Universidad de Alcalá
Escuela Politécnica Superior

Grado en Ingeniería en Sistemas de Información

Trabajo Fin de Grado

Análisis de datos con el software forense FTK

Autor: Vicente García González

Tutor: Manuel Sánchez Rubio

2021-2022

UNIVERSIDAD DE ALCALÁ

ESCUELA POLITÉCNICA SUPERIOR

Grado en Ingeniería en Sistemas de Información

Trabajo Fin de Grado

Análisis de datos con el software forense FTK

Autor: Vicente García González

Tutor: Manuel Sánchez Rubio

Tribunal:

Presidente:

Vocal 1º:

Vocal 2º:

Fecha de depósito:

Índice general

Índice general **4**

Agradecimientos **9**

Resumen **11**

Palabras Clave **12**

Abstract **14**

Keywords **16**

Índice de Ilustraciones **18**

Lista de acrónimos **21**

Introducción **23**

1.1 Presentación 23

1.2 Objetivo 23

Informática Forense **24**

2.1 Historia de la informática forense 24

2.2 Actualidad de la informática forense 25

Software FTK Imager **26**

3.1 Introducción a FTK Imager 26

3.2 Interfaz FTK Imager 27

3.3 Adicción de evidencia 30

3.4 Visualización de la evidencia 31

3.5 Creación de imagen de evidencia 36

Herramientas importantes **41**

4.1 Captura de memoria (Capture Memory) 41

Creación del entorno de prueba para el análisis forense **44**

5.1 Descarga e instalación de elementos necesarios para el entorno de pruebas 44

5.1.1 Descarga ISO Windows 10 44

5.1.2 Descarga e instalación de VirtualBox 46

5.2 Creación entorno de prueba en VirtualBox 48

Análisis de evidencias del entorno de pruebas con FTK Imager 54

6.1 Archivos que se van a analizar 54

6.2 Recopilación de información del disco duro 55

6.3 Recopilación de información de la memoria 57

6.3.1 Análisis de volcado de memoria 1 57

6.3.2 Análisis de volcado de memoria 2 61

6.4 Recopilación de información adicional 64

Conclusiones 67

Bibliografía 68

“*May your heart be your guiding key*”

Agradecimientos

Este trabajo no habría sido posible sin la ayuda y el apoyo de todas las personas que me han acompañado durante todo el tiempo que ha durado mi paso por la universidad.

Agradecer a mi familia que siempre está ahí para cualquier cosa que necesite. Pero sobre todo a mis padres que me han ayudado siempre en todo lo que ellos han podido y mucho más.

A ellos que siempre han estado tanto en mis mejores momentos, como en mis peores. A mi padre Vicente, por todos los buenos consejos que me da siempre, por ayudarme a mantener la cabeza fría en los momentos en los que ya no podía más, y por haberme enseñado que todo es posible si uno se esfuerza y trabaja. A mi madre Mª Amelia, por su amor incondicional y por estar siempre ahí ayudándome con las cosas que en principio pueden parecer pequeñas, pero que para mí resultan muy importantes. Que sepáis que este logro es tanto vuestro como mío.

A mi hermano Jaime que, a pesar de ser capaz de sacarme de mis casillas de la manera más rápida y sencilla, sé que siempre estará para ayudarme con cualquier cosa que necesite. Eres la persona más inteligente que conozco y sé que puedes llegar a realizar lo que te propongas.

Gracias también a mi grupo de amigos de siempre, Oscar, Marcos, Jorge, Álvarez, Garchi, Alberto e Irene. Desde que os conocí habéis sido una de las partes más importantes de mi vida y no os hacéis una idea de lo realmente importantes que sois para mí. Por todos los momentos y las risas que hemos pasado juntos que espero que sean muchísimos más, y de los que no me cansaré nunca de hablar. Gracias por estar ahí durante todo este tiempo siendo un apoyo muy importante para mí a la hora de conseguir mis metas.

También agradecer a mis compañeros de universidad Sandra, César y Marina. Por tantas horas de estudio y de quebraderos de cabeza entre nosotros con proyectos, exámenes y trabajos. Habéis hecho que mi etapa universitaria haya sido increíble, llevándome con ella unos amigos espectaculares y muy buenos momentos que siempre recordaré.

Agradecer a Manuel mi tutor, por haberme ayudado en la creación de este trabajo y a dar lo mejor de mí en él, y también por haberme hecho encontrar la rama de la informática que más me apasiona, la ciberseguridad.

Y por último agradecer a mis abuelos, que ya no están, pero que recuerdo cada día. En todo este tiempo habéis aportado vuestro granito de arena de una manera muy especial para mí. Gracias.

Resumen

La informática forense lleva desde hace mucho tiempo siendo una rama de la informática muy importante para la investigación de delitos, tanto realizados por internet como que puedan tener relación con delitos cometidos en la calle. Gracias a la informática forense somos capaces de poder realizar una investigación en elementos informáticos como un ordenador y obtener información necesaria, y en algunos casos crucial, para la resolución de estos casos.

En este trabajo se desarrollará una simulación de una investigación forense sobre un ordenador de un sospechoso de cometer atracos a bancos. Para realizar la investigación se utilizará la herramienta FTK Imager, una herramienta creada para realizar investigaciones forenses sobre equipos informáticos. Se someterá el ordenador ficticio del sospechoso a pruebas de análisis forenses viendo de una manera básica y sencilla como puede comenzar una investigación forense.

Palabras Clave

- FTK Imager
- Memoria RAM
- Informática forense
- Ordenador
- Evidencia
- Archivos
- Análisis forense
- Investigación

Abstract

Computer forensics has been a very important branch of computer science for a long time in the investigation of crimes, both those committed on the Internet and those that may be related to crimes committed on the street. Thanks to computer forensics we are able to carry out an investigation in computer elements such as a computer and obtain information necessary, and in some cases crucial, for the resolution of these cases.

In this work we will develop a simulation of a forensic investigation on a computer of a bank robbery suspect. The investigation will be carried out using the FTK Imager tool, a tool created to carry out forensic investigations on computer equipment. The fictitious computer of the suspect will be subjected to forensic analysis tests, showing in a basic and simple way how a forensic investigation can be started.

Keywords

- FTK Imager
- RAM memory
- Computer Forensics
- Computer
- Evidence
- Files
- Forensic Analysis
- Investigation

Índice de Ilustraciones

Ilustración 1. Página de descarga FTK Imager 26
Ilustración 2. Imagen interfaz FTK Imager 27
Ilustración 3. Barra navegación FTK Imager 27
Ilustración 4. Opciones pestaña File 28
Ilustración 5. Opciones pestaña view 29
Ilustración 6. Opciones pestaña Mode 29
Ilustración 7. Opciones pestaña Help 29
Ilustración 8. Añadir Elemento 30
Ilustración 9. Tipos de elementos a analizar 30
Ilustración 10. Selección de dispositivo 31
Ilustración 11. Interfaz FTK Imager con evidencia 32
Ilustración 12. Propiedades del dispositivo 33
Ilustración 13. Memoria del dispositivo 34
Ilustración 14. Árbol de evidencias 35
Ilustración 15. Lista de archivos y ficheros 35
Ilustración 16. Selección de elemento 36
Ilustración 17. Creación de imagen 37
Ilustración 18. Tipos de imágenes de evidencias 37
Ilustración 19. Información de la evidencia 38
Ilustración 20. Selección de destino de imagen de evidencia 39
Ilustración 21. Proceso de creado de imagen de evidencia 39
Ilustración 22. Verificación de resultados 40
Ilustración 23. Captura de memoria RAM 41
Ilustración 24. Volcado de memoria 42
Ilustración 25. Archivos de volcado de memoria 42
Ilustración 26. Análisis de volcado de memoria 43
Ilustración 27. Página de descarga ISO Windows 44
Ilustración 28. Ejecutable ISO Windows 45
Ilustración 29. Creación de medios de Windows 45
Ilustración 30. Archivo ISO Windows 45
Ilustración 31. Página de descarga VirtualBox 46
Ilustración 32. Descarga VirtualBox para Windows 46
Ilustración 33. Ejecutable VirtualBox 46
Ilustración 34. Opciones de instalación de VirtualBox 47
Ilustración 35. Segundas opciones instalación VirtualBox 47
Ilustración 36. Página de inicio VirtualBox 48
Ilustración 37. Creación máquina virtual 48
Ilustración 38. Selección de memoria RAM 49
Ilustración 39. Creación disco Máquina Virtual 49
Ilustración 40. Archivos de disco duro 50
Ilustración 41. Tipo de almacenamiento 50
Ilustración 42. Cantidad de almacenamiento 51
Ilustración 43. Máquina virtual 51
Ilustración 44. Ajustes máquina virtual 52
Ilustración 45. Procesadores máquina virtual 52
Ilustración 46. Selección disco de inicio máquina virtual 53
Ilustración 47. Elementos de investigación 54
Ilustración 48. Ruta carpeta documentos 55

Ilustración 49. Subcarpetas de la carpeta documentos 55
Ilustración 50. Archivos carpeta Información Confidencial 56
Ilustración 51. Imágenes carpeta Información Confidencial 56
Ilustración 52. Contenido archivo Bancos.xlsx 56
Ilustración 53. Contenido archivo Registro de coches.docx 57
Ilustración 54. Botón de visualización de texto de la memoria RAM 58
Ilustración 55. Cuadro de búsqueda en memoria RAM 58
Ilustración 56. Búsuqeda 1 memoria RAM 1 59
Ilustración 57. Búsuqeda 2 memoria RAM 1 59
Ilustración 58. Búsqueda 3 memoria RAM 1 59
Ilustración 59. Búsuqeda 4 memoria RAM 1 60
Ilustración 60. Página web del resultado de la búsqueda 4 60
Ilustración 61. Búsqueda 5 memoria RAM 1 60
Ilustración 62. Página web del resultado de la búsqueda 5 61
Ilustración 63. Introducir contraseña en Gmail 62
Ilustración 64. Resultado búsqueda contraseña 62
Ilustración 65. Correo de Gmail 63
Ilustración 66. Mensaje código QR 1 64
Ilustración 67. Mensaje código QR 2 64
Ilustración 68. Escritorio del disco C: 65
Ilustración 69. Ruta de la carpeta de Electrum 65
Ilustración 70. Contenido carpeta Wallets Electrum 66
Ilustración 71. Texto código cartera criptos 66

Lista de acrónimos

RAM	Random Acces Memory
FTK	Forensic Tool Kit
CD	Compact Disk
DVD	Digital versátil Disk
GB	Giga Byte
VDI	VirtualBox Disk Image
QR	Quick Response
TOR	The Onion Router

Introducción

1.1 Presentación

Actualmente uno de los campos más importantes dentro de la rama de la informática y de la tecnología es la ciberseguridad. Desde el comienzo de esta siempre se ha podido observar que la tecnología se ha utilizado tanto de una manera correcta, como de manera incorrecta por las personas.

Por esta razón la ciberseguridad es tan importante, ya que nos ayuda a la hora de poder estar seguros con las actividades que podamos realizar mediante internet y a la vez es una herramienta contra las personas que utilizan la tecnología para realizar operaciones fraudulentas o que pueden ser perjudiciales para otras personas.

Al igual que existen investigaciones cuando se ha realizado un delito y estas investigaciones tienen sus equipos forenses, la informática también cuenta con su equipo de forenses que se encargan de realizar estas investigaciones. Tanto es así que desde hace tiempo existen divisiones de la policía se encargan de los delitos que se realizan mediante internet, como estafas, suplantación de identidad, posesión de información ilegal, y muchos otros.

Relacionado con la informática forense, en este trabajo se va a realizar pruebas con un software informático especializado para este tipo de análisis, y se va a ver de manera básica los conceptos y los pasos de una investigación de este tipo.

1.2 Objetivo

El objetivo de este trabajo de fin de grado es realizar la simulación de un supuesto caso en el que se está investigando a una persona por cometer delitos de robos a bancos. A esta persona se le ha incautado el ordenador y debemos de encontrar pruebas que confirmen que efectivamente esta persona está realizando los diferentes atracos.

Para realizar esto se creará una máquina virtual en la que se simulará el ordenador del sospechoso. Esta máquina virtual se poblará de datos que prueben que efectivamente las persona que se ha detenido es culpable de cometer esos delitos.

A la hora de realizar la investigación, se utilizará el software forense FTK Imager, con el que se obtendrán los datos del ordenador simulado en la máquina virtual. Con este software se realizarán todas las pruebas de obtención e investigación de los datos, y se verá poco a poco como se puede realizar una pequeña investigación forense con este software.

Informática Forense

2.1 Historia de la informática forense

Actualmente la informática forense se ha convertido en una de las ramas más importantes de la informática. Esta es la rama de la informática encargada de realizar análisis en pruebas de investigaciones de cara a localizar evidencias. Es similar a cuando en una escena de un crimen se buscan pruebas para descubrir quién es el culpable.

La informática forense no tiene un comienzo en concreto dentro de la historia, podríamos decir que esta comenzó en el momento en el que empezaron a surgir los primeros delitos realizados mediante sistemas informáticos. El primer comienzo de estos ataques reconocidos puede ser en el año 1978 en Florida. Se comenzaron a tener en cuenta como delitos, los delitos de sabotaje modificación y alteración de datos. Como ejemplo de estos, encontramos la creación de la herramienta conocida como 'copy2pc' que se encargaba de realizar copias de los disquetes, permitiendo la modificación y la alteración de los datos.

Esto hizo que al igual que las personas tuviesen herramientas para realizar estos delitos, se creasen herramientas para poder investigarlos. La primera herramienta que podemos considerar como la primera en la informática forense fue la creada por Peter Norton en 1983. Su herramienta UnErase permitía recuperar los archivos y las aplicaciones que hubiesen sido eliminados de manera accidental, y que no podían ser recuperados en aquella época.

Debido a que en la época de los 80 se empezó a estandarizar el uso de los ordenadores personales, hubo un aumento de la cantidad de ataques a particulares, lo que llevó a que en 1984 el FBI crease un programa conocido como el Programa de Medios Magnéticos (actualmente conocido como CART), siendo este uno de los primeros pasos de la investigación forense en la informática.

Más adelante en la época de los 90, en el año 1995 se crea la Internacional Organization of Computer Evidence (IOCE). Esta organización fue creada con el propósito de crear un foro internacional en el que las diferentes agencias de seguridad del mundo intercambiasen todo lo relacionado con la investigación y forense informática.

A partir de este momento se empezaron a dar a conocer más frecuentemente casos de delitos informáticos y con ellos los investigadores forenses relacionados con la informática. Uno de los casos más famosos fue el juicio de O.J Simpson, el cual fue famosos al ser un juicio con bastantes contradicciones en cuanto a las pruebas recopiladas. Esto llevó a que se decidiese crear un protocolo único para la obtención de pruebas digitales para este tipo de casos.

2.2 Actualidad de la informática forense

Poco a poco con el paso de los años la metodología y los protocolos que se utilizan para la realización de investigaciones forenses se han estandarizado. A su vez la cantidad de lugares en los que se almacenan datos con información han ido creciendo, desde discos duros, hasta datos en la nube, correos electrónicos, y dispositivos móviles.

Debido al crecimiento exponencial de los dispositivos y los lugares con datos, actualmente se siguen una serie de principios básicos para la realización de este tipo de investigaciones. Estos pasos los podemos resumir en los siguientes tres puntos:

- Una cadena de custodia que garantice que la evidencia que va a ser examinada no es manipulada.
- Realización de una documentación exhaustiva de los procesos y las pruebas a las que son sometidas las evidencias, para que el investigador tenga contexto de la información.
- Conservación íntegra de la evidencia, permitiendo en un futuro volver a realizar una investigación sobre la prueba original

Teniendo en cuenta estos puntos, se puede tener una noción básica de los protocolos que hay que seguir a la hora de realizar una investigación sobre un delito informático.

Hoy en día encontramos diferentes tipos de ciberdelitos que antiguamente ni se consideraban, todos ellos asociado al uso de un equipo informático, siendo estos delitos como el acoso, el espionaje o la suplantación de identidad. También todo delito que pueda ser cometido a través de internet es considerado como tal, habiendo delitos como el de robo, estafa, extorsión, etc.

Para poder llevar a cabo estas investigaciones, los forenses informáticos cuentan con herramientas especializadas para obtener la mayor información de los datos que tengan. Es por ello por lo que vamos a ver cómo funciona la herramienta forense FTK Imager en este trabajo de fin de grado y a utilizarla para realizar simulaciones reales de obtención de datos de un sospechoso ficticio.

Software FTK Imager

3.1 Introducción a FTK Imager

FTK Imager es un software de análisis forense creado por *AccessData* una empresa que pertenece a la compañía *exterro*. Es un software de análisis forense que permite la obtención de datos de evidencias en investigaciones sin necesidad de hacer cambios en las evidencias originales.

FTK Imager permite la creación de imágenes forenses de discos duros y pendrives, y la visualización de datos directamente de los elementos de investigación. Además, también es posible la exportación de imágenes forenses para un posterior análisis de esta, así como la recuperación de los archivos que han podido ser eliminados en la prueba forense.

Para poder utilizar el software FTK debemos de descargarlo de la siguiente página web: https://accessdata.com/product-download/ftk-imager-version-4-5 . Una vez que entramos en el enlace seleccionamos el botón de "Download now" y nos llevara a la página que aparece en la Figura 1.

Ilustración 1. Página de descarga FTK Imager

Para poder descargar el software finalmente, deberemos de rellenar los datos que se nos piden en el formulario y en pocos minutos nos llegará un correo al email que hayamos puesto en el formulario con un enlace de descarga con el que podremos obtener el ejecutable de instalación del FTK Imager. Una vez que tenemos el ejecutable solo tenemos que ejecutarlo y seguir los pasos de la instalación y ya tendríamos el software FTK Imager instalado en nuestro ordenador.

3.2 Interfaz FTK Imager

Una vez que ya tenemos instalado FTK Imager en nuestro ordenador, vamos a ver cómo es la interfaz y que elementos tiene el software para trabajar en el análisis forense.
FTK Imager nada más abrirlo presenta la siguiente apariencia:

Ilustración 2. Imagen interfaz FTK Imager

Como vemos FTK Imager no presenta una interfaz muy compleja, por lo que vamos a ver las opciones que hay en la barra de navegación de la parte superior izquierda, y más adelante nos centraremos en ciertas opciones, que vamos a utilizar a la hora de realizar nuestras pruebas.

Lo primero que vemos en la barra de navegación, es que cuenta con cuatro elementos, *File, View, Mode* y *Help*.

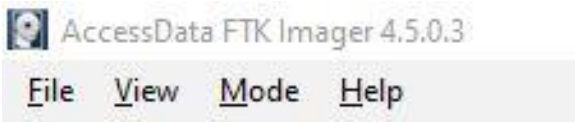


Ilustración 3. Barra navegación FTK Imager

- **File:** En esta pestaña de la barra de navegación se encuentran los elementos para poder comenzar a realizar pruebas sobre los elementos que se vayan a investigar, también podemos crear imágenes de los elementos físicos para un posterior análisis sin cambiar nada del disco principal, así como la captura de memoria si se comprueba un sistema en vivo, y la obtención de datos encriptados.

