



ANALISIS FORENSE

Master en Ciberseguridad – Trabajo Final de Master

Autor: Ruben Mesquida Gomila

Tutor: Juan Carlos Gómez Castillo

Fecha: octubre 2019

ABSTRACT

In the present Master's Thesis is intended to do the analysis and forensic investigation of a computer with Windows that has been hacked. This equipment belongs to a company which has suffered a information leakage.

The development of this Master's Thesis it will be carried out in different phases, from the collection of information, the acquisition of forensic images along with analysis and investigation, to finish with an expert report to finish the document. All this process will be accompanied by the documentation that would be carried out in an official case of judicial expertise.

To carry out the analysis, the appropriate tools (Autopsy, Log2timeline, DumptIt, Yara, ...) will be used in each of the phases developed, together with a brief description of the steps to be carried out.

PREFACIO

En el presente trabajo de final de máster se pretende realizar el análisis e investigación forense de un ordenador con Windows que ha sido vulnerado. Este equipo pertenece a una empresa la cual ha sufrido una filtración de información.

En el desarrollo del trabajo se llevarán a cabo en distintas fases, desde la recopilación de información, la adquisición de las imágenes forenses junto con el análisis y la investigación, para acabar con un informe pericial para la conclusión de este. Todo este proceso estará acompañado por la documentación que se realizaría en un caso oficial de peritaje judicial.

Para llevar a cabo el análisis se utilizarán las herramientas adecuadas (Autopsy, Log2timeline, DumpIt, Yara, ...) en cada una de las fases desarrolladas, junto a una pequeña descripción de los pasos a realizar

TABLA DE CONTENIDO

Abstract	1
Prefacio.....	2
Lista de ilustraciones	5
Lista de tablas.....	7
Lista de anexos	8
1. Introducción	9
1.1. ¿Que es el Análisis Forense?.....	10
2. Escenario	10
3. Objetivos	11
4. Herramientas.....	11
5. Planificación de etapas	13
Fase 0 – Recopilación de Información	13
Fase 1 - Adquisición de imágenes.....	13
Fase 2 - Análisis e investigación.....	13
Fase 3 – Conclusiones y redacción informe.....	14
6. Recopilación de información	14
7. Fase de Adquisición	20
7.1 Adquisición de imagen de memoria volátil.....	20
7.2 Adquisición de imagen de disco duro	21
7.3 Validación de las imágenes	26
7.4 Cadena de custodia	27
8. Fase de Análisis e investigación.....	31
8.1 Análisis de Memoria	31
8.1.1. Validación	31
8.1.2. Información de la imagen	32
8.1.3. Procesos activos	32
8.1.3. Servicios.....	37
8.1.5. Conexiones	38
8.2 Análisis de Imagen disco duro.....	39
8.2.1. Validación	39
8.2.2. Creacion caso Autopsy	40
8.2.3. ANALISIS DE MALWARE	43
8.2.4. Datos básicos del equipo	46
8.2.5. Análisis Usuarios.....	47

8.2.6. Análisis logs Sistema	48
8.2.7. Análisis archivos y datos borrados	57
8.2.8. Análisis Datos (Actividad reciente, cookies, historial web, etc.)	66
8.2.9. Análisis Email	71
8.2.10. Análisis otras aplicaciones	73
9. Fase Final	75
9.1 Hallazgos evidencias	75
9.2 Conclusiones	76
10. Anexos	79
11. Glosario	87
12. Bibliografía y referencias	90

LISTA DE ILUSTRACIONES

<i>Ilustración 1. Statista grafico daño cibercrimen en EEUU 2001-2017. Recuperado de https://www.statista.com/statistics/267132/total-damage-caused-by-cyber-crime-in-the-us/</i>	9
<i>Ilustración 2. Total, Malware Av-Test. Recuperado de https://www.av-test.org/en/statistics/malware/ 10</i>	
<i>Ilustración 3 Anexo 1a Acuerdo confidencialidad 1.....</i>	15
<i>Ilustración 4 Anexo 1a Acuerdo Confidencialidad 2</i>	16
<i>Ilustración 5 Anexo 1a Acuerdo confidencialidad 3.....</i>	16
<i>Ilustración 6. Anexo 1b. Formulario Solicitud de Servicios</i>	17
<i>Ilustración 7 Anexo 1c Presupuesto 1</i>	19
<i>Ilustración 8 Anexo 1c Presupuesto 2</i>	19
<i>Ilustración 9. Adquisición RAM DumpIT</i>	21
<i>Ilustración 10. Rufus</i>	22
<i>Ilustración 11. Arranque CAINE</i>	23
<i>Ilustración 12. Unblock CAINE</i>	24
<i>Ilustración 13. Menú CAINE</i>	24
<i>Ilustración 14. Guymager 1</i>	25
<i>Ilustración 15. Guymager 2</i>	25
<i>Ilustración 16. Guymager 3</i>	26
<i>Ilustración 17. Guymager 4</i>	26
<i>Ilustración 18. Verificación Inicial RAM</i>	26
<i>Ilustración 19. Verificación Inicial Disco</i>	27
<i>Ilustración 20. Cadena custodia formulario 1.....</i>	28
<i>Ilustración 21. Cadena custodia formulario 2.....</i>	28
<i>Ilustración 22. Cadena de custodia formulario 3</i>	29
<i>Ilustración 23. Acta notarial de presencia</i>	30
<i>Ilustración 24. Validación Imagen RAM</i>	31
<i>Ilustración 25. Imageinfo 1</i>	32
<i>Ilustración 26. Imageinfo 2.....</i>	32
<i>Ilustración 27. RAM Lista procesos.....</i>	33
<i>Ilustración 28. RAM Árbol procesos.....</i>	33
<i>Ilustración 29. RAM Psscan</i>	34
<i>Ilustración 30. RAM Psxview.....</i>	35
<i>Ilustración 31. Lista DLL PID 3204.....</i>	36
<i>Ilustración 32. SIDs Proceso 3204.....</i>	36
<i>Ilustración 33. RAM Variables entorno.....</i>	36
<i>Ilustración 34. RAM Servicios</i>	37
<i>Ilustración 35. RAM Conexiones red 1</i>	38
<i>Ilustración 36. RAM Conexiones red 2</i>	39
<i>Ilustración 37. Validación imagen disco duro.....</i>	39
<i>Ilustración 38. Creación Caso Autopsy 1.....</i>	40
<i>Ilustración 39. Creación Caso Autopsy 2.....</i>	40
<i>Ilustración 40. Creación caso Autopsy 2</i>	41
<i>Ilustración 41. Creación caso Autopsy 3</i>	41
<i>Ilustración 42. Creación caso Autopsy 4</i>	42
<i>Ilustración 43. Creación caso Autopsy 4</i>	42
<i>Ilustración 44. OSFMount 1</i>	43
<i>Ilustración 45. OSFMount 2</i>	44

