13-6-2016

Análisis Forense

Trabajo final de Máster

UNIVERSITAT ROVIRA I VIRGILI

Portero Bolaños, Samuel Francisco

MÁSTER UNIVERSITARIO EN SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES

UNIVERSITAT OBERTA DE CATALUNYA

Contenido

1 INTRODUCCIÓN

El presente Trabajo Fin de Máster (a partir de ahora TFM) consiste en el análisis forense de una serie de evidencias digitales obtenidas tras una investigación policial. Se da por supuesto que el autor de este TFM es un perito forense con las autorizaciones judiciales necesarias para poder realizar el análisis.

1.1 MODELOS DE REFERENCIA

Para la elaboración de este TFM se ha seguido el modelo PMBOK de gestión de proyectos. Según este modelo, cualquier proyecto se divide en cinco etapas o grupo de procesos [1]:

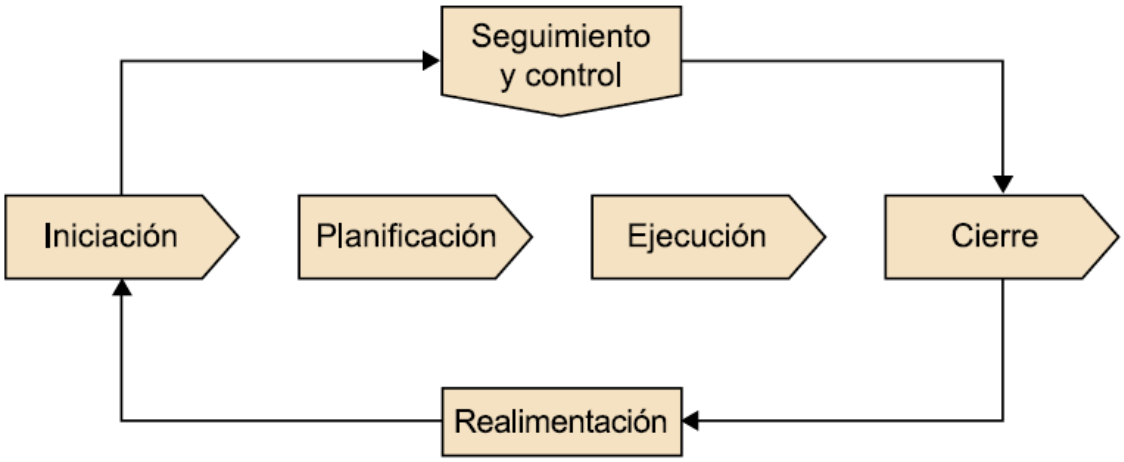


Figura 1: modelo PMBOK

Cada una de estas etapas ha sido desarrollada y entregada en las diferentes entregas parciales del trabajo fin de máster. El presente documento en concreto corresponde a las fases de iniciación y ejecución. La planificación se corresponde con la primera entrega mientras que el cierre se corresponde con la última entrega.

En todas ellas se han incluido los procesos de gestión de proyectos que se han estimado oportunos teniendo en cuenta la naturaleza de este TFM en particular.

1.2 JUSTIFICACIÓN

La motivación del autor para seleccionar este TFM es la pasión por esta rama dentro de la Seguridad de la Información. Desde siempre me ha gustado la seguridad informática y en particular el análisis forense. Me gustaría dedicarme profesionalmente a esta disciplina y he elegido este TFM para ampliar mis conocimientos forenses.

Respecto a la viabilidad, con los conocimientos adquiridos en las asignaturas superadas del Máster, la experiencia profesional de más de 10 años en el sector de la seguridad informática y el apoyo del equipo docente, considero que este TFM es más que viable.

1.3 OBJETIVO

Con el presente TFM pretendemos alcanzar los siguientes objetivos:

- Realizar el análisis forense de las evidencias digitales recibidas.
- Redactar un informe pericial como resultado del análisis realizado.
- Encontrar evidencias de posibles delitos cometidos por la pareja objeto de la investigación.
- Determinar el origen de las evidencias localizadas, ordenarlas cronológicamente y relacionarlas.
- Recoger aquellas pruebas que hayan dado resultado negativo.

1.4 ALCANCE

El alcance del TFM consiste en la redacción de la presente memoria, en la cual se irán incluyendo todas las entregas parciales hasta completarla con la entrega final. El objetivo de hacerlo de esta manera es invertir menos tiempo en la redacción final de la memoria. Al hacerlo de manera acumulativa no tenemos que perder tiempo en una redacción final, dejando tiempo para la preparación de la presentación.

Las entregas son las siguientes:

- Entrega parcial 1: Plan de trabajo.
- Entrega parcial 2: Propuesta de extremos y análisis de RAM y USB.
- Entrega parcial 3: Propuesta de memoria y análisis de disco duro.
- Entrega final de la memoria y la presentación.

La versión final de la memoria incluirá el informe pericial al completo. La presentación se entregará en un fichero independiente.

En caso de ser necesario, cada entrega parcial incluirá un directorio con todos los ficheros de evidencias referenciados en el informe pericial. En la entrega final se incluirán todos los ficheros referenciados.

2 MANIFIESTO

A continuación, se muestra el manifiesto que realizaría el perito en caso de que tuviese que defender el informe en un juicio.

Destinatario:

Nº expediente/procedimiento:

D.. Samuel Portero Bolaños, Ingeniero técnico en Informática por la Escuela Técnica Superior de Ingenieros de la Universidad de Sevilla, habiendo sido requerido por /el Juzgado de ..... Instancia número ..... de ....., sección ..... / la parte demandante/demandada ....., procurador del caso ....., para emitir informe pericial informático en el procedimiento ……

El Perito que subscribe dictamina con arreglo a su fiel saber y entender en los términos que subsiguientemente se definen y determinan, en Sevilla a 2 de Abril de 2016.

El Perito DECLARA que conoce las tachas, recogidas en el artículo 343 de la Ley de Enjuiciamiento Civil, y así mismo MANIFIESTA:

- No ser cónyuge o pariente por consanguinidad o afinidad, dentro del cuarto grado civil de una de las partes o de sus Abogados o Procuradores.
- No tener interés directo o indirecto en el asunto o en otro semejante.
- No estar o haber estado en situación de dependencia o de comunidad o contraposición de intereses con alguna de las partes o con sus Abogados o Procuradores.
- No tener amistad íntima o enemistad con cualquiera de las partes o sus Procuradores o Abogados. (Siempre que sea cierto, en otro caso tendrá que explicar el tipo de relación que existe).
- No creer que exista ninguna otra circunstancia que le haga desmerecer en el concepto profesional.

El Perito DECLARA que conoce las responsabilidades civiles, penales, disciplinarias y asociativas que comporta la aceptación del cargo de perito y la realización del presente informe, al amparo del artículo 335.2 de la Ley de Enjuiciamiento Civil, que reza así:

Al emitir el dictamen, todo perito deberá manifestar, bajo juramento o promesa de decir verdad, que ha actuado y, en su caso, actuará con la mayor objetividad posible, tomando en consideración tanto lo que pueda favorecer como lo que sea susceptible de causar perjuicio a cualquiera de las partes, y que conoce las sanciones penales en las que podría incurrir si incumpliere su deber como perito.

3 OBJETO DEL PERITAJE

El presente informe pericial debe dar respuesta a los siguientes extremos planteados:

E1: ¿QUÉ PROCESOS EN EJECUCIÓN TENÍA EL PORTÁTIL EN EL MOMENTO DE SER INTERVENIDO POR LA POLICÍA?

E2: ¿EXISTE ALGÚN TIPO DE MALWARE EN EJECUCIÓN O INSTALADO EN EL DISCO DURO? ¿EL MALWARE HA SIDO UTILIZADO POR LOS USUARIOS DEL SISTEMA COMO HERRAMIENTA O HAN SIDO INFECTADOS SIN SABERLO?

E3: ¿EXISTEN FICHEROS CIFRADOS EN EL EQUIPO INTERVENIDO? ¿SE HA PODIDO RECUPERAR SU CONTENIDO?

E4: ¿QUÉ CONEXIONES DE RED TENÍA EL PORTÁTIL EN EL MOMENTO DE SER INTERVENIDO POR LA POLICÍA?

E5: ¿QUÉ USUARIOS HAY DEFINIDOS EN EL SO? ¿CUÁLES FUERON LAS FECHAS DE CREACIÓN Y LOS ÚLTIMOS ACCESOS?

E6: ¿CUÁL DE ELLOS ESTÁ LOGADO EN EL MOMENTO DE LA INTERVENCIÓN? ¿ESTABA ESTABLECIENDO ALGÚN TIPO DE COMUNICACIÓN CON ALGUNA OTRA PERSONA EN EL MOMENTO DE LA INTERVENCIÓN O ANTES DE ELLA? ¿HA SIDO POSIBLE ACCEDER AL CONTENIDO?

E7: ¿EXISTEN EVIDENCIAS DE USO FRAUDULENTO DE TARJETAS DE CRÉDITO?

E8: ¿EXISTEN FICHEROS ELIMINADOS? ¿SE HA PODIDO RECUPERAR SU CONTENIDO?

4 ANTECEDENTES

A raíz de una investigación, un cuerpo policial realiza una entrada y registro en el domicilio de una pareja. Durante la misma se interviene un ordenador portátil, el cual, en el momento de efectuar la entrada, se encontraba en funcionamiento. Los agentes especializados que participan en la diligencia deciden realizar una captura de la memoria *RAM* del ordenador. Seguidamente, los mismos agentes realizan una imagen del disco duro del portátil decomisado.

Finalmente, los agentes hallan un dispositivo *USB* escondido en un cajón del dormitorio y deciden obtener una imagen forense del mismo, la cual se incorpora a las dos evidencias antes citadas. Todas las acciones llevadas a cabo por parte de los agentes quedan reflejadas en acta por el secretario o secretaria judicial.

Una vez finalizada la diligencia, las evidencias digitales se transportan, según los procedimientos habituales, a tu laboratorio para ser analizadas. Suponiendo que dispongas de las autorizaciones judiciales que te permitan analizar el contenido del disco duro del ordenador (correos electrónicos locales incluidos, si los hubiera) y de las otras evidencias adquiridas, tienes que realizar un análisis completo de todas las imágenes forenses y redactar el informe pericial del citado análisis, documentando todas aquellas evidencias que hayas podido localizar e indicando cuáles son los límites de tu análisis.

5 FUENTES DE INFORMACIÓN Y DATOS DE PARTIDA

Para la realización del presente análisis forense, el perito cuenta con las siguientes evidencias digitales:

- Información contenida en un volcado forense obtenido de la memoria *RAM* del ordenador portátil encontrado en el domicilio de la pareja acusada. Según el reloj del equipo local, la fecha de la intervención policial fue el 21 de Octubre de 2015.
- Imagen forense obtenida de un dispositivo *USB* encontrado en el domicilio de la pareja acusada. Las fechas de últimos accesos del dispositivo apuntan al 15 de Enero de 2016.
- Información contenida en una imagen forense obtenida de un disco duro marca *WD Scorpio Blue*, modelo *WD3200 BPVT* de 320GB, con número de serie *WX81E32FLU08*, extraído del ordenador portátil encontrado en el domicilio de la pareja. Según el log adjuntado con la imagen, fue generada el 10 de Semptiembre de 2015.

Figura 2: Fotografía pequeña disco duro

Figura 3: Fotografía grande disco duro

Se aprecian diferencias entre las fechas de las tres evidencias que serán analizadas más adelante.

6 ESTÁNDARES Y NORMAS

No existe ninguna estándar o norma de cómo hacer un informe pericial, pero para la realización del presente análisis se ha seguido la estructura del libro de Xabiel García Pañeda y David Melendi Palacio: *La peritación informática. Un enfoque práctico* [2].

También se han tenido en cuenta la guía de buenas prácticas *ISO/IEC 27037:2012* [3] para el manejo de evidencias digitales.

Respecto a los medios técnicos, se ha utilizado un portátil *HP*, modelo *EliteBook 8460p* con sistema operativo *Windows 7 Professional de 64 bits*, con las siguientes herramientas forenses instaladas:

- La comprobación de la integridad de la evidencia de la memoria RAM, así como la de los ficheros de evidencias encontradas adjuntos, se ha realizado con la herramienta *fciv* de *Microsoft* en su versión 2.05 [4].
- La imagen de la memoria RAM ha sido analizada mediante el software *Volatility* en su versión 2.5 para *Windows* [5].
- Para el análisis de la imagen de disco duro y dispositivo USB objetos de este informe, se ha utilizado el software *Autopsy* en su versión 4.0.0 para *Windows* [6]. La comprobación de la integridad de estas dos evidencias también se ha realizado con este mismo software.
- Para la extracción de información a partir de un volcado de memoria de *Skype*, vamos a utilizar una herramienta llamada *Skypeex* [7], la cual extrae información sobre conversaciones de *Skype* a partir de un volcado de memoria en formato texto.
- Para la obtención de las contraseñas del sistema operativo se ha utilizado la herramienta de fuerza bruta *John the ripper* [8], incluida en la distribución de pentesting *Kali Linux 2.0* [9].
- Se ha usado la herramienta *Foca Free 3.2* [10] para el análisis de metadatos en documentos. Algunos documentos incorporan información oculta sobre su autor, versiones de programas, etc. que podemos extraer con esta herramienta.
- Se ha usado el complemento para el navegador web Firefox *SQLite Manager* [11], para analizar el contenido de bases de datos en el formato *SQLite*.
- Se ha usado la herramienta *Windows Registry Recovery* [12] para analizar el contenido del registro *Windows* de la imagen del disco duro.
- Se ha usado la herramienta *S-tools* [13] para recuperar información oculta en imágenes a través de técnicas de esteganografía.
- Se ha usado la herramienta *SkypeLogView* [14] para analizar los *logs* de la aplicación *Skype*.
- *WinHex* [15] para analizar el contenido oculto de los ficheros *PDF*.
- Para el montaje del volumen cifrado encontrado se ha usado *TrueCrypt* [16].

7 LIMITACIONES

En el análisis mostrado a continuación, el perito no disponía de ninguna limitación a nivel legal: contaba con los permisos para analizar toda la información posible, incluidos posibles correos electrónicos.

Sin embargo, sí se ha encontrado con algunas limitaciones técnicas:

- No se han encontrado ficheros eliminados ni en el espacio asignado ni en el desasignado del dispositivo *USB*.
- Se detecta que la aplicación de intercambio de documentos *Dropbox* está instalada en el equipo, pero no se ha encontrado información subida o descargada.
- No ha sido posible encontrar la contraseña para abrir el fichero *Contc.ods* de la carpeta personal del usuario *Tom* de la imagen del disco duro.
- Tampoco se ha podido localizar el fichero llamado *Home.ods* de la carpeta personal del usuario *Tom*.
- Se han encontrado evidencias de la compra de un programador de tarjetas de crédito y de la instalación del software para utilizarlo, pero no ha sido posible determinar si ha sido utilizado en alguna ocasión para el copiado ilegal de tarjetas.

8 RESOLUCIÓN O INFORME PERICIAL

8.1 CONSIDERACIONES PRELIMINARES

Antes de comenzar el análisis de las evidencias recibidas, es necesario realizar una comprobación de su integridad. Se calcula el valor hash de las imágenes del disco duro, la memoria *RAM* y el dispositivo *USB*.

8.1.1 Integridad de la imagen de memoria RAM

Se comprueba que la integridad de la evidencia se ha mantenido ya que los valores *hash md5* recibidos coinciden con los calculados por el perito con la herramienta *fciv*:

Evidencia	MD5 Recibido	MD5 Calculado
RAM	2B5AC23E63FC7FE3627D67CE53B41738	2b5ac23e63fc7fe3627d67ce53b41738

Figura 4: Integridad RAM

8.1.2 Integridad de la imagen del dispositivo USB

Se comprueba que la integridad de la evidencia se ha mantenido ya que los valores hash md5 recibidos coinciden con los calculados por el perito con la herramienta *Autopsy*:

Evidencia	MD5 Recibido	MD5 Calculado
USB	f6ff3f7022ae6c3315ac6a1b781e72b2	f6ff3f7022ae6c3315ac6a1b781e72b2

Figura 5: Integridad USB

8.1.3 Integridad de la imagen del disco duro

Se comprueba que la integridad de la evidencia se ha mantenido ya que los valores hash md5 recibidos coinciden con los calculados por el perito con la herramienta *Autopsy*:

Evidencia	MD5 Recibido	MD5 Calculado
Disco duro	8658bbc4d7e502bfde4f7f54dd2addf4	8658bbc4d7e502bfde4f7f54dd2addf4

Figura 6: Integridad disco duro

8.1.4 Conclusiones a las consideraciones preliminares

En los tres casos se comprueba que los valores calculados coinciden con los calculados por la policía en el domicilio de la pareja. Por lo tanto, podemos garantizar que las evidencias no han sido modificadas desde su extracción.

8.2 ANÁLISIS

El análisis realizado a continuación pretende dar respuesta a los extremos planteados en el **apartado 3: Objeto del peritaje** del presente documento. Algunos de los análisis realizados no nos ofrecerán directamente la respuesta a los extremos pero serán necesarios para que otros análisis puedan responder a éstos.

Para todo este análisis se ha seguido un procedimiento que mantiene la integridad de las evidencias, es decir, sin llegar a modificar su contenido, por lo que cualquiera que repitiera el procedimiento sobre las mismas evidencias obtendría los mismos resultados.

Cada análisis realizado contiene los siguientes apartados:

- Objetivo: propósito para realizar el análisis. Por ejemplo, dar respuesta a un extremo.
- Procedimiento: los pasos seguidos para obtener los resultados.
- Hallazgos: resultados obtenidos en el análisis. Dependiendo de la importancia de los mismos, serán incluidos o no como evidencias.

8.2.1 Análisis de la memoria RAM

Como se indicó anteriormente, para el análisis de la *RAM* se utilizará la herramienta *Volatility*. Se trata de una herramienta que una vez descargada no necesita instalación.

Contiene un ejecutable al cual se le pueden pasar múltiples parámetros, los cuales nos permiten mostrar de manera clasificada la información contenida en la imagen. Para ver todos los posibles comandos [17] lo ejecutamos con el parámetro *-h*.

8.2.1.1 Prerrequisitos: Sistema operativo de la imagen

8.2.1.1.1 Objetivo

El objetivo del primer análisis es conocer el tipo de sistema operativo del portátil del que se extrajo la imagen de la memoria *RAM*. Esta información será necesaria para extraer el resto de información de la imagen.

8.2.1.1.2 Procedimiento

Usamos la herramienta *Volatility* pasándole como parámetros la imagen de la memoria *RAM* y el comando *imageinfo*:

```
D:\TFM>volatility-2.5.standalone.exe -f ANN-PC-20151021-135652.raw imageinfo
Volatility Foundation Volatility Framework 2.5
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP0x86, Win7SP1x86
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (D:\TFM\ANN-PC-20151021-135652.raw)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x8196dbe8L
          Number of Processors : 1
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0x8196ec00L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2015-10-21 13:56:57 UTC+0000
     Image local date and time : 2015-10-21 15:56:57 +0200
```

Figura 7: Identificación del SO con volatility

8.2.1.1.3 Hallazgos

La imagen ha sido obtenida de un ordenador con **Windows 7 SP0 o SP1 de 32 bits.**

8.2.1.2 Procesos en ejecución

8.2.1.2.1 Objetivo

Conocer qué procesos estaban en ejecución en el momento en el que se realizó el volcado de memoria.

8.2.1.2.2 Procedimiento

Con el perfil del sistema operativo y el parámetro *pslist* de *Volatility* obtenemos la lista de procesos en ejecución en el momento de la extracción de la memoria:

```
D:\IFM>volatility-2.5.standalone.exe -f ANN-PC-20151021-135652.raw --profile=Win7SP1x86 pslist
Volatility Foundation Volatility Framework 2.5
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------
0x83126730 System                    4      0     81      520 ------      0 2015-10-21 13:52:52 UTC+0000
0x83fe7920 smss.exe                212      4      2       29 ------      0 2015-10-21 13:52:52 UTC+0000
0x848db930 csrss.exe               296    288      9      379      0      0 2015-10-21 13:53:02 UTC+0000
0x84a3dd40 wininit.exe             352    288      3       76      0      0 2015-10-21 13:53:04 UTC+0000
0x8490aa58 csrss.exe               364    344      7      242      1      0 2015-10-21 13:53:04 UTC+0000
0x848e9030 winlogon.exe            404    344      3      111      1      0 2015-10-21 13:53:07 UTC+0000
0x8497f030 services.exe            440    352      9      186      0      0 2015-10-21 13:53:07 UTC+0000
0x83f60b38 lsass.exe               456    352      7      583      0      0 2015-10-21 13:53:07 UTC+0000
0x83f64a40 lsm.exe                 464    352     10      139      0      0 2015-10-21 13:53:07 UTC+0000
0x84b72d40 svchost.exe             572    440     10      352      0      0 2015-10-21 13:53:08 UTC+0000
0x8498c030 svchost.exe             636    440      8      265      0      0 2015-10-21 13:53:09 UTC+0000
0x84bf5030 svchost.exe             684    440     21      514      0      0 2015-10-21 13:53:09 UTC+0000
0x84c20ad0 svchost.exe             812    440     25      686      0      0 2015-10-21 13:53:10 UTC+0000
0x84c33030 svchost.exe             860    440     36     1015      0      0 2015-10-21 13:53:11 UTC+0000
0x84c3ad40 audiodg.exe             920    684      5      130      0      0 2015-10-21 13:53:11 UTC+0000
0x84c4e728 svchost.exe            1004    440     21      482      0      0 2015-10-21 13:53:12 UTC+0000
0x84c83030 svchost.exe            1176    440     15      382      0      0 2015-10-21 13:53:13 UTC+0000
0x84cb02e0 spoolsv.exe            1280    440     12      278      0      0 2015-10-21 13:53:15 UTC+0000
0x84cbe478 svchost.exe            1316    440     19      298      0      0 2015-10-21 13:53:15 UTC+0000
0x84d0c358 svchost.exe            1400    440     14      220      0      0 2015-10-21 13:53:16 UTC+0000
0x848d5d40 taskhost.exe            368    440      8      197      1      0 2015-10-21 13:54:21 UTC+0000
0x832054c8 sppsvc.exe             1120    440      7      145      0      0 2015-10-21 13:54:22 UTC+0000
0x84c06810 dwm.exe                 552    812      3       68      1      0 2015-10-21 13:54:30 UTC+0000
0x83fc4518 explorer.exe            692    240     25      844      1      0 2015-10-21 13:54:30 UTC+0000
0x849bc770 Skype.exe              1980    692     36     1089      1      0 2015-10-21 13:54:32 UTC+0000
0x84b73030 yUmikJMYd3b.ex         1776    692      6      206      1      0 2015-10-21 13:54:32 UTC+0000
0x832d0d40 SearchIndexer.         1124    440     11      700      0      0 2015-10-21 13:54:39 UTC+0000
0x832c06d0 wmpnetwk.exe            964    440      9      240      0      0 2015-10-21 13:54:44 UTC+0000
0x832ccd40 WinHex.exe              512    692      1       73      1      0 2015-10-21 13:54:46 UTC+0000
0x832c2938 TrueCrypt.exe          2244    692      5      261      1      0 2015-10-21 13:55:00 UTC+0000
0x83230d40 svchost.exe            2336   1776      6      161      1      0 2015-10-21 13:55:06 UTC+0000
0x832b2d40 notepad.exe            2396   2336      3       72      1      0 2015-10-21 13:55:07 UTC+0000
0x833acd40 svchost.exe            2840    440     14      341      0      0 2015-10-21 13:55:20 UTC+0000
0x83353560 WUDFHost.exe           1484    812      8      215      0      0 2015-10-21 13:56:44 UTC+0000
0x83fa0d40 DumpIt.exe             2948    692      2       38      1      0 2015-10-21 13:56:51 UTC+0000
0x83383030 conhost.exe            2668    364      2       52      1      0 2015-10-21 13:56:52 UTC+0000
0x832c5a60 WmiPrvSE.exe           2252    572      6        0      0      0 2015-10-21 13:57:18 UTC+0000
0x834d7538 slui.exe               1456    572      9       16 ------      0 2015-10-21 13:59:27 UTC+0000
0x833d1938 taskeng.exe            2688    860      7 181...59 ------      0 2015-10-21 14:00:00 UTC+0000
0x832689e0 DropboxUpdate.         3644   2688      6       19 ------      0 2015-10-21 14:00:00 UTC+0000
0x834c5a60 DropboxUpdate.         3744   1624      4       98 ------      0 2015-10-21 14:00:00 UTC+0000
0x834e7030 DropboxUpdate.         3856    440     13  6488175 ------      0 2015-10-21 14:00:03 UTC+0000
```

Figura 8: Listado de procesos en ejecución

8.2.1.2.3 Hallazgos

Si ignoramos los procesos del propio sistema operativo, vemos una serie de procesos que debemos tener en consideración:

- **Skype.exe**: servicio de videollamadas entre particulares. Vamos a analizar con quien estaba en contacto el sospechoso y qué información estaban intercambiando.
- **yUmikJMYd3b.exe**: tiene un nombre extraño, por lo que analizaremos si se trata de algún tipo de malware.
- **WinHex.exe**: se trata de un programa utilizado en análisis forenses. Es posible que fuera utilizado por el agente especialista, no se tendrá en cuenta de momento.

- **TrueCrypt.exe**: proceso utilizado para cifrar todo o parte de una unidad de almacenamiento. Tratar de obtener el contenido cifrado y las claves para descifrarlo.
- **Notepad.exe**: editor de textos. Se tratará de obtener el fichero que se estaba editando en el momento del volcado de memoria.
- **DumpIt.exe**: software para realizar volcados de memoria. Se considera que fue utilizado por el agente especialista y no se tendrá más en cuenta en el análisis.
- **DropboxUpdate.exe**: es un proceso de actualización de 'Dropbox', servicio en la nube para almacenamiento de información. Se analizará el historial de ficheros subidos/descargados en el análisis del disco duro (apartado 8.2.3), ya que podría utilizarse para subir o descargar ficheros utilizados por algún tipo de malware.

Se adjuntan hallazgos al informe (**evidencia A1** del Anexo).

8.2.1.3 Dependencia entre procesos

8.2.1.3.1 Objetivo

Analizar si existe dependencia entre los procesos, de manera que podamos conocer si un posible malware está haciendo uso de otros procesos del sistema.

8.2.1.3.2 Procedimiento

Utilizamos la herramienta *Volatility* a la cual le pasamos la imagen, el perfil y el comando *pstree*:

```
D:\TFM>volatility-2.5.standalone.exe -f ANN-PC-20151021-135652.raw --profile=Win7SP1x86 pstree
Volatility Foundation Volatility Framework 2.5
Name                                                 Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x848db930:csrss.exe                                296    288      9    379 2015-10-21 13:53:02 UTC+0000
 0x84a3dd40:wininit.exe                              352    288      3     76 2015-10-21 13:53:04 UTC+0000
. 0x8497f030:services.exe                            440    352      9    186 2015-10-21 13:53:07 UTC+0000
.. 0x84cb02e0:spoolsv.exe                           1280    440     12    278 2015-10-21 13:53:15 UTC+0000
.. 0x84c20ad0:svchost.exe                            812    440     25    686 2015-10-21 13:53:10 UTC+0000
... 0x83353560:WUDFHost.exe                         1484    812      8    215 2015-10-21 13:56:44 UTC+0000
... 0x84c06810:dwm.exe                               552    812      3     68 2015-10-21 13:54:30 UTC+0000
.. 0x834e7030:DropboxUpdate.                        3856    440     13 64...5 2015-10-21 14:00:03 UTC+0000
.. 0x84c83030:svchost.exe                           1176    440     15    382 2015-10-21 13:53:13 UTC+0000
.. 0x84cbe478:svchost.exe                           1316    440     19    298 2015-10-21 13:53:15 UTC+0000
.. 0x84bf5030:svchost.exe                            684    440     21    514 2015-10-21 13:53:09 UTC+0000
... 0x84c3ad40:audiodg.exe                           920    684      5    130 2015-10-21 13:53:11 UTC+0000
.. 0x833acd40:svchost.exe                           2840    440     14    341 2015-10-21 13:55:20 UTC+0000
.. 0x84b72d40:svchost.exe                            572    440     10    352 2015-10-21 13:53:08 UTC+0000
... 0x834d7538:slui.exe                             1456    572      9     16 2015-10-21 13:59:27 UTC+0000
... 0x832c5a60:WmiPrvSE.exe                         2252    572      6      0 2015-10-21 13:57:18 UTC+0000
.. 0x832054c8:sppsvc.exe                            1120    440      7    145 2015-10-21 13:54:22 UTC+0000
.. 0x832c06d0:wmpnetwk.exe                           964    440      9    240 2015-10-21 13:54:44 UTC+0000
.. 0x84c4e728:svchost.exe                           1004    440     21    482 2015-10-21 13:53:12 UTC+0000
.. 0x84c33030:svchost.exe                            860    440     36   1015 2015-10-21 13:53:11 UTC+0000
... 0x833d1938:taskeng.exe                          2688    860      7 18...9 2015-10-21 14:00:00 UTC+0000
.... 0x832689e0:DropboxUpdate.                      3644   2688      6     19 2015-10-21 14:00:00 UTC+0000
.. 0x832d0d40:SearchIndexer.                        1124    440     11    700 2015-10-21 13:54:39 UTC+0000
.. 0x848d5d40:taskhost.exe                           368    440      8    197 2015-10-21 13:54:21 UTC+0000
.. 0x84d0c358:svchost.exe                           1400    440     14    220 2015-10-21 13:53:16 UTC+0000
.. 0x8498c030:svchost.exe                            636    440      8    265 2015-10-21 13:53:09 UTC+0000
. 0x83f60b38:lsass.exe                               456    352      7    583 2015-10-21 13:53:07 UTC+0000
. 0x83f64a40:lsm.exe                                 464    352     10    139 2015-10-21 13:53:07 UTC+0000
 0x83fc4518:explorer.exe                             692    240     25    844 2015-10-21 13:54:30 UTC+0000
. 0x832ccd40:WinHex.exe                              512    692      1     73 2015-10-21 13:54:46 UTC+0000
. 0x832c2938:TrueCrypt.exe                          2244    692      5    261 2015-10-21 13:55:00 UTC+0000
 0x84b73030:yUmikJMYd3b.ex                          1776    692      6    206 2015-10-21 13:54:32 UTC+0000
. 0x83230d40:svchost.exe                            2336   1776      6    161 2015-10-21 13:55:06 UTC+0000
.. 0x832b2d40:notepad.exe                           2396   2336      3     72 2015-10-21 13:55:07 UTC+0000
. 0x83fa0d40:DumpIt.exe                             2948    692      2     38 2015-10-21 13:56:51 UTC+0000
. 0x849bc770:Skype.exe                              1980    692     36   1089 2015-10-21 13:54:32 UTC+0000
 0x83126730:System                                     4      0     81    520 2015-10-21 13:52:52 UTC+0000
. 0x83fe7920:smss.exe                                212      4      2     29 2015-10-21 13:52:52 UTC+0000
 0x848e9030:winlogon.exe                             404    344      3    111 2015-10-21 13:53:07 UTC+0000
 0x8490aa58:csrss.exe                                364    344      7    242 2015-10-21 13:53:04 UTC+0000
. 0x83383030:conhost.exe                            2668    364      2     52 2015-10-21 13:56:52 UTC+0000
 0x834c5a60:DropboxUpdate.                          3744   1624      4     98 2015-10-21 14:00:00 UTC+0000
```

Figura 9: Dependencia entre procesos

8.2.1.3.3 Hallazgos

Podemos ver que el proceso ***yUmikJMYd3b.exe*** lanza 2 procesos hijos: ***svchost.exe*** y el del editor ***notepad.exe*** visto anteriormente.

- *Svchost.exe* es un proceso que hospeda, o contiene, otros servicios individuales que usa Windows para realizar diversas funciones. Es habitual que ciertos tipos de malware hagan uso de él para conseguir sus objetivos.
- *Notepad.exe* es un editor de textos incluido en *Windows 7*.

8.2.1.4 Procesos ocultos

8.2.1.4.1 Objetivo

Conocer si existen más procesos en ejecución de los consultados anteriormente.

8.2.1.4.2 Procedimiento

Utilizamos la herramienta *volatility* a la cual le pasamos la imagen, el perfil y el comando *psxview*:

```
D:\TFM>volatility-2.5.standalone.exe -f ANN-PC-20151021-135652.raw --profile=Win7SP1x86 psxview
Volatility Foundation Volatility Framework 2.5
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
---------- -------------------- ------ ------ ------ -------- ------ ----- ------- -------- --------
0x3e964a40 lsm.exe                 464 True   True   True     True   True  True    False
0x3f4b2d40 notepad.exe            2396 True   True   True     True   True  True    True
0x3ded5d40 taskhost.exe            368 True   True   True     True   True  True    False
0x3f4ccd40 WinHex.exe              512 True   True   True     True   True  True    True
0x3da33030 svchost.exe             860 True   True   True     True   True  True    False
0x3e9c4518 explorer.exe            692 True   True   True     True   True  True    True
0x3f4689e0 DropboxUpdate.         3644 True   True   True     True   True  True    False
0x3ddf5030 svchost.exe             684 True   True   True     True   True  True    False
0x3f2c5a60 DropboxUpdate.         3744 True   True   True     False  True  True    False
0x3df8c030 svchost.exe             636 True   True   True     True   True  True    True
0x3da06810 dwm.exe                 552 True   True   True     True   True  True    False
0x3da83030 svchost.exe            1176 True   True   True     True   True  True    True
0x3da4e728 svchost.exe            1004 True   True   True     True   True  True    False
0x3df7f030 services.exe            440 True   True   True     True   True  True    False
0x3f2e7030 DropboxUpdate.         3856 True   True   True     False  True  True    False
0x3e9a0d40 DumpIt.exe             2948 True   True   True     True   True  True    False
0x3e960b38 lsass.exe               456 True   True   True     True   True  True    False
0x3f583030 conhost.exe            2668 True   True   True     True   True  True    False
0x3f2d7538 slui.exe               1456 True   True   True     True   True  True    False
0x3dc3dd40 wininit.exe             352 True   True   True     True   True  True    True
0x3f4c5a60 WmiPrvSE.exe           2252 True   True   True     True   True  True    False
0x3f4054c8 sppsvc.exe             1120 True   True   True     True   True  True    True
0x3f430d40 svchost.exe            2336 True   True   True     True   True  True    True
0x3da20ad0 svchost.exe             812 True   True   True     True   True  True    False
0x3f5d1938 taskeng.exe            2688 True   True   True     False  True  True    False
0x3dfbc770 Skype.exe              1980 True   True   True     True   True  True    True
0x3db0c358 svchost.exe            1400 True   True   True     True   True  True    False
0x3dab02e0 spoolsv.exe            1280 True   True   True     True   True  True    True
0x3f4c2938 TrueCrypt.exe          2244 True   True   True     True   True  True    True
0x3f553560 WUDFHost.exe           1484 True   True   True     True   True  True    False
0x3f4c06d0 wmpnetwk.exe            964 True   True   True     True   True  True    True
0x3f5acd40 svchost.exe            2840 True   True   True     True   True  True    False
0x3dee9030 winlogon.exe            404 True   True   True     True   True  True    True
0x3da3ad40 audiodg.exe             920 True   True   True     True   True  True    True
0x3f4d0d40 SearchIndexer.         1124 True   True   True     True   True  True    False
0x3dabe478 svchost.exe            1316 True   True   True     True   True  True    False
0x3dd72d40 svchost.exe             572 True   True   True     True   True  True    False
0x3dd73030 yUmikJMYd3b.ex         1776 True   True   True     True   True  True    True
0x3df0aa58 csrss.exe               364 True   True   True     True   False True    False
0x3e9e7920 smss.exe                212 True   True   True     True   False False   False
0x3f774730 System                    4 True   True   True     True   False False   False
0x3dcdb920 csrss.exe               396 True   True   True     True   False True    True
0x3f484358                           0 False  False  False    False  False False   True
0x11bdaa40 ?                         0 False  False  False    False  False False   True
0x3e8ba4d0 taskeng.exe             856 False  True   False    False  False False   False    2015-10-21 13:59:23 UTC+0000
0x3f4a9030 WMIADAP.exe            1112 False  True   False    False  False False   False    2015-10-21 14:00:08 UTC+0000
```

Figura 10: Procesos ocultos

8.2.1.4.3 Hallazgos

Los 4 procesos ocultos (columna *pslist* a *false*) parecen legítimos del sistema operativo.

8.2.1.5 Proceso Skype.exe

8.2.1.5.1 Objetivo

Conocer con quién estaba en contacto el usuario del portátil intervenido por la policía y qué información intercambiada.

8.2.1.5.2 Procedimiento

Lo primero que se ha hecho por tanto es pasar a texto el volcado. Para ello se ha usado el comando *strings* de *Linux*:

```
root@kali:~/TFM# strings ANN-PC-20151021-135652.raw > ANN-PC-20151021-135652.txt
```

Figura 11: volcado de memoria en formato de texto

Una vez tengamos el volcado en el formato deseado, le pasamos el script *Skypeex*:

```
root@kali:~/TFM# python2.7 skypeex26.py
Enter the path to your 'Strings' file:ANN-PC-20151021-135652.txt
Extracting chat, please wait.....
Finding Skype sessions, please wait.....
All done.

Two files have been created for you.  Skypesessions.txt and skypechat.csv
```

Figura 12: salida del script Skypeex

Obtenemos 2 ficheros. Nos quedamos con el fichero *skypesessions.txt*, en el cual podemos ver las cabeceras de las conversaciones. En primer lugar aparece el usuario que inicia la comunicación. En segundo el usuario al que contacta:

```
annetom22 $live:rickyrodriguezgarcia 2cb6f5132b1d2b2aRicky RodriguezU
`live:rickyrodriguezgarcia
annetom22 $live:aram768 b30c0d15c933f134Aram B.V.U
live:aram768
```

Figura 13: cabeceras de conversaciones por Skype

No se ha podido obtener la hora de estas conversaciones, pero analizando el volcado de memoria en modo texto generado, se ha conseguido obtener la fecha del último acceso del usuario a Skype:

```
2015-10-21 13:55:20 SkypeAccess: (Manager) Account 'annetom22' logged in
C:\Users\Ann\AppData\Roaming\Skype\shared_dynco\dc.db-mjB39C1E974
```

Figura 14: último acceso a Skype del usuario annetom22

En el volcado de memoria se aprecian datos codificados o cifrados, por lo que no se ha podido obtener la información intercambiada por esta vía.

En el análisis del disco duro se analiza con más profundidad el contenido de las conversaciones.

8.2.1.5.3 Hallazgos

Se obtienen los siguientes hallazgos tras el análisis.

- El usuario de *Skype* *annetom22* ha establecido contacto con los usuarios *rickyrodriguezgarcia* y *aram768*.
- El usuario *annetom22* inició sesión en *Skype* por última vez el 21 de Octubre a las 13:55:20 horas.

Se adjunta copia del fichero con las cabeceras de las conversaciones (**evidencia A2** del Anexo).

8.2.1.6 Proceso yUmikJMYd3b.exe

8.2.1.6.1 Objetivo

Analizar el proceso para conocer si se trata de software malicioso.

8.2.1.6.2 Procedimiento

Para analizar el proceso se va a volcar su contenido a un fichero. Como precaución, antes de hacer el volcado del proceso nos aseguramos de tener un antivirus instalado en el equipo. En este caso, el analista dispone del antivirus *Trend Micro OfficeScan*.