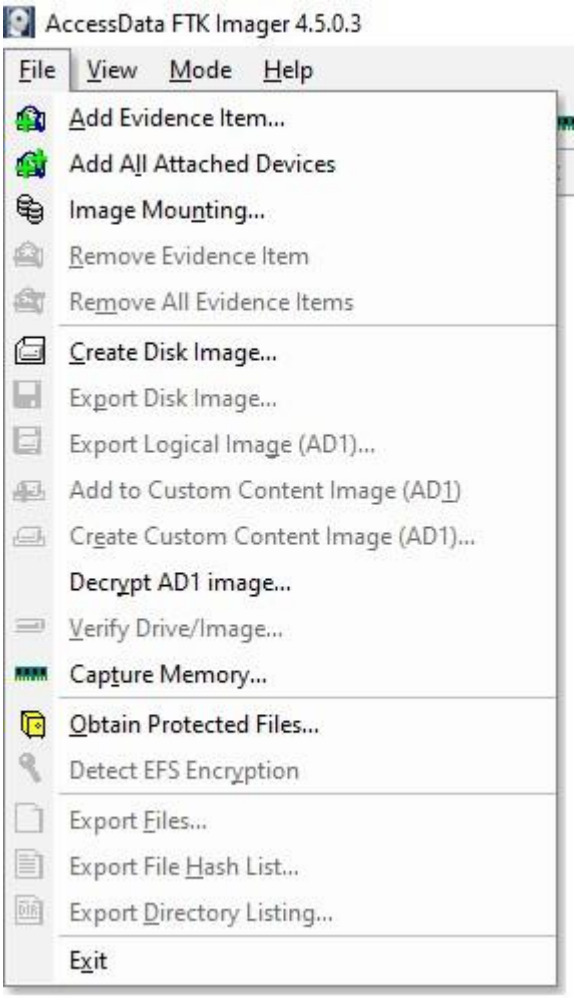


Ilustración 4. Opciones pestaña File

- **View:** En esta pestaña tenemos las diferentes vistas que hay en FTK Imager, como la barra de herramientas, la barra de estado del análisis, el árbol de evidencias, la pestaña de propiedades y la lista de archivos. Esta pestaña nos sirve para poder visualizar o no algunos elementos que nos puedan interesar ver o no cuando llevemos a cabo los análisis.

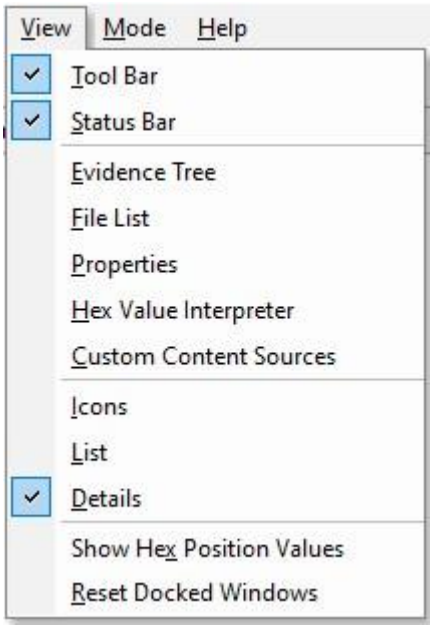


Ilustración 5. Opciones pestaña view

- **Mode:** En esta pestaña podemos seleccionar los modos en los que queremos que se visualicen los metadatos que podamos obtener de los archivos de las pruebas forenses que hagamos. Los modos son, automático, texto, o hexadecimal.

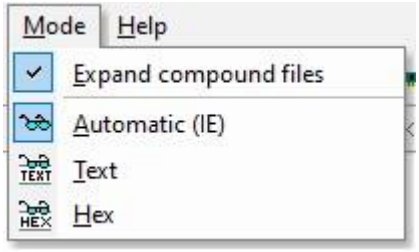


Ilustración 6. Opciones pestaña Mode

- **Help:** Esta pestaña nos sirve para poder acceder a la guía de usuario de FTK Imager, también para obtener los datos de la versión del software y todo lo relacionado con las licencias legales de este.

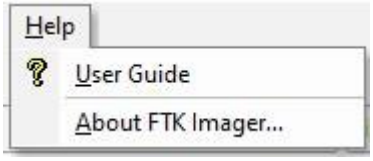


Ilustración 7. Opciones pestaña Help

3.3 Adicción de evidencia

Hemos visto como es la interfaz de FTK Imager, y las diferentes opciones que nos permite utilizar desde un primer comienzo, sin embargo, para poder poner en funcionamiento estas opciones debemos de tener un dispositivo para poder realizar el análisis. Este dispositivo puede ser desde un pendrive, un disco duro o una partición, hasta la imagen forense del propio sistema operativo que queramos como ya hemos mencionado en otras ocasiones.

Lo primero que tenemos que hacer, una vez que tenemos la evidencia en el ordenador, es pulsar sobre el icono 'Add Evidence Item'.

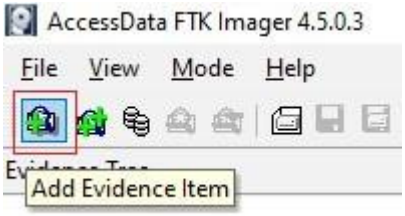


Ilustración 8. Añadir Elemento

Una vez que hemos pulsado sobre el icono de añadir elemento, nos aparecerá una ventana emergente en la que ser nos pedirá que seleccionemos el tipo de elemento que vamos a querer realizarle el análisis forense.

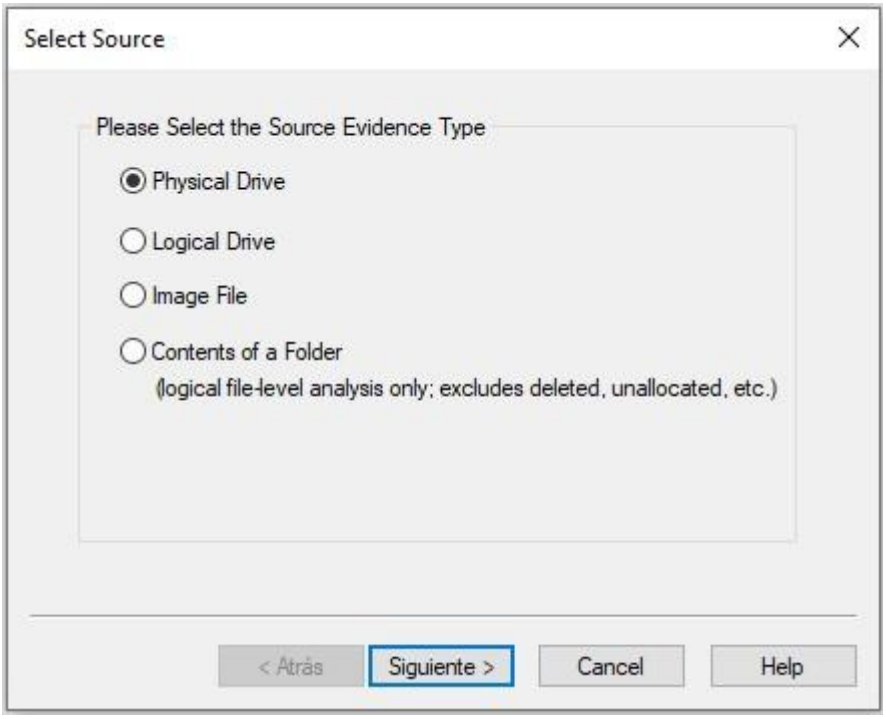


Ilustración 9. Tipos de elementos a analizar

Como vemos en la Ilustración 9, podemos analizar diferentes elementos que son los siguientes:

- **Physical Drive:** Con esta opción lo que podemos hacer es analizar todos los dispositivos físicos que se encuentren conectados en el ordenador en el que está instalado FTK Imager, ya sean discos duros, pendrives o incluso CDs y DVDs. Esta opción es útil cuando queremos investigar un disco duro en su totalidad, con todos los elementos que contenga.

- **Logical Drive:** Esta opción sirve para analizar por particiones. Si los dispositivos físicos que están conectados al ordenador cuentan con alguna partición, con esta opción podremos analizar solamente la partición que queramos, evitando de esa manera analizar el dispositivo en su totalidad si no fuera necesario.

- **Image File:** Esta opción nos permite analizar la imagen de un dispositivo, o incluso del sistema completo de un ordenador. Si nos encontramos con que debemos de hacer un análisis en el que no podemos tocar los elementos físicos o no los tenemos disponibles, siempre que tengamos una copia de la imagen del elemento que queremos podemos analizarla mediante esta opción.

- **Contents of a Folder:** Esta última opción nos muestra los contenidos de una carpeta de archivos del sistema, que nosotros seleccionemos. Sin embargo, esta opción es más limitada que las anteriores ya que es solamente va a visualizar los datos que se encuentren, no los que puedan haber llegado a ser eliminados o los que se encuentren deslocalizados.

3.4 Visualización de la evidencia

Una vez que hemos visto las opciones que nos da FTK Imager para poder analizar diferentes elementos, vamos a ver cómo es la interfaz una vez que ponemos un elemento a analizar.

En este caso el elemento que vamos a utilizar para ver cómo es la interfaz es un pendrive con algunos elementos como fotos, videos y documentos PDF. Lo primero que debemos de hacer es pulsar sobre el botón de añadir elemento de evidencia (Ilustración 8), y una vez que los hemos pulsado debemos seleccionar la opción Physical Drive (Ilustración 9), una vez que pulsamos esa opción nos aparecerá una nueva pestaña en la que se nos pedirá que seleccionemos el dispositivo que queramos, en nuestro caso el pendrive de pruebas.

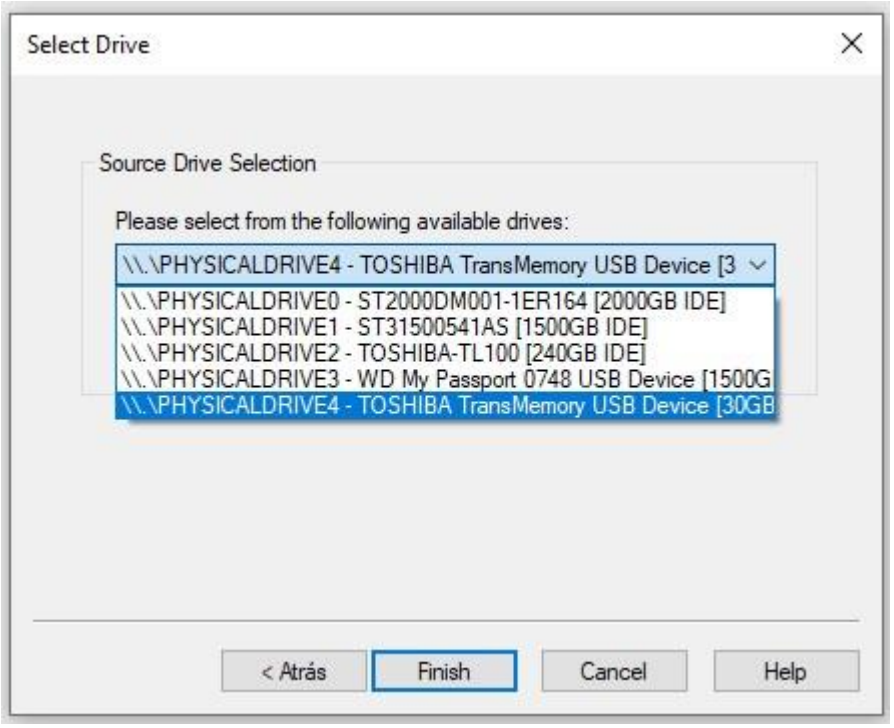


Ilustración 10. Selección de dispositivo

Una vez que ya hemos seleccionado el dispositivo FTK Imager se nos mostrará de la siguiente manera:

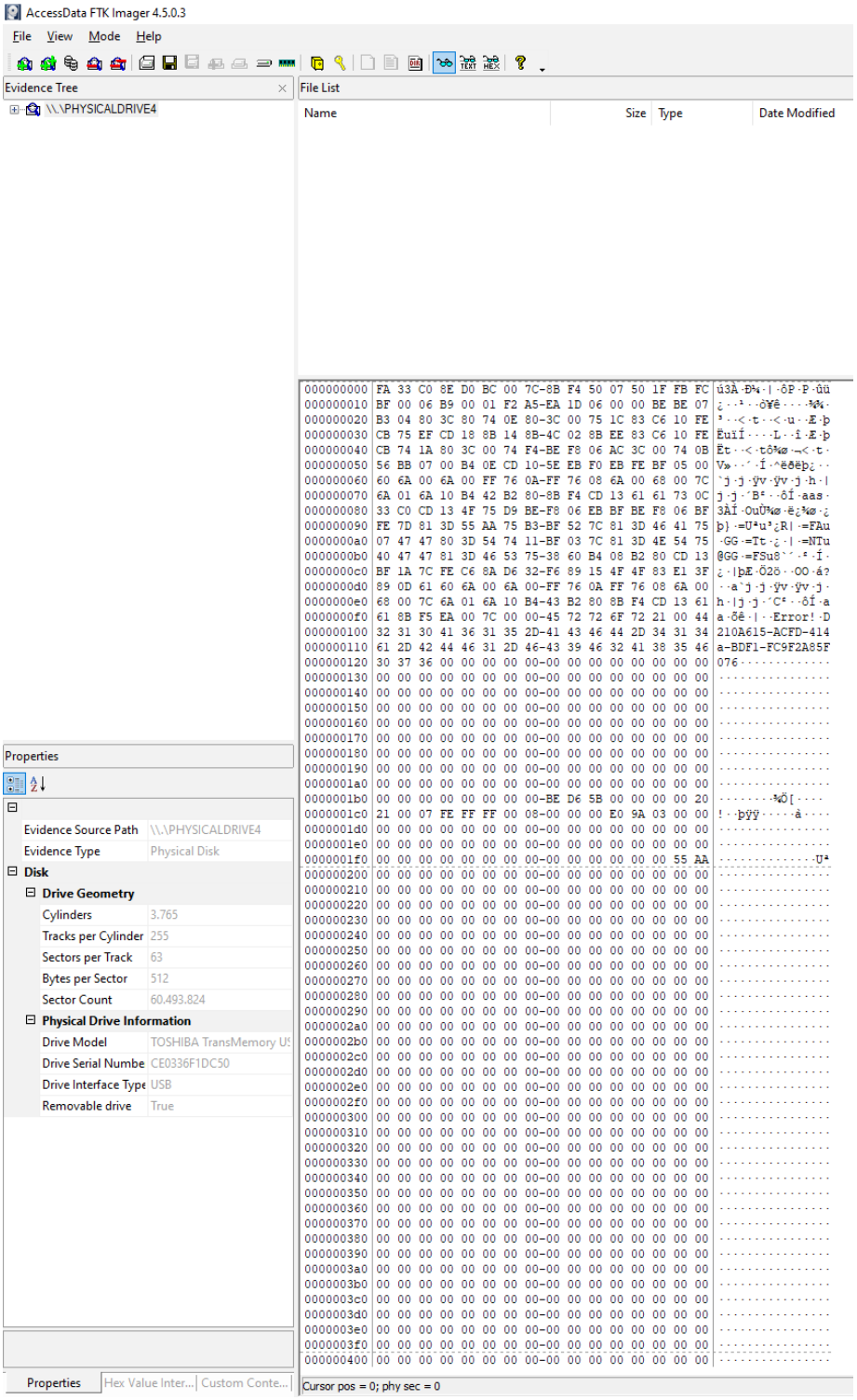


Ilustración 11. Interfaz FTK Imager con evidencia

Como vemos, una vez que seleccionamos un dispositivo para analizar la interfaz cambia para mostrarnos la información del dispositivo que estamos analizando y el contenido que tiene. Podemos diferenciarlo en 4 partes, las propiedades, la memoria, el árbol de evidencias y la lista de archivos y ficheros.

- **Propiedades:** En esta parte vemos las propiedades que tiene el dispositivo que se analiza, como son el número de sectores, los bytes por sector, el modelo de dispositivo, el número de serie, etc. Pero no solo es para mostrar la información del dispositivo, dependiendo de si estamos analizando un archivo como una imagen o un vídeo también se nos mostrará toda la información de este.

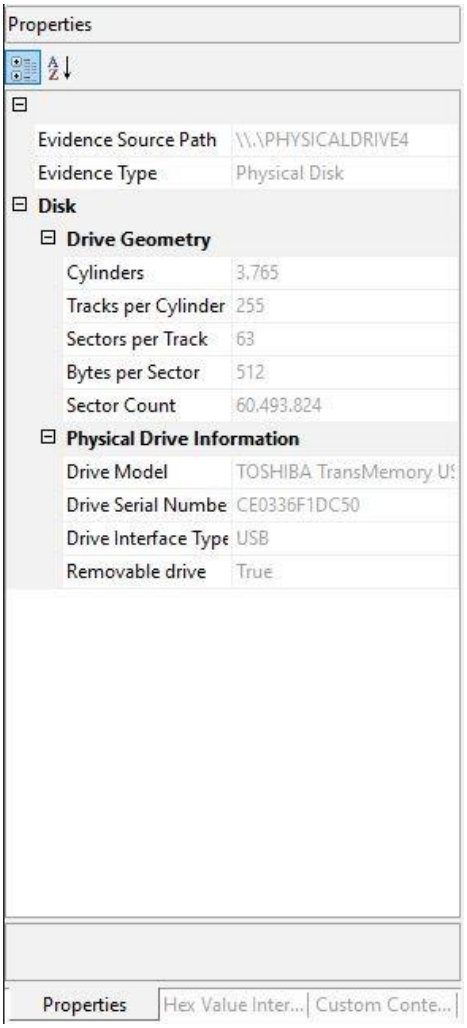
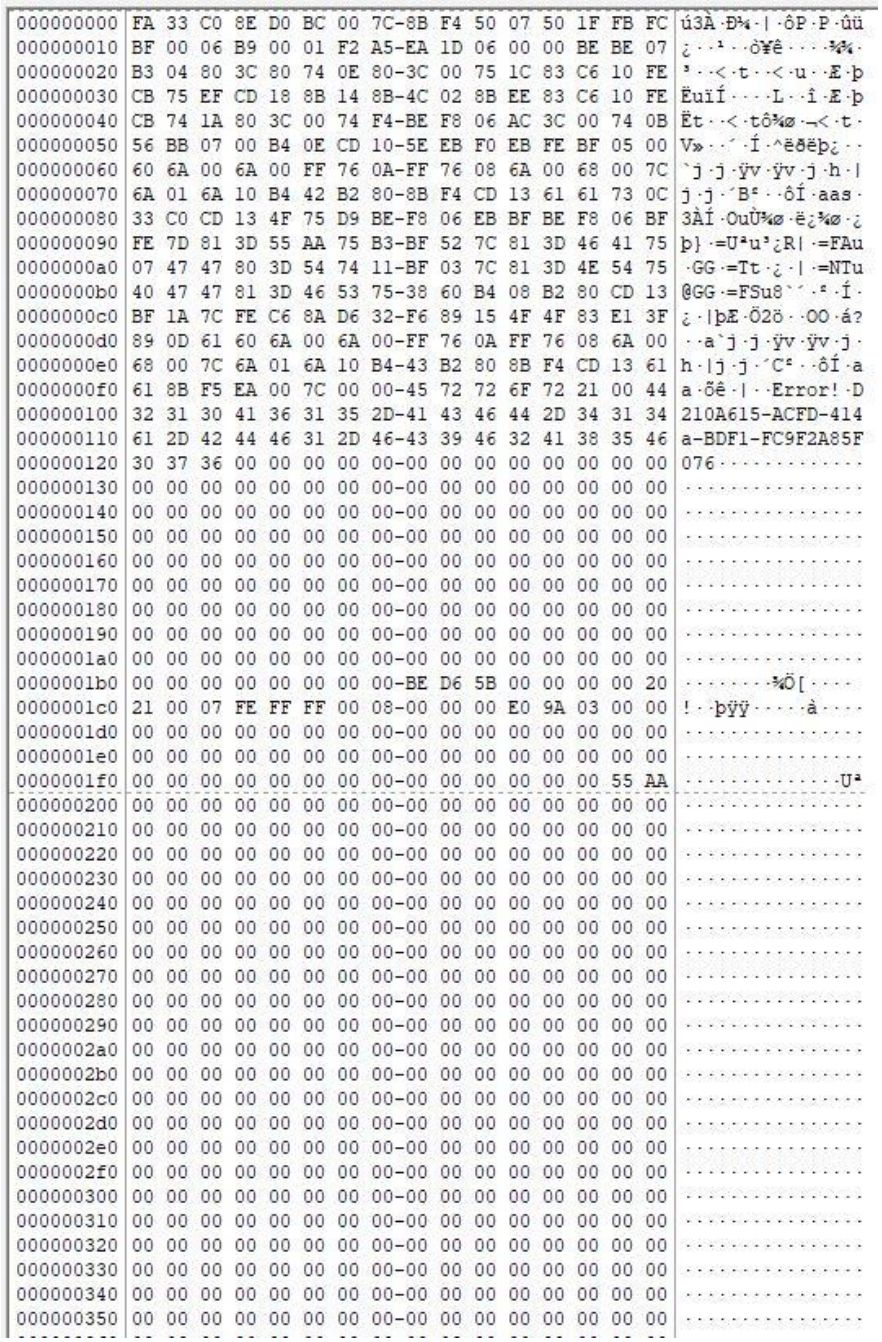