<i>Ilustración 46. OSFMount 3</i>	44
<i>Ilustración 47. Análisis ClamAV</i>	45
<i>Ilustración 48. Anexo 3 a Resultado ClamAV.....</i>	45
<i>Ilustración 49. Análisis Yara.....</i>	45
<i>Ilustración 50. Anexo 3b Resultado Yara</i>	45
<i>Ilustración 51. Información Sistema</i>	47
<i>Ilustración 52. Datos Cuenta Usuario</i>	48
<i>Ilustración 53. Datos Cuenta Administrador</i>	48
<i>Ilustración 54. Datos Cuenta Invitado</i>	48
<i>Ilustración 55. Localización Archivos Registro</i>	49
<i>Ilustración 56. Evidencia Registro.....</i>	51
<i>Ilustración 57. Localización archivos Eventos.....</i>	52
<i>Ilustración 58. Archivos Eventos Extraídos</i>	52
<i>Ilustración 59. Eventos Aplicación</i>	53
<i>Ilustración 60. Inicios de sesión día 24</i>	55
<i>Ilustración 61. Dispositivos USB.....</i>	56
<i>Ilustración 62. Windows Prefetch.....</i>	57
<i>Ilustración 63. Shellbags.....</i>	57
<i>Ilustración 64. Log2Timeline.....</i>	59
<i>Ilustración 65. Timeline a Excel</i>	59
<i>Ilustración 66. Anexo 4 Timeline Excel.....</i>	59
<i>Ilustración 67. Archivo vbs analizado</i>	63
<i>Ilustración 68. Troyano Analizado</i>	63
<i>Ilustración 69. Ransomware WannaCry Analizado.....</i>	64
<i>Ilustración 70. Archivos Borrados</i>	65
<i>Ilustración 71. Archivos huérfanos</i>	65
<i>Ilustración 72. Carved Files</i>	66
<i>Ilustración 73. Documentos Recientes.....</i>	67
<i>Ilustración 74. Descargas web</i>	67
<i>Ilustración 75. Marcadores.....</i>	68
<i>Ilustración 76. Búsqueda Pastebin.....</i>	69
<i>Ilustración 77. Análisis cookies</i>	69
<i>Ilustración 78. Análisis Historial</i>	70
<i>Ilustración 79. Web Pastebin.....</i>	71
<i>Ilustración 80. Email extraño</i>	72
<i>Ilustración 81. Análisis APK.....</i>	72
<i>Ilustración 82. Cabecera correo electrónico</i>	73
<i>Ilustración 83. Programas Registro</i>	74
<i>Ilustración 84. Program Files</i>	74
<i>Ilustración 85. Anexo 11 Informe pericial</i>	77
<i>Ilustración 86. Contenido Informe Pericial</i>	78

LISTA DE TABLAS

<i>Tabla 1. Herramientas</i>	12
<i>Tabla 2. DLLs Proceso 3204</i>	35
<i>Tabla 3. Resultados Malware</i>	46
<i>Tabla 4. Datos Equipo.....</i>	46
<i>Tabla 5. Eventos útiles System.....</i>	53
<i>Tabla 6. Eventos útiles Security</i>	54
<i>Tabla 7. Tipos de inicio de sesión.....</i>	54
<i>Tabla 8. Documentos.....</i>	62
<i>Tabla 9. Archivos Sospechosos</i>	62
<i>Tabla 10. Hallazgos encontrados.....</i>	76

LISTA DE ANEXOS

<i>Anexo 1 Acuerdo de Confidencialidad</i>	79
<i>Anexo 2 Formulario solicitud de Servicio.....</i>	80
<i>Anexo 3 Presupuesto</i>	80
<i>Anexo 4 Cadena de Custodia Imagen Disco.....</i>	81
<i>Anexo 5 Cadena de Custodia Imagen RAM</i>	82
<i>Anexo 6 Acta Notarial de presencia</i>	83
<i>Anexo 7 Salida ClamAV malware.....</i>	84
<i>Anexo 8 Salida análisis Yara Scan.....</i>	85
<i>Anexo 9 Timeline archivos</i>	85
<i>Anexo 10 Aplicación Sitsa.apk</i>	85
<i>Anexo 11 Informe Pericial.....</i>	86

1. INTRODUCCIÓN

Desde que el mundo de la tecnología prácticamente controla nuestras vidas, el número de usuario de internet solo ha hecho que aumentar. Hoy en día por todos es conocido el gran impacto de las nuevas tecnologías y el riesgo que estas suponen. A causa de este gran aumento todos los días se producen nuevas amenazas (ransomware, troyanos, RATs, etc.) que ponen en riesgo a nuestros equipos. Esta gran cantidad de malware y nuevos atacantes que aparecen todos los días, hace que el análisis forense y los analistas sean una rama y unos profesionales realmente necesarios.

Según los datos de Statista (<https://www.statista.com/statistics/267132/total-damage-caused-by-cyber-crime-in-the-us/>) el mundo del cibercrimen ha llegado a mover miles de millones al año. Como podemos ver en el grafico en los años 2016 y 2017 llegan a mover más de 1.400 millones dólares solo en los casos que se han detectado en EEUU. Se estima que este mundo puede llegar a mover más dinero que en el narcotráfico o la prostitución.

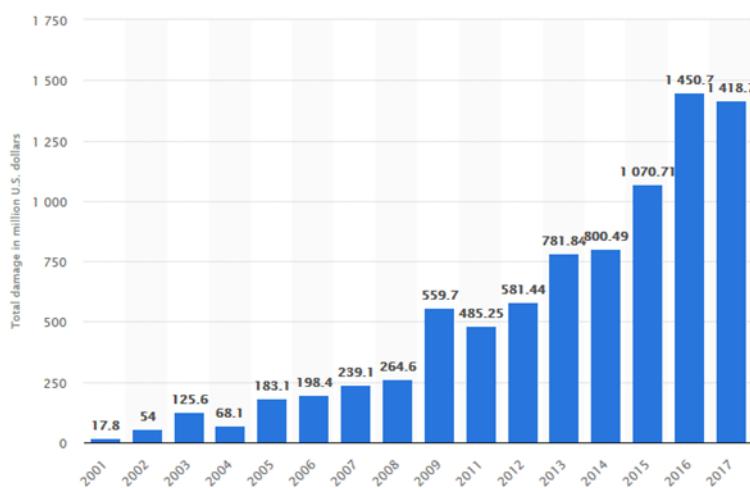


Ilustración 1. Statista grafico daño cibercrimen en EEUU 2001-2017. Recuperado de <https://www.statista.com/statistics/267132/total-damage-caused-by-cyber-crime-in-the-us/>

A causa de este gran incremento de flujo de dinero más actores y más interesados quieren entrar en este mundo. Según los datos del instituto AV-TEST la cantidad total de malware se multiplicado casi x2 desde 2015. En este 2019 ya llevamos más de 952.17 millones de amenazas detectadas y esta tendencia sigue aumentando, ofrecen datos que estiman que diariamente son encontrados 350.000 nuevas amenazas

Total malware

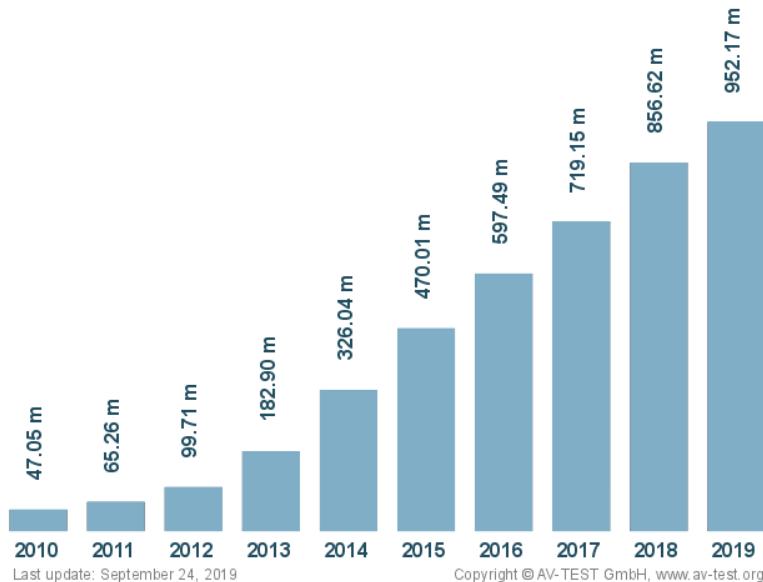


Ilustración 2. Total, Malware Av-Test. Recuperado de <https://www.av-test.org/en/statistics/malware/>

Vistos los datos vemos que la demanda de nuevos analistas y nuevos profesionales en esta rama de la ciberseguridad ira en aumento, por este motivo se ha elegido la realización de este trabajo de fin de master.

