ANALISIS FORENSE

Trabajo Final de Máster.

Nombre Estudiante:	Fredy Omar Morantes Moreno.
Programa:	Máster universitario en Seguridad de las tecnologías de la información y de las comunicaciones.
Nombre Consultor:	Carles Estorach Espinós
Centro:	Universitat Oberta de Catalunya / INCIBE
Fecha entrega:	Enero 2016

FICHA DEL TRABAJO FINAL

Título del trabajo:	Análisis Forense
Nombre del autor:	Fredy Omar Morante Moreno
Nombre del consultor:	Carles Estorach Espinós
Fecha de entrega:	01/2016
Área del Trabajo Final:	Informática Forense
Titulación:	Máster universitario en Seguridad de las tecnologías de la información y de las comunicaciones (MISTIC)

Resumen del Trabajo (máximo 250 palabras):

El presente documento ofrece al lector el análisis forense informático realizado a tres imágenes, una imagen de memoria RAM, una imagen de dispositivo USB y una imagen de un disco duro, imágenes que son utilizadas alrededor de un caso policial y la posible implicación de personas sospechosas en actividades delictivas. De estas circunstancias se desprende la importancia del presente proyecto y su análisis.

Las diferentes etapas del análisis han sido cuidadosamente abordadas utilizando como referencia una de las normas internacionalmente aceptadas en este campo, la norma ISO/IEC 27037. Esta norma abarca puntos muy importantes que han sido valorados dentro de este documento, puntos tan importantes como son las etapas de la metodología propuesta por la ISO, los roles que intervienen en la ejecución de la metodología, los principios que deben cumplir algunos datos para ser considerada evidencia digital.

Adicional al enfoque propuesto en esta norma, el autor ha adoptado una técnica de clasificación particular con el fin de modular el criterio de selección de datos que cumplan los principios de relevancia, confiabilidad y suficiencia. Proponiendo para la resolución del caso una etapa de transición dentro de la etapa de análisis y la etapa de reporte que permite aprovechar la correlación de evidencias potenciales dentro de un amplio rango de datos referentes.

Finalmente el lector obtendrá el resultado del análisis mediante un informe

conciso y claro de los hallazgos y conclusiones del caso.

Abstract:

This document provides the reader with computer forensic analysis to three images, an image of RAM, an image of USB device and an image of a hard disk images that are used around a police case and the possible involvement of suspects in criminal activities. In these circumstances the importance of this project and its analysis shows.

The different stages of the analysis has been carefully addressed using as reference one of the internationally accepted standards in this field, the ISO / IEC standard 27037. This standard covers important points that have been valued in this document, points are as important as stages of the methodology proposed by the ISO, the roles involved in the implementation of the methodology, the principles that data must meet to be considered some digital evidence.

Additional rule proposed in this approach, the author has taken a particular classification technique in order to modulate the data selection criteria respecting the principles of relevance, reliability and sufficiency. Proposing to resolve the case a transitional stage within the stage of analysis and reporting stage that leverages the correlation of potential evidence in a wide range of data references.

Finally, the reader will get the result of analysis by a concise and clear report of findings and conclusions.

Palabras clave:

- Análisis Forense.
- Norma ISO 27037.
- Imagen forense.
- Datos Volátiles.
- Artefactos forenses.
- Data carving.

INDICE

1. INTRODUCCION

1.1 Contexto y justificación del Trabajo.

La Policía ha realizado un allanamiento al domicilio de personas sospechosas de realizar actividades ilícitas, realizando procedimientos de identificación, recolección y adquisición de evidencia digital. Los agentes encargados de realizar estas tareas obtuvieron datos y los almacenaron en los siguientes archivos:

- Captura de memoria RAM.
- Imagen forense de un disco duro.
- Imagen forense de un dispositivo USB.

Estos archivos han sido entregados para realizar las actividades de preservación, análisis y documentación de la evidencia digital. Adicionalmente entregan el registro de cadena de custodia, fotografías de algunos dispositivos, cálculos de hash de los archivos de datos y algunas actas.

La policía desea conocer cualquier indicio de conducta criminal existente dentro de los datos entregados y que puedan ser clasificados como evidencia digital.

Los eventos ocurridos justifican la realización de un análisis informático forense de manera metódica, imparcial y profesional que permita garantizar el buen desarrollo y soporte de la investigación, pues las respuestas obtenidas de este tipo de análisis serán cruciales para las decisiones judiciales del personal competente.

Dentro del análisis solicitado se espera obtener, en términos generales, información que permita consolidar criterios en el momento de emitir un juicio sobre las personas involucradas.

1.2 Objetivos del Trabajo.

1.2.1 Objetivo General.

- Realizar un análisis forense informático sobre los datos entregados por la policía, para obtener evidencias que puedan demostrar las actividades delictivas de los sospechosos.

1.2.2 Objetivos específicos.

- Realizar las actividades del análisis forense siguiendo una estructura metodológica.
- Verificar la integridad de los datos recibidos para el análisis forense.
- Documentar el proceso de análisis forense informático.

- Seleccionar la evidencia que sirva como material probatorio de causa delictiva.
- Emitir un informe pericial con el resumen de hallazgos.

1.3 Enfoque y método seguido.

1.3.1 Guía utilizada.

Para la selección de evidencias se tendrán como guía los conceptos del estándar internacional *ISO/IEC 27037 Information Technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence.*

La norma ISO/IEC 27037 define las siguientes etapas con las respectivas recomendaciones en detalle:

- Identificación.
- Recolección.
- Adquisición.
- Preservación.

El estándar ISO 27037 define dos actores muy importantes dentro de un proceso forense informático, estos actores son el DEFR o primer respondiente quien está a cargo de las etapas de identificación, recolección y adquisición, y el DES o especialista de evidencia digital, quien es el encargado de continuar con las etapas de preservación, análisis y reporte.

La etapa de análisis, que no esta propuesta en la ISO/IEC 27037, será llevado a cabo bajo las siguientes sub etapas:

- Ejecución de pruebas.
- Clasificación.
- Exploración y correlación.

Es importante mencionar que el orden de ejecución de pruebas dentro de un análisis forense informático hace parte de la decisión y criterio propio del analista, el autor así lo considera y lo contempla dentro de la técnica propuesta en la etapa de análisis. El enfoque adoptado dividido en tres sub-etapas pretende que el orden elegido de las pruebas sea independiente de la capacidad de hallazgo de evidencias, pues nada ni nadie garantiza que en el momento de encontrar un archivo cifrado, por ejemplo, ya se halla encontrado una llave de descifrado.

1.3.2 Método de selección de evidencia.

El criterio para seleccionar elementos de las imágenes como evidencia digital será apoyado en los principios propuestos por el estándar ISO/IEC 27037, dichos principios son los siguientes:

- Relevancia: el material seleccionado debe ser importante para la investigación.
- Confiabilidad: los procedimientos usados deben ser auditables y repetibles.
- Suficiencia: el material seleccionado debe ser suficiente o completo para llevar a cabo la investigación.

Aunque gran parte de la tarea de garantizar el cumplimiento de estos principios recae sobre el DEFR, el DES también debe tenerlos en cuenta para los procedimientos que realiza, es decir, en la etapa de preservación, análisis y reporte también se tendrán presentes los tres principios.

1.3.3 Técnica de clasificación de evidencia.

Para lograr el cumplimiento de los principios de Relevancia y Suficiencia es necesario adoptar procedimientos de sub-clasificación a través del análisis.

Dentro de la etapa de análisis, el especialista de evidencia digital, se encuentra con diferentes tipos de evidencia que no pueden ser clasificadas directamente como relevantes y suficientes por sí mismas, estas evidencias pueden obtener un valor relativo cuando sean correlacionadas con otra evidencia.

Máscara de selección de evidencia= XYZ

X = criterio de sospecha, puede ser:

- A = evidencia que genera sospecha en el analista.
- B= evidencia que no genera sospecha.

Y = criterio de relevancia, puede ser:

- 1 = Relevante
- 0 = No Relevante

Z = criterio de suficiencia, puede ser:

- 1 = Suficiente.
- 0 = No Suficiente.

Ejemplo 1 de sub-clasificación:

> Un **password**, puede ser clasificado, dependiendo del criterio del analista, como A10, pues el password puede ser sospechoso y relevante pero por si

mismo no suficiente, ya que no se ha obtenido el “contenedor” en el que pueda ser usado. En este caso el **password** será denominado como **dato** ó **evidencia transicional A10** para la posible obtención de evidencia digital.

Ejemplo 2 de sub-clasificación:

Un conjunto de imágenes con metadatos, podría ser clasificado como A01, aunque existan los suficientes metadatos que demuestren una ubicación y hora pueden parecer en principio no relevantes. En este caso el conjunto de imágenes son datos o evidencias **transicionales A01.**

Matriz Semántica de clasificación:

Clasificación	Descripción	Necesidad
A11	Evidencia digital	Ninguna
A10	Evidencia digital potencial sin suficiencia	Deben ser correlacionados
A01	Evidencia digital potencial sin relevancia	Deben ser correlacionados
A00	Datos descartados o no analizados.	Ninguna.

Tabla 0. Relación semántica.

El objetivo de la sub-clasificación es poder catalogar un conjunto de datos como potencial evidencia sin descartarlo en principio cuando se perciba la ausencia de Relevancia y/o Suficiencia.

Dentro de la etapa de análisis se realizará una sub-etapa de exploración cuyo objetivo es realizar la correlación de datos transicionales encontrados.

Premisas con base en la norma ISO/IEC 27037:

- Toda evidencia digital seleccionada debe ser **A11.**
- Cuando la evidencia digital seleccionada haya sido obtenida a partir de un proceso de sub-clasificación o correlación, los datos **transicionales** también serán conservados sin importar que no sean de tipo A11.

1.3.4 Técnica de Confiablidad.

Con base en la norma ISO/IEC 27037 el principio de Confiabilidad debe ser garantizado dentro de todos los procedimientos realizados a lo largo de las distintas etapas de la metodología.

El analista llevará a cabo cada procedimiento con los detalles necesarios y suficientes para que estos puedan ser auditables y repetibles con las mismas o con otras herramientas, como así sea dispuesto por terceras partes.

1.4 Planificación del Trabajo.

1.4.1 Tareas Planificadas:

Se han definido las actividades necesarias para el cumplimiento de los objetivos propuestos, dichas actividades han sido clasificadas de acuerdo a su naturaleza dentro del grupo de procesos que plantea la metodología PMBOK, iniciando desde la asociación correspondiente a Planificación seguida del grupo Ejecución y posteriormente el Cierre.

Se han propuesto, dentro del listado, algunas actividades denominadas "Actividad de gestión del tiempo, AGT#", con este tipo de actividades se pretende verificar el estado de avance del proyecto y su correspondencia con lo planificado, siendo este lapso un espacio propicio para algunas correcciones, si es el caso.

Grupo de procesos PMBOK	
Entregas parciales	
Actividades de gestión de tiempo	
Entrega final	

Tabla 1: convención de grupos.

PLANIFICACION
Definición del tiempo disponible para dedicación al proyecto.
Búsqueda de bibliografía general (Metodología, Técnicas)
Investigación sobre herramientas de análisis forense informático.
Redacción de la Planificación
Entrega parcial P1 (Planificación. Oct. 2)
Selección de herramientas que harán parte del entorno de trabajo.
Actividad de gestión de integración selección-configuración.
Configuración del entorno de trabajo.
Actividad de gestión del tiempo, AGT1
EJECUCION
Verificación de la cadena de custodia
Actividades de Preservación de Datos.
Redacción de extremos.
Actividades de análisis RAM.
Profundización teórica en RAM
Identificación de artefactos
Pruebas técnicas
Actividades de análisis USB.
Profundización teórica en dispositivos USB
Identificación de artefactos

Pruebas técnicas
Entrega parcial P2 (RAM, USB, EXTREMOS)
Actividades de análisis de disco duro.
Redacción de memoria Versión 1.
Entrega parcial P3 (Memoria V1 y análisis DD. Dic. 11)
CIERRE
Redacción de memoria Versión 2 (final)
Realización de la Presentación.
Entrega memoria FINAL y Presentación. (4 ENERO)
Realización de video.

Tabla 2: Agrupación de actividades.

1.4.2 Disposición de tiempo.

La planificación temporal de las actividades ha sido definida teniendo en cuenta la disposición de tiempo del analista forense, esta disposición semanal se presenta a continuación, las "horas dedicadas" son aquellas horas fijas diarias de dedicación al proyecto, las "horas de contingencia" son aquellas horas diarias con las que se cuenta para el proyecto pero con un esfuerzo de dedicación mayor y que serán dedicadas si alguna desviación o materialización de riesgo ocurre.

	LUNES	MARTES	MIERCOLES	JUEVES	VIERNES	SABADO	DOMINGO
Horas Dedicadas	**2,5**	**2,5**	**2**	**2**	**2,5**	**7**	**3**
Horas de contingencia	**1**	**1**	**1**	**0**	**1**	**5**	**2**

Tabla 3: disponibilidad diaria.

Adicional a las horas de contingencia se cuentan con 6 días festivos no laborales (Calendario de Colombia GMT -05:00) para resolver cualquier contratiempo o retraso que pueda surgir, la siguiente tabla muestra la planificación para estos días:

	OCT 12 2015	NOV 2 2015	NOV 16 2015	DIC 8 2015	DIC 25 2015	ENE 1 2016
Horas adicionales a la Tabla 1	**6**	**6**	**6**	**4**	**4**	**4**

Tabla 4: Disponibilidad de contingencia.

1.4.3 Asignación de tiempos.

Para la definición del inicio y fin de cada grupo de procesos dentro del proyecto (Planificación, Ejecución, Cierre), se decidió tener como referencia aquellas fechas en las cuales el cliente ha solicitado la entrega de algún documento parcial que evidencie el avance del proyecto. Aunque de cumplirse los tiempos con esta programación haría que el cliente obtenga resultados muy rápido, también conlleva un mayor esfuerzo de parte del analista forense, es por eso que se ha dispuesto de un amplio número de horas de trabajo para este fin.

A continuación el rango de cada grupo de procesos:

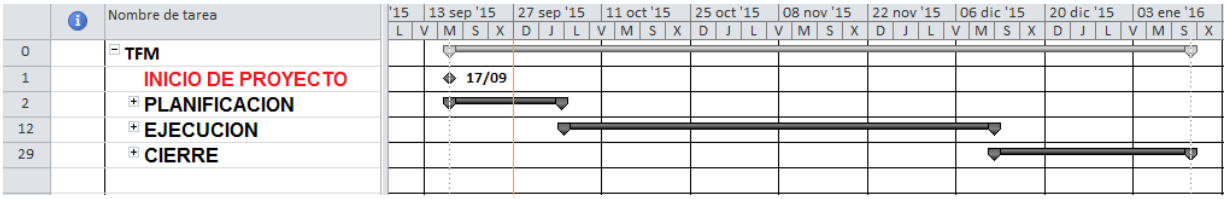


Imagen 1: planificación por grupo.

Tareas detalladas por fecha de inicio y fecha fin:

TFM				TFM			
Id		Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
0			**TFM**	**117 días?**	**jue 17/09/15**	**lun 11/01/16**	
1			INICIO DE PROYECTO	0 días	jue 17/09/15	jue 17/09/15	
2			**PLANIFICACION**	**18 días?**	**jue 17/09/15**	**dom 04/10/15**	
3			Definición del tiempo disponible para dedicación al proyecto.	1 día?	jue 17/09/15	jue 17/09/15	
4			Busqueda de bibliografía general (Metodologia, Tecnicas)	4 días?	vie 18/09/15	lun 21/09/15	3
5			Investigación sobre herramientas de análisis forense informático.	4 días?	mar 22/09/15	vie 25/09/15	4
6			Redacción de la Planificacion	8 días?	mié 23/09/15	mié 30/09/15	
7			Entrega parcial P1 (Planificación. Oct. 2)	1 día?	jue 01/10/15	jue 01/10/15	6
8			Selección de herramientas que harán parte del entorno de trabajo.	3 días?	sáb 26/09/15	lun 28/09/15	5
9			Actividad de gestión de integración selección-configuración.	2 días?	mar 29/09/15	mié 30/09/15	8
10			Configuración del entorno de trabajo.	3 días?	jue 01/10/15	sáb 03/10/15	9
11			Actividad de gestión del tiempo, AGT1	1 día?	dom 04/10/15	dom 04/10/15	10
12			**EJECUCION**	**68 días?**	**lun 05/10/15**	**vie 11/12/15**	
13			Verificación de la cadena de custodia	2 días?	lun 05/10/15	mar 06/10/15	11
14			Actividades de Preservación de Datos.	2 días?	mié 07/10/15	jue 08/10/15	13
15			Actividad de gestión del tiempo, AGT2	1 día?	vie 09/10/15	vie 09/10/15	14
16			Redacción de extremos.	2 días?	sáb 10/10/15	dom 11/10/15	15
17			**Actividades de análisis RAM.**	**10 días?**	**lun 12/10/15**	**mié 21/10/15**	**16**
18			Profundización teórica en RAM	3 días?	lun 12/10/15	mié 14/10/15	
19			Identificación de artefactos	3 días?	jue 15/10/15	sáb 17/10/15	18
20			Pruebas tecnicas	1 día?	mié 21/10/15	mié 21/10/15	19
21			**Actividades de análisis USB.**	**9 días?**	**jue 22/10/15**	**vie 30/10/15**	**17**
22			Profundización teórica en dispositivos USB	3 días?	jue 22/10/15	sáb 24/10/15	
23			Identificación de artefactos	3 días?	dom 25/10/15	mar 27/10/15	22
24			Pruebas tecnicas	3 días?	mié 28/10/15	vie 30/10/15	23
25			Entrega parcial P2 (RAM, USB, EXTREMOS)	24 días?	mié 07/10/15	vie 30/10/15	13,21FF
26			Actividades de análisis de disco duro.	17 días	sáb 31/10/15	mar 17/11/15	25
27			Redacción de memoria Versión 1.	15 días	mar 17/11/15	mié 02/12/15	26
28			Entrega parcial P3 (Memoria V1 y análisis DD. Dic. 11)	9 días	jue 03/12/15	vie 11/12/15	27
29			**CIERRE**	**31 días?**	**sáb 12/12/15**	**lun 11/01/16**	
30			Redacción de memoria Versión 2 (final)	15 días	sáb 12/12/15	sáb 26/12/15	28
31			Realización de la Presentación.	8 días	dom 27/12/15	dom 03/01/16	30
32			Entrega memoria FINAL y Presentación. (4 ENERO)	1 día?	lun 04/01/16	lun 04/01/16	31
33			Realización de video.	7 días	mar 05/01/16	lun 11/01/16	32

Imagen 2: planificación por actividad

Diagrama de Gantt de las actividades propuestas para el proyecto:

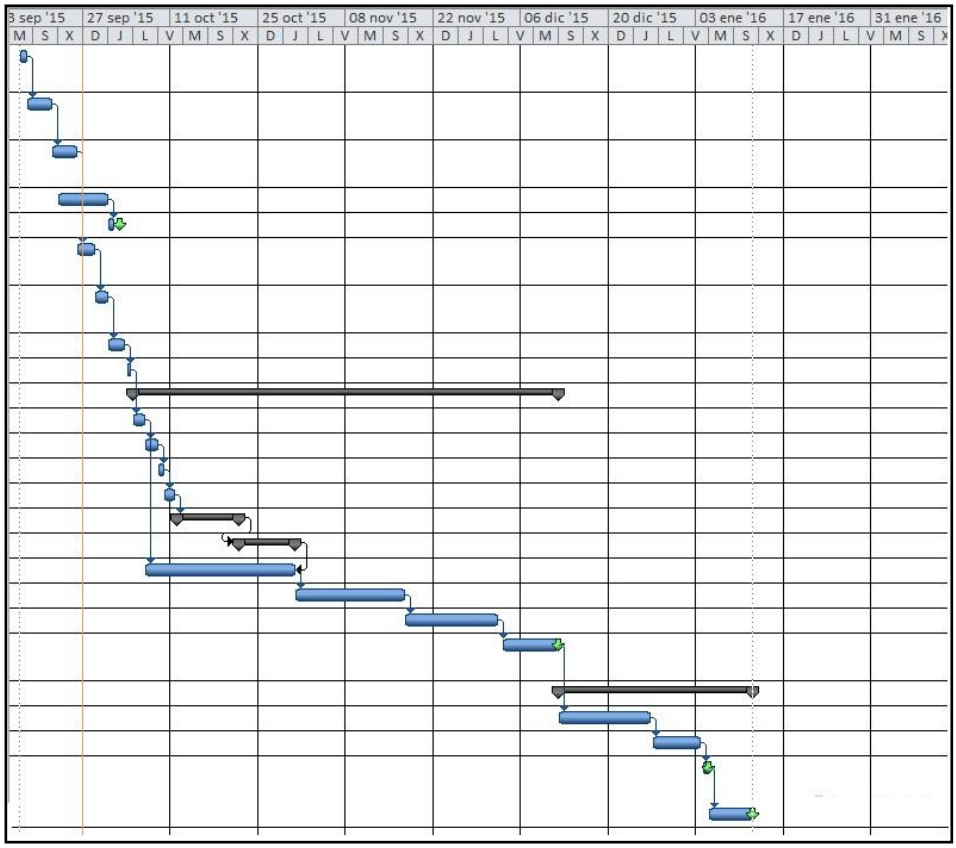


Imagen 3: diagrama de Gantt.

1.5 Resumen de productos obtenidos.

- Será entregado un documento que contiene el alcance del proyecto, la planificación de tiempos del proyecto, metodología empleada y técnicas utilizadas.
- Será entregado un documento que contiene los pasos de verificación de integridad y cadena de custodia de los archivos recibidos.
- Será entregado un documento donde se registran los pasos detallados que realizo el analista para obtener las evidencias.
- Será entregado un directorio con los archivos seleccionados como evidencia por el analista.
- Se entregará un informe pericial con el resumen de hallazgos.

1.6 Descripción de capítulos.

- Capitulo 2:
  En el capítulo 2 se presentan los extremos y pruebas técnicas que serán realizadas por el analista. Solamente se realiza una breve descripción de las pruebas técnicas,

NO se lleva a cabo la ejecución de cada una de ellas, la ejecución de las pruebas se realizarán en capítulos posteriores.

- Capitulo 3:
  En este capítulo se registran los pasos realizados por el analista al ejecutar las pruebas técnicas sobre la imagen de dispositivo USB, el archivo USB.E01.

- Capitulo 4:
  En este capítulo se registran los pasos realizados por el analista al ejecutar las pruebas técnicas sobre la imagen de memoria RAM, el archivo ANN-PC-20151021-135652.raw.

- Capitulo 5:
  En este capítulo se registran los pasos realizados por el analista al ejecutar las pruebas técnicas sobre la imagen de disco duro, el archivo ANN-PC-20151021-135652.raw.

2. EXTREMOS Y PRUEBAS TECNICAS.

2.2 EXTREMOS PROPUESTOS.

A continuación se detallan los extremos globales del análisis de las tres imágenes:

EXTREMO	PROPOSITO
¿Existen rastros de almacenamiento o ejecución de programas maliciosos? ¿A qué cuenta de usuario pertenecen?	Saber si puede haber terceros interactuando con el computador.
¿Cuántas cuentas de usuario existen en el sistema analizado?	Obtener bases de la utilización del computador.
¿Es posible conocer la fecha de creación de cuentas de cada usuario registrado en el sistema? De ser así, ¿Cuál es?	Obtener puntos de referencias de la utilización del computador.
¿Cuál ha sido el usuario con más accesos al computador?	Obtener estadísticas determinantes.
¿Qué programas se estaban ejecutando en el momento de la adquisición de los datos?	Conocer detalles de la utilización de la última sesión del usuario o usuarios que trabajaban en el computador.
¿Se han encontrado imágenes que evidencien temas de carácter delictivo? ¿Qué usuario es el dueño?	Reunir evidencia para determinar el perfil del usuario.
¿Desde qué cuenta de usuario se ha accedido a dispositivos de almacenamiento externo? ¿Cuál es el identificador del dispositivo? ¿Fecha y hora de acceso?	Obtener trazabilidad del computador y los dispositivos externos conectados.
¿Se han encontrado mensajes cuyo contenido evidencia una actividad delictiva?	Conocer si el usuario trata temas delictivos con terceros.
¿Se han usado herramientas criptográficas en el computador encontrado? ¿De ser cierto, que usuario accedió a ellas?	Conocer la capacidad, conocimiento y propósitos técnicos del usuario.
¿Se han encontrado rastros de visitas a páginas web con contenido de carácter delictivo? ¿De ser cierto, que usuario las visitó y en qué fecha?	Conocer hábitos, intereses y gustos de navegación a través de la web.

Tabla 5: Extremos.

2.3 PRUEBAS TECNICAS.

A continuación se muestra el listado de pruebas técnicas que se realizarán sobre las tres (3) imágenes obtenidas, las pruebas han sido clasificadas de acuerdo a los tipos de datos que contienen cada una estas imágenes. Aunque las pruebas se lleven a cabo de forma independiente, se tiene como objetivo relacionar los resultados y complementarlos entre sí.

Las diferentes pruebas técnicas permitirán obtener información para resolver los extremos propuestos.

2.3.1 Memoria RAM.

A continuación se señalan y describen el conjunto de pruebas que serán ejecutadas en la etapa de análisis.

En este conjunto de pruebas se obtendrán información importante como resultado del análisis de los datos volátiles.

Los resultados serán debidamente analizados e interpretados en el capítulo correspondiente a la ejecución de estas pruebas técnicas.

Prueba	Herramienta	Descripción
Identificar el sistema operativo.	Volatility Framework.	La memoria RAM puede ofrecer en la mayoría de los casos un reconocimiento básico del sistema operativo sobre el cual se realizo la captura.
Identificar los procesos que se estaban ejecutando en el sistema.	Volatility Framework.	Obtener un listado básico de los procesos ejecutados en el momento de la captura conlleva al analista a definir medianamente el panorama de ejecución dentro del equipo investigado mediante la búsqueda de procesos sospechosos, esto permite ir disminuyendo el rango de búsqueda.
Obtener una estructura de procesos ejecutados en el momento de la captura, correlacionados entre sí.	Volatility Framework.	Después de haber obtenido un listado de los procesos ejecutados en el sistema es importante realizar un análisis de correlación entre los procesos como lo es una estructura jerárquica con la cual se evidencien procesos padres e hijos, en especial si en la prueba anterior se detecto uno o varios procesos sospechosos.
Buscar objetos de la estructura EPROCESS con o sin enlace entre si	Volatility Framework.	Habiendo obtenido el listado de procesos ejecutados en el sistema será útil obtener otro listado de procesos pero con aquellos procesos ocultos al sistema, con estos dos listados se realizará una comparación para obtener el identificador de archivos que salen en el segundo listado y que no salen en el primero.
Verificar las librerías asociadas a los diferentes procesos.	Volatility Framework.	Esta prueba estará sujeta a la detección de procesos sospechosos, en caso de ser positivo, se realizara un análisis sobre las librerías relacionadas con estos procesos.
Identificar los archivos abiertos por cada proceso.	Volatility Framework.	Esta prueba estará sujeta a la detección de procesos sospechosos, en caso de ser positivo, se realizara un análisis sobre los documentos relacionados con estos procesos.
Revisar la existencia de	Volatility	Es importante recuperar los hashes de las

password de cuentas de usuario del sistema.	Framework.	cuentas de usuario del sistema en los registros, ya que estas contraseñas pueden ser útiles para correlación con otros artefactos.

Tabla 6: pruebas memoria RAM

2.3.2 Imagen de disco y memoria USB.

Teniendo en cuenta que los procedimientos para llevar a cabo las pruebas técnicas en las imágenes de disco y memoria USB son muy similares se han estructurado en la siguiente tabla sin hacer distinción entre ellas, por ejemplo, la verificación de archivos cifrados se llevará a cabo bajo un procedimiento similar en ambas imágenes, sin embargo el detalle de la prueba, con su respectivo procedimiento, será descrito en el capítulo 4 para la imagen de memoria RAM y en el capítulo 5 para la imagen de disco.

CATEGORIA DE LA PRUEBA	HERRAMIENTA	DETALLE DE LA PRUEBA
Análisis del sistema operativo.	• Autopsy. • OSForensics	• Identificación del número de Particiones. • Identificación del sistema de archivo utilizado. • Identificación de cuentas de usuario. • Identificación de fechas de acceso, encendido y apagado. • Identificación de tamaño y espacios asignados de cada volumen. • Historial de uso de programas. • Análisis de registro del sistema. • Análisis de metadatos.
Verificación de archivos.	• Autopsy. • OSForensics. • Kali Linux.	• Identificación de archivos huérfanos. • Realización de análisis *data carving.* • Revisión de archivos existentes en espacios *unallocated.* • Identificación y análisis de archivos cifrados para intentar acceder a su contenido. • Análisis de metadatos de los diferentes archivos.
Estudio de seguridad.	• Autopsy. • OSForensics	• Detección y análisis de malware.
Análisis de dispositivos	• Autopsy. • OSForensics. • Kali Linux	• Rastreo de dispositivos conectados al equipo investigado. • Definición del uso temporal de dispositivos conectados al equipo.
Análisis Web	• Autopsy. • OSForensics • Kali Linux	• Análisis de descargas.
Análisis de	• Autopsy.	• Verificación de archivos generados por

aplicaciones	• OSForensics. • Kali Linux	aplicaciones como Skype, TeamViewer, clientes de correo, entre otros. • Identificación y extracción de bases de datos para análisis del contenido.

Tabla 7: pruebas técnicas de disco y USB.

3. ANALISIS DE IMAGEN DE DISPOSITIVO USB

3.1 Ficha técnica de archivos recibidos:

#	Nombre	Tamaño	Md5 calculado	Sha1 calculado
1	USB.E01	860,386 bytes	AD5F8B40099C92711 BF72EBB9E110EDF	76DAA933056823DB3E2B 370D43D2C7428B07E33C

Tabla 8: ficha técnica USB

3.2 Verificación de integridad:

Enlace	Nro. Evidencia asignado
http://cv.uoc.edu/adf/~cv151_m1_833_web01/USB/USB.log.txt	U32

Tabla 9: información de integridad.

Se accedió a la siguiente información de la imagen USB.E01 mediante el enlace proporcionado:

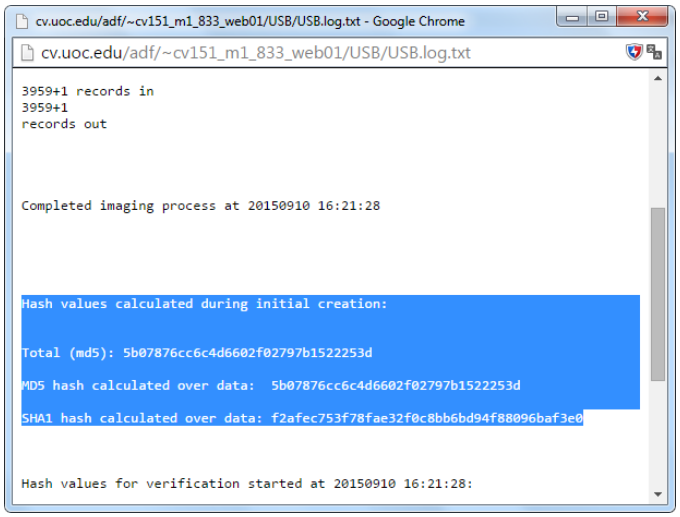


Imagen 4: Valores hash de RAM

Hash	Recibido	Calculado	Resultado
Md5	5b07876cc6c4d6602f02797b1522253d	5B07876CC6C4D6602F02797B1522253D	**Coincide**

Tabla 10: verificación de integridad.

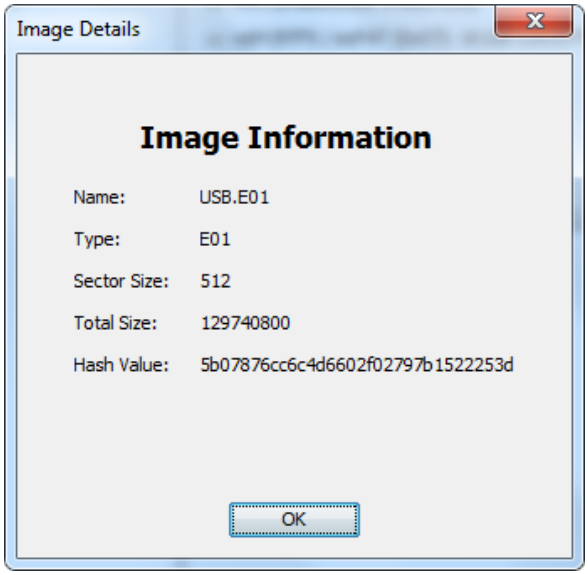


Imagen 5: verificación md5

Se procede a la realización de las pruebas técnicas.

3.3 Pruebas Técnicas.

El análisis de la imagen de dispositivo USB se llevará a cabo bajo la siguiente herramienta:

Nombre	Tamaño	Versión	Hash md5
Autopsy 3.1.3 con Sleuth Kit versión 4.1.3	334,132,224 Bytes	3.1.3 de 32 bits	A7F36C04445A65DA46CF6CA00FC86F81

Tabla 11: versión Autopsy.

3.3.1 Procedimiento de inicio.

- Se crea un caso en el Autopsy utilizando el archivo USB.E01.
- Nombre del caso: TFM_USB1
- Numero: U001.
- Examinador: Fredy Omar Morantes.
- Imagen del caso: USB.E01

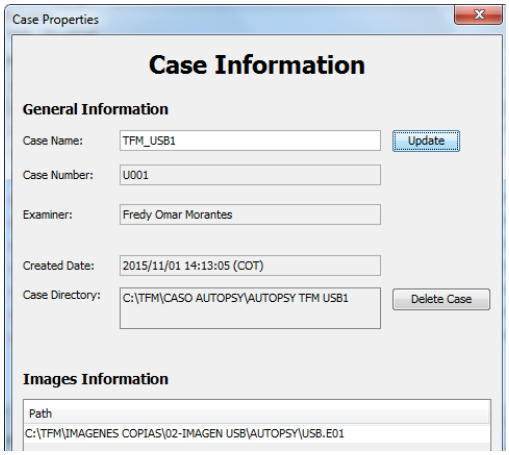


Imagen 6: creación del caso.

La herramienta muestra los siguientes detalles generales de la imagen:

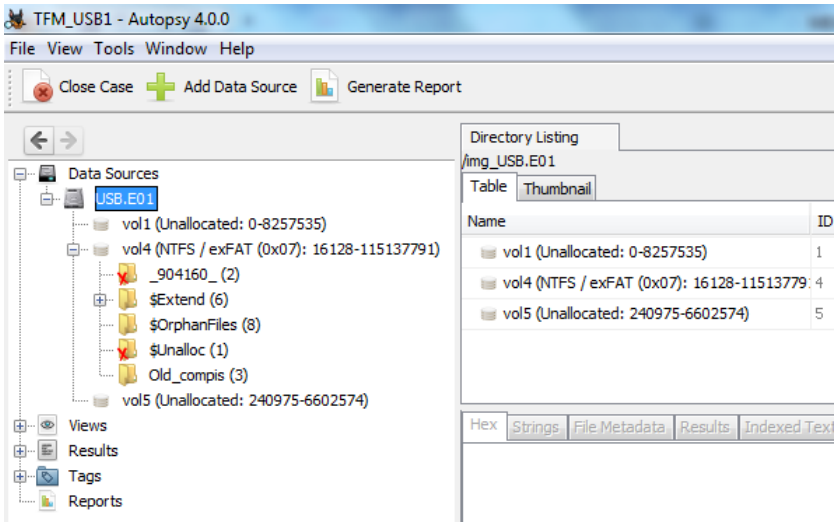


Imagen 7: Árbol de navegación del caso.

La estructura del caso creado muestra como directorio raíz el siguiente nodo: /img_USB.E01/.

3.3.2 Realización de *data carving.*

A. Hallazgos:

Se encontraron doce (12) archivos utilizando el modulo de *carving* nativo de *Autopsy*.

También se encontró un archivo llamado *Unalloc_59_8531968_123375616* en la ruta /img_USB.E01/vol_vol4/$Unalloc/Unalloc_59_8531968_123375616, este archivo no tiene una extensión que permita la identificación de su tipo.

B. Procedimiento:

El archivo *Unalloc_59_8531968_123375616* ha sido exportado del caso para un análisis detallado por medio de la distribución *Kali Linux 2.0* y su herramienta *Foremost* para la recuperación de archivos basados en sus encabezados o su estructura de datos interna.

El archivo fue cargado dentro de una maquina virtual con la distribución *Kali* previamente instalada. Se muestra el proceso de extracción a continuación con los siguientes parámetros:

 # Foremost Unalloc_59_8531968_123375616

Imagen 8: data carving con Foremost.

Después de unos segundos la herramienta ha creado un directorio llamado *output* con los resultados de la recuperación.

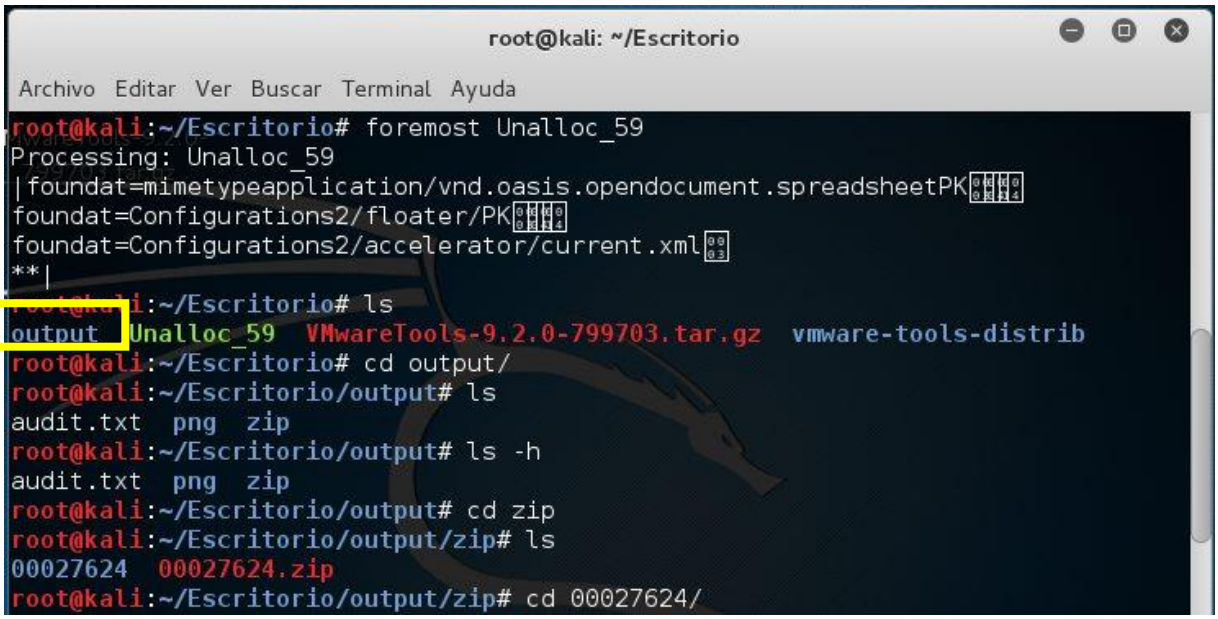


Imagen 9: resultado del proceso de carving.