Ilustración 12. Propiedades del dispositivo

- **Memoria del dispositivo:** En esta parte se nos muestran los sectores de memoria que tiene el dispositivo, podemos ver qué sectores están escritos y cuales están vacíos. Si quisiéramos podríamos ver estos datos de diferente manera pulsando en la barra de opciones, en la opción *mode* (Ilustración 6), pudiendo ver la memoria de manera automática (FTK Imager detecta cual es modo de visualizarlo), en forma de texto normal, o en lenguaje hexadecimal. En nuestro caso está puesto de manera automática, ya que de esta manera dependiendo de que estemos visualizando nos va a mostrar mejor lo que es.



```
000000000 FA 33 C0 8E D0 BC 00 7C-8B F4 50 07 50 1F FB FC  ú3À·Ð¼·|·ôP·P·ûü
000000010 BF 00 06 B9 00 01 F2 A5-EA 1D 06 00 00 BE BE 07  ¿··¹··ò¥ê·····¾¾·
000000020 B3 04 80 3C 80 74 0E 80-3C 00 75 1C 83 C6 10 FE  ³·€<€t·€<·u·ƃÆ·þ
000000030 CB 75 EF CD 18 8B 14 8B-4C 02 8B EE 83 C6 10 FE  Ëuïͷ···L··î·ƃÆ·þ
000000040 CB 74 1A 80 3C 00 74 F4-BE F8 06 AC 3C 00 74 0B  Ët··€<·tô¾ø·¬<·t·
000000050 56 BB 07 00 B4 0E CD 10-5E EB F0 EB FE BF 05 00  V»··´·Í·^ëðëþ¿··
000000060 60 6A 00 6A 00 FF 76 0A-FF 76 08 6A 00 68 00 7C  `j·j·ÿv·ÿv·j·h·|
000000070 6A 01 6A 10 B4 42 B2 80-8B F4 CD 13 61 61 73 0C  j·j·´B²€·ôÍ·aas·
000000080 33 C0 CD 13 4F 75 D9 BE-F8 06 EB BF BE F8 06 BF  3ÀÍ·OuÙ¾ø·ë¿¾ø·¿
000000090 FE 7D 81 3D 55 AA 75 B3-BF 52 7C 81 3D 46 41 75  þ}·=Uªu³¿R|·=FAu
0000000a0 07 47 47 80 3D 54 74 11-BF 03 7C 81 3D 4E 54 75  ·GG€=Tt·¿·|·=NTu
0000000b0 40 47 47 81 3D 46 53 75-38 60 B4 08 B2 80 CD 13  @GG·=FSu8`´·²€Í·
0000000c0 BF 1A 7C FE C6 8A D6 32-F6 89 15 4F 4F 83 E1 3F  ¿·|þÆŠÖ2ö‰·OOƃá?
0000000d0 89 0D 61 60 6A 00 6A 00-FF 76 0A FF 76 08 6A 00  ‰·a`j·j·ÿv·ÿv·j·
0000000e0 68 00 7C 6A 01 6A 10 B4-43 B2 80 8B F4 CD 13 61  h·|j·j·´C²€·ôÍ·a
0000000f0 61 8B F5 EA 00 7C 00 00-45 72 72 6F 72 21 00 44  a·õê·|··Error!·D
000000100 32 31 30 41 36 31 35 2D-41 43 46 44 2D 34 31 34  210A615-ACFD-414
000000110 61 2D 42 44 46 31 2D 46-43 39 46 32 41 38 35 46  a-BDF1-FC9F2A85F
000000120 30 37 36 00 00 00 00 00-00 00 00 00 00 00 00 00  076·············
000000130 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
000000140 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
000000150 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
000000160 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
000000170 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
000000180 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
000000190 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0000001a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0000001b0 00 00 00 00 00 00 00 00-BE D6 5B 00 00 00 00 20  ········¾Ö[····
0000001c0 21 00 07 FE FF FF 00 08-00 00 00 E0 9A 03 00 00  !··þÿÿ·····à····
0000001d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0000001e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0000001f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 55 AA  ··············Uª
000000200 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
000000210 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
000000220 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
000000230 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
000000240 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
000000250 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
000000260 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
000000270 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
000000280 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
000000290 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0000002a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0000002b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0000002c0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0000002d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0000002e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0000002f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
000000300 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
000000310 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
000000320 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
000000330 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
000000340 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
000000350 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
```

Ilustración 13. Memoria del dispositivo

- **Árbol de evidencias:** En esta parte se muestra la lista de los dispositivos que estamos analizando. Si vamos ampliando el árbol de evidencias, por ejemplo, en un solo dispositivo como en este ejemplo, lo que vamos a ir visualizando son las diferentes particiones o no que puede llegar a tener y dentro las carpetas y archivos que tiene el dispositivo. De esta manera podemos ir investigando cada parte y elemento que tenga el dispositivo dependiendo de lo que estemos buscando.

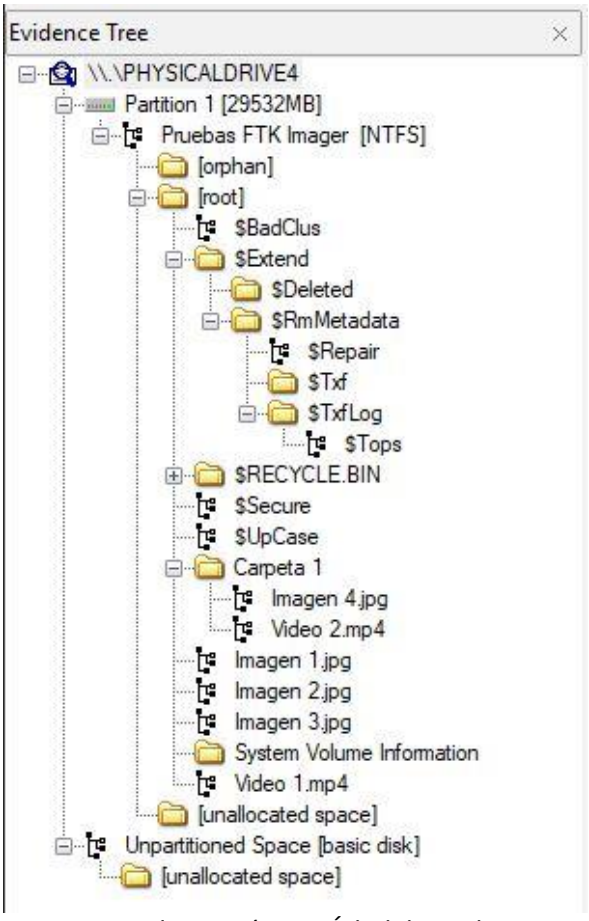


Ilustración 14. Árbol de evidencias

- **Lista de ficheros y archivos:** Aquí podemos visualizar los archivos y elementos que queremos analizar dentro de una carpeta o del propio dispositivo sobre el que estamos investigando, podemos ver desde los archivos que se encuentran en el dispositivo como los que han podido ser eliminados.

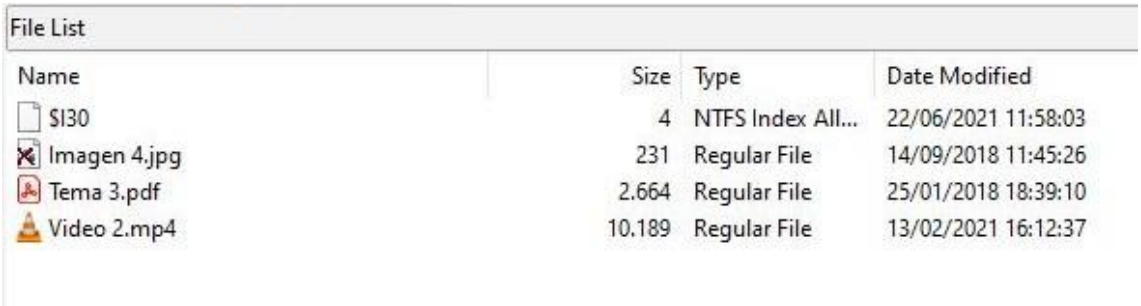


Ilustración 15. Lista de archivos y ficheros

Como hemos visto, una vez que tenemos un elemento para analizar, la interfaz cambia para poder mostrarnos toda la información que necesitemos para poder realizar nuestro análisis forense.

3.5 Creación de imagen de evidencia

Hemos visto cómo se funciona el software FTK Imager cuando analizamos un dispositivo directamente, sin embargo, esto en algunos casos no puede realizarse de esta manera ya que no podemos arriesgarnos a trabajar con el elemento original.

En estos casos lo que se debe hacer es una imagen del dispositivo con el que queremos trabajar, de esta manera conseguiremos una copia idéntica de este y evitaremos cualquier problema de borrado o corrupción con el dispositivo principal. Para realizar la imagen de la evidencia y que quede registrado de una forma correcta para una futura investigación es los siguiente.
Primero, una vez que tenemos conectado el dispositivo en nuestro ordenador, deberemos ir a la barra de navegación y seleccionar la pestaña *File* (Ilustración 4) y dentro de las opciones seleccionar *Create Disk Image*. Una vez que seleccionamos *Create Disk Image* nos aparecerá la siguiente ventana emergente de selección de elementos.

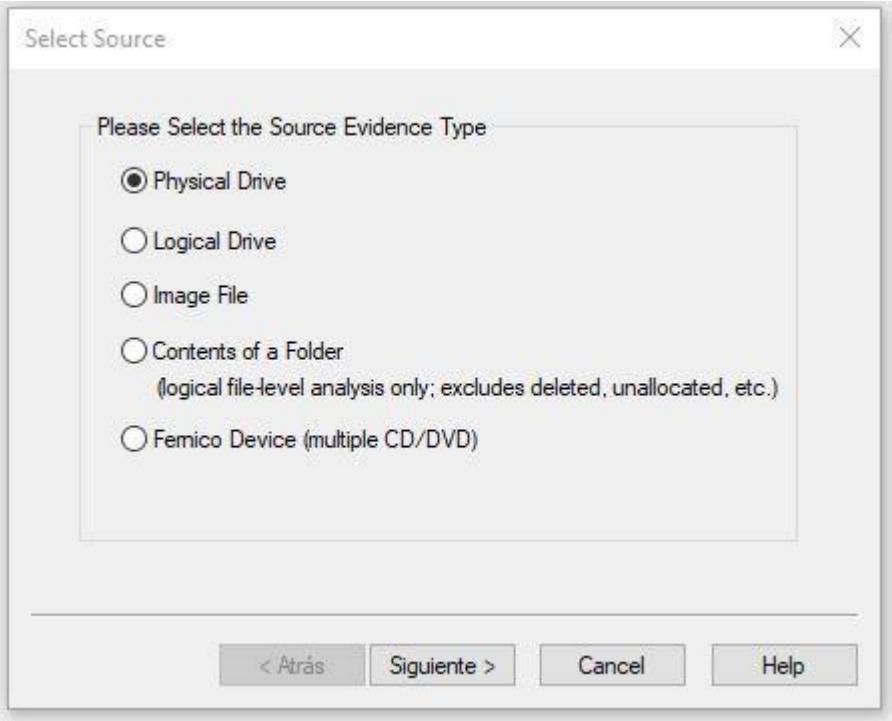


Ilustración 16. Selección de elemento

En nuestro caso, para ver cómo funciona vamos a seleccionar un *Physical Drive* ya que vamos a utilizar un pendrive para explicar este proceso, igual que en la Ilustración 10. Seleccionamos nuestro dispositivo y nos aparecerá la siguiente ventana:

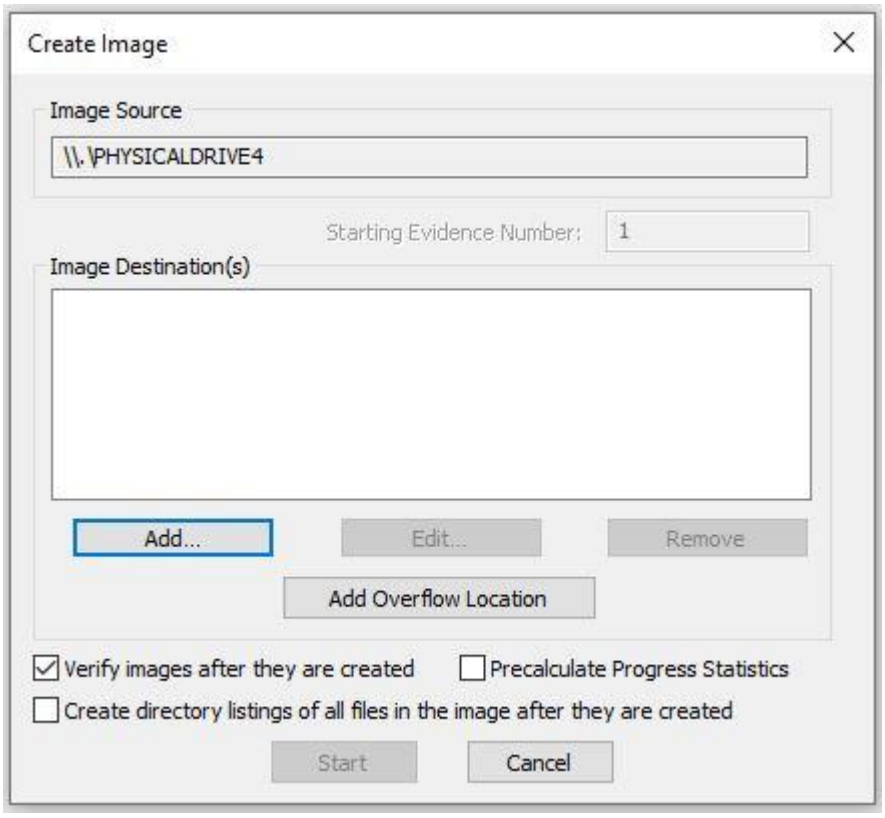


Ilustración 17. Creación de imagen

Una vez que nos sale esta ventana lo que tenemos que hacer es pulsar sobre el botón *"Add.."* y nos aparecerá otra ventana en la que se nos pedirá que seleccionemos entre las diferentes formas que tiene FTK Imager de realizar la copia de la evidencia.

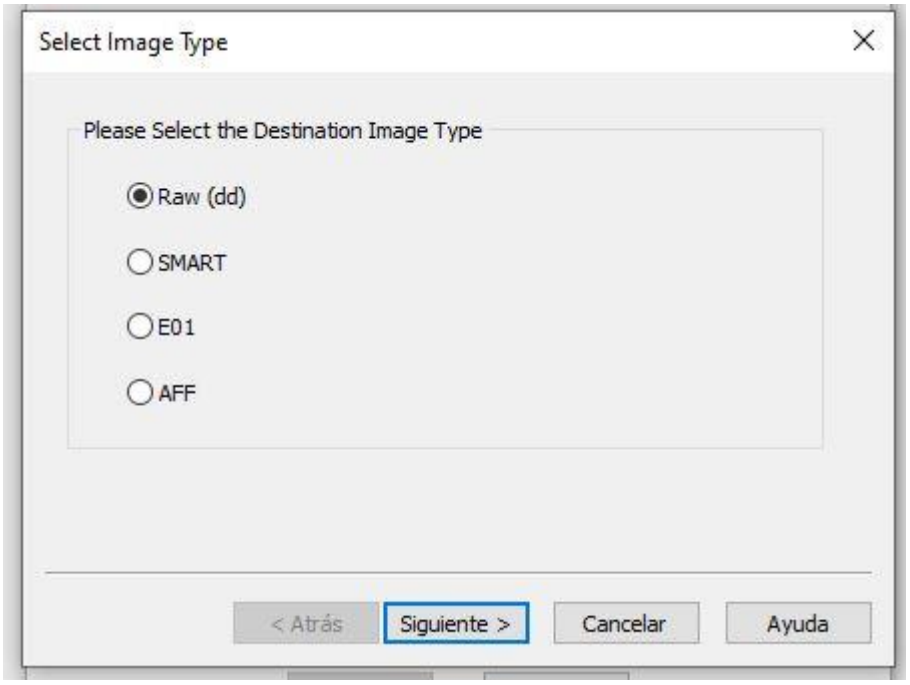


Ilustración 18. Tipos de imágenes de evidencias

Dependiendo de qué tipo de investigación se esté realizando con el dispositivo seleccionaremos un tipo de imagen u otro. Dentro de estos tipos de imagen hay que destacar la opción **Raw**, en la que se realizará una copia de todo el contenido del dispositivo tal cual, ya que es una copia exacta del dispositivo. Esta es la opción que vamos a seleccionar, ya que vamos a querer tener una copia tal cual de nuestro dispositivo. Una vez que hemos seleccionado la opción de imagen, nos aparecerá otra ventana en la que se nos pedirá rellenar unos campos de información para saber quién es el que ha realizado esta evidencia, el número de evidencia (suponiendo que se han realizado varias) y una pequeña descripción. Esto sirve principalmente para tener un control sobre las evidencias que podamos llegar a estar trabajando.

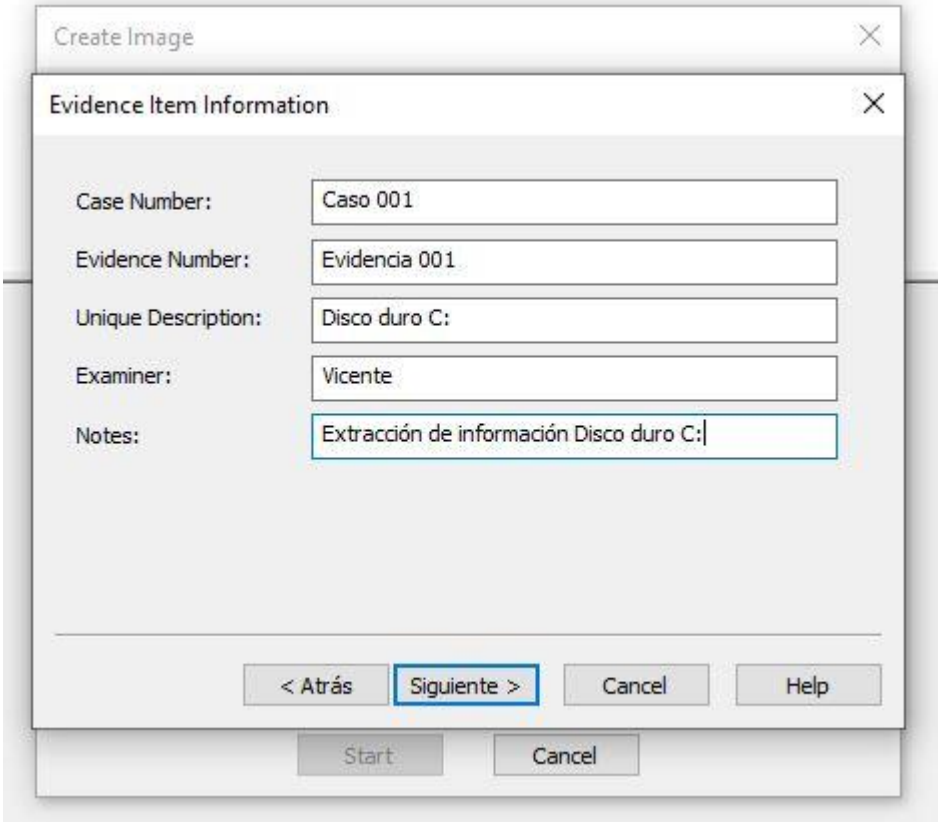


Ilustración 19. Información de la evidencia

Por último, una vez que ya hemos puesto la información de nuestra evidencia, se nos abrirá una última ventana en la que se nos pedirá que seleccionemos el lugar en nuestro ordenador donde queremos guardar la evidencia, así como el nombre de archivo que tendrá la evidencia.