Utilizamos la herramienta *volatility* a la cual le pasamos la imagen, el perfil, el comando *procdump*, el identificador del proceso y la ruta donde almacenará el fichero:

```
D:\TFM>volatility-2.5.standalone.exe -f ANN-PC-20151021-135652.raw --profile=Win7SP1x86 procdump -p 1776 -D D:\TFM
Volatility Foundation Volatility Framework 2.5
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x84b73030 0x00ac0000 yUmikJMYd3b.ex       OK: executable.1776.exe
```

Figura 15: volcado del proceso yUmikJMYd3b.exe a un fichero

Nada más generar el fichero, el Antivirus instalado en el equipo del analista lo detecta como malware de tipo troyano:

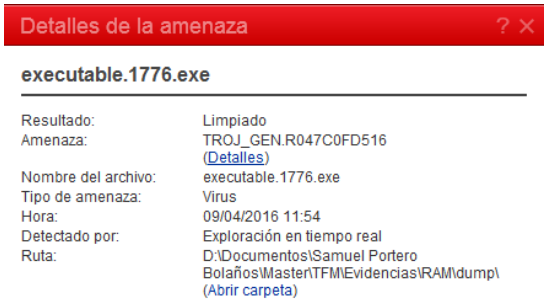


Figura 16: detección del proceso yUmikJMYd3b.exe como malware por el AV

Para asegurarnos de que no se trata de un falso positivo, subimos el fichero a la web *virustotal.com* [18], que ofrece un servicio de análisis de ficheros a través de 56 motores de antivirus de diferentes fabricantes.

Una vez subido el fichero, se ha comprobado que ha sido detectado como malware en 29 de los 56 motores de antivirus.

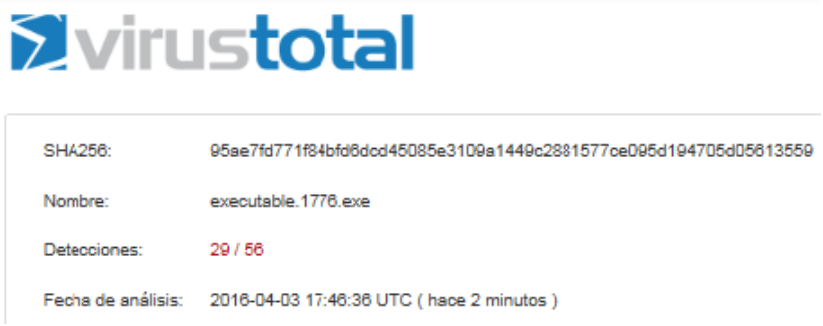


Figura 17: detección del proceso yUmikJMYd3b.exe como malware por VirusTotal

La mayoría de las firmas indican que se trata de un malware de tipo troyano. Este tipo de malware se hace pasar por otro programa, legítimo, pero en realidad ejecuta otra acción sin el consentimiento del usuario afectado.

A través de la web de *Virustotal* también podemos obtener el nombre real del ejecutable. En este caso ***TheJerm.exe***.

8.2.1.6.3 Hallazgos

Tras el análisis se encuentran los siguientes hallazgos:

- El proceso contiene un malware de tipo troyano.
- El nombre real del fichero es 'TheJerm.exe'.

Se adjunta copia del proceso con el troyano al informe. Se adjunta comprimido y con contraseña para evitar una posible infección accidental o la detección y borrado por sistemas antivirus de correos. Ver contraseña y datos del fichero en la **evidencia A3** del Anexo.

8.2.1.7 Proceso TrueCrypt.exe

8.2.1.7.1 Objetivo

Conocer si existe información cifrada en el disco duro y, en caso de existir, las claves utilizadas para dicho cifrado.

8.2.1.7.2 Procedimiento

Utilizamos la herramienta *volatility* a la cual le pasamos la imagen, el perfil y el comando *truecryptsummary* [19]:

```
D:\TFM>volatility-2.5.standalone.exe -f ANN-PC-20151021-135652.raw --profile=Win7SP1x86 truecryptsummary
Volatility Foundation Volatility Framework 2.5
Registry Version      TrueCrypt Version 7.1
Password              SafePlace at offset 0x8954bee4
Process               TrueCrypt.exe at 0x832c2938 pid 2244
Service               truecrypt state SERVICE_RUNNING
Kernel Module         truecrypt.sys at 0x89518000 - 0x8954f000
Symbolic Link         F: -> \Device\TrueCryptVolumeF mounted 2015-10-21 13:55:33 UTC+0000
Symbolic Link         F: -> \Device\TrueCryptVolumeF mounted 2015-10-21 13:55:33 UTC+0000
Symbolic Link         Volume{a5346c67-5247-11e5-bb74-0023543f71a3} -> \Device\TrueCryptVolumeF mounted 2015-10-21 13:55:33 UTC+0000
File Object           \Device\TrueCryptVolumeF\ at 0x3e652be0
File Object           \Device\TrueCryptVolumeF\ at 0x3f5785a0
Driver                \Driver\truecrypt at 0x3e9da030 range 0x89518000 - 0x8954ea00
Device                TrueCryptVolumeF at 0x833b3040 type FILE_DEVICE_DISK
Container             Path: \??\C:\Users\Ann\MyHome
Device                TrueCrypt at 0x83fdaf00 type FILE_DEVICE_UNKNOWN
```

Figura 18: volumen TrueCrypt y contraseña de cifrado

Podemos ver que el directorio cifrado y la contraseña que protege la clave de cifrado maestra. Esta clave la obtenemos con el siguiente comando:

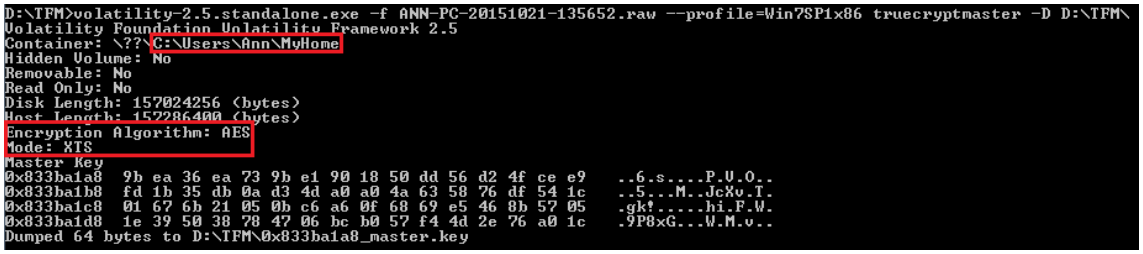


Figura 19: algoritmo y claves de cifrado TryeCrypt

8.2.1.7.3 Hallazgos

Tras el análisis obtenemos los siguientes hallazgos:

- El directorio cifrado es ***C\Users\Ann\MyHome***.
- Se ha usado un algoritmo ***AES*** y el modo ***XTS***.
- La *passphrase* es ***SafePlace***.

La información cifrada se analizará en el análisis del disco duro (apartado 8.2.3 del informe).

Se adjunta la clave de cifrado maestra al informe (**evidencia A4** del Anexo).

8.2.1.8 Proceso notepad.exe

8.2.1.8.1 Objetivo

Hemos visto en el punto 8.2.1.3 que el proceso *Notepad.exe* es lanzado por el proceso *yUmikJMYd3b.exe*, por lo que vamos a analizar si el editor de texto tiene algún fichero abierto con información de interés.

8.2.1.8.2 Procedimiento

Para mostrar y guardar todos los ficheros abiertos por el proceso, utilizamos la herramienta *volatility* a la cual le pasamos como parámetros la imagen, el perfil, el comando *dumpfiles*, la ruta donde almacenará el fichero, el identificador del proceso y un fichero donde guardará un resumen de los resultados obtenidos:

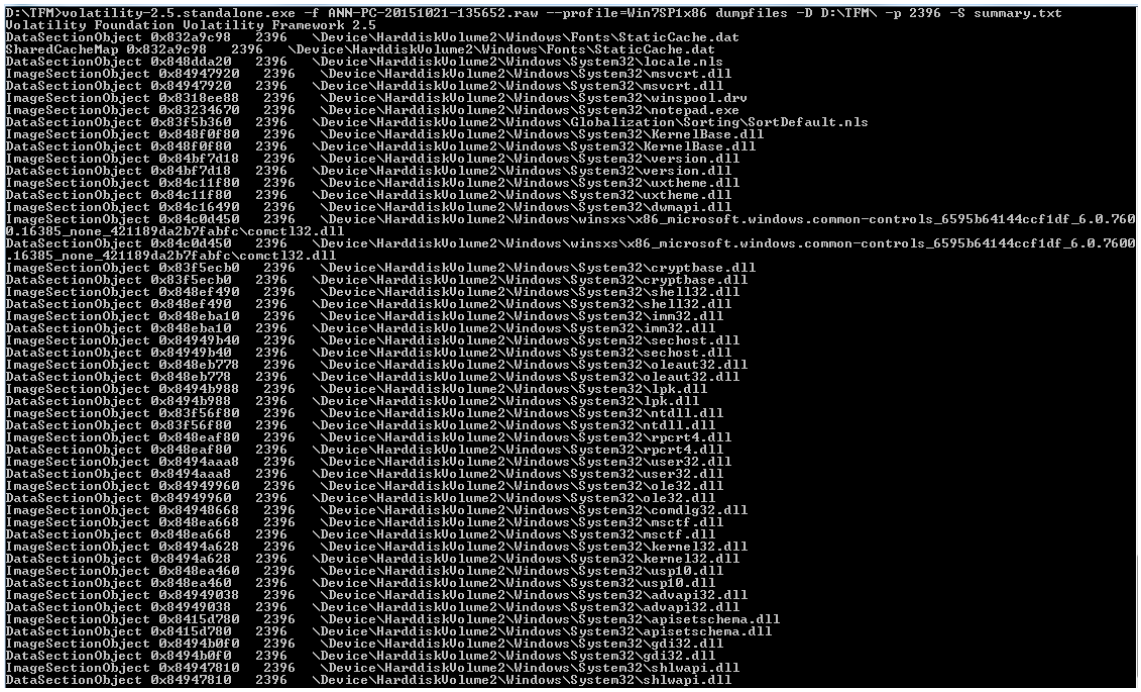


Figura 20: volcado del proceso Notepad.exe

8.2.1.8.3 Hallazgos

No se observa ningún fichero de texto abierto. Tan sólo se aprecian librerías del sistema operativo. No se encuentran evidencias destacables en este análisis.

8.2.1.9 Conexiones de red

8.2.1.9.1 Objetivo

Conocer las conexiones establecidas por el usuario en el momento de la intervención policial en el domicilio.

8.2.1.9.2 Procedimiento

Para sacar las conexiones de red, usamos la herramienta *volatility* con los parámetros habituales y el comando *netscan*:

```
volatility-2.5.standalone.exe -f ANN-PC-20151021-135652.raw --profile=Win7SP1x86 netscan
```

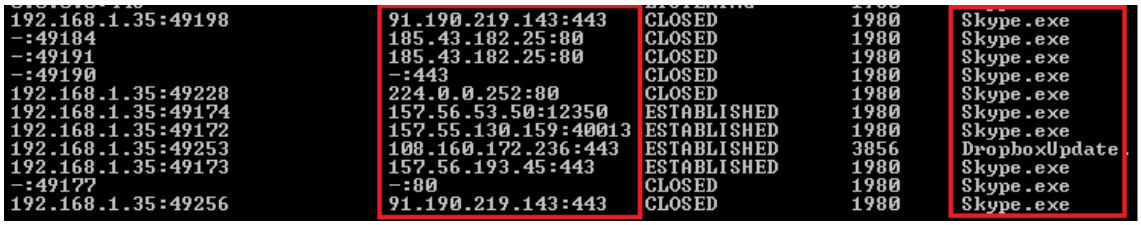


Figura 21: listado de conexiones de red

Vemos que existen 5 conexiones recientes pero cerradas, todas del proceso *Skype.exe*. Y 4 conexiones establecidas y activas, 3 de *Skype* y 1 del proceso de actualización de *Dropbox*.

Para ver la ubicación de estas IPs y si se tratan de servicios legítimos de los procesos implicados, usamos un servicio de *whois* [20]. Por ejemplo, si buscamos la IP 91.190.219.143 vemos que pertenece a *Skype DU* y está localizada en Irlanda (***ie***):

```
inetnum:        91.190.219.0 - 91.190.219.255
netname:        SKYPE-DU5
descr:          Skype Du
country:        ie
admin-c:        SN3357-RIPE
tech-c:         SN3357-RIPE
status:         ASSIGNED PA
mnt-by:         TT61201-MNT
created:        2013-04-26T13:02:37Z
last-modified:  2013-04-26T13:02:37Z
source:         RIPE

role:           Skype Noc
address:        23-29 Rives de Clausen L-2165 Luxembourg
abuse-mailbox:  noc@skype.net
admin-c:        TT3113-RIPE
tech-c:         TT3113-RIPE
nic-hdl:        SN3357-RIPE
mnt-by:         TT61201-MNT
created:        2011-08-10T10:48:16Z
last-modified:  2013-04-26T13:14:23Z
source:         RIPE # Filtered

% Information related to '91.190.218.0/23AS198097'

route:          91.190.218.0/23
descr:          Skype
origin:         AS198097
mnt-by:         TT61201-MNT
created:        2013-04-26T13:04:50Z
```

Figura 22: whois IP de Skype

8.2.1.9.3 Hallazgos

Repetimos la búsqueda del resto de IPs y determinamos que el equipo ha establecido las siguientes comunicaciones:

Dirección IP remota	Puerto/Protocolo	Proceso	Propietario IP	Ubicación IP
91.190.219.143	443/TCP	Skype.exe	Skype Du	Irlanda
185.43.182.25	80/TCP	Skype.exe	Telefónica	España
224.0.0.252	80/TCP	Skype.exe	N/D	N/D
157.56.53.50	12350/TCP	Skype.exe	Microsoft Corp	Redmond, EEUU
157.55.130.159	40013/TCP	Skype.exe	Microsoft Corp	Redmond, EEUU
157.56.193.45	443/TCP	Skype.exe	Microsoft Corp	Redmond, EEUU
108.160.172.236	443/TCP	DropboxUpdate.exe	Dropbox, Inc	San Francisco, EEUU

Figura 23: información sobre IPs contactadas

No se aprecia ninguna conexión sospechosa relacionada con páginas fraudulentas.

Se adjunta fichero de conexiones por si pudiera relacionarse con alguna evidencia más adelante (**evidencia A5** del Anexo).

* La IP 224.0.0.252 es una IP utilizada en el protocolo multicast y puede ser utilizada por cualquier organización o individuo, por lo que no tiene propietario ni ubicación fija.

8.2.1.10Usuarios

8.2.1.10.1 Objetivo

Sacar un listado de todos los usuarios creados en el sistema operativo y, si es posible, sus contraseñas.

8.2.1.10.2 Procedimiento

Usando la herramienta *volatility* con los parámetros de la imagen, el perfil y el comando *hashdump* sacamos todos los usuarios junto con el *hash* de sus contraseñas:

```
D:\TFM>volatility-2.5.standalone.exe -f ANN-PC-20151021-135652.raw --profile=Win7SP1x86 hashdump
Volatility Foundation Volatility Framework 2.5
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Ann:1000:aad3b435b51404eeaad3b435b51404ee:8a24d5beb0d94c03ffec1e186a1f88b0:::
Tom:1001:aad3b435b51404eeaad3b435b51404ee:35509e7f0e2d9b0b7f60c40b37a1f559:::
```

Figura 24: usuarios y sus hashes con volatility

Para averiguar las contraseñas de los 4 usuarios del SO, usaremos la herramienta *John the ripper* incluida en la herramienta *Kali Linux 2.0*.

Lanzamos el comando *john* al que le pasamos un fichero con el los usuarios y hashes (los que están dentro de cuadrado rojo de la imagen anterior), y con el parámetro *--format=nt2*:

```
sudo ./john hashdump.txt --format=nt2
```

```
Loaded 4 password hashes with no different salts (NT MD4 [128/128 SSE2 intrinsics 12x])
                 (Administrador)
                 (Invitado)
Ann1978          (Tom)
Tom1980          (Ann)
guesses: 4  time: 0:00:16:28 DONE (Sat Apr  9 22:24:10 2016)  c/s: 41936K  trying: Tom1911 - Tom198x
Use the "--show" option to display all of the cracked passwords reliably
```

Figura 25: usuarios y contraseñas con volatility y John the ripper

8.2.1.10.3 Hallazgos

Existen 4 usuarios en el sistema operativo, con las siguientes contraseñas:

Usuario	Contraseña
Administrador	
Invitado	
Ann	Ann1978
Tom	Tom1980

Figura 26: tabla con usuarios y contraseñas obtenidos con volatility

Se adjunta ficheros con los usuarios y sus hashes así como el fichero con el resultado de la ejecución del comando 'john' (**evidencias A6 y A7** del Anexo).

8.2.1.11Sesiones de usuarios

8.2.1.11.1 Objetivo

De los usuarios encontrados, comprobar cual o cuales (podría haber alguno conectado en remoto) están logados en el sistema en el momento de realizar el volcado.

8.2.1.11.2 Procedimiento

Hacemos uso de la herramienta *volatility* con la imagen de la memoria, el perfil y el comando *sessions*.

```
D:\TFM>volatility-2.5.standalone.exe -f ANN-PC-20151021-135652.raw --profile=Win7SP1x86 sessions
Volatility Foundation Volatility Framework 2.5
**************************************************
Session(V): 89e68000 ID: 0 Processes: 26
PagedPoolStart: 80000000 PagedPoolEnd ffbfffff
 Process: 296 csrss.exe 2015-10-21 13:53:02 UTC+0000
 Process: 352 wininit.exe 2015-10-21 13:53:04 UTC+0000
 Process: 440 services.exe 2015-10-21 13:53:07 UTC+0000
 Process: 456 lsass.exe 2015-10-21 13:53:07 UTC+0000
 Process: 464 lsm.exe 2015-10-21 13:53:07 UTC+0000
 Process: 572 svchost.exe 2015-10-21 13:53:08 UTC+0000
 Process: 636 svchost.exe 2015-10-21 13:53:09 UTC+0000
 Process: 684 svchost.exe 2015-10-21 13:53:09 UTC+0000
 Process: 812 svchost.exe 2015-10-21 13:53:10 UTC+0000
 Process: 860 svchost.exe 2015-10-21 13:53:11 UTC+0000
 Process: 920 audiodg.exe 2015-10-21 13:53:11 UTC+0000
 Process: 1004 svchost.exe 2015-10-21 13:53:12 UTC+0000
 Process: 1176 svchost.exe 2015-10-21 13:53:13 UTC+0000
 Process: 1280 spoolsv.exe 2015-10-21 13:53:15 UTC+0000
 Process: 1316 svchost.exe 2015-10-21 13:53:15 UTC+0000
 Process: 1400 svchost.exe 2015-10-21 13:53:16 UTC+0000
 Process: 1120 sppsvc.exe 2015-10-21 13:54:22 UTC+0000
 Process: 1124 SearchIndexer. 2015-10-21 13:54:39 UTC+0000
 Process: 964 wmpnetwk.exe 2015-10-21 13:54:44 UTC+0000
 Process: 2840 svchost.exe 2015-10-21 13:55:20 UTC+0000
 Process: 1484 WUDFHost.exe 2015-10-21 13:56:44 UTC+0000
 Process: 2252 WmiPrvSE.exe 2015-10-21 13:57:18 UTC+0000
 Process: 2688 taskeng.exe 2015-10-21 14:00:00 UTC+0000
 Process: 3644 DropboxUpdate. 2015-10-21 14:00:00 UTC+0000
 Process: 3744 DropboxUpdate. 2015-10-21 14:00:00 UTC+0000
 Process: 3856 DropboxUpdate. 2015-10-21 14:00:03 UTC+0000
 Image: 0x83f132b0, Address 8c450000, Name: win32k.sys
 Image: 0x84949ae8, Address 8c6a0000, Name: dxg.sys
 Image: 0x849bac88, Address 8c6d0000, Name: TSDDD.dll
**************************************************
Session(V): 89e70000 ID: 1 Processes: 14
PagedPoolStart: 80000000 PagedPoolEnd ffbfffff
 Process: 364 csrss.exe 2015-10-21 13:53:04 UTC+0000
 Process: 404 winlogon.exe 2015-10-21 13:53:07 UTC+0000
 Process: 368 taskhost.exe 2015-10-21 13:54:21 UTC+0000
 Process: 552 dwm.exe 2015-10-21 13:54:30 UTC+0000
 Process: 692 explorer.exe 2015-10-21 13:54:30 UTC+0000
 Process: 1980 Skype.exe 2015-10-21 13:54:32 UTC+0000
 Process: 1776 yUmikJMYd3b.ex 2015-10-21 13:54:32 UTC+0000
 Process: 512 WinHex.exe 2015-10-21 13:54:46 UTC+0000
 Process: 2244 TrueCrypt.exe 2015-10-21 13:55:00 UTC+0000
 Process: 2336 svchost.exe 2015-10-21 13:55:06 UTC+0000
 Process: 2396 notepad.exe 2015-10-21 13:55:07 UTC+0000
 Process: 2948 DumpIt.exe 2015-10-21 13:56:51 UTC+0000
 Process: 2668 conhost.exe 2015-10-21 13:56:52 UTC+0000
 Process: 1456 slui.exe 2015-10-21 13:59:27 UTC+0000
 Image: 0x843bc120, Address 8c450000, Name: win32k.sys
 Image: 0x848da140, Address 8c6a0000, Name: dxg.sys
 Image: 0x848365d8, Address 8c750000, Name: framebuf.dll
```

Figura 27: sesiones de usuarios activos con volatility

Obtenemos solamente 2 sesiones:

- ID 0: Sesión del propio sistema operativo. En esta sesión aislada se ejecutan solamente los servicios del sistema.
- ID 1: Sesión de usuario. Este usuario es el que está ejecutando todos los procesos estudiados anteriormente, incluyendo el malware.

Por lo tanto, sólo existe un usuario logado. Para conocer qué usuario es el que tiene la sesión activa, usamos la herramienta *volatility* con los parámetros habituales, el comando *getsids* [21] y los identificadores de los procesos (*pid*) que queramos saber quién los está ejecutando:

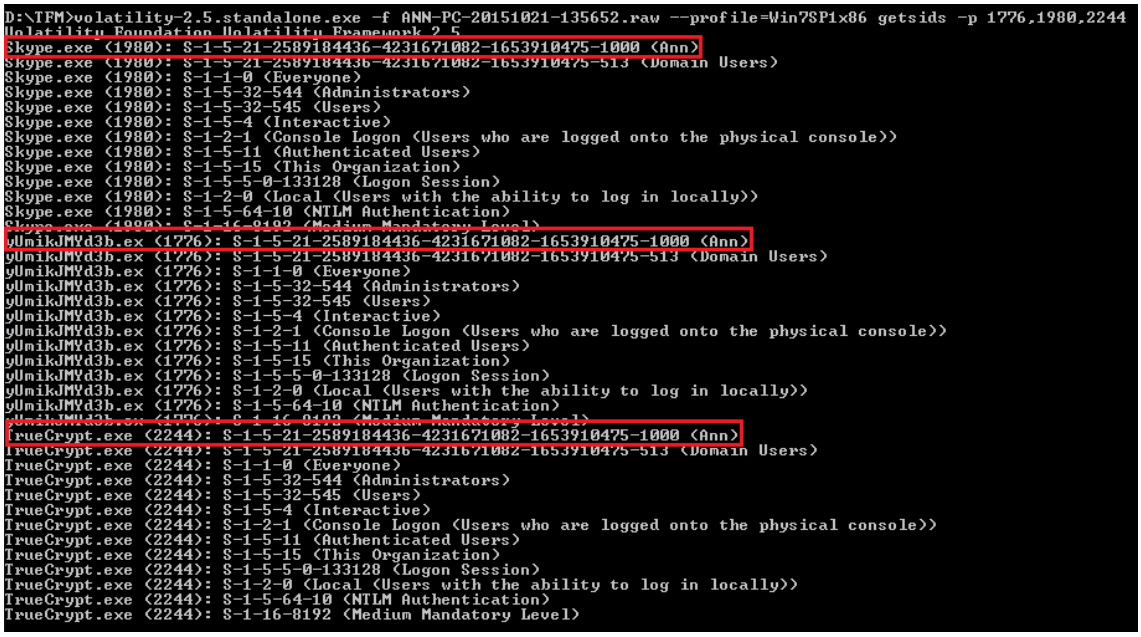


Figura 28: uid del usuario logado en el sistema

Vemos que en todos los procesos, el usuario que los ejecuta es *Ann*.

8.2.1.11.3 Hallazgos

Tras el análisis, se encuentran los siguientes hallazgos:

- **Solo hay una sesión de usuario activa** en el equipo en el momento del registro.
- El usuario logado en el sistema es ***Ann***.

Se adjuntan ficheros con las sesiones de usuarios (**evidencias A8 y A9** del Anexo).

8.2.1.12Consolas

8.2.1.12.1 Objetivo

Conocer si el usuario ha ejecutado algún comando en la consola del sistema, ya sea de manera voluntaria o involuntaria, debido por ejemplo a algún tipo de malware.

8.2.1.12.2 Procedimiento

Haciendo uso de la herramienta *volatility* con los comandos habituales y los comandos *consoles* y *cmdscan*:

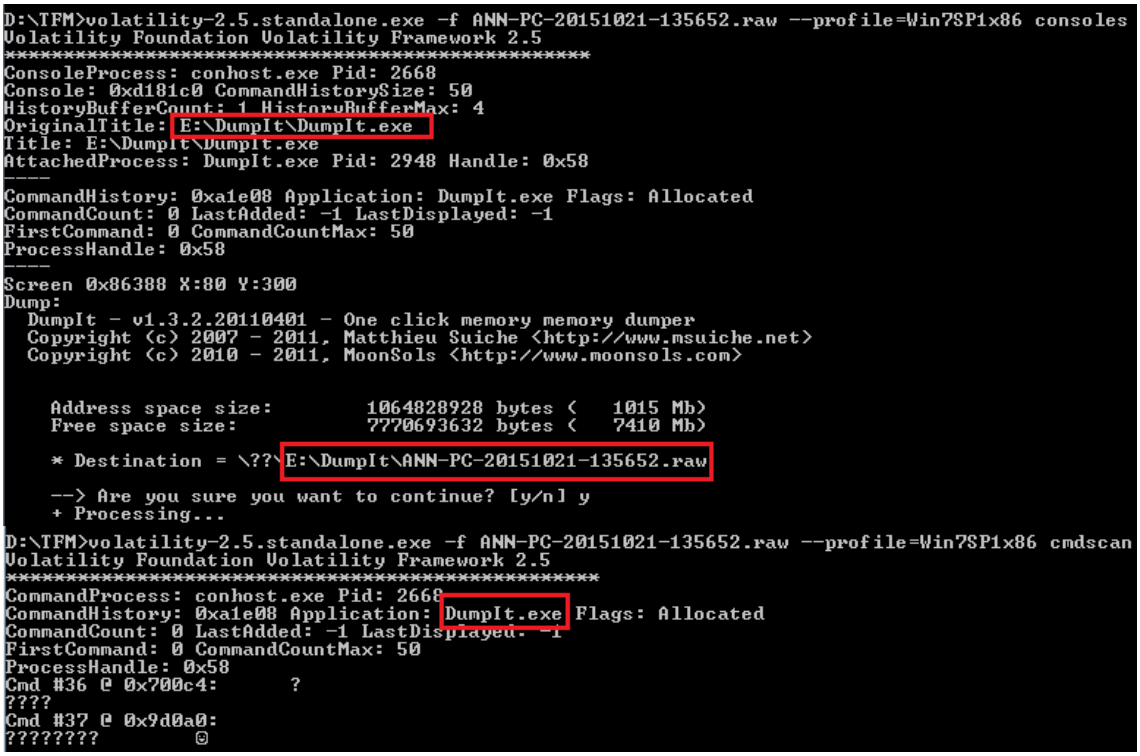


Figura 29: comandos lanzados por consola

Vemos que los únicos comandos ejecutados por consola han sido los relacionados con el proceso *DumpIt.exe*, es decir, aquellos realizados por el experto para la extracción del volcado de memoria.

8.2.1.12.3 Hallazgos

No he ha encontrado nada que ayude a la aclaración de los extremos planteados.

8.2.2 Análisis del dispositivo USB

Como se indicó anteriormente, para el análisis del dispositivo USB se utilizará la herramienta forense *Autopsy 4.0*.

8.2.2.1 Prerrequisitos: Nuevo Caso

8.2.2.1.1 Objetivo

Configurar la herramienta *Autopsy* para poder analizar la evidencia de la imagen del dispositivo *USB* recibida.

8.2.2.1.2 Procedimiento

Para configurar la herramienta lo primero que hacemos es crear un nuevo caso en *Autopsy*. Abrimos el programa y seleccionamos *New Case*. Rellenamos la información que nos va solicitando el programa. Seleccionamos como evidencia la imagen del dispositivo *USB* recibida.

8.2.2.2 Búsqueda de ficheros

8.2.2.2.1 Objetivo

Buscar en el contenido de la imagen ficheros que puedan responder a los extremos planteados en el apartado 3 del informe.

8.2.2.2.2 Procedimiento

En el menú de la izquierda de la herramienta *Autopsy*, pulsamos sobre el dispositivo *USB.E01* para ver los ficheros disponibles en la raíz:

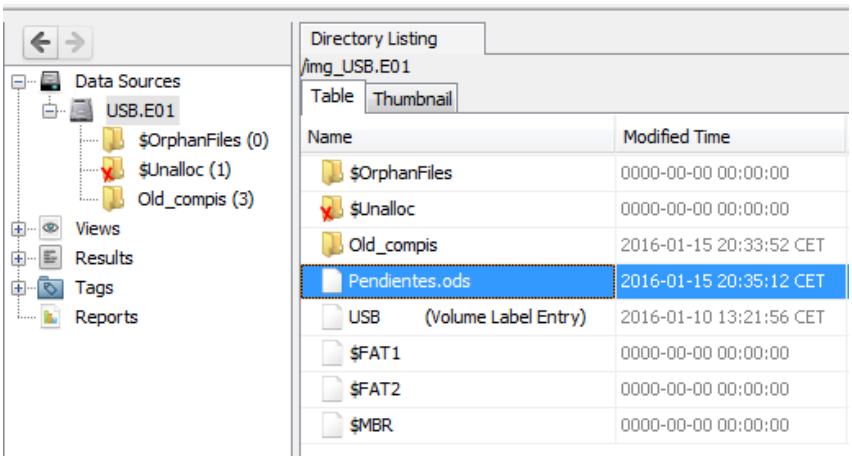


Figura 30: ficheros en el raíz del dispositivo USB

Se encuentra un documento *Pendientes.ods* y un directorio *Old_compis*. Dentro del directorio se encuentra el fichero *WhatsApp.db*:

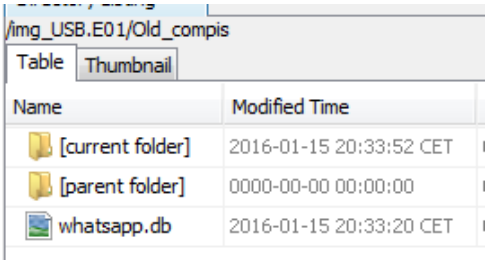


Figura 31: ficheros en el directorio Old_compis del dispositvo USBN

Extraemos ambos ficheros para su posterior análisis pulsando sobre ellos y seleccionando la opción *Extract Files*.

8.2.2.2.3 Hallazgos

Tras el análisis de los ficheros del dispositivo, se encuentra lo siguiente:

- Fichero de hoja de cálculos llamado ***pendientes.ods***.
- Fichero de base de datos ***WhatsApp.db***.

Estos ficheros serán analizados en los siguientes apartados.

8.2.2.3 Fichero pendientes.ods

8.2.2.3.1 Objetivo

Analizar la información contenida en el fichero en busca de respuestas a los extremos planteados.

8.2.2.3.2 Procedimiento

El fichero tiene un formato *ods* (*Open Document SpreadSheet*), formato abierto de hojas de cálculo. Es posible abrir dichos ficheros con el programa *Microsoft Excel 2013*, instalado en el equipo del perito. Si lo abrimos encontramos información sobre lo que parecen ser tarjetas de crédito (tipo, número y propietario). A continuación se muestra un extracto:

Visa	4539456154526870	Concepcion	Perez Pozo
Visa	4532457001051150	Jose Maria	Rodriguez Martinez
Visa	4532657981372410	Ignacio	Torres Fernandez

Figura 32: extracto de información encontrada en el fichero pendientes.ods

Se ha utilizado la herramienta *Foca Free 3.2* para extraer los metadatos del documento, obteniendo la siguiente información oculta:

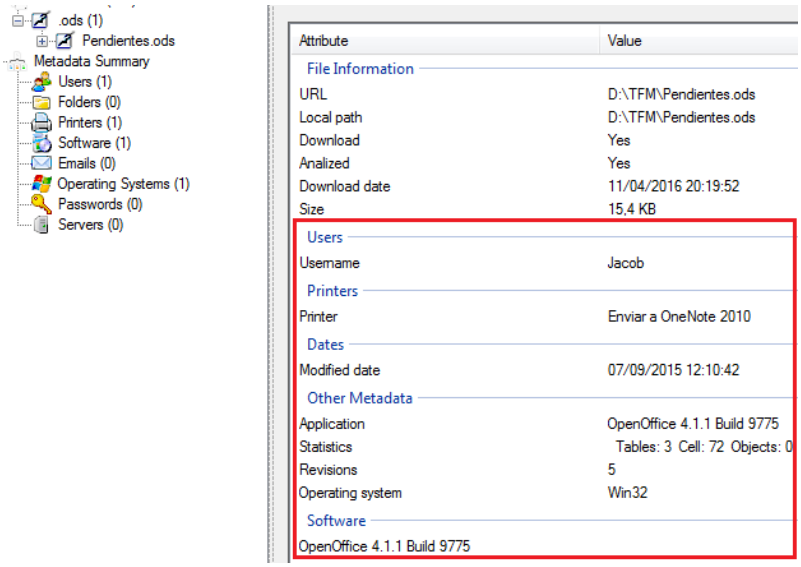


Figura 33: metadatos del fichero pendientes.ods

8.2.2.3.3 Hallazgos

Tras el análisis del fichero, encontramos los siguientes hallazgos:

- Listado de lo que parecen ser números de tarjetas de crédito con los nombres de los propietarios.
- El fichero ha sido creado desde una cuenta de usuario llamada *Jacob*, en un sistema *Windows de 32 bits*, con un procesador de textos *OpenOffice 4.1.1* y la última modificación ha sido realizada el 07/09/2015.

Se adjunta fichero *Pendientes.ods* con todos los números de tarjetas de crédito (**evidencia B1** del Anexo).

8.2.2.4 Fichero WhatsApp.db

8.2.2.4.1 Objetivo

Analizar las conversaciones incluidas en el fichero de base de datos.

8.2.2.4.2 Procedimiento

Abrimos el navegador *Firefox* y en la barra de herramientas seleccionamos el complemento *SQLite Manager*. Desde este complemento abrimos el fichero *WhatsApp.db* y si nos vamos a la tabla *messages* nos encontramos con lo siguiente:

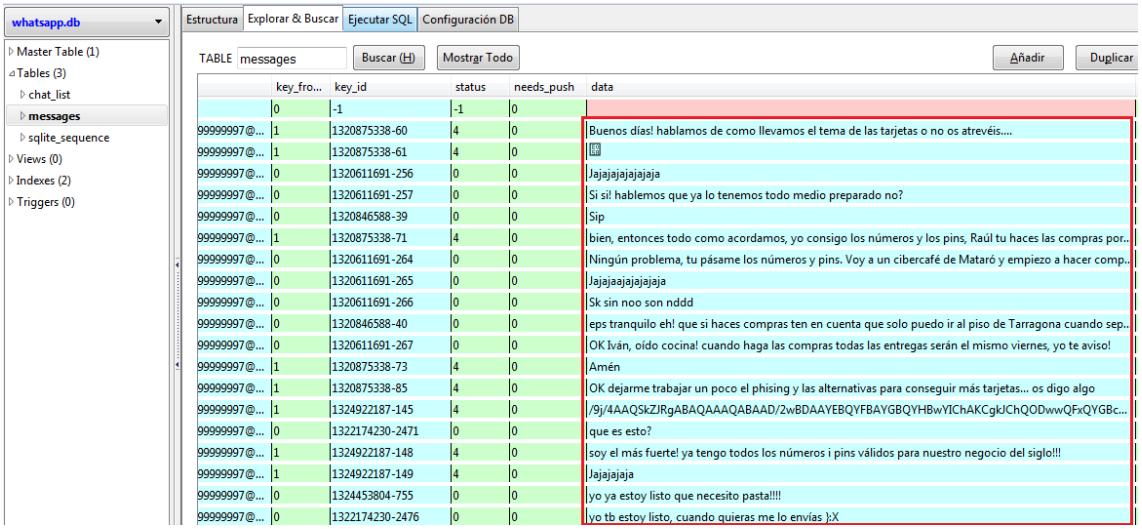


Figura 34: extracto de conversación de WhatsApp

Se aprecia lo que parece ser una conversación de la aplicación de mensajería *WhatsApp* entre varias personas (grupo).

Para extraer la máxima información de la BBDD, necesitamos conocer la estructura de la misma [22]. En la tabla *chat_list* podemos ver todas las conversaciones que ha tenido el usuario. En este caso, 4:

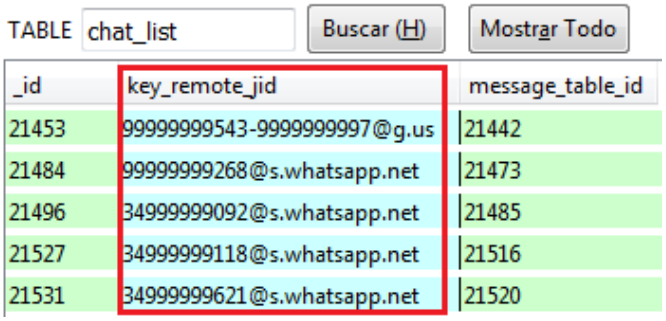


Figura 35: número de conversaciones mantenidas por WhatsApp

Cada una de estas conversaciones puede verse en la tabla *messages*, y se diferencian por la columna *key_remote_jid*. En la siguiente imagen vemos las 5 conversaciones diferentes que se mantuvieron:

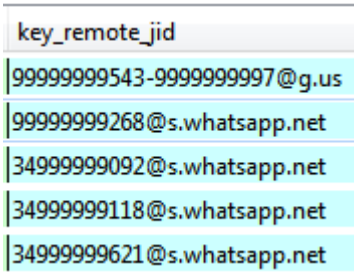


Figura 36: identificar mensajes enviados por el usuario

Los mensajes enviados por el usuario de *WhatsApp* del dispositivo donde se ha extraído la BBDD se identifican con el parámetro '1' en la columna *key_from_me*.

Dentro de las conversaciones de grupo, los mensajes enviados por los demás participantes de identifican por la columna *remote_resource*.

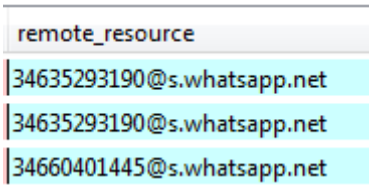


Figura 37: identificar mensajes enviados por los otros participantes

Y la hora y fecha de envío se almacenan en formato *Unix epoch* en milisegundos en la columna *timestamp*.