En el directorio de salida *output* se observan tres elementos, un directorio llamado *png,* otro llamado *zip* y un archivo de nombre *audit.txt* que contiene el registro de hora fecha y nombre de los archivos extraídos.

Dentro del directorio *png* se encuentra una imagen con el nombre *00027625.png*. La imagen describe un formato de dos columnas, la primera columna contiene datos de tipos de tarjetas bancarias conocidas, como *visa, mastercard y american express.* La segunda columna contiene datos de números relativos a cada tipo de tarjeta, la cantidad de caracteres de cada número coincide con la cantidad de caracteres reales que tiene una tarjeta de crédito según su tipo.

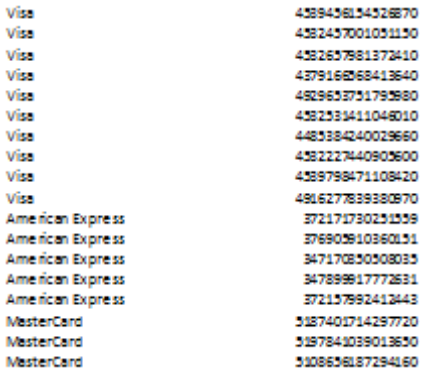


Imagen 10: imagen recuperada mediante carving

Debido al carácter de privacidad que tienen los números de tarjetas de crédito se determina que esta imagen es relevante para la demostración de acceso no autorizado o un posible fraude.

C. Clasificación:

Por falta de relevancia los doce (12) archivos clasificados como huérfanos han sido descartados como evidencia para el caso.

La imagen extraída del archivo *Unalloc_59_8531968_123375616* ha sido preservada como evidencia por la información que se observa en la imagen recuperada después del proceso de carving:

Nombre	Descripción	Hash md5	Tamaño bytes	Clasificación de evidencia
00027625.png	Resultado Foremost extraído de archivo *Unalloc_59_8531968_123375616*	945EDCB2F7B7671DFCAA43A3C781D62B	5816	A10
Unalloc_59_8531968_123375616	Archivo exportado de la ruta /img_USB.E01/vol_vol4/$Unalloc/	09108F7E36EA92F3F4C7F287120F0917	104865792	A10

Tabla 12: clasificación data carving

D. Soportes:

12 Archivos huérfanos encontrados:

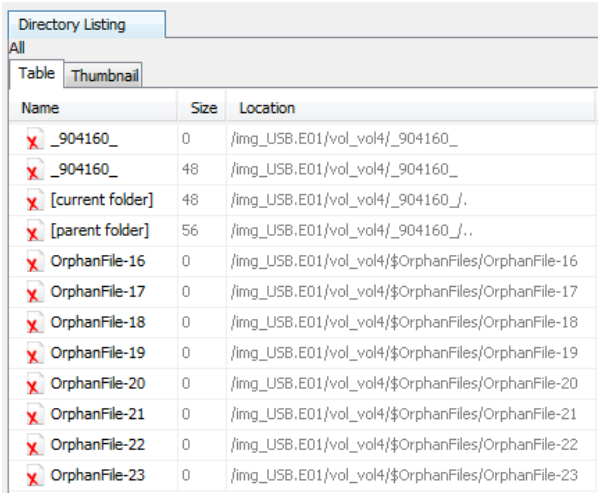


Imagen 11: archivos huérfanos encontrados.

E. Herramientas adicionales de apoyo:

Nombre	Tamaño	Versión	Hash md5
kali-linux-2.0-i386.iso	3403579392 Bytes	2.0 de 32 bits	B7464D3447811C886D141 B2C7F6CE33E
Foca	5458456	3.4.3.0 de 32 bits	E9F7F9430619614E66920 187FDCF1E5B

Tabla 13: herramientas de apoyo data carving

3.3.3 Clasificación de archivos de carácter delictivo.

A. Hallazgos:

Se hallaron los archivos sospechosos con las siguientes características, la ruta dentro del caso TFM_USB1 se muestra a continuación:

Ruta/nombre.	Tamaño. (bytes)
/img_USB.E01/vol_vol4/Pendientes.ods	15766
/img_USB.E01/vol_vol4/Old_compis/whatsapp_castellano.db	26624

Tabla 14: Hallazgos delictivos USB

B. Procedimiento:

Archivo Pendientes.ods:

El archivo Pendientes.ods ha sido extraído de la imagen para visualizarlo mediante el programa adecuado:

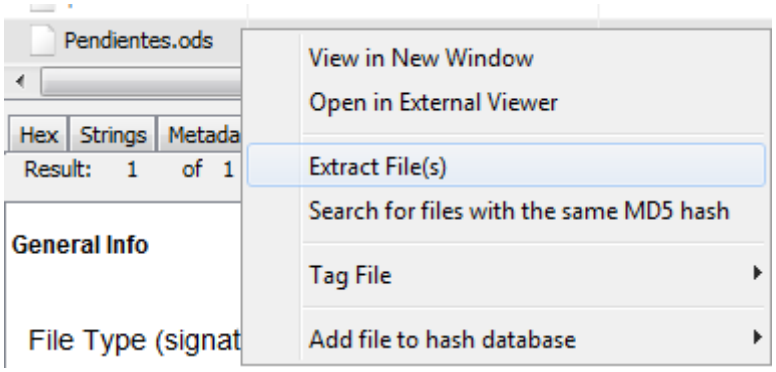


Imagen 12: extracción de archivo Pendientes.ods

El archivo se ha visualizado con el programa *Openoffice Calc.* Por medio del cual se han observado 18 registros con datos sospechosos relacionados con información de tarjetas de crédito.

Con la herramienta *Foca* se ha verificado los metadatos del archivo obteniendo detalles del nombre del computador y usuario creador del archivo *Pendientes.ods.*

Archivo *whatsapp_castellano.db:*

El archivo *whatsapp_castellano.db* ha sido extraído del caso para su correcta visualización con el programa *SQLitebrowser*.

Este archivo contiene datos almacenados de forma estructurada a través de filas y columnas, una estructura llamada *"*chat_list*"*, una estructura llamada "messages" y otra llamada "sqlite_sequence" con solo dos (2) registros.

Los elementos estructurales dentro del archivo se muestran a continuación:

# Elemento	Nombre	Tipo	Observación.
1	chat_list	Tabla	5 registros.
2	messages	Tabla	62 registros.
3	sqlite_sequence	Tabla	2 registros.

Tabla 15: estructura interna db

En el elemento # 2, "messages", se encuentran algunos mensajes con información sospechosa que hace referencia a planificación de algunas actividades delictivas.

C. Clasificación:

Los archivos exportados desde el caso forense TFM_U001se consideran relevantes para la investigación, por lo tanto se procede a etiquetarlos como evidencia:

Nombre	Descripción	Hash md5	Tamaño bytes	Clasificación de evidencia	Usuario identificado
/img_USB.E01/vol_vol4/Pendientes.ods	Hoja de cálculo con registros sospechosos de tarjetas bancos	6da97888ff474194bedc0cf99b5f67de	15766	A10	Jacob
/img_USB.E01/vol_vol4/Old_compis/whatsapp_castellano.db	Base de datos de mensajes	17c1db82b4827c126ccbcdc42de4d711	26624	A11	

Tabla 16: clasificación de Pendientes y Whatsapp

D. Soportes:

Muestra de la evidencia potencial Pendientes.ods

	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

Imagen 13: registros dentro de Pendientes.ods

El archivo *Pendientes.ods* tiene un formato de datos de cuatro columnas y dieciocho filas, la primera columna contiene datos de tipos de tarjetas bancarias conocidas, como *visa, mastercard y american express.* La segunda columna contiene datos de números relativos a cada tipo de tarjeta, la cantidad de caracteres de cada número coincide con la cantidad de caracteres reales que tiene una tarjeta de crédito según su tipo. La tercera columna contiene nombres de personas, la cuarta columna contiene el respectivo apellido de cada persona de la tercera columna.

Se observa una relación directa entre este archivo y la imagen # 10 de nombre *00027625.png* obtenida en la prueba *3.3.2 Realización de data carving*

Debido al carácter de privacidad que tienen los números de tarjetas de crédito se determina que este archivo es relevante para la demostración de un posible fraude con tarjetas de crédito.

Muestra de análisis de metadatos:

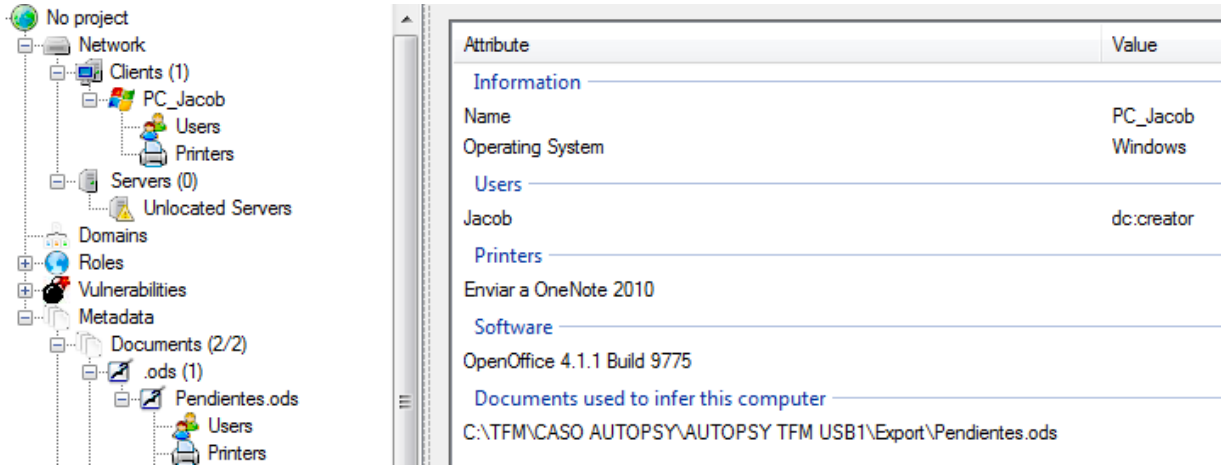


Imagen 14: metadatos en pendientes.ods

Muestras de la evidencia potencial whatsapp_castellano.db:

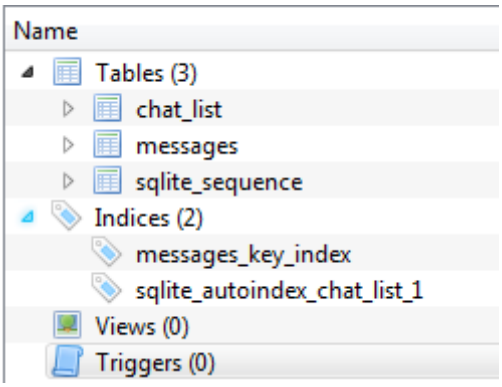
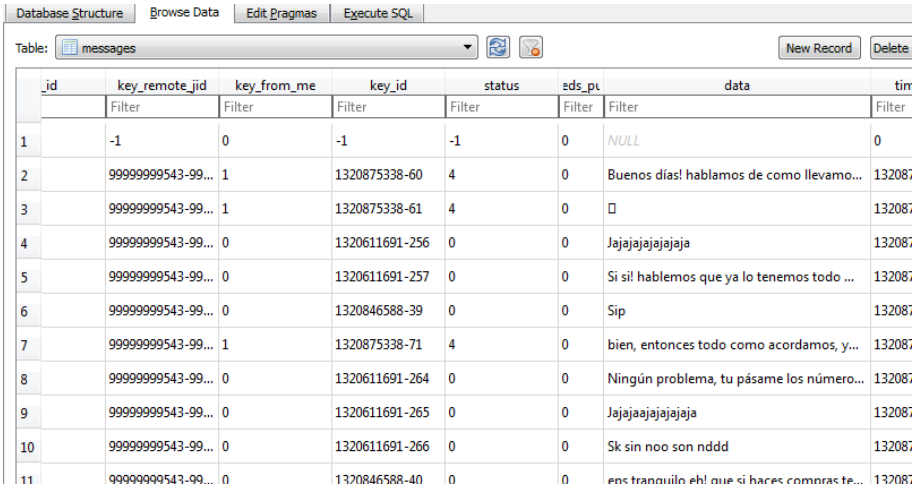


Imagen 15: estructura de información.

Se muestra un fragmento de la estructura de mensajes encontrada, los registros completos de esta estructura son explorados en su totalidad en el *Capítulo 6 Exploración y Correlación de evidencia.*



	_id	key_remote_jid	key_from_me	key_id	status	eds_pu	data	tim
		Filter	Filter	Filter	Filter	Filter	Filter	Filter
1		-1	0	-1	-1	0	NULL	0
2		99999999543-99...	1	1320875338-60	4	0	Buenos días! hablamos de como llevamo...	132087
3		99999999543-99...	1	1320875338-61	4	0	□	132087
4		99999999543-99...	0	1320611691-256	0	0	Jajajajajajaja	132087
5		99999999543-99...	0	1320611691-257	0	0	Si si! hablemos que ya lo tenemos todo ...	132087
6		99999999543-99...	0	1320846588-39	0	0	Sip	132087
7		99999999543-99...	1	1320875338-71	4	0	bien, entonces todo como acordamos, y...	132087
8		99999999543-99...	0	1320611691-264	0	0	Ningún problema, tu pásame los número...	132087
9		99999999543-99...	0	1320611691-265	0	0	Jajajaajajajaja	132087
10		99999999543-99...	0	1320611691-266	0	0	Sk sin noo son nddd	132087
11		99999999543-99...	0	1320846588-40	0	0	eps tranquilo eh! que si haces compras te...	132087

Imagen 16: registros tabulados.

E. Herramientas adicionales de apoyo:

Nombre	Tamaño	Versión	Hash md5
SQLitebrowser	19,314,370 bytes	3.7.0 de 32 bits	FC30806C443DEF49B5093B007EC271E8
Apache_OpenOffice	130,259,616	4.1.2 de 32 bits	6741AC2CBF449D964E2422AA9BA8D3B4
Foca	5,458,456	3.4.3.0 de 32 bits	E9F7F9430619614E66920187FDCF1E5B

Tabla 17: Detalle de software.

CAPITULO 4. ANALISIS DE IMAGEN DE MEMORIA RAM.

4.1 Ficha técnica de archivos recibidos:

#	Nombre	Tamaño (bytes)	Descripción
1	ANN-PC-20151021-135652.raw.7z.001	681.574.400	Archivo 1 segmentado de memoria RAM
2	ANN-PC-20151021-135652.raw.7z.002	383.254.690	Archivo 2 segmentado de memoria RAM

Tabla 18: archivos segmentados de memoria RAM

Teniendo en cuenta que estos archivos han sido recibidos de manera segmentada es necesario realizar la integración de las partes.

Con el uso de la herramienta *7-zip* se llevo a cabo la unificación de los archivos correspondientes a la imagen de la memoria RAM, como se muestra en la siguiente imagen:

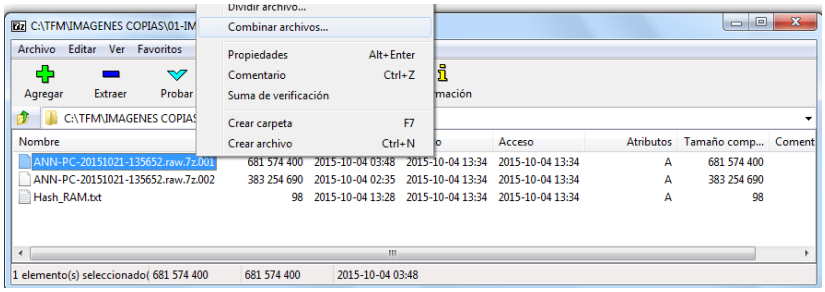


Imagen 17: unificación de archivos.

Se realiza el proceso de combinación de los dos (2) archivos:

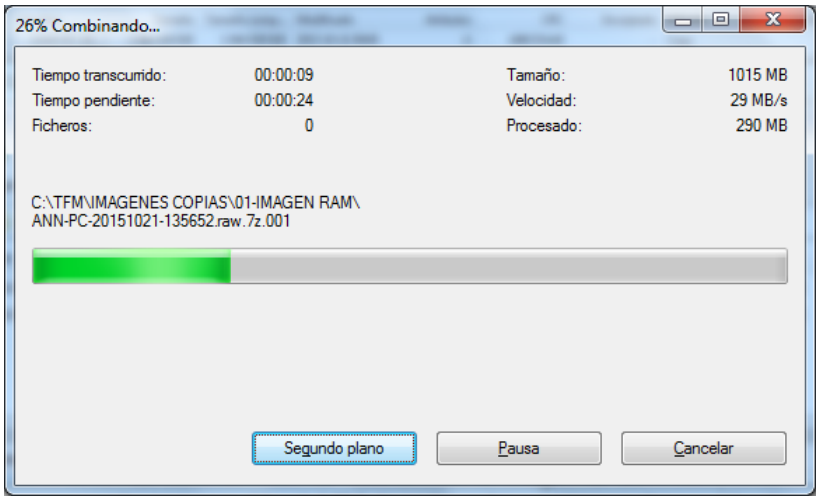


Imagen 18: transcurso de proceso.

Después de realizada la unión se extrajo un archivo resultante con el nombre *ANN-PC-20151021-135652.raw*

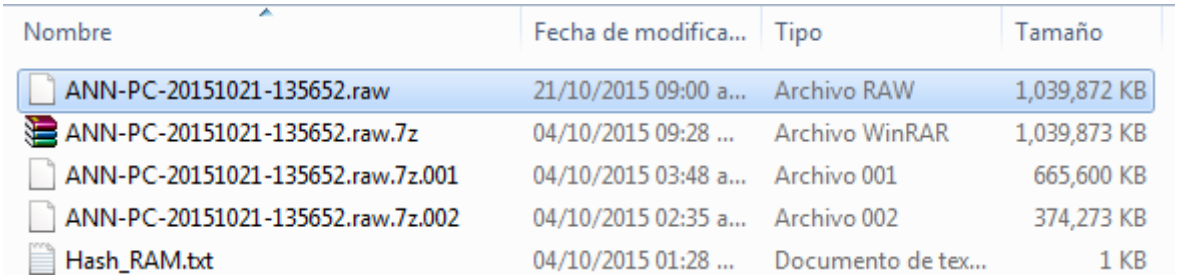


Imagen 19: archivo unificado.

4.2 Verificación de integridad

Con la herramienta *fciv.exe*
Se procedió a realizar la verificación del hash del archivo *ANN-PC-20151021-135652.raw,* resultante de la integración de las imágenes segmentadas.

Hash	Recibido	Calculado	Resultado
Md5	2B5AC23E63FC7FE3627D67C E53B41738	2B5AC23E63FC7FE3627D67C E53B41738	**Coincide**
Sha1	3B62577D24AA185D7F031E43 C6599BF25A401FC4	3B62577D24AA185D7F031E43 C6599BF25A401FC4	**Coincide**

Tabla 19: verificación hash de archivos de memoria RAM.

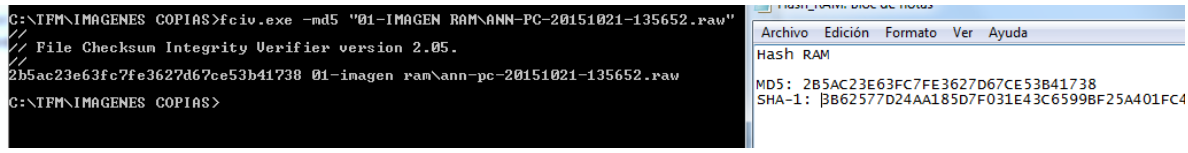


Imagen 20: verificación de integridad.

4.3 Pruebas Técnicas.

Para la realización de estas pruebas se utiliza la herramienta *Volatility Framework 2.4* incorporado dentro de la distribución *Kali Linux 2.0.*

> **Nota**: Todo archivo exportado del caso será analizado mediante el antimalware BAIDU 5.4.3.148966 con base de datos actualizado a la fecha del análisis. En este procedimiento del antimalware, por ser tan repetitivo, no se mostrarán imágenes, pero si se mostraran cuando se encuentre un archivo de tipo malicioso.

4.3.1 Identificación del sistema operativo:

A. Objetivo.

Identificar el sistema operativo base del archivo de memoria RAM para parametrizar las demás pruebas técnicas y así obtener información más precisa en el análisis.

B. Conceptos básicos.

Para el análisis de datos volátiles, mediante esta herramienta, es necesario suministrar como parámetro un *Perfil* de análisis correcto en la ejecución de cada *plugin* que se vaya a utilizar.

La herramienta *Volatility* ofrece los siguientes *plugins* para realizar una identificación del sistema operativo desde el que se extrajeron los datos volátiles.

C. Procedimiento.

Se cargó la imagen *ANN-PC-20151021-135652.raw* dentro de la maquina virtual creada anteriormente con la distribución *Kali Linux.*

A continuación:

- Se verifica la versión pre instalada de *Volatility Framework.*

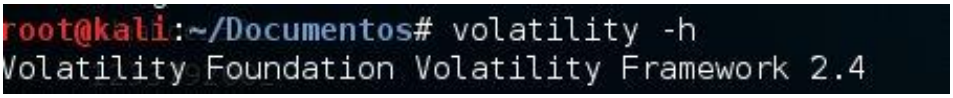


Imagen 21: revisión de versión.

- Se utiliza el plugin *imageinfo* para identificar el sistema operativo con el siguiente comando:

Volatility ident –f ANN-PC-20151021-135652.raw ***imageinfo****.*

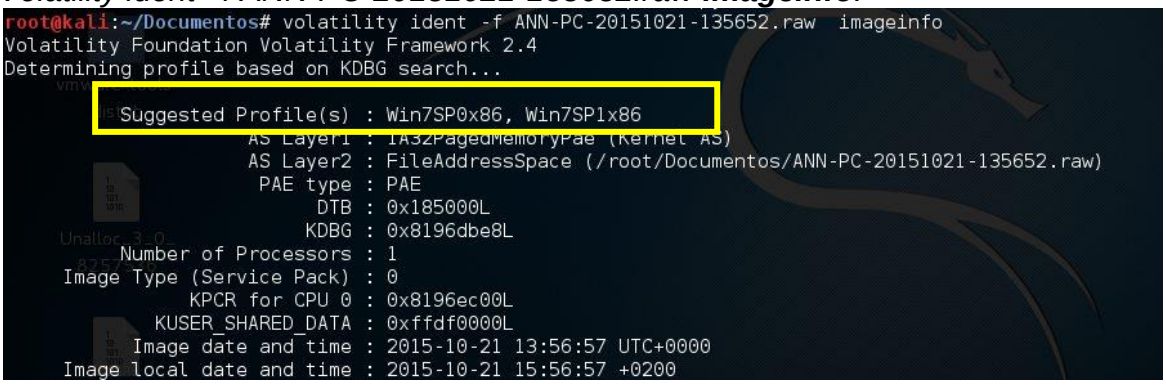


Imagen 22: sistema operativo detectado

El ítem *suggested Profile(s)* indica que los datos identificados dentro de la imagen presentan características propias de un sistema operativo Windows 7 de 32 bits sin service pack y con service pack 1, al mismo tiempo.

- Se ejecuta un segundo plugin, el *kdbgscan,* para tratar de identificar el sistema operativo con el service pack mas especifico:

Volatility –f ANN-PC-20151021-135652.raw ***kdbgscan****.*

```
root@kali:~/Documentos# volatility -f ANN-PC-20151021-135652.raw kdbgscan
Volatility Foundation Volatility Framework 2.4
**************************************************
Instantiating KDBG using: /root/Documentos/ANN-PC-20151021-135652.raw Win
Offset (P)                    : 0x196dbe8
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): Win7SP1x86
Version64                     : 0x196dbc0 (Major: 15, Minor: 7600)
PsActiveProcessHead           : 0x81985e98
PsLoadedModuleList            : 0x8198d810
KernelBase                    : 0x81845000

**************************************************
Instantiating KDBG using: /root/Documentos/ANN-PC-20151021-135652.raw Win
Offset (P)                    : 0x196dbe8
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): Win7SP0x86
Version64                     : 0x196dbc0 (Major: 15, Minor: 7600)
PsActiveProcessHead           : 0x81985e98
PsLoadedModuleList            : 0x8198d810
KernelBase                    : 0x81845000
```

Imagen 23: versión de sistema operativo confirmado.

El resultado muestra otra vez la existencia de dos service pack del mismo sistema operativo.

El plugin *kdbgscan* busca y analiza características de la estructura de datos del kernel dentro de la imagen, específicamente busca la firma presente dentro del bloque _KDDEBUGGER_DATA64, en este caso existen dos estructuras de este tipo. Esta duplicidad se puede dar cuando un sistema operativo ha sido actualizado en línea pero no ha sido reiniciado para tomar los nuevos cambios, la presencia de dobles estructuras de este tipo no impide el normal funcionamiento del sistema operativo.

Es recomendable utilizar, en este caso, el primer perfil que aparece después de la ejecución del plugin.
Se toma el perfil *Win7SP1x86* para la ejecución de las demás pruebas técnicas en este capítulo.

A partir de esta prueba se asignaran como variables globales (por defecto) el nombre del archivo de la imagen y el perfil obtenido, esta opción agiliza la ejecución de las pruebas evitando colocar en cada una el nombre del archivo y el perfil:

export VOLATILITY_LOCATION=file:///root/Documentos/ANN-PC-20151021-135652.raw

```
root@kali:~/Documentos# export VOLATILITY_LOCATION=file:///root/Documentos/ANN-PC-20151021-135652.raw
```

Imagen 24: globalización del archivo.

export VOLATILITY_PROFILE= Win7SP1x86

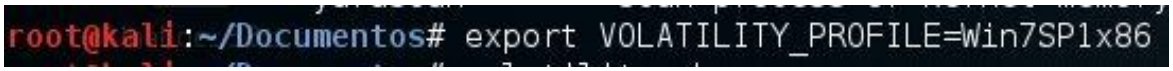


Imagen 25: globalización del perfil.

D. Resultado.

Se determinó que el sistema operativo base es **Windows 7 service pack 1 de 32 bits.**

E. Soportes.

Proceso de carácter auditable y repetible.

F. Herramientas adicionales de apoyo.

Ninguno.

4.3.2 Búsqueda de cuentas y password de usuarios

A. Objetivo.

Identificar las cuentas de usuario configuradas en el sistema operativo para diferenciar las actividades por medio de sus perfiles.

B. Conceptos básicos.

Cuando un usuario de Windows inicia sesión el sistema operativo carga en la memoria RAM un conjunto de configuraciones propias de su perfil, este conjunto es llamado *hive* del perfil de usuario, en cada *hive* se almacenan las claves, subclaves y valores que cada usuario requiere para su entorno de sesión, la memoria RAM posee información del *hive* referente a aplicaciones, escritorio, conexiones de red, entre otras.

El plugin *hivelist* incluido en *Volatility* será utilizado para buscar datos importantes del usuario o usuarios del sistema.

C. Procedimiento.

Se ejecutó el plugin *hivelist* por medio del siguiente comando:

~# Volatility hivelist

Se obtuvo la siguiente salida:

```
root@kali:~# volatility hivelist
Volatility Foundation Volatility Framework 2.4
Virtual    Physical   Name
---------- ---------- ----
0x86e44008 0x0337d008 \REGISTRY\MACHINE\HARDWARE
0x893ab008 0x3b3e6008 \SystemRoot\System32\Config\SOFTWARE
0x893c2008 0x3b5f0008 \Device\HarddiskVolume1\Boot\BCD
0x8cef3538 0x2c14e538 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0x8cf37008 0x3627c008 \SystemRoot\System32\Config\SAM
0x8cf542b0 0x35a622b0 \SystemRoot\System32\Config\SECURITY
0x8cf72650 0x35f3f650 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0x8df639d0 0x385309d0 \SystemRoot\System32\Config\DEFAULT
0x9323b950 0x2326c950 \??\C:\Users\Ann\ntuser.dat
0x93248008 0x19249008 \??\C:\Users\Ann\AppData\Local\Microsoft\Windows\UsrClass.dat
0x86e0c9d0 0x022059d0 [no name]
0x86e1a470 0x2a780470 \REGISTRY\MACHINE\SYSTEM
```

Imagen 26: resultado hivelist.

Se obtuvo el listado de archivos *hive* dentro de la 'memoria' RAM con las direcciones donde se encuentran almacenados los datos correspondientes a cada clave.

Utilizando el plugin *hashdump* se extraen los datos del *hive* para la investigación.

Se observa que la clave \SystemRoot\System32\Config\SAM está presente, esta clave señala la dirección donde esta almacenada la base de datos de contraseñas de las cuentas de usuarios.

Se ejecuta el comando: *~# Volatility hashdump –s 0x8cf37008*

```
root@kali:~# volatility hashdump -s 0x8cf37008
Volatility Foundation Volatility Framework 2.4
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Ann:1000:aad3b435b51404eeaad3b435b51404ee:8a24d5beb0d94c03ffec1e186a1f88b0:::
Tom:1001:aad3b435b51404eeaad3b435b51404ee:35509e7f0e2d9b0b7f60c40b37a1f559:::
root@kali:~#
```

Imagen 27: hashes encontrados.

Se obtiene 3 hash diferentes, estos hash han sido sometidos a un ataque de diccionario para la búsqueda del password. Como primera medida se utiliza una herramienta web para el ataque *crackstation.net*:

Imagen 28: password recuperados.

D. Resultado.

Se encontraron cuatro cuentas de usuario:

- Administrador
- Invitado
- Ann
- Tom

De acuerdo al modelo de gestión de cuentas y password del sistema operativo Windows 7 a través del Administrador de Cuentas de Seguridad (SAM), se clasifican los siguientes datos:

Nombre de Cuenta	ID	Hash NTLM	Password
Administrador	500	31d6cfe0d16ae931b73c59d7e0c089c0	(vacio)
Invitado	501	31d6cfe0d16ae931b73c59d7e0c089c0	(vacio)
Ann	1000	8a24d5beb0d94c03ffec1e186a1f88b0	Tom1980
Tom	1001	35509e7f0e2d9b0b7f60c40b37a1f559	Ann1978

T

abla 20: Hash de contraseñas de cuentas de usuarios.

E. Soportes.

NOMBRE	DESCRIPCION	HASH MD5	TAMAÑO bytes	Clasificación de evidencia
hashdump.txt	Salida de información dentro del espacio asignado al SAM de Windows.	281A2A91E3004B9A2CD9D14D7D1B50BC	325	A10
hivelist.txt	Salida de búsqueda de información hive.	75434DDA4F68A52656EB1A9BCE99049A	757	A01

Tabla 21: Clasificación de archivos resultantes de cuentas de usuarios.

F. Herramientas adicionales de apoyo.

Herramienta online: https://crackstation.net

4.3.3 Búsqueda de procesos ejecutados en el sistema

A. Objetivo.

Conocer el tipo de procesos que ejecutados para direccionar la investigación y búsqueda de datos sobre artefactos más específicos.

B. Conceptos básicos.

Windows maneja los procesos por medio de estructuras conocidas como EPROCESS, estas estructuras conforman una lista doblemente enlazada que relaciona "todos" los procesos, *Volatility Framework* permite buscar los procesos ejecutados del sistema por medio del escaneo de estas estructuras y la consulta de la información que en ellas se almacena.

Algunos procesos maliciosos pueden ocultarse dentro del sistema, este ocultamiento lo realizan des-enlazándose de la lista de "todos" los procesos.

Se realiza la búsqueda de procesos visibles y procesos ocultos.

C. Procedimiento

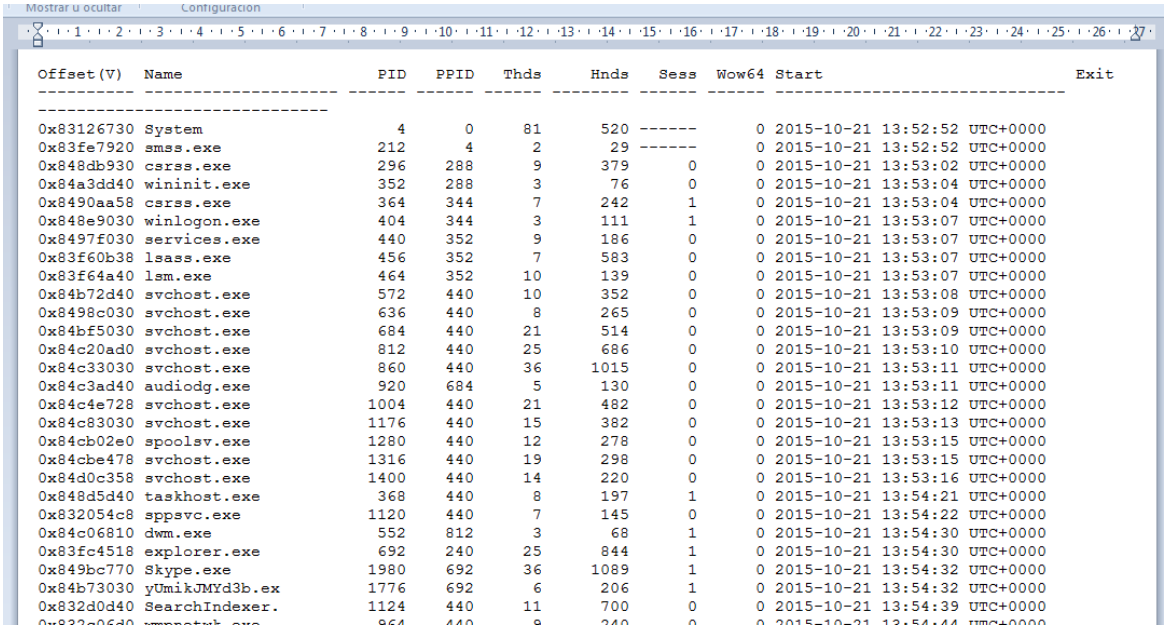
Se hace un listado de procesos visibles y procesos no visibles en búsqueda de elementos sospechosos en ejecución.

Se ejecuta el plugin *pslist,* este plugin realiza una búsqueda en la lista doblemente enlazada de procesos:

~# Volatility pslist > pslist.txt:

Imagen 29: generación de archivo de procesos.

Los procesos encontrados por el plugin han sido direccionados a un archivo de nombre pslist.txt. En total se encontraron 42 procesos.



```
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
```

Imagen 30: listado de procesos visibles.

Se ejecuta el plugin *psscan,* este plugin realiza una búsqueda de TODAS las estructuras _EPROCESS, por lo tanto permite observar aquellos procesos ocultos:

~# Volatility psscan > psscan.txt:

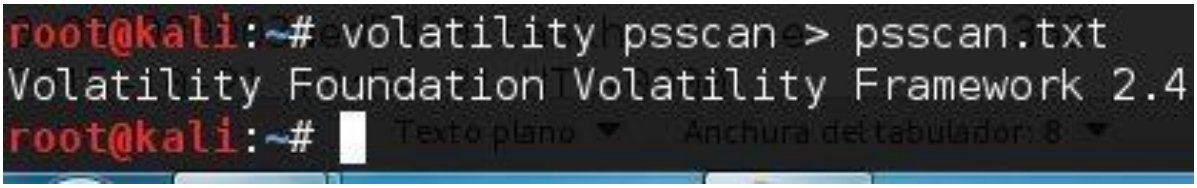
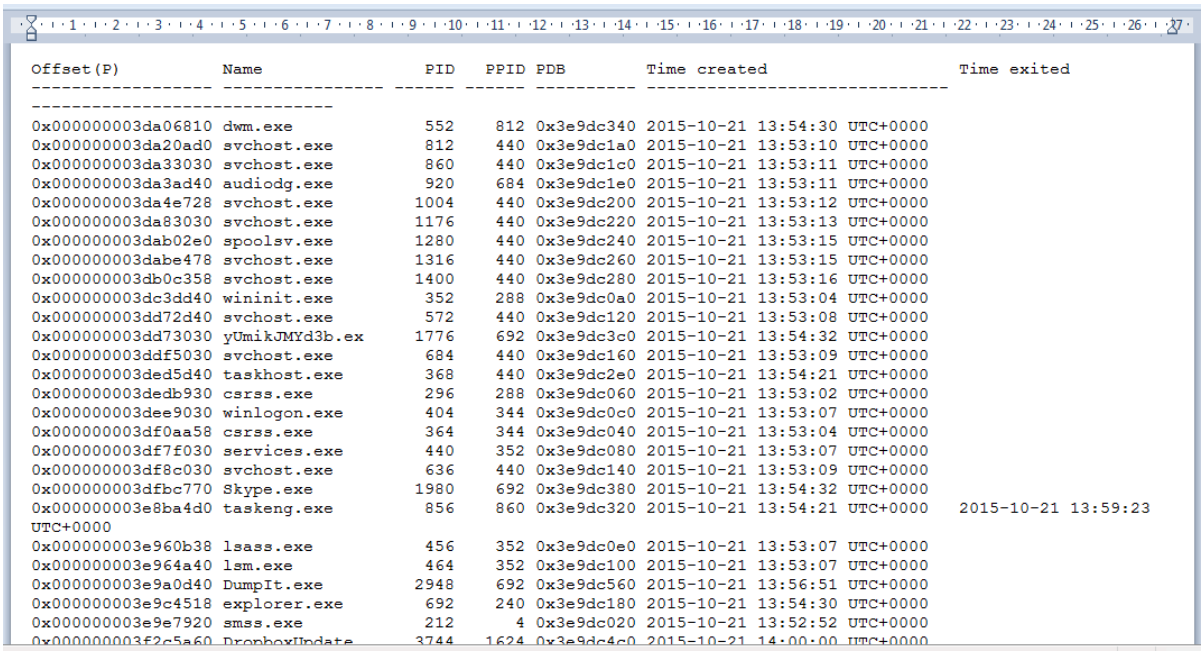


Imagen 31: generación de procesos visibles y ocultos.