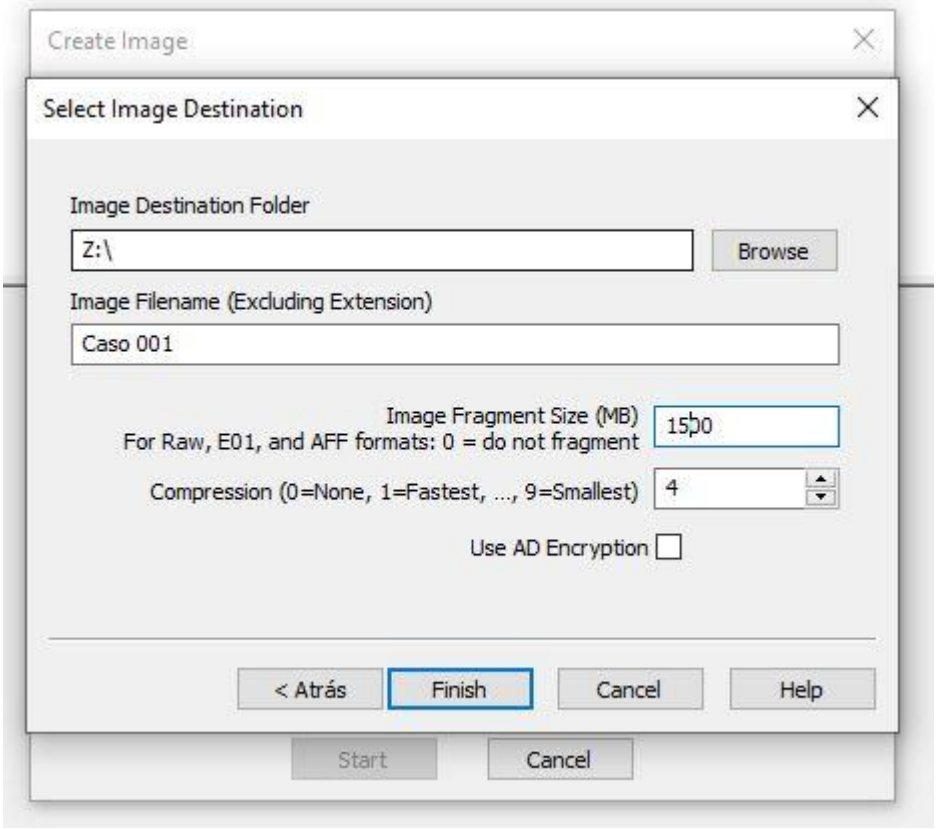


Ilustración 20. Selección de destino de imagen de evidencia

Además, podemos fragmentar la evidencia para que sea más sencillo a la hora de generarla, o también podemos no fragmentarla. En nuestro caso hemos decidido no fragmentarla para tener todo en un solo archivo. Es importante tener en cuenta que al no fragmentar la imagen está tardará más en generarse que si la fragmentásemos.
Una vez que hemos puesto los datos que se nos pedía, pulsamos en el botón **Finish** y luego el botón **Start** y FTK Imager comenzará a realizar la imagen de la evidencia según nuestras condiciones.

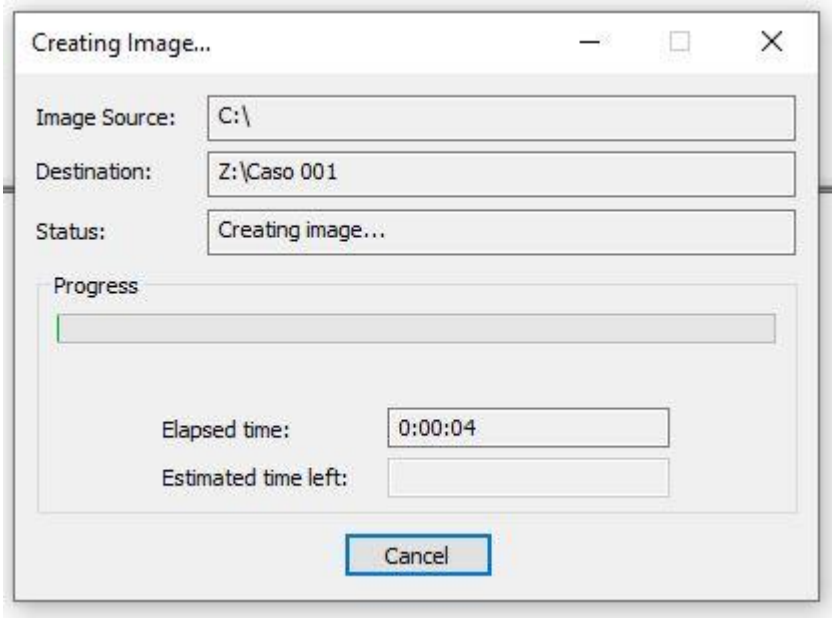


Ilustración 21. Proceso de creado de imagen de evidencia

Cuando acaba el proceso de creado de imagen de la evidencia, en nuestro caso del pendrive, tendremos

dos archivos en la ruta en la que hemos decidido generar la imagen, un archivo zip que va a ser la imagen que hemos creado, y un archivo de texto en el que vamos a tener toda la información técnica de la imagen.

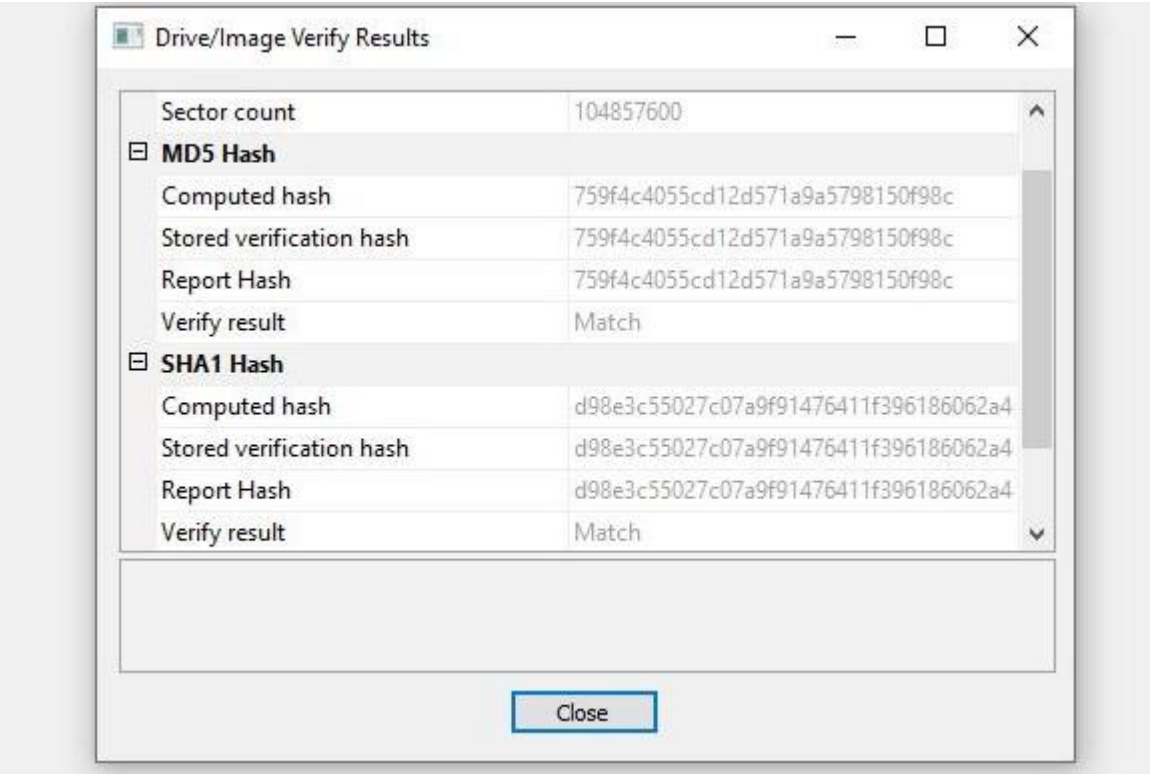


Ilustración 22. Verificación de resultados

Si seleccionamos ese archivo desde FTK Imager, seleccionando la opción de **Image File** de la Ilustración 9, veremos que se nos muestra todo el contenido que tenía nuestro pendrive a la hora de haberle realizado la copia.

Herramientas importantes

Hemos visto cómo funciona en términos generales FTK Imager, para la realización de investigaciones forenses sobre imágenes y dispositivos, hemos visto como tiene diferentes herramientas para poder realizar estas investigaciones forenses, sin embargo, FTK Imager cuenta con una herramienta, principalmente, que debemos de hablar de ella, ya que es una herramienta muy potente para algunas situaciones. Esta herramienta es **Capture Memory**. Capture Memory es una herramienta que nos permite capturar la memoria RAM del dispositivo en el que se está ejecutando FTK Imager.

4.1 Captura de memoria (Capture Memory)

Capture Memory, es una opción dentro de FTK Imager con la que podemos capturar la memoria RAM del ordenador en el que estamos ejecutando la aplicación.

Esta opción es útil cuando al realizar una investigación forense queremos obtener toda la información posible de un ordenador que se encuentra encendido y en funcionamiento, ya que capturando la memoria podemos obtener más datos que pueden complementar lo obtenido de los discos duros del ordenador.

Esto solo funcionará siempre y cuando no se reinicie ni se apague la sesión en la que está analizando FTK Imager, ya que al capturar la memoria RAM esta es volátil y no guarda los datos de una sesión a otra. Es por eso por lo que utilizando esta opción podemos guardar de manera permanente los datos que hay en la memoria en el momento en la que la capturamos para un posterior análisis forense.

Lo que tenemos que hacer para poder obtener toda la información de la memoria del ordenador es seleccionar la opción de **Capture Memory** en FTK Imager, pulsando sobre el icono en la barra de tareas o en la opción **Capture Memory** de la Figura 4. Una vez que hemos pulsado en el icono, nos aparecerá la siguiente ventana:

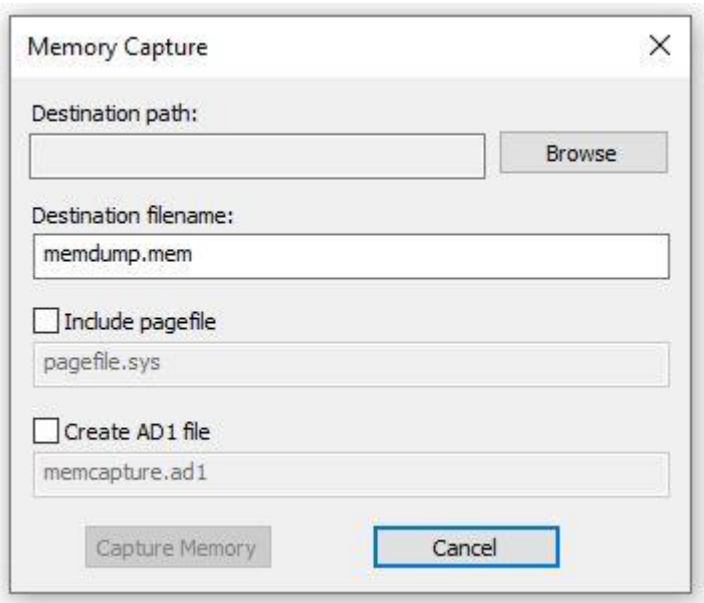


Ilustración 23. Captura de memoria RAM

Una vez que nos aparece esta ventana vemos que tenemos varias cosas. La primera es el directorio en el que se va a volcar toda la memoria para poder tenerla posteriormente, el segundo recuadro es para poner el nombre que queremos que tenga el archivo que generemos, siendo el nombre por defecto el que aparece.

Y por último tenemos dos opciones que podemos activar, que son incluir el **pagefile** y crear el **AD1 file.** El **pagefile** es la obtención de los datos del fichero pagesile.sys que contiene toda la información temporal de la memoria RAM y que es utilizado por Windows para guardar de manera temporal los datos de la memoria RAM. Y **AD1 file** es la opción con la que se crea una imagen forense de tipo AD1 para posteriormente analizarla con FTK Imager.

En nuestro caso vamos a seleccionar las dos opciones para obtener la mayor información posible de nuestra memoria RAM. Una vez que hemos pulsado el botón **Capture Memory**, FTK Imager comenzará a realizar el volcado de la memoria.

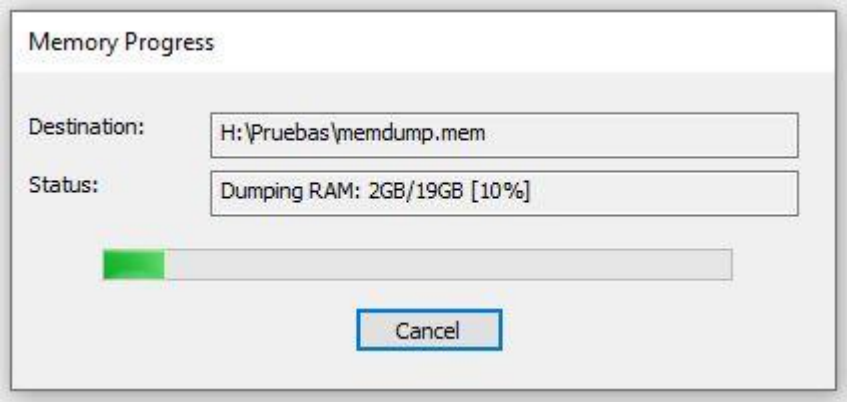


Ilustración 24. Volcado de memoria

Algo que resulta interesante al realizar el volcado de memoria es que muestra que está volcando 19GB de memoria RAM, cuando yo realmente sé que tengo 16GB de memoria RAM físicamente. Esto puede deberse a que está capturando memoria virtual, que puede ser mayor a la memoria física que tiene el ordenador, ya que en la memoria virtual puede haber parte de la capacidad que sea del disco duro y parte de la memoria RAM.

Una vez que ha acabado el volcado de la memoria vemos que ha creado los archivos de la siguiente imagen:

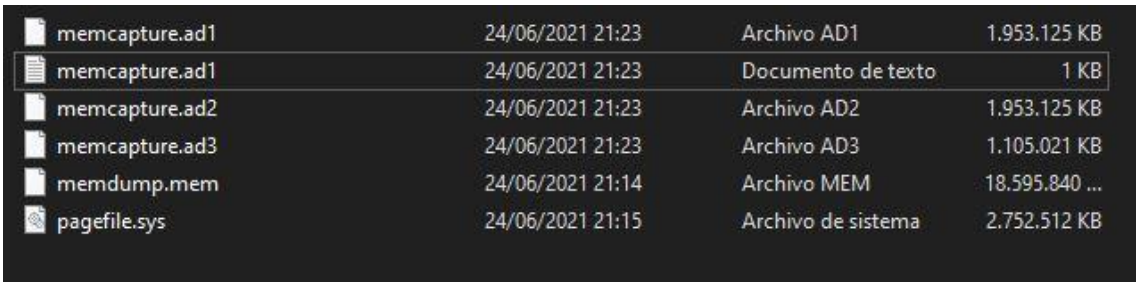


Ilustración 25. Archivos de volcado de memoria

Vemos que son 1 fichero de texto en el que se nos muestra toda la información de la creación del volcado de memoria, 1 fichero .mem que es la memoria RAM que hemos capturado, 1 fichero pagefile.sys, que es la copia del archivo del sistema que tiene el mismo nombre, y por último 3 ficheros .ad1, .ad2 y .ad3 que son las imágenes forenses que se han fragmentado en 3 (al ser ficheros grandes no se ha generado uno solo).

Si ahora nos vamos a FTK Imager y decidimos abrir estos ficheros y analizarlos nos aparece lo siguiente:

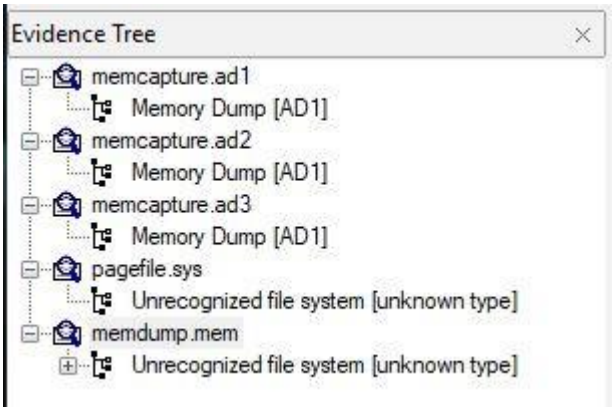


Ilustración 26. Análisis de volcado de memoria

Al poner todos los elementos que hemos obtenido vemos que el archivo **pagefile.sys** y **memdump.mem** no son capaces de ser reconocidos por FTK Imager, pero a pesar de ello siempre se puede utilizar en una investigación forense otras herramientas en caso de necesitar más información de los datos que hemos obtenido. Por otro lado, los tres archivos **memcapture** si muestran información, pero muestran los archivos pagefile.sys y memdump.mem. Si estos los seleccionamos para investigarlos, nos muestran una imagen como la de la figura 13, con símbolos que nosotros directamente nos son difíciles de entender de primera mano y sin ayuda de un software externo.

El uso de esta herramienta hemos visto que puede ser bastante beneficioso si la investigación forense que hay que realizar es muy exhaustiva, ya que con esto obtenemos mucha más información, sin embargo, nos encontramos con el problema de que para poder entender de manera más sencilla lo que hemos obtenido deberíamos de utilizar seguramente, otro software que fuese capaz de mostrarnos la información de una manera que fuese más legible para nosotros.

Creación del entorno de prueba para el análisis forense

Para poder llevar a cabo nuestro análisis forense, lo primero que vamos a hacer, es crear un entorno de pruebas seguro para ello.

La idea principal en este punto es crear una máquina virtual que simule ser el ordenador que se ha incautado para la investigación de una persona sospechosa de cometer un atraco. Para ello se creará y se configurará el sistema operativo con diferentes archivos que simularán que la máquina sea el ordenador de un sospechoso en una investigación forense.

5.1 Descarga e instalación de elementos necesarios para el entorno de pruebas

5.1.1 Descarga ISO Windows 10

Lo primero que debemos de tener en cuenta a la hora de crear el entorno de pruebas es, el programa que vamos a utilizar para la creación de la máquina virtual y el sistema operativo que vamos a montar en la máquina virtual. En este caso el programa que vamos a utilizar para crear la máquina virtual es VirtualBox, y el sistema operativo Windows 10.

Lo primero que debemos de hacer es descargar el sistema operativo Windows 10. Para ello debemos de ir al siguiente enlace: https://www.microsoft.com/es-es/software-download/windows10 . En este enlace nos aparecerán dos opciones, una que pone actualizar ahora, y otra en la que pone descargar ahora la herramienta. Pulsaremos sobre la segunda.

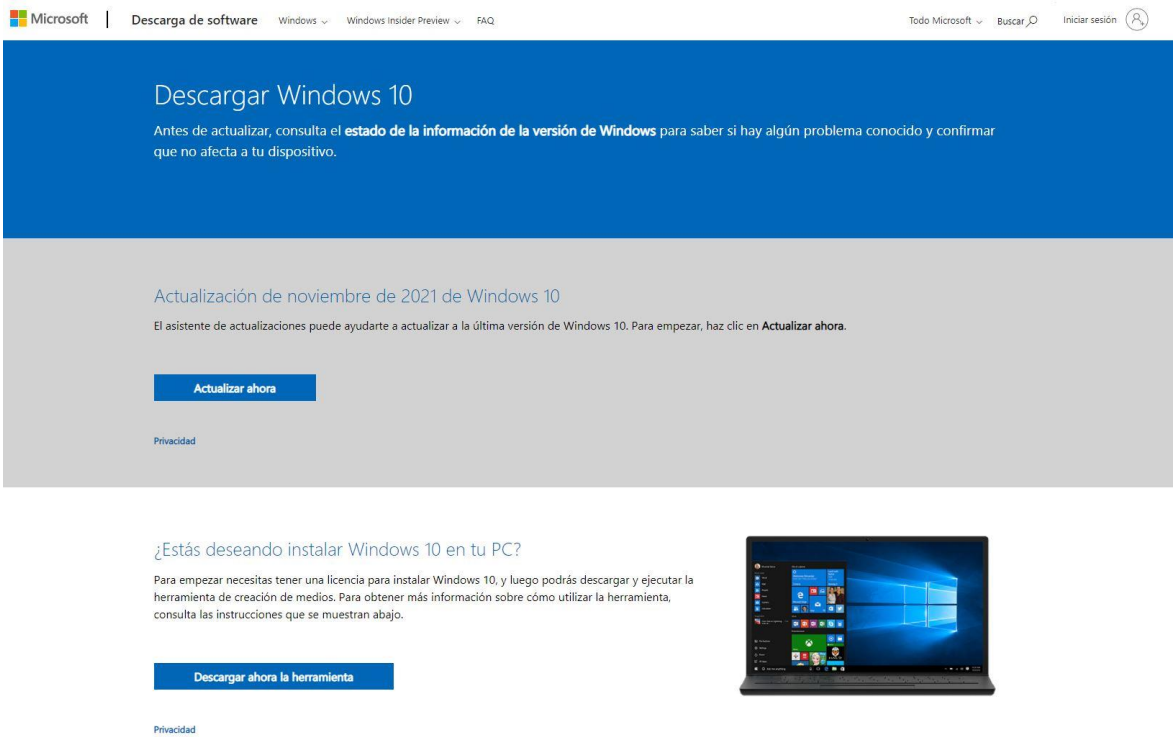


Ilustración 27. Página de descarga ISO Windows

Una vez que pulsamos sobre la opción, se nos descargará un ejecutable, que deberemos de abrir.

