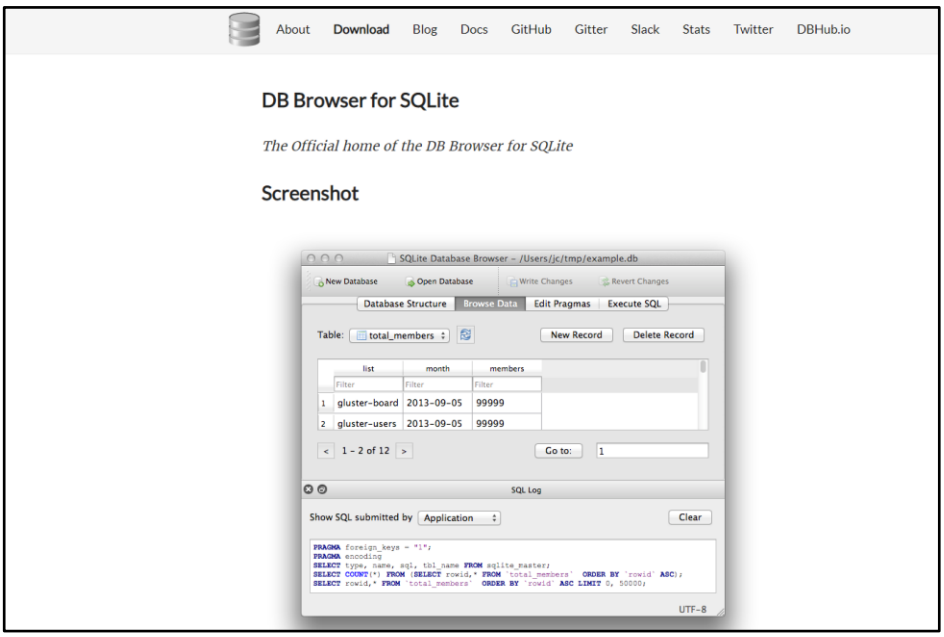

Ilustración 51 - SQLite Browser

WhatsApp las utiliza para almacenar en tu dispositivo tus contactos y mensajes que intercambias entre ellos. Con SQLite Browser podemos abrir las bases de datos y visualizar las conversaciones.

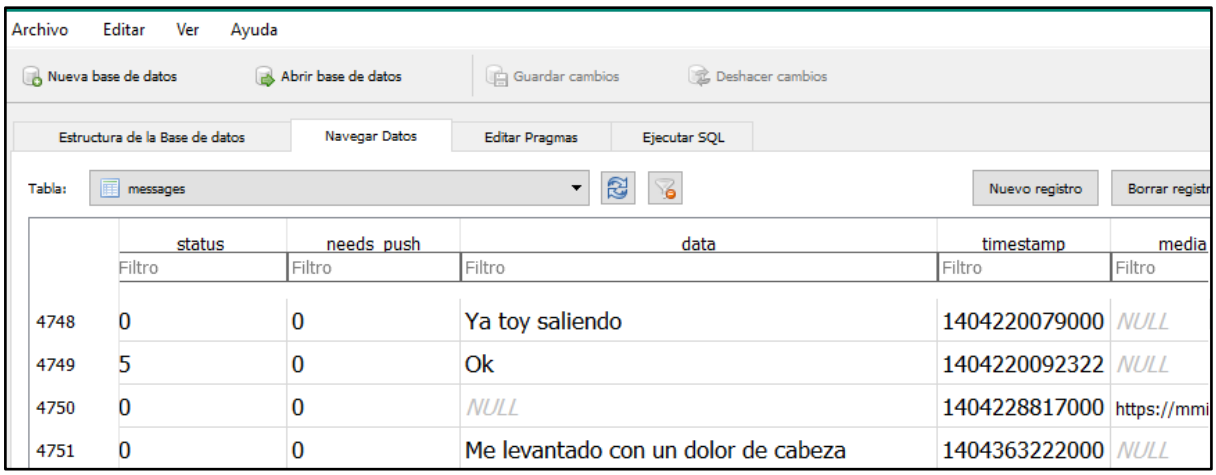

Ilustración 52 - Conversaciones de WhatsApp

4.5 Informe pericial y defensa en el juicio

Informe pericial

Para realizar un informe pericial se siguen una serie de fases:

Presentación del caso y aceptación

Primero se seleccionará y designará un perito. Se le preparará un presupuesto y aceptará o no el caso.

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

Realización del informe pericial

Una vez aceptado el caso tendremos que desarrollar y crear el informe pericial. Para ello seguiremos una serie de fases:

1. Definición de los objetivos de la pericial.
2. Análisis de las evidencias.
3. Toma y extracción de pruebas de las evidencias.
4. Análisis de las pruebas extraídas de las evidencias.
5. Conclusiones de la pericial.
6. Redacción del informe.
7. Visado.

Declaración en los juzgados

Una vez presentado el Informe Pericial tendremos que prepararnos para la declaración en los juzgados y cómo debemos actuar a la hora de declarar.

1. Vista oral. Ocurre meses después desde la redacción del dictamen. El perito debe prepararse para coordinar preguntas.
2. Declaración. El perito tendrá que ratificar el dictamen y aclarar dudas.

Durante la declaración nunca debemos dejarnos intimidar, tener un tono firme y pausado, respeto y consultar el dictamen.

Tratamiento del delito tecnológico

A la hora del tratamiento de un delito tecnológico se contemplan diferentes fases:

Instrucción del proceso

- Aceptación de la denuncia.
- Medidas cautelares para preservación de las pruebas.
- Declaración de denunciante y posible denunciado.
- Interrogatorio de los testigos.

La calificación y la vista oral

La calificación supone definir el Delito por el que se va a llevar la Causa a Juicio. Se divide en diferentes fases:

- Definición. Autor del delito y perjudicado/s.
- Conservación. Toda la prueba necesaria.
- Citación. Los testigos válidos para las partes.
- Señalamiento. Vista Oral Juzgado Penal.

Enlaces a recursos

- **https://docs.microsoft.com/en-us/sysinternals/**

Eduardo Sánchez Toril
CEO AllPentesting
formacion@allpentesting.es

- https://github.com/volatilityfoundation/volatility/wiki/Linux
- https://github.com/volatilityfoundation/volatility/wiki/Mac
- https://github.com/volatilityfoundation/profiles
- https://github.com/volatilityfoundation/volatility/wiki/Command-Reference
- https://www.nirsoft.net/utils/usb_devices_view.html
- https://www.the-sz.com/products/usbid/
- https://www.epochconverter.com/hex
- https://docs.microsoft.com/en-us/sysinternals/
- https://accessdata.com/product-download
- https://www.sleuthkit.org/autopsy/
- https://www.volatilityfoundation.org/
- https://sqlitebrowser.org/