Los procesos encontrados por el plugin han sido direccionados a un archivo de nombre psscan.txt. En total se encontraron 44 procesos.



```
Offset(P)          Name                PID   PPID PDB        Time created                   Time exited
------------------ ---------------- ------ ------ ---------- ------------------------------
------------------------------
0x000000003da06810 dwm.exe             552    812 0x3e9dc340 2015-10-21 13:54:30 UTC+0000
0x000000003da20ad0 svchost.exe         812    440 0x3e9dc1a0 2015-10-21 13:53:10 UTC+0000
0x000000003da33030 svchost.exe         860    440 0x3e9dc1c0 2015-10-21 13:53:11 UTC+0000
0x000000003da3ad40 audiodg.exe         920    684 0x3e9dc1e0 2015-10-21 13:53:11 UTC+0000
0x000000003da4e728 svchost.exe        1004    440 0x3e9dc200 2015-10-21 13:53:12 UTC+0000
0x000000003da83030 svchost.exe        1176    440 0x3e9dc220 2015-10-21 13:53:13 UTC+0000
0x000000003dab02e0 spoolsv.exe        1280    440 0x3e9dc240 2015-10-21 13:53:15 UTC+0000
0x000000003dabe478 svchost.exe        1316    440 0x3e9dc260 2015-10-21 13:53:15 UTC+0000
0x000000003db0c358 svchost.exe        1400    440 0x3e9dc280 2015-10-21 13:53:16 UTC+0000
0x000000003dc3dd40 wininit.exe         352    288 0x3e9dc0a0 2015-10-21 13:53:04 UTC+0000
0x000000003dd72d40 svchost.exe         572    440 0x3e9dc120 2015-10-21 13:53:08 UTC+0000
0x000000003dd73030 yUmikJMYd3b.ex     1776    692 0x3e9dc3c0 2015-10-21 13:54:32 UTC+0000
0x000000003ddf5030 svchost.exe         684    440 0x3e9dc160 2015-10-21 13:53:09 UTC+0000
0x000000003ded5d40 taskhost.exe        368    440 0x3e9dc2e0 2015-10-21 13:54:21 UTC+0000
0x000000003dedb930 csrss.exe           296    288 0x3e9dc060 2015-10-21 13:53:02 UTC+0000
0x000000003dee9030 winlogon.exe        404    344 0x3e9dc0c0 2015-10-21 13:53:07 UTC+0000
0x000000003df0aa58 csrss.exe           364    344 0x3e9dc040 2015-10-21 13:53:04 UTC+0000
0x000000003df7f030 services.exe        440    352 0x3e9dc080 2015-10-21 13:53:07 UTC+0000
0x000000003df8c030 svchost.exe         636    440 0x3e9dc140 2015-10-21 13:53:09 UTC+0000
0x000000003dfbc770 Skype.exe          1980    692 0x3e9dc380 2015-10-21 13:54:32 UTC+0000
0x000000003e8ba4d0 taskeng.exe         856    860 0x3e9dc320 2015-10-21 13:54:21 UTC+0000   2015-10-21 13:59:23
UTC+0000
0x000000003e960b38 lsass.exe           456    352 0x3e9dc0e0 2015-10-21 13:53:07 UTC+0000
0x000000003e964a40 lsm.exe             464    352 0x3e9dc100 2015-10-21 13:53:07 UTC+0000
0x000000003e9a0d40 DumpIt.exe         2948    692 0x3e9dc560 2015-10-21 13:56:51 UTC+0000
0x000000003e9c4518 explorer.exe        692    240 0x3e9dc180 2015-10-21 13:54:30 UTC+0000
0x000000003e9e7920 smss.exe            212      4 0x3e9dc020 2015-10-21 13:52:52 UTC+0000
0x000000003f2c5a60 DropboxUpdate      3744   1624 0x3e9dc4c0 2015-10-21 14:00:00 UTC+0000
```

Imagen 32: listado de procesos visibles y ocultos.

D. Resultado.

Se encontraron dos procesos ocultos:

- taskeng.exe
- WMIADAP.exe

Ambos procesos son conocidos de Windows, se decide no profundizar en los datos de su ejecución.

Se encontró evidencia de la ejecución de una herramienta de cifrado simétrico llamado *TrueCrypt* con el proceso TrueCrypt.exe de PID 2244. Este software es utilizado para el cifrado y descifrado de volúmenes de datos.

Nombre	PID	PPID	PDB	Time	creado	Time
WMIADAP.exe	1112	860	0x3e9dc520	21/10/2015	13:57:17	UTC+0000
TrueCrypt.exe	2244	692	0x3e9dc480	21/10/2015	13:55:00	UTC+0000
taskeng.exe	2688	860	0x3e9dc580	21/10/2015	14:00:00	UTC+0000

Tabla 22: programas seleccionados para analizar.

Se decide realizar las pruebas técnicas para la búsqueda de la clave de cifrado simétrica que se usa en el equipo investigado.

E. Soportes.

Nombre	Descripción	Hash md5	Tamaño bytes	Clasificación De evidencia
pslist.txt	Salida de búsqueda de procesos visibles	F2012B97F1C697379A 5CF210A1844BF5	6072	A10
psscan.txt	Salida de búsqueda de procesos visibles y ocultos	215CBDFB6E43F5163 13FA3FAAD0FF522	5658	A10

Tabla 23: detalle de salida de consulta de procesos.

F. Herramientas adicionales de apoyo.
Ninguna.

4.3.4 Claves de cifrado TrueCrypt.

A. Objetivo.
Encontrar claves de cifrado utilizadas por la herramienta TrueCrypt para descifrar datos hallados dentro de las evidencias obtenidas.

B. Conceptos básicos.
La herramienta de cifrado TrueCrypt es un software que permite montar y desmontar volúmenes de datos cifrados, tiene la capacidad de realizar el cifrado y descifrado de tipo “on the fly”, permitiéndole al usuario acceder a sus datos cifrados cuantas veces quiera después de haber montado el volumen y haber digitado una sola vez la clave, esta agilidad de uso es posible porque la clave proporcionada por el usuario se almacena en un espacio de la memoria RAM reservado para que el software procese los datos cuando se requiera.

El TrueCrypt cuenta con dos procesos, una interfaz que se ejecuta a nivel de usuario y un driver que se ejecuta en modo kernel, este driver es el proceso encargado de realizar el cifrado y descifrado de datos, por lo tanto es en el espacio de memoria asignado a este driver donde se encuentra alojada la clave.

C. Procedimiento.
Se ejecuta el plugin *truecryptsummary* para obtener un resumen de la información general de la herramienta TrueCrypt que se encuentre dentro de la imagen:
~# Volatility truecryptsummary:

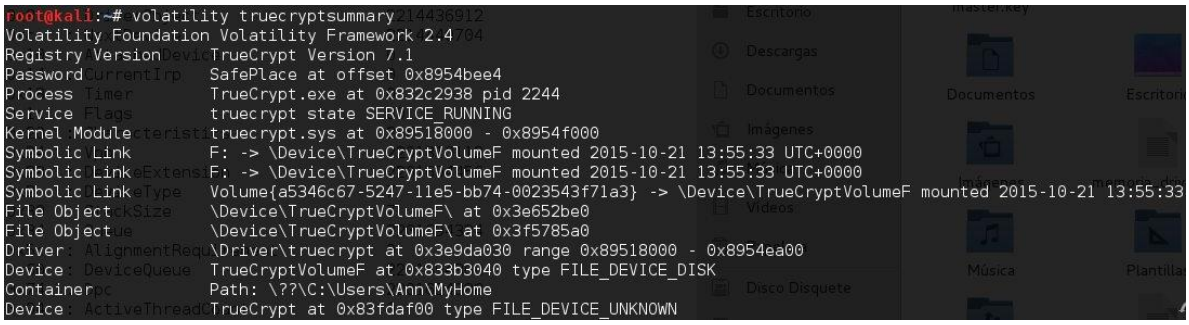


Imagen 33: contenido del espacio en TrueCrypt.

Se ejecuta el plugin *truecryptpassphrase* para buscar una o varias claves dentro del espacio de memoria:

~# Volatility truecryptpassphrase:

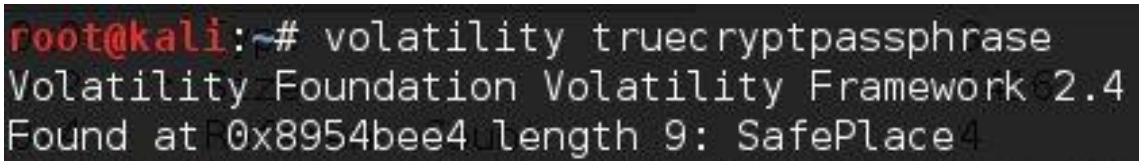


Imagen 34: password TrueCrypt encontrada.

Se ejecuta el plugin *truecryptmaster* para buscar la clave maestra utilizada por TrueCrypt:

~# Volatility truecryptmaster –D.:

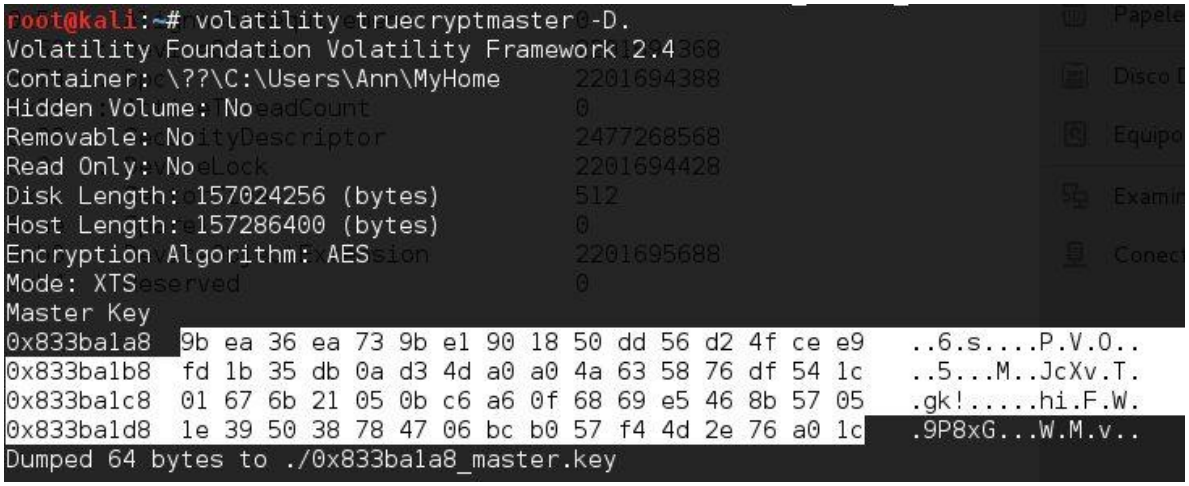


Imagen 35: llave maestra TrueCrypt.

Este plugin generó un archivo llamado 0x833ba1a8_master.key como la llave maestra hallada.

D. Resultado.

Se encontró la siguiente información relacionada con el software TrueCrypt:

- Versión: 7.1
- Volumen cifrado 1: TrueCryptVolumeF, conocido.
- Volumen cifrado 2: TrueCrypt, desconocido.
- Password: SafePlace
- Clave maestra: 0x833ba1a8_master.key
- Contenedor cifrado: C:\Users\Ann\MyHome

- Longitud del volumen: 157024256 bytes.
- Algoritmo de cifrado: AES.

E. Soportes.

Nombre	Descripción	Hash md5	Tamaño bytes	Clasificación de evidencia
summary.txt	Salida del comando resumen de TrueCrypt	A54B3A3EA9AD0896 050EB5286D722F7B	978	A10
passphrase.txt	Salida de password de TrueCrypt	940EE489B8DA1E77 AD899CA49A260298	40	A10
master.txt	Salida de búsqueda máster key de TrueCrypt	686C30C6ECB3CC6 EF8E8B82377CFA6E 1	550	A10
0x833ba1a8_maste r.key	Máster Key de TrueCrypt	0B955A82BB2D7D60 EE7BC43550764533	64	A10

Tabla 24: archivos de soporte claves TrueCrypt.

F. Herramientas adicionales de apoyo.

Ninguna.

CAPITULO 5. ANALISIS DE IMAGEN DE DISCO DURO.

5.1 Ficha técnica de archivos recibidos.

Información de los archivos recibidos como imagen del disco duro, la imagen de este dispositivo está fragmentada en 8 archivos, como se registran a continuación:

#	Nombre	Tamaño (bytes)	Descripción
1.	Ann_HD.E01	670.797.686	Imagen fragmentada
2.	Ann_HD.E02	670.801.344	Imagen Fragmentada
3.	Ann_HD.E03	670.811.003	Imagen Fragmentada
4.	Ann_HD.E04	670.801.094	Imagen Fragmentada
5.	Ann_HD.E05	670.533.457	Imagen Fragmentada
6.	Ann_HD.E06	670.806.818	Imagen Fragmentada
7.	Ann_HD.E07	670.932.936	Imagen Fragmentada
8.	Ann_HD.E08	141.145.618	Imagen Fragmentada
9.	Ann_HD.E08	141.145.618	Imagen fragmentada
10.	Ann_HD.log	892	Log del procedimiento de adquisición
11.	hash.txt	416	Hash md5 de cada archivo de imagen fragmentada

Tabla 25: detalle de archivos de disco recibidos

5.2 Verificación de integridad

Se procede a calcular el hash md5 de cada archivo que compone la imagen del disco:

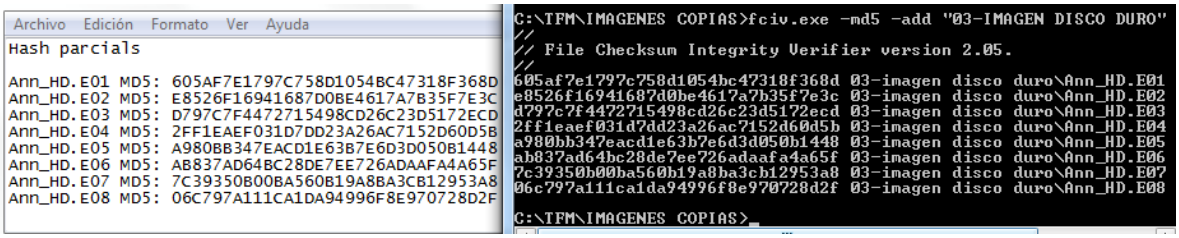


Imagen 36: verificación de integridad de disco.

Se registra el resultado de cálculo realizado:

Nombre	Hash Recibido	Hash Calculado	Resultado
Ann_HD.E01	605AF7E1797C758D1054BC47318F368D	605AF7E1797C758D1054BC47318F368D	Coincide
Ann_HD.E02	E8526F16941687D0BE4617A7B35F7E3C	E8526F16941687D0BE4617A7B35F7E3C	Coincide
Ann_HD.E03	D797C7F4472715498CD26C23D5172ECD	D797C7F4472715498CD26C23D5172ECD	Coincide
Ann_HD.E04	2FF1EAEF031D7DD23A26AC7152D60D5B	2FF1EAEF031D7DD23A26AC7152D60D5B	Coincide
Ann_HD.E05	A980BB347EACD1E63B7E6D3D050B1448	A980BB347EACD1E63B7E6D3D050B1448	Coincide
Ann_HD.E06	AB837AD64BC28DE7EE726ADAAFA	AB837AD64BC28DE7EE726ADAAF	Coincide

	4A65F	A4A65F	
Ann_HD.E07	7C39350B00BA560B19A8BA3CB12953A8	7C39350B00BA560B19A8BA3CB12953A8	Coincide
Ann_HD.E08	06C797A111CA1DA94996F8E97072828D2F	06C797A111CA1DA94996F8E97072828D2F	Coincide
Ann_HD.E08	06C797A111CA1DA94996F8E97072828D2F	06C797A111CA1DA94996F8E97072828D2F	Coincide

Tabla 26: comparación de hash recibido y hash calculado.

Se observa que el resumen hash calculado para cada archivo coincide con el hash contenido dentro del archivo hash.txt.

5.3 Pruebas técnicas.

Para la realización de las pruebas sobre la imagen de disco se ha decidido utilizar dos herramientas de análisis:

- *Autopsy 3.1.3 con Sleuth Kit versión 4.1.3*
- OSForensics 3.2 build 1003

El objetivo es complementar algunos resultados ofrecidos por una y otra herramienta, así como algunas funcionalidades en las cuales se diferencian.

5.3.1 Procedimiento de inicio.

CREACION DEL CASO EN AUTOPSY:

- Se crea un caso en el Autopsy utilizando la imagen del disco.
- Nombre del caso: TFM_DISCO1
- Numero: 002.
- Examinador: Fredy Omar Morantes
- Timezone: (GMT -5:00) América Bogotá.

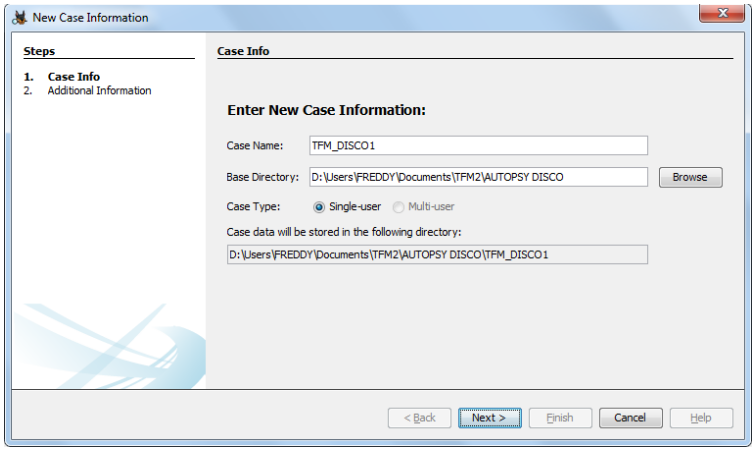


Imagen 37: creación de caso en Autopsy.

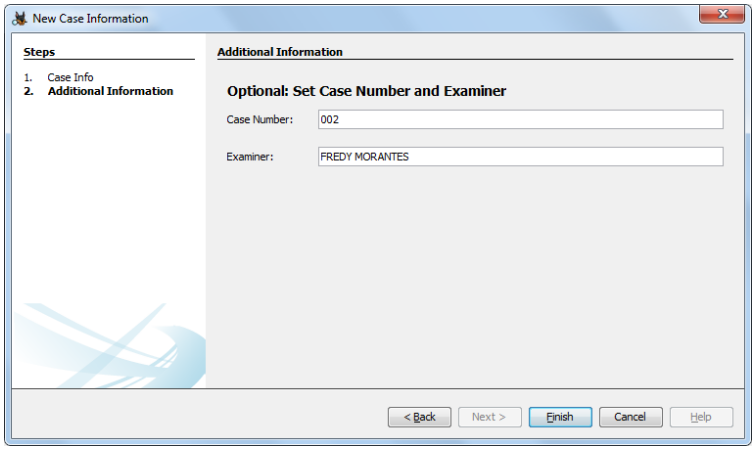


Imagen 38: asignación de número al caso.

Después de creado el caso se procede a cargar la fuente de datos, en este caso la imagen del disco Ann_HD.E01:

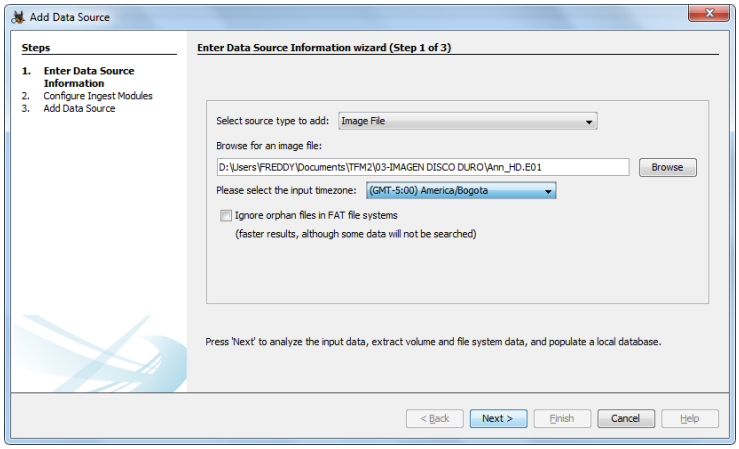


Imagen 39: asignación de zona horaria.

Cargada la imagen se procede a ejecutar los módulos de recolección incluidos en el Autopsy para analizar los datos, la siguiente imagen muestra la ejecución de *Run Ingest Modules:*

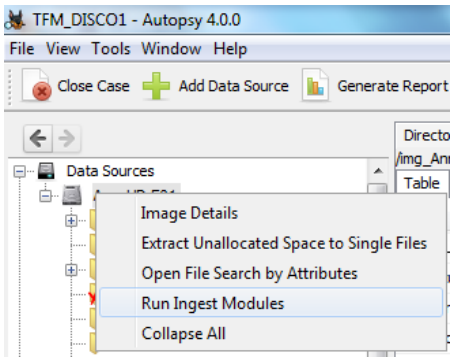


Imagen 40: módulos.

Se han seleccionado los siguientes módulos:

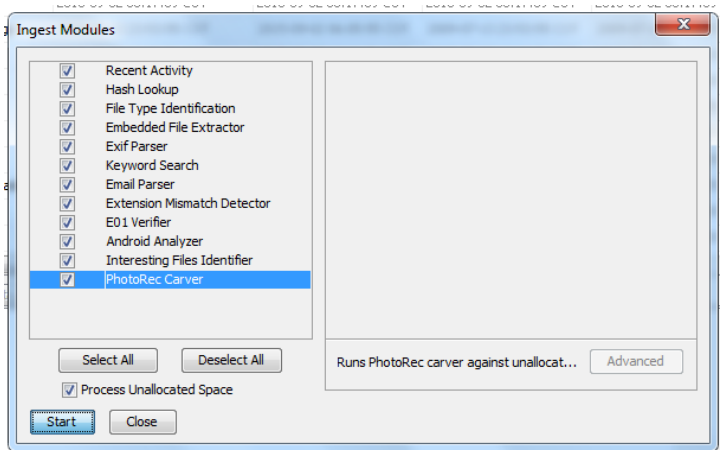


Imagen 41: selección de módulos.

Después de realizado la carga y ejecución de los módulos se procede a verificar los datos recopilados por el Autopsy dentro del árbol de resultados:

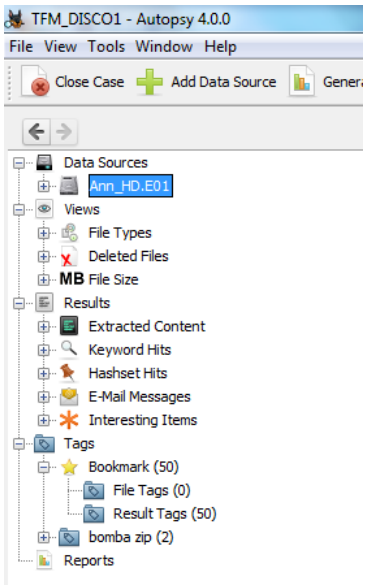


Imagen 42: árbol de resultados

CREACION DEL CASO EN OSFORENSIC:

- Nombre del caso: TFM DISCO
- Numero de caso: 001.
- investigador: FREDY MORANTES
- Organización: UOC.TFM
- Time Zone: Local (GMT -5:00).

A continuación se muestran los parámetros de la creación del caso:

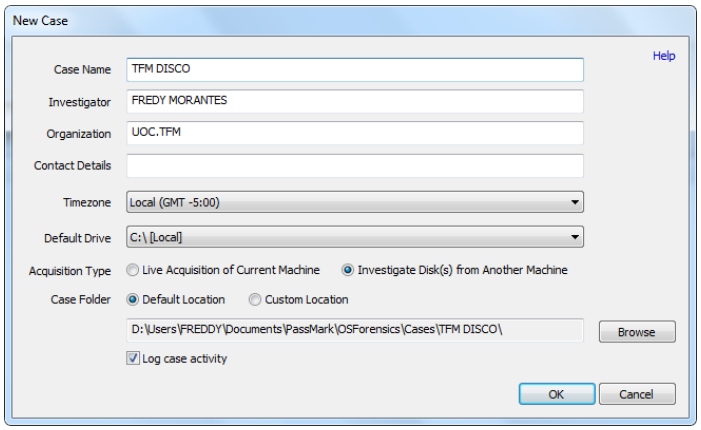


Imagen 43: creación de caso OSForensics.

Paso seguido se carga la imagen del disco como un dispositivo del caso creado:

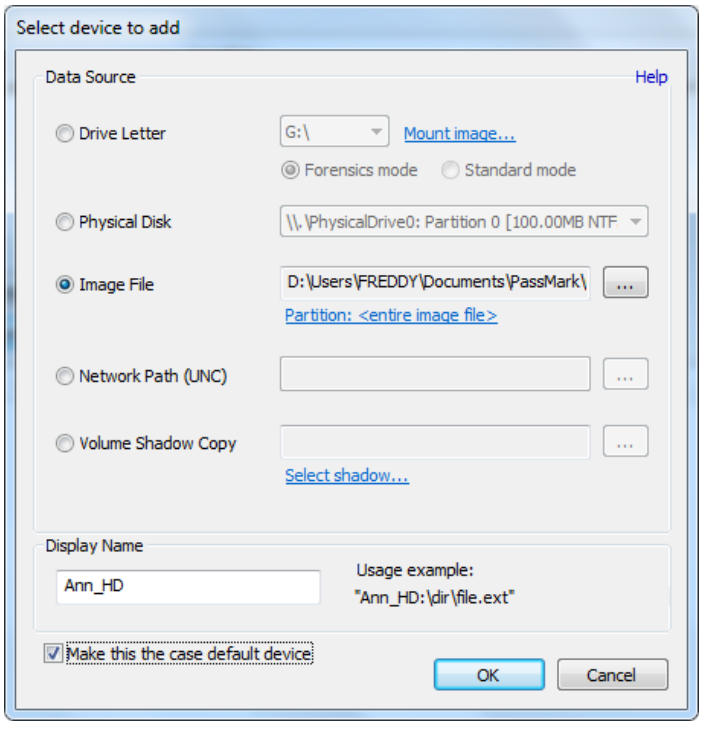


Imagen 44: carga de imagen.

Después de cargado la imagen, la herramienta nos ofrece todos los módulos de análisis:

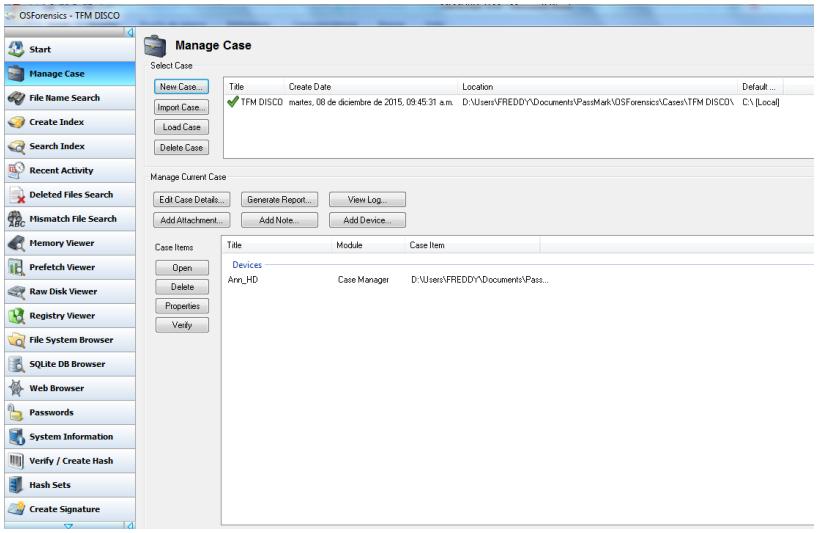


Imagen 45: módulos de OSForensics.

Los módulos que se observan en la barra vertical izquierda serán utilizados a lo largo del análisis.

5.3.2 Estudio del sistema operativo.

- Sistema Operativo:

En el caso de Autopsy se observa que:
El sistema operativo instalado es **Windows 7 Professional** instalado en la ruta **C:\Windows, equipo de nombre ANN-PC.**
Esta información se obtiene de los siguientes elementos:

En el árbol de resultados, dentro del nodo *Extracted Content,* se encuentra un sub-nodo llamado *Operating System Information* en el que se ha agrupado la información del sistema encontrada por los módulos de recolección:

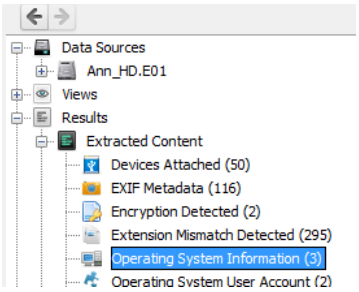


Imagen 46: nodo de información.

Después de seleccionado el sub-nodo *Operating System Information* se observa la información del sistema operativo.

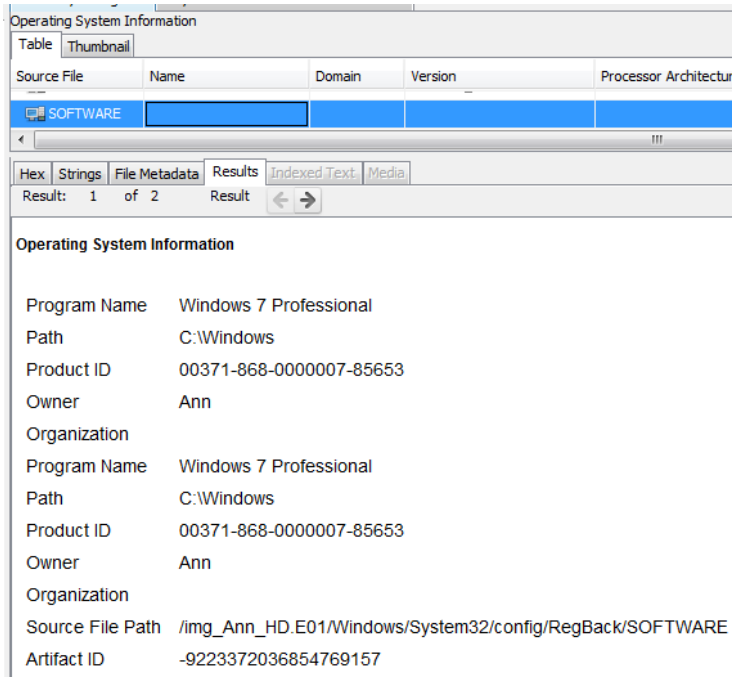


Imagen 47: información del sistema.

- Identificación de usuarios:

Para la identificación de datos de creación y acceso de usuarios del sistema se utilizo el caso creado anteriormente en la herramienta OSFORENSICS.

El procedimiento se realiza ingresando en la opción *System Information.*

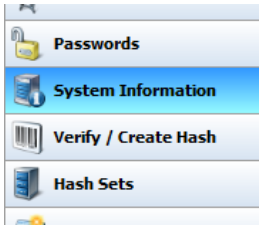


Imagen 48: modulo de información.

Se selecciona y ejecuta la opción *System Information From Registry*

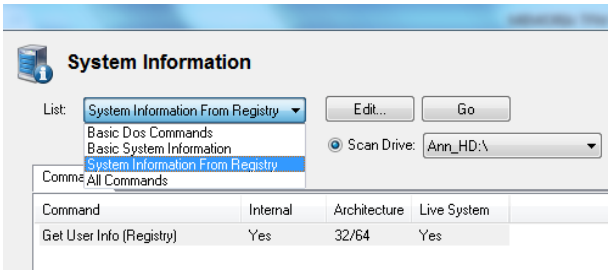


Imagen 49: grupo de comandos.

Después de ejecutado el comando anterior, se obtuvo un resultado en el que se observa el registro de 4 usuarios en el sistema: Administrador, Invitado, Ann y Tom.

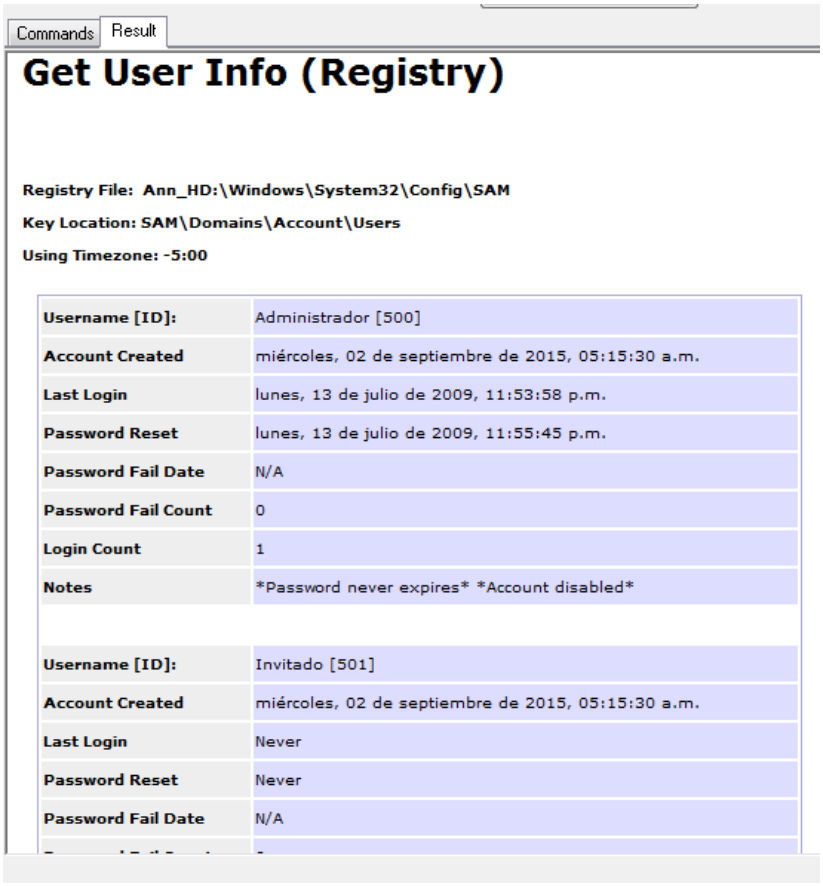


Imagen 50: información de usuarios del sistema.

Ordenando los resultados se obtienen los siguientes datos:

Usuario	creado (GMT -5:00)				ultimo login (GMT -5:00)				cantidad de login
	Año	Mes	Día	Hora	Año	Mes	Día	Hora	
Administrador [500]	2015	9	2	05:15:30 Am	2009	7	13	11:53:58 p.m.	1
Invitado [501]	2015	9	2	05:15:30 a.m.	n/a	n/a	n/a	n/a	0
Ann [1000]	2015	9	2	05:17:37 a.m.	2015	10	21	08:54:18 a.m.	26
Tom [1001]	2015	9	2	05:20:02 a.m.	2015	10	21	04:03:02 a.m.	8

Tabla 27: resumen histórico de usuarios.

- Fecha de último apagado del sistema:

Windows 7 almacena el registro de eventos del sistema en la siguiente ruta %windir%/Windows/System32/winevt/Logs/System.evtx, en el árbol de resultados se ha realizado la navegación hasta el archivo system.evtx a través de la siguiente ruta:

- */img_Ann_HD.E01/Windows/System32/winevt/Logs/System.evtx*

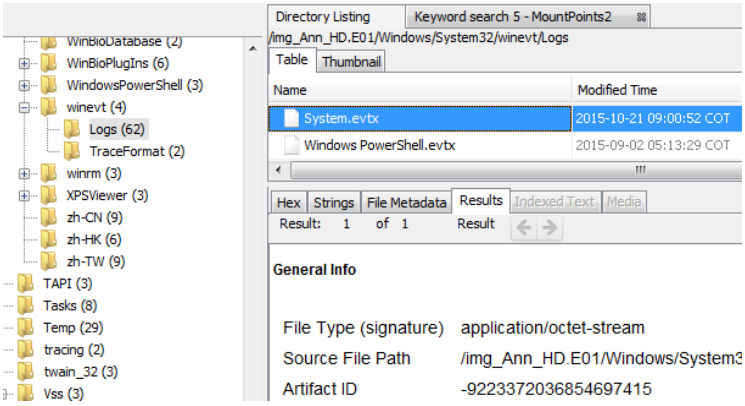


Imagen 51: log de eventos detectado.

Se ha exportado el archivo *system.evtx* para ser analizado con el visor de eventos de Windows.

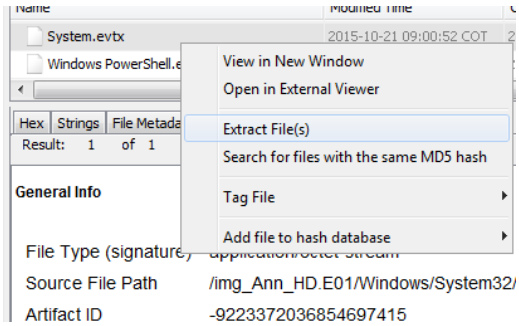


Imagen 52: Extracción del log de eventos.

Se ha buscado el último evento que corresponda al apagado en Windows 7.