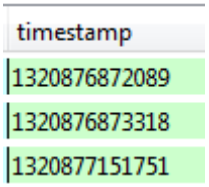


Figura 38: identificar fecha y hora del envío de los mensajes

También existen campos con coordenadas para la geolocalización del usuario que envía el mensaje, pero su contenido está a 0 en todos los mensajes. Por lo tanto lo más probable es que tuvieran desactivado el GPS.

Con toda esta información, se ha creado una tabla con la información más importante de las conversaciones. Se ha asignado un color a los mensajes de cada usuario. Las filas en blanco corresponden a mensajes que no han podido ser identificados, al estar el campo *remote_resource* vacío. A continuación se muestra un extracto de la tabla (en el Anexo se muestra completa):

key_remote_jid	data	remote_resource	timestamp	
99999999543-9999999997@g.us	Buenos días! hablamos de como llevamos el tema de las tarjetas o no os atrevéis....		09/11/2011	23:10:25
99999999543-9999999997@g.us	?		09/11/2011	23:14:09
99999999543-9999999997@g.us	Jajajajajajajaja	34635293190@s.*WhatsApp*.net	09/11/2011	23:14:32
99999999543-9999999997@g.us	Si si! hablemos que ya lo tenemos todo medio preparado no?	34635293190@s.*WhatsApp*.net	09/11/2011	23:14:33
99999999543-9999999997@g.us	Sip	34660401445@s.*WhatsApp*.net	09/11/2011	23:19:12
99999999543-9999999997@g.us	bien, entonces todo como acordamos, yo consigo los números y los pins, Raúl tu haces las compras por internet y Iván te enviamos la mercancía al piso falso de Tarragona con el dni falso que tienes. Hasta aquí todo claro como siempre..."		09/11/2011	23:20:06
99999999543-9999999997@g.us	Ningún problema, tu pásame los números y pins. Voy a un cibercafé de Mataró y empiezo a hacer compras a saco!!!	34635293190@s.*WhatsApp*.net	09/11/2011	23:20:09
99999999543-9999999997@g.us	Jajajaajajajajaja	34635293190@s.*WhatsApp*.net	09/11/2011	23:20:17
99999999543-9999999997@g.us	Sk sin noo son nddd	34635293190@s.*WhatsApp*.net	09/11/2011	23:20:23
99999999543-9999999997@g.us	eps tranquilo eh! que si haces compras ten en cuenta que solo puedo ir al piso de Tarragona cuando sepa que los propietarios no son! así que las entregas solo pueden ser los viernes por la mañana!! o la liamos..."	34660401445@s.*WhatsApp*.net	09/11/2011	23:20:32
99999999543-9999999997@g.us	OK Iván, oído cocina! cuando haga las compras todas las entregas serán el mismo viernes, yo te aviso!	34635293190@s.*WhatsApp*.net	09/11/2011	23:20:34
99999999543-9999999997@g.us	Amén		09/11/2011	23:23:55
99999999543-9999999997@g.us	OK dejarme trabajar un poco el phising y las alternativas para conseguir más tarjetas... os digo algo		09/11/2011	23:27:10
99999999543-9999999997@g.us	/9j/4AAQSkZJRgABAQAAAQABAAD/2wBDAAYEBQYFBAYGBQYHBwYIChAKCgkJChQODwwQFxQYGBcUFhYaHSUfGhsjHBYWICwgIyYnKSopGR8tMC0oMCUoKSj/2wBDAQcHBwoIChMKChMoGhYaKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCj/wAARCABkAEgDASIAAhEBAxEB/8QAHwAAAQUBAQEBAQEAAAAAAAAAAAECAwQFBgcICQoL/8QAtRAAAgEDAwIEAwUFBAQAAAF9AQIDAAQRBRIhMUEGE1FhByJxFDKBkaEII0KxwRVS0fAkM2JyggkKFhcYGRolJicoKSo0NTY3ODk6Q0RFRkdISUpTVFVWV1hZWmNkZWZnaGlqc3R1dnd4eXqDhIWGh4iJipKTlJWWl5iZmqKjpKWmp6ipqrKztLW2t7i5usLDxMXGx8jJytLT1NXW19jZ2uHi4+Tl5ufo6erx8vP09fb3+Pn6/8QAHwEAAwEBAQEBAQEBAQAAAAAAAAECAwQFBgcICQoL/8QAtREAAgECBAQDBAcFBAQAAQJ3AAECAxEEBSExBhJBUQdhcRMiMoEIFEKRobHBCSMzUvAVYnLRChYkNOEI8RcYGRomJygpKjU2		26/12/2011	0:20:57

	Nzg5OkNERUZHSElKU1RVVldYWVpjZGVmZ2hpanN0dXZ3eHl6goOEhYaHilmKkpOUlZaXmJmaoqOkpaanqKmqsrO0tba3uLm6wsPExcbHyMnK0tPU1dbX2Nna4uPk5ebn6Onq8vP09fb3+Pn6/9oADAMBAAIRAxEAPwD6ZsQDZQHHWNf5VPtHoKg0/wD48Lb/AK5L/KrFQIbtHpRtHpQxwpNcrdeILqKZ41jDbDjOQM/pUTmoasaV9jqwB6UuB6VxJ8WT+d5OIhNt3bPMG7HrjHSnReLJpC6qqMyHawVwdp64PHBxUe3h3DlZ2RjQ9VU/hTflhPWJP++RWRourS385Vl2KvXoc8H2rcFaRkpK6EQm0tyOYIv++BRU/aiqAq6d/wAg+2/65L/Kp6h0/wD48bf/AK5r/Kp6AGv90/SvOr9n+3T7WTG7oa9Ff7przbUQjXdypzyxBrnxCvFFQdmcTcawh8TmSJ1WRJVspAwHBYMwYH6Adu9bem27W95fvFcxO9w4dAUC+pPTr1rj9d06c6le+U0dvFFMkglLcE7Dtzu4yOP++selang+8F7f3EzZdTErk9gxJ6ZOR0PGO3PNc04qKVioycr3VrHpngN53kkF15fmDbkpnGcHOM9q7cdK43wSVM8pUY5H8jXZCuyj8BD3FPSijtRWoivY/wDHlB/1zX+VTGobL/jzg/65r/KpqAGt9015bqv2hdVuglJSu/lYIcGvUj901kNBIBnY35VnOPMrAeQ6mtxFdPINPuZoHIeRoiVcMBgYHcYx+tYOkrrllqt20WmTG1uCNhkkICAFu3JHXpXuzwyAEEP/AN8k1E0bAcpIT/uGs1Tt0G22rXMb4cvK01wJo3T5hjcMdjXf1iaUjLdL8rAcnlSO1bg6VrBWQkrCdqKXtRVgV7P/AI9IP9xf5VLUVp/x6w/7g/lUtACV49478X+JNJ8QzW9peCO1YN5SrAmRxxywPU+vUg8YxXsPavmj4oavMviaOGQBpRJMiyFTkIW+X2wCpx+P0pdRPYl8OfFbxTdausN1qUJt8ksz28SgjPrle3PfrivXF8XyzIYrJ4Zpd5UyMhwp9No5zXynCjxzPEkXmsSD97GFyOefoO1blteXNlYl3uyDkCOJfm5zxz25GfpTavsZxk47n1bp+sFpI4LqaA3DOEKhShJwDwCeev8AStwHivnn4X3CTeJNK/0qR7jf+9D4LM205yfqK+hhURNb3Foo7GirAr2n/HrD/uD+VS1FZ/8AHpD/ALi/yqWgBD0r5I+JcuuPf3Ul8skkEV0RAMAll3swGe3G73r63PQ18wfEOeaOHVTBIrtvKhI0B25bng8nrWc3ZouEU73MnS73TJNNb7XY25lDExnZ+8I9GYdeQf0rEh0G51bXZ7WWExxWar5kMhIRWbOApPJ4BwT9a5S8mc3MBKfLEqkk5xHnn+ZNeknWr652GWFY3U5LYycEdMHrz7e2TUcrp633NueNW0eXY7n4Z6I9r4nsp5IYo9rk8Nyx6Zx9M172OleB/DnVLmXxPplu27ymk5l4B+UnoK98HSnRd0zOsknoL2oo7UVsZFey/wCPOD/cX+VNQAh6GvmDW4o5NUvVlt/keR9xKHpk8cV9PkcV51qPw1+13U8o1DKyOXAZMEZ7cH/PtWNWMpW5TWlJRvc+dtRsvOXXZFVSzPEQGyMFcMeT/vGupjjRFXcPv8bSvAPPOa9MufhLIhVb2EknJZgwJ98jnPTmi3+FN3EpH9pQFQMKuw4HX1z7fl+WMoTfQ3jUiupzvgAGPxfpaqglMhywPGMHpXvg6V574a+H9xperW15cXsUghcviNSM9cDn/AD/KvQxW1GLjGzMa0lJ6B2oo7UVsYle0P+iw/wC4v8qmzRRQACiiigBc0UUUAFHaiigAz1oooAKKKKAP/9k=				
99999999543-9999999997@g.us	que es esto?	34635293190@s.*WhatsApp*.net	26/12/2011	0:23:06
99999999543-9999999997@g.us	soy el más fuerte! ya tengo todos los números i pins válidos para nuestro negocio del siglo!!!		26/12/2011	0:23:40
99999999543-9999999997@g.us	Jajajajaja		26/12/2011	0:23:43
99999999543-9999999997@g.us	yo ya estoy listo que necesito pasta!!!!	34660401445@s.*WhatsApp*.net	26/12/2011	0:23:54
99999999543-9999999997@g.us	yo tb estoy listo, cuando quieras me lo envías }:X	34635293190@s.*WhatsApp*.net	26/12/2011	0:23:56
99999999543-9999999997@g.us	además soy un crack, porqué lo tengo todo escondido en mi ordenador, no me lo encontraría ni la poli ;p		26/12/2011	0:32:22
99999999543-9999999997@g.us	somos unos profesionales! mira que es fácil hacer pasta.... vivan los sobresueldos!		26/12/2011	0:32:28
99999999543-9999999997@g.us	Jajajaja		26/12/2011	0:32:30
99999999543-9999999997@g.us	contigo estamos tranquilos, eres un crack!	34660401445@s.*WhatsApp*.net	26/12/2011	0:33:08
99999999543-	eres la ...	34635293190@s.*WhatsApp*.net	26/12/2011	0:34:15

9999999997@g.us				
99999999543-9999999997@g.us	□	34635293190@s.*WhatsApp*.net	26/12/2011	0:34:43
99999999543-9999999997@g.us	Jajajjaajaja	34635293190@s.*WhatsApp*.net	26/12/2011	0:34:48
99999999543-9999999997@g.us	Raúl ya lo tienes en el correo, el pwd del zip es somosunoscracks... coordínate con Iván y hablamos de repartir...		27/12/2011	10:21:56
99999999543-9999999997@g.us	OK	34635293190@s.*WhatsApp*.net	27/12/2011	10:22:28
99999999268@s.*WhatsApp*.net	Feliz sanvalentin□		14/02/2012	20:56:44
99999999268@s.*WhatsApp*.net	Q ironia		14/02/2012	21:03:18

Figura 39: extracto de conversaciones por WhatsApp

Se puede apreciar que hay una fila en la que el campo *data* no es legible. Esto es debido a que se trata de una imagen y su contenido está codificado en base 64. Podemos ver el contenido de la imagen en un navegador si construimos una URL, anteponiéndole *data:image/png;base64*, al código en base 64 del campo data y pegando el resultado en la barra de direcciones del navegador:

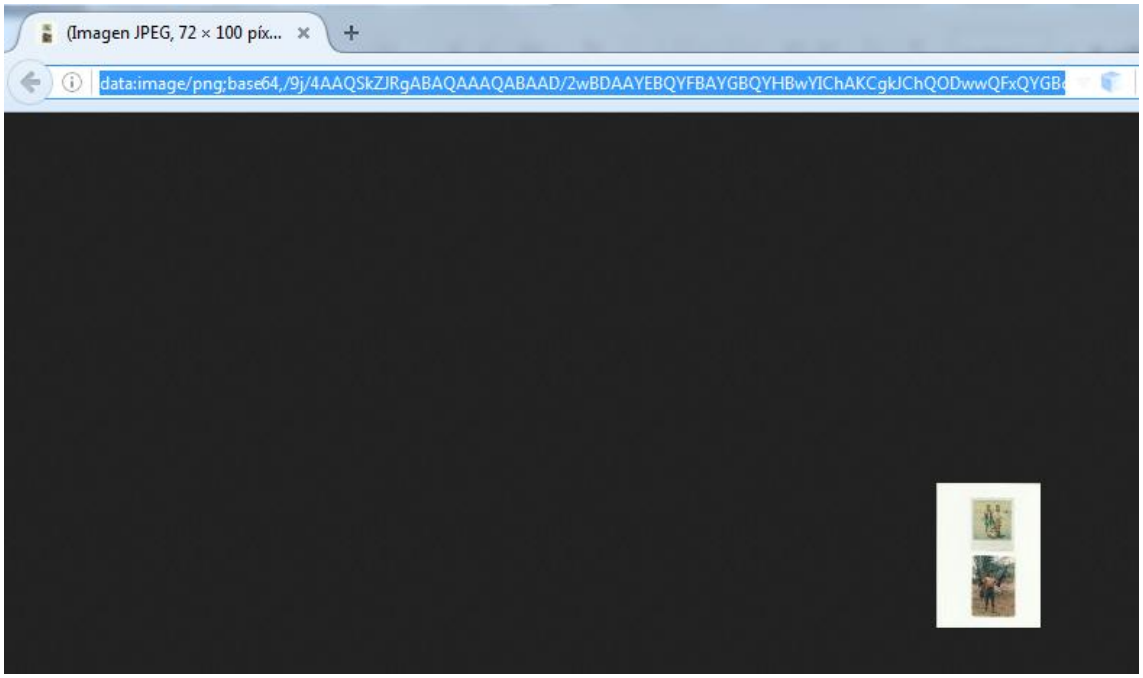


Figura 40: miniatura de imagen enviada por WhatsApp

La imagen tiene poca resolución pero se aprecia que consta de dos fotografías. En la primera aparecen dos personas y en la segunda una, con lo que podrían ser dos armas en sus manos.

8.2.2.4.3 Hallazgos

Tras el análisis se ha encontrado:

- Una copia de una base de datos con mensajes intercambiados por *WhatsApp* en noviembre de 2011.
- Se aprecia que el usuario del *WhatsApp* del que se ha analizado la BBDD ha establecido 5 conversaciones diferentes: 4 individuales y 1 de grupo. En las individuales no hay indicios de delito.
- En la conversación de grupo intervienen 3 personas diferentes.
    - Carlos: <número desconocido>
    - Raúl: 34635293190
    - Iván: 34660401445
- En la conversación hablan de lo que parece un fraude de tarjetas de crédito, en la que una vez robados los números realizan compras que envían a un piso de Mataró.
- Fotografía en miniatura en la que aparecen 3 personas. Posiblemente se trate de una miniatura con baja resolución de una imagen más grande. Con la imagen completa podríamos comprobar si existe algún fichero oculto (esteganografía). Se adjunta como evidencia por si pudiera ser de utilidad más adelante.

Se adjuntan fichero con la BBDD, la tabla completa y la fotografía (**evidencias B2 y B3** del Anexo).

8.2.2.5 Ficheros eliminados

8.2.2.5.1 Objetivo

Analizar si ha sido eliminado algún fichero del dispositivo y en caso de ser así tratar de recuperar su contenido.

8.2.2.5.2 Procedimiento

Autopsy nada más crear un caso nos pregunta si queremos analizar el espacio sin asignar. Lo marcamos y comienza el análisis en busca de ficheros eliminados, entre otras cosas:

Figura 41: análisis en curso de ficheros eliminados con Autopsy

Una vez finalizado el análisis automático, comprobamos que existen 4019138560 bytes sin asignar (unos 4GB), pero no ha encontrado ningún fichero eliminado.

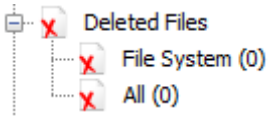


Figura 42: resultado del análisis de ficheros eliminados

8.2.2.5.3 Hallazgos

No se han encontrado ficheros eliminados en el dispositivo *USB*.

8.2.3 Análisis del disco duro

En nuestro caso de *Autopsy*, agregamos la imagen del disco duro y ejecutamos la opción de *Run Ingest Modules* para analizar de manera automática toda la información contenida en la fuente.

8.2.3.1 Identificación del SO y programas instalados

8.2.3.1.1 Objetivo

Obtener información sobre qué sistema operativo está instalado en la imagen de manera que podamos conocer la arquitectura del mismo y saber por tanto donde buscar el resto de la información.

8.2.3.1.2 Procedimiento

En los resultados del análisis automático de *Autopsy*, existe el menú *Extracted Content* y dentro de este la opción *Operating System Information*. De las tres fuentes encontradas, pinchamos sobre *SOFTWARE* y en la pestaña *Results* encontramos lo siguiente:

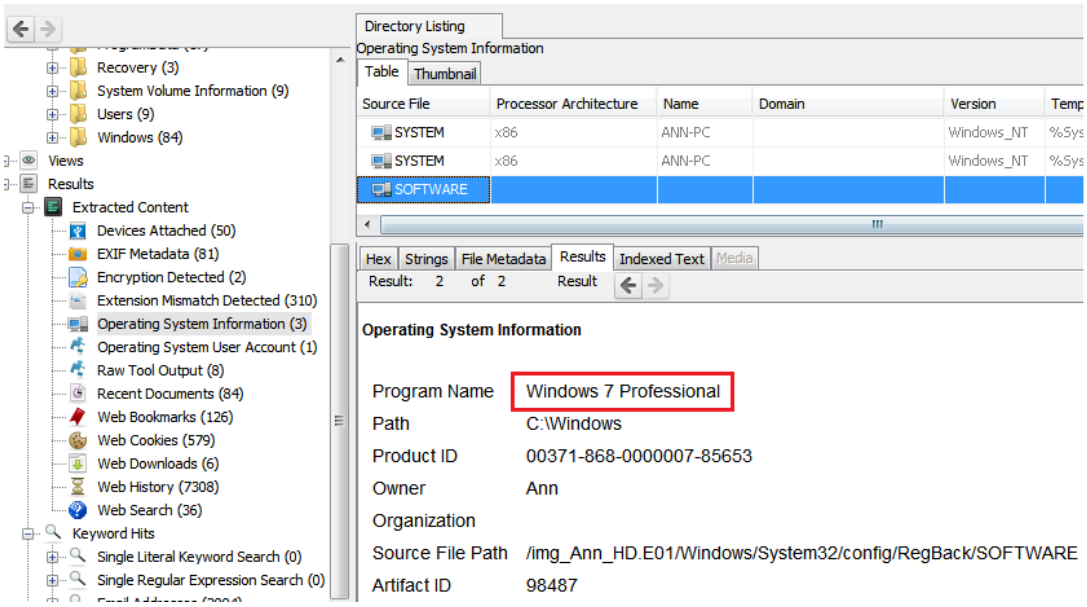


Figura 43: identificación del SO con Autopsy

Vemos que se trata de un sistema *Windows 7*, tal y como vimos en el análisis de la memoria *RAM* (apartado 8.2.1.1). Conociendo este dato, podemos obtener más información sobre el sistema del registro de *Windows*. Como no tenemos acceso al Sistema Operativo en ejecución sino que disponemos de una imagen del disco duro, no podemos ejecutar la herramienta *Regedit* para consultar la información. Sin embargo, podemos obtenerla de las copias de seguridad que se realizan periódicamente del registro. Estas copias se ubican en el directorio *C:\Windows\system32\config*. En particular, la información de los programas instalados la podemos obtener del fichero *SOFTWARE*:

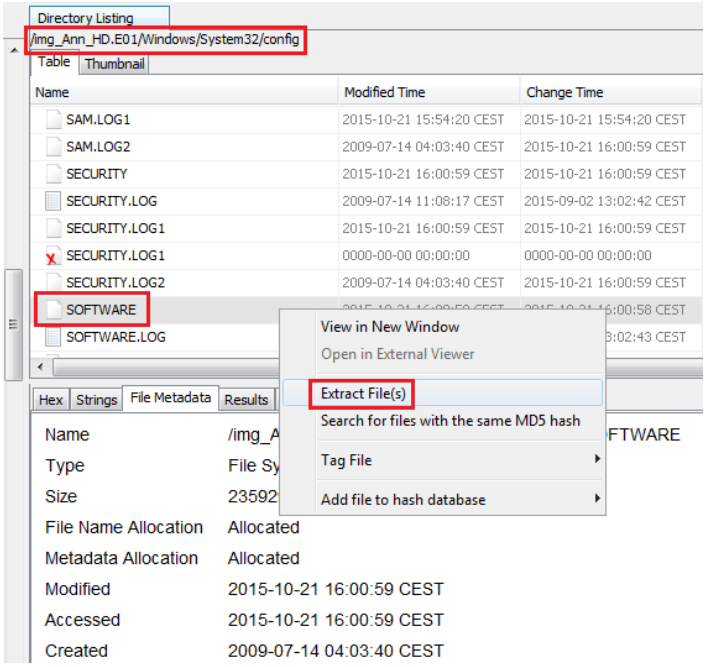


Figura 44: extracción del fichero de registro SOFTWARE

Extraemos el fichero para analizarlo con la herramienta *Windows Registry Recovery*. Ejecutamos el programa *WRR.exe* y abrimos el fichero *SOFTWARE*, extraído anteriormente, a través de *File/Open*:

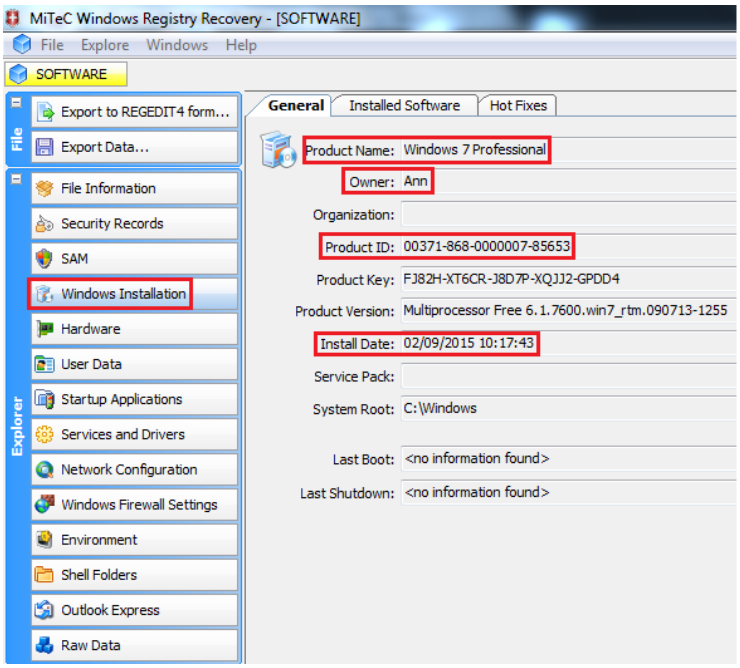


Figura 45: información del SO con WRR

También podemos consultar la lista de programas instalados, pulsando sobre la pestaña *Installed Software*:

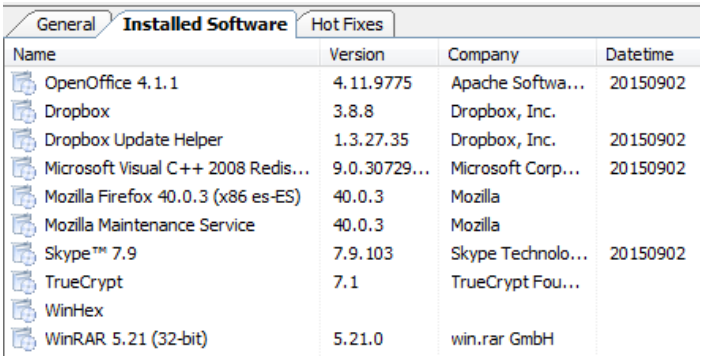


Figura 46: información sobre programas instalados con WRR

Podemos corroborar estos datos consultando el directorio *Program Files* de la imagen del disco duro utilizando *Autopsy*:

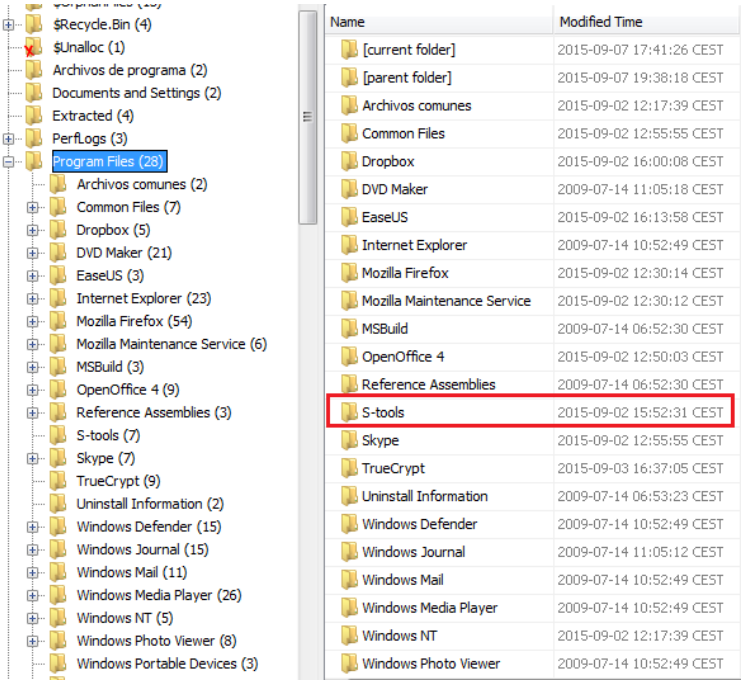


Figura 47: directorios de Windows con programas instalados

Además de los programas comentados anteriormente, vemos que también aparece uno llamado ***S-tools***. Se trata de un programa para ocultar información en ficheros utilizando técnicas de esteganografía.

8.2.3.1.3 Hallazgos

Según la información obtenida, podemos determinar lo siguiente respecto al sistema operativo:

- Es un ***Windows 7 Professional de 32 bits***.
- El programa está registrado a nombre de ***Ann***.
- El ID de producto es **00371-868-0000007-85653**.
- Fue instalado el **2 de septiembre de 2015, a las 10:17:43**.

- También fueron instalados los siguientes programas:
    - *OpenOffice 4.1.1*
    - *Dropbox 3.8.8*
    - *Firefox 40.0.3*
    - *Skype 7.9*
    - *TryeCrypt 7.1*
    - *WinHex*
    - *WinRAR 5.21*
    - *S-tools*

Se adjunta fichero *SOFTWARE* con la información sobre el registro (**evidencia C1** del Anexo).

8.2.3.2 Información sobre el disco duro

8.2.3.2.1 Objetivo

Obtener detalles sobre el disco duro del cual se extrajo la imagen para determinar si coincide la marca, modelo, tamaño con la información recibida, así como determinar si existen otras particiones visibles u ocultas en el mismo.

8.2.3.2.2 Procedimiento

Podemos sacar información sobre la imagen a través de *Autopsy* pulsando con el botón derecho sobre *Data Source/Ann_HD.E01* y después en *Image Details*:

Figura 48: tamaño de la imagen del disco duro según Autopsy

En la información sobre la imagen podemos ver su tamaño (**10462593024 bytes, unos 10 GB**) entre otras cosas.

En el apartado anterior, vimos cómo obtener información de registro a través de ficheros de copias de seguridad. Estas copias se ubican en el directorio *C:\Windows\system32\config*. En particular, la información del disco la podemos obtener del fichero *SYSTEM*.

Extraemos el fichero para analizarlo con la herramienta *Windows Registry Recovery*. Ejecutamos el programa *WRR.exe* y abrimos el fichero *SYSTEM* extraído a través de *File/Open*. Una vez abierto pulsando sobre Raw Data podemos navegar sobre las claves del registro.

Vamos hasta *ControlSet001\Enum\IDE\DiskWDC_WD3200BPVT-22JJ5T0_____01.01A01* y vemos que solo hay una entrada (*5&11c6677e&0&0.0.0*). Esto nos indica que sólo hay una partición del dispositivo y que como su segundo carácter es un *&* no se corresponde con su número de serie:

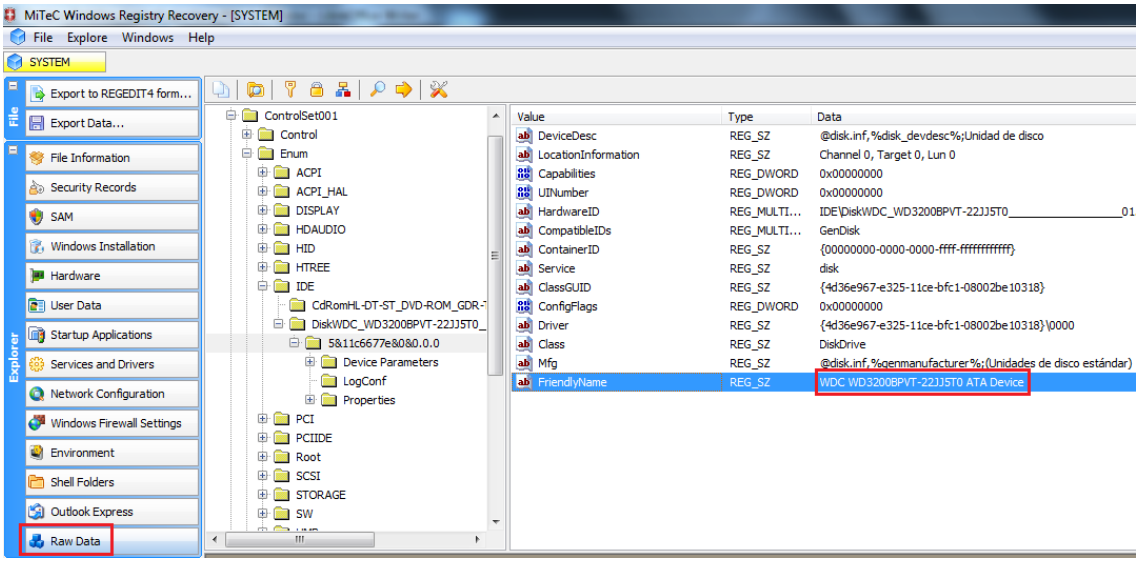


Figura 49: marca y modelo del disco duro

En esta entrada vemos que el disco duro tiene el identificador *WDC WD3200BPVT-22JJ5T0 ATA Device*. Buscando en Internet información sobre las especificaciones de este disco [23], obtenemos:

Specifications	320 GB	320 GB
Model number	WD3200LPVT	WD3200BPVT
Interface	SATA 3 Gb/s	SATA 3 Gb/s
Formatted capacity[1]	320,072 MB	320,072 MB
User sectors per drive	625,142,448	625,142,448
Advanced Format (AF)	Yes	Yes
Form factor	2.5-inch	2.5-inch
RoHS compliant[2]	Yes	Yes

Figura 50: especificaciones del disco duro

8.2.3.2.3 Hallazgos

Según la información obtenida, podemos determinar que se trata de un disco duro de **320GB** con una sola partición, en el que sólo **se están utilizando 10GB**. La marca y modelo coinciden con la información recibida en las evidencias digitales.

Se adjunta fichero *SYSTEM* con la información sobre el registro (**evidencia C2** del Anexo).

8.2.3.3 Fecha del último apagado del equipo

8.2.3.3.1 Objetivo

Conocer la fecha y horas del último apagado del equipo.

8.2.3.3.2 Procedimiento

Esta información también es almacenada en el fichero de registro *SYSTEM* (evidencia C2 del Anexo). Ejecutamos el programa *WRR.exe* y abrimos el fichero extraído a través de *File/Open*. Pulsamos sobre *Raw Data* podemos navegar sobre las claves del registro. Vamos hasta *ControlSet001\Control\Windows\ShutdownTime* y pulsamos dos veces sobre la clave para ver su valor:

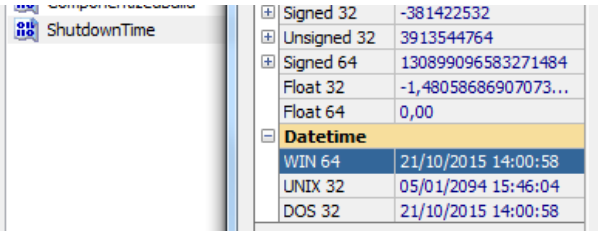


Figura 51: fecha del último apagado del equipo

8.2.3.3.3 Hallazgos

Podemos determinar que el equipo fue apagado por última vez el día **21 de octubre de 2015 a las 14:00:58**.

8.2.3.4 Usuarios del S.O.

8.2.3.4.1 Objetivo

Obtener todos los usuarios creados en el S.O. así como sus fechas de creación y últimos accesos.

8.2.3.4.2 Procedimiento

Esta información también es almacenada en los ficheros de copias de seguridad del registro. En particular, la información de los usuarios la podemos obtener del fichero *SAM*.

Extraemos usando *Autopsy* el fichero para analizarlo con la herramienta *Windows Registry Recovery*. Ejecutamos el programa *WRR.exe* y abrimos el fichero *SAM* extraído a través de *File/Open*. Una vez abierto pulsando sobre *SAM* y la pestaña *Groups and Users*. Vemos que hay creados 4 usuarios:

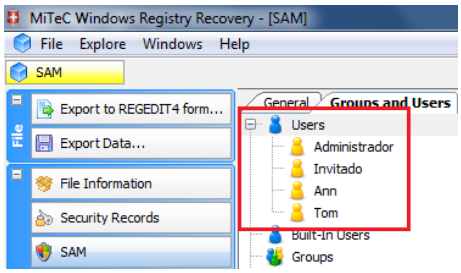


Figura 52: usuarios del SO extraídos mediante WRR

Pulsando sobre cada uno de ellos podemos ver las fechas de creación y último acceso:

Administrador:

Property	Value
SID	S-1-5-21-2589184436-4231671082-1653910475-500
Comment	Cuenta integrada para la administración del equipo o dominio
Last logon	14/07/2009 4:53:58
Last password set	14/07/2009 4:55:45

Figura 53: información del usuario Administrador

Invitado:

Property	Value
SID	S-1-5-21-2589184436-4231671082-1653910475-501
Comment	Cuenta integrada para el acceso como invitado al equipo o dominio
Account expiration	30/12/1899 2:48:05

Figura 54: información del usuario invitado

Ann:

Property	Value
SID	S-1-5-21-2589184436-4231671082-1653910475-1000
Last logon	21/10/2015 13:54:18
Last password set	02/09/2015 10:17:38
Account expiration	30/12/1899 2:48:05
Last incorrect password	07/09/2015 13:33:15

Figura 55: información del usuario Ann

Tom:

Property	Value
SID	S-1-5-21-2589184436-4231671082-1653910475-1001
Full name	Tom
Last logon	21/10/2015 9:03:02
Last password set	02/09/2015 10:20:38
Account expiration	30/12/1899 2:48:05
Last incorrect password	07/09/2015 13:33:31

Figura 56: información del usuario Tom

8.2.3.4.3 Hallazgos

Según la información hallada en el registro, podemos determinar que existían 4 usuarios creados en el sistema en el momento que fue extraída la imagen del disco duro.

Los usuarios *Administrador* e *Invitado* nunca han sido utilizados para acceder al sistema. Los otros dos usuarios (*Ann* y *Tom*) cambiaron su contraseña el mismo día y prácticamente a la misma hora que se instaló el sistema operativo, por lo que esta fecha coincide con la creación de los usuarios:

Usuario	Fecha de Creación	Fecha de último acceso
Administrador	-	14/07/2009 4:53
Invitado	-	-
Ann	02/09/2015 10:17	21/10/2015 13:54
Tom	02/09/2015 10:20	21/10/2015 9:03

Figura 57: usuarios del SO con sus fechas de creación y acceso

Se adjunta fichero *SAM* con la información sobre el registro (**evidencia C3** del Anexo).

8.2.3.5 Dispositivos conectados

8.2.3.5.1 Objetivo

Obtener un listado de todos los dispositivos USB conectados al equipo desde la fecha de instalación del SO.

8.2.3.5.2 Procedimiento

A través de *Autopsy*, podemos consultar todos los dispositivos conectados al equipo: marca, modelo, identificador y fechas en las que fueron conectados:

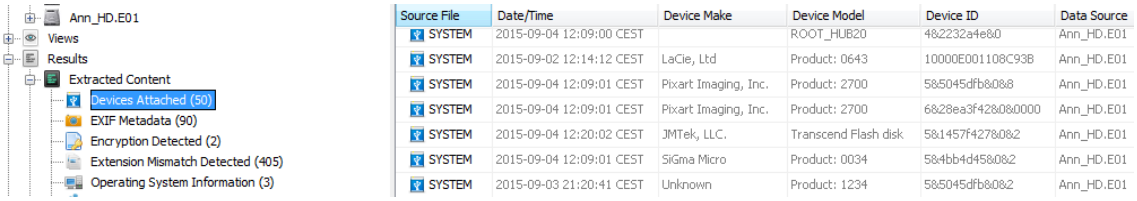


Figura 58: dispositivos conectados según Autopsy

8.2.3.5.3 Hallazgos

Se encuentran un total de 50 entradas, entre las cuales tan sólo hay 5 dispositivos únicos. A continuación mostramos un resumen de la última vez que fueron conectados:

Fecha	Fabricante	Modelo	Identificador
2015-09-02 12:14:12 CEST	LaCie, Ltd	Product: 0643	10000E001108C93B
2015-09-07 18:05:47 CEST	JMTek, LLC.	Transcend Flash disk	5&4bb4d45&0&2
2015-10-21 15:53:00 CEST	Pixart Imaging, Inc.	Product: 2700	6&28ea3f42&0&0000
2015-10-21 15:53:00 CEST	SiGma Micro	Product: 0034	5&1457f427&0&2
2015-10-21 15:56:31 CEST	Unknown	Product: 1234	5&5045dfb&0&3

Figura 59: resumen de dispositivos conectados

Se adjunta tabla completa (**evidencia C4** del Anexo)

8.2.3.6 Papelera de reciclaje

8.2.3.6.1 Objetivo

Recuperar los ficheros enviados a la papelera de reciclaje por los usuarios del equipo.

8.2.3.6.2 Procedimiento

Mediante *Autopsy*, navegamos hasta el directorio *$Recycle.Bin* de la imagen del disco duro:

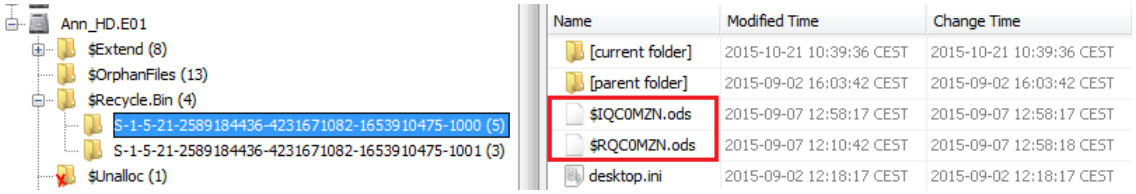


Figura 60: vista de la papelera de reciclaje en Autopsy

Se encuentran dos directorios en la papelera de reciclaje. Cada uno de estos directorios está asociado a un usuario, y tienen como nombre su SID. Si consultamos el apartado 8.2.3.4, comprobamos que el que acaba en 1000 pertenece al usuario *Ann* y el terminado el 1001 a *Tom*.