Ilustración 28. Ejecutable ISO Windows

El programa se empezará a ejecutar, y nos dará dos opciones, una opción en la que nos actualizará el equipo en el que hemos descargado el programa, y una segunda opción para crear un medio de instalación. En nuestro caso lo que queremos es crear un medio de instalación, por lo que seleccionaremos la segunda opción.

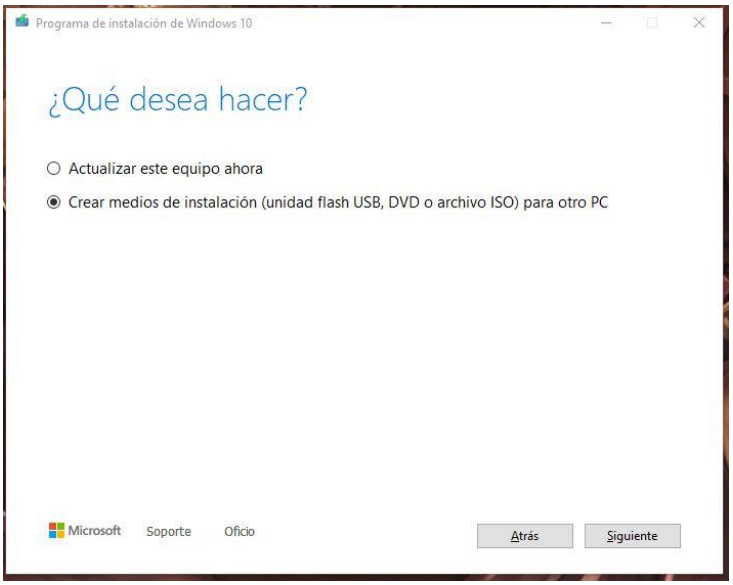


Ilustración 29. Creación de medios de Windows

Al seleccionar la segunda opción y pulsar siguiente nos aparecerá una ventana en la que se nos pedirá que seleccionemos las características que va a tener la versión de Windows 10 que vamos a descargar. En este caso vamos a utilizar la opción de usar las opciones recomendadas para este equipo. Cuando hayamos seleccionado esa opción aparecerá una nueva pestaña en la que nos pedirá que elijamos un medio para instalar Windows. Nosotros seleccionaremos la opción de Archivo ISO, ya que descargaremos el archivo en el ordenador, para más adelante usarlo en la máquina virtual que creemos.

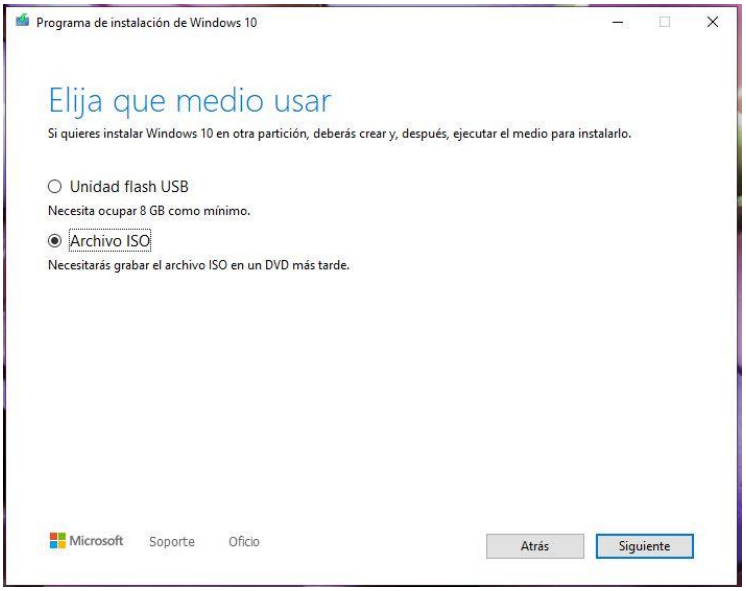


Ilustración 30. Archivo ISO Windows

Una vez que seleccionemos la opción se nos pedirá que seleccionemos una ubicación en nuestro ordenador, en la que se descargará la ISO. Una vez que haya terminado la descarga, tendremos ya el archivo ISO para poder utilizarlo en nuestra máquina virtual.

5.1.2 Descarga e instalación de VirtualBox

Teniendo ya descargado el sistema operativo, lo siguiente que debemos de hacer es descargarnos el programa para instalar la máquina virtual en nuestro ordenador, para ello debemos de ir a la siguiente página: https://www.virtualbox.org , en esta página pulsamos sobre el botón de Download.

Ilustración 31. Página de descarga VirtualBox

Al pulsar sobre el botón se nos abrirá una nueva página en la que deberemos de seleccionar el sistema operativo para el que vamos a descargar la máquina virtual, Windows en nuestro caso.

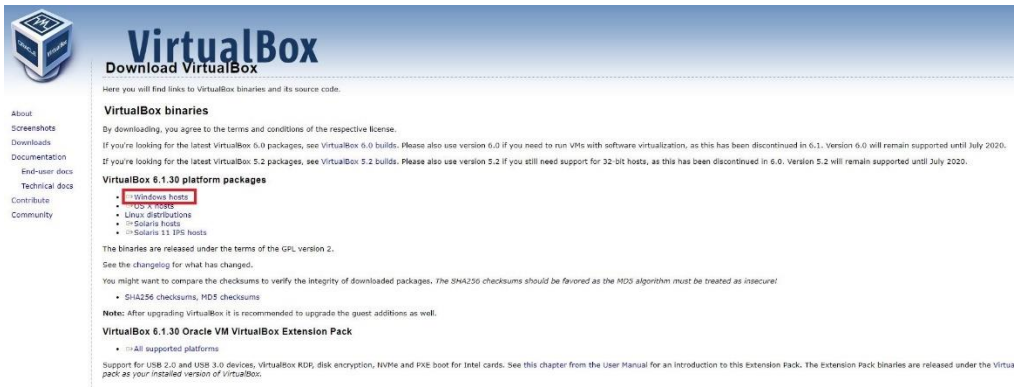


Ilustración 32. Descarga VirtualBox para Windows

Pulsamos sobre la opción de Windows y se nos descargará el ejecutable para instalar el programa en nuestro ordenador.

Ilustración 33. Ejecutable VirtualBox

Ejecutamos el programa, y se nos iniciará el instalador de VirtualBox. Lo primero que nos aparecerá, serán las opciones de instalación del programa, como la ruta de instalación, o las diferentes opciones del programa.

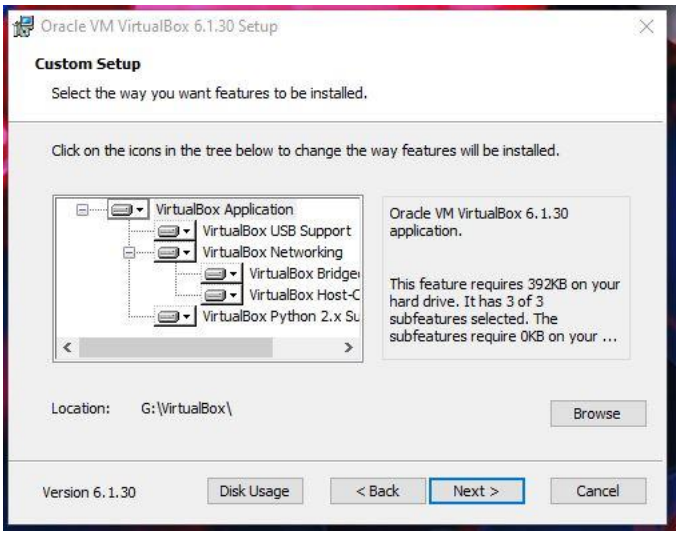


Ilustración 34. Opciones de instalación de VirtualBox

Seleccionamos la ruta en la que queremos instalar el programa y le damos a **next**. Nos aparecerá una nueva ventana en la que se nos pedirá que seleccionemos algunas opciones, si queremos. En este caso podemos darles a todas las opciones que sí.

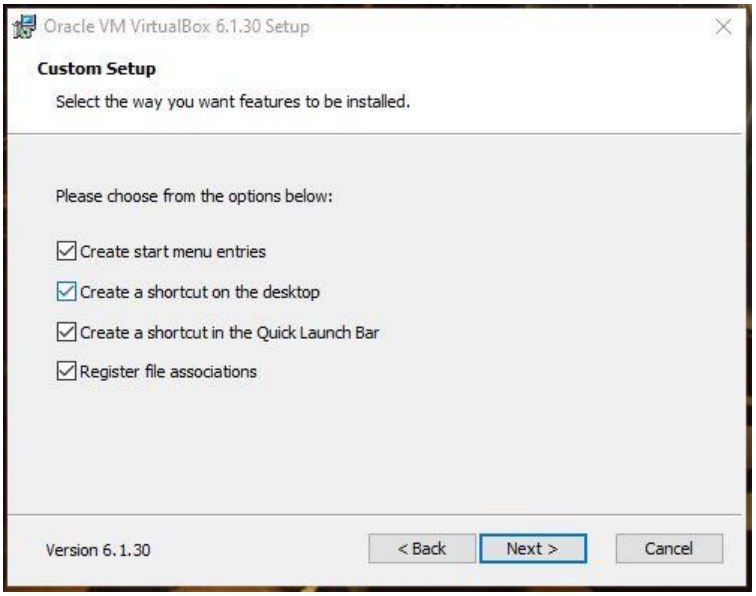


Ilustración 35. Segundas opciones instalación VirtualBox

Pulsamos **next** y nos aparecerá una ventana de confirmación de instalación, y le damos al botón **install**. Se nos empezará a instalar el programa automáticamente.

Una vez que tengamos el programa instalado podremos crear nuestra máquina virtual para nuestro entorno de pruebas.

5.2 Creación entorno de prueba en VirtualBox

Teniendo ya descargado el sistema operativo, e instalado el programa de máquina virtuales, podemos crear nuestro entorno de pruebas.

Lo primero que debemos de hacer es iniciar el programa VirtualBox. Una vez iniciado nos aparecerán varias opciones.

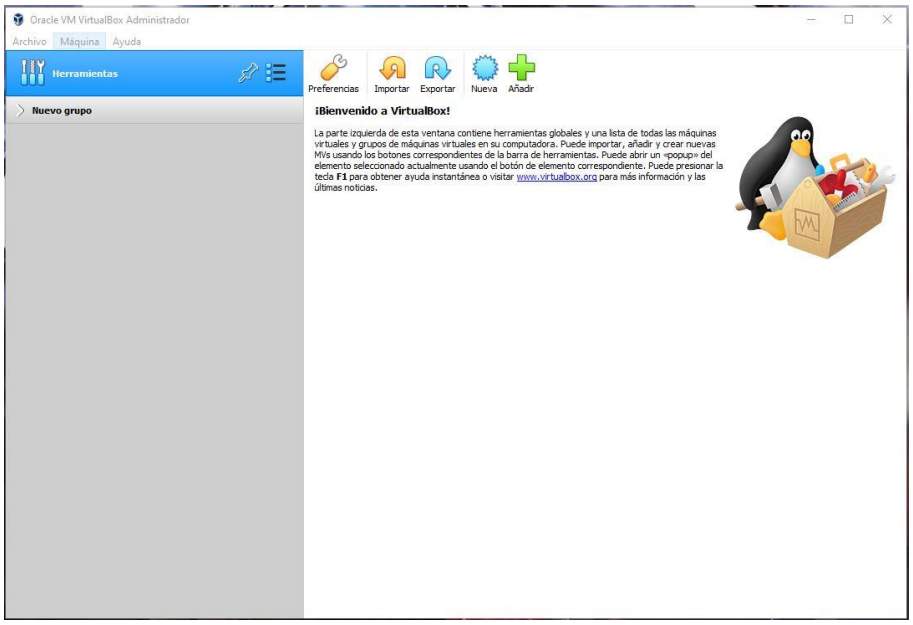


Ilustración 36. Página de inicio VirtualBox

Para crear nuestra máquina virtual deberemos de pulsar sobre la opción nueva, que nos aparece en la ilustración 35. Una vez que hemos pulsado sobre esa opción se nos abrirá una ventana en la que se nos pedirá un nombre para la máquina virtual, un lugar de instalación, y el tipo de sistema que se va a instalar. Nosotros vamos a poner, como nombre Entorno de Pruebas, y como sistema a instalar Windows 10.

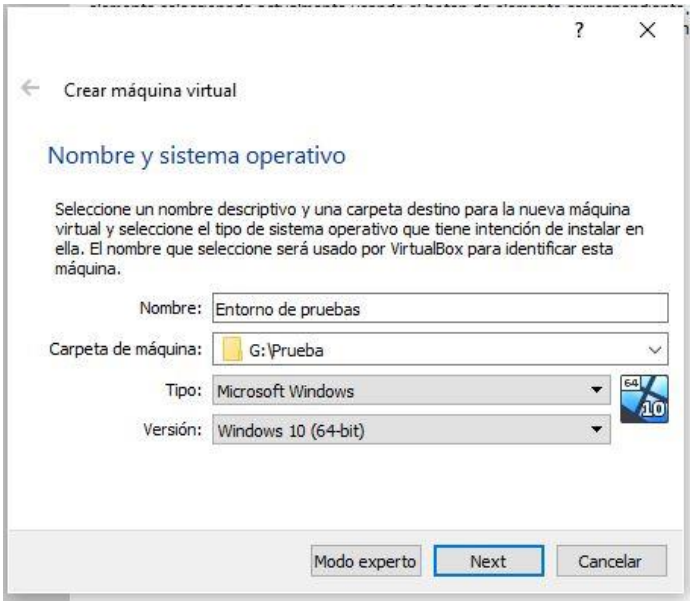


Ilustración 37. Creación máquina virtual

Al pulsar next nos aparecerá una ventana nueva en la que deberemos de seleccionar la cantidad de memoria RAM para nuestra máquina. En nuestro caso, vamos a seleccionar entorno a unos 12 GB de memoria RAM, ya que esto nos permitirá obtener más información de cara a las pruebas que se realicen, ya demás estaremos dentro de los parámetros de seguridad que nos marca VirtualBox para que no haya problemas de rendimiento con la máquina virtual.

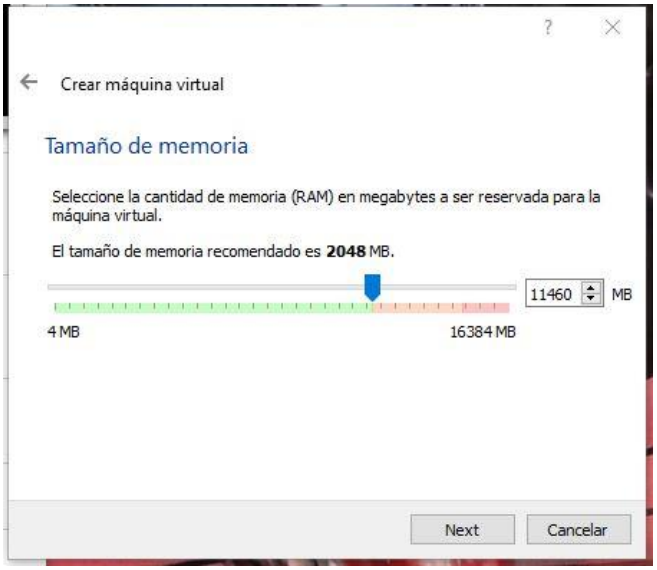


Ilustración 38. Selección de memoria RAM

Una vez que hemos seleccionado la cantidad de memoria RAM, pulsamos **next** y se nos aparecerá una ventana en la que deberemos de crear un disco físico para la máquina, no crearlo o usar uno ya existente. En nuestro caso vamos a crear uno nuevo.

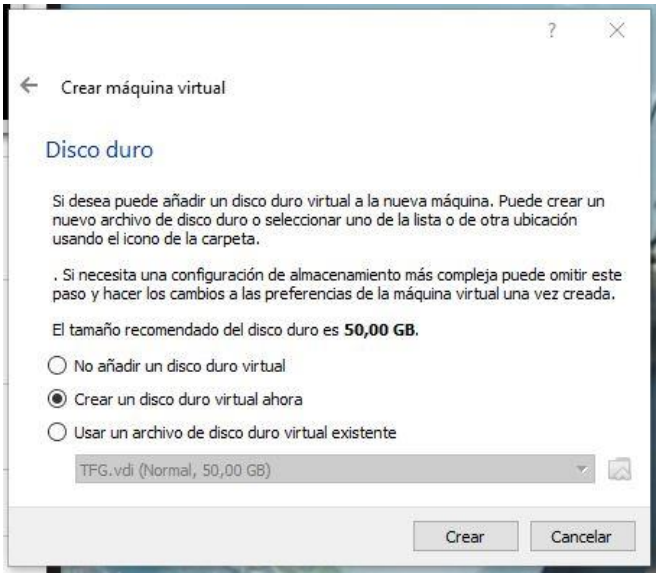


Ilustración 39. Creación disco Máquina Virtual

Pulsamos sobre el botón crear y se nos abrirá una nueva ventana en la que nos pedirá el tipo de archivo de disco duro. Nosotros seleccionaremos la opción VDI.

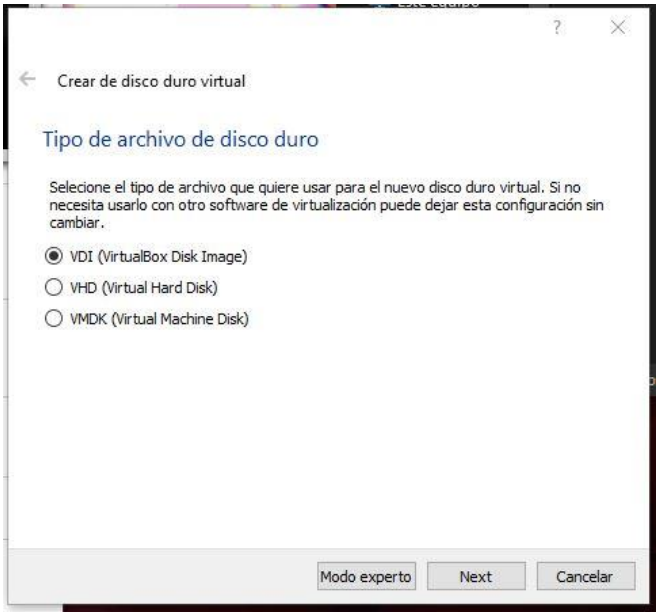


Ilustración 40. Archivos de disco duro

Al pulsar **next** aparecerá otra nueva pestaña en la que se nos pedirá elegir entre crear el disco con espacio dinámico o con un tamaño fijo, para nuestra máquina virtual seleccionaremos la opción de tamaño fijo.