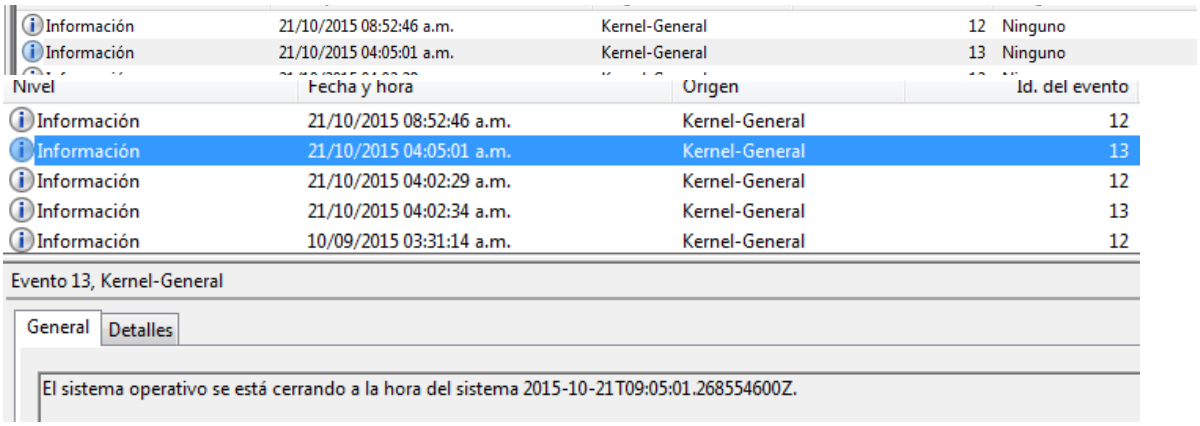


Imagen 53: registro de ultimo apagado del sistema.

Se determina que el ultimo apagado fue el 21 de Octubre de 2015 a las 04:05:01 am (GMT -05:00).

5.3.3 Recuperación de archivos borrados.

Autopsy agrupó 4145 archivos clasificados como recuperados por técnica de análisis de la estructura de sistema de archivos, no data carving.

Los archivos han sido exportados de la imagen para su exploración.

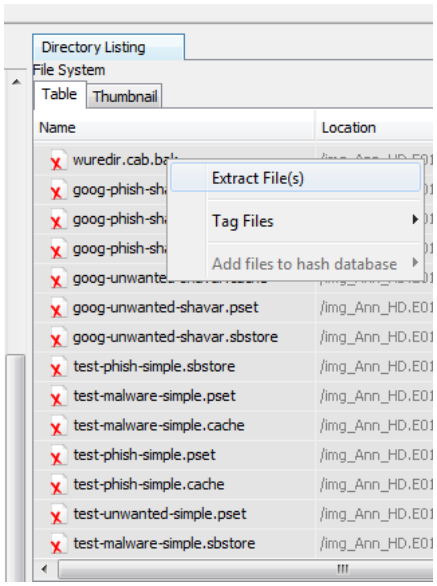


Imagen 54: archivos borrados.

Los archivos se descartan por ser irrelevantes, debido a que son archivos propios del sistema operativo.

Clasificación de evidencia: A00.

5.3.4 Dispositivos USB conectados.

Por medio del repositorio de datos (Hive) /img_Ann_HD.E01/Windows/System32/config/SYSTEM se ha recuperado información del historial de dispositivos USB conectados al equipo investigado, como se muestra a continuación:

En el árbol de resultados se halla el nodo *Extracted Content,* con el sub-nodo *Device Attached,* esta agrupación contiene 50 registros que pertenecen al historial de conexiones encontrados en el archivo SYSTEM.

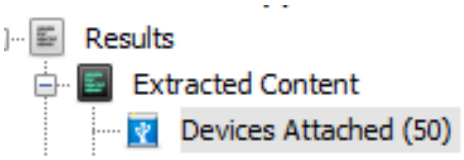


Imagen 55: nodo de dispositivos conectados.

Ingresando al sub-nodo se encuentra el detalle de cada registro anteriormente señalado, correspondiente a 5 dispositivos diferentes que han sido conectados en varias ocasiones.

SYSTEM	2015-09-02 05:14:12 COT	LaCie, Ltd	Product: 0643	10000E001108C93B	Ann_HD.E01
SYSTEM	2015-09-04 05:09:01 COT	Pixart Imaging, Inc.	Product: 2700	5&5045dfb&0&8	Ann_HD.E01
SYSTEM	2015-09-04 05:09:01 COT	Pixart Imaging, Inc.	Product: 2700	6&28ea3f42&0&0000	Ann_HD.E01
SYSTEM	2015-09-04 05:20:02 COT	JMTek, LLC.	Transcend Flash disk	5&1457f427&0&2	Ann_HD.E01
SYSTEM	2015-09-04 05:09:01 COT	SiGma Micro	Product: 0034	5&4bb4d45&0&2	Ann_HD.E01

Imagen 56: registros de dispositivos conectados.

El resumen de los dispositivos conectados en su última fecha se observan a continuación

Marca	Modelo	Id	Ultima conexión
JMTek, LLC.	Transcend Flash disk	5&1457f427&0&2	2015-09-07 11:05:47 COT
LaCie, Ltd	Product: 0643	10000E001108C93B	2015-09-02 05:14:12 COT
Pixart Imaging, Inc.	Product: 2700	5&5045dfb&0&8	2015-10-21 08:53:00 COT
SiGma Micro	Product: 0034	5&1457f427&0&2	2015-10-21 08:53:00 COT
Unknown	Product: 1234	5&5045dfb&0&3	2015-10-21 08:56:31 COT

Tabla 28: Detalle de dispositivos USB conectados.

Clasificación de evidencia: A10.

5.3.5 Análisis de papelera de reciclaje.

Por medio del árbol de resultados se accedió a la carpeta $Recycle.bin:

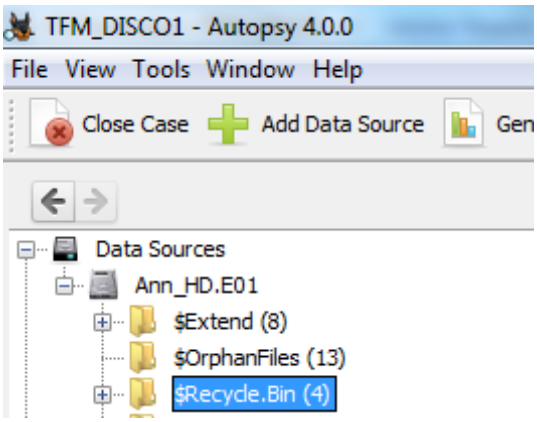


Imagen 57: nodo de papelera.

Encontrando los siguientes resultados:

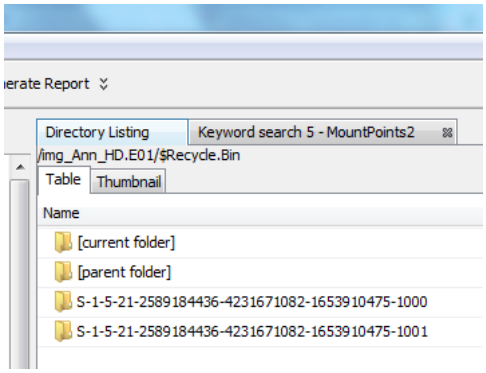


Imagen 58: contenido de papelera

Se hallaron 2 carpetas, la primera con el nombre S-1-5-21-2589184436-4231671082-1653910475-**1000,** otra con el nombre S-1-5-21-2589184436-4231671082-1653910475-**1001.**

Dentro de la carpeta $recycle.bin se crean subcarpetas de archivos borrados por cada usuario, con un SID como nombre de estas subcarpetas, siendo los últimos cuatro dígitos del SID el identificador del usuario del sistema que eliminó el archivo.

Por los 4 últimos dígitos (1000) del código de la primera carpeta se determina que pertenece al usuario de sistema Ann, conociendo que su ID de usuario es 1000, la segunda carpeta pertenece al usuario Tom.

Dentro de la carpeta del usuario Ann se han encontrado los siguientes archivos:

- $IQC0MZN.ods
- $RQC0MZN.ods

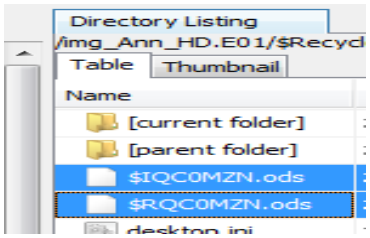


Imagen 59: archivos en papelera.

Se procede a exportar ambos archivos para su visualización.

El archivo de nombre $IQC0MZN.ods contiene los datos observados en la siguiente imagen:

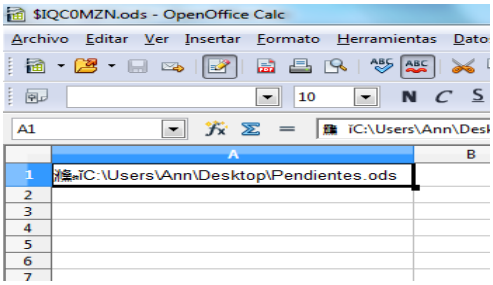
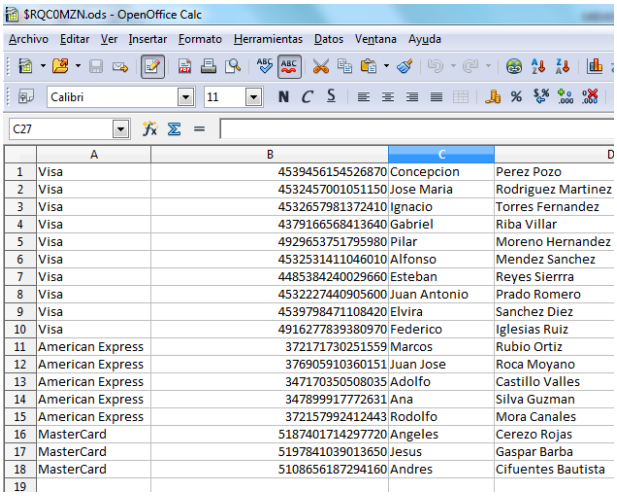


Imagen 60: contenido archivo $IQC0MZN

En la celda A1 se observa la ruta de un archivo llamado Pendientes.ods. Este hallazgo confirma que este archivo correspondía a la cuenta del usuario Ann del sistema operativo.

El archivo de nombre $RQC0MZN.ods contiene la misma estructura y datos que el archivo Pendientes.ods hallado en *3.3.3 Clasificación de archivos de carácter delictivo,* una vez más se encuentra información de lo que parece ser datos de tarjetas de crédito relacionados con su tipo y aparente titular, adicional a su contenido se encuentra la relación con el usuario *Ann.*



	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
19				

Imagen 61: contenido archivo $RQC0MZN

De acuerdo a la forma en que Windows estructura los archivos dentro de la papelera se sabe que el archivo $IQC0MZN.ods es un “descriptor” del archivo $RQC0MZN.ods, este ultimo llamado Pendientes.ods antes de ser eliminado.

Con base en esta información se deduce que el usuario Ann eliminó este archivo que anteriormente se almacenaba en el escritorio del sistema.

Clasificación de evidencia: A10.

5.3.6 Análisis de archivos huérfanos.

En el grupo de archivos creado por Autopsy, se observa la carpeta con nombre $OrphanFiles con 13 archivos.

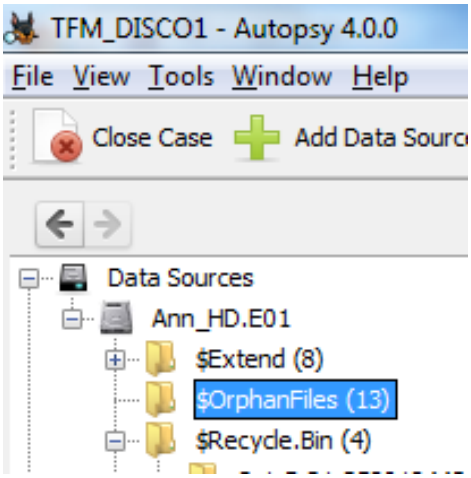


Imagen 62: Nodo de archivos huérfanos.

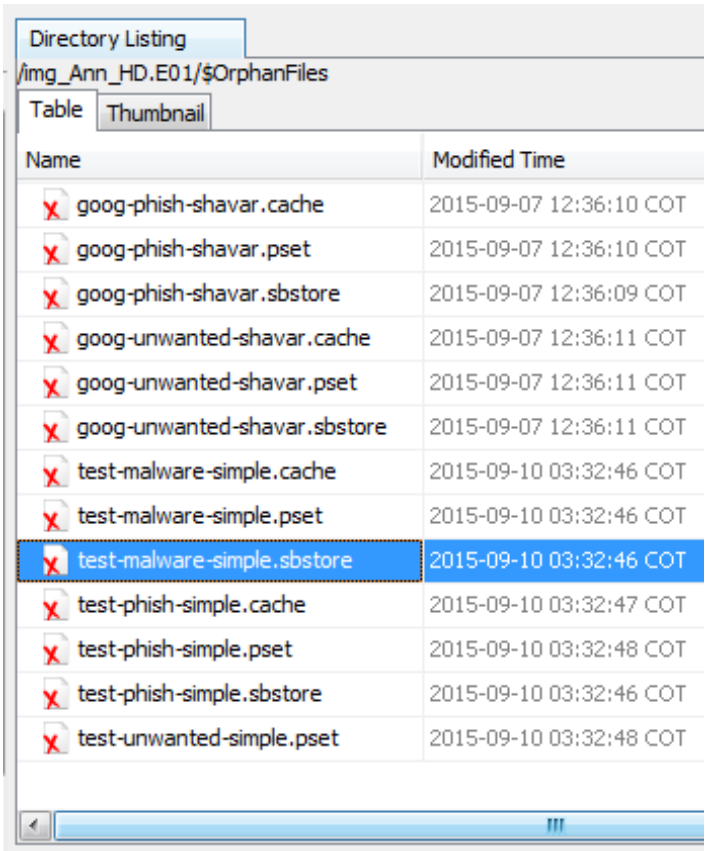


Imagen 63: archivos de recolección.

Este tipo de archivos es utilizado por empresas como Google para recolectar información de sitios potencialmente maliciosos.

Clasificación de evidencia: B00.

5.3.7 Archivos recuperados con técnica *Data Carving.*

Se obtuvieron 3647 archivos con la técnica de data carving realizada por el modulo de Autopsy.

El análisis de estos archivos arrojo un resultado que permite catalogar esta evidencia como irrelevante, la mayoría de estos archivos son archivos propios del sistema.

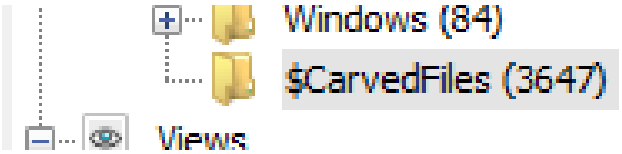


Imagen 64: nodo de archivos recuperados por técnica carving

Resumen de archivos *carved.*

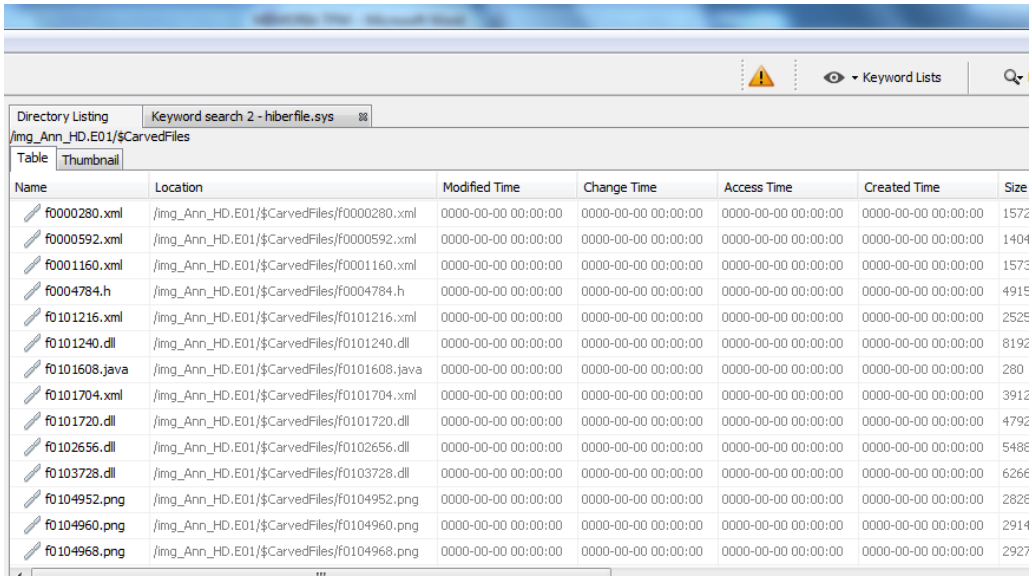


Imagen 65: listado de archivos *carved*

Por medio de la herramienta seleccionada se verifica la existencia de archivos borrados que pueden ser recuperados.

La verificación de estos archivos conduce a determinar que son archivos propios del sistema operativo.

Clasificación de evidencia: B00.

5.3.8 Análisis de metadatos.

En el árbol de resultados se accede a la carpeta llamada *EXIF Metadata,* en esta carpeta se observan 116 imágenes con estructura de metadatos exif.

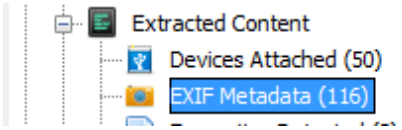
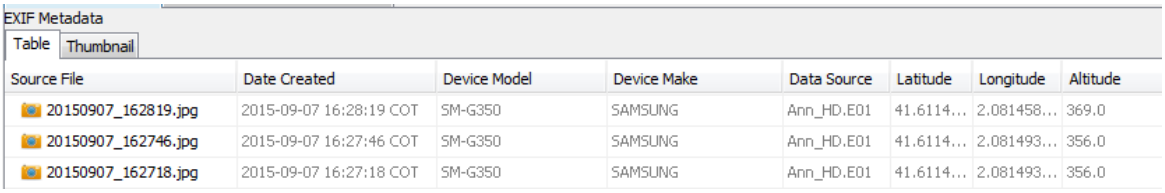


Imagen 66: nodo de metadatos.

Los archivos se extraen para su exploración.

Dentro del directorio EXIF se detectan imágenes con datos de posicionamiento geográfico.



Source File	Date Created	Device Model	Device Make	Data Source	Latitude	Longitude	Altitude
20150907_162819.jpg	2015-09-07 16:28:19 COT	SM-G350	SAMSUNG	Ann_HD.E01	41.6114...	2.081458...	369.0
20150907_162746.jpg	2015-09-07 16:27:46 COT	SM-G350	SAMSUNG	Ann_HD.E01	41.6114...	2.081493...	356.0
20150907_162718.jpg	2015-09-07 16:27:18 COT	SM-G350	SAMSUNG	Ann_HD.E01	41.6114...	2.081493...	356.0

Imagen 67: imágenes con metadatos relevantes.

Imagen 67a: imágenes con coordenadas.

Se procede a verificar la ubicación de las coordenadas a través del sitio web http://www.verexif.com/ que permite corroborar la existencia de metadatos en imágenes y mostrar el lugar donde se tomó mediante las coordenadas GPS halladas.

Las coordenadas obtenidas dentro de las imágenes son:

Latitud: N 41° 36’ 41.4”

Longitud: E 2° 4’ 53.4”

Altitud: 356 m

Longitud GPS :	E 2° 4' 53.4"
Altitud GPS :	356.00m
Comentarios :	User comments

LUGAR DONDE SE HIZO LA FOTO

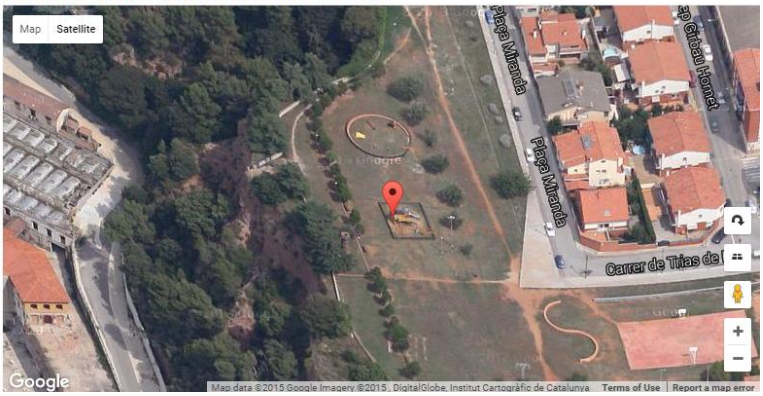


Imagen 67b: imagen de ubicación aérea.

Con acercamiento y visualización horizontal se comprueba que el sitio es el mismo de las fotos.

Imagen 67c: Imagen de ubicación horizontal.

El lugar corresponde a la Plaza Miranda de **castellar del vallés,** municipio español de la provincia de Barcelona, Cataluña España.

Estas imágenes se clasifican como evidencia potencial debido a que las coordenadas de este sitio pueden ser correlacionadas con otra evidencia.

Nombre	Descripción	Hash md5	Tamaño bytes	Clasificación de evidencia
12034-20150907_162718.jpg	Imagen con metadatos de posición geográfica	68EC0B8CEF946E6403D7D222768163FD	1058873	A10
12036-20150907_162746.jpg	Imagen con metadatos de posición geográfica	994823F3803436B04E0552F36179347A	915872	A10
12038-20150907_162819.jpg	Imagen con metadatos de posición geográfica	25152D446AA96024F187BC54D81EFA6E	1916793	A10

Tabla 29: imágenes con metadatos relevantes.

5.3.9 Análisis de software instalado.

Mediante el navegador de archivos de Autopsy se verifican el software instalado en búsqueda de alguna herramienta de carácter sospechosa o delictiva.

El directorio muestra 28 programas instalados.

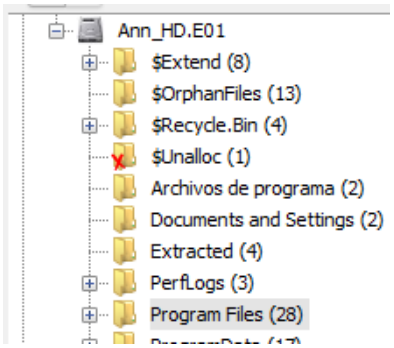


Imagen 68: nodo de software instalado.

Se encuentra el siguiente listado de aplicaciones:

Programa	Fecha de modificación
Dropbox	2015-09-02 09:00:08 COT
DVD Maker	2009-07-14 04:05:18 COT
EaseUS	2015-09-02 09:13:58 COT
Internet Explorer	2009-07-14 03:52:49 COT
Mozilla Firefox	2015-09-02 05:30:14 COT
Mozilla Maintenance Service	2015-09-02 05:30:12 COT
MSBuild	2009-07-13 23:52:30 COT
OpenOffice 4	2015-09-02 05:50:03 COT
Reference Assemblies	2009-07-13 23:52:30 COT
S-tools	**2015-09-02 08:52:31 COT**
Skype	**2015-09-02 05:55:55 COT**
TrueCrypt	**2015-09-03 09:37:05 COT**
Uninstall Information	2009-07-13 23:53:23 COT

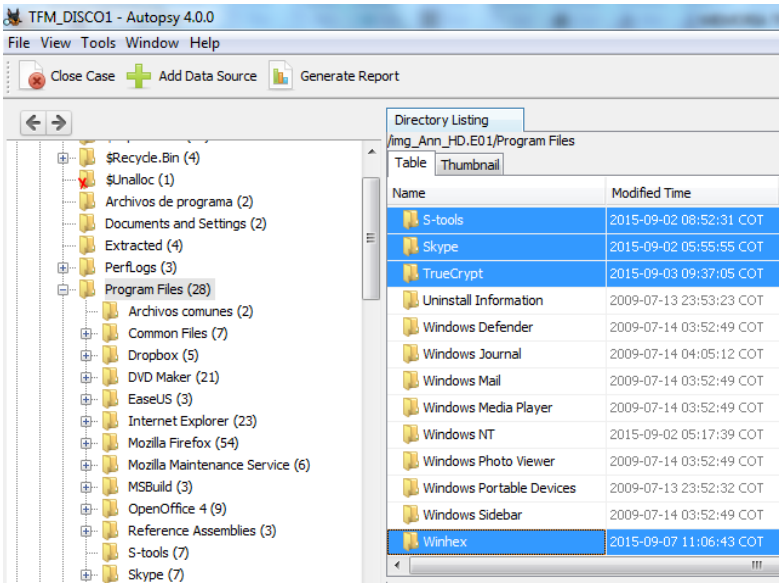
Windows Defender	2009-07-14 03:52:49 COT
Windows Journal	2009-07-14 04:05:12 COT
Windows Mail	2009-07-14 03:52:49 COT
Windows Media Player	2009-07-14 03:52:49 COT
Windows NT	2015-09-02 05:17:39 COT
Windows Photo Viewer	2009-07-14 03:52:49 COT
Windows Portable Devices	2009-07-13 23:52:32 COT
Windows Sidebar	2009-07-14 03:52:49 COT
Winhex	**2015-09-07 11:06:43 COT**
WinRAR	2015-09-07 05:39:48 COT

Tabla 30: lista de programas instalados en el sistema.

Se observa la instalación de algunos programas que podrían ofrecer datos relevantes para la investigación como:

- S-Tools
- Skype.
- TrueCrypt.
- Winhex.

Se observan los directorios de instalación de cada programa:



En el directorio de S-Tools, TrueCrypt y Winhex se encuentran archivos propios de su configuración, dentro de estos no se ha encontrado un directorio de salida de archivos procesados con cada herramienta, en el caso de estos tres programas se debe buscar por otros métodos archivos con rastros de procesamiento mediante S-Tools, TrueCrypt y Winhex. La búsqueda se realizará en la etapa de exploración sobre los archivos obtenidos en otras pruebas.

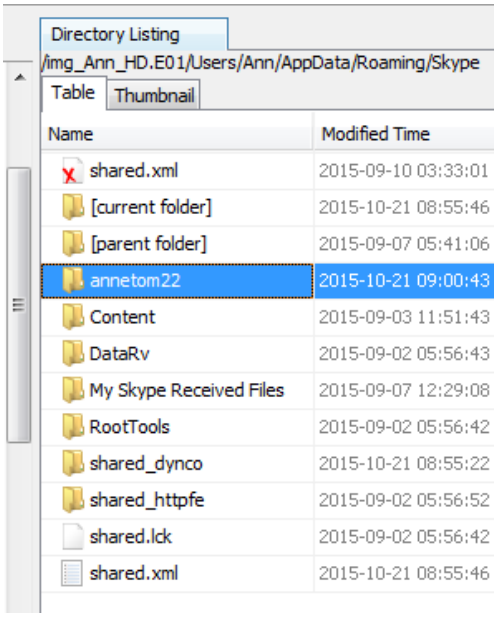
En el caso del programa Skype, dentro de su directorio se ha encontrado artefactos propios de su uso y un registro de mensajes enviados y recibidos a través del mismo.

5.3.10 Búsqueda de historial en Skype.

Los artefactos de la aplicación Skype en Windows 7 se hallan en la ruta C:\Users\<username>\AppData\Roaming\Skype\<skype-name> para el caso del usuario Ann se encuentran en la siguiente ruta:

*/img_Ann_HD.E01/Users/Ann/AppData/Roaming/Skype/**Ann.***

Se procede a verificar la anterior ruta.



Se observa que el usuario de Skype de Ann es “annetom22”.

Se procede a exportar el directorio SKYPE del usuario Ann para la exploración posterior.

Clasificación de evidencia: A10.

5.3.11 Archivos cifrados de TrueCrypt.

En el análisis de la imagen de memoria RAM se obtuvo el nombre, ruta, tamaño y password de un volumen cifrado con la herramienta TrueCrypt.

Se procede a buscar en la ruta *C:\users\Ann* un archivo de nombre *MyHome*.

El archivo es hallado en la ruta encontrada en el análisis de datos volátiles.

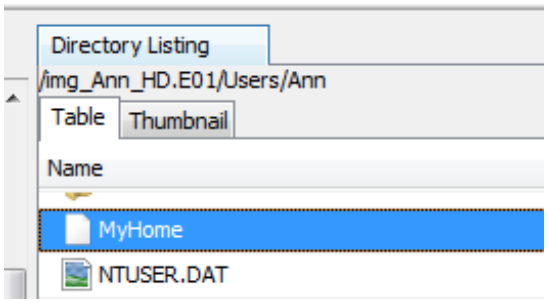


Imagen 69: detección de archivo cifrado.

El archivo es exportado y clasificado como evidencia potencial. La exploración de este archivo será correlacionada con información hallada en el análisis de la imagen de memoria RAM utilizando el password obtenido en ese análisis.

El procedimiento en el que se intentará descifrar este volumen se lleva a cabo en el Capítulo 6 *Exploración y Correlación de evidencia.*

Nombre	Descripción	Hash md5	Tamaño bytes	Clasificación de evidencia
MyHome	Volumen cifrado mediante TrueCrypt	F45DEA81E1A23BB693 D36EBE7EEAFDAC	157286400	A10

Tabla 31: detalle y clasificación de archivo cifrado.

5.3.12 Búsqueda de archivos descargados.

Por medio del explorador de archivos de Autopsy se verifico el directorio de descargas del usuario Ann.

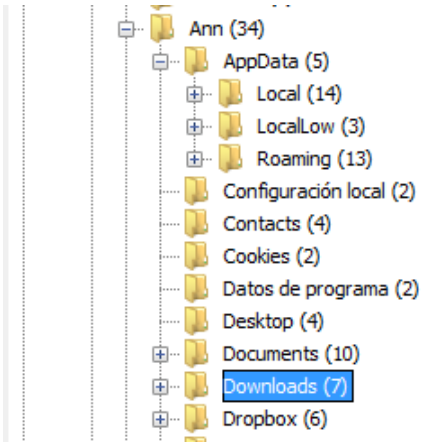


Imagen 70: nodo de archivos descargados.

Se hallaron 2 archivos comprimidos, estos archivos se han exportado de la imagen para su análisis.

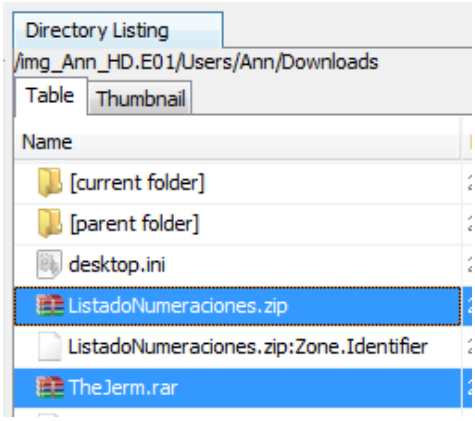


Imagen 71: archivos descargados.

Después de exportados, el archivo *TheJerm.rar* ha sido clasificado como un troyano por el antivirus, el tipo de malware reconocido por el antimalware BAYDU es el siguiente:

Trojan.MSIL.Ijector.LVE

Imagen 72: detección de posible troyano.

El otro archivo encontrado en el directorio Descargas llamado ListadoNumeraciones.zip es un archivo cuyo contenido está cifrado. Debido a que no se logró acceder a su contenido, ya que solicita una contraseña para su apertura, este archivo se marca como evidencia potencial para su exploración posterior.

Se procede a verificar el directorio de descargas del usuario Tom.

El directorio de descargas del usuario Tom está vacío.

Tabla de selección de evidencias:

Nombre	Descripción	Hash md5	Tamaño bytes	Clasificación de evidencia
11905-ListadoNumeraciones.zip	Archivo cifrado exportado del directorio descargas de usuario Ann.	28B6C7E90762A2174A32F9E7A2077F9A	62151	A10
11907-TheJerm.rar	Malware exportado del directorio descargas de usuario Ann.	D01C1211D42FB78B7937FBDEFCA5E573	812659	A10

Tabla 32: detalle y clasificación de archivos en el directorio Descargas.

5.3.13 Búsqueda en espacios no asignados.

Se ha encontrado un archivo sin extensión en el directorio *$Unalloc* del navegador de archivos de Autopsy.

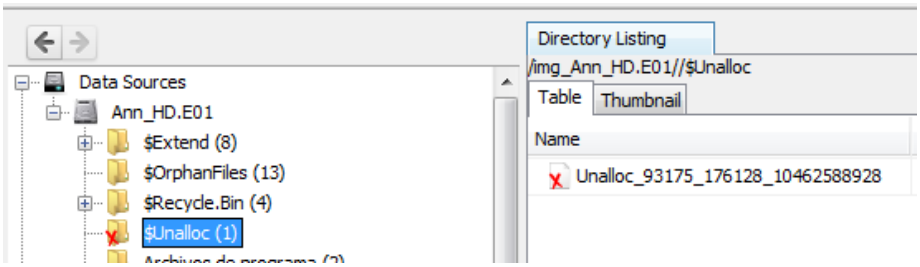


Imagen 73: nodo de archivos en espacio no asignado.

El archivo se exporta para ser sometido a una prueba de data carving con la herramienta *Foremost.*

Nombre	Descripción	Hash md5	Tamaño bytes	Clasificación de evidencia
Unalloc_93175_176128_10462588928	Archivo del espacio no asignado exportado del directorio $unalloc	F2E4A04E36FC4F6104A7C04706F858E5	1191473152	A10

Tabla 33: detalle de archivo recuperado del espacio no asignado.

5.3.14 Búsqueda de malware.

Por medio de la herramienta *OSForensics* se procede a realizar un montaje de la imagen para ser analizada como un volumen más del equipo forense.

Se selecciona la opción **Mount Drive Image**

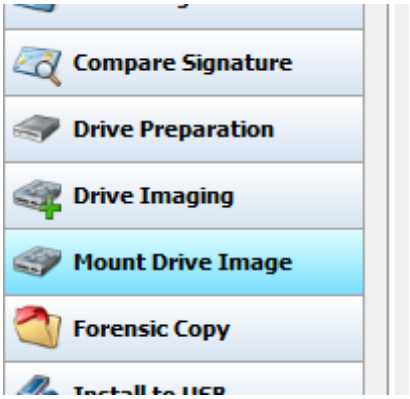


Imagen 74: modulo mount drive image.

A continuación se selecciona la opción **Mount new…**

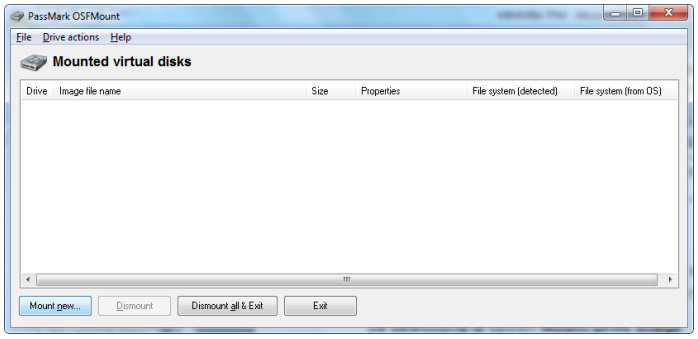


Imagen 75: inicio de proceso de montaje.

Se ingresan los parámetros necesarios para el montaje, seleccionando la opción de solo lectura para cuidar la integridad de la imagen:

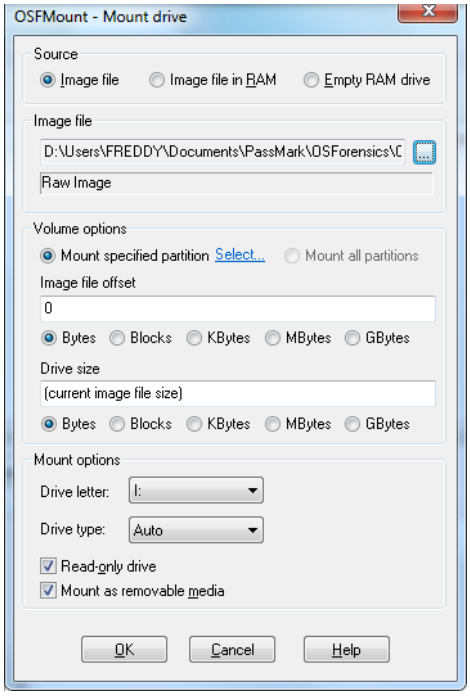


Imagen 76: parámetros del montaje.

La imagen ha sido montada como una unidad extraíble dentro del equipo forense asignándose la unidad I:

Se procede a realizar un análisis directo sobre la unidad montada con el antimalware BAYDU 2015

Imagen 77: detección de malware en la unidad montada.

En una búsqueda más profunda se ha encontrado el siguiente malware adicional dentro del directorio del árbol de navegación de Autopsy llamado *Extracted*:

- excel_server.exe: tercer malware encontrado.

Se obtienen los siguientes archivos clasificados como malware:

Nombre	Descripción	Hash md5	Tamaño bytes	Clasificación de evidencia
yUmikJMYd3b.exe	Archivo potencialmente malicioso	88db5e8a850bb9e863e8b118e730a201	639488	A10
TheJerm.rar	Archivo potencialmente malicioso	d01c1211d42fb78b7937fbdefca5e573	812659	A10
excel_server.exe	Archivo potencialmente malicioso	c223f994f4d3f10e6f4ca5289c140dec	13824	A10

Tabla 34: detalle y clasificación de malware encontrado.

5.3.15 Búsqueda de palabra clave “Password”

En este punto del análisis se han detectado varios archivos cuya suficiencia como evidencia depende de una contraseña para poder ser explorada en su totalidad.

Por medio de la herramienta OSFORENSICS se emite una búsqueda a través del índice de la palabra Password (el motor de búsqueda de OSForensics es una de las diferencias con Autopsy).

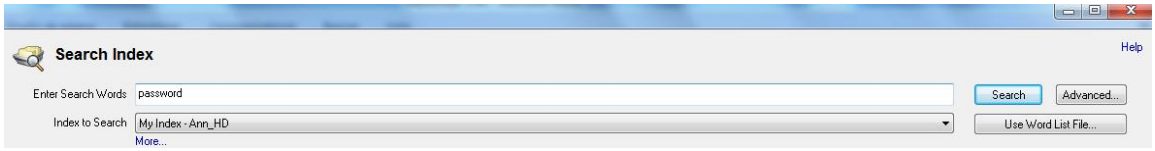


Imagen 78. Modulo de búsqueda de OSForensics.

Se obtuvo un total de 1393 coincidencias con el parámetro de búsqueda.

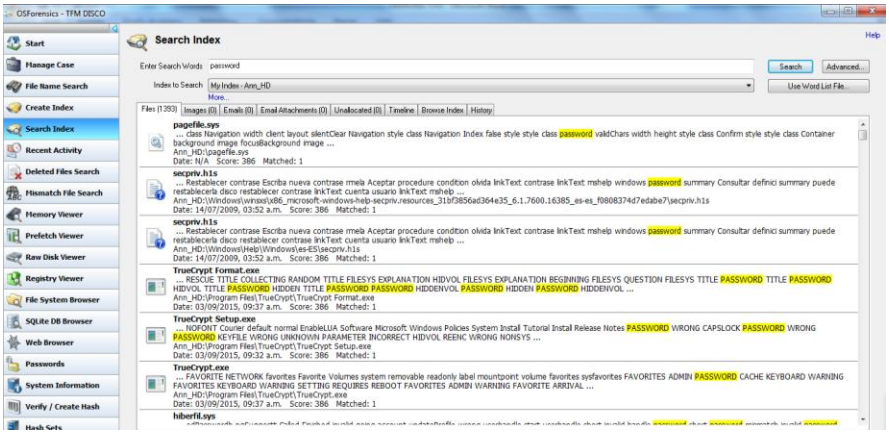


Imagen 79: resultados de búsqueda.