El directorio de *Tom* está vacío mientras que el de *Ann* tiene 2 ficheros de tipo *ods* (hoja de cálculos).

El fichero cuyo nombre comienza por $I, seguido de caracteres aleatorios, contiene la ruta y nombre del fichero original que fue enviado a la papelera de reciclaje:

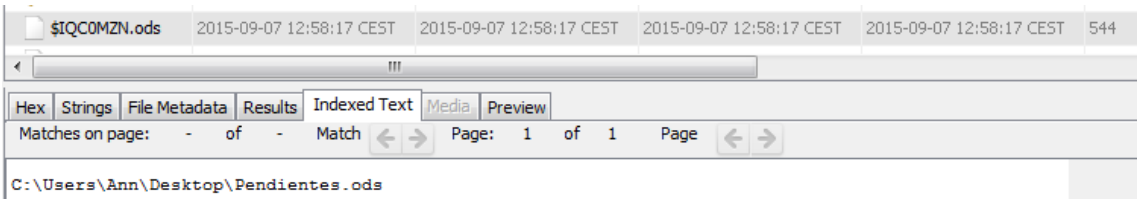
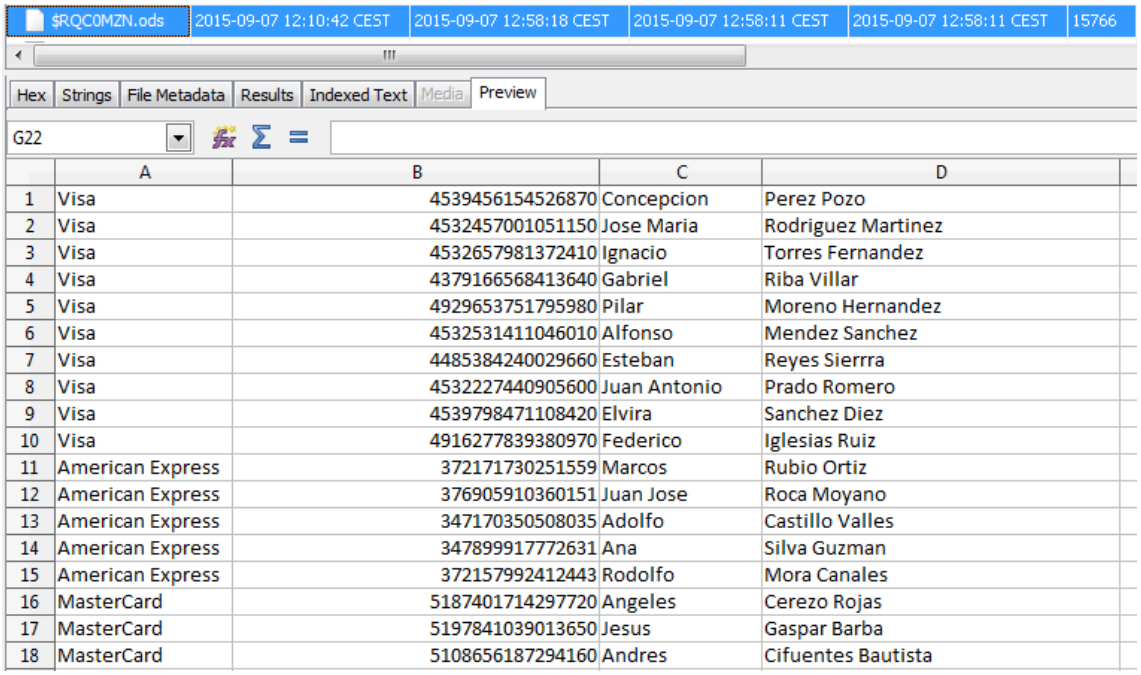


Figura 61: ruta original del fichero enviado a la papelera

El fichero cuyo nombre comienza por $R, seguido de los mismos caracteres aleatorios que el fichero anterior, contiene los datos del fichero original:



	A	B	C	D
1	Visa	4539456154526870	Concepcion	Perez Pozo
2	Visa	4532457001051150	Jose Maria	Rodriguez Martinez
3	Visa	4532657981372410	Ignacio	Torres Fernandez
4	Visa	4379166568413640	Gabriel	Riba Villar
5	Visa	4929653751795980	Pilar	Moreno Hernandez
6	Visa	4532531411046010	Alfonso	Mendez Sanchez
7	Visa	4485384240029660	Esteban	Reyes Sierrra
8	Visa	4532227440905600	Juan Antonio	Prado Romero
9	Visa	4539798471108420	Elvira	Sanchez Diez
10	Visa	4916277839380970	Federico	Iglesias Ruiz
11	American Express	372171730251559	Marcos	Rubio Ortiz
12	American Express	376905910360151	Juan Jose	Roca Moyano
13	American Express	347170350508035	Adolfo	Castillo Valles
14	American Express	347899917772631	Ana	Silva Guzman
15	American Express	372157992412443	Rodolfo	Mora Canales
16	MasterCard	5187401714297720	Angeles	Cerezo Rojas
17	MasterCard	5197841039013650	Jesus	Gaspar Barba
18	MasterCard	5108656187294160	Andres	Cifuentes Bautista

Figura 62: contenido del fichero enviado a la papelera de reciclaje

8.2.3.6.3 Hallazgos

Hemos comprobado que el usuario *Ann* envió a la papelera de reciclaje el fichero *Pendientes.ods* el 7 de Septiembre a las 12:58:11.

Este fichero tiene el mismo contenido que el encontrado en el análisis del dispositivo USB realizado en el apartado 8.2.2.2 (*Pendientes.ods*, evidencia B1 del Anexo).

Se adjuntan ficheros encontrados (**evidencias C5 y C6** del Anexo)

8.2.3.7 Ficheros eliminados

8.2.3.7.1 Objetivo

Analizar qué ficheros fueron eliminados en el sistema de manera que podamos tratar de recuperar el contenido si se encontrara alguno que fuera interesante para la investigación.

8.2.3.7.2 Procedimiento

Los ficheros eliminados podemos localizarlos mediante la herramienta *Autopsy*. Para ello pulsamos sobre el botón del menú lateral izquierdo *View/Deleted Files*. Aparecerá un listado con todos los ficheros eliminados:

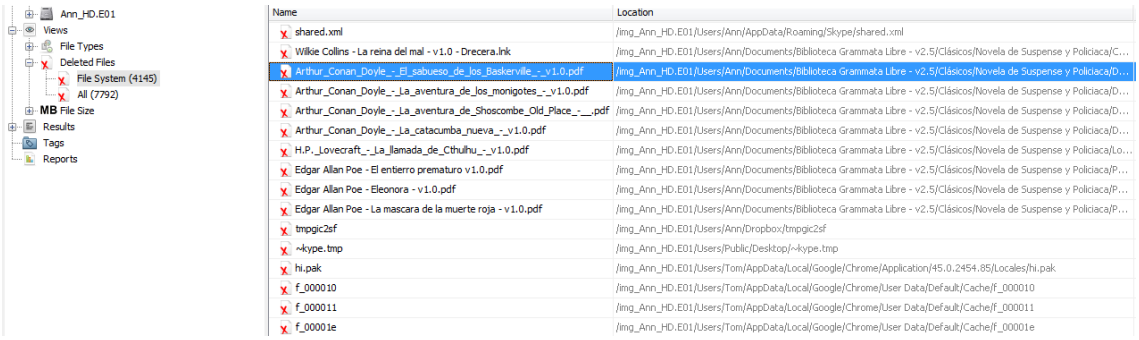


Figura 63: ficheros eliminados según Autopsy

Hay un total de 4145 ficheros eliminados. Casi todos ellos son ficheros del propio sistema operativo o de aplicaciones instaladas. Relacionados con los usuarios del SO, tan sólo se han encontrado 8 ficheros PDF de lo que parecen ser libros clásicos, eliminados por el usuario *Ann*. Los ficheros PDF pueden ser utilizados para albergar *malware*, por lo que se intentará encontrar estos ficheros analizando los ficheros recuperados mediante técnicas de *file carving*.

8.2.3.7.3 Hallazgos

No se ha encontrado ninguna evidencia con esta técnica, tan sólo algunos ficheros PDF para ser analizados en el siguiente apartado.

8.2.3.8 File Carving

8.2.3.8.1 Objetivo

Recuperar el contenido de los ficheros eliminados en el sistema y buscar en ellos evidencias que ayuden en la investigación.

8.2.3.8.2 Procedimiento

Es posible recuperar parte de los ficheros eliminados mediante técnicas de *File Carving*. *Autopsy* incorpora una herramienta de este tipo, la cual fue ejecutada al importar la imagen del disco duro (*Ingest Modules*). Para ver los ficheros recuperados pulsamos sobre el botón del menú lateral izquierdo *$CarvedFiles*. Aparecerá un listado con todos los ficheros eliminados:

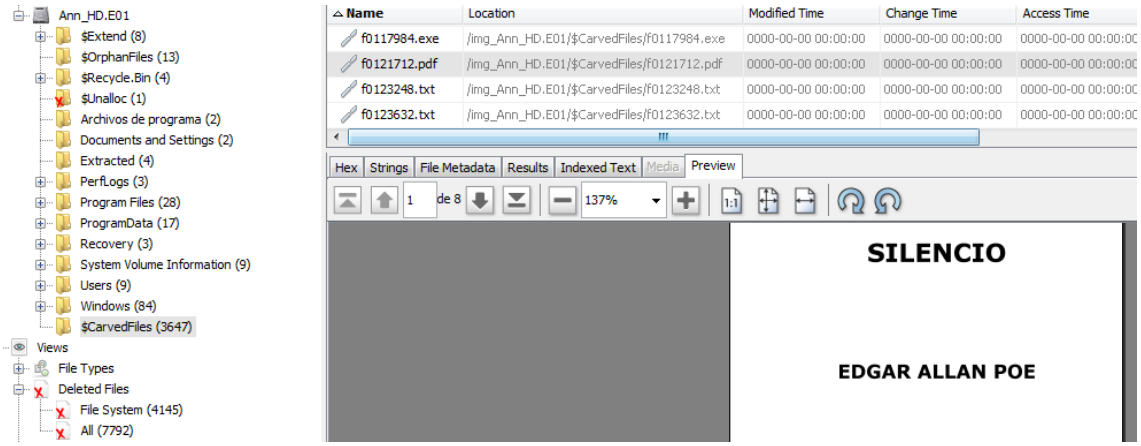


Figura 64: ficheros recuperados mediante file carving

Casi la totalidad de los ficheros encontrados pertenecen al propio sistema operativo.

Se ha encontrado un fichero de tipo PDF (*f0121712.pdf*), y no parece ser ninguno de los 8 eliminados por el usuario *Ann* referenciados en el apartado anterior.

Se analiza mediante *VirusTotal* sin encontrar ningún indicio de que esté infectado por malware.

También se analiza con *Foca* y no se encuentran metadatos.

Sin embargo, existen otra técnicas para ocultar información en metadatos de ficheros *PDF*. Algunas de ellas consisten en añadir información usando un editor hexadecimal en secciones no visibles del documento final. En el apartado 8.2.3.1 se encontró que el equipo tenía instalado el software *WinHex*, un editor hexadecimal que podría haberse utilizado para ocultar datos.

Abrimos por lo tanto el fichero *f0121712.pdf* con *WinHex* y encontramos los siguiente:

```
6D 70 6D 65 74 61 3E 0A | F> </x:xmpmeta>
20 20 20 20 20 20 20 20 |
35 38 33 34 37 39 32 20 | 370555595834792
6F 6D 65 7A 20 44 75 72 | Teresa Gomez Dur
20 20 20 20 20 20 20 20 | an
30 38 31 30 38 36 36 20 | 375388340810866
72 61 6C 65 73 20 46 65 | Maria Morales Fe
20 20 20 20 20 20 20 20 | rnandez
20 20 20 20 20 20 20 20 |
20 20 20 20 20 20 20 20 |
6B 65 74 20 65 6E 64 3D |   <?xpacket end=
64 73 74 72 65 61 6D 0A | 'w'?> endstream
```

Figura 65: información oculta en el fichero eliminado f0121712.pdf

8.2.3.8.3 Hallazgos

Se ha recuperado un fichero *PDF* eliminado con información de lo que parecen datos de tarjetas bancarias de dos personas:

- 370555595834792 Teresa Gomez Duran
- 375388340810866 Maria Morales Fernandez

Se adjunta documento *PDF* (**evidencia C7** del Anexo).

8.2.3.9 Ficheros huérfanos

8.2.3.9.1 Objetivo

Analizar los ficheros huérfanos del sistema, es decir, aquellos cuya aplicación padre ha sido desinstalada o borrada.

8.2.3.9.2 Procedimiento

Los ficheros huérfanos podemos localizarlos mediante la herramienta *Autopsy*. Para ello pulsamos sobre el botón del menú lateral izquierdo *$OrhanFiles*. Aparecerá un listado con todos los ficheros huérfanos:

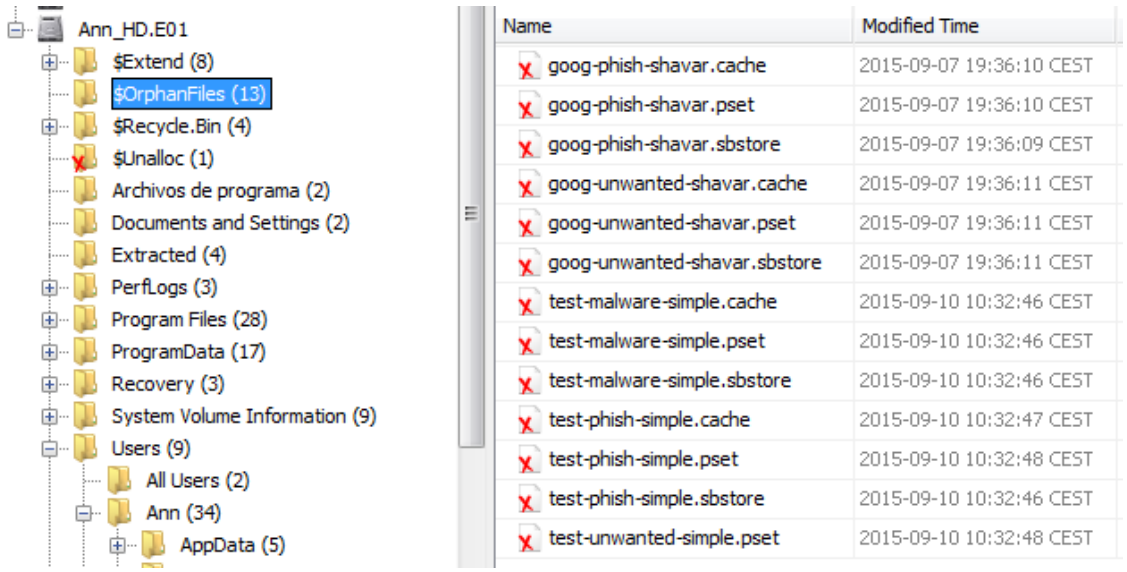


Figura 66: ficheros huérfanos según Autopsy

Se encuentran un total de 13 ficheros huérfanos. Según los nombres y extensiones, se trata de ficheros utilizados por complementos *Safe Browsing* de Firefox [24]. Estos complementos normalmente bloquean código *javascript, java applets* y *flash* con el objetivo de evitar anuncios así como cualquier tipo de malware.

8.2.3.9.3 Hallazgos

No se han encontrado evidencias de ficheros sospechosos en los ficheros huérfanos.

8.2.3.10Documentos recientes

8.2.3.10.1 Objetivo

Comprobar qué documentos han sido accedidos recientemente para tener una idea de la actividad que han tenido los usuarios en un momento determinado.

8.2.3.10.2 Procedimiento

Desde *Autopsy* podemos revisar la lista de ficheros accedidos recientemente por lo usuario del sistema. En el menú izquierdo, vamos a *Results/Extracted Content/Recent Documents*:

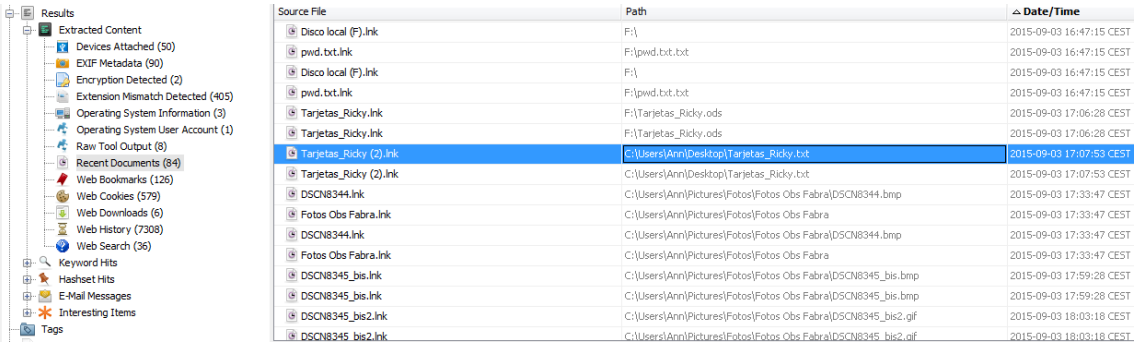


Figura 67: documentos accedidos recientemente según Autopsy

En este apartado no vamos a analizar los documentos recientes. Nos limitamos a registrar qué documentos han sido accedidos y cuándo. Ordenamos los ficheros por fecha, los exportamos a una tabla, eliminamos los repetidos y añadimos una columna indicando si el fichero se encuentra disponible en la imagen o ha sido eliminado sin dejar rastro. En la siguiente tabla mostramos un resumen:

Fichero	Ruta de acceso	Fecha	Presente
Disco local (F).lnk	F:\	2015-09-03 16:47:15 CEST	-
pwd.txt.lnk	F:\pwd.txt.txt	2015-09-03 16:47:15 CEST	No
Tarjetas_Ricky.lnk	F:\Tarjetas_Ricky.ods	2015-09-03 17:06:28 CEST	No
Tarjetas_Ricky (2).lnk	C:\Users\Ann\Desktop\Tarjetas_Ricky.txt	2015-09-03 17:07:53 CEST	No
DSCN8344.lnk	C:\Users\Ann\Pictures\Fotos\Fotos Obs Fabra\DSCN8344.bmp	2015-09-03 17:33:47 CEST	Sí
Fotos Obs Fabra.lnk	C:\Users\Ann\Pictures\Fotos\Fotos Obs Fabra	2015-09-03 17:33:47 CEST	Sí

Figura 68: extracto de documentos accedidos recientemente

8.2.3.10.3 Hallazgos

Se obtiene listado con los ficheros y la fecha de cuándo fueron accedidos. Los ficheros serán analizados en el apartado 8.2.3.12 y 8.2.3.13.

Se adjunta tabla completa en la **evidencia C8** del Anexo.

8.2.3.11Logs de Skype

8.2.3.11.1 Objetivo

Obtener información sobre las actividades realizadas por los usuarios del equipo a través de los registros (*logs*) de la aplicación de mensajería instantánea y videoconferencia *Skype*.

8.2.3.11.2 Procedimiento

Los registros de comunicaciones establecidas por *Skype* se almacenan en una base de datos *SQLite* en el fichero *main.db* del directorio personal del usuario. En nuestro caso, se ha encontrado el fichero */Users/Ann/AppData/Roaming/Skype/annetom22/main.db*. Lo extraemos a través de *Autopsy* siguiendo el procedimiento habitual.

Una vez extraído, lo abrimos con la herramienta *SkypeLogView*. Vemos que existen 2 conversaciones mantenidas en 2 días diferentes.

<u>Conversación 1:</u>

Action Time	E..	User Name	Display Name	Chat Message
04/09/2015 14:49:32			Anne G.H.	
		echo123	Echo / Sound ...	
04/09/2015 17:52:08		annetom22 live:rickyrodriguezgarcia		
04/09/2015 17:52:40		live:rickyrodriguezgarcia	Ricky Rodriguez	Saludos, ya he recibido las fotos...
04/09/2015 17:50:44		annetom22 live:rickyrodriguezgarcia		
04/09/2015 17:53:04		annetom22	Anne G.H.	Me alegro... ¿Todo bien?
04/09/2015 17:53:16		live:rickyrodriguezgarcia	Ricky Rodriguez	De fábula, pero... he olvidado la contraseña...
04/09/2015 17:53:33		annetom22	Anne G.H.	¡Pues qué bien!
04/09/2015 17:53:40		live:rickyrodriguezgarcia	Ricky Rodriguez	...lo siento...
04/09/2015 17:54:19		live:rickyrodriguezgarcia	Ricky Rodriguez	¿Puedes pasármela?
04/09/2015 17:54:48		annetom22	Anne G.H.	Tú mismo... ¿A ti qué te parece?
04/09/2015 17:55:00		live:rickyrodriguezgarcia	Ricky Rodriguez	Tampoco entremos en modo paranoico... No creo que pase nada
04/09/2015 17:55:38		annetom22	Anne G.H.	Evidentemente, nunca pasa nada... En fin, aquí va: KaPow581!
04/09/2015 17:55:52		live:rickyrodriguezgarcia	Ricky Rodriguez	Gracias, recuerdos a Tom
04/09/2015 17:56:06		annetom22	Anne G.H.	Hasta luego Ricky

Figura 69: conversación por Skype del 4 de septiembre de 2015

<u>Conversación 2:</u>

07/09/2015 19:18:57	annetom22 live:rickyrodriguezgarcia		
07/09/2015 19:19:18	annetom22 live:aram768		
07/09/2015 19:19:37	live:aram768	Aram B.V.	Hola, hace días que tenemos que quedar... Todavía tengo que pagarte el últi...
07/09/2015 19:20:22	live:aram768	Aram B.V.	Precisamente este sábado estuve en tu ciudad y descubrí un sitio muy discre...
07/09/2015 19:24:50	live:aram768	Aram B.V.	Ei! disculpa, te lo paso en 5 min...tengo alguien al telf
07/09/2015 19:25:08	annetom22	Anne G.H.	No te preocupes, yo tambien algo liada...
07/09/2015 19:28:35	live:aram768	Aram B.V.	hola ya estoy aqui de nuevo... ahi van las fotos
07/09/2015 19:28:48	live:aram768	Aram B.V.	
07/09/2015 19:28:48	live:aram768	Aram B.V.	
07/09/2015 19:28:48	live:aram768	Aram B.V.	
07/09/2015 19:31:10	annetom22	Anne G.H.	Pues si, lo conozco. Tienes razon, es muy discreto. ¿Que tal el proximo sabad...
07/09/2015 19:31:18	live:aram768	Aram B.V.	Perfecto, hasta luego pues
07/09/2015 19:35:05	live:rickyrodriguezgarcia	Ricky Rodriguez	Hola Anne, te mando algo que te va a interesar
07/09/2015 19:35:17	live:rickyrodriguezgarcia	Ricky Rodriguez	http://we.tl/e14LIZzkSz
07/09/2015 19:35:25	annetom22	Anne G.H.	A ver... Te digo algo...
07/09/2015 19:37:42	annetom22	Anne G.H.	¿Es lo que parece?
07/09/2015 19:37:54	annetom22	Anne G.H.	Tiene una contraseña y supongo que sera la de siempre...
07/09/2015 19:38:11	live:rickyrodriguezgarcia	Ricky Rodriguez	Efectivamente! <ss type="wink">;-)</ss>
07/09/2015 19:41:16	annetom22	Anne G.H.	Esto es un poco raro...
07/09/2015 19:41:45	live:rickyrodriguezgarcia	Ricky Rodriguez	Ups... creo que me he confundido, te lo reenvio más tarde
07/09/2015 19:41:52	annetom22	Anne G.H.	De acuerdo!

Figura 70: conversación por Skype del 7 de septiembre de 2015

8.2.3.11.3 Hallazgos

- Los logs de la aplicación han sido hallados en el directorio personal del usuario ***Ann*** del sistema.
- Por un lado vemos una conversación entre 2 personas, Ricky Rodriguez y Anne G.H., el día 4 de septiembre de 2015 entre las 17:53 y 17:56, en la que intercambian una contraseña: **KaPow581!**
- Además, Ricky envía a Anne un enlace acortado de ***wetransfer.com***, servicio en la nube de intercambio de ficheros, e indica que tiene la contraseña de siempre. Poco después, Ann descarga el fichero con el malware ***ListadoNumeraciones.zip***.
- Por otro lado, existe otra conversación entre 3 personas, Ricky Rodríguez, Anne G.H y Aram G.H, mantenida el día 7 de septiembre entre las 19:19 y las 19:41.
- En esta segunda conversación, hablan de quedar en un lugar para hacer *el pago del último lote de tarjetas* supuestamente de Aram a Anne. Además intercambian 3 fotografías:
    - *C:\Users\Ann\AppData\Roaming\Skype\My Skype Received Files\20150907_162718.jpg*
    - *C:\Users\Ann\AppData\Roaming\Skype\My Skype Received Files\20150907_162746.jpg*
    - *C:\Users\Ann\AppData\Roaming\Skype\My Skype Received Files\20150907_162819.jpg*

Las fotogragías serán analizadas en el siguiente apartado.

Se adjunta BBDD con las conversaciones completas (**evidencia C9** del Anexo).

8.2.3.12Directorios de usuarios

8.2.3.12.1 Objetivo

Analizar los ficheros ubicados en los directorios personales de los usuarios del SO.

8.2.3.12.2 Procedimiento

Si ignoramos los usuarios del sistema, sólo existen 2 usuarios creados en el SO: *Ann* y *Tom*. Vamos a ver los ficheros de cada uno de ellos. Nos centraremos en los ficheros recientes, encontrados en el apartado 8.2.3.10.

8.2.3.12.2.1 Imágenes Skype

En *Users\Ann\AppData\Roaming\Skype\My Skype Received Files*, encontramos las 3 imágenes enviadas a través de *Skype*, según vimos en el apartado 8.2.3.11:

- 20150907_162718.jpg
- 20150907_162746.jpg
- 20150907_162819.jpg

Figura 71: imágenes enviadas por Skype

Si analizamos los metadatos de las imágenes con *Foca*, encontramos que todas fueron realizadas con una cámara marca *Samsung* modelo *SM-G350*:

Exif Makernote	
Make	SAMSUNG
Model	SM-G350

Figura 72: marca y modelo de la cámara fotográfica según Foca

Todas incluyen coordenadas GPS:

GPS Makernote	
GPS Version ID	2 2 0 0
GPS Latitude Ref	N
GPS Latitude	41°36'41,375
GPS Longitude Ref	E
GPS Longitude	2°4'53,375
GPS Altitude Ref	Sea level
GPS Altitude	356 metres
GPS Time-Stamp	14:27:12 UTC

Figura 73: coordenadas GPS de las fotografías

Las cuales apuntan a un parque público del municipio de Castellar del Vallés, en la provincia de Barcelona:

https://www.google.es/maps/place/41%C2%B036'41.0%22N+2%C2%B004'53.0%22E/@41.6113889,2.0808375,19.12z/data=!4m5!3m4!1s0x0:0x0!8m2!3d41.6113889!4d2.0813889

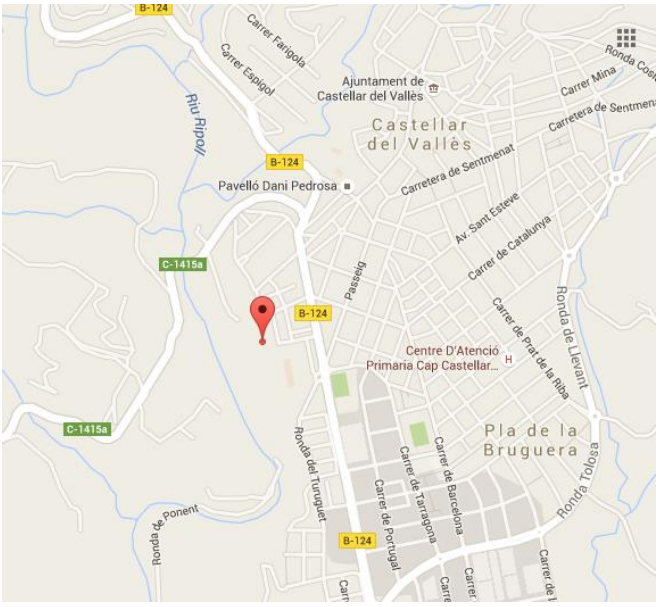


Figura 74: mapa de la ubicación encontrada en las fotografías

Se adjuntan imágenes (**evidencias C10, C11 y C12** del Anexo).

8.2.3.12.2.2 Escritorio

En *Users\Ann\Desktop* no se han encontrado los ficheros referenciados *Tarjetas_Ricky.txt* ni *Test.txt*. Tampoco se encuentran entre los ficheros eliminados. No se encuentra ningún otro fichero destacable.

8.2.3.12.2.3 Fotografías

En el directorio *Users\Ann\Pictures\Fotos* encontramos las siguientes fotos:

Figura 75: fichero \Fiestas Gracia\DSC_6537 (Medium).JPG

Figura 76: \Fotos Obs Fabra\DSCN8333.gif

Figura 77: \Fotos Obs Fabra\DSCN8344.gif

Figura 78: \Fotos Obs Fabra\DSCN8345.gif

Analizamos sus metadatos y aparentemente no contienen ninguna información importante. Sin embargo, si abrimos la imagen *DSCN8333.gif* con la herramienta *S-tool*, tras pulsar el revelar e introducir la contraseña *KaPow581!*, vemos que aparece un fichero oculto:

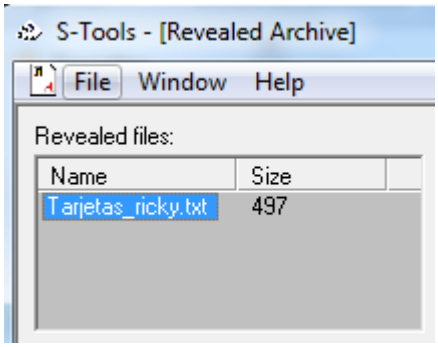


Figura 79: fichero oculto usando S-tool

Este fichero contiene la siguiente información:

```
0         10        20        30        40
4532472207641240  Juan Ramon  Felices Rodriguez
4532742511361320  Antonia   Cano Bermudez
4916040584664660  Nieves    Sepulveda Diaz
4929624362589750  Pedro   Gimenez Garcia
4556317310821640  Josefa    Herrero Vazquez
4532994302733610  Soledad   Garcia Soto
347747094943519   Eva Maria Martinez Medina
346686278890925   Alvaro    Menendez Benitez
375536039161138   Rafael    Ibañez Orozco
5500019643068870  Catalina  Vazquez Gamez
5315235040873250  Juan    Alonso Canovas
5432652478052620  Francisco Sancho Leal
```

Figura 80: contenido del fichero oculto en la imagen

Se adjutna imagen *DSCN8333.gif* y fichero oculto *Tarjetas_ricky.txt* (**evidencias C13 y C14** del Anexo).

8.2.3.12.2.4 Biblioteca

En *Users\Ann\Documents\Biblioteca Grammata Libre - v2.5\Clásicos\Novela de Suspense y Policiaca* se encuentran múltiples ficheros PDF de novelas clásicas. Vamos a analizar si contienen información oculta, tal y como se comprobó en el apartado 8.2.3.8, de los documentos accedidos recientemente:

- **Fichero**: *\Doyle\Arthur_Conan_Doyle_-_El_espanto_de_la_cueva_de_Juan_Azul_-_.pdf*
- **Resultado**: No se encuentra nada

- **Fichero**: *\Doyle\Arthur_Conan_Doyle_-_El_gato_del_Brasil_-_v1.0.pdf*
- **Resultado**: No se encuentra nada

- **Fichero**:*\Doyle\Arthur_Conan_Doyle_-_La_aventura_de_Shoscombe_Old_Place_-__.pdf*

- **Resultado**:

  5410-2027-1270-4680 Leandro Valero Moyano

  5112-3373-9748-5880 Joaquina Miralles Cortes

- **Fichero**: *Doyle**Arthur_Conan_Doyle_-_La_catacumba_nueva_-_v1.0.pdf*
- **Resultado**:

  4916-4198-0562-7420 Aurelia Muñoz Luque

  4532-2993-5073-4170 Victor Nuñez Pascual

- **Fichero**: *LeFanu**Joseph Thomas Sheridan le Fanu - El fantasma y el ensalmador - v1.0.pdf*
- **Resultado**:

  5281-6485-4498-6410 Mario Padilla Sanz

  5499-5853-9072-5730 Javier Fuertes Martin

- **Fichero**: *Lovecraft**H._P._Lovecraft_-_El_modelo_de_Pickman_-_v1.0.pdf*
- **Resultado**:

  4716-2196-6835-2520 Benito Lopez Lopez

  4716-3777-7146-9310 Feliciano Huertas Villar

Se adjuntan ficheros PDF (**evidencias C15 a C18** del Anexo).

8.2.3.12.2.5 Descargas

En el directorio *Users/Ann/Downloads/* encontramos los ficheros:

- ListadoNumeraciones.zip
- The Jerm.rar

Descomprimimos el primero de ellos, para lo cual usamos la contraseña *KaPow581!*. En su interior se encuentra un ejecutable llamado *LlistatNumeracions.exe*. Nada más descomprimirlo, el antivirus local lo detecta como un malware de tipo *backdoor* (puerta trasera). Parece ser que el nombre original del fichero es *excel_server.exe*:

Figura 81: detección de malware por AV en el fichero LlistatNumeracions.exe

El segundo de ellos, *The Jerm.rar*, no está protegido por contraseña. Lo descomprimimos y subimos el ejecutable *TheJerm.exe* a *VirusTotal*, clasificándolo como un malware tipo troyano. Parece ser el mismo ejecutable que se encontró en la memoria, en el apartado 8.2.1.6. Para asegurarnos, lo buscamos y encontramos en el siguiente directorio:

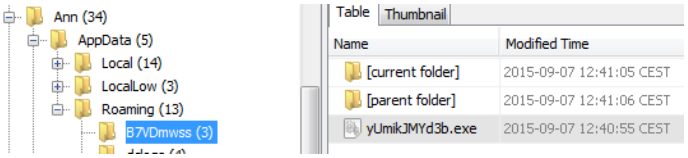


Figura 82: directorio del fichero yUmikJMYd3b.exe

Tras calcular el hash de los dos ficheros, comprobamos que efectivamente son el mismo fichero.

Todos estos ficheros se analizan en mayor profundidad en el apartado 8.2.3.15.

Se adjuntan ambos ficheros (**evidencias C19 y C20** del Anexo).

8.2.3.12.2.6 Documentos

En *Users**Ann**Documents*\ encontramos el fichero *pwd2.txt.txt*, con el siguiente contenido:

```
Annetom22@hotmail.com
AnneTom1980!

FromTom75@hotmail.com
Tommane75!
```

Figura 83: contenido del fichero pwd2.txt.txt

Parecen ser las credenciales de dos cuentas de correo electrónico de *hotmail*.

También encontramos el fichero *Listado numeraciones.exe*. Es catalogado por el antivirus como el mismo tipo de malware que el encontrado en el apartado 8.2.3.12.2.5, es decir un *backdoor* (*excel_server.exe*). El fichero ejecutable tiene el mismo *hash md5*, por lo que puede considerarse como el mismo fichero con diferente nombre. No se tendrá en cuenta.

Se adjunta fichero con contraseñas (**evidencia C21** del Anexo).

8.2.3.12.2.7 Documentos de Tom

Hasta ahora, todos los ficheros encontrados pertenecen al usuario *Ann*.

En *\Users\Tom\Documents* encontramos el fichero *Contc.ods*. Sin embargo, el fichero está protegido por contraseña y no hemos podido recuperarla ni romperla pro fuerza bruta (*John the Ripper).*

Tampoco se ha podido localizar el fichero llamado *Home.ods*.

Se adjunta fichero *Contc.ods* (**evidencia C24** del Anexo).

8.2.3.12.3 Hallazgos

Se ha localizado la siguiente información en los directorios de Ann:

- Imágenes con información *GPS* supuestamente de un lugar de encuentro de los tres interlocutores de una sesión de *Skype*. Esta localización apunta a Castellar del Vallés, Barcelona (**evidencia C9**).
- Fotografía con información oculta sobre lo que parecen ser tarjetas bancarias (**evidencias C13 y C14**).
- Ficheros PDF con información oculta sobre lo que parecen ser tarjetas bancarias (**evidencias C15 a C18**).
- Ficheros con malware (**evidencias C19 y C20**).
- Fichero con 2 usuarios y contraseñas de correo y Skype (**evidencia C21**).

8.2.3.13Ficheros cifrados

8.2.3.13.1 Objetivo

Recuperar información cifrada en el disco duro para analizar si contiene datos sobre algún hecho delictivo.

En el apartado 8.2.1.7 correspondiente al análisis de la memoria RAM, se encontró la existencia de un directorio cifrado con *TrueCrypt* en *C\Users\Ann\MyHome*, y que la contraseña era *SafePlace*. En este apartado vamos a intentar localizar el directorio y acceder a su contenido.

8.2.3.13.2 Procedimiento

Localizamos y extraemos en fichero *MyHome* desde *Autopsy*.

Una vez extraído, lo montamos en nuestro equipo usando *TrueCrypt*:

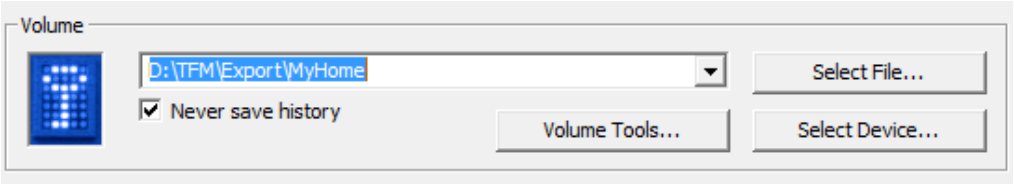


Figura 84: montando volumen cifrado con TrueCrypt

Al montarlo, accedemos a la unidad y vemos el contenido:

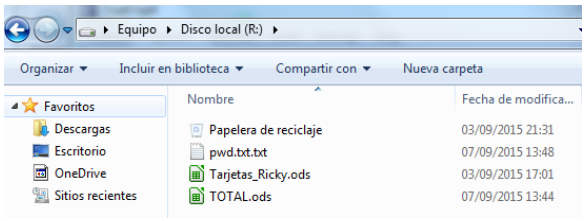


Figura 85: contenido del volumen cifrado

Encontramos un nuevo fichero de contraseñas (*pwd.txt.txt*):

SO:

Ann: Tom1980

Tom: Ann1978

S-tools:

KaPow581!

Pwd Tom:

100Pm!710GGh1??6dh**

E-mail:

Annetom22@hotmail.com

pwd: AnneTom1980!

FromTom75@hotmail.com

pwd: Tommane75!

Skype:

Annetom22

pwd:Anneconde22

Y dos nuevas tablas con información sobre tarjetas bancarias (*Tarjetas_Ricky.ods* y *TOTAL.ods*). A continuación se muestra un extracto:

19	Visa	4539798471108420	Elvira	Sanchez Diez
20	Visa	4916277839380970	Federico	Iglesias Ruiz
21	American Express	347747094943519	Eva Maria	Martinez Medina
22	American Express	346686278890925	Alvaro	Menendez Benitez

Figura 86: extracto del contenido del fichero Tarjetas_Ricky.ods

Además, en la papelera de reciclaje del volumen, se encuentra el fichero *LlistatNumeracions.exe*:

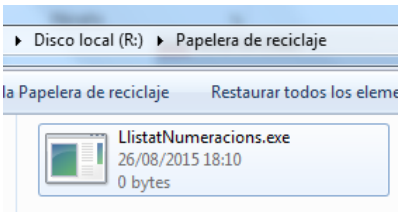


Figura 87: contenido de la papelera de reciclaje del volumen cifrado

8.2.3.13.3 Hallazgos

Se encuentran un fichero con contraseñas y dos tablas con información bancaria.