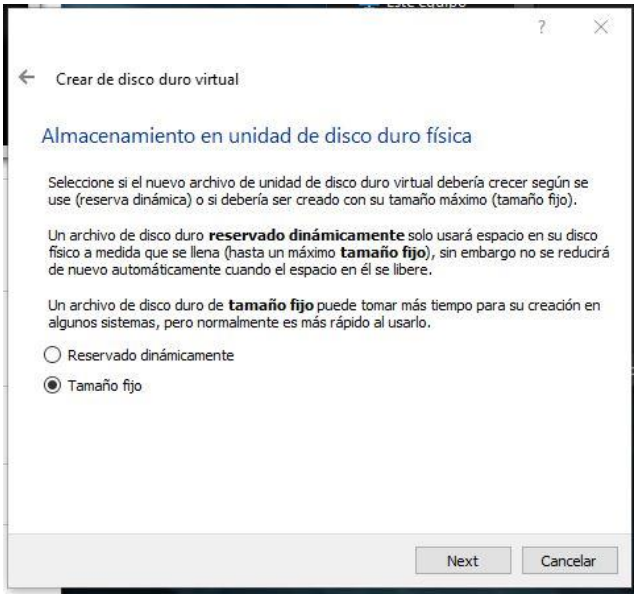


Ilustración 41. Tipo de almacenamiento

Pulsamos **next**, y nos aparecerá otra ventana en la que se nos pedirá que seleccionemos la cantidad de almacenamiento que queremos para la máquina virtual. Lo mínimo recomendado es 50 GB, pero nosotros vamos a poner 60 GB, por tener un poco más.

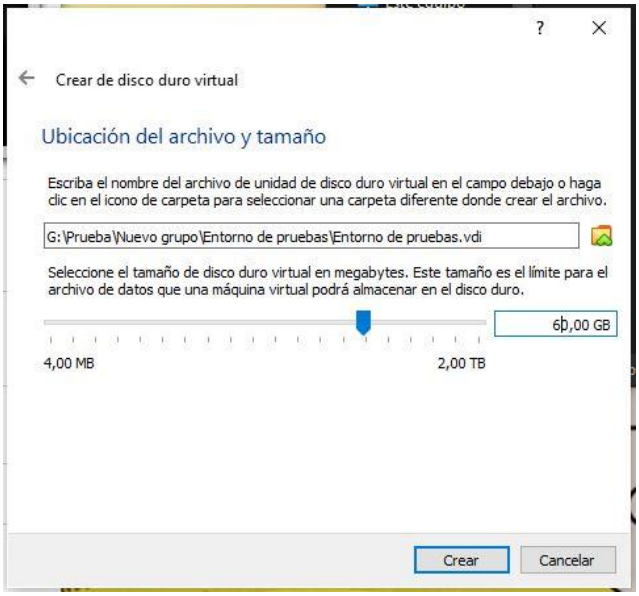


Ilustración 42. Cantidad de almacenamiento

Pulsamos crear, y se nos creará el disco duro para la máquina de nuestro entorno de pruebas.

Una vez que se nos ha creado el disco virtual, volveremos a la ventana de inicio de VirtualBox, ahí nos aparecerá la máquina virtual que hemos creado.

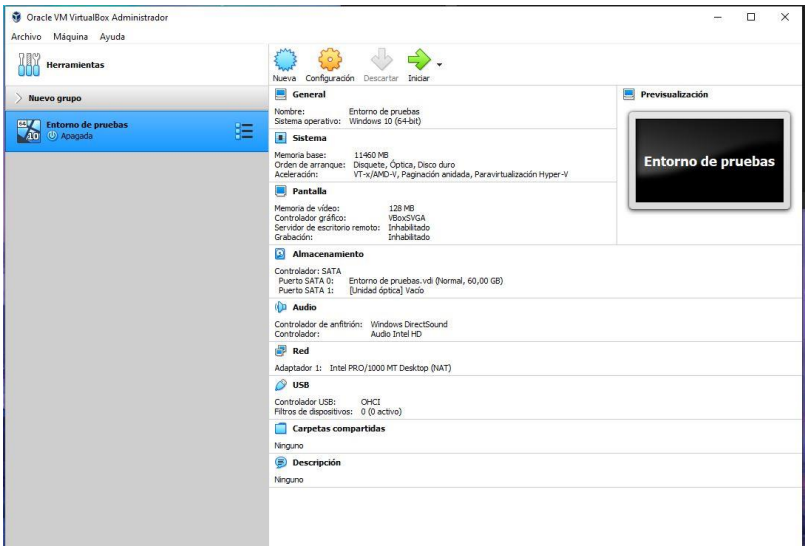


Ilustración 43. Máquina virtual

Antes de iniciar la máquina virtual e instalar el sistema operativo, vamos a cambiar algunas cosas de la configuración del sistema, para que el entorno de pruebas funcione mejor. Para ello vamos a pulsar en la opción de configuración de nuestra máquina virtual. Nos aparecerá una ventana con los ajustes de nuestra máquina, y pulsaremos sobre la opción sistema.

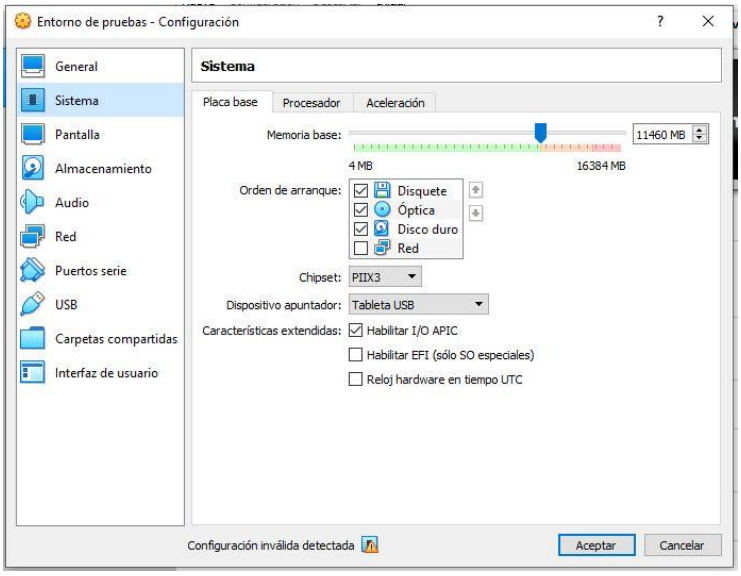


Ilustración 44. Ajustes máquina virtual

Dentro del ajuste de sistema pulsaremos sobre la opción de procesador y seleccionaremos en la barra de procesador 4.

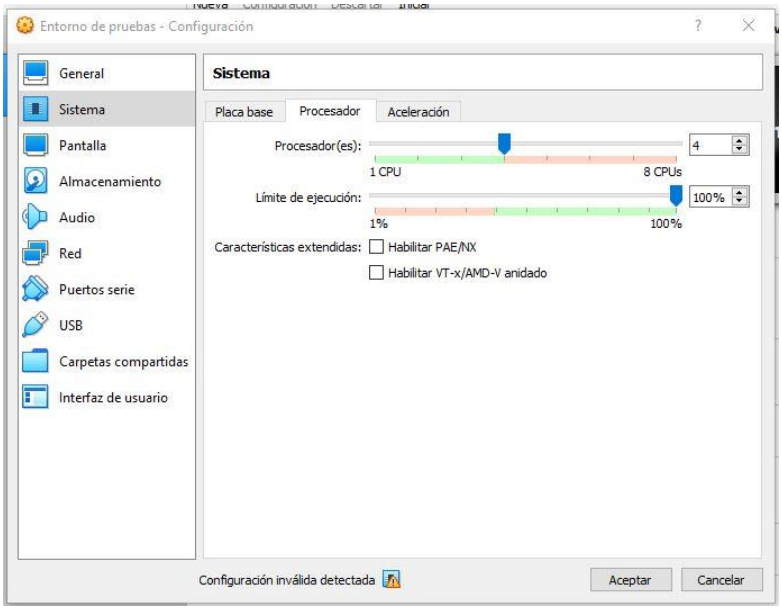


Ilustración 45. Procesadores máquina virtual

Una vez que hemos cambiado este ajuste pulsamos aceptar y volveremos a la pantalla principal de VirtualBox. En la pantalla de VirtualBox, pulsaremos iniciar para instalar el sistema operativo.

Al pulsar iniciar se nos pedirá que seleccionemos un disco de inicio, en nuestro caso será el disco de Windows que hemos descargado siguiendo los pasos del punto ***5.1.1 Descarga ISO Windows 10***.

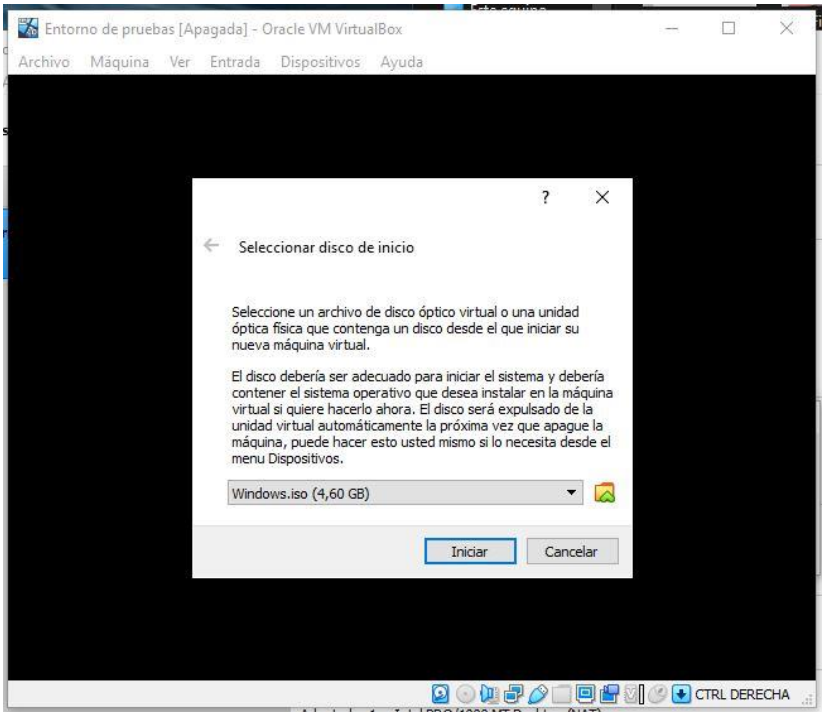


Ilustración 46. Selección disco de inicio máquina virtual

Una vez que hemos seleccionado nuestro archivo ISO de Windows, pulsamos iniciar y nuestra máquina virtual comenzará a iniciar el proceso de instalación de Windows.

Desde aquí se nos iniciará el proceso de instalación de Windows, se seguirán los pasos que nos indique y se creará una cuenta local con el nombre de usuario Paco. Esta instalación será una instalación limpia, ya que más adelante rellenaremos el sistema con archivos y datos que deberemos de obtener y analizar con el software forense FTK Imager, los únicos programas que se instalarán será el programa de FTK Imager y un navegador web.

Análisis de evidencias del entorno de pruebas con FTK Imager

En este entorno de pruebas que hemos creado, como hemos visto antes, vamos a suponer que es el ordenador de una persona que es sospechosa de cometer delitos de robos. En este punto vamos a ver hasta dónde puede llegar el software FTK Imager en el análisis de pruebas forenses, y los pasos que podría seguir un investigador forense para obtener la mayor información del entorno de pruebas como si del ordenador de la persona que ha sido detenida se tratase.

6.1 Archivos que se van a analizar

Cuando se realiza una investigación forense, lo primero que se debe hacer es recopilar la información y crear diferentes archivos de investigación, nunca trabajar sobre la prueba original, ya que si se realizan modificaciones sobre la prueba original esta no podría servir en un juicio, además de que podríamos perder información importante.

Debido a eso, lo que tenemos que hacer es seguir los pasos del punto ***3.5 Creación de evidencia*** para realizar la copia de la evidencia del disco duro del sistema para analizar, y del punto ***4.1 Captura de Memoria (Capture Memory)*** para realizar la captura de memoria RAM también.

Una vez que hemos realizado estas copias, tenemos los siguientes archivos para analizar e investigar:

- **El archivo *Caso 001.E01*:** Se trata de una copia íntegra del disco C: del ordenador del sospechoso, en él se encuentran todos los documentos y programas que contiene el ordenador del sospechoso.
- **El archivo *Datos de búsquedas.mem*:** Es un archivo que cuenta con una copia de la memoria RAM del ordenador en un momento en específico en el que se encontraba el navegador del sospechoso abierto con diferentes páginas web.
- **El archivo *Información correo.mem***: Este archivo es otro archivo que cuenta con una copia de la memoria RAM, pero en este caso el ordenador solo contaba con información de un correo electrónico, que se había abierto en el navegador.

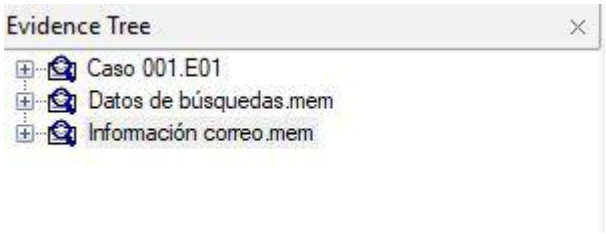


Ilustración 47. Elementos de investigación

6.2 Recopilación de información del disco duro

El primer archivo con el que vamos a empezar la investigación es el archivo ***Caso 001.E01***. Este archivo, como hemos mencionado antes, corresponde al disco duro C: del ordenador del sospechoso.

Al principio debemos de pensar por donde podemos empezar a buscar información, debemos de pensar que es un ordenador normal y donde se guardan normalmente los archivos. Lo primero que se nos puede venir a la mente es la carpeta de documentos que tiene cualquier ordenador con Windows. Esta carpeta está en la siguiente ruta en nuestro archivo de la evidencia: [root]\Users\Paco\Documents

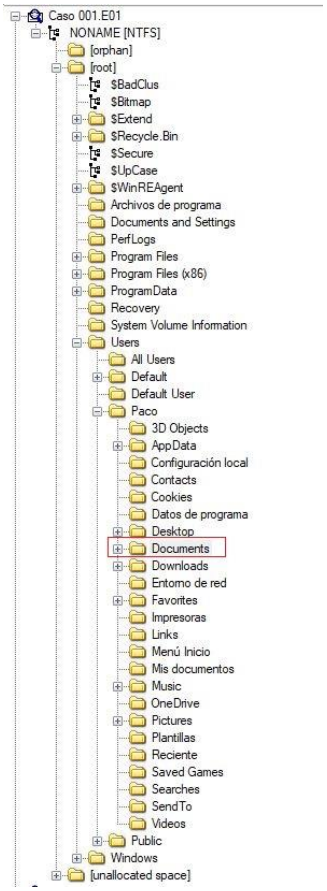


Ilustración 48. Ruta carpeta documentos

Dentro de esta carpeta encontramos otras subcarpetas que contienen datos de videojuegos, de archivos de programas de programación, imágenes, vídeos, etc. En principio no se ve nada raro, menos por una carpeta que tiene como nombre ***Información Confidencial***.

File List

Name	Size	Type	Date Modified
Assassin's Creed IV Black Flag	1	Directory	31/10/2021 18:28:52
Assassin's Creed Valhalla	1	Directory	31/10/2021 18:28:52
Call Of Duty Black Ops Cold War	1	Directory	31/10/2021 18:28:55
Codelite Projects	1	Directory	31/10/2021 18:28:59
Información Confidencial	1	Directory	22/12/2021 11:28:27
Mi música	1	Reparse Point	16/09/2021 18:26:57
Mis imágenes	1	Reparse Point	16/09/2021 18:26:57
Mis vídeos	1	Reparse Point	16/09/2021 18:26:57
NetBeansProjects	1	Directory	31/10/2021 18:29:14
Plantillas personalizadas de Office	1	Directory	31/03/2021 10:57:09
Python Scripts	1	Directory	22/04/2021 18:10:02
$I30	4	NTFS Index All...	24/12/2021 11:54:59
desktop.ini	1	Regular File	16/09/2021 18:28:07

Ilustración 49. Subcarpetas de la carpeta documentos

Si accedemos a la carpeta de Información Confidencial, dentro podemos encontrar varios archivos interesantes. Un documento Excel que tiene como nombre *Bancos*, un documento Word con el nombre *Registro de coches,* y tres imágenes que tienen como nombre *Coche 1, Coche 2* y *Coche 3.*

File List

Name	Size	Type	Date Modified
$I30	4	NTFS Index All...	22/12/2021 11:28:27
Bancos.xlsx	11	Regular File	18/12/2021 12:02:47
Bancos.xlsx.FileSlack	2	File Slack	
Coche 1.JPG	214	Regular File	18/12/2021 12:08:46
Coche 1.JPG.FileSlack	3	File Slack	
Coche 2.JPG	165	Regular File	18/12/2021 12:29:39
Coche 3.JPG	94	Regular File	18/12/2021 12:37:30
Coche 3.JPG.FileSlack	3	File Slack	
Registro de coches.docx	488	Regular File	20/12/2021 11:31:47

Ilustración 50. Archivos carpeta Información Confidencial

Si analizamos, las fotos vemos que son solo fotos de 3 coches estacionados, lo que en principio no nos da mucha información.

Ilustración 51. Imágenes carpeta Información Confidencial

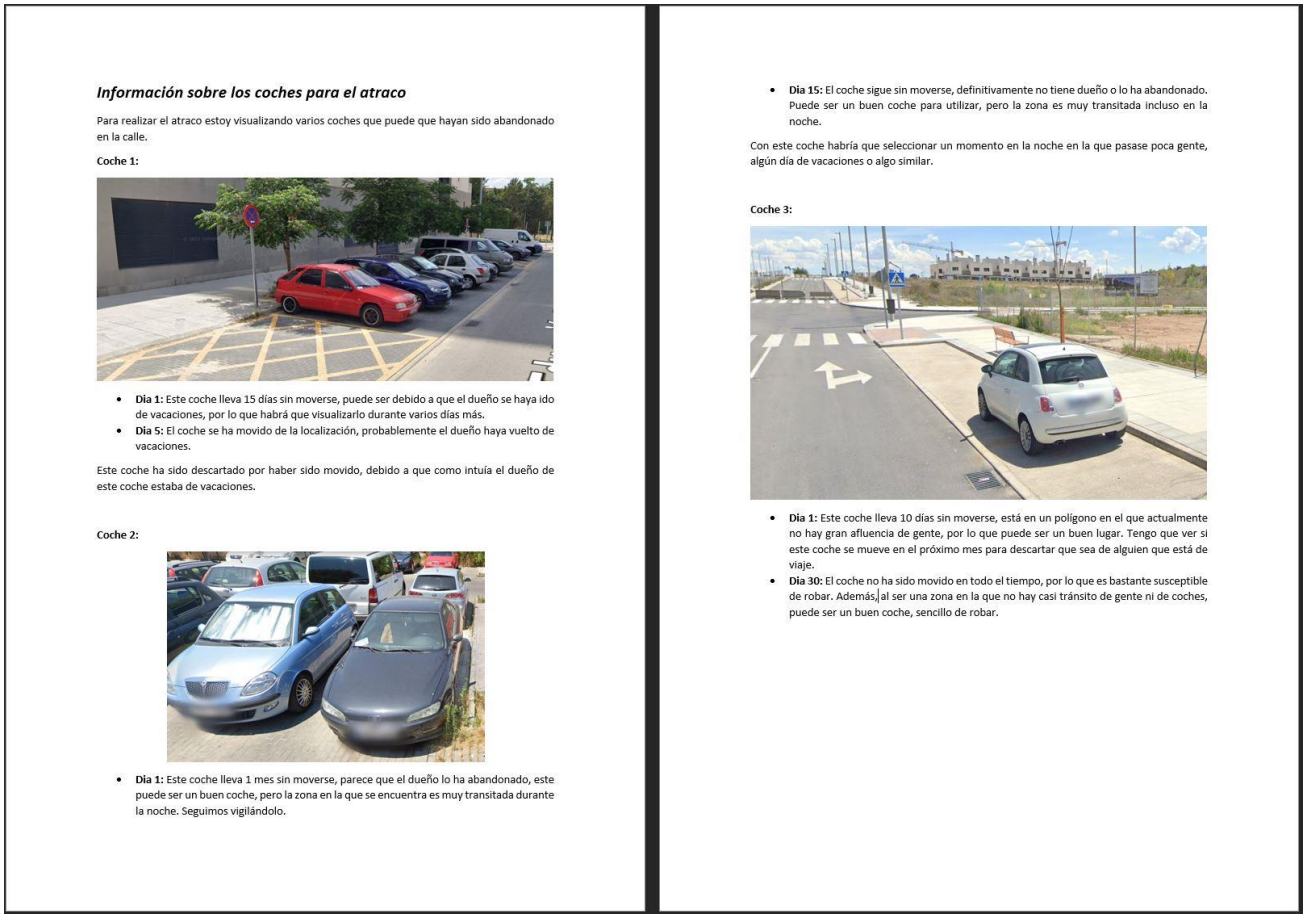
Si pasamos a analizar el archivo Excel y lo abrimos vemos que es un archivo Excel que contiene información sobre ciertas sucursales de bancos de la zona de Alcalá de Henares, Torrejón de Ardoz y San Fernando de Henares. Esto nos puede dar primeros indicios de que efectivamente esta persona puede estar obteniendo información para atracar algún banco, que es precisamente por lo que se le está realizando esta investigación forense.