Después de una búsqueda exhaustiva con gran cantidad de falsos positivos, se detecto un archivo con contenido relevante.

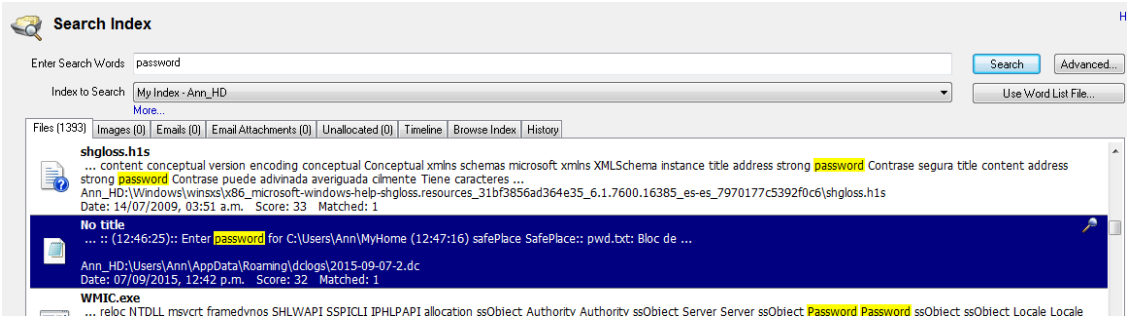


Imagen 80: archivo relevante detectado.

El archivo ha sido detectado en la ruta Ann_HD:\Users\appData\Roaming\dclogs\2015-09-07.dc

Se procede a exportar el archivo para su inspección.

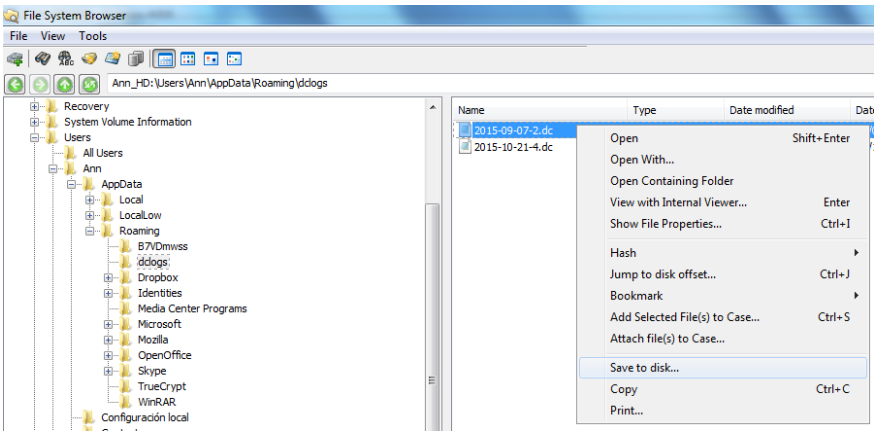


Imagen 81: archivo de password.

Dentro del archivo exportado se encuentran algunos posibles password para diferentes programas y archivos, entre ellos se encuentra en password “SafePlace”, el cual había sido detectado anteriormente como la llave de TrueCrypt en el análisis de la RAM.

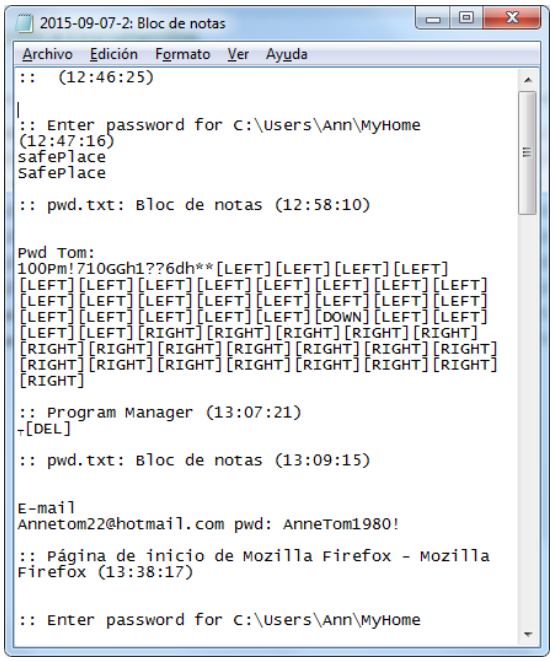


Imagen 82: contenido del archivo de password.

Nombre	Descripción	Hash md5	Tamaño bytes	Clasificación de evidencia
2015-09-07-2.dc	Archivo contenedor de posibles password	9BC3BCCD8917BEE6EEF11CC4F2276A48	157311800	A10

Tabla 35: detalle y clasificación de archivo con posibles contraseñas.

Nota: Dentro del archivo se observó un formato particular con algunas “etiquetas” extrañas.

CAPITULO 6. EXPLORACION Y CORRELACION DE EVIDENCIA.

6.1 Contextualización.

Teniendo en cuenta que en este caso forense se ha realizado una etapa de análisis sobre tres imágenes diferentes a través de tres capítulos diferentes, se ha decidido documentar la sub-etapa de exploración en un capítulo adicional, con el fin de consolidar los resultados obtenidos en los capítulos 3, 4 y 5 de este documento. Entiéndase este capítulo como una sub-etapa y no como otra etapa de la metodología aplicada.

En esta capitulo se inicia la exploración de la evidencia clasificada como datos transicionales. El objetivo es tomar cada dato transicional y enfocarse en su exploración, la ventaja de este enfoque iterativo es que, en este punto, el analista cuenta con la muestra de todos los datos recuperados en las pruebas técnicas realizadas anteriormente, lo que le permite manejar un universo de datos mejor conocidos.

6.2 Resumen de evidencias.

A continuación se presenta el resumen de la evidencia obtenida en la ejecución de pruebas y clasificación y sobre las que se trabajarán en este capítulo:

Etiqueta	Nombre	Descripción	Obtenido en Numeral	Hash md5	Tamaño bytes	Clasificación de evidencia
U1	Unalloc_59_8531968_123375616	Archivo exportado de la ruta /img_USB.E01/vol_vol4/$Unalloc/	3.3.2	09108F7E36EA92F3F4C7F287120F0917	104865792	A10
U2	00027625.png	Resultado de análisis con Foremost	3.3.2	945EDCB2F7B7671DFCAA43A3C781D62B	5816	A10
U3	Pendientes.ods	Hoja de cálculo con registros sospechosos de tarjetas bancos	3.3.3	6da97888ff474194bedc0cf99b5f67de	15766	A10
U4	whatsapp_castellano.db	Base de datos de mensajes	3.3.3	17c1db82b4827c126ccbcdc42de4d711	26624	A11
R1	hashdump.txt	Salida de información dentro del espacio asignado al SAM de Windows.	4.3.2	281A2A91E3004B9A2CD9D14D7D1B50BC	325	A10
R2	hivelist.txt	Salida de búsqueda de información hive.	4.3.2	75434DDA4F68A52656EB1A9BCE99049A	757	A01
R3	pslist.txt	Salida de búsqueda de procesos visibles	4.3.3	F2012B97F1C697379A5CF210A1844BF5	6072	A10
R4	psscan.txt	Salida de búsqueda de procesos visibles y ocultos	4.3.3	215CBDFB6E43F516313FA3FAAD0FF522	5658	A10
R5	summary.txt	Salida del comando de resumen de TrueCrypt	4.3.4	A54B3A3EA9AD0896050EB5286D722F7B	978	A10

R6	passphrase.txt	Salida de password de TrueCrypt	4.3.4	940EE489B8DA1E77AD899CA49A260298	40	A10
R7	master.txt	Salida de búsqueda master key de TrueCrypt	4.3.4	686C30C6ECB3CC6EF8E8B82377CFA6E1	550	A10
R8	0x833ba1a8_master.key	Master Key de TrueCrypt	4.3.4	0B955A82BB2D7D60EE7BC43550764533	64	A10
D1	$RQC0MZN.ods	Versión de Pendientes.ods encontrado en papelera de reciclaje.	5.3.5	6DA97888FF474194BEDC0CF99B5F67DE	15766	A10
D2	12034-20150907_162718.jpg	Imagen con metadatos de posición geográfica	5.3.8	68EC0B8CEF946E6403D7D222768163FD	1058873	A10
D3	12036-20150907_162746.jpg	Imagen con metadatos de posición geográfica	5.3.8	994823F3803436B04E0552F36179347A	915872	A10
D4	12038-20150907_162819.jpg	Imagen con metadatos de posición geográfica	5.3.8	25152D446AA96024F187BC54D81EFA6E	1916793	A10
D5	Skype	Directorio de procesos y actividades realizadas por medio de Skype	5.3.10	* Se omite hasta el momento	11230763	A10
D6	MyHome	Volumen cifrado mediante TrueCrypt	5.3.11	F45DEA81E1A23BB693D36EBE7EEAFDAC	157286400	A10
D7	11905-ListadoNumeraciones.zip	Archivo cifrado exportado del directorio descargas de usuario Ann.	5.3.12	28B6C7E90762A2174A32F9E7A2077F9A	62151	A10
D8	11907-TheJerm.rar	Malware hallado y exportado del directorio descargas del usuario Ann.	5.3.12	D01C1211D42FB78B7937FBDEFCA5E573	812659	A10
D9	Unalloc_93175_176128_10462588928	Archivo del espacio no asignado exportado del directorio $unalloc	5.3.13	F2E4A04E36FC4F6104A7C04706F858E5	1191473152	A10
D10	/img_Ann_HD.E01/Users/Ann/AppData/Roaming/B7VDmwss/yUmikJMYd3b.exe	Archivo potencialmente malicioso	5.3.14	88db5e8a850bb9e863e8b118e730a201	639488	A10
D11	/img_Ann_HD.E01/Users/Ann/Downloads/TheJerm.rar	Archivo potencialmente malicioso	5.3.14	d01c1211d42fb78b7937fbdefca5e573	812659	A10
D12	/img_Ann_HD.E01/Extracted/excel_server.exe	Archivo potencialmente malicioso	5.3.14		13824	A10
D13	2015-09-07-2.dc	Archivo contenedor de posibles password	5.3.15	9BC3BCCD8917BEE6EEF11CC4F2276A48	157311800	A10

Tabla 36. Resumen general de evidencias.

La columna “etiqueta” cuyos datos están marcados en **azul**, se utilizará para referenciar cada dato transicional cuando sea utilizado en las pruebas de exploración.

Convención de etiquetado:

- **U#**: Dato encontrado en imagen USB, # numero consecutivo.
- **R#**: Dato encontrado en imagen de memoria RAM, # numero consecutivo.
- **D#**: Dato encontrado en imagen de disco, # numero consecutivo.
- **E#**: Dato encontrado en proceso de exploración, # numero consecutivo.

6.3 Técnica de correlación.

Paso 1.

El analista iniciará la exploración seleccionando a criterio propio uno de los datos transicionales para buscar la correlación con los demás, el objetivo de este paso es subir el nivel de clasificación de los datos que actualmente aparecen aislados.

Cada iteración tendrá un nombre referente al artefacto forense del cual se extrajo el dato transicional base para la exploración.

Paso 2.

Se realiza una trazabilidad semántica de los datos transicionales utilizados.

Paso 3.

Se selecciona la evidencia digital.

6.4 Pruebas de exploración y correlación.

A continuación se inician las diferentes iteraciones teniendo como base la tabla 36.

6.4.1 TrueCrypt.

6.4.1.1 Procedimiento.

Se procede a instalar la misma versión de TrueCrypt que se encontró en el resultado en la evidencia etiquetada como **R5.**

Nombre	Tamaño	Versión	Hash md5
TrueCrypt	3466248 bytes	7.1a 32 bits	7A23AC83A0856C352025A6F7C9CC1526

Tabla 37: ficha técnica de software TrueCrypt.

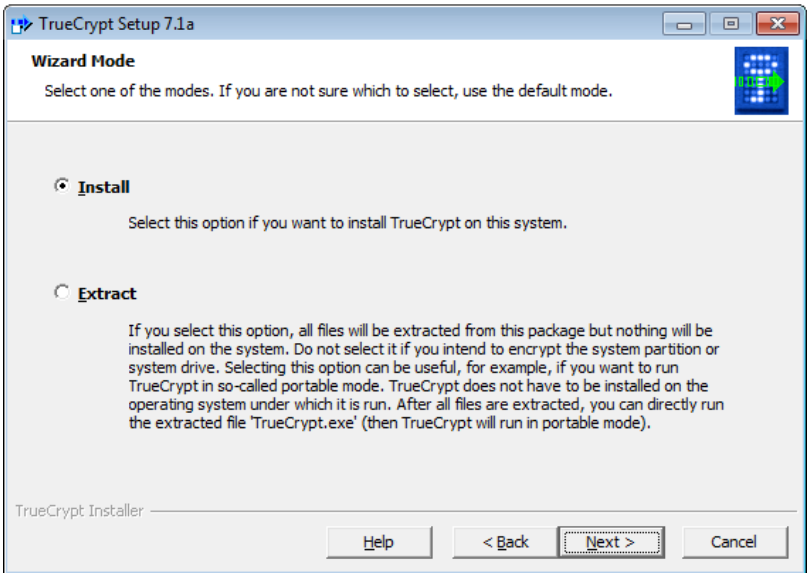


Imagen 83. Instalación de TrueCrypt.

Después de instalada la aplicación, se inicia el montaje del presunto volumen recuperado y etiquetado como **D6**

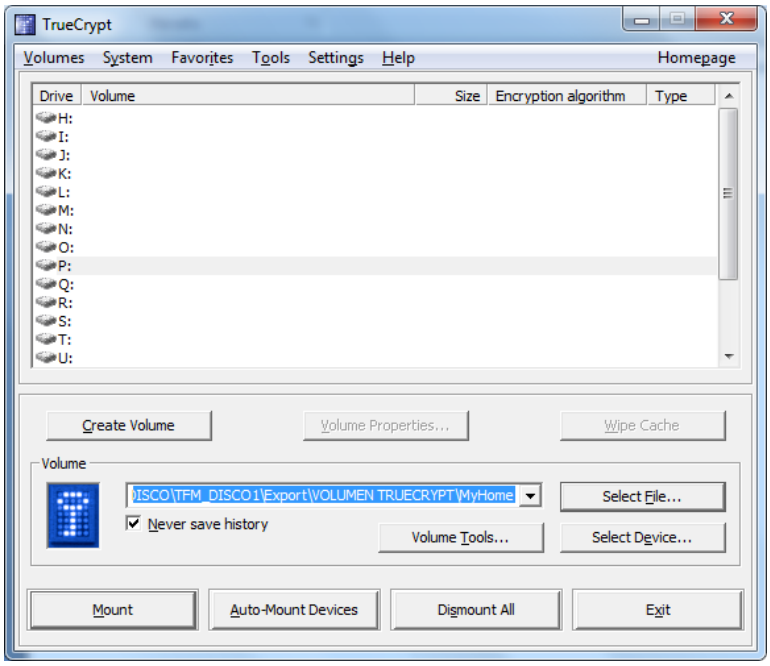


Imagen 84. Montaje de volumen.

En cuanto se ha montado el volumen el software ha solicitado un password, en este caso la llave simétrica para descifrar el volumen.
Se procede a digitar el texto obtenido mediante los datos transicionales **R5** y **D13.**

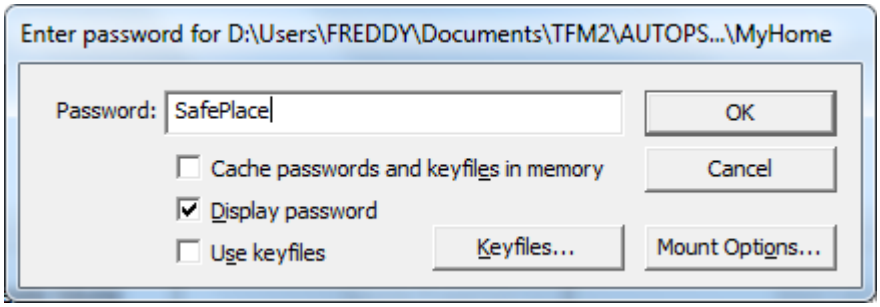


Imagen 85. Ingreso de password.

El password utilizado, *SafePlace,* es correcto, el software TrueCrypt ha montado un volumen, en este caso en la unidad P, de 148 MB

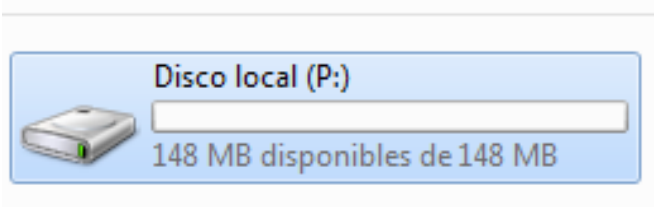


Imagen 86. Volumen MyHome montado.

Dentro del volumen se encuentran los siguientes 3 archivos:

Etiqueta	Nombre	Descripción	Encontrado en	Hash md5	Tamaño bytes
E1	pwd.txt.txt	Archivo con grupo de usuarios y password	MyHome/	255F79DADF9131F91C66A072A63C136C	221
E2	Tarjetas_Ricky.ods	Archivo con 12 registros de números nombres de personas.	MyHome/	0FA1F944C5BFAA86B25E2A8C7B54688F	14062
E3	TOTAL.ods	Archivo con 40 registros de aparentes números de tarjetas y nombres de personas.	MyHome/	5CE84B1CFAE53AFE1CC3B5F5ABDF0861	17816

Tabla 38: Contenido general de volumen cifrado.

Dentro del archivo etiquetado como **E1** se observa los siguientes Password's relacionados con un software o ambiente de uso:

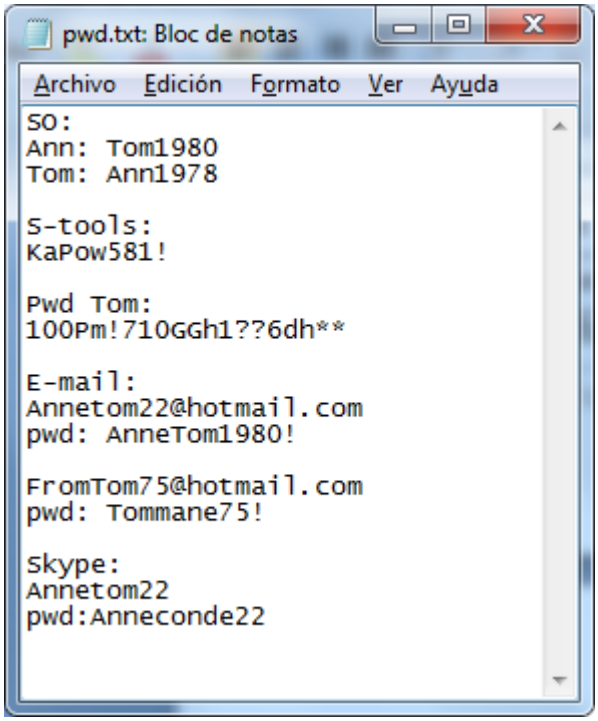


Imagen 87. Password's en MyHome.

Contexto	Usuario	Password
S.O	Ann	Tom1980
S.O	Tom	Ann1978
S-Tools		KaPow581!
	Tom	100Pm!710GGh1??6dh**
Hotmail.com	Annetom22@hotmail.com	AnneTom1980!
Hotmail.com	FromTom75@hotmail.com	Tommane75!
Skype	Annetom22	Anneconde22

Tabla 39: Password's dentro de volumen cifrado

Con los usuarios y password encontrados dentro de **E1** se exploraran los contextos de cada dato para tratar de acceder a información relevante.

En la prueba llevada a cabo en el numeral *5.3.9 Análisis de software instalado.* Se evidenció la instalación del software S-Tools, hasta aquí se ha obtenido un indicio claro de su utilización.

Con los datos encontrados en el volumen descifrado el analista toma las siguientes decisiones:

- Buscar archivos procesados con S-Tools.

- Credenciales de *Hotmail* y *Skype*, como encargado de aplicar la metodología de análisis forense sobre las imágenes entregadas por la policía, se entiende que el acceso a las cuentas de las plataformas de *Hotmail* y *Skype* hacen parte de un

contexto de investigación y análisis diferente y sobre el cual no se ha concedido la debida autorización de acceso por parte de las autoridades pertinentes. Por esta razón solo se resalta el hallazgo de estas credenciales sin llegar a la utilización de las mismas.

Se procede a descargar la herramienta S-Tools.

Nombre	Tamaño	Versión	Hash md5
S-Tools	370176 bytes	4.00	E245319BDB383C5A3A65DE238E6B25F1

Tabla 40: ficha técnica de software S-Tools.

Se inicia la investigación con enfoque en el password relacionado a S-tools.

El enfoque se selecciona teniendo en cuenta el uso que se le da a esta aplicación.

S-tools es un software dedicado al ocultamiento de información mediante la técnica de esteganografía, utiliza tres tipos de archivos como “contenedor” de la información que se desea ocultar, estos tipos de archivo son:

- .bmp
- .gif
- .wav

Con base en el conocido funcionamiento de S-Tools se procede a realizar una búsqueda de archivos de cualquiera de estos tres tipos para buscar información oculta.

Archivos .wav encontrados:

- ninguno relevante.

Archivos .gif encontrados:

- Se encontraron 8 archivos con extensión .gif en la ruta: */img_Ann_HD.E01/Users/Ann/Pictures/Fotos/Fotos Obs Fabra/*

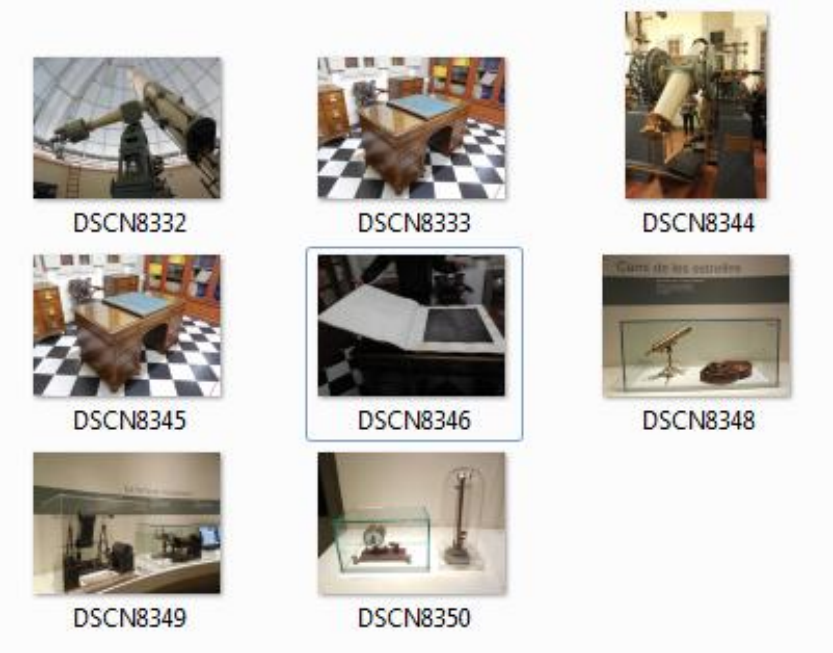


Imagen 88. Resumen de imágenes sospechosas.

Se procede a realizar el análisis de cada imagen utilizando el password **KaPow581!** de la tabla # 38 correspondiente al contexto S-Tools.

Después de realizado el análisis a las 8 imágenes encontradas, se obtuvo el siguiente resultado en la imagen *DSCN8333.gif*:

Imagen 89. Imagen con archivo oculto.

Se encontró oculto un archivo de nombre **Tarjetas_ricky.txt.**

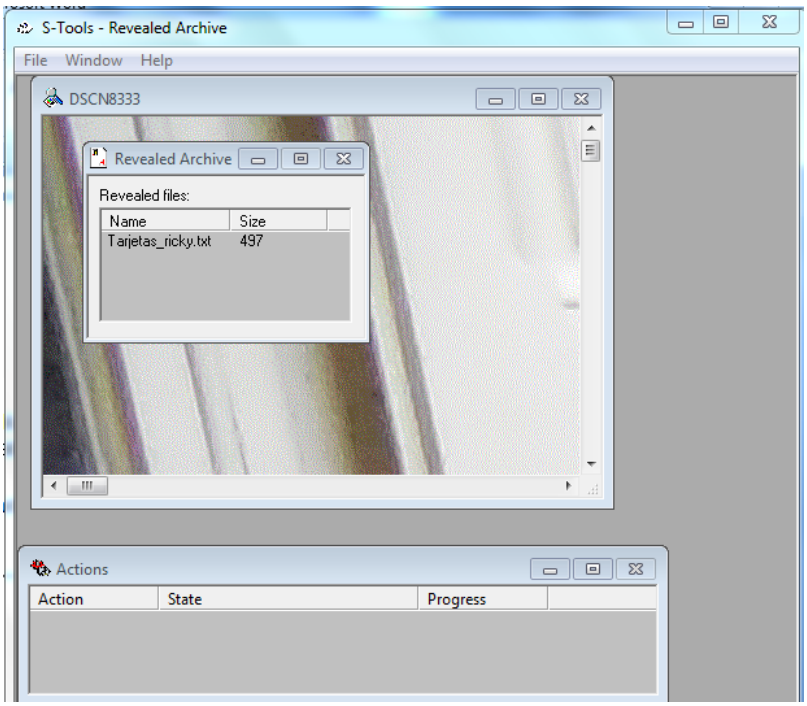


Imagen 90. Hallazgo con S-Tools.

El contenido del archivo oculto es el siguiente:

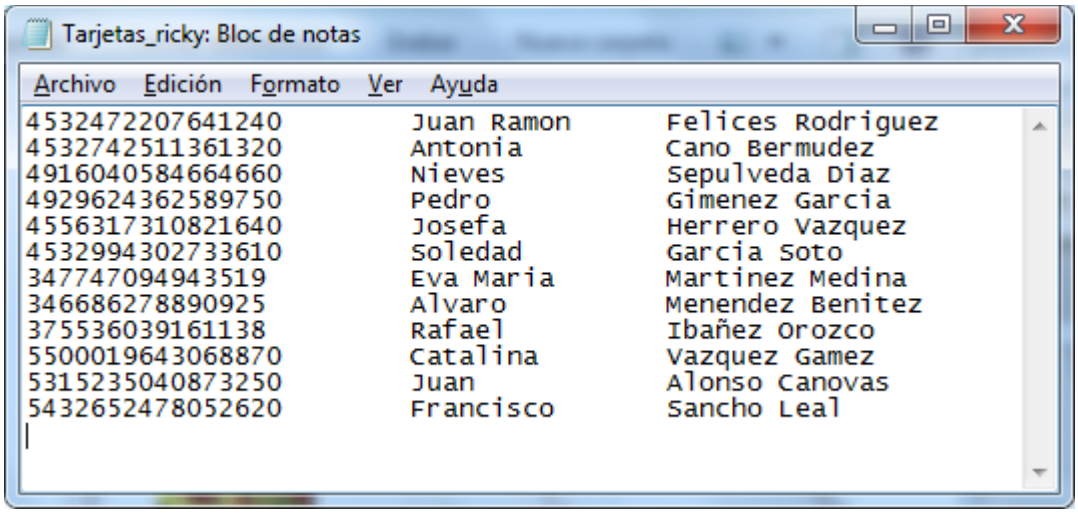


Imagen 91. Tarjetas_ricky.txt hallado oculto.

Se reconoce el mismo formato que relaciona lo que parece ser números de tarjetas de crédito, cada uno relacionado con el nombre de una persona, probablemente su titular.

Etiqueta	Nombre	Descripción	Hash md5	Tamaño bytes
E4	DSCN8333.gif	Imagen procesada con S-Tools, con archivo oculto	7D57A47B2E31D0B8C 149CEDAEB835767	7026074
E5	Tarjetas_Ricky.txt	Archivo oculto mediante técnica de esteganografía dentro de **E4**	BC05392EEE0D51A78 81C7800E94F9B9B	14062

Tabla 41. Archivos tratados con S-Tools.

6.4.1.2 Correlación y trazabilidad semántica.

Las siguientes premisas describen la conexión entre los datos:

a. En el análisis de memoria RAM se encontraron rastros de uso de la herramienta de cifrado llamada TrueCrypt.
b. Se obtuvo rastros de un volumen cifrado de nombre *MyHome*, con la ruta de almacenamiento y su aparente llave de cifrado y descifrado.
c. En el análisis de imagen de disco duro se encontró un archivo con la ruta, el tamaño y el nombre correspondiente a los datos de la memoria RAM, se observó un formato extraño en la estructura de este archivo.
d. En el análisis de imagen de disco duro se encontró un archivo con diferentes Password's en el que se confirmo la utilización del password *SafePlace* relacionado con un archivo de nombre *MyHome.*
e. Se descifró el volumen *MyHome* mediante el password *SafePlace,* dentro del cual se encontraron tres archivos, uno llamado *pwd.txt.txt* que contiene dos correos electrónicos y sus respectivas contraseñas de acceso, otro archivo llamado *Tarjetas_Ricky.ods* y un tercer archivo llamado *Total.ods.*
f. El archivo *Tarjetas_Ricky.ods* contiene doce registros que coinciden con los primeros doce registros del archivo *Pendientes.ods.*
g. El archivo *Total.ods* contiene cuarenta registros con la misma estructura del archivo *Pendientes.ods,* este archivo contiene registros que están en *Pendientes.ods,* en *Tarjetas_Ricky.ods* y los que se observan en la imagen *00027625.png.*
h. El archivo *Tarjetas_Ricky.txt* contiene los mismos registros que el archivo *Tarjetas_Ricky.ods.*
i. Con la exploración del volumen *MyHome* se confirma el vínculo entre el usuario *Ann* y parte de los datos transicionales hallados en la imagen USB.

6.4.1.3 Selección de evidencia digital.

En este punto se decide seleccionar la evidencia digital que ha sido correlacionada y aporta relevancia y suficiencia a la investigación o sirve como soporte de trazabilidad.

Etiqueta	Nombre	Obtenido en prueba	Clasificación
R5	summary.txt	4.3.4	A10
D6	MyHome	5.3.11	A11
D13	2015-09-07-2.dc	5.3.15	A10
E1	pwd.txt.txt	6.4.1.1	A10
E2	Tarjetas_Ricky.ods	6.4.1.1	A11
E3	TOTAL.ods	6.4.1.1	A11
E4	DSCN8333.gif	6.4.1.1	A10
E5	Tarjetas_Ricky.txt	6.4.1.1	A11
R1	hashdump.txt	4.3.2	A10
U1	00027625.png	3.3.2	A11
U2	Pendientes.ods	3.3.3	A11

Tabla 42. Evidencia digital relacionada con TrueCrypt.

Se ha decidido incluir evidencia de clasificación A10 teniendo en cuenta que es evidencia de soporte que ha sido útil para la correlación de datos transicionales, como es el caso de **R1**, por ejemplo, por medio de la cual se evidencia la existencia de cuentas de usuarios del sistema operativo.

6.4.2 Directorio de *Skype*.

6.4.2.1 Procedimiento.

Se selecciona la evidencia **D5**, obtenida en el punto *5.3.10 Búsqueda de historial Skype,* dentro de este directorio se encontró la siguiente estructura de archivos:

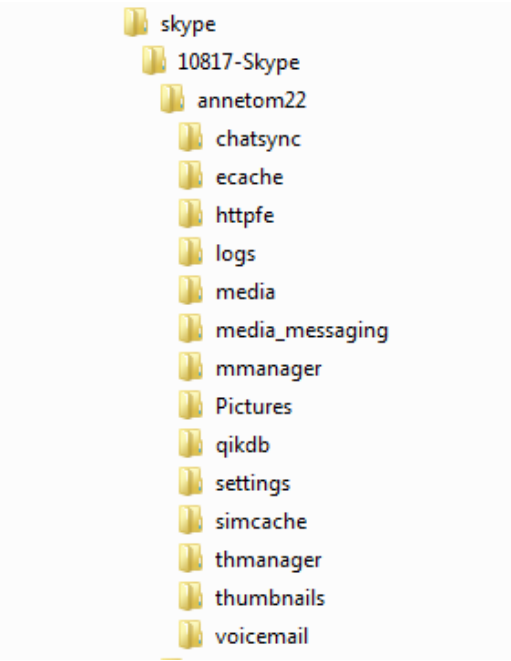


Imagen 92. Estructura de directorio Skype.

De acuerdo al sitio oficial de Skype, https://support.skype.com/es/faq/FA392/donde-puedo-encontrar-mi-historial-de-chats-en-skype-para-el-escritorio-de-windows-y-que-puedo-hacer-con-el, existe un archivo donde se almacena el historial de mensajes llamado *main.db* en sistemas operativos Windows.

Dentro del directorio annetom22, en la ruta */img_Ann_HD.E01/Users/Ann/AppData/Roaming/Skype/annetom22/*, se ha encontrado el archivo *main.db*:

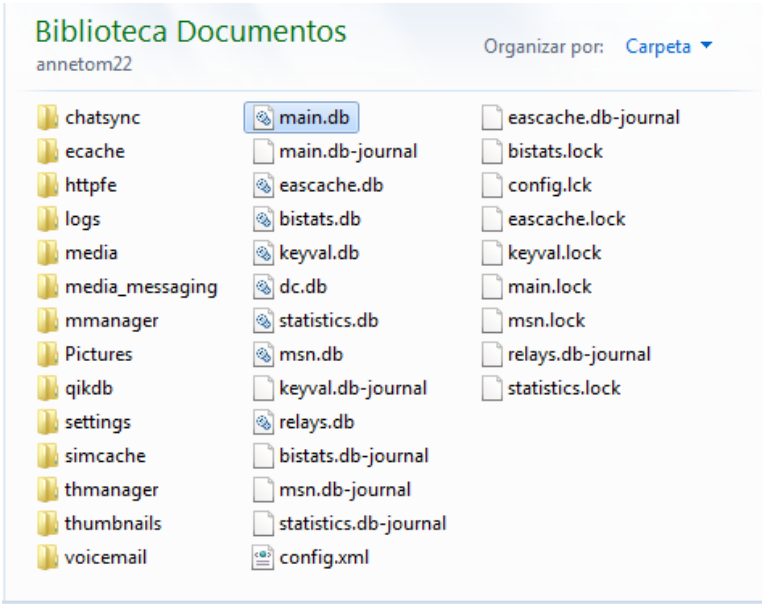


Imagen 93. Archivo main.db encontrado.

Hallado el archivo *main.db* se visualiza por medio del programa *SQLitebrowser.*

Etiqueta	Nombre	Descripción	Hash md5	Tamaño bytes
E6	main.db	Archivo con estructura de mensajes de *Skype.*	BB68E7232C9BD346DB3 AD82EBEEDA214	458752

Tabla 43. Base de datos con mensajes de Skype.

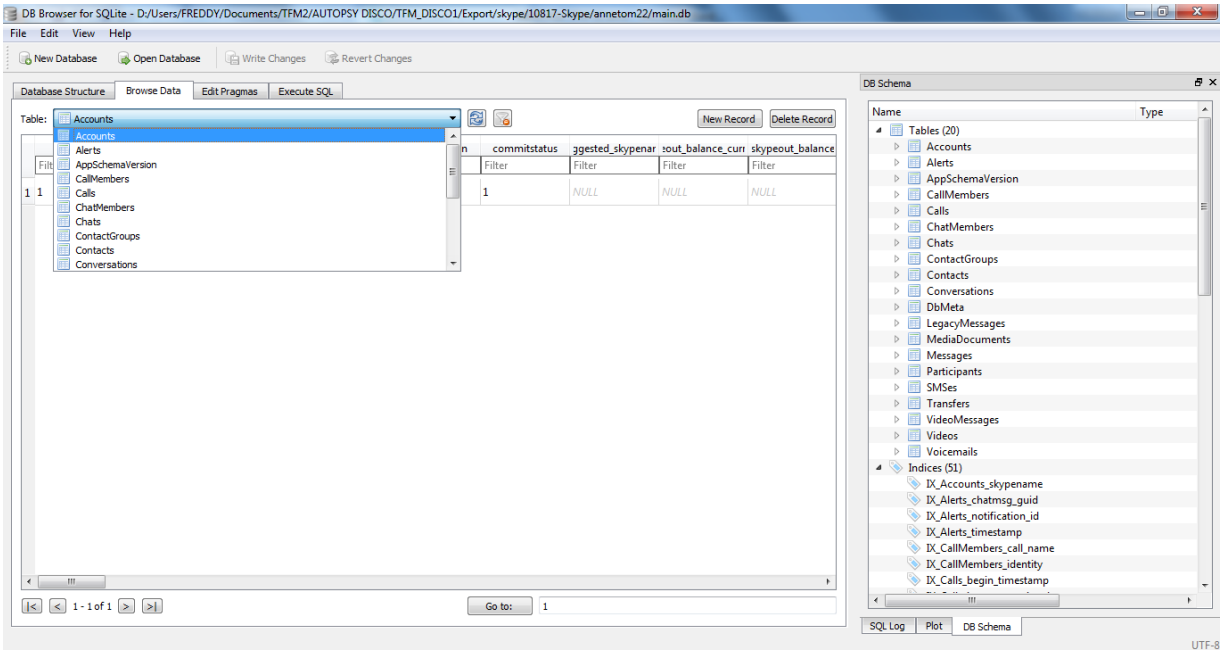


Imagen 94. Apertura de main.db con SQLitebrowser.