Se adjuntan ficheros (**evidencias C22, C23 y C24** del Anexo)**.** El fichero con el volumen cifrado no se adjunta debido a su tamaño (150MB).

8.2.3.14Navegación por Internet

8.2.3.14.1 Objetivo

Identificar qué páginas web han visitado los usuarios y cuándo para tratar de complementar la información obtenida hasta ahora.

8.2.3.14.2 Procedimiento

En *Autopsy* vamos a *Extracted Content/Web History* y vamos navegando por el historial:

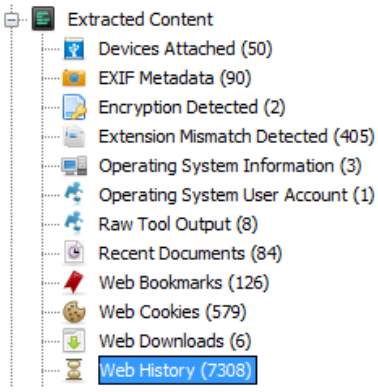


Figura 88: acceso al historial de navegación del usuario Ann

8.2.3.14.3 Hallazgos

En el historial de navegación del usuario *Ann* vemos algunas actividades sospechosas y otras que complementan el análisis de las evidencias realizado hasta el momento.

Vemos que el día 4 de septiembre de 2015, el usuario buscó información de cómo abrir una cuenta bancaria en Suiza y cómo evadir impuestos:

https://www.google.es/#q=abrir+cuenta+suiza+no+residente	2015-09-04 15:13:43 CEST
http://www.rankia.com/blog/opiniones/1992727-como-abrir-cuenta-bancaria-suiza	2015-09-04 15:12:20 CEST
https://www.google.es/#q=abrir+cuenta+suiza+no+residente	2015-09-04 15:13:43 CEST
https://www.google.es/#q=como+evadir+impuestos	2015-09-04 15:14:32 CEST
http://www.bbc.com/mundo/noticias/2014/05/140521_economia_impuestos_evasion_yv	2015-09-04 15:13:59 CEST
https://www.google.es/#q=como+evadir+impuestos	2015-09-04 15:14:32 CEST
http://www.gerencie.com/manual-para-evadir-impuestos.html	2015-09-04 15:14:15 CEST
https://www.google.es/#q=como+evadir+impuestos	2015-09-04 15:14:32 CEST

Figura 89: búsqueda de cómo evadir impuestos

El 7 de septiembre sobre las 12:30 el usuario *Ann* realiza la siguiente navegación:

https://www.google.es/search?q=msr+206&ie=utf-8&oe=utf-8&gws_rd=cr&ei=eGftVfzGNYO5UeeUhdAL	2015-09-07 12:31:21	1
http://www.google.es/aclk?sa=L&ai=CXOumeWftVdu8H951bIeYlfgLtZ7X2Aet1MXMtQK6iaqDAQgAEAIoAmDWjdOC3AjIAQGpAmC2BCx3t7I-qgQfT9BNY3o3ewn-T8Kl_...	2015-09-07 12:31:37	
http://www.ebay.es/sch/i.html?adpos=1t2&ul_noapp=true&geo_id=2918&MT_ID=1958&crlp=83066490149_627&keyword=msr+206&rlsatarget=kwd-275416250&_n...	2015-09-07 12:31:40	2
http://www.ebay.es/itm/Magnetic-Card-Reader-Writer-Encoder-Stripe-Magstripe-Credit-Compat-MSR206-MSR606-/250903989398?hash=item3a6b0b0c96	2015-09-07 12:32:04	
https://signin.ebay.es/ws/eBayISAPI.dll?SignIn&ru=http%3A%2F%2Foffer.ebay.es%2Fws%2FeBayISAPI.dll%3FBinConfirm%26item%3D250903989398%26quan...	2015-09-07 12:32:19	
https://guestcheckout.payments.ebay.es/ws/eBayISAPI.dll?GuestXOProcessor&sessionid=594245756&pagename=rypaddress	2015-09-07 12:32:39	
https://www.google.es/search?q=msr+206+software&ie=utf-8&oe=utf-8&gws_rd=cr&ei=A2jtVdbPMcz9Usq-rbAG	2015-09-07 12:33:41	3
https://www.youtube.com/watch?v=Cz5ovVUccCY	2015-09-07 12:33:51	
http://www.mediafire.com/download/z1x1b8vgqg7dst8/TheJerm.rar	2015-09-07 12:34:24	
http://download1489.mediafire.com/bx63qjk6k0bg/z1x1b8vgqg7dst8/TheJerm.rar	2015-09-07 12:35:17	
http://download1489.mediafire.com/bx63qjk6k0bg/z1x1b8vgqg7dst8/TheJerm.rar	2015-09-07 12:35:22	

Figura 90: navegación relacionada con programación de tarjetas de crédito

- En el punto 1, hace una búsqueda en google de *msr 206*. Se trata de un programador de tarjetas bancarias.
- En el punto 2, hace la búsqueda en el portal de subastas *eBay* y presuntamente realiza la compra de uno de ellos:

https://guestcheckout.payments.ebay.es/ws/eBayISAPI.dll?GuestXOProcessor&sessionid=594245756&pagename=rypaddress

http://www.ebay.es/itm/Magnetic-Card-Reader-Writer-Encoder-Stripe-Magstripe-Credit-Compat-MSR206-MSR606-/250903989398?hash=item3a6b0b0c96

- En el punto 3 visualiza un video en el portal *Youtube* en el que explican cómo utilizar el programador y en el que existe un enlace para la descarga del software necesario. Acto seguido, el usuario descarga el software.
- El software descargado es el fichero con malware *TheJerm.rar* (evidencia C20).

Ese mismo día, a las 19:36 descarga el otro fichero con malware, *ListadoNumeraciones.zip*, del servicio online de almacenamiento en nube *WeTransfer* [25].

https://www.wetransfer.com/downloads/481306a6847e3343a084d1ca5d514b3a20150904181722/2dc0a1	2015-09-07 19:35:51 CEST	WeTransfer
https://wetransfer-eu1.s3.amazonaws.com/481306a6847e3343a084d1ca5d514b3a20150904181722?respons...	2015-09-07 19:36:23 CEST	ListadoNumeraciones.zip

Figura 91: descarga del backdoor 'ListadoNumeraciones.zip'

Se adjunta fichero con el historial *places.sqlite* (**evidencia C25**).

8.2.3.15Análisis de malware

8.2.3.15.1 Objetivo

Conocer el propósito y funcionamiento del malware detectado en el equipo.

8.2.3.15.2 Procedimiento

Subimos los ejecutables encontrados dentro de los ficheros comprimidos (evidencias C19 y C20) a la web de análisis de malware *Hybrid-analysis.com* [26].

LlistatNumeracions.exe

Al subir este fichero, nos indica que una vez ejecutado extrae dos ficheros. Uno malicioso y otro limpio:

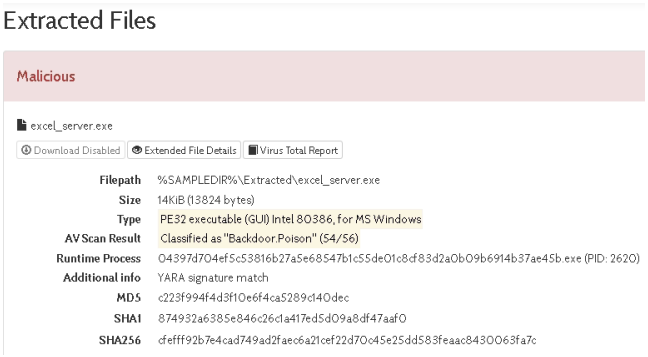


Figura 92: fichero malicioso alojado en Listado numeraciones.exe

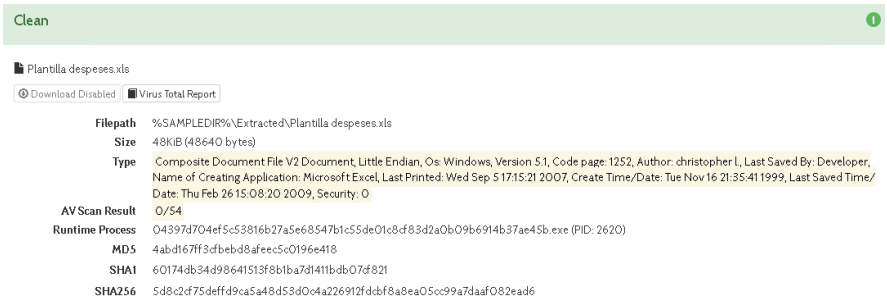


Figura 93: fichero limpio alojado en Listado numeraciones.exe

En *Autopsy* podemos ver estos dos ficheros:

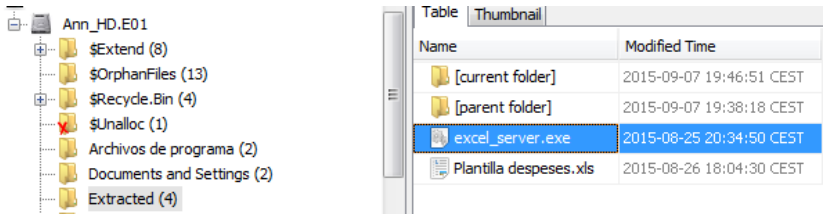


Figura 94: ficheros extraídos de Listado numeraciones.exe

El primero contiene un troyano tipo *Backdoor Poison*.

El segundo una tabla excel con datos financieros:

Plantillas definidas por el usuario en @RISK

Finanzas.xls con una plantilla definida por el usuario

Este modelo demuestra el uso de los reportes definidos por el usuario con plantillas en @RISK. Un reporte de plantilla le permite crear un reporte de simulación directamente en el Excel que contiene sólo la información específica en la cual usted está interesado. Para usar una plantilla primero se tiene que crear una hoja de plantilla que contenga uno o más funciones de estadísticos y/o de gráficos. Asegúrese que el nombre de la hoja de cálculo inicie con el texto (en inglés) "RiskTemplate_". Cuando usted genera sus reportes de @RISK, asegúrese de seleccionar la opción de "Hojas de plantilla". Una copia de la hoja de plantilla se hará para reemplazar todas las funciones con valores. Esto "congela" el reporte de forma tal que en futuras simulaciones no se sobreescriban los resultados que recién han sido creados. De esta manera, usted puede ejecutar muchas simulaciones con la copia correspondiente de la hoja de plantilla para cada una.

VPN (10%) #¿NOMBRE?

Año	2017	2018	2019	2020	2021
Flujo de efectivo					
Total Ingresos	$ -	$ -	#¿NOMBRE?	#¿NOMBRE?	#¿NOMBRE?
Costo de mercadería vendida	$ -	$ -	#¿NOMBRE?	#¿NOMBRE?	#¿NOMBRE?
Margen bruto	$ -	$ -	#¿NOMBRE?	#¿NOMBRE?	#¿NOMBRE?
Gastos operativos	#¿NOMBRE?	#¿NOMBRE?	#¿NOMBRE?	#¿NOMBRE?	$ 20.000,00
Utilidades antes de impuest	#¿NOMBRE?	#¿NOMBRE?	#¿NOMBRE?	#¿NOMBRE?	#¿NOMBRE?
Base de impuestos	#¿NOMBRE?	#¿NOMBRE?	#¿NOMBRE?	#¿NOMBRE?	#¿NOMBRE?

Modelo RiskTemplate_Reporte

Figura 95: contenido del fichero Plantilla despeses.xls

@RISK es una herramienta para el cálculo de riesgos [27] muy apreciada y que tiene un coste elevado. Este documento parece una plantilla de dicho programa.

Por la fecha de creación de este fichero en el sistema, parece que *Ann* lo ejecuto en la fecha: 2015-09-07 19:38:44 (evidencia C8). Según el extracto de la conversación es posible que Ann no supiera que estaba ejecutando un malware:

07/09/2015 19:41	*annetom22*	*Anne G.H.*	*Esto es un poco raro...*
07/09/2015 19:41	*live:rickyrodriguezgarcia*	*Ricky Rodriguez*	*Ups... creo que me he confundido, te lo reenvio más tarde*
07/09/2015 19:41	*annetom22*	*Anne G.H.*	*De acuerdo!*

Por el nombre, es posible que esperara otro tipo de información, como nuevos números de tarjetas de crédito.

TheJerm.exe

Al analizar este fichero, vemos que cuando se ejecuta contacta con una IP de Albania:

Contacted Hosts

Host Address	Host Port	Host Protocol	Host Details
92.60.26.195	1607	TCP	Albania

Figura 96: PI contactada por malware

También crea varios ficheros. El primero de ellos es detectado como una herramienta de hacking de tarjetas de crédito:

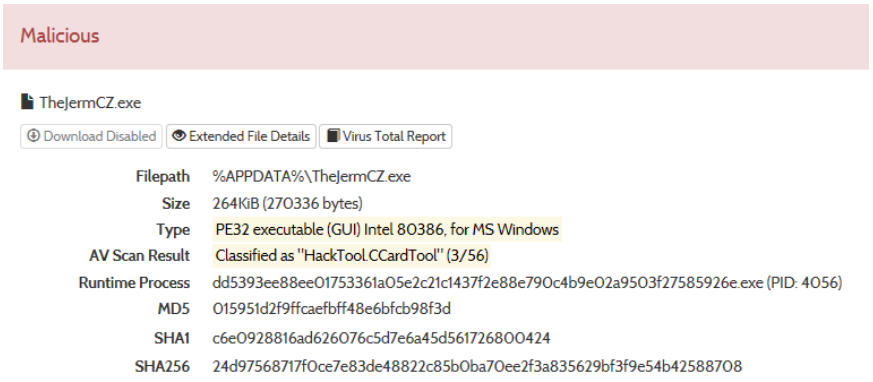


Figura 97: fichero malicioso alojado en Listado numeraciones.exe

El segundo es un enlace directo al fichero *yUmikJMYd3d.exe* y lo mete en el menú de inicio:

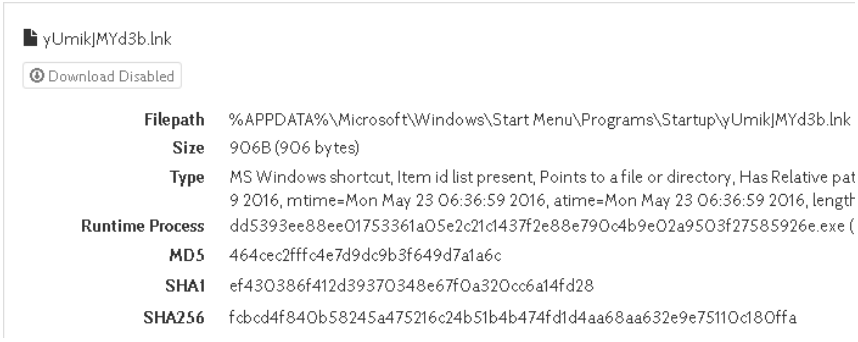


Figura 98: acceso directo al malware

Otro fichero lo crea en el directorio *APPDATA*:

Figura 99: directorio creado por

Si miramos en la imagen del disco duro, vemos que hay creados dos ficheros:

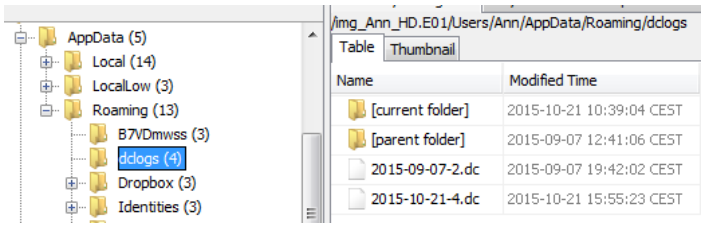


Figura 100: ficheros de texto creados por thejerm.exe

Mirando el contenido del primero, se observa lo que parece un registro de las pulsaciones de las teclas:

```
::  (12:46:25)


:: Enter password for C:\Users\Ann\MyHome (12:47:16)
safePlace
SafePlace

:: pwd.txt: Bloc de notas (12:58:10)


Pwd Tom:
100Pm!710GGh1??6dh**[LEFT][LEFT][LEFT][LEFT][LEFT][LEFT]
LEFT][LEFT][LEFT][LEFT][LEFT][LEFT][LEFT][LEFT][LEFT][LE
T][RIGHT][RIGHT][RIGHT][RIGHT][RIGHT][RIGHT][RIGHT][RIGH
][RIGHT][RIGHT][RIGHT][RIGHT][RIGHT][RIGHT]

:: Program Manager (13:07:21)
□[DEL]

:: pwd.txt: Bloc de notas (13:09:15)
```

El segundo no contiene nada destacable.

Probablemente el malware contenga un *Keylogger* que haya estado registrando las pulsaciones del usuario *Ann* desde que ejecutó el malware.

8.2.3.15.3 Hallazgos

Tras el análisis del malware, podemos determinar lo siguiente:

- El primer fichero (ListadoNumeraciones.zip) contiene un *Backdoor* y una herramienta financiera. El *backdoor* permitiría a un usuario remoto tomar el control del equipo en el que se ejecutara.
- El segundo fichero contiene una herramienta para utilizar un programador de tarjetas de crédito (*msr 206*). Además de esta herramienta, contiene un *keylogger* que probablemente envía la información recolectada a una IP de Albania.

Se adjunta fichero de *logs* con los registros del *Keylogger* (**evidencia C26** del Anexo).

8.2.3.16Análisis de logs del sistema

8.2.3.16.1 Objetivo

Analizar si en los *logs* se encuentran evidencias de cambios de configuración importantes en el sistema, como puede ser el cambio de fecha/hora.

8.2.3.16.2 Procedimiento

Mediante *Autopsy* podemos extraer los ficheros de *logs* de eventos de *Windows* para analizarlos. El directorio donde *Windows 7* almacena estos ficheros es *Windows/System32/winevt/Logs.*

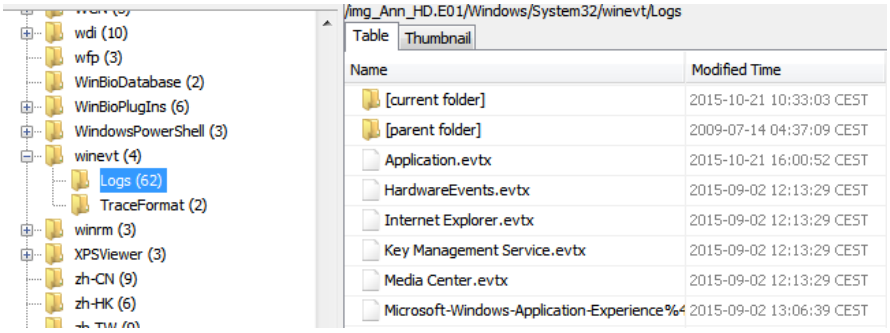


Figura 101: logs de eventos de Windows

Los extraemos y analizamos mediante el visor de eventos del equipo del analista.

En el fichero *Security.evtx* se ha descubierto que se realizó un cambio de fecha y hora del sistema:

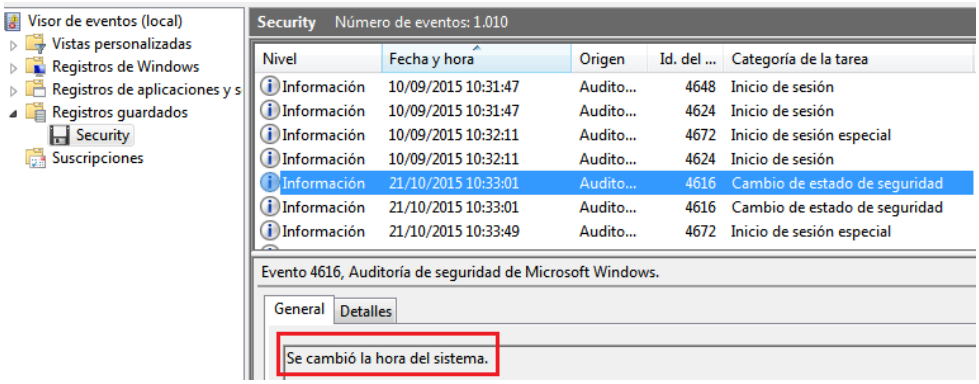


Figura 102: evento de cambio de hora del sistema

Podemos ver los detalles del cambio:

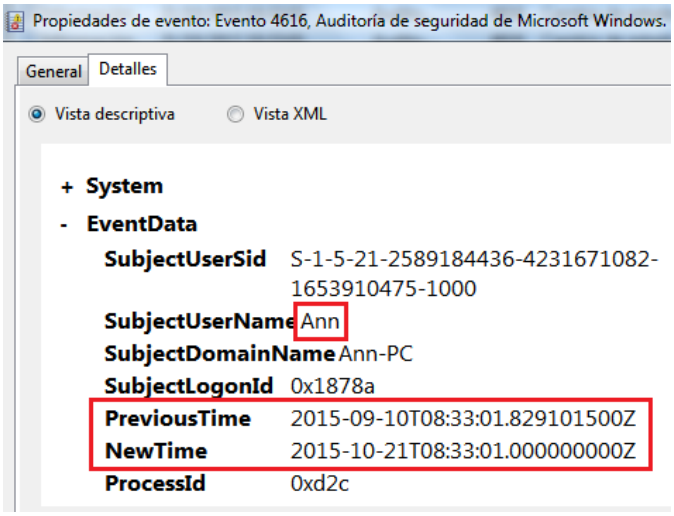


Figura 103: detalles del cambio de hora del sistema

8.2.3.16.3 Hallazgos

Tras el análisis de los *logs* de eventos, se ha descubierto que el usuario ***Ann*** realizó un cambio de fecha y hora del sistema:

- **Hora anterior:** **10/09/2015 08:33:01**
- **Nueva hora:** **21/10/2015 08:33:01**

Se adjunta fichero *Security.evtx* (**evidencia C27**).

Este cambio es muy importante ya que afecta a las fechas de las evidencias posteriores a la fecha del cambio (10/9/2015). A las fechas indicadas en el Anexo habría que restarle **42 días** para adaptarlas a la fecha real.

9 CONCLUSIONES

A continuación se muestran las conclusiones del análisis realizado:

9.1 RESUMEN

Este apartado es un resumen a alto nivel de las evidencias halladas tras el análisis realizado. Para más información, consultad el apartado 9.3.

- Hubo un cambio de hora el 10 de Septiembre de 2015 que afecta a todas las horas recogidas en las evidencias del Anexo. A las fechas de las evidencias posteriores a la fecha del cambio (10/9/2015), hay que restarle 42 días para adaptarlas a la fecha real.
- Se han encontrado ficheros con malware, de tipo *backdoor, troyano* y *keylogger.*
- Se han encontrado conversaciones sobre actividades delictivas:
    - Las primeras fueron mantenidas entre 3 personas 2011-2012.
    - En septiembre de 2015 de produjeron conversaciones entre otras 3 personas presuntamente diferentes a través de Skype.
- Múltiples ficheros con información sobre tarjetas bancarias.
- Evidencia de compra de programador de tarjetas y descarga de programa para usarlo.
- No se han detectado evidencias de que hayan utilizado el programador.
- Tomaron medidas de seguridad en el intercambio y almacenamiento de información.
- Todas las actividades sospechosas fueron realizadas por el usuario del sistema *Ann.*
- No se ha detectado actividad sospechosa del otro usuario del sistema, *Tom*.

9.2 RELACIÓN ENTRE LAS TRES EVIDENCIAS

En este apartado se relacionan algunos de los hallazgos encontrados en los tres análisis realizados: memoria RAM, dispositivo USB y disco duro.

- En la memoria RAM se detectan procesos, ficheros y usuarios detectados también en el disco duro.
- La contraseña de cifrado encontrada en el análisis de la RAM, ha servido para descifrar un volumen encontrado en el análisis del disco duro.
- En la memoria USB se detecta un fichero (*pendientes.ods*) que también se localiza en la papelera de reciclaje del usuario *Ann* en el disco duro. El fichero con las conversaciones de *WhatsApp* encontrado en el mismo dispositivo, podría relacionar los hechos ocurridos en 2011-2012 con los ocurridos en 2015.

Por lo tanto, las tres evidencias se encuentran relacionadas.

9.3 LÍNEA DE TIEMPO

A continuación se muestran los hallazgos más importantes detectados en el análisis, ordenados por su ubicación temporal.

Figura 104: línea de tiempo de hallazgos

No se han incluido las conversaciones de *WhatsApp* al haberse producido con bastante anterioridad a los hechos de 2015. Esto no significa que no estén relacionadas con los hechos mostrados pero no tenemos más evidencias aparte de las conversaciones y se han sacado para no distorsionar la línea temporal.

9.4 RESPUESTA A EXTREMOS

A modo de conclusión, mostramos las respuestas que se han encontrado tras los análisis a los extremos planteados:

E1: ¿Qué procesos en ejecución tenía el portátil en el momento de ser intervenido por la policía?

Cuando el portátil fue intervenido, existía una sesión del usuario *Ann* con los siguientes procesos en ejecución:

- *Skype*
- *yUmikJMYd3b.exe*
- *Winhex*
- *TrueCrypt.exe*
- *Notepad.exe*

Evidencias A1, A2, A3 y A4.

E2: ¿Existe algún tipo de malware en ejecución o instalado en el disco duro? ¿El malware ha sido utilizado por los usuarios del sistema como herramienta o han sido infectados sin saberlo?

Sí, existían al menos 2 tipos de malware instalados en el equipo:

- **TheJerm.exe (evidencia C20) ->** herramienta para programar tarjetas de crédito. Se han encontrado evidencias de que el usuario había adquirido un programador hardware para programar las tarjetas (**C25**), pero no se han encontrado evidencias de que lo haya utilizado.

  Esta herramienta a su vez contiene un malware de tipo *keylogger* que ha almacenado en el disco duro las pulsaciones que ha realizado el usuario *Ann* durante varios días (**C26**). Este *keylogger* establece comunicación con una IP de Albania, probablemente

para enviar los registros obtenidos. No hay evidencias de que el usuario fuese consciente de que estuviera instalado.

- **LlistatNumeracions.exe (C19) ->** *backdoor* oculto en una hoja de cálculo con el cual es posible controlar el sistema de la persona infectada. Se han encontrado evidencias de que el usuario *Ann* descargó el fichero con el troyano desde un servicio de Internet, debido a que el usuario de *Skype, Ricky Rodríguez,* le envió un enlace (**C25**).

  Este fichero podría ser distribuido a posibles víctimas para el robo de los números de tarjetas, pero no se han encontrado evidencias de que el usuario *Ann* ni el usuario *Tom* lo hayan realizado desde el equipo intervenido.

Según la conversación de *Skype* mantenida minutos después de la descarga del fichero, así como el nombre del mismo, es posible que *Ann* esperara otro tipo de información, como nuevos números de tarjetas.

E3: ¿Existen ficheros cifrados en el equipo intervenido? ¿Se ha podido recuperar su contenido?

Si, se ha hallado un volumen cifrado, del cual se ha obtenido la contraseña (**A4**). Se ha conseguido descifrar el volumen, el cual contiene tres ficheros:

- **pwd.txt.txt (C22)**: fichero con contraseñas de cuentas de correo,
- **Tarjetas_Ricky.ods (C23) y TOTAL.ods (C24)**: dos tablas con información sobre tarjetas bancarias.

E4: ¿Qué conexiones de red tenía el portátil en el momento de ser intervenido por la policía?

Las únicas conexiones destacables del equipo son hacia servidores *Skype* y *Dropbox*.

E5: ¿Qué usuarios hay definidos en el SO? ¿Cuáles fueron las fechas de creación y los últimos accesos?

Se han encontrado (**C3**) cuatro usuarios: dos del sistema y otros dos creados en las siguientes fechas:

Usuario	Fecha de Creación	Fecha de último acceso
Administrador	-	14/07/2009 4:53
Invitado	-	-
Ann	02/09/2015 10:17	21/10/2015 13:54
Tom	02/09/2015 10:20	21/10/2015 9:03

Figura 105: tabla de usuarios y fechas de creación y acceso

E6: ¿Cuál de ellos está logado en el momento de la intervención? ¿Estaba estableciendo algún tipo de comunicación con alguna otra persona en el momento de la intervención o antes de ella? ¿Ha sido posible acceder al contenido?

El usuario logado en el momento de la intervención, 21/10/2015 a las 13:55:20, se encontraba logado el usuario *Ann (evidencias **A8 y A9**)*.

Tenía establecida una conexión con el servicio de mensajería instantánea de *Skype*, pero no se han encontrado evidencias de que estuviera manteniendo comunicación con otras personas en ese mismo instante.

E7: ¿Existen evidencias de uso fraudulento de tarjetas de crédito?

Se han encontrado múltiples ficheros con información sobre tarjetas de crédito (**B1, C6, C14, C23, C24**).

Se han encontrado ficheros con conversaciones sobre el uso fraudulento de las tarjetas (**B3 y C9**). La primera conversación es de noviembre de 2011 e intervienen 3 personas diferentes.

- Carlos: <número desconocido>
- Raúl: 34635293190
- Iván: 34660401445

En la conversación hablan de lo que parece un fraude de tarjetas de crédito, en la que una vez robados los números realizan compras que envían a un piso de Mataró. Debido a la fecha y el nombre del directorio donde se ha encontrado la evidencia (*Old_compis*), es probable que esta conversación esté relacionada con actividades presuntamente fraudulentas anteriores a las encontradas en el resto del análisis.

La segunda conversación es de septiembre de 2015 e intervienen tres personas: Ricky Rodríguez, Anne G.H y Aram G.H.

Además se ha detectado en estas conversaciones que el intercambio de los ficheros con los datos de las tarjetas de crédito lo hacían usando técnicas de ofuscación (esteganografía), a través de ficheros de imágenes (**C13)**. De esta conversación se observa que utilizan el servicio en la nube *wetransfer.com* para el intercambio de ficheros.

Para supuestas reuniones, intercambian información con las coordenadas GPS ocultas en fotografías (**C10, C11, C12**).

E8: ¿Existen ficheros eliminados? ¿Se ha podido recuperar su contenido?

Existen miles de ficheros eliminados, pero casi todos ellos son del sistema. Se localizan ficheros PDF eliminados, con nombre de novelas clásicas. Se consigue recuperar uno de ellos (**C7**) y se localiza en su interior información oculta de tarjetas de crédito.

A raíz de este descubrimiento, se localizan más ficheros PDF con información oculta sobre tarjetas de crédito (**C15, C16, C17 y C18)**.

10 BIBLIOGRAFÍA

[1] Módulo 3 de la asignatura: La gestión del proyecto a lo largo del trabajo final

[2] La peritación informática. Un enfoque práctico (Xabiel García Pañeda y David Melendi Palacio), Colegio Oficial de Ingenieros en Informática del Principado de Asturias, ISBN: 978-84-612-4594-9.

[3] http://www.iso.org/iso/catalogue_detail?csnumber=44381

[4] https://support.microsoft.com/en-us/kb/841290

[5] http://www.volatilityfoundation.org/#!25/c1f29

[6] http://www.sleuthkit.org/autopsy/download.php

[7] http://www.csitech.co.uk/skypeex-2/

[8] http://www.openwall.com/john/

[9] https://www.kali.org/releases/kali-linux-20-released/

[10] https://www.elevenpaths.com/es/labstools/foca-2/index.html

[11] https://addons.mozilla.org/es/firefox/addon/sqlite-manager/

[12] http://www.mitec.cz/wrr.html

[13] http://www.cs.vu.nl/~ast/books/mos2/zebras.html

[14] http://nirsoft.net/utils/skype_log_view.html

[15] https://www.x-ways.net/winhex/

[16] https://sourceforge.net/projects/truecrypt/?source=typ_redirect

[17] https://github.com/volatilityfoundation/volatility/wiki/Command%20Reference

[18] https://www.virustotal.com/es/

[19] http://volatility-labs.blogspot.com.es/2014/01/truecrypt-master-key-extraction-and.html

[20] http://who.is/

[21] http://moyix.blogspot.com.es/2008/08/linking-processes-to-users.html

[22] http://arxiv.org/pdf/1507.07739.pdf

[23] http://www.wdc.com/wdproducts/library/SpecSheet/ENG/2879-701278.pdf

[24] http://forums.mozillazine.org/viewtopic.php?f=38&t=2627735

[25] https://www.wetransfer.com/

[26] https://www.hybrid-analysis.com

[27] http://www.palisade-lta.com/risk/

11 ANEXO

En este anexo de enumeran las evidencias encontradas en el análisis forense efectuado.

A1 PSLIST.TXT

- Descripción: listado de procesos en ejecución
- Origen: generado por *volatility* en el apartado 8.2.1.2
- Contenido:

```
D:\TFM>volatility-2.5.standalone.exe -f ANN-PC-20151021-135652.raw --profile=Win7SP1x86 pslist
Volatility Foundation Volatility Framework 2.5
Offset(V)  Name                PID   PPID   Thds     Hnds   Sess  Wow64 Start                      Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x83126730 System                4     0     81      520 ------      0 2015-10-21 13:52:52 UTC+0000
0x83fe7920 smss.exe            212     4      2       29 ------      0 2015-10-21 13:52:52 UTC+0000
0x848db930 csrss.exe           296   288      9      379      0      0 2015-10-21 13:53:02 UTC+0000
0x84a3dd40 wininit.exe         352   288      3       76      0      0 2015-10-21 13:53:04 UTC+0000
0x8490aa58 csrss.exe           364   344      7      242      1      0 2015-10-21 13:53:04 UTC+0000
0x848e9030 winlogon.exe        404   344      3      111      1      0 2015-10-21 13:53:07 UTC+0000
0x8497f030 services.exe        440   352      9      186      0      0 2015-10-21 13:53:07 UTC+0000
0x83f60b38 lsass.exe           456   352      7      583      0      0 2015-10-21 13:53:07 UTC+0000
0x83f64a40 lsm.exe             464   352     10      139      0      0 2015-10-21 13:53:07 UTC+0000
0x84b72d40 svchost.exe         572   440     10      352      0      0 2015-10-21 13:53:08 UTC+0000
0x8498c030 svchost.exe         636   440      8      265      0      0 2015-10-21 13:53:09 UTC+0000
0x84bf5030 svchost.exe         684   440     21      514      0      0 2015-10-21 13:53:09 UTC+0000
0x84c20ad0 svchost.exe         812   440     25      686      0      0 2015-10-21 13:53:10 UTC+0000
0x84c33030 svchost.exe         860   440     36     1015      0      0 2015-10-21 13:53:11 UTC+0000
0x84c3ad40 audiodg.exe         920   684      5      130      0      0 2015-10-21 13:53:11 UTC+0000
0x84c4e728 svchost.exe        1004   440     21      482      0      0 2015-10-21 13:53:12 UTC+0000
0x84c83030 svchost.exe        1176   440     15      382      0      0 2015-10-21 13:53:13 UTC+0000
0x84cb02e0 spoolsv.exe        1280   440     12      278      0      0 2015-10-21 13:53:15 UTC+0000
0x84cbe478 svchost.exe        1316   440     19      298      0      0 2015-10-21 13:53:15 UTC+0000
0x84d0c358 svchost.exe        1400   440     14      220      0      0 2015-10-21 13:53:16 UTC+0000
0x848d5d40 taskhost.exe        368   440      8      197      1      0 2015-10-21 13:54:21 UTC+0000
```

```
0x832054c8 sppsvc.exe          1120    440     7     145     0     0 2015-10-21 13:54:22 UTC+0000
0x84c06810 dwm.exe              552    812     3      68     1     0 2015-10-21 13:54:30 UTC+0000
0x83fc4518 explorer.exe         692    240    25     844     1     0 2015-10-21 13:54:30 UTC+0000
0x849bc770 Skype.exe           1980    692    36    1089     1     0 2015-10-21 13:54:32 UTC+0000
0x84b73030 yUmikJMYd3b.ex       1776    692     6     206     1     0 2015-10-21 13:54:32 UTC+0000
0x832d0d40 SearchIndexer.       1124    440    11     700     0     0 2015-10-21 13:54:39 UTC+0000
0x832c06d0 wmpnetwk.exe          964    440     9     240     0     0 2015-10-21 13:54:44 UTC+0000
0x832ccd40 WinHex.exe            512    692     1      73     1     0 2015-10-21 13:54:46 UTC+0000
0x832c2938 TrueCrypt.exe        2244    692     5     261     1     0 2015-10-21 13:55:00 UTC+0000
0x83230d40 svchost.exe          2336   1776     6     161     1     0 2015-10-21 13:55:06 UTC+0000
0x832b2d40 notepad.exe          2396   2336     3      72     1     0 2015-10-21 13:55:07 UTC+0000
0x833acd40 svchost.exe          2840    440    14     341     0     0 2015-10-21 13:55:20 UTC+0000
0x83353560 WUDFHost.exe         1484    812     8     215     0     0 2015-10-21 13:56:44 UTC+0000
0x83fa0d40 DumpIt.exe           2948    692     2      38     1     0 2015-10-21 13:56:51 UTC+0000
0x83383030 conhost.exe          2668    364     2      52     1     0 2015-10-21 13:56:52 UTC+0000
0x832c5a60 WmiPrvSE.exe         2252    572     6       0     0     0 2015-10-21 13:57:18 UTC+0000
0x834d7538 slui.exe             1456    572     9      16 ------     0 2015-10-21 13:59:27 UTC+0000
0x833d1938 taskeng.exe          2688    860     7 181...59 ------     0 2015-10-21 14:00:00 UTC+0000
0x832689e0 DropboxUpdate.       3644   2688     6      19 ------     0 2015-10-21 14:00:00 UTC+0000
0x834c5a60 DropboxUpdate.       3744   1624     4      98 ------     0 2015-10-21 14:00:00 UTC+0000
0x834e7030 DropboxUpdate.       3856    440    13  6488175 ------     0 2015-10-21 14:00:03 UTC+0000
```

- Tamaño lógico del fichero: 4846 bytes
- Hash del fichero (MD5): b3c7f0fda6f4fe1dd47bdf0fde1f762d

A2 SKYPESESSIONS.TXT

- Descripción: listado de sesiones de *skype*
- Origen: generado por *volatility* en el apartado 8.2.1.5
- Tamaño lógico del fichero: 25665 bytes
- Hash del fichero (MD5): 0fcf5f2ebe92a19ce92b8d0ddd5a4523

A3 EXECUTABLE.1776.ZIP

- Descripción: volcado del proceso *yUmikJMYd3b.exe*
- Origen: generado por *volatility* en el apartado 8.2.1.6
- Tamaño lógico del fichero: 550.821 bytes

- Hash del fichero (MD5): 5afef55644468a20fbaab056cf224a7f
- Contraseña: TFM-Mistic2015

A4 0X833BA1A8_MASTER.KEY

- Descripción: clave maestra de cifrado *TrueCrypt*
- Origen: generado por *volatility* en el apartado 8.2.1.7
- Tamaño lógico del fichero: 64 bytes
- Hash del fichero (MD5): 0b955a82bb2d7d60ee7bc43550764533