1.1. ¿QUE ES EL ANÁLISIS FORENSE?

El análisis forense es una rama de la ciberseguridad en la cual se utilizan un conjunto de técnicas y herramientas, que se utilizan en revisar y extraer evidencias de un dispositivo que haya sufrido un incidente sin modificar o alterar este dispositivo.

2. ESCENARIO

En el presente trabajo se establece el siguiente escenario:

Después de una filtración de distintos diseños de diferentes dispositivos de una importante compañía, los responsables TIC de dicha compañía descubren que la filtración se produjo desde el equipo del director, al darse cuenta nos piden un

análisis forense junto con su informe pericial de dicho equipo, en busca de las diferentes evidencias y pruebas que se puedan obtener.

El equipo se trata de un ordenador portátil con sistema operativo Windows 7 desde el cual trabaja el director en su jornada laboral y que a veces es utilizado desde su domicilio. Además, dicha persona dispone de un dispositivo Android el cual utiliza para realizar su trabajo y también como dispositivo personal.

NOTA: Los datos personales, de la empresa, firmas, etc. Son datos ficticios cualquier parecido a la realidad es coincidencia.

3. OBJETIVOS

El presente trabajo pretende conseguir los siguientes puntos:

A1 – La adquisición de las diferentes imágenes, RAM, disco duro, etc.

A2 – Investigación y realización del análisis

A3 – Utilización correcta de diferentes herramientas para llevar a cabo el análisis

A4 – Realización de toda la documentación necesaria en un informe pericial

A5 – Resolución del escenario planteado incluyendo las diferentes evidencias encontradas.

4. HERRAMIENTAS

Para la realización del análisis forense se han utilizado las siguientes herramientas en distintos casos:

Nombre	Descripción	Utilización	Enlace
Autopsy	Es una herramienta para análisis forense que implementa distintas herramientas como The Sleuth Kit y otras. Además,	Realización de las investigaciones y análisis de las imágenes	Autopsy

	puede ser extendido con plugin de terceros.		
CAINE	Es una distribución Linux enfocada al análisis forense, incluye diversas herramientas de utilidad para realizar investigaciones. En nuestro caso será utilizada como live-cd para ejecutar la herramienta Guymanager para crear la imagen forense.	Adquisición de imágenes de disco.	CAINE
Volatility	Es un framework para análisis forense de memoria	Análisis forense de la memoria RAM.	Volatility
Dumplt	Es una herramienta utilizada para la obtención de imágenes de la memoria de forma fácil en un solo clic.	Realizar la adquisición de la memoria RAM del equipo	Dumplt
OSFMount	Es una herramienta que permite montar imágenes de disco, como disco físico o lógico para su posterior análisis	Montar imagen para análisis de malware	OSFMount
YARA	Yara es una herramienta desarrollada por Virustotal, y principalmente se centra en la investigación y detección de malware.	Realizar análisis en búsqueda de malware de la imagen obtenida	YARA
CLAMAV	Clamav es una antivirus de código libre y multiplataforma, que proporciona múltiples utilidades para la detección de malware.	Realizar análisis en búsqueda de malware de la imagen obtenida	CLAMAV
Log2timeline	Es una herramienta de código libre diseñada para extraer las marcas de tiempo de archivos de un sistema	Creación del timeline de la imagen adquirida	Log2timeline

Tabla 1. Herramientas

5. PLANIFICACIÓN DE ETAPAS

El análisis lo podemos dividir en 4 fases destacadas, donde se realizarán distintas tareas, a continuación, comentamos estas distintas fases que se realizarán

FASE 0 – RECOLAJO DE INFORMACIÓN

En esta fase 0 o fase inicial el objetivo principal será poner ese en contacto con el cliente al fin de obtener la mayor información posible sobre el caso. Se le aportaran la distinta documentación como puede ser el acuerdo de confidencialidad, el formulario de solicitud de servicio donde nos aportara la información principal del caso, y para finalizar después de ser revisada la información se le ofrecerá un presupuesto aproximado.

FASE 1 - ADQUISICIÓN DE IMÁGENES

En esta primera fase se procederá a adquirir las distintas imágenes que se utilizaran para llevar acabo el análisis. Se realizará la documentación y las medidas pertinentes para mantener la cadena de custodia.

Tiempo estimado: 3 días.

FASE 2 - ANÁLISIS E INVESTIGACIÓN

En esta segunda fase se llevará a cabo el análisis de las distintas imágenes obtenidas en la primera fase de adquisición.

Se analizará la imagen obtenida de la memoria RAM donde primera se verificará la imagen y se analizaran los procesos activos, los servicios y las posibles conexiones que pueda haber en ese momento.

La imagen del disco duro se verificará mediante su MD5 y SHA1, y se analizaran los distintos usuarios del dispositivo, los archivos y posibles datos borrados, los logs Sistema, los distintos datos de interés (Actividad reciente, cookies, historial web, etc.).

análisis del correo electrónico si el usuario lo tiene instalado y el análisis de otras aplicaciones que pueda haber de interés.

Tiempo estimado: 8 semanas

FASE 3 – CONCLUSIONES Y REDACCIÓN INFORME

En esta última, fase se sacarán los hallazgos y las conclusiones, y como punto final se elaborará el informe pericial del caso.

Tiempo estimado: 1 semana

6. RECOPILACIÓN DE INFORMACIÓN

En esta primera fase donde el cliente se pone en contacto con nosotros, deberemos recopilar la máxima información posible sobre el caso. Para ellos se utilizará un formulario de solicitud de servicio donde se incluirán los datos del cliente, la información del caso y los detalles y servicios que solicita el cliente.

Además, le haremos firmar un acuerdo de confidencialidad y secreto en el que nos comprometemos a utilizar únicamente la información que contenga solamente para la realización del informe pericial. En este documento se incluirá distintas cláusulas para el cumplimiento de la protección de datos, la duración del contrato, los derechos sobre la información, etc. Estos documentos están disponibles como anexos a este trabajo.



ACUERDO DE CONFIDENCIALIDAD Y SECRETO

Menorca, 1 de octubre[de 2019]

REUNIDOS

D. Ruben Mesquida Gomila, mayor de edad y con domicilio en Menorca, con DNI 417452523Q, Perito Judicial Informática Forense con N.º de colegiado 07760.

D. Juan García Pérez mayor de edad y con DNI. 45875365H en nombre y representación de la empresa Servicios Integrales Tecnológicos S.A con CIF A07818501

EXPONEN

- Que ambas partes de reconocen capacidad suficiente para suscribir el presente contrato.
- Que durante el tiempo de relación las partes intercambiarán o crearán información, la cual están interesadas en regular la confidencialidad y secreto mediante las siguientes:

CONDICIONES

Objeto

Con el presente contrato las partes fijan formalmente y por escrito los términos y las condiciones bajo las que mantendrán la confidencialidad de la información suministrada y creada entre ellos.