Entidades bancarias

BANCO	DIRECCION	CIUDAD	ENTIDAD	SEGURIDAD
Santander	C. Antonio Machado, 1, 28805	Alcalá de Henares, Madrid	Santander	Alta
BBVA	Calle José María Pereda, 12, 28806	Alcalá de Henares, Madrid	BBVA	Media
Caixa Bank	Av. Reyes Católicos, 28-30, 28802	Alcalá de Henares, Madrid	Caixa Bank	Baja
Santander	PL. DE Europa, 1, 28850	Torrejón de Ardoz, Madrid	Santander	Alta
Caixa Bank	Av. de la Constitución, S/n, 28850	Torrejón de Ardoz, Madrid	Caixa Bank	Media
BBVA	C. Enmedio, 8, 28850	Torrejón de Ardoz, Madrid	BBVA	Alta
Sabadell	C. Marques de Alonso Martínez, 6, 28805	Alcalá de Henares, Madrid	Sabadell	Media
Caixa Bank	C. de la Libertad, 3, 28830	San Fernando de Henares, Madrid	Caixa Bank	Baja
Santander	Av. de Zarauz, 37, 28830	San Fernando de Henares, Madrid	Santander	Alta

Ilustración 52. Contenido archivo Bancos.xlsx

Nos queda por analizar el archivo Registro de coches de la carpeta. Si abrimos el archivo vemos que se trata de un documento Word en el que se encuentra un registro de si se han movido o no los diferentes coches de las imágenes que hemos visto antes. Este seguimiento vemos que indica si el coche está abandonado o no, lo que puede darnos una pista de que el sospechoso está intentando robar un coche abandonado, que probablemente quiera usar en alguno de sus próximos atracos.



Información sobre los coches para el atraco

Para realizar el atraco estoy visualizando varios coches que puede que hayan sido abandonado en la calle.

Coche 1:

- **Dia 1:** Este coche lleva 15 días sin moverse, puede ser debido a que el dueño se haya ido de vacaciones, por lo que habrá que visualizarlo durante varios días más.
- **Dia 5:** El coche se ha movido de la localización, probablemente el dueño haya vuelto de vacaciones.

Este coche ha sido descartado por haber sido movido, debido a que como intuía el dueño de este coche estaba de vacaciones.

Coche 2:

- **Dia 1:** Este coche lleva 1 mes sin moverse, parece que el dueño lo ha abandonado, este puede ser un buen coche, pero la zona en la que se encuentra es muy transitada durante la noche. Seguimos vigilándolo.
- **Dia 15:** El coche sigue sin moverse, definitivamente no tiene dueño o lo ha abandonado. Puede ser un buen coche para utilizar, pero la zona es muy transitada incluso en la noche.

Con este coche habría que seleccionar un momento en la noche en la que pasase poca gente, algún día de vacaciones o algo similar.

Coche 3:

- **Dia 1:** Este coche lleva 10 días sin moverse, está en un polígono en el que actualmente no hay gran afluencia de gente, por lo que puede ser un buen lugar. Tengo que ver si este coche se mueve en el próximo mes para descartar que sea de alguien que está de viaje.
- **Dia 30:** El coche no ha sido movido en todo el tiempo, por lo que es bastante susceptible de robar. Además, al ser una zona en la que no hay casi tránsito de gente ni de coches, puede ser un buen coche, sencillo de robar.

Ilustración 53. Contenido archivo Registro de coches.docx

Con la información de los archivos de la carpeta de Información confidencial, podemos empezar a sacar algo de información del sospechoso, como que tiene diferentes bancos vigilados y que opera en zonas concretas, así como que estaba vigilando varios coches abandonados para usar en los atracos. Esto también nos puede servir para más adelante saber que buscar concretamente en los elementos de memoria RAM que se han recopilado en la investigación.

6.3 Recopilación de información de la memoria

La información que hemos recopilado del disco duro C: del sospechoso nos sirve como un buen punto de partida para continuar con la investigación. Aprovechando las opciones que nos permite FTK Imager, podemos obtener información también de la memoria RAM y analizarla. En este caso hemos volcado la memoria RAM del ordenador del sospechoso y vamos a analizarla teniendo en cuenta la información de la que ya disponemos.

6.3.1 Análisis de volcado de memoria 1

Al realizar el volcado de la memoria RAM del ordenador del sospechoso se vio que no servía con un solo volcado para recopilar toda la información posible, por lo que se realizaron dos volcados. El primer volcado es el que tiene el nombre de archivo *Datos de búsquedas.mem*, y el segundo volcado es el archivo con nombre *Información correo.mem*.

En este apartado vamos a intentar recopilar la mayor información posible del primer volcado de memoria RAM, para ello lo primero que tenemos que hacer es añadir el archivo de la evidencia para analizarlo, esto tenemos que hacerlo siguiendo los pasos del punto ***3.3 Adicción de evidencia***.

Una vez que hemos realizado esto, en la parte inferior a la derecha nos aparecerán los datos del volcado de la memoria RAM. En nuestro caso para trabajar de una manera más cómoda y que sea más sencillo a la hora de visualizar la información haremos que FTK Imager nos visualice la información solo en formato texto. Para visualizar en solo texto deberemos de pulsar con el botón derecho del navegador sobre los datos y seleccionar la opción **Show Text Only**.

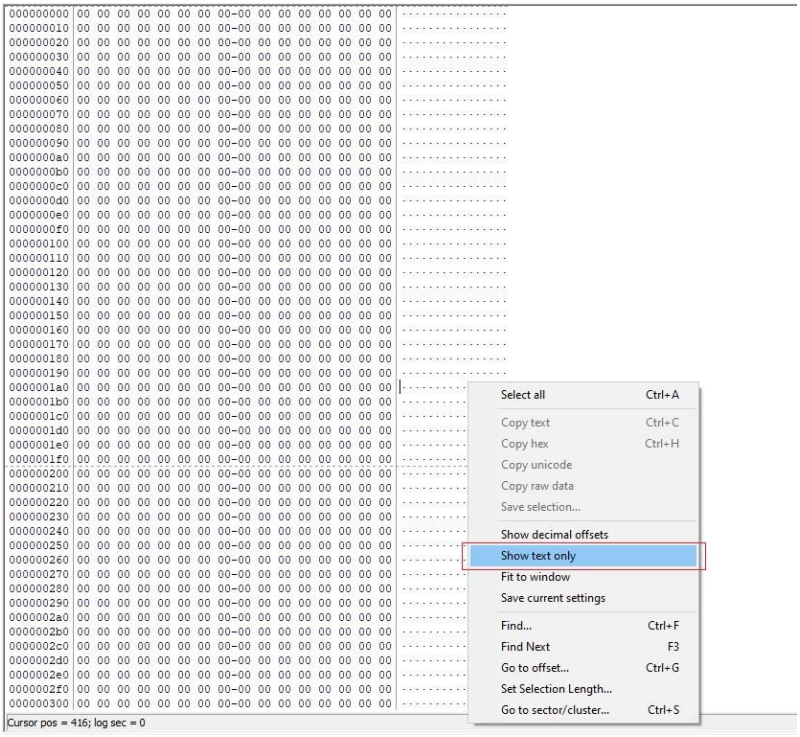


Ilustración 54. Botón de visualización de texto de la memoria RAM

Si pulsamos el botón se nos mostrará el texto en un formato más grande cuando realicemos las búsquedas. El siguiente paso es empezar con la búsqueda, para empezar una búsqueda podemos pulsar el botón derecho y elegir la opción **Find…**, como aparece en la Ilustración 53 o pulsar la combinación de teclas Ctrl + F. Al hacer una de estas dos opciones nos aparecerá una pestaña en la que podremos seleccionar diferentes parámetros de la búsqueda, que son el tipo de búsqueda y la dirección. En cuanto al tipo de búsqueda esta puede ser por caracteres binarios o por texto, y en dirección puede ser ascendente o descendente. En nuestro caso siempre vamos a buscar por texto y en dirección descendente, ya que vamos a empezar a buscar desde el principio del volcado de la memoria.

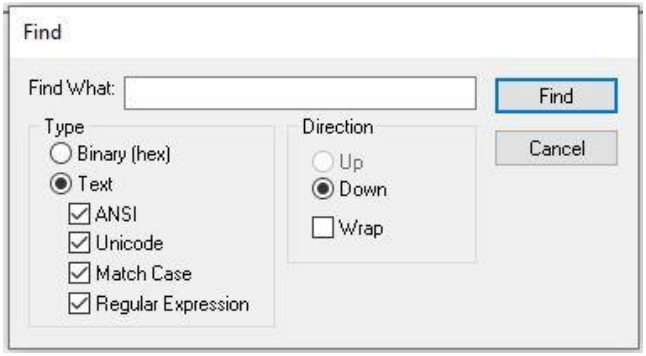


Ilustración 55. Cuadro de búsqueda en memoria RAM

Dentro de la opción de búsqueda por texto, marcaremos todas las casillas para que busque cualquier tipo de texto que escribamos.

Teniendo ya preparado el buscador de FTK para analizar la memoria debemos de pensar por dónde empezar nuestra búsqueda, en este caso podemos pensar en los datos que hemos encontrado en el disco duro C: más concretamente en el archivo Excel de bancos. Por eso, lo primero que podemos poner en el buscador es 'bancos'.
Si ponemos eso en el buscador y le damos a buscar, lo primero que nos aparece con la búsqueda es una página web de una búsqueda que se ha realizado en internet, sobre una página de bancos en Alcalá de henares.

Ilustración 56. Búsuqeda 1 memoria RAM 1

Si copiamos este enlace y lo pegamos en un navegador podemos ver la página web que ha visitado el sospechoso. Podemos seguir avanzando en la búsqueda que hemos hecho sobre bancos, pulsando la tecla F3.
Si seguimos buscando encontramos otra evidencia que nos lleva a otra búsqueda en internet sobre bancos Santander en Alcalá de Henares.

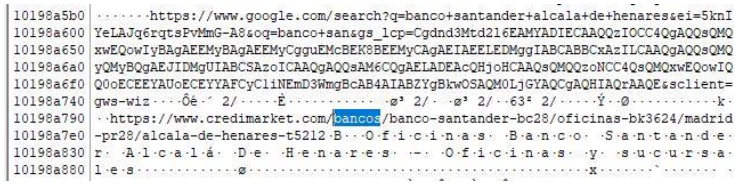


Ilustración 57. Búsuqeda 2 memoria RAM 1

Al igual que antes, si copiamos el enlace y lo pegamos en el navegador este enlace nos llevará a la página que visitó el sospechoso.

En este punto de la búsqueda podemos empezar a intuir que el sospechoso se mueve por la zona de Alcalá de Henares y alrededores. Pensando en zonas de alrededor se nos puede venir a la mente la zona de Torrejón de Ardoz, por lo que podemos pensar en buscar directamente Torrejón de Ardoz y ver si hay algo. Si realizamos la búsqueda, encontramos una búsqueda en la que aparece Torrejón de Ardoz junto a las palabras banco CaixaBank, esto nos hace pensar que también se mueve por esta zona a la hora de realizar sus atracos.

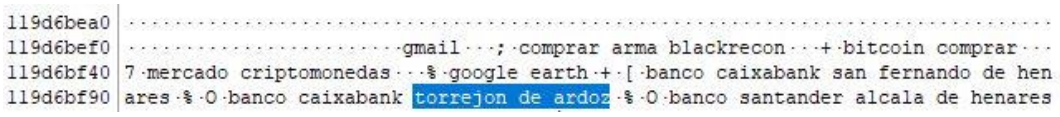


Ilustración 58. Búsqueda 3 memoria RAM 1

Si nos fijamos en el resultado de la búsqueda vemos que podemos obtener muchísima más información, como que el sospechoso ha buscado también bancos en la zona de San Fernando de Henares, también como comprar un arma en Blackrecon, información sobre criptomonedas, y también la página de Google Earth, de la que podemos intuir que ha sacado la información para hacer el seguimiento del documento de los coches que vimos al analizar la imagen forense del disco duro.

Teniendo en cuenta esta búsqueda podemos profundizar más en otros elementos como son las criptomonedas y el bitcoin. Podemos pensar que ha buscado esta información para realizar operaciones monetarias de las que no se puede tener un registro y que puede que sean para la compra de elementos ilegales. Si lo enlazamos con la búsqueda de la ilustración 58 podemos pensar que tiene que ver con la búsqueda de la compra de armas de Blackrecon. Con esto vamos a realizar una búsqueda en la memoria con la palabra 'criptomonedas' para ver que podemos encontrar.

Al realizar la búsqueda lo que podemos encontrar es una búsqueda en Google sobre mercado criptomonedas.

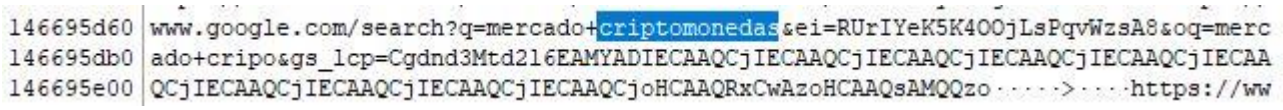


Ilustración 59. Búsuqeda 4 memoria RAM 1

Si el enlace lo copiamos y los pegamos en un navegador, podemos llegar a pensar que ha accedido a la primera página web, que muestra la capitalización de mercado de las 100 principales criptomonedas.

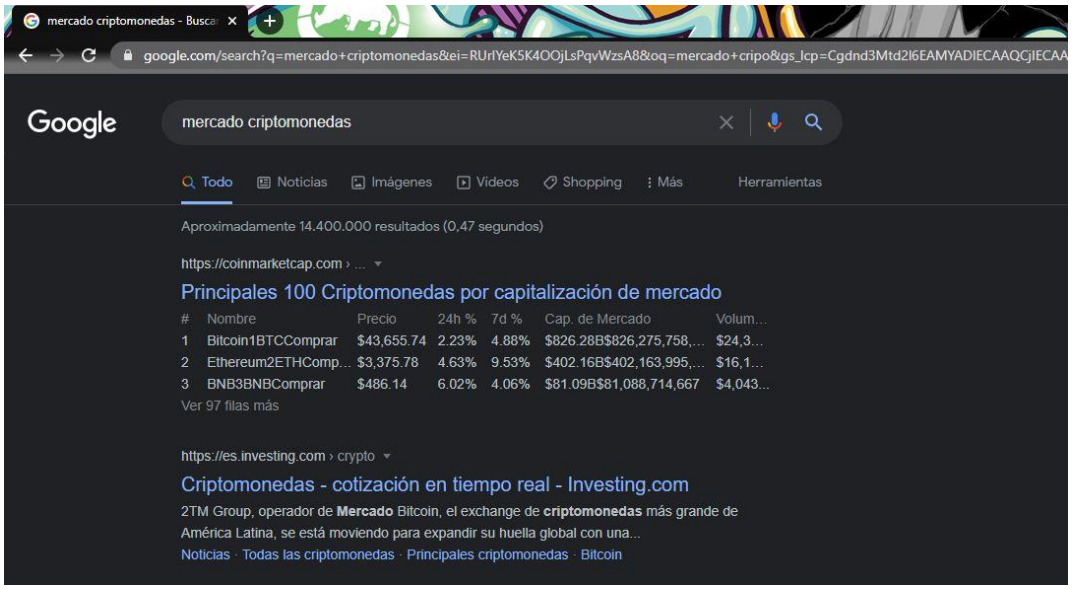


Ilustración 60. Página web del resultado de la búsqueda 4

Con esto podemos pensar que efectivamente el sospechoso está interesado en todo lo relacionado con las criptomonedas porque quiere realizar alguna operación con ellas o similar. Si seguimos pensando en criptomonedas, podemos llegar a pensar en bitcoin pudiendo buscar en FTK 'bitcoin comprar' y ver qué resultado arroja la búsqueda.
El resultado que arroja la búsqueda en FTK es similar al de la búsqueda anterior de criptomonedas, encontramos un enlace en el que aparece la búsqueda 'bitcoin comprar' y si pegamos en el navegador vemos los resultados de la búsqueda.

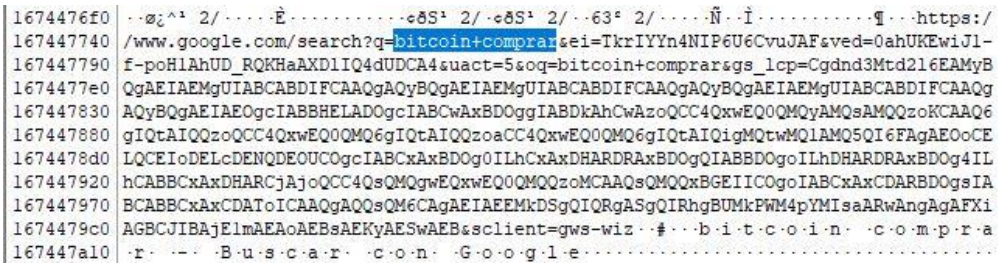


Ilustración 61. Búsqueda 5 memoria RAM 1

Ilustración 62. Página web del resultado de la búsqueda 5

Con la información que hemos obtenido de esta memoria hemos encontrado pruebas que poco a poco no van dando pistas relacionadas con el sospechoso que hemos detenido.

6.3.2 Análisis de volcado de memoria 2

Hemos analizado el archivo forense de la memoria RAM 1, pero todavía nos queda el segundo archivo de memoria que se extrajo del ordenador del sospechoso, que tiene como nombre ***Información correo.mem***. Este archivo fue tomado en el momento en el que el sospechoso tenía una cuenta de correo de Gmail cerrando sesión, teniendo en cuenta esto lo que vamos a buscar en este archivo es información de la cuenta y la contraseña de Gmail.

Para empezar a realizar la búsqueda de la cuenta de Gmail debemos de pensar en que nos pide Gmail a la hora de iniciar sesión en internet. Nos pide en primer lugar el usuario de correo electrónico y después la contraseña. En el caso de la contraseña vemos que pone una frase muy concisa que es 'Introduce tu contraseña', esto nos puede servir como punto de partida a la hora de comenzar nuestra búsqueda en el archivo de la memoria con FTK.