A5 NETSCAN.TXT

- Descripción: listado de conexiones de red
- Origen: generado por *volatility* en el apartado 8.2.1.9
- Conenido:

```
D:\TFM>volatility-2.5.standalone.exe -f ANN-PC-20151021-135652.raw --profile=Win7SP1x86 netscan

Volatility Foundation Volatility Framework 2.5

Offset(P)       Proto    Local Address             Foreign Address     State         Pid     Owner          Created

0x3d838308      UDPv4    0.0.0.0:3702              *:*                                 1400    svchost.exe    2015-10-21 13:53:25
 UTC+0000

0x3d8456c0      UDPv4    0.0.0.0:3702              *:*                                 1400    svchost.exe    2015-10-21 13:53:25
 UTC+0000

0x3d845e78      UDPv4    0.0.0.0:3702              *:*                                 1400    svchost.exe    2015-10-21 13:53:25
 UTC+0000

0x3d845e78      UDPv6    :::3702                   *:*                                 1400    svchost.exe    2015-10-21 13:53:25
 UTC+0000

0x3d8529f0      UDPv4    0.0.0.0:3702              *:*                                 1400    svchost.exe    2015-10-21 13:53:25
 UTC+0000

0x3d8529f0      UDPv6    :::3702                   *:*                                 1400    svchost.exe    2015-10-21 13:53:25
 UTC+0000

0x3da09e08      UDPv4    127.0.0.1:59891           *:*                                 1980    Skype.exe      2015-10-21 13:55:10
 UTC+0000

0x3da70e38      UDPv4    192.168.1.35:68           *:*                                 684     svchost.exe    2015-10-21 14:00:05
 UTC+0000

0x3db389f8      UDPv4    0.0.0.0:49153             *:*                                 1400    svchost.exe    2015-10-21 13:53:17
 UTC+0000

0x3db389f8      UDPv6    :::49153                  *:*                                 1400    svchost.exe    2015-10-21 13:53:17
 UTC+0000

0x3db3b168      UDPv4    0.0.0.0:49152             *:*                                 1400    svchost.exe    2015-10-21 13:53:17
```

```
UTC+0000
0x3db48180      UDPv4   0.0.0.0:5355            *:*                     1176    svchost.exe     2015-10-21 13:55:27
UTC+0000
0x3db48180      UDPv6   :::5355                 *:*                     1176    svchost.exe     2015-10-21 13:55:27
UTC+0000
0x3dbbaca0      UDPv4   192.168.1.35:137        *:*                     4       System          2015-10-21 13:53:18
UTC+0000
0x3dbc0310      UDPv4   192.168.1.35:138        *:*                     4       System          2015-10-21 13:53:18
UTC+0000
0x3da19708      TCPv4   0.0.0.0:49153           0.0.0.0:0       LISTENING       684     svchost.exe
0x3da1a498      TCPv4   0.0.0.0:49153           0.0.0.0:0       LISTENING       684     svchost.exe
0x3da1a498      TCPv6   :::49153                :::0            LISTENING       684     svchost.exe
0x3daa1508      TCPv4   0.0.0.0:49154           0.0.0.0:0       LISTENING       860     svchost.exe
0x3db333d0      TCPv4   0.0.0.0:5357            0.0.0.0:0       LISTENING       4       System
0x3db333d0      TCPv6   :::5357                 :::0            LISTENING       4       System
0x3db7c6b8      TCPv4   0.0.0.0:445             0.0.0.0:0       LISTENING       4       System
0x3db7c6b8      TCPv6   :::445                  :::0            LISTENING       4       System
0x3db9a220      TCPv4   0.0.0.0:49155           0.0.0.0:0       LISTENING       440     services.exe
0x3db9a220      TCPv6   :::49155                :::0            LISTENING       440     services.exe
0x3db9a4a0      TCPv4   0.0.0.0:49155           0.0.0.0:0       LISTENING       440     services.exe
0x3dbbad58      TCPv4   0.0.0.0:49156           0.0.0.0:0       LISTENING       456     lsass.exe
0x3dbbad58      TCPv6   :::49156                :::0            LISTENING       456     lsass.exe
0x3dbc1488      TCPv4   192.168.1.35:139        0.0.0.0:0       LISTENING       4       System
0x3ddc67d8      TCPv4   0.0.0.0:135             0.0.0.0:0       LISTENING       636     svchost.exe
0x3ddc67d8      TCPv6   :::135                  :::0            LISTENING       636     svchost.exe
0x3ddcc1e8      TCPv4   0.0.0.0:135             0.0.0.0:0       LISTENING       636     svchost.exe
0x3ddf4008      TCPv4   0.0.0.0:49152           0.0.0.0:0       LISTENING       352     wininit.exe
0x3ddf4008      TCPv6   :::49152                :::0            LISTENING       352     wininit.exe
0x3ddf4670      TCPv4   0.0.0.0:49152           0.0.0.0:0       LISTENING       352     wininit.exe
0x3dee50f0      UDPv4   0.0.0.0:5355            *:*                     1176    svchost.exe     2015-10-21 13:55:27
UTC+0000
0x3df47668      UDPv4   0.0.0.0:0               *:*                     1176    svchost.exe     2015-10-21 13:53:19
UTC+0000
0x3df47668      UDPv6   :::0                    *:*                     1176    svchost.exe     2015-10-21 13:53:19
UTC+0000
0x3e4b22d8      TCPv4   0.0.0.0:49154           0.0.0.0:0       LISTENING       860     svchost.exe
0x3e4b22d8      TCPv6   :::49154                :::0            LISTENING       860     svchost.exe
0x3e6d85e8      TCPv4   0.0.0.0:49156           0.0.0.0:0       LISTENING       456     lsass.exe
0x3e9df2d8      UDPv4   0.0.0.0:50903           *:*                     1176    svchost.exe     2015-10-21 14:00:16
UTC+0000
```

0x3e8a98c8 TCPv4 192.168.1.35:49208 109.236.36.217:1607 ESTABLISHED 2336 svchost.exe

0x3f41e160 UDPv4 127.0.0.1:1900 *:* 1400 svchost.exe 2015-10-21 13:54:56

UTC+0000

0x3f420e38 UDPv4 192.168.1.35:1900 *:* 1400 svchost.exe 2015-10-21 13:54:56

UTC+0000

0x3f4f45a8 UDPv6 ::1:1900 *:* 1400 svchost.exe 2015-10-21 13:54:56

UTC+0000

0x3f5092b0 UDPv4 127.0.0.1:65206 *:* 1980 Skype.exe 2015-10-21 13:55:10

UTC+0000

0x3f50c538 UDPv4 0.0.0.0:26120 *:* 1980 Skype.exe 2015-10-21 13:55:20

UTC+0000

0x3f518158 UDPv4 0.0.0.0:0 *:* 1980 Skype.exe 2015-10-21 13:55:11

UTC+0000

0x3f51ae10 UDPv4 192.168.1.35:62639 *:* 1400 svchost.exe 2015-10-21 13:54:56

UTC+0000

0x3f520920 UDPv6 fe80::288b:c128:c611:e0a:62637 *:* 1400 svchost.exe 2015-10-21 13:54:56

UTC+0000

0x3f569190 UDPv4 0.0.0.0:3702 *:* 1004 svchost.exe 2015-10-21 13:54:51

UTC+0000

0x3f56cda8 UDPv6 ::1:62638 *:* 1400 svchost.exe 2015-10-21 13:54:56

UTC+0000

0x3f582a08 UDPv4 0.0.0.0:3702 *:* 1004 svchost.exe 2015-10-21 13:54:51

UTC+0000

0x3f594380 UDPv4 0.0.0.0:443 *:* 1980 Skype.exe 2015-10-21 13:55:20

UTC+0000

0x3f5d1158 UDPv4 127.0.0.1:62640 *:* 1400 svchost.exe 2015-10-21 13:54:56

UTC+0000

0x3f5e06c8 UDPv4 0.0.0.0:62636 *:* 1004 svchost.exe 2015-10-21 13:54:51

UTC+0000

0x3f5e06c8 UDPv6 :::62636 *:* 1004 svchost.exe 2015-10-21 13:54:51

UTC+0000

0x3f5e0950 UDPv4 0.0.0.0:62635 *:* 1004 svchost.exe 2015-10-21 13:54:51

UTC+0000

0x3f5e0c80 UDPv4 0.0.0.0:3702 *:* 1004 svchost.exe 2015-10-21 13:54:51

UTC+0000

0x3f5e0c80 UDPv6 :::3702 *:* 1004 svchost.exe 2015-10-21 13:54:51

UTC+0000

0x3f5e0df0 UDPv4 0.0.0.0:3702 *:* 1004 svchost.exe 2015-10-21 13:54:51

UTC+0000

0x3f5e0df0 UDPv6 :::3702 *:* 1004 svchost.exe 2015-10-21 13:54:51

```
UTC+0000
0x3f5e2400      UDPv6   fe80::288b:c128:c611:e0a:1900  *:*                    1400    svchost.exe    2015-10-21 13:54:56
UTC+0000
0x3f4db560      TCPv4   0.0.0.0:80              0.0.0.0:0       LISTENING       1980    Skype.exe
0x3f5183f0      TCPv4   0.0.0.0:26120           0.0.0.0:0       LISTENING       1980    Skype.exe
0x3f531d80      TCPv4   0.0.0.0:443             0.0.0.0:0       LISTENING       1980    Skype.exe
0x3f490810      TCPv4   192.168.1.35:49198      91.190.219.143:443  CLOSED      1980    Skype.exe
0x3f4c4008      TCPv4   -:49184                 185.43.182.25:80    CLOSED      1980    Skype.exe
0x3f4cea18      TCPv4   -:49191                 185.43.182.25:80    CLOSED      1980    Skype.exe
0x3f4ea008      TCPv4   -:49190                 -:443           CLOSED      1980    Skype.exe
0x3f50a7f8      TCPv4   192.168.1.35:49228      224.0.0.252:80      CLOSED      1980    Skype.exe
0x3f52edf8      TCPv4   192.168.1.35:49174      157.56.53.50:12350  ESTABLISHED     1980    Skype.exe
0x3f540008      TCPv4   192.168.1.35:49172      157.55.130.159:40013 ESTABLISHED    1980    Skype.exe
0x3f594008      TCPv4   192.168.1.35:49253      108.160.172.236:443  ESTABLISHED    3856    DropboxUpdate.
0x3f59f3a8      TCPv4   192.168.1.35:49173      157.56.193.45:443   ESTABLISHED     1980    Skype.exe
0x3f5b0008      TCPv4   -:49177                 -:80            CLOSED      1980    Skype.exe
0x3f5c2008      TCPv4   192.168.1.35:49256      91.190.219.143:443  CLOSED      1980    Skype.exe
```

- Tamaño lógico del fichero: 10864 bytes
- Hash del fichero (MD5): 379f3a536b3dc2c63f718622179b9fc4

A6 HASHDUMP.TXT

- Descripción: volcado de usuarios y contraseñas cifradas
- Origen: generado por *volatility* en el apartado 8.2.1.10
- Contenido:

```
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Ann:1000:aad3b435b51404eeaad3b435b51404ee:8a24d5beb0d94c03ffec1e186a1f88b0:::
Tom:1001:aad3b435b51404eeaad3b435b51404ee:35509e7f0e2d9b0b7f60c40b37a1f559:::
```

- Tamaño lógico del fichero: 327 bytes
- Hash del fichero (MD5): 45285ca9c2b35080546a0e10e036b80a

A7 JOHN.POT

- Descripción: listado de contraseñas descifradas
- Origen: generado por *john the ripper* en el apartado 8.2.1.10
- Contenido:

```
$NT$31d6cfe0d16ae931b73c59d7e0c089c0:
```

```
$NT$35509e7f0e2d9b0b7f60c40b37a1f559:Ann1978

$NT$8a24d5beb0d94c03ffec1e186a1f88b0:Tom1980
```

- Tamaño lógico del fichero: 128 bytes
- Hash del fichero (MD5): f08e84e3588e0d2e8c8498bc843beb26

A8 SESSIONS.TXT

- Descripción: listado de sesiones de usuarios
- Origen: generado por *volatility* en el apartado 8.2.1.11
- Contenido:

```
D:\TFM>volatility-2.4.standalone.exe -f ANN-PC-20151021-135652.raw --profile=Win7SP1x86

sessions

Volatility Foundation Volatility Framework 2.4

**************************************************

Session(V): 89e68000 ID: 0 Processes: 26

PagedPoolStart: 80000000 PagedPoolEnd ffbfffff

 Process: 296 csrss.exe 2015-10-21 13:53:02 UTC+0000

 Process: 352 wininit.exe 2015-10-21 13:53:04 UTC+0000

 Process: 440 services.exe 2015-10-21 13:53:07 UTC+0000

 Process: 456 lsass.exe 2015-10-21 13:53:07 UTC+0000

 Process: 464 lsm.exe 2015-10-21 13:53:07 UTC+0000

 Process: 572 svchost.exe 2015-10-21 13:53:08 UTC+0000

 Process: 636 svchost.exe 2015-10-21 13:53:09 UTC+0000

 Process: 684 svchost.exe 2015-10-21 13:53:09 UTC+0000

 Process: 812 svchost.exe 2015-10-21 13:53:10 UTC+0000

 Process: 860 svchost.exe 2015-10-21 13:53:11 UTC+0000

 Process: 920 audiodg.exe 2015-10-21 13:53:11 UTC+0000

 Process: 1004 svchost.exe 2015-10-21 13:53:12 UTC+0000

 Process: 1176 svchost.exe 2015-10-21 13:53:13 UTC+0000

 Process: 1280 spoolsv.exe 2015-10-21 13:53:15 UTC+0000

 Process: 1316 svchost.exe 2015-10-21 13:53:15 UTC+0000

 Process: 1400 svchost.exe 2015-10-21 13:53:16 UTC+0000

 Process: 1120 sppsvc.exe 2015-10-21 13:54:22 UTC+0000

 Process: 1124 SearchIndexer. 2015-10-21 13:54:39 UTC+0000

 Process: 964 wmpnetwk.exe 2015-10-21 13:54:44 UTC+0000
```

```
Process: 2840 svchost.exe 2015-10-21 13:55:20 UTC+0000
Process: 1484 WUDFHost.exe 2015-10-21 13:56:44 UTC+0000
Process: 2252 WmiPrvSE.exe 2015-10-21 13:57:18 UTC+0000
Process: 2688 taskeng.exe 2015-10-21 14:00:00 UTC+0000
Process: 3644 DropboxUpdate. 2015-10-21 14:00:00 UTC+0000
Process: 3744 DropboxUpdate. 2015-10-21 14:00:00 UTC+0000
Process: 3856 DropboxUpdate. 2015-10-21 14:00:03 UTC+0000
Image: 0x83f132b0, Address 8c450000, Name: win32k.sys
Image: 0x84949ae8, Address 8c6a0000, Name: dxg.sys
Image: 0x849bac88, Address 8c6d0000, Name: TSDDD.dll
**************************************************
Session(V): 89e70000 ID: 1 Processes: 14
PagedPoolStart: 80000000 PagedPoolEnd ffbfffff
Process: 364 csrss.exe 2015-10-21 13:53:04 UTC+0000
Process: 404 winlogon.exe 2015-10-21 13:53:07 UTC+0000
Process: 368 taskhost.exe 2015-10-21 13:54:21 UTC+0000
Process: 552 dwm.exe 2015-10-21 13:54:30 UTC+0000
Process: 692 explorer.exe 2015-10-21 13:54:30 UTC+0000
Process: 1980 Skype.exe 2015-10-21 13:54:32 UTC+0000
Process: 1776 yUmikJMYd3b.ex 2015-10-21 13:54:32 UTC+0000
Process: 512 WinHex.exe 2015-10-21 13:54:46 UTC+0000
Process: 2244 TrueCrypt.exe 2015-10-21 13:55:00 UTC+0000
Process: 2336 svchost.exe 2015-10-21 13:55:06 UTC+0000
Process: 2396 notepad.exe 2015-10-21 13:55:07 UTC+0000
Process: 2948 DumpIt.exe 2015-10-21 13:56:51 UTC+0000
Process: 2668 conhost.exe 2015-10-21 13:56:52 UTC+0000
Process: 1456 slui.exe 2015-10-21 13:59:27 UTC+0000
Image: 0x843bc120, Address 8c450000, Name: win32k.sys
Image: 0x848da140, Address 8c6a0000, Name: dxg.sys
Image: 0x848365d8, Address 8c750000, Name: framebuf.dll
```

- Tamaño lógico del fichero: 3024 bytes
- Hash del fichero (MD5): d395af9fd873097b26c6603d78f4865e

A9 GETSIDS.TXT

- Descripción: identificador del usuario con la sesión activa
- Origen: generado por *volatility* en el apartado 8.2.1.11
- Contenido:

```
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Ann:1000:aad3b435b51404eeaad3b435b51404ee:8a24d5beb0d94c03ffec1e186a1f88b0:::
Tom:1001:aad3b435b51404eeaad3b435b51404ee:35509e7f0e2d9b0b7f60c40b37a1f559:::
```

- Tamaño lógico del fichero: 2525 bytes
- Hash del fichero (MD5): f2c7c1991b3ed631c5bf687aaacbf1c2

B1 PENDIENTES.ODS

- Descripción: hoja de cálculo con información de tarjetas de crédito
- Origen: extraído del dispositivo USB mediante *Autopsy* en el apartado 8.2.2.3
- Contenido:

Visa	4539456154526870	Concepcion	Perez Pozo
Visa	4532457001051150	Jose Maria	Rodriguez Martinez
Visa	4532657981372410	Ignacio	Torres Fernandez
Visa	4379166568413640	Gabriel	Riba Villar
Visa	4929653751795980	Pilar	Moreno Hernandez
Visa	4532531411046010	Alfonso	Mendez Sanchez
Visa	4485384240029660	Esteban	Reyes Sierrra
Visa	4532227440905600	Juan Antonio	Prado Romero
Visa	4539798471108420	Elvira	Sanchez Diez
Visa	4916277839380970	Federico	Iglesias Ruiz
American Express	372171730251559	Marcos	Rubio Ortiz
American Express	376905910360151	Juan Jose	Roca Moyano
American Express	347170350508035	Adolfo	Castillo Valles
American Express	347899917772631	Ana	Silva Guzman
American Express	372157992412443	Rodolfo	Mora Canales
MasterCard	5187401714297720	Angeles	Cerezo Rojas
MasterCard	5197841039013650	Jesus	Gaspar Barba
MasterCard	5108656187294160	Andres	Cifuentes Bautista

- MAC time:
    - Modified 2016-01-15 20:35:12 CET
    - Accessed 2016-01-15 00:00:00 CET
    - Created 2016-01-15 20:35:20 CET
    - Changed 0000-00-00 00:00:00
- Tamaño lógico del fichero: 15766 bytes
- Hash del fichero (MD5): 6da97888ff474194bedc0cf99b5f67de

B2 *WHATSAPP*_IMAGE.PNG

- Descripción: Imagen enviada por *WhatsApp*
- Origen: extraído del dispositivo USB mediante *SQLite Manager* en el apartado 8.2.2.3
- Contenido:

Figura 106: imagen enviada por WhatsApp

- Tamaño lógico del fichero: 9869 bytes
- Hash del fichero (MD5): aa45db3d848ac089a3eacb37a143241d

B3 *WHATSAPP*.DB

- Descripción: BBDD con conversaciones *WhatsApp*
- Origen: extraído del dispositivo USB mediante *Autopsy* en el apartado 8.2.2.4
- Contenido:

key_remote_jid	data	remote_resource	timestamp	
99999999543-9999999997@g.us	Buenos días! hablamos de como llevamos el tema de las tarjetas o no os atrevéis....		09/11/2011	23:10:25
99999999543-9999999997@g.us	?		09/11/2011	23:14:09
99999999543-9999999997@g.us	Jajajajajajajaja	34635293190@s.*WhatsApp*.net	09/11/2011	23:14:32
99999999543-9999999997@g.us	Si si! hablemos que ya lo tenemos todo medio preparado no?	34635293190@s.*WhatsApp*.net	09/11/2011	23:14:33
99999999543-9999999997@g.us	Sip	34660401445@s.*WhatsApp*.net	09/11/2011	23:19:12