A los efectos de este acuerdo, tendrá la consideración de información confidencial, toda la información susceptible de ser revelada por escrito, de palabra o por cualquier otro medio o soporte. Este acuerdo obliga a las partes a adoptar las medidas oportunas para asegurar el tratamiento confidencial de la información.

Duración

Este acuerdo tendrá una duración indefinida desde el momento de su firma. En caso de que no se renueve el contrato, ambas partes deberán devolver a la otra toda la información remitida entre sí, comprometiéndose a la destrucción de la misma.

Cada parte se compromete a mantener el compromiso de confidencialidad respecto a la información y material intercambiado entre las partes, de forma indefinida tras la finalización de este acuerdo.

Confidencialidad

Las partes se obligan a entregar todo el material que sea necesario, y en el caso de ser este confidencial se comprometen a:

- a. Utilizar dicha información de forma reservada.
- b. No divulgar ni comunicar la información facilitada por la otra parte.
- c. Impedir la copia o revelación de esa información a terceros, salvo que gocen de aprobación escrita de la otra parte.
- d. Restringir el acceso a la información a sus empleados y subcontratados, en la medida en que razonablemente puedan necesitarla para el cumplimiento de sus tareas acordadas.

Ilustración 3 Anexo 1a Acuerdo confidencialidad 1



ACUERDO DE CONFIDENCIALIDAD Y SECRETO

e. No utilizar la información o fragmentos de ésta para fines distintos de la ejecución de este contrato. Las partes serán responsables entre sí, ante el incumplimiento de esta obligación, ya sea por sus empleados o por subcontratados. Las partes mantendrán esta confidencialidad y evitarán revelar la información a toda persona que no sea empleado o subcontratado.

Derechos previos sobre la información

Toda información puesta en común entre las partes es de propiedad exclusiva de la parte de donde proceda, y no es precisa la concesión de licencia para dicho intercambio. Ninguna de las partes utilizará información previa de la otra parte para su propio uso, salvo que se autorice lo contrario.



Clausula penal

Las partes se comprometen a cumplir con todos los términos fijados en el presente contrato, y muy especialmente aquellos relativos a las cláusulas sobre propiedad intelectual e industrial, confidencialidad y obligación de secreto. El incumplimiento de estas obligaciones determinará a elección de la parte que no incumplió el contenido de los términos fijados en el presente contrato:

- a. La resolución del contrato.
- b. El abono 50% de la parte presupuestada en concepto de penalización

Derechos de propiedad

Toda información intercambiada es de propiedad exclusiva de la parte de la cual proceda. Ninguna de las partes utilizará información de la otra para su beneficio independiente.

Protección de datos

Para la correcta aplicación del presente acuerdo, ambas partes podrían tener acceso a datos de carácter personal protegidos por la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, por lo que se comprometen a efectuar un uso y tratamiento de los datos afectados que será acorde a las actuaciones que resulten necesarias para la correcta prestación de servicios regulada en este acuerdo.

Asimismo, las partes asumen la obligación de guardar secreto profesional sobre cuanta información pudieran recibir, gestionar y articular con relación a los datos personales y a no comunicarlos a terceros, salvo las excepciones mencionadas, así como a destruirlos, cancelarlos o devolverlos en el momento de la finalización de la relación contractual entre ambas partes, así como a aplicar las medidas de seguridad necesarias.

Los derechos de acceso, rectificación, cancelación y oposición podrán ejercitarse mediante escrito dirigido a las direcciones de los firmantes del presente documento que constan en el encabezamiento.

Confidencialidad del acuerdo

Las partes acuerdan que este acuerdo reviste el carácter de confidencial y por tanto se prohíbe su divulgación a terceros.

Modificación o cancelación

Ilustración 4 Anexo 1a Acuerdo Confidencialidad 2



ACUERDO DE CONFIDENCIALIDAD Y SECRETO

Este acuerdo sólo podrá ser modificado con el consentimiento expreso de ambas partes, en documento escrito y mencionando la voluntad de las partes de modificar el presente acuerdo.

Jurisdicción

Las partes se comprometen a resolver de manera amistosa cualquier desacuerdo que pueda surgir en el desarrollo del presente contrato.

Firmando este documento usted está aceptando los Términos y Condiciones contenidos en este contrato y declara expresamente su aceptación. En caso de no aceptar en forma absoluta y completa los términos y condiciones de este contrato se dará por cancelado el contrato como el caso creído.	
Firma Cliente 	Firma Perito

Ilustración 5 Anexo 1a Acuerdo confidencialidad 3

 <h2 style="text-align: center;">Formulario Solicitud de Servicio</h2>				N.º Caso: IB07683811
Información del Cliente				
Fecha: 01/10/2019	Nombre: Juan	Apellidos: García Pérez (SITSA)	NIF / CIF: CIF A07818501	
País: España		Correo electrónico: j.garcia@sitsa.com	N.º Teléfono: 605 26 57 85	
Dirección: Av. Jaime el Conquistador 3		Código Postal: 07760	Provincia: Baleares	
Información del Caso				
Nombre Caso: Sitsa / IB07683811		Tipo Caso: Filtración información		
Impacto: <input checked="" type="radio"/> Alto <input type="radio"/> Medio <input type="radio"/> Bajo	Proceso Judicializado: <input checked="" type="radio"/> Sí <input type="radio"/> no	Valoración: Se valora con un impacto medio debido a que la filtración de la información puede acarrear perdidas a la empresa, pero no significa que esta empresa vaya a cerrar o para su habitual funcionamiento.		
Perito responsable: Ruben Mesquida Gomila			N.º Colegiado: 07760	
Correo Electrónico del perito: ruben.mesquida@perito.com			N.º Teléfono perito: 600 80 50 40	
Firma Cliente: 	Firmando usted acepta la información presentada es correcta para la realización del análisis forense. Este formulario debe ser entregado antes con máximo de 45 días después de la fecha especificada			Firma Perito: 
Más Información				
Tipo de dispositivo: <input checked="" type="checkbox"/> Sobre mesa <input checked="" type="checkbox"/> Portátil <input checked="" type="checkbox"/> Móvil <input type="checkbox"/> Otros		Sistema Operativo/s: <input checked="" type="checkbox"/> Windows <input type="checkbox"/> Apple / Mac <input type="checkbox"/> Linux / Unix <input checked="" type="checkbox"/> Android <input type="checkbox"/> Otros		
Ha sido analizado antes: <input checked="" type="checkbox"/> Sí <input type="checkbox"/> No		En caso afirmativo indique el resultado y por quien se realizó:		
Contienen información sensible: <input checked="" type="checkbox"/> Sí <input type="checkbox"/> No		En caso afirmativo indique: Contiene distintos diseños de dispositivos y patentes de la empresa		
Requiere un manejo o cuidado especial: <input checked="" type="checkbox"/> Sí <input type="checkbox"/> No		En caso afirmativo indique:		
Servicios Demandados: Por favor, enumere cada dispositivo con sus números de serie. Describa EN DETALLE el problema y el servicio que solicita; consulte la página 2 para obtener más información. Si usted tiene documentos suplementarios que pueden ayudar en el análisis, adjúntelos a esta solicitud.				
<p>El pasado 30 de septiembre detectamos una filtración de distintos diseños y planos de nuestros nuevos dispositivos que tenían que salir al mercado en breve. Esto nos puede provocar problemas en el lanzamiento lo que provocaría perdidas para la empresa.</p> <p>Después de investigar internamente el suceso, se descubrió que los dispositivos afectados fueron los de uno de los directores, estos dispositivos son los siguientes:</p> <ul style="list-style-type: none"> • Ordenador portátil Dell XPS con sistema Windows 7 y número de serie 0417852369 El usuario dejó de utilizar el ordenador el 23 debido a que empezó vacaciones. <p>Por eso pedimos que se analicen estos dispositivos en busca de malware, algún acceso remoto, y en búsqueda de información que haya sido sustraída o accedida sin el consentimiento de la empresa. Dependiendo del resultado nos gustaría que se judicializara el proceso.</p>				
Si se produce la aceptación de su caso se le proporcionará un nuevo documento con su presupuesto y la información relativa.				