Se encuentran datos ordenados y estructurados por medio de filas y columnas perteneciente a la cuenta de Skype **annetom22.** El índice de la estructuración de los datos es el siguiente:

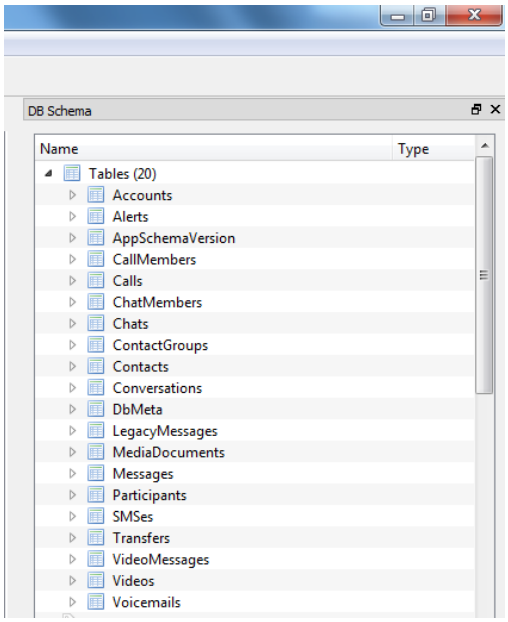


Imagen 95. Agrupaciones lógicas.

Se detecta que existe una agrupación de mensajes de la cuenta dentro de la entrada *Messages* del índice mostrado anteriormente.

Después de inspeccionar la entrada *Messages*, se han encontrado las siguientes tres conversaciones que serán enunciadas en su orden cronológico.

Conversación # 1:

En esta conversación se hace referencia a algunas fotos que el usuario **annetom22** le ha enviado al usuario **rickyrodriguezgarcia** accesibles a través de la contraseña **KaPow581!**

Fecha	Hora	usuario	nombre	Mensaje
04/09/2015	03:51:06 p.m. GMT	Rickyrodriguez garcia	Ricky Rodriguez	*Hola Anne G.H., m'agradaria afegir-te com a contacte.*
04/09/2015	03:52:40 p.m. GMT	Rickyrodriguez garcia	Ricky Rodriguez	*Saludos, ya he recibido las fotos...*
04/09/2015	03:53:04 p.m. GMT	annetom22	Anne G.H.	*Me alegro... ¿Todo bien?*
04/09/2015	03:53:16 p.m. GMT	Rickyrodriguez garcia	Ricky Rodriguez	*De fábula, pero… he olvidado la contraseña…*
04/09/2015	03:53:33 p.m. GMT	annetom22	Anne G.H.	*¡Pues qué bien!*
04/09/2015	03:53:40 p.m. GMT	Rickyrodriguez garcia	Ricky Rodriguez	*...lo siento...*
04/09/2015	03:54:19 p.m. GMT	Rickyrodriguez garcia	Ricky Rodriguez	*¿Puedes pasármela?*
04/09/2015	03:54:48 p.m. GMT	annetom22	Anne G.H.	*Tú mismo... ¿A ti qué te parece?*
04/09/2015	03:55:00 p.m. GMT	Rickyrodriguez garcia	Ricky Rodriguez	*Tampoco entremos en modo paranoico… No creo que pase nada*
04/09/2015	03:55:38 p.m. GMT	annetom22	Anne G.H.	*Evidentemente, nunca pasa nada... En fin, aquí va:* ***KaPow581!***
04/09/2015	03:55:52 p.m. GMT	Rickyrodriguez garcia	Ricky Rodriguez	*Gracias, recuerdos a Tom*
04/09/2015	03:56:06 p.m. GMT	annetom22	Anne G.H.	*Hasta luego Ricky*

Tabla 44. Conversación 1 de Skype.

Conversación # 2:

Esta conversación se produce entre el usuario **aram768** y el usuario **annetom22,** en ella se hace referencia a la necesidad de una reunión entre ambos usuarios para saldar una deuda que tiene aram768 con annetom22 por un “lote de tarjetas” que Anne le ha entregado.

El sitio de la reunión lo especifica Aram mediante tres archivos enviados a Anne.

Fecha	Hora	usuario	nombre	Mensaje
07/09/2015	05:19:13 p.m. GMT	aram768	live:aram768	*Hola, Anne G.H., me gustaría agregarlo como contacto.*
07/09/2015	05:19:19 p.m. GMT	annetom22	Anne G.H.	*NULL*

07/09/2015	05:19:37 p.m. GMT	aram768	Aram B.V.	*Hola, hace días que tenemos que quedar… Todavía tengo que pagarte el último lote de tarjetas…*
07/09/2015	05:20:22 p.m. GMT	aram768	Aram B.V.	*Precisamente este sábado estuve en tu ciudad y descubrí un sitio muy discreto para quedar… Te mando algunas fotos, a ver si lo reconoces…*
07/09/2015	05:24:50 p.m. GMT	aram768	Aram B.V.	*Ei! disculpa, te lo paso en 5 min...tengo alguien al telf*
07/09/2015	05:25:08 p.m. GMT	annetom22	Anne G.H.	*No te preocupes, yo tambien algo liada...*
07/09/2015	05:28:35 p.m. GMT	aram768	Aram B.V.	*hola ya estoy aqui de nuevo... ahi van las fotos*
07/09/2015	05:28:48 p.m. GMT	aram768	Aram B.V.	*<files alt=envió los archivos "20150907_162718.jpg" , "20150907_162746.jpg" , "20150907_162819.jpg" ">*
07/09/2015	05:31:10 p.m. GMT	annetom22	Anne G.H.	*Pues si, lo conozco. Tienes razon, es muy discreto. ¿Que tal el proximo sabado a las 17:00?*
07/09/2015	05:31:18 p.m. GMT	aram768	Aram B.V.	*Perfecto, hasta luego pues*

Tabla 45. Conversación 2 de Skype.

La fecha y hora de la transferencia de los archivos es el 7 de septiembre de 2015 a las 05:28:35 p.m GMT, dentro del directorio *Skype* se encuentra un directorio llamado *My Skype Received Files* en el que se han encontrado tres archivos que concuerdan con el nombre, tipo y fecha de creación de las imágenes referenciadas en la conversación # 2.

Las imágenes encontradas coinciden con las imágenes recuperadas en las pruebas realizadas en el punto ***5.3.8 Análisis de metadatos*** y etiquetadas como **D2**, **D3** y **D4**. En esta prueba se había ubicado el lugar correspondiente a la toma de fotos por medio de coordenadas GPS encontradas en estas imágenes. Dicho lugar es la Plaza Miranda de **castellar del Vallés,** municipio español de la provincia de Barcelona, Cataluña.

Conversación # 3:

En esta conversación interviene el usuario **rickyrodriguezgarcia** y el usuario **annetom22**, se hace referencia a una transferencia iniciada por Ricky enviándole "algo" a Anne.

- Anne recibe lo enviado por Ricky entre las 5:35 pm GMT y las 5:37 pm GMT.
- Lo que recibió Anne está cifrado por una contraseña de uso habitual como el mismo usuario lo especifica.
- El usuario Ricky manifiesta haberse confundido en el envío.

Fecha	Hora	usuario	nombre	Mensaje
07/09/2015	05:35:05 p.m. GMT	rickyrodriguezgarcia	Ricky Rodriguez	*Hola Anne, te mando algo que te va a interesar*
07/09/2015	05:35:17 p.m. GMT	rickyrodriguezgarcia	Ricky Rodriguez	*http://we.tl/e14LlZzkSz"*
07/09/2015	05:35:25 p.m. GMT	annetom22	Anne G.H.	*A ver... Te digo algo...*
07/09/2015	05:37:42 p.m. GMT	annetom22	Anne G.H.	*¿Es lo que parece?*
07/09/2015	05:37:54 p.m. GMT	annetom22	Anne G.H.	*Tiene una contraseña y supongo que sera la de siempre...*
07/09/2015	05:38:11 p.m. GMT	rickyrodriguezgarcia	Ricky Rodriguez	*Efectivamente! <ss type=wink">;-)</ss>"*
07/09/2015	05:41:16 p.m. GMT	annetom22	Anne G.H.	*Esto es un poco raro...*
07/09/2015	05:41:45 p.m. GMT	rickyrodriguezgarcia	Ricky Rodriguez	*Ups... creo que me he confundido, te lo reenvio más tarde*
07/09/2015	05:41:52 p.m. GMT	annetom22	Anne G.H.	*De acuerdo!*

Tabla 46. Conversación 3 de Skype.

Se procede a revisar el directorio de descargas del usuario Ann en búsqueda de archivos que coincidan con la fecha y hora de descarga de la conversación.

Se observa que uno de los archivos obtenidos de la prueba técnica del numeral ***5.3.12 búsquedas de archivos descargados,*** etiquetado como **D7**, coincide dentro del rango de fecha y hora.

Fecha/hora de modificación-creación	Nombre	Descripción	Hash md5	Tamaño bytes
2015-09-07 / 12:36:29 GMT -05:00	ListadoNumeraciones.zip	Archivo cifrado exportado del directorio descargas de usuario Ann.	28B6C7E90762A2174A32F9E7A2077F9A	62151

Tabla 47. Archivo relacionado en conversación de Skype.

Se encuentra que el archivo está protegido por contraseña, como se esperaba, según la conversación.

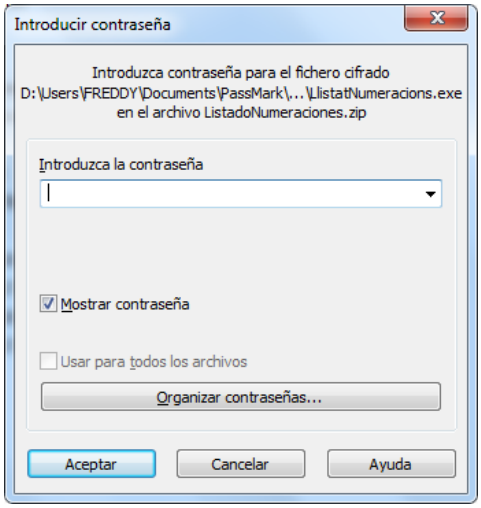


Imagen 96. Apertura de archivo enviado por Ricky.

En este punto recordamos que en la conversación # 1 el usuario Anne y el mismo usuario, Ricky, manejan una contraseña que fue revelada dentro de esa conversación, ***KaPow581!*** y anteriormente encontrada en las evidencias **E1** y **D13**

Se procede a utilizar esta contraseña para intentar descifrar el archivo *ListadoNumeraciones.zip.*

La contraseña es correcta. En el instante del descifrado el antimalware lo ha reconocido como una amenaza de tipo *Backdoor*. Se decide apartar el archivo en el directorio de cuarentena del antimalware para su posterior exploración, al igual que el malware encontrado en las pruebas del numeral *5.3.14 Búsqueda de malware*.

Imagen 97. Detección del antimalware.

Etiqueta	Nombre	Descripción	Hash md5	Tamaño bytes
E7	LlistatNumeracions.exe	Malware encontrado en archivo ListadoNumeraciones.zip	F91F42D1EDB22D65DC2DB703D63A895B	119565

Tabla 48. Malware enviado por Ricky rodríguez.

6.4.2.2 Correlación y trazabilidad semántica.

Las siguientes premisas describen la conexión entre los datos:

a. En el análisis de memoria RAM se encontraron rastros de la ejecución del proceso *skype.exe* correspondiente al software de comunicaciones *Skype,* soportado en **R3** y **R4.**
b. Se determinó que el historial de mensajes enviados y recibidos por medio de este software queda almacenado en el archivo *main.db*, etiquetado como **E6.**
c. Dentro del historial se encontraron tres conversaciones realizadas entre el 04/09/2015 y el 07/09/2015, con formato de fecha dd/mm/aaaa, en los que intervinieron tres usuarios diferentes, el primero ***annetom22*** registrado con el nombre ***Anne G.H***, el segundo ***Rickyrodriguezgarcia*** registrado con el nombre ***Ricky Rodriguez*** y el tercer usuario ***aram768*** registrado con el nombre ***Aram B.V.***
d. La conversación # 1 se inició el 04 de septiembre del 2015 a las 03:51:06 p.m GMT y finalizó el mismo día cinco minutos después entre el usuario ***annetom22*** y el usuario ***Rickyrodriguezgarcia***, esta conversación hasta el momento solo ha sido útil para conocer el password utilizado entre estos dos usuarios.
e. La conversación # 2 se inició el lunes 07 de septiembre del 2015 a las 05:19:13 p.m. GMT y finalizó a las 05:31:18 p.m. GMT del mismo día entre el usuario ***annetom22*** y el usuario ***aram768***. En esta conversación se resalta el tercer mensaje en el que ***aram768*** manifiesta deber dinero a ***annetom22*** por el *"lote de tarjetas"* recibido. Teniendo en cuenta las evidencias digitales obtenidas en el numeral ***6.4.1 TrueCrypt*** se percibe un posible tráfico de tarjetas de crédito implicando al usuario *Ann.*
f. En la misma conversación # 2 se menciona una reunión entre ambos usuarios el "próximo sábado", con lo que se deduce que la reunión se llevaría a cabo el sábado 12 de septiembre del 2015 a las 17:00 hora local. El lugar de la reunión se deduce por medio de las evidencias **D2**, **D3** y **D4** y el procedimiento llevado a cabo en el numeral ***5.3.8 Análisis de metadatos.***
g. Habiendo obtenido el lugar de la reunión, la Plaza Miranda de **castellar del Vallés,** municipio español de la provincia de Barcelona, Cataluña, se infiere que *Anne G.H* vive cerca de este sitio como lo manifiesta *Aram B.V.* en esta conversación.
h. La conversación # 3 se inició el lunes 07 de septiembre del 2015 a las 05:35:05 p.m. GMT y finalizó a las 05:41:52 p.m. GMT del mismo día entre el usuario ***annetom22*** y el usuario ***rickyrodriguezgarcia***. En esta conversación se evidenció que *Ricky Rodriguez* le envío un malware a *Anne G.H,* que coincide con la evidencia **D7**obtenida en el numeral ***5.3.12 Búsqueda de archivos descargados.***

i. En este punto el analista percibe la necesidad de una exploración a los archivos catalogados como malware.

6.4.2.3 Selección de evidencia digital.

Se selecciona la evidencia digital que ha sido correlacionada y aporta relevancia y suficiencia a la investigación o sirve como soporte de trazabilidad.

Etiqueta	Nombre	Obtenido en prueba	Clasificación
E6	main.db	6.4.2.1	A11
D2	12034-20150907_162718.jpg	5.3.8	A11
D3	12036-20150907_162746.jpg	5.3.8	A11
D4	12038-20150907_162819.jpg	5.3.8	A11
E7	LlistatNumeracions.exe	6.4.2.1	A10
D13	2015-09-07-2.dc	5.3.15	A10
E1	pwd.txt.txt	6.4.1.1	A10
R3	pslist.txt	4.3.3	A10
R4	psscan.txt	4.3.3	A10

Tabla 49. Evidencia digital relacionada con Skype.

6.4.3 Mensajes de Whatsapp.

6.4.3.1 Procedimiento:

Se procede a visualizar la información que está estructurada dentro de la evidencia **U4,** el archivo ***whatsapp_castellano.db***, mediante el software *SQLitebrowser.*

La aplicación *Whatsapp* utiliza un protocolo llamado *FunXMPP* para la gestión de mensajería, incluido su almacenamiento e histórico, los usuarios en este protocolo son gestionados bajo la siguiente máscara: *número_telefonico@s.whatsapp.net*. Dentro de la estructura se encontraron los siguientes usuarios:

- 99999999268@s.whatsapp.net
- 34999999092@s.whatsapp.net
- 34999999118@s.whatsapp.net
- 34999999621@s.whatsapp.net

De la estructura “messages” se obtienen los siguientes mensajes allí guardados:
De la conversación se deduce

Fecha / hora	Contacto	Mensaje
null	mié, 09 noviembre 2011 22:10:25.308 GMT	Buenos días! hablamos de como llevamos el tema de las tarjetas o no os atrevéis....
null	mié, 09 noviembre 2011 22:14:09.419 GMT	梵

34635293190@s.whatsapp.net	mié, 09 noviembre 2011 22:14:32.089 GMT	Jajajajajajajaja
34635293190@s.whatsapp.net	mié, 09 noviembre 2011 22:14:33.318 GMT	Si si! hablemos que ya lo tenemos todo medio preparado no?
34660401445@s.whatsapp.net	mié, 09 noviembre 2011 22:19:11.751 GMT	Sip
null	mié, 09 noviembre 2011 22:20:06.297 GMT	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...
34635293190@s.whatsapp.net	mié, 09 noviembre 2011 22:20:08.781 GMT	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	mié, 09 noviembre 2011 22:20:16.775 GMT	Jajajaajajajajaja
34635293190@s.whatsapp.net	mié, 09 noviembre 2011 22:20:22.716 GMT	Sk sin noo son nddd
34660401445@s.whatsapp.net	mié, 09 noviembre 2011 22:20:31.622 GMT	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...
34635293190@s.whatsapp.net	mié, 09 noviembre 2011 22:20:33.976 GMT	OK Iván, oído cocina! cuando haga las compras todas las entregas serán el mismo viernes, yo te aviso!
Null	mié, 09 noviembre 2011 22:23:54.984 GMT	Amén
Null	mié, 09 noviembre 2011 22:27:09.642 GMT	OK dejarme trabajar un poco el phising y las alternativas para conseguir más tarjetas... os digo algo
Null	lun, 26 diciembre 2011 23:20:56.700 GMT	***fragmento extraído**
34635293190@s.whatsapp.net	lun, 26 diciembre 2011 23:23:06.404 GMT	que es esto?
Null	lun, 26 diciembre 2011 23:23:39.691 GMT	soy el más fuerte! ya tengo todos los números i pins válidos para nuestro negocio del siglo!!!
Null	lun, 26 diciembre 2011 23:23:42.584 GMT	Jajajajaja
34660401445@s.whatsapp.net	lun, 26 diciembre 2011 23:23:54.109 GMT	yo ya estoy listo que necesito pasta!!!!
34635293190@s	lun, 26 diciembre 2011 23:23:55.546 GMT	yo tb estoy listo, cuando quieras me lo envías }:X

.whatsapp.net		
Null	lun, 26 diciembre 2011 23:32:22.327 GMT	además soy un crack, porqué lo tengo todo escondido en mi ordenador, no me lo encontraría ni la poli ;p
Null	lun, 26 diciembre 2011 23:32:27.850 GMT	somos unos profesionales! mira que es fácil hacer pasta.... vivan los sobresueldos!
Null	lun, 26 diciembre 2011 23:32:30.047 GMT	Jajajaja
34660401445@s .whatsapp.net	lun, 26 diciembre 2011 23:32:30.047 GMT	contigo estamos tranquilos, eres un crack!
34635293190@s .whatsapp.net	lun, 26 diciembre 2011 23:34:14.756 GMT	eres la ...
34635293190@s .whatsapp.net	lun, 26 diciembre 2011 23:34:43.323 GMT	滌
34635293190@s .whatsapp.net	lun, 26 diciembre 2011 23:34:47.626 GMT	Jajajjaajaja
Null	mar, 27 diciembre 2011 09:21:55.949 GMT	Raúl ya lo tienes en el correo, el pwd del zip es somosunoscracks... coordínate con Iván y hablamos de repartir...
34635293190@s .whatsapp.net	mar, 27 diciembre 2011 09:22:28.284 GMT	OK
Null	mar, 14 febrero 2012 19:56:44.000 GMT	Feliz sanvalentin覦
Null	mar, 14 febrero 2012 20:03:17.912 GMT	Q ironia
Null	mar, 14 febrero 2012 20:03:19.689 GMT	Vv
Null	mar, 14 febrero 2012 20:03:23.555 GMT	En fin gracias jeje
Null	mar, 14 febrero 2012 20:03:33.443 GMT	傑
Null	mar, 14 febrero 2012 20:11:03.000 GMT	艕
Null	mié, 15 febrero 2012 11:43:30.000 GMT	籥
Null	mié, 15 febrero 2012 13:52:58.541 GMT	Jjjajajasjs
Null	mié, 15 febrero 2012 13:53:10.119 GMT	Ya sapsss 傑
34635293190@s .whatsapp.net	mié, 15 febrero 2012 22:31:57.691 GMT	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...

Null	jue, 16 febrero 2012 11:51:16.668 GMT	:P
Null	jue, 16 febrero 2012 21:00:39.000 GMT	:)
Null	jue, 16 febrero 2012 21:49:36.542 GMT	Feooo
Null	jue, 16 febrero 2012 21:51:54.476 GMT	?
Null	jue, 16 febrero 2012 21:55:04.791 GMT	Jejeje
Null	jue, 16 febrero 2012 21:55:46.102 GMT	蠣 a buena hora
Null	jue, 16 febrero 2012 21:55:49.893 GMT	褒
34999999621@s.whatsapp.net	jue, 16 febrero 2012 22:31:08.571 GMT	Hola Josep!
34999999621@s.whatsapp.net	jue, 16 febrero 2012 22:31:11.935 GMT	no me acordé de avisarte... pero hay que hacer una práctica de la uoc y es muy difícil!
34999999621@s.whatsapp.net	jue, 16 febrero 2012 22:31:20.832 GMT	y se tiene que entregar este fin de semana X_D
34999999118@s.whatsapp.net	jue, 16 febrero 2012 22:31:42.659 GMT	Laia :*
34999999118@s.whatsapp.net	jue, 16 febrero 2012 22:31:45.853 GMT	Mña a k hora hay k ir al cole????
34999999118@s.whatsapp.net	jue, 16 febrero 2012 22:32:03.837 GMT	A las 8:15
34999999118@s.whatsapp.net	jue, 16 febrero 2012 22:32:14.168 GMT	Clase normal?
34999999118@s.whatsapp.net	jue, 16 febrero 2012 22:29:24.000 GMT	Las 3 primeras horas si
34999999118@s.whatsapp.net	jue, 16 febrero 2012 22:33:45.220 GMT	Justo las k tngo
34999999118@s.whatsapp.net	jue, 16 febrero 2012 22:33:47.165 GMT	:/
34999999118@s.whatsapp.net	jue, 16 febrero 2012 22:33:51.286 GMT	XD

34999999118@s.whatsapp.net	jue, 16 febrero 2012 22:34:00.872 GMT	Bueno ps nos vemos.mña :)
34999999621@s.whatsapp.net	vie, 17 febrero 2012 08:10:09.000 GMT	hola carlos
34999999621@s.whatsapp.net	vie, 17 febrero 2012 08:10:14.000 GMT	ah! yo ya la he hecho y entregado
34999999621@s.whatsapp.net	vie, 17 febrero 2012 09:06:50.790 GMT	y ahora me lo dices! ya te preguntaré lo que no me salga...
34999999621@s.whatsapp.net	vie, 17 febrero 2012 09:06:55.450 GMT	¬¬

Tabla 50. Mensajes de Whatsapp.

Dentro de la estructura se encuentra el siguiente ** fragmento extraído:*

/9j/4AAQSkZJRgABAQAAAQABAAD/2wBDAAYEBQYFBAYGBQYHBwYIChAKCgkJChQODwwQFxQYGBcUFhYaHSUfGhsjHBYWICwgIyYnKSopGR8tMC0oMCUoKSj/2wBD
AQcHBwoIChMKChMoGhYaKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCj/wAARCABkAEgDASIAAhEBAxEB/8QAHwAAAQU
BAQEBAQEAAAAAAAAAAAECAwQFBgcICQoL/8QAtRAAAgEDAwIEAwUFBAQAAAF9AQIDAAQRBRIhMUEGE1FhByJxFDKBkaEII0KxwRVS0fAkM2JyggkKFhcYGRolJicoK
So0NTY3ODk6Q0RFRkdISUpTVFVWV1hZWmNkZWZnaGlqc3R1dnd4eXqDhIWGh4iJipKTlJWWl5iZmqKjpKWmp6ipqrKztLW2t7i5usLDxMXGx8jJytLT1NXW19jZ2uHi4+Tl5ufo
6erx8vP09fb3+Pn6/8QAHwEAAwEBAQEBAQEBAQAAAAAAAAECAwQFBgcICQoL/8QAtREAAgECBAQDBAcFBAQAAQJ3AAECAxEEBSExBhJBUQdhcRMiMoEIFEKRobHB
CSMzUvAVYnLRChYkNOEl8RcYGRomJygpKjU2Nzg5OkNERUZHSElKU1RVVldYWVpjZGVmZ2hpanN0dXZ3eHl6goOEhYaHiImKkpOUlZaXmJmaoqOkpaanqKmqsrO0tba3u
Lm6wsPExcbHyMnK0tPU1dbX2Nna4uPk5ebn6Onq8vP09fb3+Pn6/9oADAMBAAIRAxEAPwD6ZsQDZQHHWNf5VPtHoKg0/wD48Lb/AK5L/KrFQIbtHpRtHpQxwpNcrdeILqKZ41
jDbDjOQM/pUTmoasaV9jqwB6UuB6VxJ8WT+d5OIhNt3bPMG7HrjHSnReLJpC6qqMyHawVwdp64PHBxUe3h3DlZ2RjQ9VU/hTfIhPWJP++RWRourS385Vl2KvXoc8H2rcFaRkp
K6EQm0tyOYIv++BRU/aiqAq6d/wAg+2/65L/Kp6h0/wD48bf/AK5r/Kp6AGv90/SvOr9n+3T7WTG7oa9Ff7przbUQjXdypzyxBrnxCvFFQdmcTcawh8TmSJ1WRJVspAwHBYMwYH
6Adu9bem27W95fvFcxO9w4dAUC+pPTr1rj9d06c6le+U0dvFFMkglLcE7Dtzu4yOP++selang+8F7f3EzZdTErk9gxJ6ZOR0PGO3PNc04qKVioycr3VrHpngN53kkF15fmDbkpnGc
HOM9q7cdK43wSVM8pUY5H8jXZCuyj8BD3FPSijtRWoivY/wDHlB/1zX+VTGobL/jzg/65r/KpqAGt9015bqv2hdVugIJSu/IYIcGvUj901kNBIBnY35VnOPMrAeQ6mtxFdPINPuZoHI
eRoiVcMBgYHcYx+tYOkrrllqt20WmTG1uCNhkkICAFu3JHXpXuzwyAEEP/AN8k1E0bAcpIT/uGs1Tt0G22rXMb4cvK01wJo3T5hjcMdjXf1iaUjLdL8rAcnlSO1bg6VrBWQkrCdqKXt
RVgV7P/AI9IP9xf5VLUVp/x6w/7g/lUtACV49478X+JNJ8QzW9peCO1YN5SrAmRxxywPU+vUg8YxXsPavmj4oavMviaOGBpRJMiyFTkIW+X2wCpx+P0pdRPYI8LRFbxTdausN
1qUJt8ksz28SgjPrle3PfrivXF8XyzIYrJ4Zpd5UyMhwp9No5zXynCjxzPEkXmsSD97GFyOefoO1blteXNlYl3uyDkCOJfm5zxz25GfpTavsZxk47n1bp+sFpI4LqaA3DOEKhShJwDwC
eev8AStwHivnn4X3CTeJNK/0qR7jf+9D4LM205yfqK+hhURNb3/HrD/uD+VS1FZ/8AHpD/ALi/yqWgBKTABzilooAKKKKAP//Z

En el que se observan caracteres sin sentido semántico a simple vista.

Explorando con más detalle se encuentra que en este mensaje se envió una imagen de tipo *jpg,* como se muestra a continuación:

OK dejarme trabajar un poco el phi...	1320877629642	NULL
/9j/4AAQSkZJRgABAQAAAQABAA...	1324941656700	https://mms301.whatsapp.net/d8/26/15/e/1/e184d7ae1b7ab6bf9a74417569612613.jpg
que es esto?	1324941786404	NULL

Imagen 98. Detección como imagen .jpg

Investigando el uso del protocolo de *Whatsapp* se encontró que el envío de imágenes se realiza transformándolas a código en base 64, lo que quiere decir que cualquier navegador actualizado podrá reconstruir el código concatenándolo de la siguiente forma:

*****segmento_de_codigo_base64.*

Se procede a realizar el proceso sintáctico que permita la decodificación de la imagen.

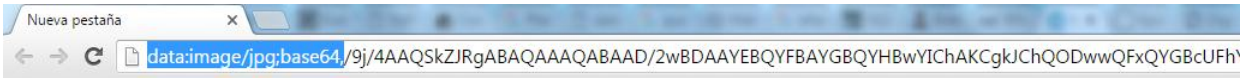


Imagen 99. Técnica de decodificación base 64.

Por medio del navegador *Chrome* se obtuvo la siguiente imagen:

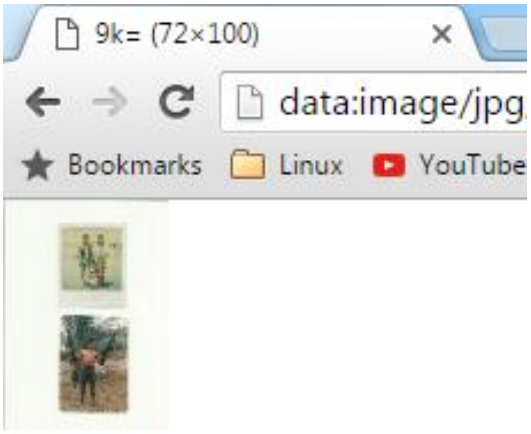


Imagen 100. Imagen obtenida de código base64.

Se percibe una imagen de dos niños y una persona con dos armas. Se descarta como evidencia.

En la prueba ***5.3.4 Dispositivos USB conectados*** se obtuvo un listado de cinco dispositivos USB conectados recientemente al equipo ANN-PC, se decide montar la imagen de memoria USB como un dispositivo mas del equipo forense, en modo de solo lectura.

Por medio del caso creado en OSForensics se monta la imagen como unidad ***U:***

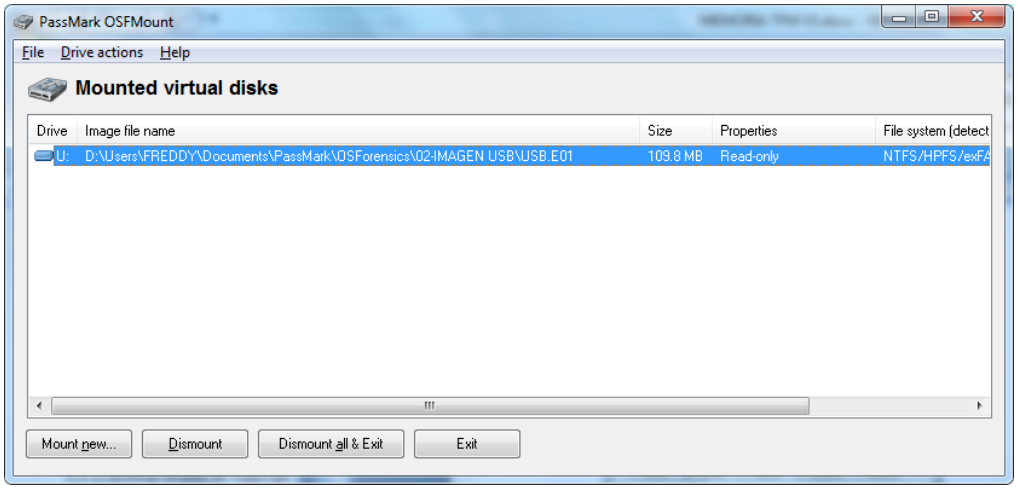


Imagen 101. Montaje de imagen USB con OSForensics.

El sistema operativo reconoce automaticamente un nuevo volumen U:

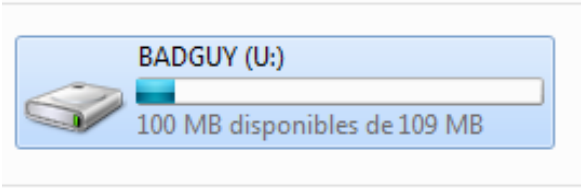


Imagen 102. USB montada.

Se observa que el nombre pre-configurado por el propietario para este dispositivo es **BADGUY.**

Con esta información se realiza una búsqueda dentro de los dispositivos de tipo USB conectados con el equipo ANN-PC.

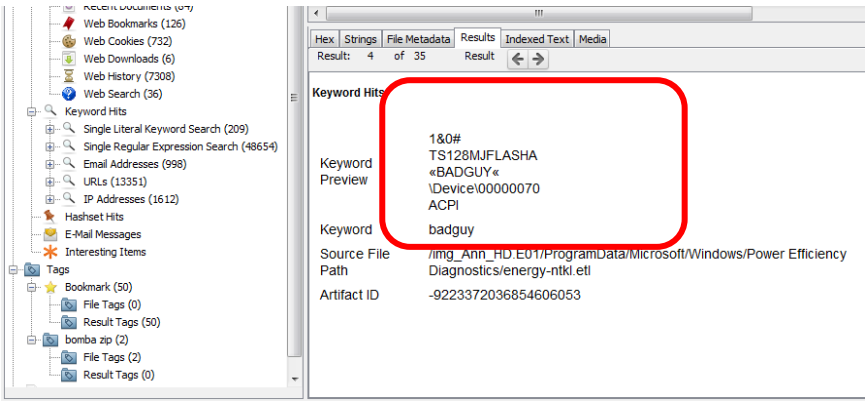


Imagen 103. Rastros de conexión de USB badguy en ANN-PC.

El uso de este dispositivo USB de serial TS128MJFLASHA establece un enlace entre la información allí almacenada y la información en el equipo ANN-PC.

6.4.3.2 Correlación y trazabilidad semántica.

Las siguientes premisas describen la conexión entre los datos:

a. En la exploración de la evidencia **U4** se determina que este archivo es un historial de conversaciones realizadas a través de la aplicación *Whatsapp.*
b. se encontraron varias conversaciones. Se destaca la conversación sostenida mediante un chat grupal entre *Raul, Ivan* y *Carlos.*
c. Por la correlación de los mensajes y sentido de las actividades que en ellas se asignan a los participantes, se deduce que el usuario de *Raul* es el 34635293190@s.whatsapp.net.
d. El usuario de *Ivan* es 34660401445@s.whatsapp.net.
e. El usuario que al parecer es el propietario de la cuenta a la cual pertenece el historial de mensajes se llama *Carlos,* sin embargo su número de cuenta no es deducible, ya que el remitente de los mensajes aparece como *NULL* en los registros:

remote_resource	received_timestamp	send_timestamp	receipt_server_t
Filter	Filter	Filter	Filter
34660401445@s.whatsapp.net	1320877151801	-1	-1
NULL	1320877206304	-1	1320877206964
34635293190@s.whatsapp.net	1320877208835	-1	-1
34635293190@s.whatsapp.net	1320877216819	-1	-1
34635293190@s.whatsapp.net	1320877222764	-1	-1
34660401445@s.whatsapp.net	1320877231683	-1	-1
34635293190@s.whatsapp.net	1320877234044	-1	-1
NULL	1320877434991	-1	1320877435647
NULL	1320877629652	-1	1320877630291
NULL	1324941656753	-1	1324941659705
34635293190@s.whatsapp.net	1324941786460	-1	-1
NULL	1324941819699	-1	1324941820319
NULL	1324941822590	-1	1324941823295
34660401445@s.whatsapp.net	1324941834145	-1	-1
34635293190@s.whatsapp.net	1324941835674	-1	-1

Tabla 104. Mensajes con remitente NULL.

f. En la conversación entre *Raul, Ivan* y *el Remitente* se describe un plan para obtener tarjetas con las cuales se puedan realizar compras por internet con un DNI falso y posteriormente enviarlas a un piso falso.
g. *El Remitente* menciona la técnica de *Phishing* como medio para conseguir las tarjetas, esta técnica es de uso común para el robo de datos bancarios.
h. En un mensaje el lunes, 26 diciembre de 2011 23:23:39.691 GMT *El Remitente* confirma el éxito del plan para conseguir de manera fraudulenta los números y pines de las tarjetas.
i. La información de las tarjetas obtenidas es enviada a *Raul* quien sería el encargado de realizar las compras.
j. El miércoles, 15 febrero 2012 22:31:57.691 GMT *Raul* manifiesta a sus cómplices que fue visitado por la policía.
k. En este punto de la exploración se encuentra información puntual de la planificación de actividades para lo obtención de tarjetas utilizando conocidas técnicas fraudulentas, falsificación de documento y suplantación de identidad.

6.4.3.3 Selección de evidencia digital.

Se selecciona la evidencia digital que ha sido correlacionada y aporta relevancia y suficiencia a la investigación o sirve como soporte de trazabilidad.

Etiqueta	Nombre	Obtenido en prueba	Clasificación
U4	whatsapp_castellano.db	3.3.3	A11

Tabla 51. Evidencia digital Whatsapp.

6.4.4 Infección de Malware.

6.4.4.1 Procedimiento.

El objetivo de la exploración de estos archivos es identificar si la posible ejecución e infección al equipo ANN-PC pudo tener incidencia en el almacenamiento de las evidencias digitales que han sido encontradas en este equipo.

En este punto se han reconocido cuatro archivos como Malware durante el transcurso de la ejecución de pruebas y exploración de evidencias.

Se parte de los archivos etiquetados como **D10**, **D11**, **D12** y **E7.**

Se procede a verificar cada archivo en la página https://www.virustotal.com.

A continuación se muestra el resultado de cada uno:

Malware yUmikJMYd3b.exe:

Estado malicioso:	Confirmado.
Tipo:	Troyano.
Categoría:	*Trojan.MSIL.Injector.LVE*

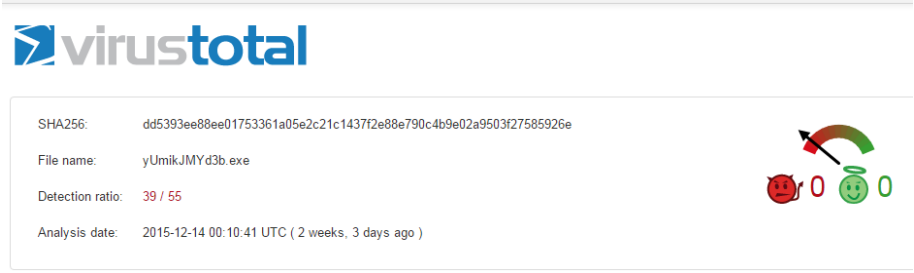


Imagen 105. Detección de yUmikJMYd3b.exe en virus total.

Características generales de operación:

- Utiliza técnicas avanzadas de ocultamiento.
- Reúne detalles del funcionamiento y características del sistema operativo infectado.
- Sirve de plataforma de funcionamiento para otros malware's.
- Su principal objetivo es el robo de información financiera.
- Por medio de la plataforma web http://anubis.iseclab.org/ se identifico la relación de este archivo con el archivo TheJerm.rar.