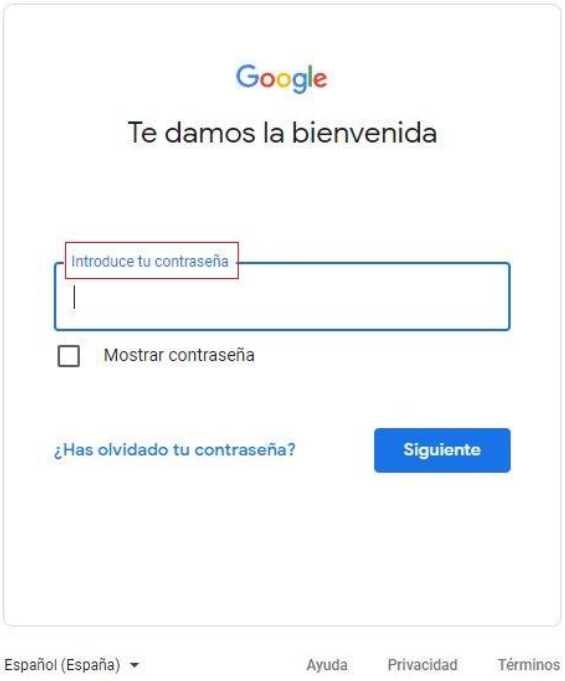


Ilustración 63. Introducir contraseña en Gmail

Si nos vamos a FTK y buscamos en el archivo de la memoria que estamos investigando la frase concreta 'Introduce tu contraseña', encontraremos una búsqueda similar a la siguiente:

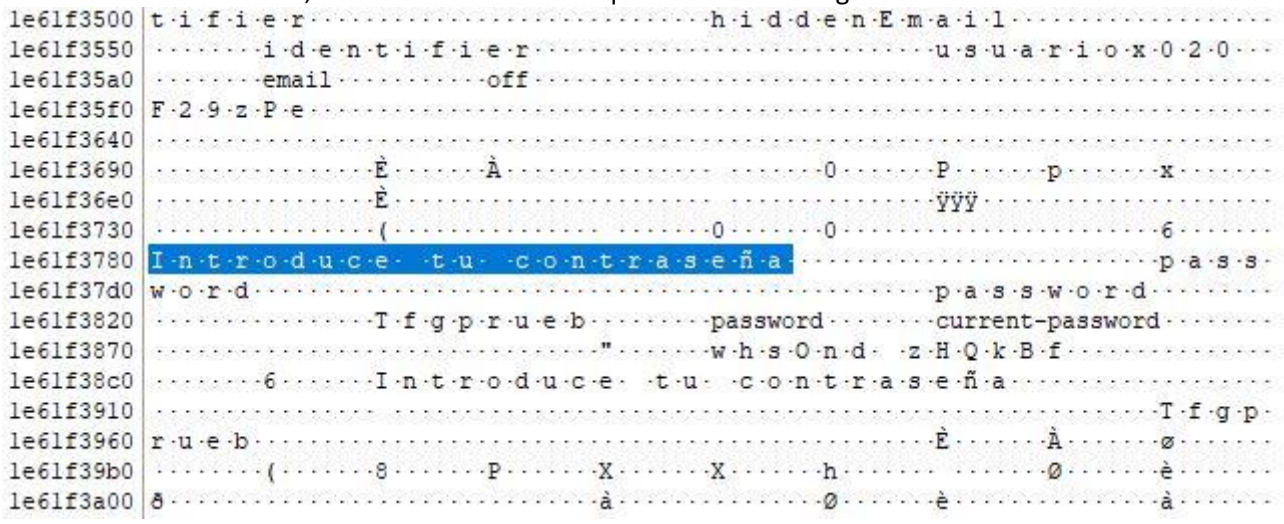


Ilustración 64. Resultado búsqueda contraseña

Si nos fijamos en el resultado de la búsqueda podemos ver que hemos encontrado muchísima información sobre la cuenta de correo de Gmail del sospechoso. Si nos fijamos al principio del resultado de la búsqueda vemos que pone **'hiddenEmail' 'identifier'** y luego pone usuariox020, esto nos indica cual es la dirección del correo de Gmail.

Si seguimos analizando la ilustración 63 veremos que justo donde aparece 'Introduce tu contraseña' pone más adelante **'password'** y justo después Tfgprueb. Esta puede ser la contraseña de la cuenta de Gmail del sospechoso. En este caso al ser una prueba creada por nosotros sabemos que no es la contraseña completa, ya que esta es TFGprueba20, pero esta búsqueda nos puede ayudar a buscar de manera más sencilla la contraseña entera dentro de todo el archivo de la memoria.

Con la información que hemos obtenido y realizando una búsqueda un poco más exhaustiva de la contraseña, podemos conseguir obtener todos los datos de inicio de sesión de la cuenta de Gmail del usuario.

Una vez que tenemos los datos, iniciamos sesión en Gmail e investigamos los correos que tiene. Vemos un correo que tiene como asunto compra. Si pinchamos en el correo vemos que es el siguiente:

Ilustración 65. Correo de Gmail

Si leemos el correo de Gmail, vemos que el sospechoso ha comprado un arma a una persona y que el pago lo ha realizado mediante una Wallet que tendría criptomonedas. Esto podemos confirmarlo con los datos que nosotros hemos obtenido de la anterior memoria RAM que hemos investigado, en la que aparecían búsquedas de criptomonedas y otra búsqueda de armas de la página Blackrecon. Además, si nos fijamos en el correo del que proviene este mensaje es un correo de tipo Protonmail, siendo este un correo más seguro que Gmail, por lo que podemos intuir que es de alguien que no quiere ser localizado ni asociado a ninguna operación de compra y venta de armas.

A parte del correo vemos que hay dos imágenes que son 2 códigos QR, que según el mensaje uno es para realizar la operación del traspaso de las criptomonedas de una Wallet a otra para la compra del arma, y el otro QR es para confirmar la realización de esta compraventa. Podemos descargarnos estos QR y en una página web ver que contiene cada uno de ellos.

Nos descargamos los QR y nos vamos a la siguiente dirección web: https://4qrcode.com/scan-qr-code.php?lang=es , que es una página web donde leer QR online. Si escaneamos el primer código QR que tiene como nombre '**QR Pago**' al analizarlo en la página vemos que nos muestra la dirección de una cartera bitcoin, la cantidad de la operación, que son 0.0005 BTC, y el mensaje de la operación que es **Pago Arma**.

Ilustración 66. Mensaje código QR 1

Con esta información podemos confirmar que el sospechoso ha realizado una operación en la que ha comprado un arma. Lo siguiente que analizamos es el segundo código QR, que tiene como nombre '**QR confirmación**', al analizarlo en el escáner nos muestra un mensaje en el que pone que el dinero ha sido enviado correctamente al destinatario.

Ilustración 67. Mensaje código QR 2

Como vemos es solo un QR que muestra un mensaje de confirmación de que la operación anterior se ha realizado con éxito.

Con la información que hemos obtenido podemos deducir que el sospechoso debe de tener una wallet con la que ha realizado esta operación, por lo que podemos volver a investigar nueva información de este estilo en el disco duro C: .

6.4 Recopilación de información adicional

Al realizar todo el análisis de los elementos que habíamos obtenido del ordenador del sospechoso hemos descubierto que este puede tener una wallet para realizar operaciones de compraventa y que estas sean más difíciles de registrar, por ello vamos a volver a analizar el disco duro C: , para ver si encontramos información nueva sobre esto.

Para buscar más información en este caso vamos a mirar que tiene el sospechoso en el escritorio del ordenador. Si accedemos al escritorio vemos que tiene dos accesos directos interesantes, uno es el acceso directo a TOR y otro es un acceso directo a Electrum. TOR es el navegador web mediante el que ha podido realizar todo lo relacionado con la búsuqeda del arma que ha comprado, y Electrum es una aplicación de wallet de criptomonedas que puede ser mediante la que ha hecho la transacción para comprar el arma.

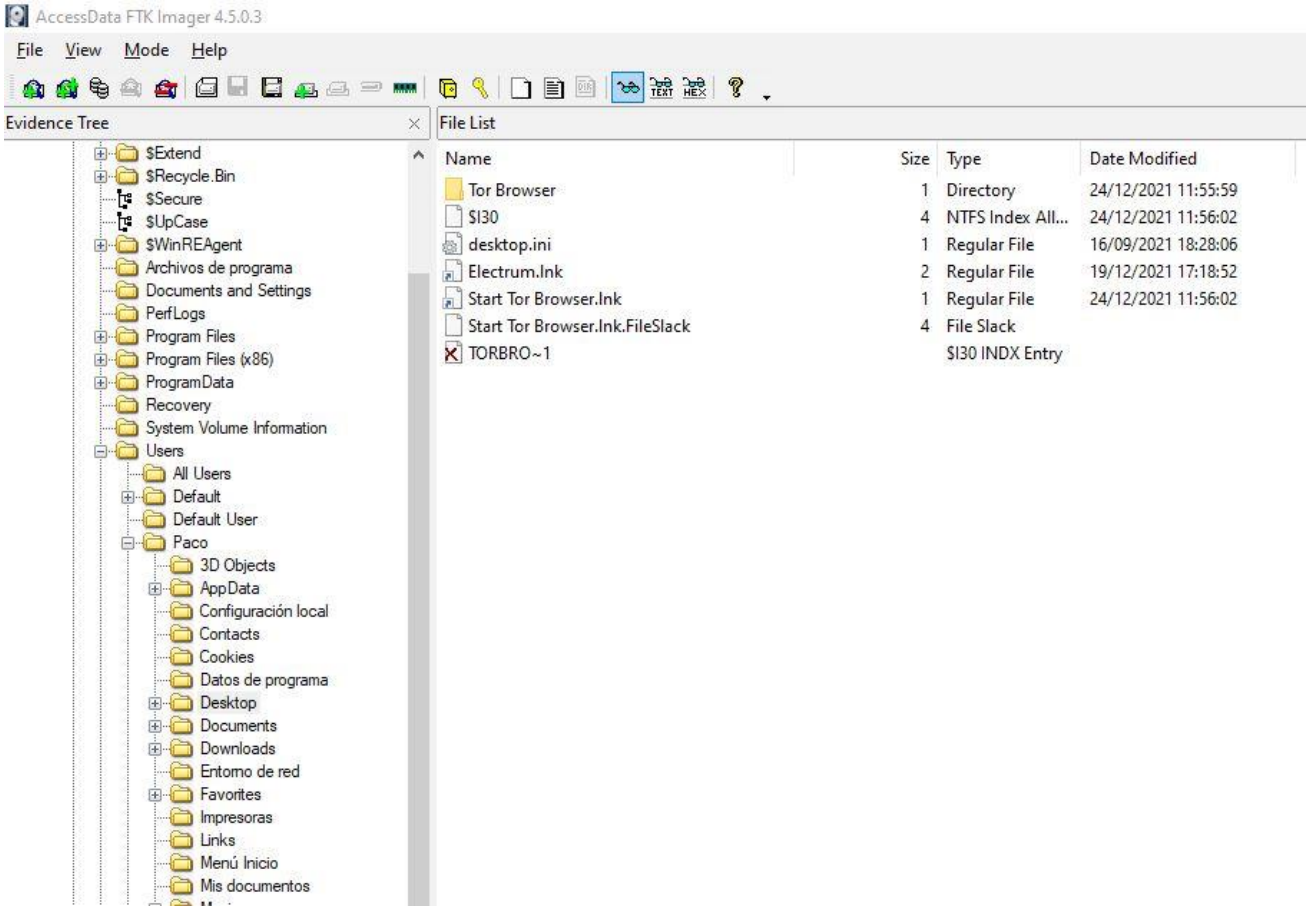


Ilustración 68. Escritorio del disco C:

Para obtener más información sobre las Wallet que pueda tener el sospechoso en el ordenador, podemos pensar en instalar nosotros el programa en otro ordenador y ver cuál es la ruta de instalación y donde se guardan las Wallet. Si hacemos eso podemos saber que la ruta en la que se guardan los datos de Electrum es la siguiente: C:\Users\Paco\AppData\Roaming\Electrum

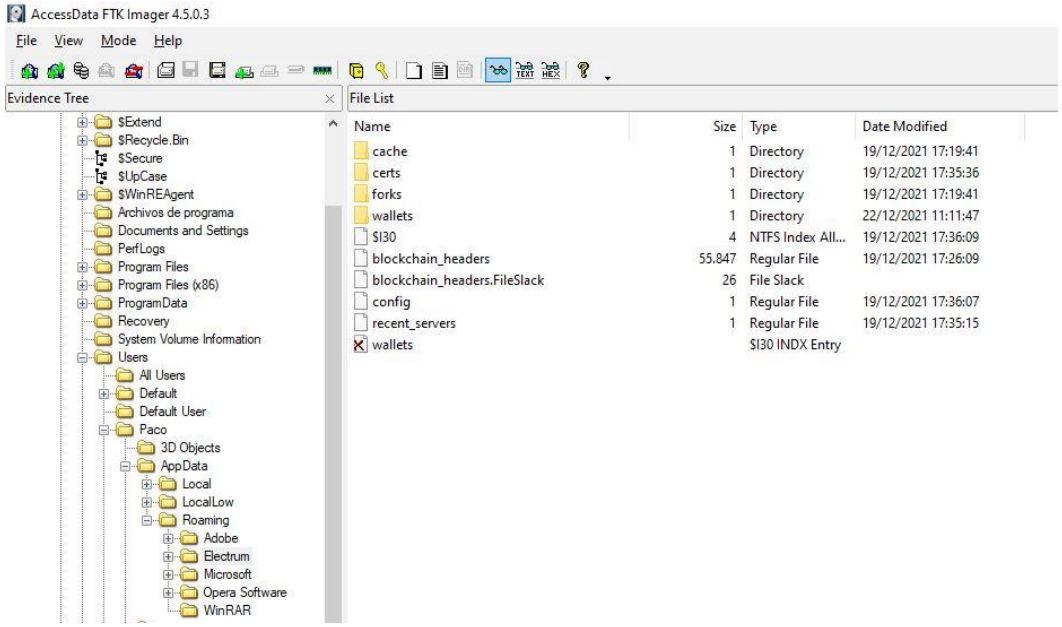


Ilustración 69. Ruta de la carpeta de Electrum

Si nos fijamos en la ilustración anterior vemos que dentro de la carpeta de Electrum encontramos una carpeta que es la que contiene las wallet que pueda tener el sospechoso. Si accedemos a la carpeta nos encontramos con dos archivos, uno que es la cartera de criptomonedas, que la ha llamado 'cartera_criptos' y un archivo de texto que tiene como nombre '**Código cartera criptos**'.

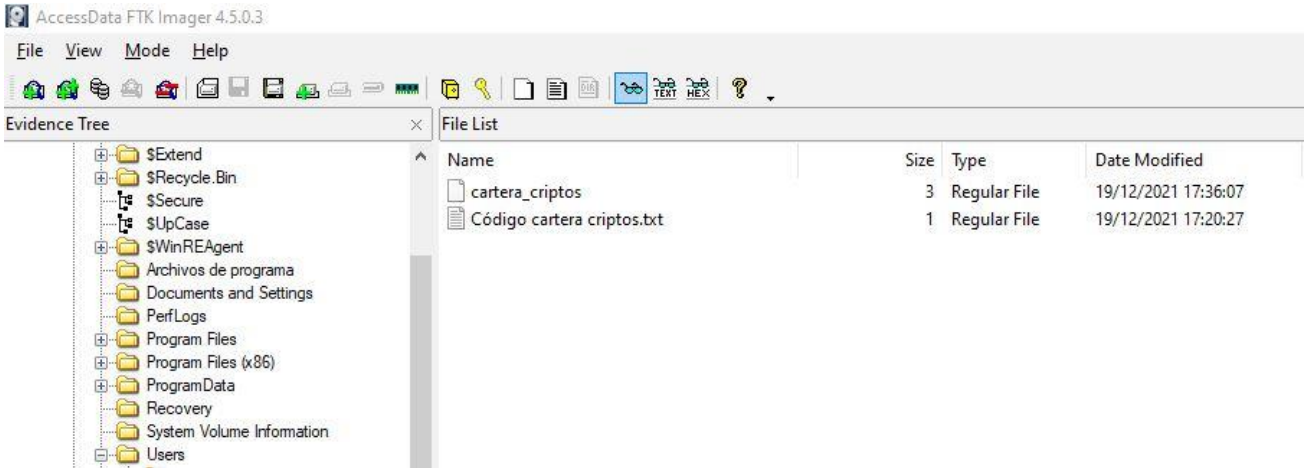


Ilustración 70. Contenido carpeta Wallets Electrum

El archivo de texto, si lo abrimos vemos que es una combinación de palabras que sirve como recuperación de la Wallet en caso de no poder acceder a ella o haber olvidado la contraseña.

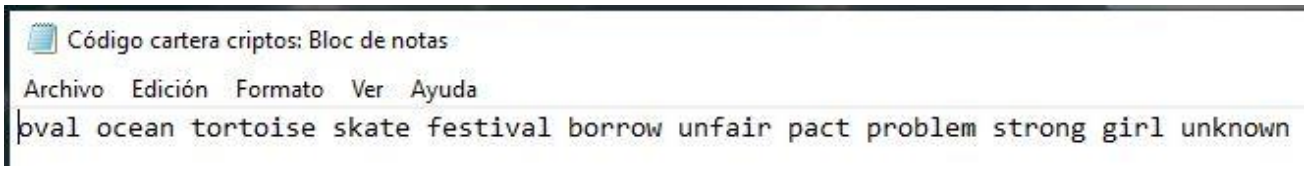


Ilustración 71. Texto código cartera criptos

Con esto podemos tener un buen comienzo para obtener información sobre la cartera de criptomonedas que tiene el sospechoso, y las diferentes operaciones que pueda haber realizado con ella.

Conclusiones

Una vez finalizado todo el análisis de los datos que se han obtenido del sospechoso podemos sacar conclusiones y un perfil de la persona.

El perfil del sospechoso que obtenemos es, que esta persona se dedica a realizar atracos a sucursales de bancos de la zona del Corredor del Henares como son Alcalá de Henares, Torrejón de Ardoz y San Fernando de Henares. A parte también sabemos que, a la hora de realizar todos los atracos, realiza previamente un seguimiento de coches abandonados que más adelante utilizará para llevar a cabo los atracos que realice. También hemos descubierto que realiza las búsquedas de las diferentes sucursales mediante búsquedas en Google. Además, es un atracador que realiza los atracos a mano armada, ya que hemos accedido a su correo de Gmail y hemos descubierto una operación de compraventa de un arma, realizada mediante el pago con criptomonedas de una Wallet que había en su ordenador.

Con esta información podemos tener pruebas sólidas de que la persona a la que se le ha incautado el ordenador ha sido debido a implicársele en diferentes atracos realizados en la zona del Corredor del Henares.

Este proyecto ha sido una prueba básica de obtención de información, en el caso de una investigación forense real se utilizan muchos más elementos y se hacen búsquedas más exhaustivas de todos los elementos que se obtengan del sospechoso, a pesar de ello, podemos decir que con el software FTK Imager se puede obtener bastante información inicial a la hora de realizar una investigación forense, ya que se trata de una herramienta muy potente. Sin embargo, no todo depende del software forense y de lo potente que sea, gran parte del trabajo se basa en realizar una investigación previa de la persona para saber por dónde empezar a la hora de realizar la investigación de los elementos informáticos que se recopilen.

Como conclusión un buen análisis forense en el que se obtengan pruebas para una investigación consta principalmente de dos cosas, un análisis previo de la persona por parte del equipo forense que se vaya a encargar de la investigación; y el uso de uno o varios softwares los suficientemente potentes que sirvan para obtener la mayor información posible de los elementos de análisis. El tener un software potente que nos permita obtener la mayor información no nos sirve de nada por sí solo, si no sabemos por dónde empezar a realizar la búsqueda de información de cara a la investigación forense.

Bibliografía

[1] Álvarez, L. (2021, 25 junio). Volcado de Memoria RAM con AccessData FTK Imager. Pyxius. https://www.pyxius.com/volcado-de-memoria-ram-con-accessdata-ftk-imager/

[2] Castillo, J. A. (2018, 26 noviembre). Qué es pagefile.sys y para qué sirve. Profesional Review. https://www.profesionalreview.com/2018/11/30/pagefile-sys-windows-10/

[3] CTIN. (s. f.). Mounting virtual hard drives. Slideshare. https://es.slideshare.net/ctin/mounting-virtual-hard-drives

[4] Focus, F. (2020, 12 mayo). Evidence Acquisition Using Accessdata FTK Imager. Forensic Focus. https://www.forensicfocus.com/articles/evidence-acquisition-using-accessdata-ftk-imager/

[5] Moore, P. (2017, 11 diciembre). Understanding Orphaned Files. ThinkDFIR. https://thinkdfir.com/2017/08/18/understanding-orphaned-files/

[6] Historia de la informática forense. (2021, 31 marzo). Detectives Madrid. https://detectives-madrid.es/historia-informatica-forense-aplicacion/

[7] Historia Informática Forense (s.f.). Scribd. https://es.scribd.com/document/367314600/Historia-Informatica-Forense

[8] J.E.L.P. (s. f.). International Organisation on Computer Evidence - GTI - Glosario Terminología Informática. Glosario Terminología Informática. http://www.tugurium.com/gti/termino.php?Tr=International%20Organisation%20on%20Computer%20Evidence

[9] Fundamentos de la Informática Forense. (2021, 31 mayo). Cloud DataCenter DANTIA Tecnología. https://datacenter.dantia.es/fundamentos-de-la-informatica-forense/

Universidad de Alcalá
Escuela Politécnica Superior

Universidad
de Alcalá