Ilustración 6. Anexo 1b. Formulario Solicitud de Servicios

En nuestro caso vemos que se trata de una empresa que ha sufrido una filtración detectada el 30 de septiembre y que sospechan que los dispositivos de uno de sus directores han podido ser comprometidos en el formulario se comenta que:

"El pasado 30 de septiembre detectamos una filtración de distintos diseños y planos de nuestros nuevos dispositivos que tenían que salir al mercado en breve. Esto nos puede provocar problemas en el lanzamiento lo que provocaría perdidas para la empresa.

Después de investigar internamente el suceso, se descubrió que los dispositivos afectados fueron los de uno de los directores, estos dispositivos son los siguientes:

- *Ordenador portátil Dell XPS con sistema Windows 7 y número de serie 0417852369*

El usuario dejó de utilizar el ordenador el 23 debido a que empezó vacaciones.

Por eso pedimos que se analicen estos dispositivos en busca de malware, algún acceso remoto, y en búsqueda información que haya sido sustraída o accedida sin el consentimiento de la empresa. Dependiendo del resultado nos gustaría que se judicializara el proceso.”

En el formulario nos comentan que los dispositivos afectados son un ordenador portátil Dell XPS con Windows 7 y N.º de serie 04178523697 que se dejó de utilizar día 23 de septiembre. Teniendo en cuenta esto se nos pide que analicemos estos dispositivos en busca de malware, algún acceso remoto, y en búsqueda información que haya sido sustraída o accedida sin el consentimiento de la empresa.

Como apunte debemos tener en cuenta que según lo comentado el proceso sea judicializado por lo tanto en la siguiente fase de adquisición debemos tener en cuenta que debe realizarse delante de un notario.

Teniendo la información, deberemos preservar los dispositivos, es decir mantenerlos para que se conserven de una forma íntegra, y que se eviten manipulaciones o posibles efectos adversos sobre ellos. Para ello hasta que llegue el personal técnico deberá ser desconectado de la red y evitar su uso.

El personal que lo manipule deberá hacerlo con la indumentaria adecuada (pulsera antiestática, evitar llevar equipos de radiofrecuencia...), una vez manipulados deberán ser precintados y sellados hasta que se le haga el análisis forense. Además, estos dispositivos deberán ser almacenados de forma segura en una caja fuerte o en un lugar adecuado.

Revisado el caso por parte del perito se le ofrecerá un presupuesto aproximado al cliente de los honorarios del perito.



Ruben Mesquida Gomila

Presupuesto

Menorca, 1 de octubre de 2019

REUNIDOS

D. **Ruben Mesquida Gomila**, mayor de edad y con domicilio en Menorca, con DNI 417452523Q, Perito Judicial Informática Forense con N.^º de colegiado 07760.

D. **Juan García Pérez** mayor de edad y con DNI. 45875365H en nombre y representación de la empresa **Servicios Integrales Tecnológicos S.A** con CIF A07818501

EXPONEN

Que ambas partes de reconocen capacidad suficiente para suscribir el presente contrato.

SERVICIOS SOLICITADOS

El cliente solicita los servicios para que se realice un informe pericial de los siguientes dispositivos que pertenecen a susodicha empresa

Los dispositivos incluidos en el caso son los siguientes:

- Ordenador portátil Dell XPS con sistema Windows 7 y número de serie 0417852369

Donde se analizarán en búsqueda de malware, algún acceso remoto, y en búsqueda información que haya sido sustraída o accedita sin el consentimiento de la empresa

ACEPTACIÓN DEL CASO

El Perito **Ruben Mesquida Gomila**, acepta el caso que se abrió con código IB07683811 por parte de la empresa **Servicios Integrales Tecnológicos S.A** con CIF A07818501, y este, por parte de satisfacer la correspondiente minuta de honorarios por el trabajo a realizar de análisis forense se determinan los siguientes honorarios descritos a continuación.

HONORARIOS

Los honorarios serán determinados, conforme a los usos y normas de la informática forense, atendiendo al asunto, su complejidad de su desarrollo, esfuerzo profesional, éxito o fracaso de las pretensiones del cliente, incidencias habidas en su tramitación, etc.

El Perito Informático fijará su minuta, atendiendo las circunstancias antes expresadas o cualesquier otras que considere dignas de ser tenidas en cuenta.

Salidas del despacho, laboratorio, recursos, incidencias, dietas, viajes, etc., serán honorarios con independencia del asunto principal.

METODO DE PAGO

El cliente **Servicios Integrales Tecnológicos S.A** con CIF A07818501, realizará el pago en 2 plazos personalmente o de manera telemática la cantidad de 3561,83 euros, correspondientes al 50% de la cuantía mínima calculada, importe total estimado del peritaje es de 7123,66 euros

Ilustración 7 Anexo 1c Presupuesto 1



Ruben Mesquida Gomila

al 50% de la cuantía mínima calculada, importe total estimado del peritaje es de 7123,66 euros impuestos incluidos. Si el pago es realizado de forma telemática se deberá realizar en la cuenta N.^º ES65 0123 4567 7890 3216 5498 cuyo titular es D. **Ruben Mesquida Gomila**. El resto se abonará una vez se haya entregado el informe pericial completo.

<p>Firmando este documento usted está aceptando los Términos y Condiciones contenidos en este contrato y declara expresamente su aceptación. En caso de no aceptar en forma absoluta y completa los términos y condiciones de este contrato se dará por cancelado el contrato como el caso creído.</p>	
	

Ilustración 8 Anexo 1c Presupuesto 2

7. FASE DE ADQUISICIÓN

Una vez completada la fase inicial y después de recopilar toda la información posible, y haber llenado toda la documentación necesaria nos dispondremos a adquirir las imágenes.

Como indica el cliente dependiendo de los resultados quiere judicializar el proceso, por lo tanto deberemos contar con un notario al realizar la adquisición de estas imágenes.

En la fase de adquisición se tiene que tener en cuenta la orden de la volatilidad, en primer lugar, se tendrán que adquirir las pruebas más volátiles como memoria RAM y por último las menos volátiles como el disco duro.

7.1 ADQUISICIÓN DE IMAGEN DE MEMORIA VOLÁTIL

En primer lugar, se adquirirá la memoria RAM debido a que es una memoria volátil y si se apagará el equipo se perderían posibles evidencias que podrían existir. Gracias a esta imagen podremos obtener los procesos en ejecución, procesos en fase de finalización, conexiones activas, datos, contraseñas, etc. Por este motivo es importante en estos casos antes de apagar el equipo realizar la adquisición de la memoria volátil.

En nuestro caso para la realización del volcado de la memoria la hemos realizado con la herramienta Dumplt que es una herramienta portable y fácil de utilizar, con lo que evitamos crear un impacto mayor en el equipo no teniendo que instalar ninguna aplicación de este modo habrá menos “manchas” en el equipo.