Imagen 106. Detección de yUmikJMYd3b.exe en Anubis.

- El análisis por medio de Anubis muestra que la ejecución del archivo *yUmikJMYd3b.exe* genera un ejecutable de nombre *TheJermCZ.exe.*

Se decide explorar con más detalle el archivo por medio de la plataforma https://www.hybrid-analysis.com/.

Evaluación de riesgo:

- Contiene un modulo de escritorio remoto.
- Realiza lecturas inusuales del Identificador Único Global de la maquina (GUID).
- Lee el nombre del equipo
- Contacta una dirección IP en **Albania.**

Imagen 107. Enlace realizado por el malware

- El malware estableció un enlace con la IP 31.44.70.40 por el puerto 1607 de tipo TCP en Albania
- La cadena de ejecución del malware muestra que después de ejecutado el ***yUmikJMYd3b.exe***, se cargaron dos ejecutables mas, como son el archivo ***ThejermCZ.exe***, el proceso ***svchost.exe,*** y finalmente ejecuta la aplicación de Windows ***notepad.exe.***

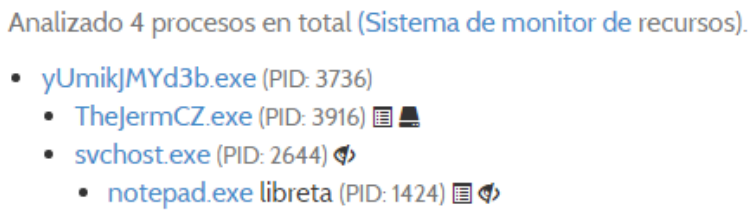
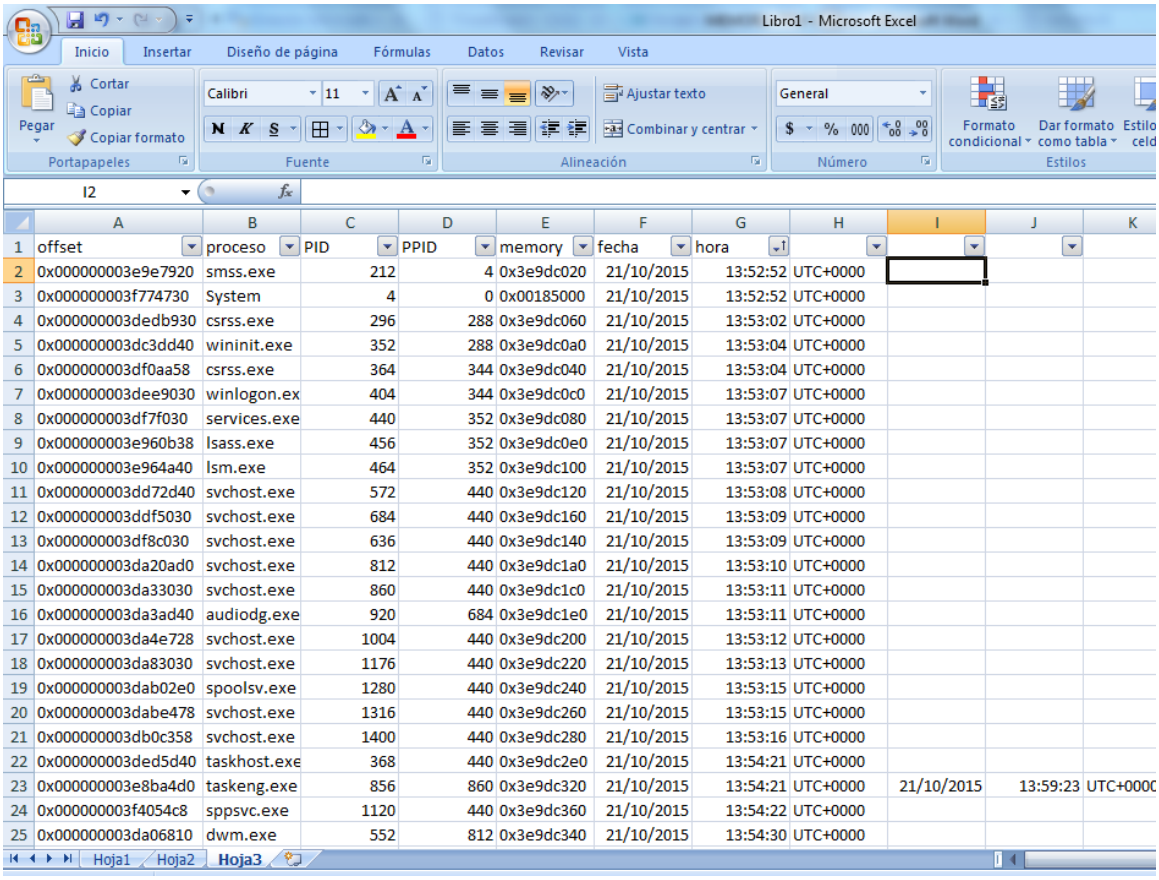


Imagen 108. Cadena de ejecución de yUmikJMYd3b.exe.

Después de obtener datos relevantes de la ejecución del malware se procede a revisar rastros de su ejecución en el equipo ANN-PC, el artefacto candidato para esta revisión es la muestra de procesos en ejecución tomada en la prueba ***4.3.3 Búsqueda de procesos ejecutados en el sistema*** y etiquetadas como **R3** y **R4.**

Se procede a ordenar el listado de procesos en forma ascendente en cuanto a su hora de ejecución:



	A	B	C	D	E	F	G	H	I	J	K
1	offset	proceso	PID	PPID	memory	fecha	hora				
2	0x000000003e9e7920	smss.exe	212	4	0x3e9dc020	21/10/2015	13:52:52	UTC+0000			
3	0x000000003f774730	System	4	0	0x00185000	21/10/2015	13:52:52	UTC+0000			
4	0x000000003dedb930	csrss.exe	296	288	0x3e9dc060	21/10/2015	13:53:02	UTC+0000			
5	0x000000003dc3dd40	wininit.exe	352	288	0x3e9dc0a0	21/10/2015	13:53:04	UTC+0000			
6	0x000000003df0aa58	csrss.exe	364	344	0x3e9dc040	21/10/2015	13:53:04	UTC+0000			
7	0x000000003dee9030	winlogon.ex	404	344	0x3e9dc0c0	21/10/2015	13:53:07	UTC+0000			
8	0x000000003df7f030	services.exe	440	352	0x3e9dc080	21/10/2015	13:53:07	UTC+0000			
9	0x000000003e960b38	lsass.exe	456	352	0x3e9dc0e0	21/10/2015	13:53:07	UTC+0000			
10	0x000000003e964a40	lsm.exe	464	352	0x3e9dc100	21/10/2015	13:53:07	UTC+0000			
11	0x000000003dd72d40	svchost.exe	572	440	0x3e9dc120	21/10/2015	13:53:08	UTC+0000			
12	0x000000003ddf5030	svchost.exe	684	440	0x3e9dc160	21/10/2015	13:53:09	UTC+0000			
13	0x000000003df8c030	svchost.exe	636	440	0x3e9dc140	21/10/2015	13:53:09	UTC+0000			
14	0x000000003da20ad0	svchost.exe	812	440	0x3e9dc1a0	21/10/2015	13:53:10	UTC+0000			
15	0x000000003da33030	svchost.exe	860	440	0x3e9dc1c0	21/10/2015	13:53:11	UTC+0000			
16	0x000000003da3ad40	audiodg.exe	920	684	0x3e9dc1e0	21/10/2015	13:53:11	UTC+0000			
17	0x000000003da4e728	svchost.exe	1004	440	0x3e9dc200	21/10/2015	13:53:12	UTC+0000			
18	0x000000003da83030	svchost.exe	1176	440	0x3e9dc220	21/10/2015	13:53:13	UTC+0000			
19	0x000000003dab02e0	spoolsv.exe	1280	440	0x3e9dc240	21/10/2015	13:53:15	UTC+0000			
20	0x000000003dabe478	svchost.exe	1316	440	0x3e9dc260	21/10/2015	13:53:15	UTC+0000			
21	0x000000003db0c358	svchost.exe	1400	440	0x3e9dc280	21/10/2015	13:53:16	UTC+0000			
22	0x000000003ded5d40	taskhost.exe	368	440	0x3e9dc2e0	21/10/2015	13:54:21	UTC+0000			
23	0x000000003e8ba4d0	taskeng.exe	856	860	0x3e9dc320	21/10/2015	13:54:21	UTC+0000	21/10/2015	13:59:23	UTC+0000
24	0x000000003f4054c8	sppsvc.exe	1120	440	0x3e9dc360	21/10/2015	13:54:22	UTC+0000			
25	0x000000003da06810	dwm.exe	552	812	0x3e9dc340	21/10/2015	13:54:30	UTC+0000			

Imagen 109. Procesos ordenados cronológicamente.

Se inicia la búsqueda de los procesos implicados en la ejecución del malware.

26	0x000000003e9c4518	explorer.exe	692	240	0x3e9dc180	21/10/2015	13:54:30	UTC+0000
27	0x000000003dd73030	yUmikJMYd3b.ex	1776	692	0x3e9dc3c0	21/10/2015	13:54:32	UTC+0000
28	0x000000003dfbc770	Skype.exe	1980	692	0x3e9dc380	21/10/2015	13:54:32	UTC+0000
29	0x000000003f4d0d40	SearchIndexer.	1124	440	0x3e9dc2c0	21/10/2015	13:54:39	UTC+0000
30	0x000000003f4c06d0	wmpnetwk.exe	964	440	0x3e9dc400	21/10/2015	13:54:44	UTC+0000
31	0x000000003f4ccd40	WinHex.exe	512	692	0x3e9dc420	21/10/2015	13:54:46	UTC+0000
32	0x000000003f4c2938	TrueCrypt.exe	2244	692	0x3e9dc480	21/10/2015	13:55:00	UTC+0000
33	0x000000003f430d40	svchost.exe	2336	1776	0x3e9dc300	21/10/2015	13:55:06	UTC+0000
34	0x000000003f4b2d40	notepad.exe	2396	2336	0x3e9dc3e0	21/10/2015	13:55:07	UTC+0000
35	0x000000003f5acd40	svchost.exe	2840	440	0x3e9dc500	21/10/2015	13:55:20	UTC+0000

Imagen 110. Ejecución de malware en memoria RAM detectado.

En la línea 27 se observa el proceso ***yUmikJMYd3b.ex*** ejecutado el 21/10/2015 a las 13:54:32 UTC+0000 con ID **1776,** este proceso generó un proceso "hijo" en la línea 33 de nombre ***svchost.exe*** con ID **2336**, En la línea 34 se observa que el proceso 2336 generó un proceso "hijo", en este caso la aplicación de Windows ***notepad.exe*** el mismo día a las13:55:07 UTC+0000.

Se realiza una búsqueda con base en la fecha, hora y tipo de archivo (texto plano) que coincida con la generación, modificación o acceso de un archivo de *notepad*.

Se encontró el archivo con nombre ***2015-10-21-4.dc*** el cual fue modificado por última vez el 2015-10-21 a las 08:55:23 COT, teniendo en cuenta que COT tiene -5:00 horas de diferencia, se calcula que las fechas concuerdan por una diferencia de segundos, segundos que se entienden transcurrieron desde la ejecución del proceso y la actualización del archivo.

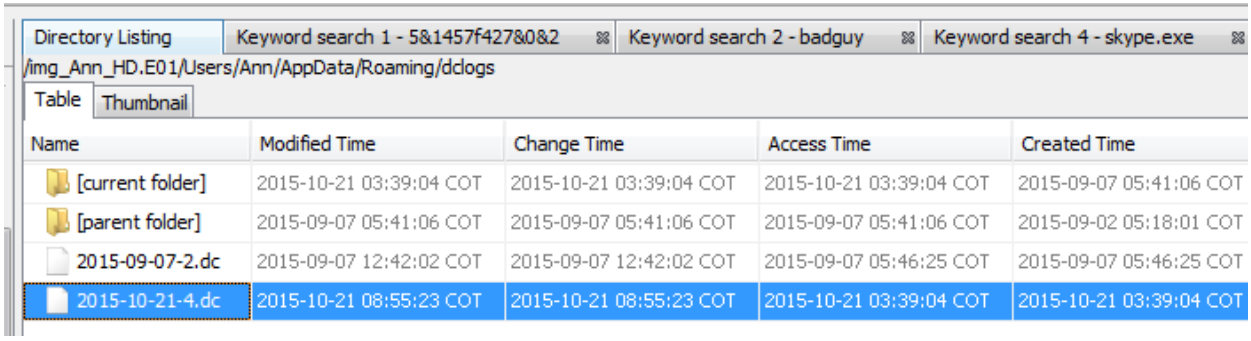


Imagen 111. Archivo generado por el malware.

El contenido de este archivo genera sospecha al observase que tiene el mismo formato del archivo ***2015-09-07-2.dc*** el cual había sido obtenido anteriormente en las pruebas realizadas en el numeral ***5.3.15 Búsqueda de palabra clave "Password"***, en el que ya se había advertido el formato extraño en el que estaban estructurados los password allí encontrados.

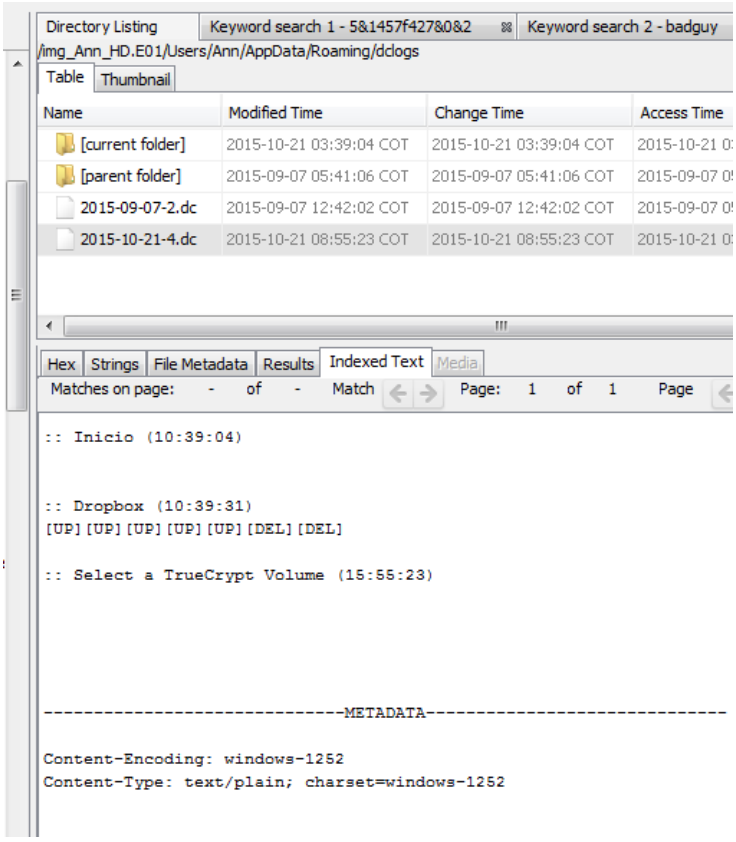


Imagen 112. Contenido de archivo generado por el malware.

Aumenta la sospecha el hecho de que estos dos archivos, el ***2015-10-21-4.dc*** y el ***2015-09-07-2.dc,*** tienen en común el mismo formato interno, el mismo formato en el nombre, la misma extensión (.dc) y están guardados en el mismo directorio, en la ruta ***/img_Ann_HD.E01/Users/Ann/AppData/Roaming/dclogs/***

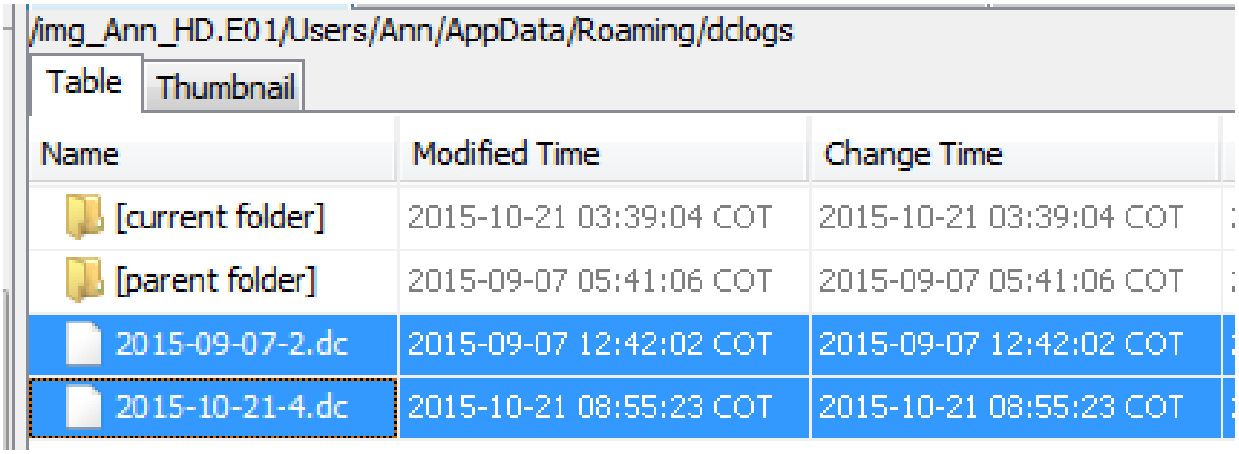


Imagen 113. Coincidencia de archivos.

Se deduce que estos archivos hacen parte de la intersección y registro de credenciales del equipo ANN-PC, técnica conocida como ***KeyLoger,*** generada por la ejecución del malware ***yUmikJMYd3b.exe.***

Malware TheJerm.rar:

Estado malicioso:	Confirmado.
Tipo:	Troyano.
Categoría:	*Trojan.MSIL.Injector.LVE*

Características generales de operación:

- Este archivo es detectado como otra versión del malware *yUmikJMYd3b.exe*.
- Las características de operación de este malware son similares a la del malware anterior.
- Permite acceso remoto.
- Genera puertas traseras para gestión de otros malware.

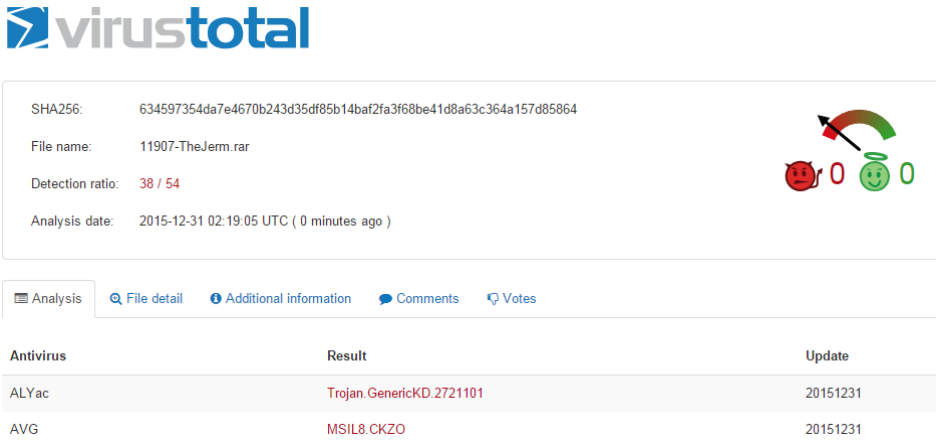


Imagen 114. Detección de TheJerm.rar por virustotal.

- Posee capacidad de espionaje e interceptación de caracteres.

La exploración por medio de la plataforma https://www.hybrid-analysis.com/ muestra algunos archivos generados en la ejecución de este malware:

- Se genera el ejecutable ***TheJrmCZ.exe.***

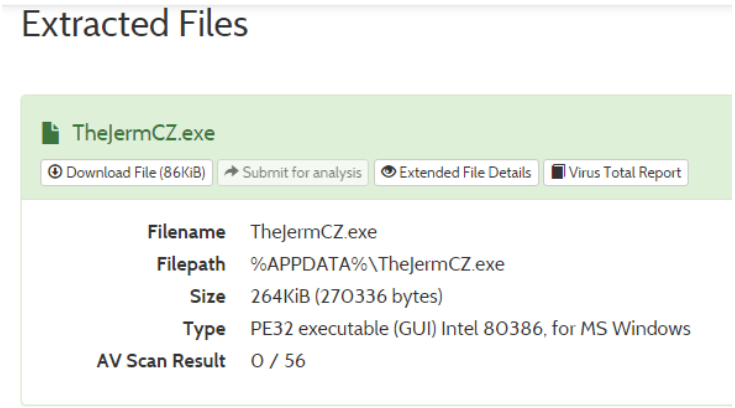


Imagen 115. Archivo 1 generado por TheJerm.rar.

- Se generó el archivo ***2016-01-01.dc***

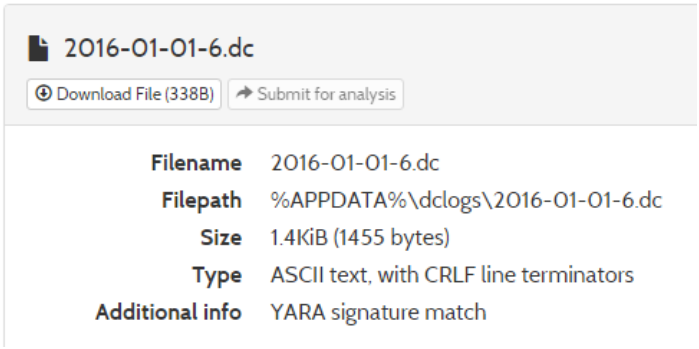


Imagen 116. Archivo 2 generado por TheJerm.rar.

- Se confirmó, con la generación de este archivo, el origen del archivo encontrado con Password's en la prueba del numeral 5.3.15.

Malware excel_server.exe:

Estado malicioso:	Confirmado.
Tipo:	BackDoor.
Categoría:	*Backdoor.Win32.Poison.aec*

Características generales de operación:

- Posee capacidad para generar accesos remotos en el equipo infectado.
- Capacidad de recolección y robo de información a través de conexiones remotas.
- Disminuye altamente el rendimiento y capacidad de procesamiento del equipo infectado.

Se procede a explorar este malware en la plataforma http://anubis.iseclab.org/.

- La plataforma muestra la cadena de ejecución del malware.

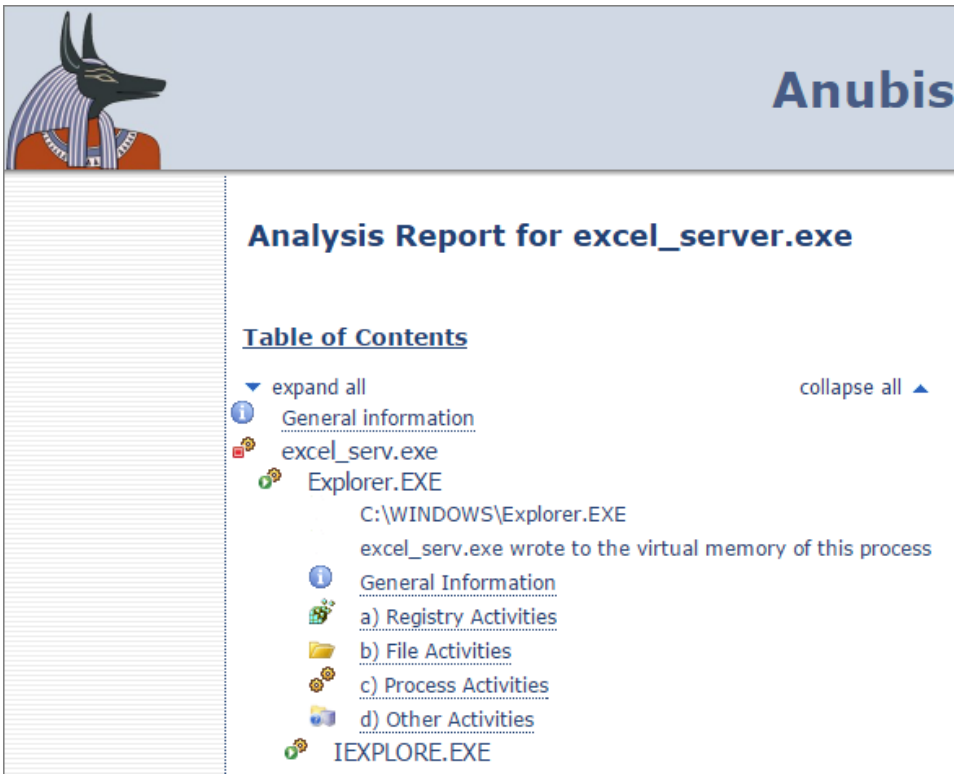


Imagen 117. Detección de excel_server.exe en Anubis.

- Se observa la ejecución del proceso ***Explorer.EXE*** y el proceso ***IEXPLORE.EXE***.
- Se buscó rastros de ejecución de estos procesos mediante las evidencias **R3** y **R4**, el resultado ha sido negativo, no se evidenciaron rastros concretos de la ejecución del malware durante la toma de la imagen de memoria RAM.

- La exploración mediante la plataforma https://www.hybrid-analysis.com/ no ha mostrado detalles adicionales relevantes de este malware.

Malware LlistatNumeracions.exe:

Estado malicioso:	Confirmado.
Tipo:	Troyano.
Categoría:	*Trojan.Downloader.Agent*

Imagen 118. Detección de LlistatNumeracions.exe en virustotal.

Características generales de operación:

- La principal característica de este archivo es la capacidad de descarga de otros archivos maliciosos.

Se procede a explorar este malware en la plataforma http://anubis.iseclab.org/.

- La plataforma muestra la cadena de ejecución del malware.

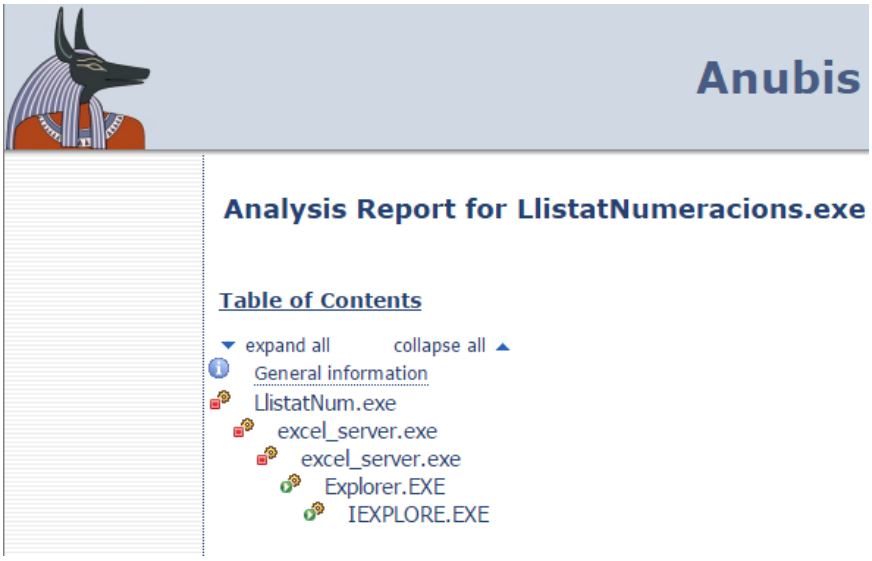


Imagen 119. Detección LlistatNumeracions.exe en Anubis.

- Se encuentra que este malware tiene una relación con el malware ***excel_server.exe*** explorado anteriormente.
- Según la secuencia de ejecución, el malware ***LlistatNumeracions.exe*** genera un proceso llamado ***LlistatNum.exe:***

Imagen 120. Secuencia de ejecución de LlistatNumeracions.exe.

- El proceso ***LlistatNum.exe*** genera el malware ***excel_server.exe*** en la ruta C:\Extracted\excel_server.exe. Esta ruta concuerda exactamente con la ruta en la que fue hallado el malware ***excel_server.exe*** durante la prueba del numeral ***5.3.14 Búsqueda de malware.***

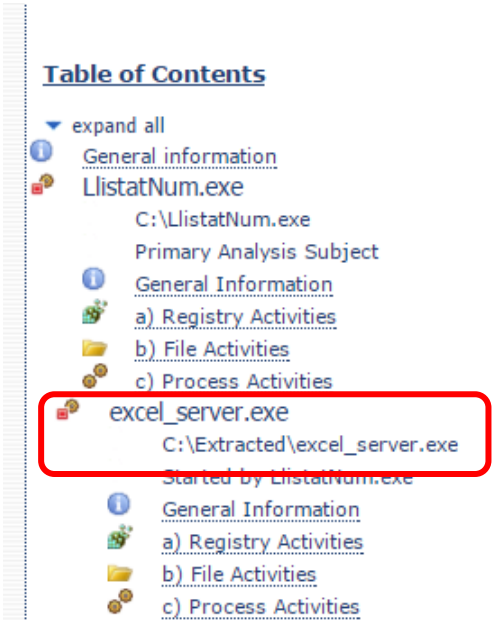


Imagen 121. Segundo paso de la ejecución de LlistatNumeracions.exe.

- El proceso ***excel_server.exe*** es iniciado posteriormente:

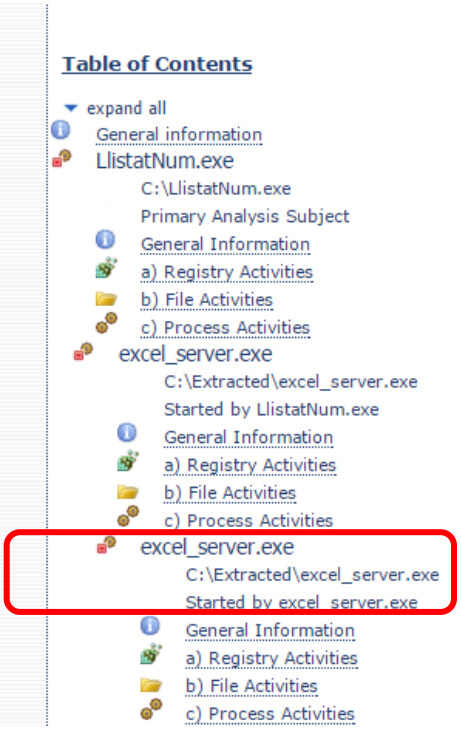


Imagen 122. Tercer paso de ejecución de LlistatNumeracions.exe.

- Después de la ejecución el proceso ***excel_server.exe*** inicia un proceso ***Explorer.EXE*** y este inicia otro llamado ***IEXPLORE.EXE***

Imagen 123. Ejecución final de LlistatNumeracions.exe.

- En este punto se ha obtenido muestras del plan de ejecución del malware.

Se procede a realizar la exploración mediante la plataforma https://www.hybrid-analysis.com/.

Evaluación de riesgo:

- Realiza lecturas inusuales del Identificador Único Global de la maquina (GUID).
- Envía datos a procesos remotos.
- Consulta información sensible de las configuraciones de seguridad.
- Genera archivos ejecutables.
- Asigna memoria virtual a procesos desconocidos.
- Modifica configuraciones de proxy.
- En la sección de archivos extraídos por la ejecución del malware se evidencian los siguientes archivos generados:

  Plantilla_despeses.xls:

  La exploración dentro de esta plataforma ha mostrado un archivo que no había sido detectado en la plataforma de Anubis, un archivo del programa Excel que almacena en la ruta ***C:\Extracted\Plantilla_despeses.xls.***

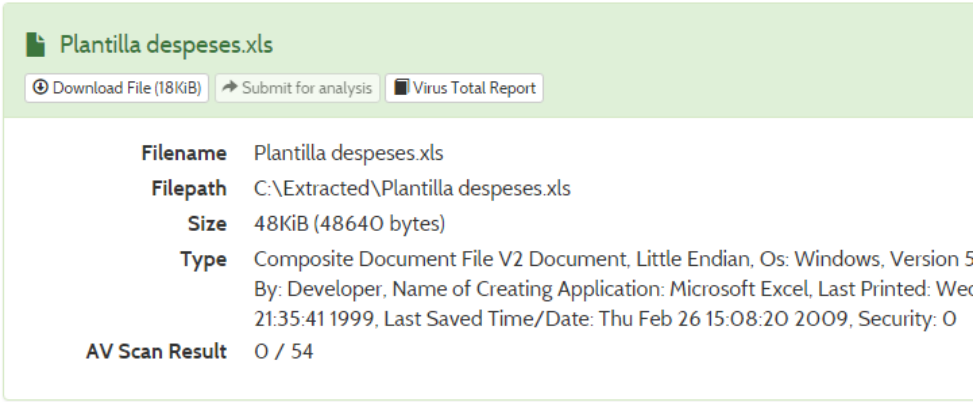


Imagen 124. Archivo 1 generado por LlistatNumeracions.exe.

Este archivo no ha sido catalogado como malicioso, la ejecución dentro del ***sandbox*** de la plataforma muestra la siguiente imagen como resultado.

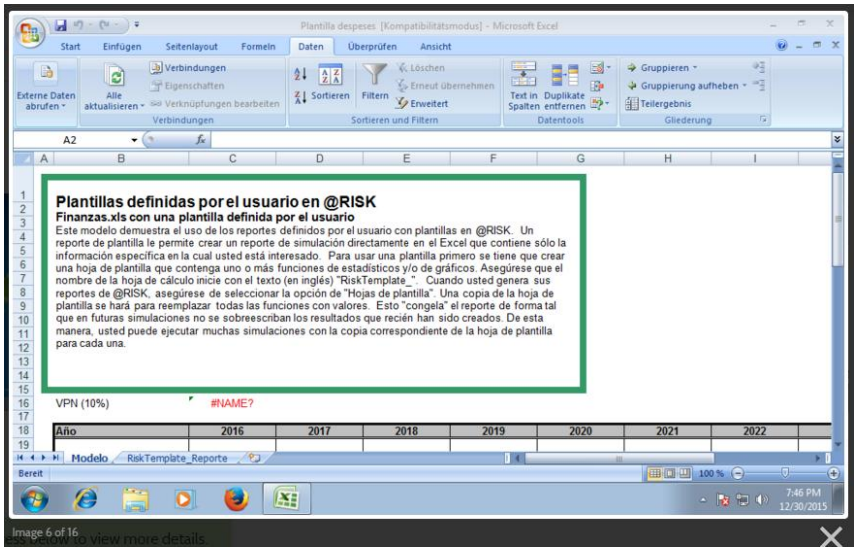


Imagen 125. Contenido de archivo 1 generado por LlistatNumeracions.exe.

Excel_server.exe:

Se confirma la generación de este archivo en la misma ruta, como se había observado en la exploración con Anubis.

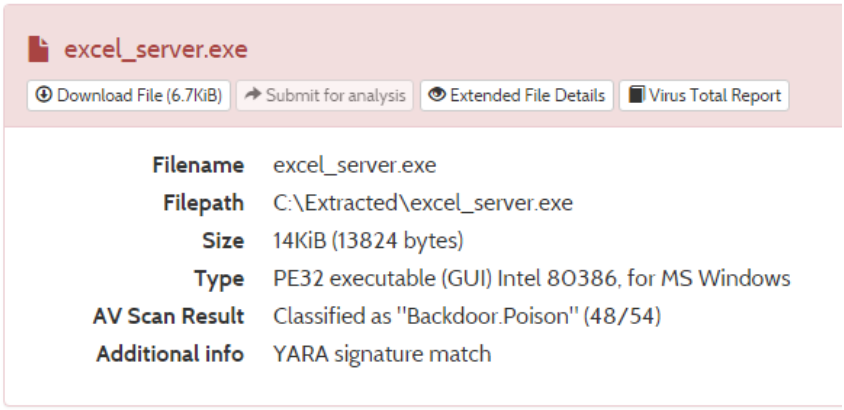


Imagen 126. Archivo 2 generado por LlistatNumeracions.exe.

Mediante la exploración de este malware se ha obtenido información sobre dos archivos generados después de su ejecución, uno de estos archivos ya ha sido localizado dentro de la imagen como lo es el mismo malware ***excel_server.exe*** ya explorado.

Se procede a realizar la búsqueda del archivo ***Plantilla_despeses.xls*** en la ruta ***C:\Extracted***.

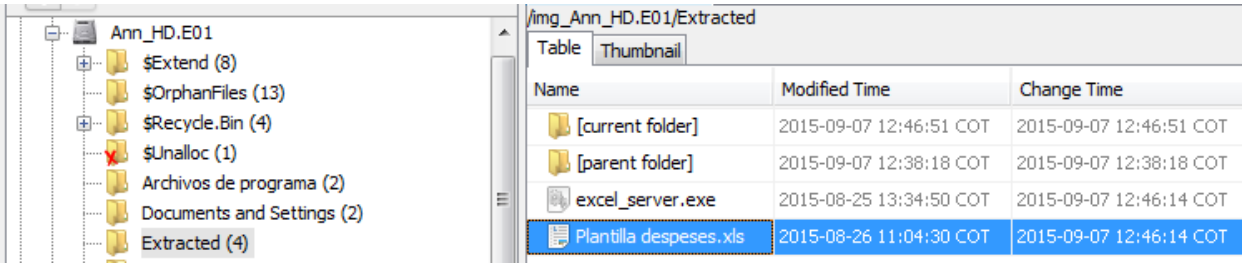


Imagen 127. Prueba de ejecución del malware.