99999999543-9999999997@g.us	bien, entonces todo como acordamos, yo consigo los números y los pins, Raúl tu haces las compras por internet y Iván te enviamos la mercancía al piso falso de Tarragona con el dni falso que tienes. Hasta aquí todo claro como siempre..."		09/11/2011	23:20:06
99999999543-9999999997@g.us	Ningún problema, tu pásame los números y pins. Voy a un cibercafé de Mataró y empiezo a hacer compras a saco!!!	34635293190@s.*WhatsApp*.net	09/11/2011	23:20:09
99999999543-9999999997@g.us	Jajajaajajajajaja	34635293190@s.*WhatsApp*.net	09/11/2011	23:20:17
99999999543-9999999997@g.us	Sk sin noo son nddd	34635293190@s.*WhatsApp*.net	09/11/2011	23:20:23
99999999543-9999999997@g.us	eps tranquilo eh! que si haces compras ten en cuenta que solo puedo ir al piso de Tarragona cuando sepa que los propietarios no son! así que las entregas solo pueden ser los viernes por la mañana!! o la liamos..."	34660401445@s.*WhatsApp*.net	09/11/2011	23:20:32
99999999543-9999999997@g.us	OK Iván, oído cocina! cuando haga las compras todas las entregas serán el mismo viernes, yo te aviso!	34635293190@s.*WhatsApp*.net	09/11/2011	23:20:34
99999999543-9999999997@g.us	Amén		09/11/2011	23:23:55
99999999543-9999999997@g.us	OK dejarme trabajar un poco el phising y las alternativas para conseguir más tarjetas... os digo algo		09/11/2011	23:27:10
99999999543-9999999997@g.us	/9j/4AAQSkZJRgABAQAAAQABAAD/2wBDAAYEBQYFBAYGBQYHBwYIChAKCgkJChQODwwQFxQYGBcUFhYaHSUfGhsjHBYWICwgIyYnKSopGR8tMC0oMCUoKSj/2wBDAQcHBwoIChMKChMoGhYaKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCj/wAARCABkAEgDASIAAhEBAxEB/8QAHwAAAQUBAQEBAQEAAAAAAAAAAAECAwQFBgcICQoL/8QAtRAAAgEDAwIEAwUFBAQAAAF9AQIDAAQRBRIhMUEGE1FhByJxFDKBkaEII0KxwRVS0fAkM2JyggkKFhcYGRolJicoKSo0NTY3ODk6Q0RFRkdISUpTVFVWV1hZWmNkZWZnaGlqc3R1dnd4eXqDhIWGh4iJipKTlJWWl5iZmqKjpKWmp6ipqrKztLW2t7i5usLDxMXGx8jJytLT1NXW19jZ2uHi4+Tl5ufo6erx8vP09fb3+Pn6/8QAHwEAAwEBAQEBAQEBAQAAAAAAAAECAwQFBgcICQoL/8QAtREAAgECBAQDBAcFBAQAAQJ3AAECAxEEBSExBhJBUQdhcRMiMoEIFEKRobHBCSMzUvAVYnLRChYkNOEl8RcYGRomJygpKjU2Nzg5OkNERUZHSElKU1RVVldYWVpjZGVmZ2hpanN0dXZ3eHl6goOEhYaHiImKkpOUlZaXmJmaoqOkpaanqKmqsrO0tba3uLm6wsPExcbHyMnK0tPU1dbX2Nna4uPk5ebn6Onq8vP09fb3+Pn6/9oADAMBAAIRAxEAPwD6ZsQDZQHHWNf5VPtHoKg0/wD48Lb/AK5L/KrFQIbtHpRtHpQxwpNcrdeILqKZ41jDbDjOQM/pUTmoasV9jqwB6UuB6VxJ8WT+d5OIhNt3bPMG7HrjHSnReLJpC6qqMyHawVdp64fVU/hTfIhPWJP++RWou++BRU/aiqAq6d/wA+2bf/AK5r/Kp6AGv90/SvOr9n+3T7WTG7o9pUQjXdypzyBrnxCvFFQdmcTawh8TmSJ1WRJVspAw4VXTJvHYMwYH6Adu9bem27W95fvFcxO9w4du+pPPGcHOM9qR0ZO9wOIxkjWWMo+++selang+8F7f3EzTGyvPY3Bc1klHVAuUOHXAFLhwHSnRNpJVpFDNApSivS9TTvAWsl4VTzvdjYC+XFemoiWCkpU3Vv0kNBIBnY35VnOPMrAeQ6mtxFdPINuZZoHIeRoiVcMBgYHcYx+tYOkr8W9MEWmTG1m7M1W2YnsAEu3DhlhtM3bmRqAEFTVa/jhjJHwPvdz6ZXrXmNhX4zpvYEjOkcMrkfcXHMbkbHAAFhWwxw5yJBL8vZVcF3t8TKuwbJlIhvv1Ewl+6HMdTDo4FXCmyKY7qvuJ8KH5vgFujMi+eUUGt9vpnaRK+CBhdUnhNmZQ3uekV7ak3/+BrXt5xn4wqzgtkgeCYsOCdzPdb9yHmEfzUz5RgXE5ESNzxXtA0YXpcjgxYtYV2sHSHwdthB0KPFYtqm9P5dpF3F2rVHQR/UOlJDaqWYhTKrJYB01BDCimSNUYF/RgD8bAqHEHnwXF/rP2gebzfjTaqEbVUXAuRSHaMYIbw4hZ9LxBmfkHAHqvjd0i7tkTH8M70+C8ocTd4ja/9tdXrvlv9xoPTWPkKwWv1iPtUTxc1iuAh2hNDfa+2Zd2kPCsuTYcVWJw4d4jdYCEFNgu0MXpldMwFzOEjqqv/t3b9d/tJQsAP0IEOwsWpQmlCZuh4yc7etxrr8LF3m7vf7XI+n0d/n+12+2h9kq9b67t2mw8Uy8NqQm5WbJ1KXY4ooTKhHXtA0XiAU5DHUMnZ/0NP0TzFMHc3jGjdW+Qvj2zMXwgnBwtdTbjXkTaBx0RXVqq3UxM6Dg9YOyxhEIhrHoXqrv5uD8eCY7wW9cNfIa7gp3WzI9Tp3O91pwTvmFYzmUnB4CWRhwBKAqKGFaV6fBvw5fLlsFMaYdtBcpm7YEqYuz8eNBQq4EPcxhS+TOIEN8BfQmA4V3O5NMjLTZ1b8uSs2YyZ2HlW8EbRs2eXAGwSeycoFxmuS9ucfMoOcXjt1GBhbA3cmzVdYR2hGo0nnQ1jFoKNDFumNAaXLeV6s3U+VC8KfW3ZM7+jHbzgxIqp1OORmnXa7bRxjQl9wm9UiXnVhAjSE1hXtX2yqI27dR1a3NhAJbtPYU0Udqq5DV7XfMkUw/0v0KoaeBLv3P+yiv2V2g16l1JNwDUsw+YbrO6oEUZOOD37yXDX/m5ciQAjLeXfXgCUEGHKE/mL/v8BqJuiU+MaC9jRN0o21pMV3B2+TW6b6JgqkyIEJ7SHLDjzTRxqFUIyMHJgdYo6hsEkSNXd/LzUwBWomgl/vRzdYTnsUoW5D/JZ7vX/YMs3T/ZfiddHXZ1LhrEcdHhUjYsK/4AVZjyCRppN+GIMnN2r+o0KvqnI4dE3Y1ZbXmPdLLjNKXRuzoJVwvaiVuqI8d/ns8NiYVgr0E2nNl8k/zwXvCYgdhb9M7ScQ0z0ScMAnFaXCZ6y3eH9iW3+g9O8dWBYPo/RyrAv4e/tn3/7ijjBmdFsFnbEfvl3q7CBP40RShtCFOaurQfObiEO2Ikb6pQMDpwZDtP8TKnCUVJKShPdHlZRR9yoMTX4Kv9PKEh3v9jiGqTPlEBLlGM7hcVhIEoH1fK+W8yGt8HyjKsTyj6eqxOA4HjhbaJCPUpBKE2Pqjt3JIgDczkfBMPUvwPm0r1E8L0ua9WhnvqgfBi0smOlvP3lkaAbuyUV8vlMIs9sl/e3j2P0vXBnl2Cvp+7DjUuk7u96DyGNRyWVkW2drLJfWzD/UEzpNSAVo+FNkgu7hnfxx6DqP8WLYwplovrKbbIZjH6+A3YkvY3XXvc8MnKLXcyUq3vJHNFFj/3cwcwrBnwLOh1V9vIm9gc3YRjb23mjHSOBZ8TAh9DoyNBKqlJdJO7mvkTIffUHiIgHCvI/Ya8UjvNZlXI7RJ2wkrcyhJQoz3eS3g3Gj90tSnnJ9LbRf9D8Vg08TeUPmiDTUGm9VOUqvd5gHH/l86ekWk6tdnDWqN95P4n7yHuq6oDcdeBW7szADdANd+c2j1YpV3tY+e2hvkBcWC0mW+HrKG1aKmR5cKg8PnEnwoMQVhpEN0TcLyw7uyB0gt+dPFBbOxwyd08e0c80vXTG9tGN4PVrdVtrn5GSBHmF0I90Z7B84AAyQ7trJ9CxR1aFs1fs7oYK2uZ43/55J4Nyd1Js/gxAebLFbKHKg4HFbaq1q6PbW4sbZ9CmDdrVmcAaOp9S8BtfLcHw/uhd4h1UIX1a1WxoHqXx8Ndtv2OKOXKNNn0j8kcOp/TT5fspp3Xtrqg/WQZ9HdHAhBuz0m6KnSxz09mCPVgg0uWBwAEBhcHyYxbY21tSHWpzFuWxPQ8yiSe/J1vAwxfKh7AeOGvvBnJGBtPWSqShIPaOxmD3GKiCs0vVR33sM9OkCm/hMgXkTn8yQxCm2J+QgNCpTHMXHJO0i9xzyGa81j6/eD0G0LSbDD/PGOrzN6aPtobajENMz7H4cUp4G3KwBAV5RGaeNQTKBmpQp+/4wQqfq8Kf0OQXWkR7PzU9qrXeIgq4RGahDNcvhz07V9sU42gXZB3z6OVvlyxjiOIWp/jN/8VVbT/O9qSJjrwvnzU4hdhXB6hQmL9OyNlW5e2LKWZp25RfJHjVqLEAh6oNWmsPuHV6hmhy3hU4fijOL12jwHvsGK7UI7uBAqu3IJkIvqhw8Vb4BGpNo+NyATNPMf/7k/qGZFIZmKhJtzn+hQ2xMFJD7SOmIShAHc5uLhbR/OyxMyIeXf7yjvFDvC3OHJvxMrH41wZx6rkeSjwcWa0Vf/uSi8IJ9jJPC0Yr7f6dcwNWXcHl9QmP3wRCu0AtgZc9TaROAp0qI45bbdO5U23UGJ6gNDfrL+2Lz4+iVklsLU7ymyOkmNGL3MRXqTzQmx5RTNsBU0VNcTLj0EZmrE4+J8wL+NHdGFyNaM9dMHlSWI5BoKXB+TNbG6jWDMqZbnPwOoqgVCvqaf1KZyrETIgkrUUw/oN87eRVtcrFBKUyF00VhvBJZdC2d5yW9eibn5G30hNIHWvjiMOWXSIJbv3SNjOjB3RtJNKsn44HSAnKpfMtoarbGj9pokLBxqu9TBRp7jRfrK1HB6u0AENFh5yVKfiCqFHQ7a+hCCqPFPB6vqlrRz21ZZ9JPzD/bSPZR12QdeDr8bkLh5nDuPS9mgZMXDl7oncUm0a3cXk4QEOSb6+Dlb5B7g9k3tJ07JkJ+s1HfRW0SZngXBl9QTSgXc7GFs2u/cDYgrBfuSbRuJqeZYoqdUTzS4N58HScCxZamG4l7b3MNL2HXDP8X5ueltbbvR7yQ61lXLLbh3RlL53Hw1Oc7XPu4evtU0A2lHYOMQ/+2UNYCw4LHb8ARENtHSDxYCYIrOGFR/QgoDZ1SFXAZFBaWTeSAlEHzFzL+CwJTc4T6KwNSv1gwTHHsmlhq/6f8wUIsaqRKFASWyaoOB6UjL1vaFLYY4uHzSEOaHGTLKdfzy6x9EOSpIYpLwBo3MwrXqWq+PGFXMX6s6ah4d69aBtFdvMQHNsLHs8c2X4JA0NQoDt4Ov5vPx9IOLS5eMWdDH5aiS/0yqEm0pKOkJIImk/6TOAxABSu9TBuKJYn4Z0IbxvOCZvBwOLuvBaGAwD1+fYI8qyuJcsWXYUBCDL5nMJpzIKT2T56U/Ebyn1Uc2x3W3E5mdDoqRfkGP8z2FG5hK6e3gAT+Twrr+rYvxTbYMn0HjJzuZdyNQRO3VLhZ9hXMsmv4xoOaWxA28rW+IvwFbn40+4h27xHUP4jo3vOjpbVIhwP+A7D9WIwBsTUJb7BXvj5gbJ4w0Aa7EVQi/ZmZmCZp4S9g1xyYKYmlZEKq9t8KRIK1ltsUKsmmY3LzpMGBW3ENcE1QcsDl+fVdIzYBWK9tF4IbpMNpZ9CVqa4fJVYPo2a0XG+Tlo5LBDo6IFIMjpqxUPmIa1PyIvmMq4O5ecjU5jp0eK/ZSZ7Krfax3h7I8c5c0ZvmgT3yNLW0wsnjMi3B9TP7KTEl4wvgPFtwJmwFxQEMfzxH3t9mr5a5r96F/jIe2DvD2tEI4I8ChOxWpH0c2+IBAX4I0+7EGiGQ7mLGQ3vRXJ9Ilkxz5XLcXnBTEalMEtyMR8d5qbEbW5vKpkhzkiq5tq9R+T9ofyqiYAE6VNd3wVg1o2bBfMYYm8PArCW7F9jUzYLYU6jD+ZYjmAOGwv7GbJYgR3LB1bYkpRJvOSJGwKuLDYPFmA8FjGP4tnf3PoB5wr6RVZIgpzsfKYDjxfMBBhlDqDKILnmQTbgeMUZsx6lU9ClMp7OrwInpxDfsd1WGPXLRYY9xyfjr8qNmjBmgpQF9sEgq9CNUhIoEINGpr3T3bC7jsNxpT+VK5uSLSDBE8gyRqZGQ4x6Rbd9C6jZiRNAhJpVJiuGxMTWm1oh8NTDxkrZ/ZDvKLNlbAL/uD2BRJVBOx0c5aOwvzTrzC7lBUMuNsqRGuRbwYcbwpJsjzhp4y/b/LDrsbUjsBLyXx4qCVKfBT6C5V5ZqfKBzR1CsoGvkwFdG8MPXPuFgLIlIz3r6J3xwE9Fs7C2M2sAVyL2NvlQuS+tV+Jf0RnWJ1zTjiIuFr8Y3sUOySnRkY40bE0RTQ/d3S+cuwRR2xB5LUD2D4XjyT4MR9t6uePuvKFLO/GATwJQ+vVC/sWQfS2K2hPA1KSN5BwiQI+GXmlNm0uDqJpRfOaIQ84izU8jMQd49ryNSvXXn5w1qV/Aszq/BHm0hQJUdbohhtsD8GvQeLfX6CmdsgNiQxoezp1jj1cn+MBt4LPx1sC/AnC0slxKqtRo9FRqjeu1vZO58FixjG9yhHlFJF7G0+MtjFOU8XjpsdTJ8LJQC1TTmhs3kYHNKgzhw7f0PTzXJEqVe1u5MPHcoL1Y4ZrhcEaejbn6HlrcJ4y2Un8j7cSkdX0GQRXYYSHJPy8fQqY/Z4Vn9+SPuBXj0pOMhT3jJfJuftnyPwNx5eIQ/z2dDa5wYZCBYAlfHKNE4ZJ+Gz+aFl+zqAq9b4dF5e+UX1+rRfN1a7pqKEMC0fixOJ3NQ7r+7oPh7Mi6m8SBSPUA7YnU/lgPqJaB8I2uAP6V3Z/cZuHS24gg2l4GeNw/GrCs3v5ALpt6yOTbgQvcgGKx+jJ1NGXJDpZqdNwH+MiXtDh2NFOpA3Ivt5fJbgKMnG0J7nJOCGQNqDPDSJ5cx2gY+9cXsDMHUPqKxm+EmM6GDbm6fG4K5MsR9q4c2TZBdNMAJKmArObRnuAx63VyvRKHd2E9f2vp/iZSLYKlaS0Rr6ypFsnpJL6zr0Zx1VJqSs/jM7BKLm7QiP8nbsu7ruoBfxSD57CR9RgJU5S2FDR1n8nsUlHbmVVtkwOp7Vpgi8nBq5VbrLeSKaTL8Ke2QxwJDY1vR8QSbT05WmZH9VDnzlc7p0m53NfWrSBbC3ZBlwKaoR+ToaXFjEsCfbD64bSkjcKFezN+qA/wLMQN2S2wA/VVZSLFs40v8gLk2WZ1DjE7AwzEKF7xBmExSn5Y5dS2iIvEIv9t4C+uJ2kPJoL/KrFQIbtHpRtHpQxwpNcrdeILqKZ41jDbDjOQM/pUTmoasaV9jqwB6UuB6VxJ8WT+d5OIhNt3bPMG7HrjHSnReLJpC6qqMyHawVwdp64PHBxUe3h3DlZ2RjQ9VU/hTfIhPWJP++RWourS385Vl2KvXoc8H2rcFaRkpK6EQm0tyOYIv++BRU/aiqAq6d/wAg+2/65L/Kp6h0/wD48bf/AK5r/Kp6AGv90/SvOr9n+3T7WTG7oa9Ff7przbUQjXdypzyxBrnxCvFFQdmcTcawh8TmSJ1WRJVspAwHBYMwYH6Adu9bem27W95fvFcxO9w4dAUC+pPTr1rj9d06c6le+U0dvFFFMkglLcE7Dtzu4yOP++selang+8F7f3EzTGyvZdTErk9gxJ6ZO0PGO3PNc04qVioKVioycr3VrHpngN53kkkkQr0HK4KyMUu9PIhaatoz/Smb4JsPBG3s1a3XM+vKMY+M6qdCH1pqvDcMZaWXrLdCdDXxgGHJZoVOkyFcdhqoL+2kyi7TmmVkrpKHBrpHFhrgiJrnHOiOqzZqSd5Y5z/DeS4YvCamshZdu+BiNqFUypOZ4kcgRrjwC+ZPM0UTjX2qvf/Xwo/9T3irl/eb3vk+/iJ9j7ngBmxthm7xL/jN9LoMHcsGknL5n2RQ/6Qvo7xJOT+ytm99MA2u4LJHvePSA/4aN2OHxN8rzeNWRm4+P8zAG5OQ8E/m7hIMt/CC6f2KEu0FyG3nhjqIfIeaD51LknM5p0m5G5Jw0qEcI7HJo4C0jEqlgfodjmHFv+vz4fCLVHZGudh2sv8cuJwXn3hM4ji2ncAyWQQ7TGCJOu8IzLu5bjNI35lRr6A5qJwp2VZOXbYeqnp4c1I3C84S9VG2Jr7aOgZCUO8Oc17t8HHdlbUfrAn1ToCYq6ydt82C0QkhP9yMBzQP5gq0Pm8mk04dZgYtOqL5hrvNXGPo1/pK1zI5UXDLIDL2Ul+CCXFgNbX9XzlNbS2nFIFl7e7Fl/sBP7I7mjH/1Wbpl9tNYB8kTeIO3Ug6yYTxl1Ov1NBIHvR4EODdBuYJUtaIrr2Q7MuSvBq2iuGRZ9NCWyIxnaq4zvjt7AC73jSDD3rgtzU2V2MqxZh20oPQ4LCjPsJQIrVTBuWSR5P9QlK3xe3R9XjNcwo9iKKmBkPhXyz12MZSwUi4EXSMfQlZuX5ZXGkO0E4PrMD5URb5YmIuqpf6mgJV7ROMSgOZ9SypYpmFlTyDbcprmBH7Gt0DOyKY8s7pyAeGcMLK6HxaSbcgqrBqDymDcpIdq4E2Cxl1QnNvJNVv1fXJqCOjkqhbSLS9a6DipZvW1JHBgE4Y0q2tjCqnjp6dI14qEqAn8RcDHSbeY9zmjgY4VcsEqrtL9jkIDaONX6QLqJGt6L2DNxu6pK1RvKPwJTsqA8Dh7aKYjCQ1wq8hU9VUrXqYNZZB9Dwq3tiZkKA0jPXWdCuS6ccCxSpsoI2RnoowtCQpxmtqEJcQHE0d4W+kSM7oR3txjPb/WlrnLFQT8SZ/ss1ZOzn2jj9cQeyoTwDgXBKtb6QXP8TdBM1zspzUiTmxnvVBl4H+qm0yiFYwO3O2KUmZXvZbDnKgjDbXgvVzRSxN52BWPIbD/qUEFBFGZaYDaHkZCTBHhGh1fHHqRY2mwpLMzp9xTc9A8uK0cAnV9pDRWF9NT9u2KzJzmwa+A9a3YEGpBvWAOBNH2XOJbk6hzWz7WcJMgR6khhKuOLNIyQQJ0z3qL9ew1R9SfN/L46Jp6qBMSa0HsE7BUx5bOZwfA3KgCtI6+PBLImi6fC9z6/HxJvhEK/rEW9RZuTv4Lv1WD+UQN9d6Drd7sWIqeXvvUfMqt3lSjgABvb5IkOy4vkjtk3DkGzO6NYQo5Mr9LCYLFkWEwNmwIZJ+SQSUrPdkZUYlDIt8c4yr9X8mYn4A8YgXjI0XWl4NG6G1V0TRmlLp6BxSyCyA4fYchoUNPJ3LkLzpC9LshwRoQmVbHTqZ1LlQ8GoXkBAMbFP9cP+aqByZxaYtDOtOTn0Uz8DxGJpd8CLyqM6SZLtXDkT46NEvkBDe39l7P1c6Ke7SHBTQODg9sE+Jh06xD/jATbn1q8CzjRDbZu3l8m4d2xDcYYBNVm3NEj6ssl0+x5m9mhBzmvMnz0nQ5Z0LgZTk8Zzwa1bj4BttDwVlWJgrFAaj7o+ehHcD9kfWbf87Z1o0PbpWdQNEoHvW3l0qN2o1Qw5pRHhxI/m5W1Qf1AihvVqlRIIB3E+iJNaiZ0tg/2/dPwzHX4lbHr6UkPamGnuQ66hbLwYAO4mFaGu8bJ1RcoQlLr0Li34XsvVh+pe6bdxcS3RFHoS3Ph2YQVMhyHMFsN6KQV+1nAPoAwc26jhR7V+7wIpXHnzoB0B1m6/j4rPbDsGSkR4SmUSShQMb2/5yTFXrZh3Vk6JQvNIyRvAd5azj3u0u0r92xGczVpZPZtJ7IvOTDdWlBIdhDIT3sSfPQ5Xt/ERRyBYK45dFTsvYRkYjTh0XYvgG/8NXRE9i3G49k2dywAf7ZVfKQNdb3bX32wBkYzEsIfljZ2G5zRtxsh18jFJ1qJ/FUsRMiD2BR3uBsR9XbRdeXNXj9t1vcaHefADXsZuNtCHZ0c8l5LZ7XAfr8OCJzRVkDUxRubfV3o3xZUUFDUvUNSgOh17XAQQxsiXx3fqzwKFzGPMNPj/yvNq8wYsiSd3Vn12Uf0HwHFp5LPaLiDo/RhBJ6Jk6bqjBbgmXIf8n5iQpoo4sgJrWpqcHkq3bNqK5fJ4/RYyP/PBrUGDnbUVIIaAlkSl6gzr7LPVS2cXXuvSX3J0KaQkTTP7dC5fc/9Rw/5d53sJNHdGeKWzhgCsCv5k8WiwTNBx4TNqobSnm3edQb/sNzm2B2z+y9h5rKC/sCl38Q4NxVPiD9D+YnAULq1ta18wvtQ1QtdI71uaSw0Tg6chZk2utmuF9AT6gTBRzX0rE52WAOWsI5o31jaRfeD/OGaIvc6wnb+TPy+O1nrTNvFg0wr2+oXmVFEZjXd3HVKMPRvcV8bR7yB3e88Hl0CkPjaCtYEPCFh8e6djiGK2l9PJbCjIB0SaUFHgyHkHHWgOSI8Bl/7YKLkhwf2Ykz4Jl+uK3aG5gtMmtqk+4ci7vYUlVk6cJljsAo7CuvvLVMsbAmyDjvuSuRBrGbqk7yhpgDc9Gdq2/BXKmKhGuSS21yZeDhk6GxCZgN2pRCDHsjBVqQB3DjK6EsBZsFM5czF9tVVYUzN+Glbla41Bu0aMnN2Dtc7ipdIgNZfKl17ty8TSxXD0SuX7mNwW8VN8FXqeC0q8m9MpeDVS7aiYZGPD8fWwE9XJXVFf2xR/kpLzWtMnkoQ4HgwG6lYV2Ytm3Y3RuKH3Y/LDt1tkwaNGJrUJPiwZjvdVAEmazBtcKUzbxNudQNRtoDuAWjiHE1PIzbqbnE1FR8cj5CSz+e9Ebw5kM2fUMW6VpMeCVm5Sxm8XFZi0ucoFwsv7mpqsJbXoO3C8XC4Bvml3DSbJTwlEFj3kqK1zNTa9t0iz1YKXz9xl6Hmr71aC8vZSTgx1ZyyXtm+4zXQ/tEGrOwtqbVPnRYmqyK+9f0iOfqBL2TGQJ3E3VwjD9+xcZnGfbgkRc4L0Shl6mf9E9VNJ0/Ai4KXbCYAoRHuT4d7q3dlEpSeDLfpAGmUTQKzrfHcH7pZZ6l1WslQdoqgeeVEo0vshVIuBwPEy0PGgCgOYJl0RbEUgTnLLx7TfDq8nrb/tNbfCfjqf+KyyYByIH3OoQ6GiWLlIpDEtvqL2z8N2f+n0P/ACW2DbOTFJtLt4MY5EV4S6nEqfLI+fBxk6bo6SfjFpa5MJIKjhCD7UvLFsmjGydLSBgU9M8KNKRO8tP8+lItYB3a5E5q7gO8nyR7BVNuO1aJb5rfZEO6uMBpcWjs6nTJ2DLxG/Lnc9Kcq6fRMvqxGkxdmOHsTkBjZ48BRYbtoTFxeI0GPYd6SezZiQJbGGcHBijbpf7eFKbDMd2kSfYb6dzXDvrMSuxhvUhXkqtyVBt8O/2kBw9hgnhwmnZLBPWGPy+qjrI+IrhCa7xOMhhETJLC3Ek3XKzEXQ7pX7QklWOrOh9T0jAWZHP6LjpjPhRiJQwL6ZSKPkcR5YPTtB4aAjHrnVgL5SqOZmoJ4vHg0EEl4iWugVHEtHlMP3xmhM3bKGoTHvqWQe61XIbEqhyyCGyvdZPUg8DE0TvBWq3ifdUcNzw5yt6S8gOp6XdvYMsV2y7uEUGkBg8fNtD8HpO6qswlEwzQpXhTKphyz8hJnLvbe0cd6TvYDvSbLdJ4L4l6UmiVzWgdZS13pAz0EVZUm1YjWB4cOFmgfSfMmR4K2WBTv1XwoxVHe1a3cYKR+ldL8QT5rVRsH3NQW7g7aHPqvqWBBXKHlAFlkmDNkt0HPxOeeyfiHmKsJ7INRAxz8ixZKw6kaDHHmTH1K/ZgVq+8JVRS0kPFKszW7f8X9FQHnLXOVdmVS3gOiORu1Q4kIaWs3EAt8BQ1+7LEOVFj3BHoeHzHcmLUj4T7cs8dsVMyOXCyMp/ywJ1DnTdTwG0hBs3LTNJFD6bAMeSAUFXr6U34HT36b9Dc0OYAFdZ4sBPI6SZVrP7y0ADwkYqcGwN0fhMq/Wnh0Z9nQ8KaFA0k9YWpcwDuqYpwV4Ak9fdJTR6+GJVrxN4DB8RqapHiwpJ4VzRfUI4FRiAjRrSGPX5d0zgDT6pUCPkQsEtvxfB9MJyGZnLYB9sl6Rud03HQaPzMlTNtyIE8BbnG7HGlPVxNq3zt2QuodAeGFcUrn6lkAh9TTBOUXtE4cDwxLNHpMpOIKtD1yLX1dqHUqDNKwH9FOsJxJKGgeMrSKmZ6IAAcrB0BlIgzQWI3UH87CmQPFdrgqgAdNavBKQpZSJ4hAPZ2x3Z4SNlNP8UVDQBdsK0kEH3i1JhgmE0MAdGUJzsqOAFc4Z7sQxmUJqZfLPEvdEa2zh9aAmyqyqcc3b73jjYv59l1JgO8I3jh9XZqvWdwyHL3jf6SubQXsUfrkGPYMCsPLSHT7FyBm2MVOjVE8W+uJlhhGHFDeTcDsrKjKUXfEx6nPXjRBJrp5qGUvdjjHQqd1ZJ7e3SHgMBdJcIlgTmB8Vqn1jI2hgcXpCrFsh2UFFlMbFnBJWJIuPoSr1S+rHKK3y8fyqp6Dlc6ALXWaGnkUGO0fh5VupMpsyvvpJx5B9IwbiFvwHmmF9AvmpP3i+n7PuXD+qYn6mFD7yfxJhD29ck4sYB9t7fwCRnQrwMhmrhPmPlC7pDSpI3XNbRkfhMXgWK6F6mVKk1jYpD/gGN4OOuXaCuTzJM3HXhCk0tiOgjWZ2bYXBtjdmxODa9Fw6fkcZ7P3MIHU9gqCaE06YRltuhwHqWbQn95ZlGkZ6w1HADEZ7wKlZZ6bXG+d6KBkCmvkVGJ+6WL1TYdk4F3bw2D2DmFtBE/c7E0Wjm1qCNbPp6dbQyh8jAsJkYe2XuxTZxXjY2PWv3T19ztrb8H8Jy/WkvAvyRrt4ZJZSz7tyA6dLhfbEcyhS5nHCA4PZOLkvd9RLpsdPF1PlKYVklkHaaNnklZXW02IMdx5V5Eoj3ciMJ8H/4jqFKQoOMLVI8RAfKm0E6G5p/mUh3w1bsJbEnnvHMBVeiz/EqRhaAwHl3JN+PRWUtXdq9GDZb2R9mJ43xQzCQoLzhIbm9FJsUUnVN7HZM+xQ0bYm6+kZl5t0Q1bOsBJfdzF4PbsM7kqEKrZkfx4AiDDwrk/0HrvuhTOxJh8w0IsqLh9F9mSmdjsz8pjn1I0JV7fWVRA42w5yNZvz73OYpOp5RtqnQMVwfAN8xSbDkTfbb3ZmPWEUMDTJn0LCZG2HwC4qGYAAplvlhczDUvhXc2i+ixfmKKNEP7JYVGeC7grEb62sMW8UiJQUPKm1jVbHd3vdeABD6bTJddKHP6tGX6lhpzDeHyIgnqIMw0yrkTRVAW6SlYzuHmhrHYUXSfTR2HCeOzdX2VIHdyKNdLIEWX2UzhdSBknmEUcHXuXWPb3HD1lJXwtFuWdlfkt68Ue4h6VyrvXQn/Q2bmFEbYMUqIRHtMn3KpWjhn2dZ7TBaKBR+PAbYXRmkQLiXHm05w5cnKmDNrc4LmdQQTmUVb7SObNxDfXRaVRi8PwEW0OnUVe9hBm4mM8Uo8SLglp/8G2PSXAkC16/U7Rv+Wp6aJ8k6LjsxdGqBNzKprI0jY2WkiJN0HU27eZ6RxIl8b8c06fTJqEGrLt03cpPQfvIC38RJyxCtyMTnj8Ny7iWL6bUEqxV5PObnTrNDiDXuSnYWRzsV2l1V2mvpEAmK4nARBX8E60AoJuAoaWRuQgfH5dL9DQRrlAJzWNPdnEcX9yVz5F47UGGXB2BDz3gRMQ6tc2kQFd7DhxY6mJJhg6sTlRvFjzKbB9wJXFnHbU1W6h9g8WS1HMDWsOrLhT9rKHN2tBG7aW8EPq2ZD9nRQ3bUmnxq8yUWGPGIK1zhQRRrDu84XkMo6qD2KXfpi0H+aMxuc4w8U+CGQ2o4vzITeKTaaBm88DPHi1OgN0Ar7gNj6TbFuVTLB3Nnmcpf6kq9IzwmDpO0YBsoCfhy8kxw9z86ZPHVx3Xd3LT7dWu4Ha81JTLyE3BZxaq6AoGT5N8OiFwj5UuCiGvoXHBB23P2KORZs7SG+f3xXTy2UlFo06QMS1f1ppUO0ISXYNYCiGVvQrsWbBpbIZqiLvG1pMC+1r2AGLnFDpxpkqyGD4gNY2DIRyTc3Op3zkLMYlJRKjkqYWPL0lGtfzO0T1vTW6ISI8BXbFOPjAT8gZYhYPw8kp20oNlIojUpTJUo/qAQNlJaB1m4a5Ri+cLdzZXMQPSxA9GNsw2LKHhn2VsGMyrp6UfMoiO6lhtqupSGF62u9PUK2RMFGHZG9e4mqb8jyiE4qBuCW/8QYpjrY6TjKLq62x8qnn2E/JInxuJ4Qo+IS5aPpkDpPK2r5Fq3NqMc5RvIoiGSIz6xnG06ebsY9Xfp6s0yV3+kkcX5Z6MzJMJNzqcAZ29S9yqWUNXDU2D/RSvN9dYIsa0qc8Ve34VlHhoK/OZVRNBxGtNSwtBP8hsrALqQs8l8/8TOUJA3KcAOZ+e5dkBwnHeZJI5wbYuMP3cWgnhVXQx5rBNa3Igv2EhtdD4yCvXq6dprFzV1XNItEWyXE86Jq6Me7vqX3BH2dYSwbRr1n5cwNspMLN6iBT8Khwx93ShrMWfeEBW7Mzc8SlhP7PQnFtQ0Wv2s2GBDyVCTcEa7f1IzGMX2YyJLu5s2+UTrm3qlXqeBtgUiP7y5GnMlvTS5K48Cx0Zu58E07b4rAAGw+g0gOmnSmzeZ1ew+r48TGQF7cW4uLWV3sB4UlH9Qk5NeMGKStTqJKtrHHMZDZ4Wdvq+LnwS8VJrFs0KZTHzvsJuROrDpyyukSt6N8zLIkPDIamHz8Y1oNOsHI8FEyK4jmmxMjVa7t0rSdrS+S8Wao9k4PKaEWcX3yNPlT1EYBDRt4pYQoWrrs0xWi0M+w9N48gmu4Jn6ul3AMPpzUOkkCoRcjImOUH7h2Y+MJvaJVRSkeZZpXpAd/IVmb5sM0NbFGeRR6dFNIJvJuW1E6VEFmw7XJd7LiPsXtjDqe9n7T2EoDJ5QKFEpXB1Is+bbLdqLpgXnYt9U6gfg0O1QcMnqt2dQZcBqKmnKPjahQ7RJ7dKRk4mD44tdZOCbQH0Y1djaIX/sKGrjE5pDZxrOkRArqEvgD2P9SwrCSI4XDc9J5fNFGGsTzrmLWeAI8tgNYqQP5VRv3F1JbBtuFgA8z0sbLqEibBjTyQZq3M9ExvBb9V1IafT1bU4svwwiLNdCO9Wk0BZTTcZjUp7k5GPjxvsK8kvxpV2sxq45ejXA0eaPWmhcZUAxzfwHt5rPzx5yuk+ELqlq9JmJQIdr5XmDg1CJcNPT2iz5SyZaB9UmbRtpHg5tHp5GDVP0A1TZ0ggkzZFhIE7Kk0YeO5qBZMHmmHqWwqR1xMGeWKkzVeMvNQ6BWAuVCYuOj12wkpLO5fCVjKgpcvfZLmCVrPBKGcdVTZx3fvHm2Ei4A6LMgXJD0btSctu2DXLvu1ShLTPwJMnXZeHWoRiVHOpmJxOm0eRk5Vfzbsj+EzHtlp0Un87DpAsDuwngg6j6jBLIbVr3FwWITfdhKxJ5qKxDGvYGNzCjS3O3iLzy/o3PYtFGiHj/tAChQKt8yOeFyEn2UJKgMCdbVh5rP6EB2YOrbo4aDdE7JCKIgQ67uNShHc2lXBQIoUDxi02LUXCBu9ROqFCPLbg0S4hr4+DDAhZKcz8F2CQbJT9xLr96vMLIzdN9o4u62ZfmpKaUtL5v3Xg78M+eIdbhPOJiPU4mIKBUKWSd6QDHfhLpZ4zUuNxbfHxvYpLfIppvIXySEV2EDD1TxmB/9OdWnfwljftGFa4ZqzuZOWFjyubB8BbtLyyLWzKwExHGBbBGN3A8jQExw9IMMD1u6m3n9eOYCbAKe2aH7L7DB3htRO6Ld7ZnJ8S9KVq5h3kCEqxHvqB3O7BzvgeNyNbaNGYH5oZFoyhWYJaPNWwu4t9jiEdDv3GJeb7rTMpd7dwDl7Rk4NpNNZmtnCsCmcxYFqMFHsOpk6MQnN8BRrQ0bn0qq8tl3RIXT8N6o3wsgTszQ67S+fPhDvOvUfkPyJ3ah8Qaa8ibJRn6pFMuSLROnUHG4PbjHq7qKqPw0Uu5G7n7Imp0L7HBlvFw2RgzVCbFwYmxSsMf6hMnH6OdtCJWsBAkoCjm6SZn69MuF7VjM5D+jv1CwTeGqKD5L6I9w+k2lIQsr6ETxS7xSQI8ynyDNh0LdgszvUthyd9zZwBFlCj3LmY2cnMBtUKlAa7zzgLRtZXsQuM0Dc9vCT6AA9mZ0MOVrLKTJTdhvR0c0DoIEWaRg1VgfRZBNcDq7FeEhxYf0ZPeJOM0IHvuoWdRhiJ5yk8Bvv6yxd9edfcuX5PoQSq2KBKVxhOhmAGnkumtK0Dm3IJnPxZ4ihGdb8YtGgQvyifGSuG6pOdxSWRYcmGtAcHgsHYdEo6Uov0A1q4nMnzsFsrl0PN3UBjwiVWgMY5OthSW2TiN4GekV0uXGxLo5cIazY8VFoqCyTugVbXaYUq1BKlbBeUSjRbwLMIhv3HoSLd8s4xODZ4FGXFMWsn1Glrk9Q4JKc0h47oXqdTkS4X9BqZnBSh76uVPNRK4yuaKHKxO2wUVWTz7wNF8ocAnrO1cBjj2pK1xwgmoK7gEbkEMpAJwrTeThEf6wQkhEgMmk4wFyWqLSygtyWtgknPr17ggtB4NqaiTdtwX9ktLYb4OcCjXYIgmmWItFHx25EF5dXaZgyoXNHoBx8OE9hFaokAYgGn1zvH+oasKFgScENr9OxuJPDOXcKHEjihNmAEMTvpB1Y8bXU5Ye7dtlvKJBQqSFPEbmFr2EHXtNSzrFSzInXF+vkG3CqJFAFuQzqPXhYOJZJ5VpjDk8ZPvA2SyKHPJkhuVR+8Ee4Jp91ZmkygSkg1RnQNxsPNE3y/cG/J0O8QuwCfBBxwi8DM5cl04cgMsOhMAhv1E9VsnmkvJPhahCe7cwHa0Bta+eHYHgvKwPcMfzzUg5pRjVsArDfXOn1HmMKnQXzfWGwm6JtJYzs0E8vPs7crsVzgq1kELttsJjTp2RcdE15jfbZawJb8T8H55R5PfWFKlGxd5QDoZmdRhIRA0JG2TrzhdvdVQpvPxlWUgYAYzgZJyxTGWBJjPHsIBJ3qfa9KBYXTx09bZ69mKUgOvbGJ9ojC3gtxoIZFcqgNIOVXohAGRGS1eRr9UtK5mZvo4sSIqqbk6Um93v2MORHmAWgeUvL2pxtRSnzSmjwyqyT+QpthQrCAl1DiA3QtHZkuNzhr5rdVdg9kImjTIgIJaXi0xg0A6dOjcOcWOC6OXSyc5RMvV2qz5CYbgBqeUTbTtE4t1H+3QIc8e9HQ3RqtrRZE0Vw6GShXwhl94KvEwzjSkKZhp3HEB2tIDIDLvSbJ7RNSgkBK4yEs6gyK6xXW5Yv1oJIDGf6m1T1zLkYmNAKvA0uO2C2xwGPjE3NO2TYUT0YqjqZvsiCnXdv0JvZfgm86aDQj9ie7DdyfxMCbtqJmyVxMpOyMvjBGVkUFIwvDh7JmjjCHf8fTzeGwkjWLCZcLJbktJ2UvphZbvCJqb9VCb94pPvi3uyu2cmcUBkKt9GHIzaScfsVTfsj7T6cDqYjvjRNv5Dx5sdLuNZtqpQcDKDxNbC6N9oMh0GuKhq4TjGSGS0O7TQeCp9RX7nEe5qg5n2IJshOFWEOHWG1q3jJJYTHuWGBWXIlJYVz02REm0ehMo9g7YjsLGE4Lg3A59j3xhBkH3trQzl1lXYVwiXN3iX0z4aEL5f7VWc6KAvlqfi/6CqJoIlPFLjo5P1VkbAuqWx53S6BgRaOCjYhDV9D73mRShTFbr9gqSW9Gf4k3vv6aVbmX8tC7Lv4Mk1OIpSzLpG4n7g2kMRcJnMJfEj5kFKJuG2chGmFOH2ZoXtWGyCbdoCjj8EaexEKF8l0InOAw4lY1hjZ9XMWxpMKuTkkvdpxYsL1p7ABs3NyhEJqFRy9iTSqAmbwbX3v4Kc4aWXHbBVtiTuk51yEdFyWfBFLCkK3lxklPmX6GQ5c2S8h2OYtWzpTtZGuEQYsfxBAfOfqOgy1T76gjzi6v76rHTsCm5PCs86rkJOcpTSKZnHrH5jSs0AXWXO6pk6qbXZ5qxcDT4p6TLo9gUtlsDeC3bmdBPYB6nnCMtY0qzYvXufSgBfBqi9XPYvVHlcRWVIpu6NPGFPUmXgsWfUjuCfsbd6pzW2pm00EWyyM9LnHeBAHiZOUjyu0LwNbm3h3y92iRxXWj1HIpb9HHFzG2FMzFvQGsQr7ye8XaDs9vHOYMnvOGuo7eRzjmRdqWL4Qm6vydSnjcdfXpCMFtShr7dUQRyoh4U6h6xuJ76PaDxIpIAD5dVfaYSRJ5Kx0W3EKJ81QYXx2QRUDzGs8ZOtTxbCl3BpSmKRcYs0rHhtj4RQdJj8iqaWgAmKDQMG96DxMpG6TvFvtAZ5OqqC6A3MBzVdAnYrW4wbGpQTnzdEWqXIkbaUzt4n9LGKUHADw4PLDmNUHwhk8aGkCeNyhJcQX8QzY6o7Gl2WQxvgwDxXpb2Hv2qcA4nYRG8qvCdPwJ0JDa8rj7ohIlvfGeYOGkGcV9Bzf76FqVhMBfX5d3fJeXBYdPN5g3KGjk7QGw8lmEQrWYdnIqMWwjUOnMoKx6LRNyVCKeIaaRZaAX3EoEzFJZxQOJAwO8CJcEzt5qhVeBcr2yVTp4jI3sfw5kYs1Plkv8Nh74CuTSFF4OgQwrYu+dKCeDKUTJW3AmzMVTNmSkchS6hZ8wf9sqYcUpkvw6DzO9RCm3zfa3SdVGc2F8y2K3y7GtHMGAq8fSBUrc2xxKPeUwN0GxdxzTNOjSXAKGTC8zR0xgIiTZZhXtBhINfmVRGUBr4Q8MMtqIwbshBupuW07VV0WoXHSX3jMbwWfnzPgP8q/ulmZHxw0edL6QYN8QiX6mHnq8OxN8OEK4F9qBNqYkkWoxWGWJpd7cTxtwJyHRQyrNB9qRbrEYbRNXwH1qgpUJ06ZIXKwHaxMPFo9Mmox1zQCrmWRsPAaxLRaOX3qRAsVyqWR3RqRPvomwF6TGZYupaUdqLdGfa7z3THYkTCKTxqsLzqnqApvhMeh4QhsHgx7KgxsECpDuQPwBnV0KHVGYtcRbiuBVJuqxG3FTrlDF2I7TFNC8ZuqUzs7hf2HuIP2K7jxfzwjd5cxcvM0sWeNHsi4fPGAyiNvmbGA8pcDJXDZpTu1WIHLi3Y7M9CLw4hKbX7lB0dmwW7TsACyIeo4IXyj5wCpixpRGWPA8Vtl5X7drWvZ3w4pT4pnYM8CQKVzsqTfs2XTnZZF9bnVNc4Nk7FhxTYPYxvmGwpQDQbDJ6VGrg0DKBb4EhUqX8pnOzOqYDcvHJU1Ka2ZmcKqjt4SY7cwu7czZ8Q8zpeu6pE3xJ5UJZ4pqJhtuSxmuEhQWFfwTJPrIg6KlLzLXAHxxlFg9qz08wyl2J0q4x4AfcUnEfxHhP9BfS1xS5AaPOdRdyc5TqjjaSSgg5fhBuiS5qb5uTlT8HmlbZhhj8RJqCTLNzKhoagqCj8hy2mvCnsd2o9wrdrN3QGwoWy3NnQ0cAJKhfBvaCB6sKAsUuOpExQAFaxX6NvUPnmwcYDGqFEFbxNVPvsNjzcxYsm4ZKNfwRMdySq6MRqrddwxv5Dvr0k3t0dzk2WCtlhqBK9SxHVQn5TxWI5hZm3pIH9fFQH4FGTEpR0Il8PZd6wF3EZfxT5UoDGeKBtJzTgJhWsCUKwFjOblxBBJUdxtDjhG5zdytmOBIsJZlHXMvYLx6fbphiXi57a1RC9QbBZnGgxlC5FCnbp0jkrkGiHrJtXnQn2aSQW68Mg2ZBfHRpBKexQRy12LBGWYLz1WQYHb0vAwh1pxMlcTgIU9aECJY7t3VVrIHUpmYrQyh7BzMA1tGcNEeqx5mvJHSGtBAjhRV3BXSW5hdaOCl9fGRJdtN3jubUCvzxgDoQdRKvW26DUgyB0hlCq5X1xjU3zuCd1xCR4p6M1EhYsqUSmX7ZXFQJmz4RLNL1wWgkPjWCmfy7SGfRgSpL2wdOXtZ23y2t4ZlhSgqgKDu3jBpUUYTdSw97k9LB8c3uCttYCSBM3iRYJlj9Z8LB4OdVhhpOPRqo7T9IzaFtZvYLhlRYqh8ZUXOgRQ0L5HlCRsGENwHFUeTnvUjXYQ1fKyXg8qsJdBcR8Q4m12yRvTBT3dl3lkqYlJTfgiEOD9WSJPw13HMVPb3Q5sVwgTwnBW9DZlhWtAK9yWiYc0gd1RWpHqQ5EP0UDPFs0rHXtN98Kxb6o1U4bqPKh2FXgkM5tXNEgJb2xs63gZXIYSUf9b4xDQrR1xXcFYpzLCQAYfg09tzz4XWNWyUN3O4OV1r6ZRWGxxhlVxb0dDjtRMNaVQdzfC5jtGMqbZ9iHImPgWMBWKmt2LZGVaUDSeqHbrtpwL8fDAvhsJpkdmhMZxqKbb7aXbe2rkvCBcIKJ2iBQCNjRoqIJKaFjKl6Nk0Myz1wVDFBR3s3CBYc1FAHRGvk7gY1AaWLXrKBFmEMAt1nf1DOkW6qZBT0Z9vNmtbtIj2SOAdM1gy7rQhLKwf9vDvMmgEDTULMNxxTy7ZlaTLoqpU6JqFpSp7D6z4fHfv0Lz3Ik9DmC7Db9XdX1HE2uDwWFAZcTQPkJnEtV6ftzsLk1sL1SRBhhkHnp5rtqS0AHD4SYJb3IcZq0uGGYYk8ZRN3cXkEbiBoqcf7eO9R0TTfjj4zVbWzqjwnYn5Ysn5mHVgDPhEcDT25AmkN1xVpnqY9jjfvfXsFjJOlwPxKdkeJdqvaTOAhq3SyKBIpd2VzCnJ1yj1Hy7JmGfVx4ESyYplUrQFIMbujC4JJDbFZSGKvHshEK8wexjvRMTqpGxtKUR9Jd6BGpATtoSH6xfn5C1VFrgt2ldGnZ3ZTL7fBkSxu1Mpa9PGbfeGBbiUmAvhm9nOtVQZTbkPnzbMHyd7SDWdf6vGp6yRbtfUgdIZmX1J9bPa3rwYzq7HDpDsQ0f3Ch8HtXzIvRVs0rfJnKzSbLEBzcc5ybm1JWrYOSBZZ8NHRLIO6JNH4mbUEiZCX4xP8mfRZ6v6knwjVKfs4c4mlV9HpE4ZXrD7OyzzYe0vNRzDsPuF0dPxhz1IkiNDxDUlkz6bZNgo4WLN4pj6EEWF4w5n9r9Pnj9Xg7h72ChXc5CcRCvzXI9u9QfKVdmbUptl5ctu6SgIeGt0sqWzUQ2BWWMsMfrZxXEAZ0U18sLXnEzfYQ4gOSpnGvq5G6N53ArU4mZg6FbYCv9A1B8X1JpYyMJ0u3U9uSyb1Z4aRdGLsRCnUKo1Y7cr2xC0JkIU5dnAIEm7ZI9QuNkcrDrRGpC6Mb4lmqC8QDN4dg7vZphydo3Ig4YsTNmUyE2nDwTDvCRs1fiG5BfgaSTZTc0Rp7AcfVv6qdh6pr3tmB5pEvQFEEVLCwWxuqSXlPaYSQ5PTQsyhuujnfnmBkw0dUM7SSxJ7yDGw1K5QWX3LhdbfLtyyEz84T5VVmOwu0EqvqOTq1rbB4PR0oLq8J5dl7fKg1vzSfOv1lLE0YuC6NmkPE5DP7O6vRC9FS4s9s8EmrMllqt20WmTG1uCNhkkICAFu3JHXpXuzwyAEEP/AN8k1E0bAcpIT/uGs1Tt0G22rXMb4cvK01wJo3T5hjcMdjXf1iaUjLdL8rAcnlSO		26/12/2011	0:20:57

	1bg6VrBWQkrCdqKXtRVgV7P/AI9IP9xf5VLUVp/x6w/7g/lUtAC V49478X+JNJ8QzW9peCO1YN5SrAmRxxywPU+vUg8YxXsPavm j4oavMviaOGQBpRJMiyFTkIW+X2wCpx+P0pdRPYl8OfFbxTdau sN1qUJt8ksz28SgjPrle3PfrivXF8XyzIYrJ4Zpd5UyMhwp9No5zXy nCjxzPEkXmsSD97GFyOefoO1blteXNlYl3uyDkCOJfm5zxz25Gfp TavsZxk47n1bp+sFpl4LqaA3DOEKhShJwDwCeev8AStwHivnn4 X3CTeJNK/0qR7jf+9D4LM205yfqK+hhURNb3Foo7GirAr2n/Hr D/uD+VS1FZ/8AHpD/ALi/yqWgBD0r5I+JcuuPf3Ul8skkEV0RAM All3swGe3G73r63PQ18wfEOeaOHVTBIrtvKhI0B25bng8nrWc3 ZouEU73MnS73TJNNb7XY25lDExnZ+8I9GYdeQf0rEh0G51bXZ 7WWExxWar5kMhIRWbOApPJ4BwT9a5S8mc3MBKfLEqkk5xH nn+ZNeknWr652GWFY3U5LYycEdMHrz7e2TUcrp633NueNW0 eXY7n4Z6I9r4nsp5IYo9rk8Nyx6Zx9M172OleB/DnVLmXxPplu2 7ymk5I4B+UnoK98HSnRd0zOsknoL2oo7UVsZFey/wCPOD/cX+ VT1DZD/Q4P9xf5VNQAh6GvmDW4o5NUvVlt/keR9xKHpk8cV 9PkcV51qPw1+13U8o1DKyOXAZMEZ7cH/PtWNWMpW5TWIJ Rvc+dtRsvOXXZFVSzPEQGyMFcMeT/vGupjjRFXcPv8bSvAPPOa 9MufhLJIhVb2EknJZgwJ98jnPTmi3+FN3EpH9pQFQMKuw4HX1 z7fl+WMoTfQ3jUiupzvgAGPxfpaqgIMhywPGMHpXvg6V574a+ H9xperW15cXsUghcviNSM9cDn/AD/KvQxW1GLjGzMa0lJ6B2o o7UVsYle0P+iw/wC4v8qmzRRQACiiigBc0UUUAFHaiigAz1oooo A//9k=			
99999999543-9999999997@g.us	que es esto?	34635293190@s.*WhatsApp*.net	26/12/2011	0:23:06
99999999543-9999999997@g.us	soy el más fuerte! ya tengo todos los números i pins válidos para nuestro negocio del siglo!!!		26/12/2011	0:23:40
99999999543-9999999997@g.us	Jajajajaja		26/12/2011	0:23:43
99999999543-9999999997@g.us	yo ya estoy listo que necesito pasta!!!!	34660401445@s.*WhatsApp*.net	26/12/2011	0:23:54
99999999543-9999999997@g.us	yo tb estoy listo, cuando quieras me lo envías }:X	34635293190@s.*WhatsApp*.net	26/12/2011	0:23:56
99999999543-9999999997@g.us	además soy un crack, porqué lo tengo todo escondido en mi ordenador, no me lo encontraría ni la poli ;p		26/12/2011	0:32:22
99999999543-9999999997@g.us	somos unos profesionales! mira que es fácil hacer pasta.... vivan los sobresueldos!		26/12/2011	0:32:28
99999999543-9999999997@g.us	Jajajaja		26/12/2011	0:32:30
99999999543-9999999997@g.us	contigo estamos tranquilos, eres un crack!	34660401445@s.*WhatsApp*.net	26/12/2011	0:33:08
99999999543-9999999997@g.us	eres la ...	34635293190@s.*WhatsApp*.net	26/12/2011	0:34:15
99999999543-9999999997@g.us	□	34635293190@s.*WhatsApp*.net	26/12/2011	0:34:43
99999999543-9999999997@g.us	Jajajjaajaja	34635293190@s.*WhatsApp*.net	26/12/2011	0:34:48
99999999543-9999999997@g.us	Raúl ya lo tienes en el correo, el pwd del zip es somosunoscracks... coordínate con Iván y hablamos de repartir...		27/12/2011	10:21:56
99999999543-9999999997@g.us	OK	34635293190@s.*WhatsApp*.net	27/12/2011	10:22:28
99999999268@s.*WhatsApp*.net	Feliz sanvalentin□		14/02/2012	20:56:44

99999999268@s.*WhatsApp*.net	Q ironia		14/02/2012	21:03:18
99999999268@s.*WhatsApp*.net	Vv		14/02/2012	21:03:20
99999999268@s.*WhatsApp*.net	En fin gracias jeje		14/02/2012	21:03:24
99999999268@s.*WhatsApp*.net	□		14/02/2012	21:03:33
99999999268@s.*WhatsApp*.net	□		14/02/2012	21:11:03
99999999268@s.*WhatsApp*.net	□		15/02/2012	12:43:30
99999999268@s.*WhatsApp*.net	Jjjajajasjs		15/02/2012	14:52:59
99999999268@s.*WhatsApp*.net	Ya sapsss □		15/02/2012	14:53:10
99999999543-9999999997@g.us	estais aquí? mi vecina me ha dicho que ha venido la policia a mi casa pero no han dicho nada...sera una multa... pero por si acaso os aviso...	34635293190@s.*WhatsApp*.net	15/02/2012	23:31:58
99999999268@s.*WhatsApp*.net	:P		16/02/2012	12:51:17
99999999268@s.*WhatsApp*.net	:)		16/02/2012	22:00:39
34999999092@s.*WhatsApp*.net	Feooo		16/02/2012	22:49:37
34999999092@s.*WhatsApp*.net	?		16/02/2012	22:51:54
34999999092@s.*WhatsApp*.net	Jejeje		16/02/2012	22:55:05
34999999092@s.*WhatsApp*.net	□ a buena hora		16/02/2012	22:55:46
34999999092@s.*WhatsApp*.net	□		16/02/2012	22:55:50
34999999621@s.*WhatsApp*.net	Hola Josep!		16/02/2012	23:31:09
34999999621@s.*WhatsApp*.net	no me acordé de avisarte... pero hay que hacer una práctica de la uoc y es muy difícil!		16/02/2012	23:31:12
34999999621@s.*WhatsApp*.net	y se tiene que entregar este fin de semana X_D		16/02/2012	23:31:21
34999999118@s.*WhatsApp*.net	Laia :*		16/02/2012	23:31:43
34999999118@s.*WhatsApp*.net	Mña a k hora hay k ir al cole????		16/02/2012	23:31:46
34999999118@s.*WhatsApp*.net	A las 8:15		16/02/2012	23:32:04
34999999118@s.*WhatsApp*.net	Clase normal?		16/02/2012	23:32:14
34999999118@s.*Wh*	Las 3 primeras horas si		16/02/2012	23:29:24

atsApp.net				
34999999118@s.*Wh atsApp*.net	Justo las k tngo		16/02/2012	23:33:45
34999999118@s.*Wh atsApp*.net	:/		16/02/2012	23:33:47
34999999118@s.*Wh atsApp*.net	XD		16/02/2012	23:33:51
34999999118@s.*Wh atsApp*.net	Bueno ps nos vemos.mña :)		16/02/2012	23:34:01
34999999621@s.*Wh atsApp*.net	hola carlos		17/02/2012	9:10:09
34999999621@s.*Wh atsApp*.net	ah! yo ya la he hecho y entregado		17/02/2012	9:10:14
34999999621@s.*Wh atsApp*.net	y ahora me lo dices! ya te preguntaré lo que no me salga...		17/02/2012	10:06:51
34999999621@s.*Wh atsApp*.net	¬¬		17/02/2012	10:06:55