Para el proceso de adquisición conectaremos un dispositivo de almacenamiento al equipo con la herramienta, abriremos una terminal nos dirigiremos a la ruta y ejecutaremos el siguiente comando.

```

Administrator: Símbolo del sistema
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>Z:
Z:\>cd Herramientas
Z:\Herramientas>winpmem_v3.3.rc3.exe --format=raw -o win7-ram
Z:\Herramientas>dumpit.exe

DumpIt 3.0.20190919.1 (X64) (Sep 19, 2019)
Copyright (c) 2007 - 2020, Matt Suiche (nsuiche)
Copyright (c) 2016 - 2020, Comae Technologies DMCC <https://www.comae.com>
All rights reserved.

DumpIt is the best for acquisition but... our platform Stardust is the also best for analysis!
Access it on https://my.comae.com - info@comae.com if you have any questions.

Destination path:      Z:\Herramientas\USUARIO-PC-20191003-102619.dmp
Computer name:          USUARIO-PC

--> Proceed with the acquisition ? [y/n] y
[+] Information:
Dump Type:              Microsoft Crash Dump

[+] Machine Information:
Windows version:        6.1.7601
MachineId:               269E14E4-9D90-D249-B46C-604C844DAB35
TimeStamp:                132145719023957500
Cr3:                      0x1879000
KdDebuggerData:           0xfffff800027f40a0
Current date/time:       [2019-10-03 (YYYY-MM-DD) 10:26:22 (UTC)]
+ Processing... Done.

Acquisition finished at: [2019-10-03 (YYYY-MM-DD) 10:26:42 (UTC)]
Time elapsed:             0:20 minutes:seconds (20 secs)

Created file size:        2147024996 bytes (2047 Mb)
Total physical memory size: 2047 Mb
NtStatus (troubleshooting): 0x00000000
Total of written pages:   524174
Total of inaccessible pages: 0
Total of accessible pages: 524174

SHA-256: 58B6D9C9BF2F1C934BC3302D60F42C94E1CC06D2A8B299B933075A17531C8C678

JSON path:                Z:\Herramientas\USUARIO-PC-20191003-102619.json

Z:\Herramientas>
```

Ilustración 9. Adquisición RAM DumpIT

Al ejecutarlo empezara el proceso que tardara algunos minutos.

7.2 ADQUISICIÓN DE IMAGEN DE DISCO DURO

Después de haber adquirido la imagen de la memoria RAM, procederemos a crear la imagen del disco duro. Para la creación de esta hemos elegido CAINE es una distribución Linux enfocada al análisis forense que tiene disponibles distintas herramientas para dicho fin.

En nuestro caso la herramienta utilizada será Guymager que es una herramienta gratuita para la adquisición de imágenes forenses. Se ha elegido esta herramienta debido a que es una herramienta gratuita y libre, no hay que instalar ningún tipo de software sobre el equipo debido a que ese ejecuta sobre el live-cd de CAINE y según distintos test en segun casos es más rápida que otras herramientas disponibles en el mercado como FTK Imager. [Test Software Creación de imágenes](#)

El primer paso para crear la imagen debemos crear un live-cd para ello hemos utilizado Rufus que nos permite crear el live-cd de CAINE en un pendrive

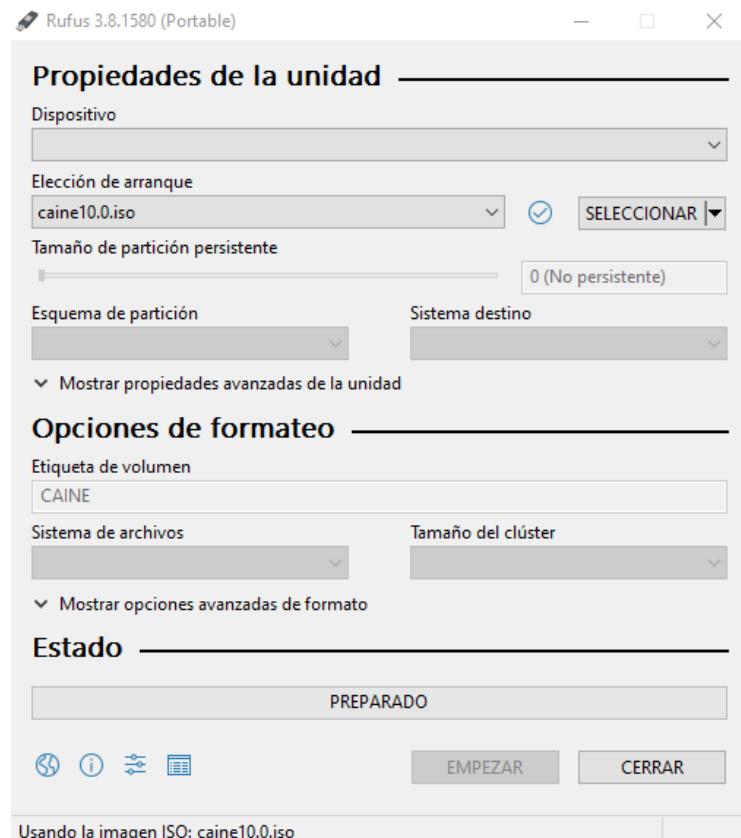


Ilustración 10. Rufus

Una vez creado el live-cd debemos enchufar el pendrive en uno de los puertos de la máquina y deberemos arrancar desde el.



Ilustración 11. Arranque CAINE

Una vez cargado CAINE conectaremos el disco duro donde copiaremos la imagen, debemos tener en cuenta que CAINE monta por precaución los discos como solo lectura, por lo tanto, el disco duro donde copiaremos la imagen debemos ponerlo de forma que podamos escribir en él. Para ello tenemos una herramienta que se llama UNBLOCK que otorga los permisos de escritura al disco que seleccionemos

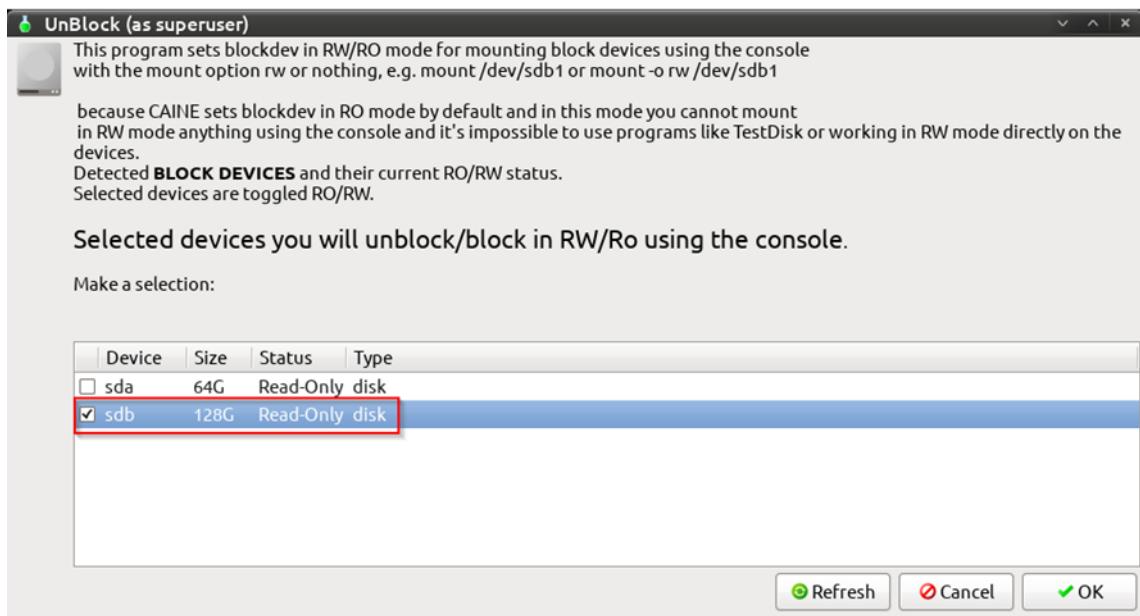


Ilustración 12. Unblock CAINE

O desde la terminal podemos montar de nuevo el disco, con el siguiente comando

```
Sudo mount -o remount, rw /dev/sd? /media/punto_de_montaje
```