Se ha detectado el archivo buscado, se procede a exportar para su revisión:

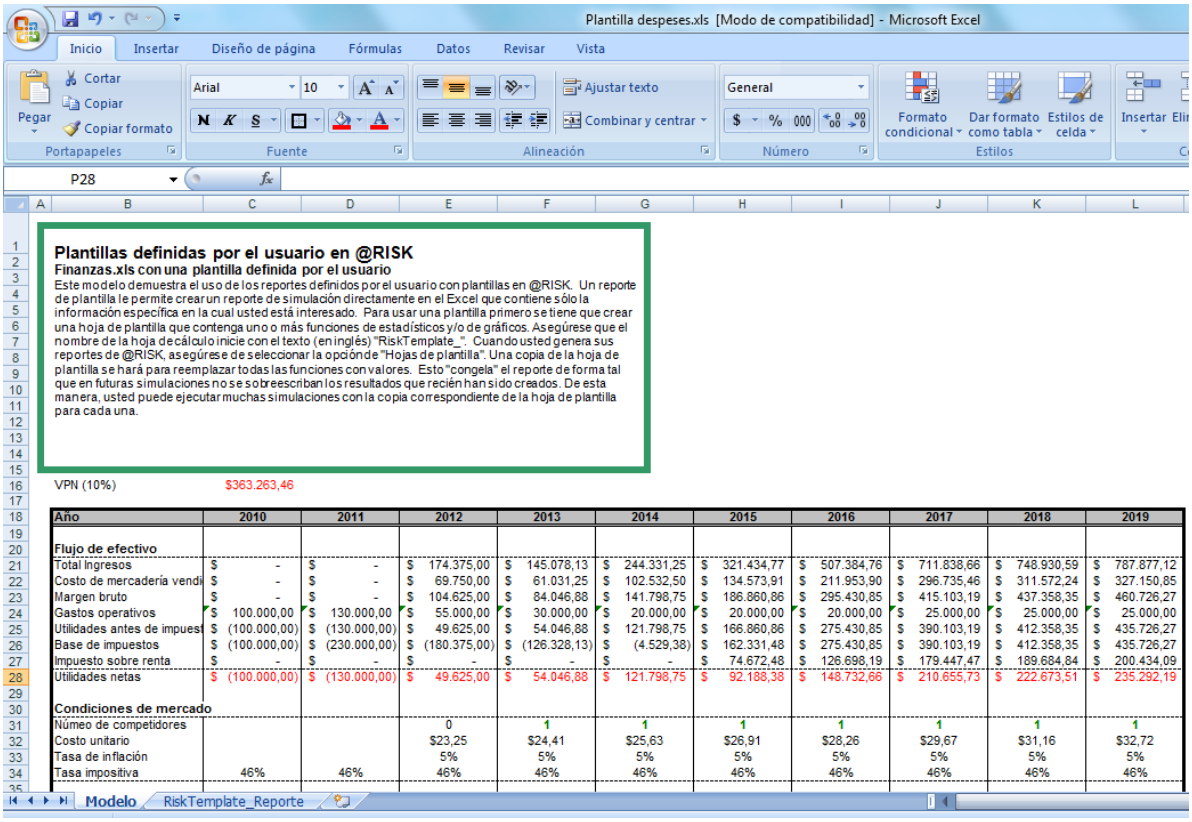


Imagen 128. Contenido de archivo Plantilla_despeses.xls encontrado en ANN-PC.

El contenido del archivo parece ser datos financieros periódicos. No se percibe claridad o significado en esta información.

6.4.4.2 Correlación y trazabilidad semántica

En este punto es importante conocer el detalle cronológico de cada archivo para obtener alguna relación con evidencias obtenidas en puntos anteriores de la exploración.

Utilizando el modulo de ordenamiento cronológico que brinda la herramienta ***Autopsy*** y a través del caso creado anteriormente procedemos a realizar una exploración de los eventos en los que intervino cada uno de estos archivos.

yUmikJMYd3b.exe:

- Se encontraron dos días en los que se registra actividad de este archivo, el 07-09-2015 y el 21-10-2015.

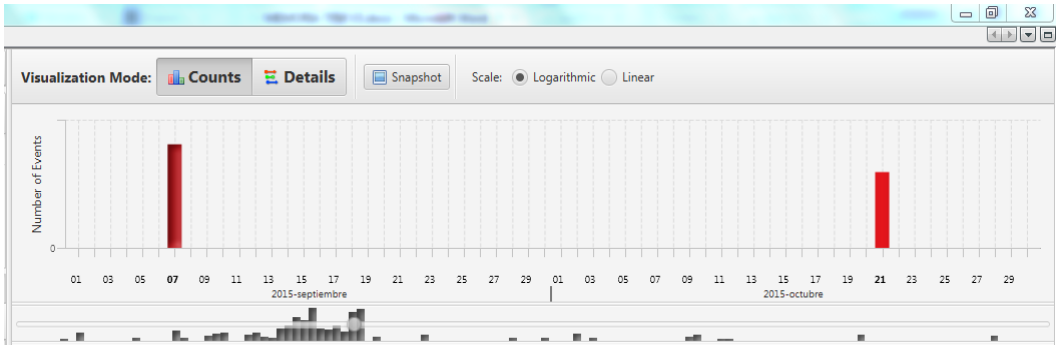


Imagen 129. Actividades de yUmikJMYd3b.exe en ANN-PC.

- La creación del archivo en el equipo aparece registrada en la fecha del 2015-09-07 a las 10:40:55 GMT

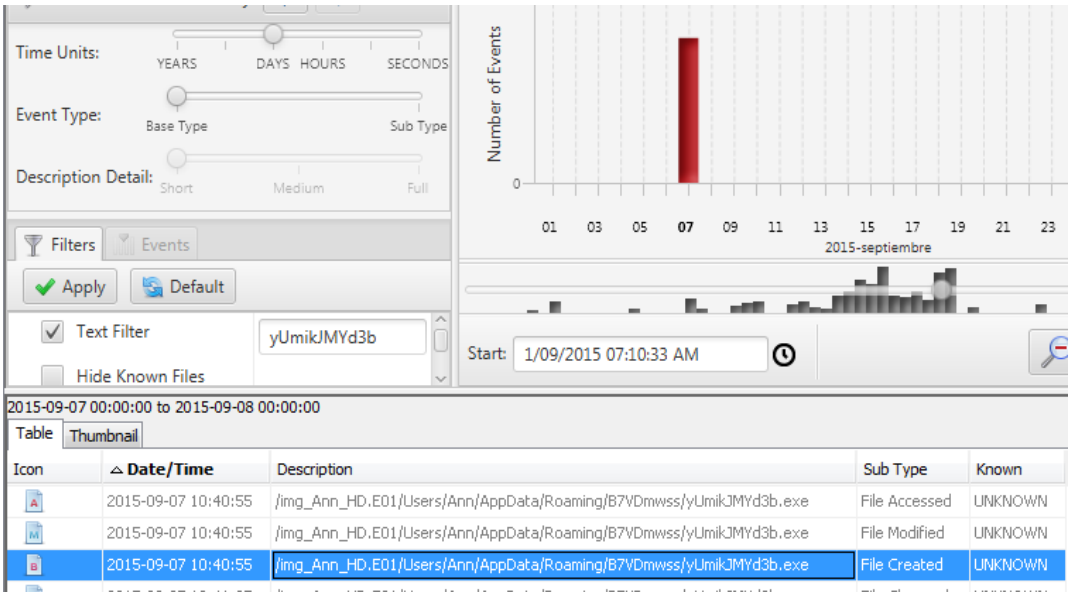


Imagen 130. Actividad en septiembre de yUmikJMYd3b.exe en ANN-PC.

- se ejecutó a las 10:41:05 del mismo día, produciéndose la infección por medio de un enlace que se ejecutaría desde ese momento en cada inicio de Windows.

- El 21 de octubre de 2015 se cargo el malware durante el inicio de sesión de la cuenta ***Ann*** a las 13:55:06 GMT.

TheJerm.rar:

Sobre este malware el modulo de relación cronológica nos muestra lo siguiente:

- Desde la cuenta de usuario ***Ann*** se inicio un proceso de descarga desde la dirección web ***https://www.youtube.com/watch?v=CzSovVUccCY*****,** a las 10:33:51 GMT del 07-09-2015.

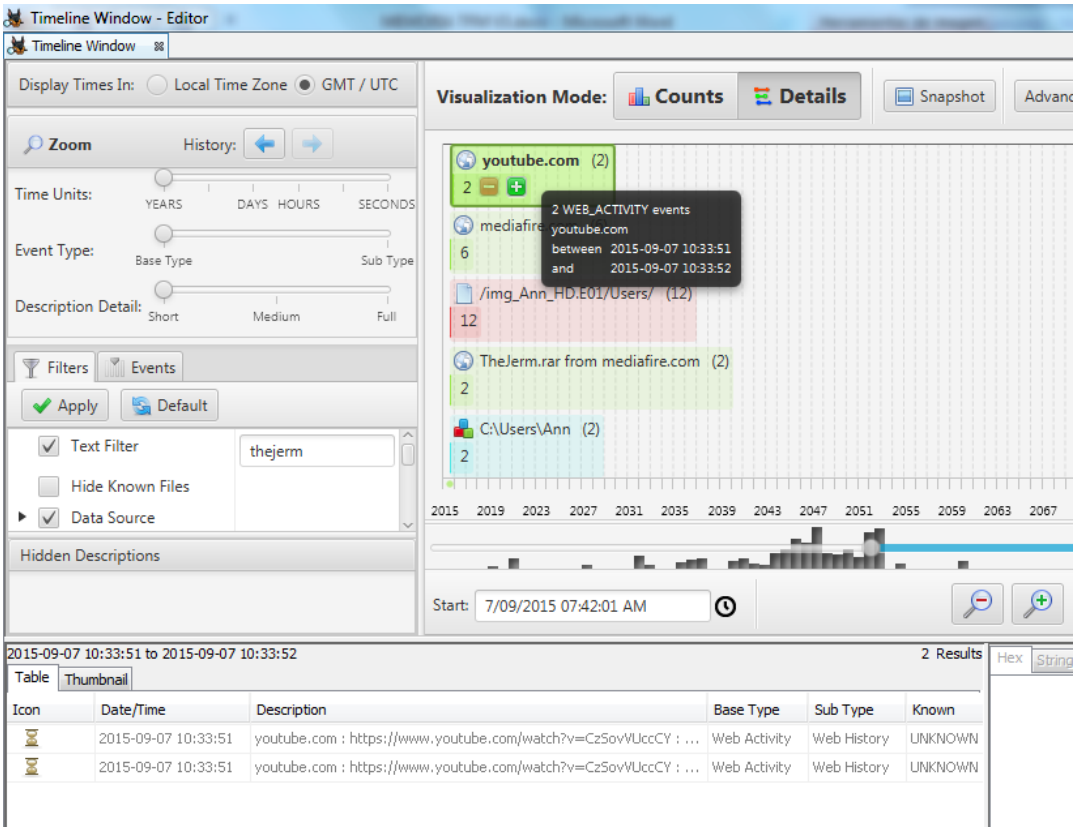


Imagen 131. Actividades de TheJerm.rar en ANN-PC.

- Esta dirección web conduce a un video llamado ***"MSR 206 Software Manual + Free Download Link , Thejerm Software Original",*** donde se muestra el procedimiento con algunas tarjetas.
- La descarga continuó desde la dirección web ***http://www.mediafire.com/download/z1x1b8vgqg7dst8/TheJerm.rar***

- Desde esta dirección se obtuvo el archivo, como se muestra en la secuencia, fue almacenado en el directorio de descargas del usuario ***Ann*** a las 10:35:17 GMT del 07-09-2015.

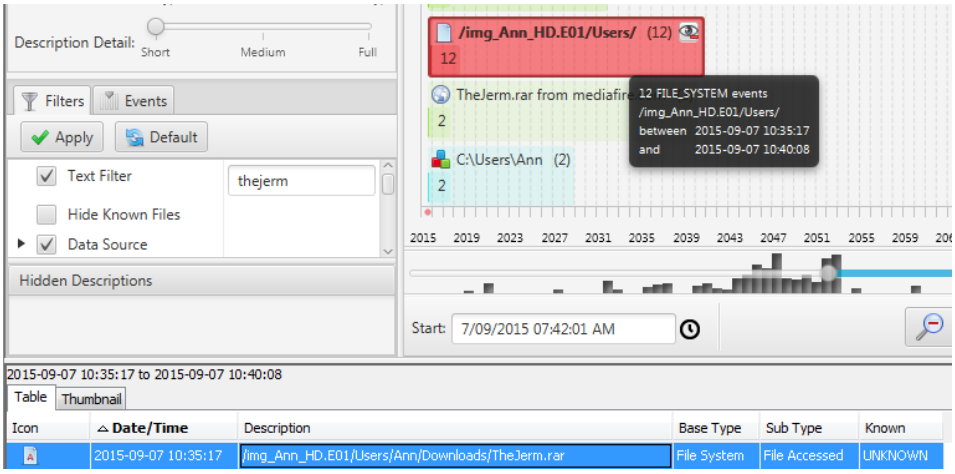


Imagen 132. Descarga de TheJerm.rar desde cuenta Ann.

LlistatNumeracions.exe

Se confirman los datos cronológicos obtenidos de este malware en la exploración realizada en el numeral ***6.4.2. Directorio de Skype.***

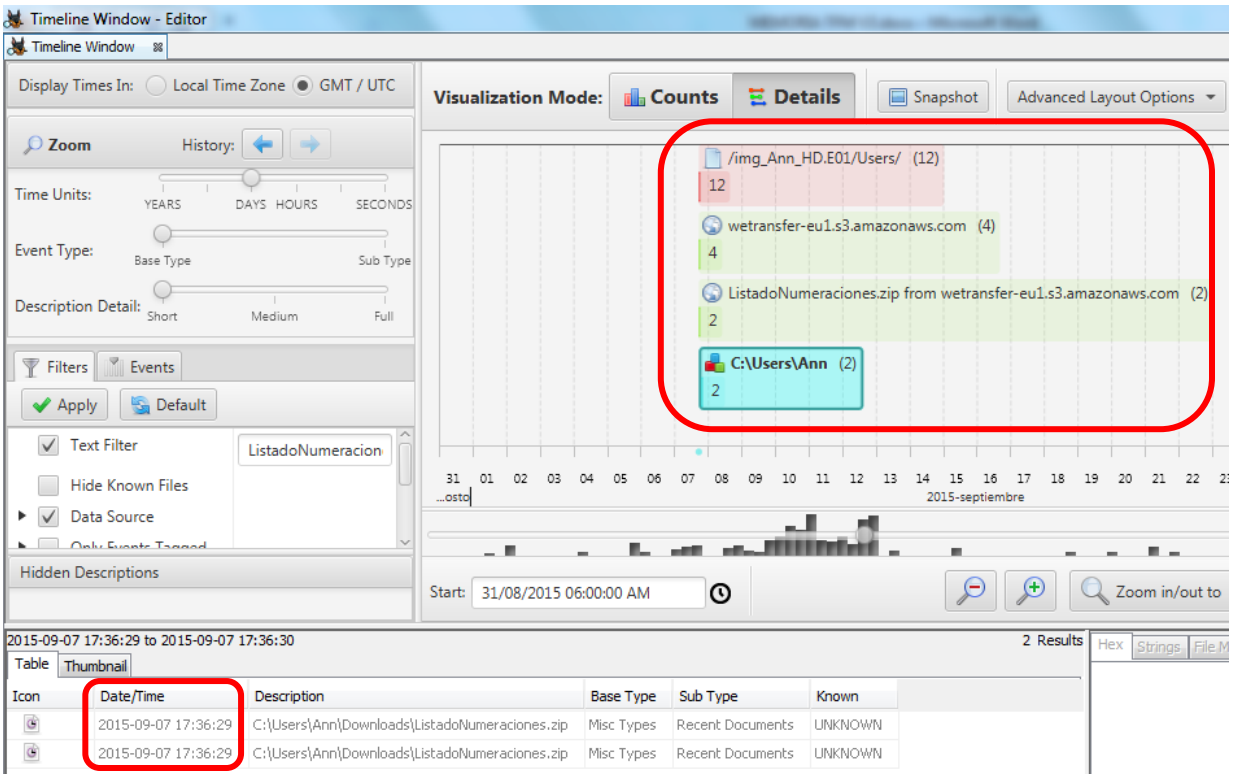


Imagen 133. Actividades de LlistatNumeracions.exe en ANN-PC.

excel_server.exe

Se encuentra registrada una fecha de creación de este fichero el 25-08-2015 a las 18:34:50 GMT, igualmente se registra actividad el 07-09-2015 a las 17:38:30 GMT.

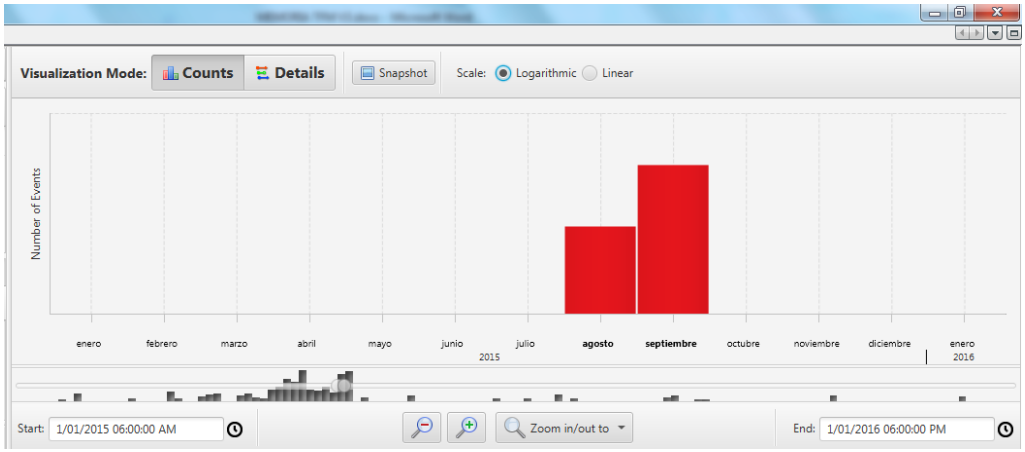


Imagen 134. Actividades de excel_server.exe en ANN-PC.

Después de obtener datos de ejecución en el tiempo del malware, se procede a resumir los detalles más importantes de la siguiente manera:

- La ocurrencia de eventos.

Secuencia	Fecha	Hora	Relación
1ª	25/08/2015	18:34:50	creación de excel_server.exe
2ª	07/09/2015	10:35:17	TheJerm descargado de youtube.
3ª	07/09/2015	10:40:55	Creación de yUmikJMYd3b.exe
4ª	07/09/2015	10:41:05	ejecución de yUmikJMYd3b.exe
5ª	07/09/2015	17:36:29	Descarga de LlistatNumeracions.exe referenciado por Skype
6ª	07/09/2015	17:38:30	inicio de ejecución excel_server.exe
7ª	07/09/2015	17:46:39	fin de ejecución excel_server.exe
8ª	21/10/2015	13:55:06	ejecución de yUmikJMYd3b.exe

Tabla 52. Secuencia eventos de malware.

- Se encontró evidencia de la ejecución e infección de malware dentro del equipo ANN-PC.
- El malware ***excel_server.exe*** se registra desde el mes de agosto sin pistas encontradas que permitan definir bajo qué circunstancias fue obtenido este archivo.

- Se detectó que fue ejecutado y ha generado el archivo ***Plantilla_despeses.xls*** encontrado en la ruta ***C: \Extracted***, esto demuestra su ejecución basado en la exploración mediante la plataforma https://www.hybrid-analysis.com/.
- El 7 de septiembre del 2015 desde la cuenta de usuario ***Ann*** se accedió a un video de *youtube* donde se aprecia la utilización del software ***Thejerm*** para la práctica conocida como *Skimming* o clonación de tarjetas.
- El usuario fue re-direccionado a otra página mediante la que se descargo el archivo ***TheJerm.rar,*** el archivo se almacenó en el equipo ANN-PC a las 10:35:17 GMT.
- El archivo ***excel_server.exe*** se ejecutó e infectó el equipo, fue esta infección la que generó el archivo etiquetado como **D13** de nombre ***2015-09-07-2.dc.***
- El archivo ***LlistatNumeracions.exe*** fue enviado por un contacto de Skype llamado Ricky el 07/09/2015 a las 17:36:29 GMT, se comprobó que la ejecución de este archivo genera otro ejecutable de nombre e***xcel_server.exe*** del cual también se comprobó su ejecución a las 17:38:30 GMT.
- El usuario de la cuenta Ann fue infectado mediante el archivo que su contacto le envió por Skype.
- Aunque el equipo fue infectado por diferente malware, no se detectan indicios de que hayan incidido en la creación de alguna de las evidencias obtenidas hasta este momento.

6.4.4.3 Selección de evidencia digital.

De esta exploración se selecciona los reportes que demuestran el carácter malicioso de los archivos, como soporte de este numeral.

CAPITULO 7. CONCLUSIONES.

A continuación se presentan las conclusiones clasificadas en dos formas, conclusiones técnicas y conclusiones generales, las conclusiones técnicas presentan al lector aquellas terminaciones obtenidas sobre el procedimiento e incidencias técnicas del análisis, las conclusiones generales le presentan al lector las terminaciones deducidas de las evidencias digitales puras.

7.1 Conclusiones Técnicas.

- Los datos encontrados han direccionado la etapa de análisis sobre los archivos procedentes de una cuenta en particular, la cuenta de usuario llamada Ann.

- La persona que administra la cuenta de usuario Ann posee un conocimiento técnico medio en el uso de tecnologías de información, este conocimiento le ha permitido tomar medidas de seguridad mediante el cifrado de la información y el uso de técnicas de esteganografía para aumentar la privacidad de sus archivos.

- Se comprobó una relación lógica entre la imagen de memoria USB y la imagen del disco duro por medio de archivos almacenados en ambos dispositivos con cierta información en común.

- Los datos obtenidos en el análisis de cada imagen por separado lograron ser confirmados y aplicados, siendo determinante su correlación en la selección de evidencias.

- El equipo ANN-PC ha sido infectado en diferentes ocasiones por distintos tipos de malware con un objetivo en común, robar información.

7.2 Conclusiones Generales.

- En el equipo ANN-PC y en el dispositivo USB se ha encontrado información financiera de un total de cuarenta personas diferentes con una estructura que permite identificar información suficiente y necesaria para realizar un fraude bancario electrónico por medio de transacciones no autorizadas.

- Se evidenció la conformación de una red de comunicación tecnológica entre personas identificadas como Anne G. H, Ricky Rodriguez, Aram B. V, Raul, Ivan y Carlos. Estas personas han utilizado diferentes programas de mensajería para planificar, coordinar y confirmar actividades tipificadas por la ley como fraude electrónico, falsificación de documentos, suplantación y robo de identidad.

- Sé identifica a una persona de nombre parcial Anne G. H. como la persona que administra la cuenta de usuario Ann del equipo llamado ANN-PC y que vive en castellar del vallés, Barcelona. Esta persona es responsable de llevar a cabo

procedimientos logísticos de cifrado y ocultamiento de datos bancarios para su almacenamiento, transferencia y posterior venta a terceros, de esta persona se ha evidenciado el interés por la adquisición de tecnologías de hardware y software, así como manuales utilizados para la clonación de tarjetas electrónicas.

- El equipo ANN-PC ha sido víctima de diversos ataques informáticos por medio de malware, el usuario Ann ha sido infectado en diferentes ocasiones vulnerando la seguridad por medio de un robo de contraseñas del cual se desconoce con exactitud su origen, ya que en alguna ocasión ha sido el mismo usuario quien ha descargado el archivo malicioso.

- Se ha descartado la posibilidad de que el malware que infectó el equipo investigado haya incidido de alguna manera en la creación o descarga de archivos relacionados con tarjetas de crédito. Tampoco existen rastros de su incidencia en una posible generación y falsificación de mensajes.

CAPITULO 8. GLOSARIO.

A

ANÁLISIS FORENSE INFORMÁTICO
es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

ARTEFACTOS FORENSES
registro sobre toda actividad realizada por el sistema o el usuario, programas utilizados, accesos, conexiones, aplicaciones, descargas desde Internet, etc.

AUTOPSY
Plataforma de analisis forense digital con interfaz grafica desarrollada por Basis Technology.

B

BASE DE DATOS
Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso

BMP
Extensión del tipo de archivo de mapa de bits de Windows (Windows bitmap).

C

CADENA DE CUSTODIA
se define como el procedimiento controlado que se aplica a los indicios materiales relacionados con el delito, desde su localización hasta su valoración por los encargados de su análisis, normalmente peritos, y que tiene fin no viciar el manejo que de ellos se haga y así evitar alteraciones, sustituciones, contaminaciones o destrucciones.

CIFRADO
un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.

CONDUCTA CRIMINAL
Es una conducta antisocial que abarca un amplio rango de actos y actividades que infringen reglas y expectativas sociales, muchas de ellas reflejan acciones contra el entorno, personas y propiedades. · 7

CONFIABILIDAD
es una propiedad psicométrica que hace referencia a la ausencia de errores de medida.

CONTINGENCIA
En el sentido más universal, implica tener uno o varios objetivos a realizar junto con las acciones requeridas para concluirse exitosamente.

CORRELACION
Poner en relación mutua o recíproca dos o más cosas mediante un sentido lógico.

D

DATO
es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa. Los datos describen hechos empíricos, sucesos y entidades.

DISCO DURO
es el dispositivo de almacenamiento de datos que emplea un sistema de grabación magnética para almacenar archivos digitales.

E

EVIDENCIA
cualquier conocimiento o prueba que corrobora la verdad de una proposición.

EVIDENCIA DIGITAL
abarca cualquier información en formato digital que pueda establecer una relación entre un delito y su autor. Desde el punto de vista del derecho probatorio, puede ser comparable con “un documento” como prueba legal. Con el fin de garantizar su validez probatoria, los

documentos deben cumplir con algunos requerimientos.

G

GIF
es un formato gráfico utilizado ampliamente en la World Wide Web, tanto para imágenes como para animaciones.

H

HASH
es una función computable mediante un algoritmo,que tiene como entrada un conjunto de elementos, que suelen ser cadenas, y los convierte (mapea) en un rango de salida finito, normalmente cadenas de longitud fija.

I

IMAGEN FORENSE
es uno o varios archivos que contienen la estructura y contenidos completos de un dispositivo o medio de almacenamiento de datos, como un disco duro, un disquete o un disco óptico (CD, DVD).

INFORME PERICIAL
es una estructura formal de presentación de resultados periciales, adecuada para su comprensión e interpretación por parte de lectores que no son especialistas en la materia peritada. Normalmente, pero no de manera excluyente, se trata de operadores del derecho, en particular funcionarios judiciales.

K

KALI LINUX
es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general.

M

MEMORIA RAM
se utiliza como memoria de trabajo de computadoras para el sistema operativo, los programas y la mayor parte del software.

MEMORIA USB
es un tipo de dispositivo de almacenamiento de datos que utiliza memoria flash para guardar datos e información.

METODOLOGÍA
el estudio o elección de un método pertinente o adecuadamente aplicable a determinada practica.

P

PASSWORD
contraseña o clave, es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso.

PLANIFICACIÓN
Implica tener uno o varios objetivos a realizar junto con las acciones requeridas para concluirse exitosamente.

PMBOK
Metodologia reconocida y estandarizada para la gerencia de proyectos.

PROGRAMAS MALICIOSOS
software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o Sistema de información sin el consentimiento de su propietario.

S

SKYPE
es un software que permite comunicaciones de texto, voz y vídeo sobre Internet (VoIP).

SQLITE
es un sistema de gestión de bases de datos relacional compatible con ACID, contenida en una relativamente pequeña (~275 kiB)2 biblioteca escrita en C.

S-TOOLS

es un programa para Windows que permite encriptar y ocultar datos en archivos .wav o en imágenes en formato BMP y GIF.

SUFICIENCIA

Capacidad o aptitud mínima para conseguir, demostrar o cumplir algo.

T

TARJETA DE CRÉDITO

es un instrumento material de identificación, que puede ser una tarjeta de plástico con una banda magnética, un microchip y un número en relieve. Es emitida por un banco o entidad financiera que autoriza a la persona a cuyo favor es emitida.

TRANSICIONAL

Elemento que pasa de un estado a otro.

TRUECRYPT

es una aplicación informática freeware que sirve para cifrar y ocultar datos que el usuario considere reservados empleando para ello diferentes algoritmos de cifrado como AES, Serpent y Twofish o una combinación de los mismos. Permite crear un volumen virtual cifrado en un archivo de forma rápida y transparente o cifrar una partición o una unidad extraible entera.

V

INFORMACION VOLÁTIL

Conjunto de datos que se pierden al interrumpirse el flujo eléctrico.

W

WAV

es un formato de audio digital normalmente sin compresión de datos desarrollado y propiedad de Microsoft y de IBM que se utiliza para almacenar sonidos en el PC, admite archivos mono y estéreo a diversas resoluciones y velocidades de muestreo, su extensión es .wav.

CAPITULO 9. BIBLIOGRAFIA.

1. ISO/IEC. (2012). *ISO/IEC 27037 Information Technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence*. Suiza: ISO.

2. Hale, M., Case, A., Levy, J., & Walters, A. (2014). *The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory*. Canadá: Wiley.

3. Carvey, H. (2012). *Windows forensic, analysis toolkit. Advanced analysis techniques for windows 7*. USA: Syngress.

4. Hale, M. (2012). *Volatility Introduction*. Noviembre 10, 2015, de Google Sitio web: https://code.google.com/p/volatility/wiki/DocFiles.

5. MediaWiki. (2012). *List of Volatility Plugins*. Noviembre 12, 2015, de Forensics Wiki Sitio web: http://www.forensicswiki.org/wiki/List_of_Volatility_Pluginshttps://technet.microsoft.com/en-us/sysinternals/bb842062.aspx.

6. Kang, M. (2013). *Using Mutex Objects*. Noviembre 20, 2015, de Microsoft Sitio web: https://msdn.microsoft.com/en-us/library/windows/desktop/ms686927(v=vs.85).aspx.

7. Cobb, A., & Hale, J. (2013). Common areas to investigate: USB devices. *En Data Exfiltration and Forensic Analysis in a Microsoft Windows Environment* (pp. 19-21). USA: ISSA.

8. Sans DFIR. (2014).*Know Abnormal Find evil*. Noviembre 21, 2015, de Sans DFIR Sitio web: https://digital-forensics.sans.org/media/poster_2014_find_evil.pdf.

9. Hale, M. (2012). *CommandReference23*. Noviembre 07, 2013, de Google Sitio web: https://code.google.com/p/volatility/wiki/CommandReference23.

10. Caballero, A. (2015). *Autopsy 3 open extensible fast*. USA: Reydes.

11. Rhodes, M. (2013). ISO 27000 Series. En *The Complete Reference Information Security Second Edition* (pp. 57-60). USA: McGrawHill.

12. Sans DFIR. (2015). *Memory Forensics*. Noviembre22, 2015, de Sans DFIR Sitio web: https://digital-forensics.sans.org/media/Poster-2015-Memory-Forensics2.pdf.

13. Sans DFIR. (2013). *Evidence Collection Cheat Sheet*. Noviembre 24, 2015 , de Sans DFIR Sitio web: https://digital-forensics.sans.org/media/evidence_collection_cheat_sheet.pdf.

14. Sans DFIR. (2015).*Volatility Memory Forensic Framework*. Noviembre 25, 2015 , de Sans DFIR Sitio web: https://digital-forensics.sans.org/media/volatility-memory-forensics-cheat-sheet.pdf.

15. ministerio del interior. (2013). Ley *Orgánica 10/1995, de 23 de noviembre.* Diciembre 15, 2015, de ministerio del interior Sitio web: http://www.interior.gob.es/web/servicios-al-ciudadano/normativa/leyes-organicas/ley-organica-10-1995-de-23-de-noviembre.

16. Skype. (2014).*¿Dónde puedo encontrar mi historial de chats en Skype para el escritorio de Windows y qué puedo hacer con él?*. diciembre 16,2015, de Skype Sitio web: https://support.skype.com/es/faq/FA392/donde-puedo-encontrar-mi-historial-de-chats-en-skype-para-el-escritorio-de-windows-y-que-puedo-hacer-con-el.

17. Kali Linux. (2015). *Category: 07. Kali Community Support*. noviembre 30, 2015, de Offensive Security Sitio web: http://docs.kali.org/category/community.

18. Microsoft. (2014). *Windows registry information for advanced users*. diciembre 02, 2015, de Microsoft Sitio web: https://support.microsoft.com/en-us/kb/256986.

19. Microsoft. (2009). *Windows 7: Troubleshooting and Support*. diciembre 01, 2015, de Microsoft Sitio web: https://technet.microsoft.com/en-us/library/dd349347(v=ws.10).aspx.

20. Karpisek, F., Baggili, I., & Breitinger, F.. (2015). *WhatsApp network forensics: Decrypting and understanding the WhatsApp call signaling messages*. diciembre 19, 2015, de Brno University of Technology Sitio web: http://www.fit.vutbr.cz/research/pubs/index.php?file=%2Fpub%2F10979%2FWhatsApp.pdf&id=10979.

21. Mehta, L. (2013). *Malware Analysis Basics - Part 1 Static Malware Analysis*. diciembre 20, 2015, de Infosec Institute Sitio web: http://resources.infosecinstitute.com/malware-analysis-basics-static-analysis/.

22. Ligh, M. (2014). *TrueCrypt Master Key Extraction And Volume Identification*. noviembre 24, 2015, de Volatility Labs Sitio web: http://volatility-labs.blogspot.com.co/2014/01/truecrypt-master-key-extraction-and.html.

CAPITULO 10. ANEXOS.

Se anexan las evidencias digitales validadas y correlacionadas en la sub-etapa de exploración, los archivos están estructurados en el directorio ANEXOS.

El índice del directorio ANEXOS se muestra a continuación.

Etiqueta	Nombre	Obtenido en prueba	Breve descripción	Ruta donde se halló	Usuario	Tamaño bytes	hash md5
U1	00027625.png	3.3.2	Imagen con tarjetas.	/img_USB.E01/vol_vol4/$Unalloc/Unalloc_59_8531968_123375616		5816	945edcb2f7b7671dfcaa43a3c781d62b
U2	Pendientes.ods	3.3.3	Hoja de cálculo con lista de tarjetas.	/img_USB.E01/vol_vol4/		15766	6da97888ff474194bedc0cf99b5f67de
U4	whatsapp_castellano.db	3.3.3	Archivo con mensajes estructurados de Whatsapp.	/img_USB.E01/vol_vol4/Old_compis/		26624	17c1db82b4827c126ccbcdc42de4d711
R1	hashdump.txt	4.3.2	Archivo que evidencia las cuentas de usuario existentes.	Resultado.[1]			281a2a91e3004b9a2cd9d14d7d1b50bc
R3	pslist.txt	4.3.3	Listado de procesos ejecutados en el sistema.	Resultado.			F2012b97f1c697379a5cf210a1844bf5
R4	psscan.txt	4.3.3	Listado jerárquico de procesos visible y ocultos ejecutados.	Resultado.			215cbdfb6e43f516313fa3faad0ff522
R5	summary.txt	4.3.4	Lista de datos relativos al archivo cifrado y usuario implicado.	Resultado.			A54b3a3ea9ad0896050eb5286d722f7b
D6	MyHome	5.3.11	Archivo cifrado de Ann.	/img_Ann_HD.E01/Users/Ann/	Ann		F45dea81e1a23bb693d36ebe7eeafdac
D13	2015-09-07-2.dc	5.3.15	Archivo que contiene Password's, producto de un ataque de Keylogger.	*/img_Ann_HD.E01/Users/Ann/AppData/Roaming/*	Ann	157311800	9bc3bccd8917bee6eef11cc4f2276a48
D2	12034-20150907_162718.jpg	5.3.8	Imagen con metadatos, utilizada para ubicación GPS, enviada por usuario Aram.	/img_Ann_HD.E01/Users/Ann/Pictures/Fotos/Otras fotos/	Ann	1058873	68ec0b8cef946e6403d7d222768163fd

[1] Archivo que ha sido calculado mediante la ejecución de un comando o plugin de otra herramienta.

D3	12036-20150907_162746.jpg	5.3.8	Imagen con metadatos, utilizada para ubicación GPS, enviada por usuario Aram.	/img_Ann_HD.E01/Users/Ann/Pictures/Fotos/Otras fotos/	Ann	915872	994823f3803436b04e0552f36179347a
D4	12038-20150907_162819.jpg	5.3.8	Imagen con metadatos, utilizada para ubicación GPS, enviada por usuario Aram.	/img_Ann_HD.E01/Users/Ann/Pictures/Fotos/Otras fotos/	Ann	1916793	25152d446aa96024f187bc54d81efa6e
E1	pwd.txt.txt	6.4.1.1	Credenciales halladas en *MyHome,* incluye credenciales de correos electrónicos.	/img_Ann_HD.E01/Users/Ann/MyHome/	Ann	221	255f79dadf9131f91c66a072a63c136c
E2	Tarjetas_Ricky.ods	6.4.1.1	Listado de tarjetas estructuradas con numero, nombre y apellido.	/img_Ann_HD.E01/Users/Ann/MyHome/	Ann	14062	0fa1f944c5bfaa86b25e2a8c7b54688f
E3	TOTAL.ods	6.4.1.1	Listado de 40 tarjetas estructurado con tipo, numero, nombre y apellido.	/img_Ann_HD.E01/Users/Ann/MyHome/	Ann	17816	5ce84b1cfae53afe1cc3b5f5abdf0861
E4	DSCN8333.gif	6.4.1.1	Imagen con información oculta por medio de S-Tools.	/img_Ann_HD.E01/Users/Ann/Pictures/Fotos/Fotos Obs Fabra/	Ann	7026074	7d57a47b2e31d0b8c149cedaeb835767
E5	Tarjetas_Ricky.txt	6.4.1.1	Listado de tarjetas oculto en **E4.**	/img_Ann_HD.E01/Users/Ann/Pictures/Fotos/Fotos Obs Fabra/DSCN8333.gif/	Ann	14062	Bc05392eee0d51a7881c7800e94f9b9b
E6	main.db	6.4.2.1	Archivo con mensajes estructurados de Skype.	/img_Ann_HD.E01/Users/Ann/AppData/Roaming/Skype/annetom22/	Ann	458752	Bb68e7232c9bd346db3ad82ebeeda214
E8	reporte_malware_1.pdf	6.4.4.1	Reporte de malware yUmikJMYd3b.exe	Procesado.[2]		324685	Cef17fab4086756f1763b4494d65567d
E9	reporte_malware_2.pdf	6.4.4.1	Reporte de malware LlistatNumeracions.exe	Procesado.		383359	356c990ba1ce99abb851e6e867875002
E10	reporte_malware_3.pdf	6.4.4.1	Reporte de malware excel_server.exe	Procesado.		300596	F18979a82721dfe6d53c5774848903bc
E11	reporte_malwar	6.4.4.1	Reporte de	Procesado.		324685	B9f5421dfc0d52ad

[2] Reporte obtenido del análisis en la plataforma anubis.iseclab.org.

	e_4.pdf		malware TheJerm.exe				d17c65c545997046

Tabla 53. Total de evidencia digital seleccionada.