- MAC time:
    - Modified 2016-01-15 20:33:20 CET
    - Accessed 2016-01-15 00:00:00 CET
    - Created 2016-01-15 20:34:26 CET
    - Changed 0000-00-00 00:00:00
- Tamaño lógico del fichero: 26624 bytes
- Hash del fichero (MD5): 17c1db82b4827c126ccbcdc42de4d711

C1 SOFTWARE

- Descripción: fichero con información del registro de *Windows*
- Origen: extraído de la imagen del disco duro mediante *Autopsy* en el apartado 8.2.3.1
- MAC time:
    - Modified 2015-10-21 16:00:59 CEST
    - Accessed 2015-10-21 16:00:59 CEST
    - Created 2009-07-14 04:03:40 CEST
    - Changed 2015-10-21 16:00:58 CEST
- Tamaño lógico del fichero: 23592960 bytes
- Hash del fichero (MD5): f026ba5ab758239a161a53de5b8c2380

C2 SYSTEM

- Descripción: fichero con información del registro de *Windows*
- Origen: extraído de la imagen del disco duro mediante *Autopsy* en el apartado 8.2.3.2
- MAC time:
    - Modified 2015-10-21 16:00:59 CEST
    - Accessed 2015-10-21 16:00:59 CEST
    - Created 2009-07-14 04:03:40 CEST
    - Changed 2015-10-21 16:00:58 CEST
- Tamaño lógico del fichero: 11010048 bytes
- Hash del fichero (MD5): 36c228523725c83a215af5b94c73e6c6

C3 SAM

- Descripción: fichero con información del registro de *Windows*
- Origen: extraído de la imagen del disco duro mediante *Autopsy* en el apartado 8.2.3.4
- MAC time:
    - Modified 2015-10-21 16:00:59 CEST
    - Accessed 2015-10-21 16:00:59 CEST
    - Created 2009-07-14 04:03:40 CEST
    - Changed 2015-10-21 15:54:20 CEST
- Tamaño lógico del fichero: 262144 bytes
- Hash del fichero (MD5): dcb20542697bbafef2f67e3906e763a4

C4 DISPOSITIVOS_CONECTADOS.XLSX

- Descripción: listado de dispositivos *USB* conectados al equipo.
- Origen: obtenido mediante *Autopsy* en el apartado 8.2.3.5
- Contenido:

Fecha	Fabricante	Modelo	Identificador
2015-09-02 12:14:12 CEST	LaCie, Ltd	Product: 0643	10000E001108C93B
2015-09-02 12:14:12 CEST	LaCie, Ltd	Product: 0643	10000E001108C93B
2015-09-02 12:14:12 CEST	LaCie, Ltd	Product: 0643	10000E001108C93B
2015-09-02 12:14:12 CEST	LaCie, Ltd	Product: 0643	10000E001108C93B
2015-09-03 21:20:41 CEST	Unknown	Product: 1234	5&5045dfb&0&2
2015-09-03 21:20:41 CEST	Unknown	Product: 1234	5&5045dfb&0&2

2015-09-04 12:09:00 CEST		ROOT_HUB	4&16b9d63d&0
2015-09-04 12:09:00 CEST		ROOT_HUB	4&2c291eb0&0
2015-09-04 12:09:00 CEST		ROOT_HUB	4&583c4fa&0
2015-09-04 12:09:00 CEST		ROOT_HUB	4&feb8379&0
2015-09-04 12:09:00 CEST		ROOT_HUB20	4&2232a4e&0
2015-09-04 12:09:00 CEST		ROOT_HUB	4&16b9d63d&0
2015-09-04 12:09:00 CEST		ROOT_HUB	4&2c291eb0&0
2015-09-04 12:09:00 CEST		ROOT_HUB	4&583c4fa&0
2015-09-04 12:09:00 CEST		ROOT_HUB	4&feb8379&0
2015-09-04 12:09:00 CEST		ROOT_HUB20	4&2232a4e&0
2015-09-04 12:09:01 CEST	Pixart Imaging, Inc.	Product: 2700	5&5045dfb&0&8
2015-09-04 12:09:01 CEST	Pixart Imaging, Inc.	Product: 2700	6&28ea3f42&0&0000
2015-09-04 12:09:01 CEST	SiGma Micro	Product: 0034	5&4bb4d45&0&2
2015-09-04 12:09:01 CEST	Pixart Imaging, Inc.	Product: 2700	5&5045dfb&0&8
2015-09-04 12:09:01 CEST	Pixart Imaging, Inc.	Product: 2700	6&28ea3f42&0&0000
2015-09-04 12:09:01 CEST	SiGma Micro	Product: 0034	5&4bb4d45&0&2
2015-09-04 12:20:02 CEST	JMTek, LLC.	Transcend Flash disk	5&1457f427&0&2
2015-09-04 12:20:02 CEST	JMTek, LLC.	Transcend Flash disk	5&1457f427&0&2
2015-09-04 15:23:01 CEST	Unknown	Product: 1234	5&5045dfb&0&2
2015-09-04 15:23:01 CEST	Unknown	Product: 1234	5&5045dfb&0&2
2015-09-04 16:28:56 CEST	JMTek, LLC.	Transcend Flash disk	5&1457f427&0&2
2015-09-04 16:28:56 CEST	JMTek, LLC.	Transcend Flash disk	5&1457f427&0&2
2015-09-04 17:17:42 CEST	SiGma Micro	Product: 0034	5&4bb4d45&0&2
2015-09-04 17:17:42 CEST	SiGma Micro	Product: 0034	5&4bb4d45&0&2
2015-09-07 18:05:47 CEST	JMTek, LLC.	Transcend Flash disk	5&4bb4d45&0&2
2015-09-07 18:05:47 CEST	JMTek, LLC.	Transcend Flash disk	5&4bb4d45&0&2
2015-10-21 15:52:59 CEST		ROOT_HUB	4&16b9d63d&0
2015-10-21 15:52:59 CEST		ROOT_HUB	4&2c291eb0&0
2015-10-21 15:52:59 CEST		ROOT_HUB	4&583c4fa&0
2015-10-21 15:52:59 CEST		ROOT_HUB	4&feb8379&0
2015-10-21 15:52:59 CEST		ROOT_HUB20	4&2232a4e&0
2015-10-21 15:52:59 CEST		ROOT_HUB	4&16b9d63d&0
2015-10-21 15:52:59 CEST		ROOT_HUB	4&2c291eb0&0
2015-10-21 15:52:59 CEST		ROOT_HUB	4&583c4fa&0
2015-10-21 15:52:59 CEST		ROOT_HUB	4&feb8379&0
2015-10-21 15:52:59 CEST		ROOT_HUB20	4&2232a4e&0
2015-10-21 15:53:00 CEST	Pixart Imaging, Inc.	Product: 2700	5&5045dfb&0&8
2015-10-21 15:53:00 CEST	Pixart Imaging, Inc.	Product: 2700	6&28ea3f42&0&0000
2015-10-21 15:53:00 CEST	SiGma Micro	Product: 0034	5&1457f427&0&2
2015-10-21 15:53:00 CEST	Pixart Imaging, Inc.	Product: 2700	5&5045dfb&0&8
2015-10-21 15:53:00 CEST	Pixart Imaging, Inc.	Product: 2700	6&28ea3f42&0&0000
2015-10-21 15:53:00 CEST	SiGma Micro	Product: 0034	5&1457f427&0&2
2015-10-21 15:56:31 CEST	Unknown	Product: 1234	5&5045dfb&0&3

2015-10-21 15:56:31 CEST	Unknown	Product: 1234	5&5045dfb&0&3

Figura 107: dispositivos USB conectados

- Tamaño lógico del fichero: 9934 bytes
- Hash del fichero (MD5): 5b0d26d57ef237d1332802e5c8e8ffdf

C5 $IQC0MZN.ODS

- Descripción: fichero encontrado en la papelera de reciclaje del usuario *Ann*.
- Origen: extraído de la papelera de reciclaje mediante *Autopsy* en el apartado 8.2.3.6
- Contenido:

瀲ₙ□□ĭC:\Users\Ann\Desktop\Pendientes.ods

- MAC time:
  - Modified 2015-09-07 12:58:17 CEST
  - Accessed 2015-09-07 12:58:17 CEST
  - Created 2015-09-07 12:58:17 CEST
  - Changed 2015-09-07 12:58:17 CEST
- Tamaño lógico del fichero: 544 bytes
- Hash del fichero (MD5): 3206f6e0ab9bca176e0ddfd645df0b63

C6 $RQC0MZN.ODS

- Descripción: fichero encontrado en la papelera de reciclaje del usuario *Ann*.
- Origen: extraído de la papelera de reciclaje mediante *Autopsy* en el apartado 8.2.3.6
- Contenido:

Visa	4539456154526870	Concepcion	Perez Pozo
Visa	4532457001051150	Jose Maria	Rodriguez Martinez
Visa	4532657981372410	Ignacio	Torres Fernandez
Visa	4379166568413640	Gabriel	Riba Villar
Visa	4929653751795980	Pilar	Moreno Hernandez
Visa	4532531411046010	Alfonso	Mendez Sanchez
Visa	4485384240029660	Esteban	Reyes Sierrra
Visa	4532227440905600	Juan Antonio	Prado Romero
Visa	4539798471108420	Elvira	Sanchez Diez
Visa	4916277839380970	Federico	Iglesias Ruiz
American Express	372171730251559	Marcos	Rubio Ortiz
American Express	376905910360151	Juan Jose	Roca Moyano
American Express	347170350508035	Adolfo	Castillo Valles

American Express	347899917772631	Ana	Silva Guzman
American Express	372157992412443	Rodolfo	Mora Canales
MasterCard	5187401714297720	Angeles	Cerezo Rojas
MasterCard	5197841039013650	Jesus	Gaspar Barba
MasterCard	5108656187294160	Andres	Cifuentes Bautista

- MAC time:
    - Modified 2015-09-07 12:10:42CEST
    - Accessed 2015-09-07 12:58:11 CEST
    - Created 2015-09-07 12:58:11 CEST
    - Changed 2015-09-07 12:58:18 CEST
- Tamaño lógico del fichero: 544 bytes
- Hash del fichero (MD5): 3206f6e0ab9bca176e0ddfd645df0b63

C7 F0121712.PDF

- Descripción: fichero eliminado y recuperad mediante *File Carving*
- Origen: extraído de la imagen del disco duro mediante *Autopsy* en el apartado 8.2.3.8
- MAC time:
    - Modified 0000-00-00 00:00:00 CEST
    - Accessed 0000-00-00 00:00:00 CEST
    - Created 0000-00-00 00:00:00 CEST
    - Changed 0000-00-00 00:00:00 CEST
- Tamaño lógico del fichero: 47.035 bytes
- Hash del fichero (MD5): 85fce71f4c6eec0670098f1ab35df068

C8 DOCUMENTOS_RECIENTES.XLSX

- Descripción: listado de documentos accedidos recientemente
- Origen: obtenido mediante *Autopsy* en el apartado 8.2.3.10
- Contenido:

Fichero	Ruta de acceso	Fecha	Presente
Disco local (F).lnk	F:\	2015-09-03 16:47:15 CEST	-
pwd.txt.lnk	F:\pwd.txt.txt	2015-09-03 16:47:15 CEST	No
Tarjetas_Ricky.lnk	F:\Tarjetas_Ricky.ods	2015-09-03 17:06:28 CEST	No

Tarjetas_Ricky (2).lnk	C:\Users\Ann\Desktop\Tarjetas_Ricky.txt	2015-09-03 17:07:53 CEST	No
DSCN8344.lnk	C:\Users\Ann\Pictures\Fotos\Fotos Obs Fabra\DSCN8344.bmp	2015-09-03 17:33:47 CEST	Sí
Fotos Obs Fabra.lnk	C:\Users\Ann\Pictures\Fotos\Fotos Obs Fabra	2015-09-03 17:33:47 CEST	Sí
DSCN8345_bis.lnk	C:\Users\Ann\Pictures\Fotos\Fotos Obs Fabra\DSCN8345_bis.bmp	2015-09-03 17:59:28 CEST	No
DSCN8345_bis2.lnk	C:\Users\Ann\Pictures\Fotos\Fotos Obs Fabra\DSCN8345_bis2.gif	2015-09-03 18:03:18 CEST	Sí*
Test.lnk	C:\Users\Ann\Desktop\Test.txt	2015-09-03 18:04:43 CEST	No
DSCN8345_bis (2).lnk	C:\Users\Ann\Pictures\Fotos\Fotos Obs Fabra\DSCN8345_bis.gif	2015-09-03 18:20:01 CEST	Sí*
Crisantemo.lnk	C:\Users\Public\Pictures\Sample Pictures\Chrysanthemum.jpg	2015-09-03 18:53:10 CEST	Sí
Imágenes de muestra.lnk	C:\Users\Public\Pictures\Sample Pictures	2015-09-03 18:53:10 CEST	Sí
DSCN8333.lnk	C:\Users\Ann\Pictures\Fotos\Fotos Obs Fabra\DSCN8333.gif	2015-09-03 21:12:53 CEST	Sí
DSC_6537 (Medium).lnk	C:\Users\Ann\Pictures\Fotos\Fiestas Gracia\DSC_6537 (Medium).JPG	2015-09-03 21:21:53 CEST	Sí
Fiestas Gracia.lnk	C:\Users\Ann\Pictures\Fotos\Fiestas Gracia	2015-09-03 21:21:53 CEST	Sí
pwd2.txt.lnk	C:\Users\Ann\Documents\pwd2.txt.txt	2015-09-03 21:24:55 CEST	Sí
Disco local (E).lnk	E:\	2015-09-03 21:28:59 CEST	-
Descargas.lnk	C:\Users\Ann\Downloads	2015-09-07 12:35:26 CEST	Sí
TheJerm.lnk	C:\Users\Ann\Downloads\TheJerm.rar	2015-09-07 12:40:07 CEST	Sí
Arthur_Conan_Doyle_-_La_catacumba_nueva_-_v1.0.lnk	C:\Users\Ann\Documents\Biblioteca Grammata Libre - v2.5\Cl £ sicos\Novela de Suspense y Policiaca\Doyle\Arthur_Conan_Doyle_-_La_catacumba_nueva_-_v1.0.pdf	2015-09-07 17:43:07 CEST	Sí
Doyle.lnk	C:\Users\Ann\Documents\Biblioteca Grammata Libre - v2.5\Cl £ sicos\Novela de Suspense y Policiaca\Doyle	2015-09-07 17:43:07 CEST	Sí
Arthur_Conan_Doyle_-_El_espanto_de_la_cueva_de_Juan_Azul_-_.lnk	C:\Users\Ann\Documents\Biblioteca Grammata Libre - v2.5\Cl £ sicos\Novela de Suspense y Policiaca\Doyle\Arthur_Conan_Doyle_-_El_espanto_de_la_cueva_de_Juan_Azul_-_.pdf	2015-09-07 18:07:29 CEST	Sí
Arthur_Conan_Doyle_-_El_gato_del_Brasil_-_v1.0.lnk	C:\Users\Ann\Documents\Biblioteca Grammata Libre - v2.5\Cl £ sicos\Novela de Suspense y Policiaca\Doyle\Arthur_Conan_Doyle_-_El_gato_del_Brasil_-_v1.0.pdf	2015-09-07 18:08:00 CEST	Sí

Joseph Thomas Sheridan le Fanu - El fantasma y el ensalmador - v1.0.lnk	C:\Users\Ann\Documents\Biblioteca Grammata Libre - v2.5\Cl £ sicos\Novela de Suspense y Policiaca\LeFanu\Joseph Thomas Sheridan le Fanu - El fantasma y el ensalmador - v1.0.pdf	2015-09-07 18:11:55 CEST	Sí
LeFanu.lnk	C:\Users\Ann\Documents\Biblioteca Grammata Libre - v2.5\Cl £ sicos\Novela de Suspense y Policiaca\LeFanu	2015-09-07 18:11:55 CEST	Sí
Arthur_Conan_Doyle_-_La_aventura_de_Shoscombe_Old_Place_-__.lnk	C:\Users\Ann\Documents\Biblioteca Grammata Libre - v2.5\Cl £ sicos\Novela de Suspense y Policiaca\Doyle\Arthur_Conan_Doyle_-_La_aventura_de_Shoscombe_Old_Place_-__.pdf	2015-09-07 18:13:04 CEST	Sí
H._P._Lovecraft_-_El_modelo_de_Pickman_-_v1.0.lnk	C:\Users\Ann\Documents\Biblioteca Grammata Libre - v2.5\Cl £ sicos\Novela de Suspense y Policiaca\Lovecraft\H._P._Lovecraft_-_El_modelo_de_Pickman_-_v1.0.pdf	2015-09-07 18:15:03 CEST	Sí
Lovecraft.lnk	C:\Users\Ann\Documents\Biblioteca Grammata Libre - v2.5\Cl £ sicos\Novela de Suspense y Policiaca\Lovecraft	2015-09-07 18:15:03 CEST	Sí
Poe.lnk	C:\Users\Ann\Documents\Biblioteca Grammata Libre - v2.5\Cl £ sicos\Novela de Suspense y Policiaca\Poe	2015-09-07 18:16:21 CEST	Sí
Edgar Allan Poe - Silencio - v1.0.lnk	No preferred path found	2015-09-07 18:16:21 CEST	Sí
Poe.lnk	C:\Users\Ann\Documents\Biblioteca Grammata Libre - v2.5\Cl £ sicos\Novela de Suspense y Policiaca\Poe	2015-09-07 18:16:21 CEST	Sí
Edgar Allan Poe - Silencio - v1.0.lnk	No preferred path found	2015-09-07 18:16:21 CEST	Sí
Home.lnk	C:\Users\Tom\Documents\Home.ods	2015-09-07 18:26:35 CEST	No
Contc.lnk	C:\Users\Tom\Documents\Contc.ods	2015-09-07 18:27:33 CEST	Sí
20150907_162819.lnk	C:\Users\Ann\Pictures\Fotos\Otras fotos\20150907_162819.jpg	2015-09-07 19:29:13 CEST	Sí
My Skype Received Files.lnk	C:\Users\Ann\AppData\Roaming\Skype\My Skype Received Files	2015-09-07 19:29:13 CEST	Sí
Otras fotos.lnk	C:\Users\Ann\Pictures\Fotos\Otras fotos	2015-09-07 19:29:37 CEST	Sí
20150907_162718.lnk	C:\Users\Ann\Pictures\Fotos\Otras fotos\20150907_162718.jpg	2015-09-07 19:29:46 CEST	Sí
20150907_162746.lnk	C:\Users\Ann\Pictures\Fotos\Otras fotos\20150907_162746.jpg	2015-09-07 19:29:55 CEST	Sí
ListadoNumeraciones.lnk	C:\Users\Ann\Downloads\ListadoNumeraciones.zip	2015-09-07 19:36:29 CEST	Sí
Extracted.lnk	C:\Extracted	2015-09-07 19:38:44 CEST	Sí
Plantilla despeses.lnk	C:\Extracted\Plantilla despeses.xls	2015-09-07 19:38:44 CEST	Sí

Figura 108: documentos accedidos recientemente

- Tamaño lógico del fichero: 10.587 bytes

- Hash del fichero (MD5): 0e8f06c876df91b9b5d55856c5d10de1

C9 MAIN.DB

- Descripción: BBDD con *logs* de conversaciones de *Skype*
- Origen: extraído de la imagen del disco duro mediante *Autopsy* en el apartado 8.2.3.11
- MAC time:
    - Modified 2015-10-21 15:55:25 CEST
    - Accessed 2015-09-03 18:51:35 CEST
    - Created 2015-09-03 18:51:35 CEST
    - Changed 2015-10-21 15:55:25 CEST
- Tamaño lógico del fichero: 458.752 bytes
- Hash del fichero (MD5): bb68e7232c9bd346db3ad82ebeeda214

C10 20150907_162718.JPG

- Descripción: Imagen con metadatos de coordenadas *GPS*
- Origen: extraído de la imagen del disco duro mediante *Autopsy* en el apartado 8.2.3.12
- Contenido:

Figura 109: primera imagen con datos GPS

- MAC time:
    - Modified 2015-09-07 19:29:05 CEST
    - Accessed 2015-09-07 19:28:59 CEST
    - Created 2015-09-07 19:28:59 CEST
    - Changed 2015-09-07 19:29:05 CEST
- Tamaño lógico del fichero: 1.058.873 bytes
- Hash del fichero (MD5): 68ec0b8cef946e6403d7d222768163fd

C11 20150907_162746.JPG

- Descripción: Imagen con metadatos de coordenadas GPS

- Origen: extraído de la imagen del disco duro mediante *Autopsy* en el apartado 8.2.3.12
- Contenido:

Figura 110: segunda imagen con datos GPS

- MAC time:
    - Modified 2015-09-07 19:29:05 CEST
    - Accessed 2015-09-07 19:28:59 CEST
    - Created 2015-09-07 19:28:59 CEST
    - Changed 2015-09-07 19:29:05 CEST
- Tamaño lógico del fichero: 915.872 bytes
- Hash del fichero (MD5): 994823f3803436b04e0552f36179347a

C12 20150907_162819.JPG

- Descripción: Imagen con metadatos de coordenadas GPS
- Origen: extraído de la imagen del disco duro mediante *Autopsy* en el apartado 8.2.3.12
- Contenido:

Figura 111: tercera imagen con datos GPS

- MAC time:
    - Modified 2015-09-07 19:29:08 CEST
    - Accessed 2015-09-07 19:28:58 CEST
    - Created 2015-09-07 19:28:58 CEST
    - Changed 2015-09-07 19:29:13 CEST
- Tamaño lógico del fichero: 1.916.793 bytes
- Hash del fichero (MD5): 25152d446aa96024f187bc54d81efa6e

C13 DSCN8333.GIF

- Descripción: Imagen con información oculta en un fichero txt (esteganografía).
- Origen: extraído de la imagen del disco duro mediante *Autopsy* en el apartado 8.2.3.12
- Contenido:

Figura 112: imagen con fichero oculto

- MAC time:
    - Modified 2015-09-03 18:03:20 CEST
    - Accessed 2015-09-03 18:03:17 CEST
    - Created 2015-09-03 18:03:17 CEST
    - Changed 2015-09-03 21:12:49 CEST
- Tamaño lógico del fichero: 7.026.074 bytes
- Hash del fichero (MD5): 7d57a47b2e31d0b8c149cedaeb835767

C14 TARJETAS_RICKY.TXT

- Descripción: Fichero oculto dentro de la imagen DSCN8333.GIF (esteganografía) con información de tarjetas bancarias.
- Origen: extraído de la imagen del disco duro mediante *Autopsy* en el apartado 8.2.3.12
- Contenido:

4532472207641240	Juan Ramon	Felices Rodriguez
4532742511361320	Antonia	Cano Bermudez

4916040584664660	Nieves	Sepulveda Diaz
4929624362589750	Pedro	Gimenez Garcia
4556317310821640	Josefa	Herrero Vazquez
4532994302733610	Soledad	Garcia Soto
347747094943519	Eva Maria	Martinez Medina
346686278890925	Alvaro	Menendez Benitez
375536039161138	Rafael	Ibañez Orozco
5500019643068870	Catalina	Vazquez Gamez
5315235040873250	Juan	Alonso Canovas
5432652478052620	Francisco	Sancho Leal

- Tamaño lógico del fichero: 497 bytes
- Hash del fichero (MD5): bc05392eee0d51a7881c7800e94f9b9b

C15 ARTHUR_CONAN_DOYLE_-_LA_AVENTURA_DE_SHOSCOMBE_OLD_PLACE_-__.PDF

- Descripción: PDF con información oculta en su interior (esteganografía).
- Origen: extraído de la imagen del disco duro mediante *Autopsy* en el apartado 8.2.3.12
- Contenido:

5410-2027-1270-4680 Leandro Valero Moyano

5112-3373-9748-5880 Joaquina Miralles Cortes

- MAC time:
  - Modified 2015-09-07 18:13:04 CEST
  - Accessed 2015-09-07 18:13:04 CEST
  - Created 2015-09-04 16:30:13 CEST
  - Changed 2015-09-07 18:13:44 CEST
- Tamaño lógico del fichero: 126.756 bytes
- Hash del fichero (MD5): 58e2e274d873530b81d8026cde2a1330

C16 ARTHUR_CONAN_DOYLE_-_LA_CATACUMBA_NUEVA_-_V1.0.PDF

- Descripción: PDF con información oculta en su interior (esteganografía).
- Origen: extraído de la imagen del disco duro mediante *Autopsy* en el apartado 8.2.3.12
- Contenido:

4916-4198-0562-7420 Aurelia Muñoz Luque

4532-2993-5073-4170 Victor Nuñez Pascual

- MAC time:
    - Modified 2015-09-07 18:09:02 CEST
    - Accessed 2015-09-07 18:09:02 CEST
    - Created 2015-09-04 16:30:13 CEST
    - Changed 2015-09-07 18:09:14 CEST
- Tamaño lógico del fichero: 141.072 bytes
- Hash del fichero (MD5): ce68a4432c8bd24a0f023f498a1f10be

C17 JOSEPH THOMAS SHERIDAN LE FANU - EL FANTASMA Y EL ENSALMADOR - V1.0.PDF

- Descripción: *PDF* con información oculta en su interior (esteganografía).
- Origen: extraído de la imagen del disco duro mediante *Autopsy* en el apartado 8.2.3.12
- Contenido:

```
5281-6485-4498-6410 Mario Padilla Sanz

5499-5853-9072-5730 Javier Fuertes Martin
```

- MAC time:
    - Modified 2015-09-07 18:11:54 CEST
    - Accessed 2015-09-07 18:11:54 CEST
    - Created 2015-09-04 16:30:25 CEST
    - Changed 2015-09-07 18:11:58 CEST
- Tamaño lógico del fichero: 75.548 bytes
- Hash del fichero (MD5): 055d0d733c17f172eb85787d82740e34

C18 H._P._LOVECRAFT_-_EL_MODELO_DE_PICKMAN_-_V1.0.PDF

- Descripción: PDF con información oculta en su interior (esteganografía).
- Origen: extraído de la imagen del disco duro mediante *Autopsy* en el apartado 8.2.3.12
- Contenido:

```
4716-2196-6835-2520 Benito Lopez Lopez

4716-3777-7146-9310 Feliciano Huertas Villar
```

- MAC time:
    - Modified 2015-09-07 18:15:03 CEST
    - Accessed 2015-09-07 18:15:03 CEST
    - Created 2015-09-04 16:30:34 CEST

- Changed 2015-09-07 18:15:08 CEST

- Tamaño lógico del fichero: 128.418 bytes
- Hash del fichero (MD5): 190f9993df62d0fc290802d49768209e

C19 LISTADONUMERACIONES.ZIP

- Descripción: contenedor *ZIP* protegido con contraseña con malware en su interior.
- Origen: extraído de la imagen del disco duro mediante *Autopsy* en el apartado 8.2.3.12
- Contraseña: KaPow581!
- MAC time:
  - Modified 2015-09-07 19:36:29 CEST
  - Accessed 2015-09-07 19:36:23 CEST
  - Created 2015-09-07 19:36:23 CEST
  - Changed 2015-09-07 19:36:29 CEST
- Tamaño lógico del fichero: 62.151 bytes
- Hash del fichero (MD5): 28b6c7e90762a2174a32f9e7a2077f9a

C20 THEJERM.RAR

- Descripción: contenedor *RAR* con malware en su interior
- Origen: extraído de la imagen del disco duro mediante *Autopsy* en el apartado 8.2.3.12
- MAC time:
  - Modified 2015-09-07 12:35:23 CEST
  - Accessed 2015-09-07 12:35:17 CEST
  - Created 2015-09-07 12:35:17 CEST
  - Changed 2015-09-07 12:35:25 CEST
- Tamaño lógico del fichero: 812.659 bytes
- Hash del fichero (MD5): d01c1211d42fb78b7937fbdefca5e573

C21 PWD2.TXT.TXT

- Descripción: fichero de texto con usuarios y contraseñas de correo electrónico.
- Origen: extraído de la imagen del disco duro mediante *Autopsy* en el apartado 8.2.3.12
- Contenido:

```
Annetom22@hotmail.com
```

AnneTom1980!

FromTom75@hotmail.com

Tommane75!

- MAC time:
    - Modified 2015-09-07 18:18:45 CEST
    - Accessed 2015-09-07 18:08:26 CEST
    - Created 2015-09-07 18:08:26 CEST
    - Changed 2015-09-07 18:18:45 CEST
- Tamaño lógico del fichero: 72 bytes
- Hash del fichero (MD5): 9fc3ae950d6d9a7cf1f69dbf138404f5

C22 PWD.TXT.TXT

- Descripción: fichero de texto con usuarios y contraseñas de SO, correo electrónico, *Skype* y *S-tools*.
- Origen: extraído de la imagen del disco duro mediante *Autopsy* en el apartado 8.2.3.13
- Contenido:

SO:

Ann: Tom1980

Tom: Ann1978

S-tools:

KaPow581!

Pwd Tom:

100Pm!710GGh1??6dh**

E-mail:

Annetom22@hotmail.com

pwd: AnneTom1980!

FromTom75@hotmail.com

pwd: Tommane75!

Skype:

Annetom22

pwd:Anneconde22

- MAC time:
    - Modified 2015-09-07 13:48 CEST
    - Created 2015-09-03 21:28:26 CEST
- Tamaño lógico del fichero: 221 bytes
- Hash del fichero (MD5): 255f79dadf9131f91c66a072a63c136c

C23 TARJETAS_RICKY.ODS

- Descripción: Tabla con información de tarjetas bancarias encontrado en volumen cifrado con *TrueCrypt*
- Origen: extraído de la imagen del disco duro mediante *Autopsy* en el apartado 8.2.3.13
- Contenido:

4532472207641240	Juan Ramon	Felices Rodriguez
4532742511361320	Antonia	Cano Bermudez
4916040584664660	Nieves	Sepulveda Diaz
4929624362589750	Pedro	Gimenez Garcia
4556317310821640	Josefa	Herrero Vazquez
4532994302733610	Soledad	Garcia Soto
347747094943519	Eva Maria	Martinez Medina
346686278890925	Alvaro	Menendez Benitez
375536039161138	Rafael	Ibañez Orozco
5500019643068870	Catalina	Vazquez Gamez
5315235040873250	Juan	Alonso Canovas
5432652478052620	Francisco	Sancho Leal

- MAC time:
    - Modified 2015-09-03 17:01:48 CEST
    - Created 2015-09-03 21:28:57 CEST
- Tamaño lógico del fichero: 14.062 bytes
- Hash del fichero (MD5): 0fa1f944c5bfaa86b25e2a8c7b54688f

C24 TOTAL.ODS

- Descripción: Tabla con información de tarjetas bancarias encontrado en volumen cifrado con *TrueCrypt*

- Origen: extraído de la imagen del disco duro mediante *Autopsy* en el apartado 8.2.3.13
- Contenido:

Visa	4532472207641240	Juan Ramon	Felices Rodriguez
Visa	4532742511361320	Antonia	Cano Bermudez
Visa	4916040584664660	Nieves	Sepulveda Diaz
Visa	4929624362589750	Pedro	Gimenez Garcia
Visa	4556317310821640	Josefa	Herrero Vazquez
Visa	4532994302733610	Soledad	Garcia Soto
Visa	4716377771469310	Feliciano	Huertas Villar
Visa	4716219668352520	Benito	Lopez Lopez
Visa	4916419805627420	Aurelia	Muñoz Luque
Visa	4532299350734170	Victor	Nuñez Pascual
Visa	4539456154526870	Concepcion	Perez Pozo
Visa	4532457001051150	Jose Maria	Rodriguez Martinez
Visa	4532657981372410	Ignacio	Torres Fernandez
Visa	4379166568413640	Gabriel	Riba Villar
Visa	4929653751795980	Pilar	Moreno Hernandez
Visa	4532531411046010	Alfonso	Mendez Sanchez
Visa	4485384240029660	Esteban	Reyes Sierrra
Visa	4532227440905600	Juan Antonio	Prado Romero
Visa	4539798471108420	Elvira	Sanchez Diez
Visa	4916277839380970	Federico	Iglesias Ruiz
American Express	347747094943519	Eva Maria	Martinez Medina
American Express	346686278890925	Alvaro	Menendez Benitez
American Express	375536039161138	Rafael	Ibañez Orozco
American Express	370555595834792	Teresa	Gomez Duran
American Express	375388340810866	Maria	Morales Fernàndez
American Express	372171730251559	Marcos	Rubio Ortiz
American Express	376905910360151	Juan Jose	Roca Moyano
American Express	347170350508035	Adolfo	Castillo Valles

American Express	347899917772631	Ana	Silva Guzman
American Express	372157992412443	Rodolfo	Mora Canales
MasterCard	5500019643068870	Catalina	Vazquez Gamez
MasterCard	5315235040873250	Juan	Alonso Canovas
MasterCard	5432652478052620	Francisco	Sancho Leal
MasterCard	5187401714297720	Angeles	Cerezo Rojas
MasterCard	5197841039013650	Jesus	Gaspar Barba
MasterCard	5410202712704680	Leandro	Valero Moyano
MasterCard	5112337397485880	Joaquina	Miralles Cortes
MasterCard	5108656187294160	Andres	Cifuentes Bautista
MasterCard	5281648544986410	Mario	Padilla Sanz
MasterCard	5499585390725730	Javier	Fuertes Martin

- MAC time:
    - Modified 2015-09-07 13:44:26 CEST
    - Created 2015-09-07 13:46:57 CEST
- Tamaño lógico del fichero: 17.816 bytes
- Hash del fichero (MD5): 5ce84b1cfae53afe1cc3b5f5abdf0861

C25 PLACES.SQLITE

- Descripción: fichero historial de navegación del usuario *Ann*.
- Origen: extraído de la imagen del disco duro mediante *Autopsy* en el apartado 8.2.3.14
- MAC time:
    - Modified 2015-09-07 19:36:27 CEST
    - Accessed 2015-09-02 12:30:26 CEST
    - Created 2015-09-02 12:30:26 CEST
    - Changed 2015-09-07 19:36:27 CEST
- Tamaño lógico del fichero: 10485760 bytes
- Hash del fichero (MD5): 799894e4b9a1e717d15ac2ea353fa28d

C26 2015-09-07-2.DC

- Descripción: fichero de texto con registro de las pulsaciones de teclas del usuario *Ann*.

- Origen: extraído de la imagen del disco duro mediante *Autopsy* en el apartado 8.2.3.15
- Contenido:

:: (12:46:25)

:: Enter password for C:\Users\Ann\MyHome (12:47:16)

safePlace

SafePlace

:: pwd.txt: Bloc de notas (12:58:10)

Pwd Tom:

100Pm!710GGh1??6dh**[LEFT][DOWN][LEFT][LEFT][LEFT][LEFT][RIGHT][RIGHT][RIGHT][RIGHT][RIGHT][RIGHT][RIGHT][RIGHT][RIGHT][RIGHT][RIGHT][RIGHT][RIGHT][RIGHT][RIGHT][RIGHT][RIGHT][RIGHT][RIGHT]

:: Program Manager (13:07:21)

[DEL]

:: pwd.txt: Bloc de notas (13:09:15)

E-mail

Annetom22@hotmail.com pwd: AnneTom1980!

:: Página de inicio de Mozilla Firefox - Mozilla Firefox (13:38:17)

:: Enter password for C:\Users\Ann\MyHome (13:38:33)

SafePlace

:: pwd.txt: Bloc de notas (13:46:26)

[DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN]

E-
mail:[UP][UP][UP][UP][UP][UP][RIGHT][RIGHT][RIGHT][RIGHT][RIGHT][RIGHT][RIGHT]:[UP][UP][UP][UP][RIGHT][RIGHT][RIGHT][LEFT]:[DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][RIGHT][RIGHT][RIGHT][RIGHT][RIGHT][RIGHT][RIGHT][RIGHT][RIGHT]

Annetom22@ot[<-][<-]hotmail.com

pwd: AnneTom1980![UP][RIGHT][RIGHT][RIGHT][RIGHT]

Anne>[<-]tom222@hotmail.com[DOWN]

fr[<-][<-]

FromTom75@hotmail.com

pwd: Tommane75!

Skype:

Annetom22

pwd:Anneconde22

:: Disco local (F:) (13:46:33)

:: Página de inicio de Mozilla Firefox - Mozilla Firefox (13:48:27)

c

:: Dropbox (15:01:46)

Aram

:: Archivos compartidos (15:28:15)

m768Aram768[<-][<-][<-][<-][<-][<-][<-][<-]

:: Dropbox (15:28:35)

[DEL]

:: Inicio (16:08:23)

:: Dropbox (16:09:27)

[DEL]

:: Doyle (16:10:17)

:: Dropbox (17:40:59)

:: Archivos de programa (17:53:15)

:: Skype™ - annetom22 (17:55:52)

[DEL][INS][INS][DEL]

:: Página de inicio de Mozilla Firefox - Mozilla Firefox (18:01:47)

avast on line

:: Winhex (18:06:31)

[UP][UP][UP][UP][UP][UP][DEL]

:: Archivos de programa (18:10:27)

:: Doyle (18:10:43)

[DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][UP][UP][UP]

:: Dropbox (18:17:10)

:: Papelera de reciclaje (18:18:02)

:: Inicio (19:24:52)

:: Skype™ - annetom22 (19:38:00)

No te preocupes, yo tambi[<-][<-]en al[<-][<-][<-][<-][<-][<-][<-]en [<-][<-][<-][<-][<-]en algo liada...

Puess[<-] si,[<-][<-][<-][<-]i, lo conozco. Tierne[<-][<-][<-]nes razon, es muy discreto ym[<-][<-][<-]. ¿Que tal esl proximo sabado a las 17:00?[LEFT][DOWN][DOWN][RIGHT][<-]

A ver... Te digo algo...

¿Es lo que parece?

Tiene una constr[<-][<-][<-]traseña y supongo que sera la de sime[<-][<-]empre...

:: Introducir contraseña (19:39:33)

Kapo[<-][<-][<-][<-][<-]KaPoe[<-]w581!KaPow581!

:: Documentos (19:41:09)

[F2][<-]Listado n[<-][<-][<-][<-][<-][<-][<-][<-][<-][<-]Listado numeracions[<-]es

:: Skype™ - annetom22 (19:42:02)

Esto es un poco raro...

De acuerdo!

- MAC time:
    - Modified 2015-09-07 18:18:45 CEST
    - Accessed 2015-09-07 18:08:26 CEST
    - Created 2015-09-07 18:08:26 CEST
    - Changed 2015-09-07 18:18:45 CEST
- Tamaño lógico del fichero: 72 bytes
- Hash del fichero (MD5): 9fc3ae950d6d9a7cf1f69dbf138404f5

C27 SECURITY.EVTX

- Descripción: fichero de *logs* del sistema con eventos de seguridad
- Origen: extraído de la imagen del disco duro mediante *Autopsy* en el apartado 8.2.3.16
- MAC time:
    - Modified 2015-10-21 16:00:52 CEST

    - Accessed 2015-09-02 12:30:26 CEST
    - Created 2015-09-02 12:30:26 CEST
    - Changed 2015-10-21 16:00:52 CEST
- Tamaño lógico del fichero: 1118208 bytes
- Hash del fichero (MD5): d3f9eff558827fbcb736b307a1e5455c

12 ÍNDICE DE FIGURAS