Solucionado el tema del disco, abriremos la herramienta Guymager

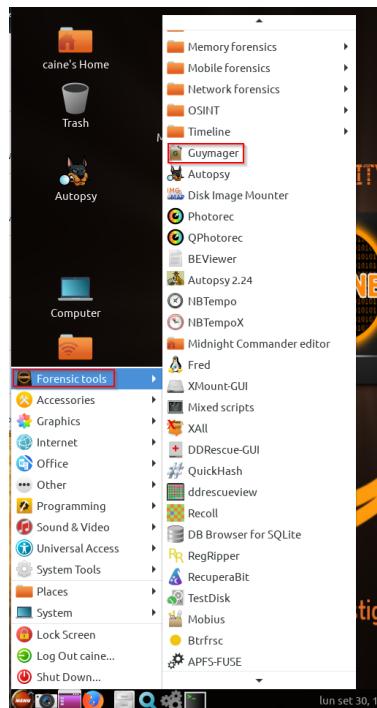


Ilustración 13. Menú CAINE

Abierta la herramienta Guymager seleccionamos el disco (debemos tener cuidado en elegir el disco adecuado), con botón derecho Acquire Image

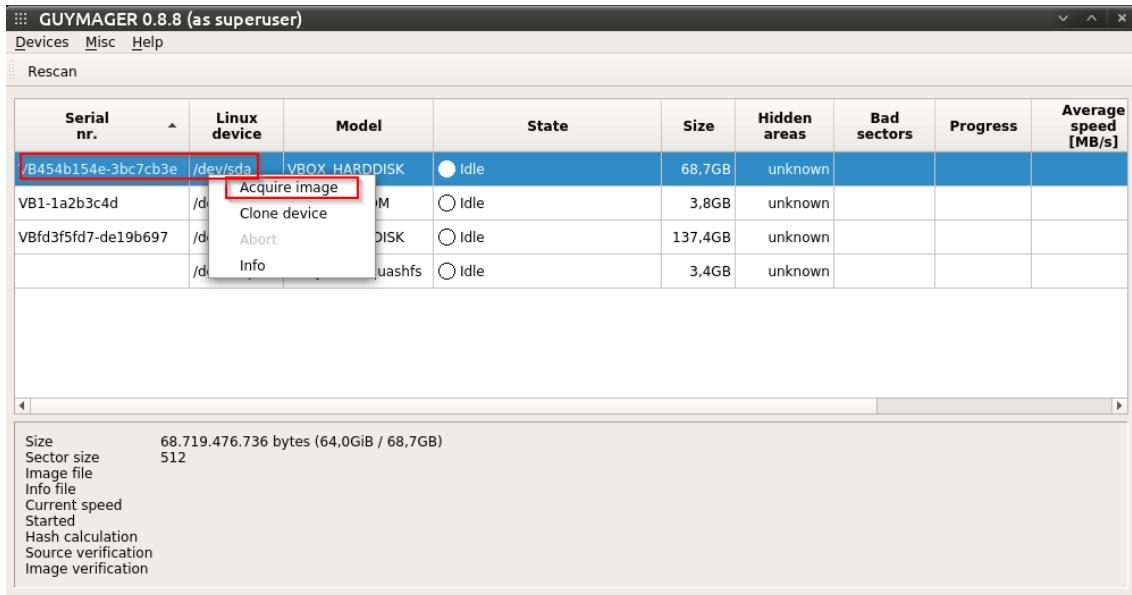


Ilustración 14. Guymager 1

En la siguiente ventana, hemos elegido el formato dd en un único archivo, debido a que el formato dd es compatible con la gran mayoría de herramientas forenses. Seleccionaremos el lugar de almacenamiento en este caso el disco duro comentado antes

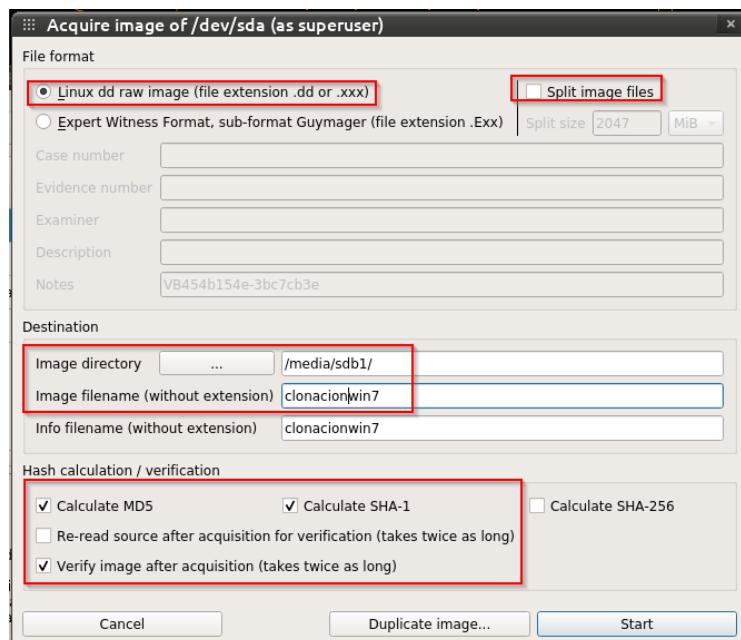


Ilustración 15. Guymager 2

Completado el paso anterior comenzara la adquisición de la imagen

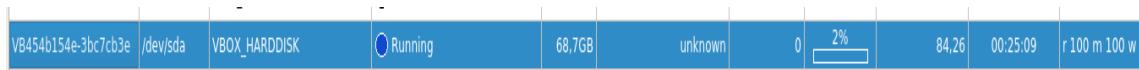


Ilustración 16. Guymager 3

Cuando haya acabado veremos que nos aparecerá 100% y cambiara el símbolo a verde



Ilustración 17. Guymager 4

Terminada la clonación podemos quitar el disco y el pendrive, y podemos apagar el equipo. Tanto el disco como el equipo deberán almacenarse en un lugar seguro para evitar posibles alteraciones.

7.3 VALIDACIÓN DE LAS IMÁGENES

Obtenidas las imágenes deberemos obtener las respectivas sumas de verificación tanto en MD5 como en SHA1. Para ello desde Windows hemos utilizado FCIV que por defecto no viene instalado, pero se puede obtener desde el siguiente paquete de Microsoft <https://support.microsoft.com/en-us/help/841290>. Desde sistemas UNIX se puede utilizar los comandos md5sum y sha1sum.

Bien teniendo instalado FCIV procederemos a calcular las sumas de verificación

```
C:\Users\MesQ\Desktop\TFM_RubenMesquidaGomila\Imagenes>fciv -md5 -sha1 USUARIO-PC-20191003-102619.dmp
//
// File Checksum Integrity Verifier version 2.05.
//
      MD5           SHA-1
4c7964abccef792f0f3c49f96a1b006a 3d373b2cf20a54926b68b4902e30b306cf7eb8 usuario-pc-20191003-102619.dmp
C:\Users\MesQ\Desktop\TFM_RubenMesquidaGomila\Imagenes>
```

Ilustración 18. Verificación Inicial RAM

```
C:\Users\MesQ\Desktop\TFM_RubenMesquidaGomila\Imagenes>fciv -md5 -sha1 d:\clonacionwin7.dd
//
// File Checksum Integrity Verifier version 2.05.
//
      MD5           SHA-1
-----
93bbf050c944575865bde97ed815b09a 9b6f2e9e39b125a77d2ec672bbda4cc14411e839 d:\clonacionwin7.dd
C:\Users\MesQ\Desktop\TFM_RubenMesquidaGomila\Imagenes>
```

Ilustración 19. Verificación Inicial Disco

7.4 CADENA DE CUSTODIA

Al ser un caso judicializado, deberemos cumplir de forma correcta la cadena de custodia, debido a que, si no se cumple bien, todo el trabajo hecho podría ser inútil a causa de que en el juicio se podría rechazar debido a no haber cumplido dicha cadena de custodia.

Para ello antes de empezar la adquisición deberemos hacer fotos del entorno, identificar los equipos, crear un video con fecha y hora de la creación. Y deberíamos separar y asegurar todos los dispositivos que van a intervenir.

Aparte deberemos crear una documentación donde tendremos un formulario de la adquisición de las imágenes, registros de control (entrada-salida) de las evidencias obtenidas, y por último un acta notarial creado por este fedatario público que garantizará que el trabajo de adquisición esté ajustado a la más estricta legalidad.

A continuación, tenemos el formulario creado para nuestro caso que incluye la información referente donde se ha recogido, los detalles del dispositivo, los detalles de la imagen y la firma del acta.

Como segunda parte de este documento se incluye el formulario de registro entrada-salida que comentábamos antes.

Evidencia	
Caso N.º: IB07683811	Evidencia N.º: 02
Sección A: Evidencia Recogida	
Fecha 01/10/2019 14:33	Realizado por Ruben Mesquida Gomila
Dirección Av. Constitución 3, Ciutadella de Menorca	
Sección B: Detalles Evidencia	
Fecha 01/10/2019 14:33	
Localización Ciutadella de Menorca,	
Tipo de Dispositivo Portátil	Capacidad 64GB
Marca Dell	Modelo XPS 15 2019
N.º Serie 0417852369	
Información Adicional...	
No se han detectado arañazos ni desperfectos en el equipo	
Imagen tomada <input checked="" type="checkbox"/> Sí <input type="checkbox"/> No	
Detallar daños, desperfectos o arañazos	
Sección C: Detalles Imagen	
Fecha 01/10/2019 15:33	Realizada por Ruben Mesquida Gomila
Localización Ciutadella de Menorca	
Nombre archivo clonacionwin7.dd	Tamaño Imagen 64 (GB)
MD5 93bbf050c9445758655de97ed815b09a	
SHA-1 9b6f2e9e39b125a77d2ec672bbda4cc14411e639	
Información Adicional...	
Esta segunda evidencia se trata de la imagen del disco duro del equipo.	
<p>Este formulario se utiliza para recoger un dispositivo de hardware que contiene datos que pueden ser de interés en un caso. Directrices:</p> <ul style="list-style-type: none"> - Asegurarse de que este formulario sólo se refiere a un elemento de prueba y de que se cumple uno para cada elemento de prueba. - Este formulario debe ir acompañado de formularios de Cadena de Custodia que detallan los individuos que han manejado la evidencia. - En la Sección D se pueden encontrar otras observaciones al dorso: Observaciones - Es importante que estos formularios se mantengan junto con las pruebas en todo momento. - En el momento de la entrega o eliminación, por favor complete la Sección E: Entrega de pruebas. 	

Ilustración 20. Cadena custodia formulario 1

<p>Este formulario se utiliza para recoger un dispositivo de hardware que contiene datos que pueden ser de interés en un caso. Directrices:</p> <ul style="list-style-type: none"> - Asegurarse de que este formulario sólo se refiere a un elemento de prueba y de que se cumple uno para cada elemento de prueba. - Este formulario debe ir acompañado de formularios de Cadena de Custodia que detallan los individuos que han manejado la evidencia. - En la Sección D se pueden encontrar otras observaciones al dorso: Observaciones - Es importante que estos formularios se mantengan junto con las pruebas en todo momento. - En el momento de la entrega o eliminación, por favor complete la Sección E: Entrega de pruebas. 	
Evidencia	
Sección D: Observaciones	
Se realizó la adquisición de la imagen del disco con la distribución Linux CAINE, mediante la herramienta Guymager . se adquirió la imagen bit a bit donde se almacenó en un disco duro Western Digital con N.º de serie 0305048796	

Ilustración 21. Cadena custodia formulario 2

Sección E: Acta	
Fecha 01/10/2019	
Propietario Juan García Pérez	Firma 

Perito Ruben Mesquida Gomila	Firma 
Atestiguado por Notario. Pablo Pérez Pérez	Firma 
Cadena de Custodia	
Caso N.º IB07683811	Evidencia N.º 02
Este formulario debe acompañar a un formulario de Evidencia y la respectiva evidencia.	
Cadena de Custodia	
Recoge	Devuelve
Nombre: Juan García Pérez	Nombre: Ruben Mesquida Gomila
Firma: 	Firma:

Ilustración 22. Cadena de custodia formulario 3

Después del formulario tendríamos el acta de presencia del notario atestiguando la adquisición de las imágenes y dando fe a las sumas de verificación obtenidas por parte del perito.

ACTA NOTARIAL DE PRESENCIA

En la ciudad de Ciutadella de Menorca, a 1 de octubre del año 2019 siendo las doce horas, YO: PABLO PÉREZ PÉREZ, Notario, constituido en la Avenida Constitución N.º 3 de esta ciudad, a requerimiento del señor RUBEN MESQUIDA GOMILA con JUAN GARCIA PEREZ Gerente de Sitsa SA, a quien juramento de la manera siguiente: ¿Prometéis bajo juramento decir verdad en lo que fuereis preguntado?

CONTESTAN: Sí, bajo juramento prometemos decir verdad en lo que se nos pregunté, por lo que acto seguido les hice saber lo relativo al delito de Perjurio y pena consiguiente, de lo cual me dicen estar perfectamente enterados y seguidamente dicen llamarse Ruben Mesquida Gomila con número de identificación 41745223 y Perito N.º Colegiado 07760, y JUAN GARCIA PEREZ Gerente de Sitsa SA y en representación de esta con número de identificación 45875365H. Con el objeto de asentar la presente acta notarial, para el efecto procedo de la manera siguiente:

PRIMERO: El requirente Ruben Mesquida Gomila en este acto procede a la adquisición de las distintas imágenes de los equipos del señor Juan García Pérez Ordenador portátil Dell XPS con sistema Windows 7 y número de serie 0417852369 y Google Pixel 3 con sistema Android 8.1 con número de serie 369258147, se obtienen las distintas imágenes con las siguientes sumas de verificación:

- Imagen RAM Ordenador portátil: MD5: 4c7964abcef792f0f3c49f96a1b006a SHA1: 3d373b2fd20a54926b68b4902e30b306cf7eb8
- Imagen Disco Ordenador portátil: MD5: 93bbf050c944575865bde97ed815b09a SHA1: 9b6f2e9e39b125a77d2ec672bbda4cc14411e839

SEGUNDO: No habiendo más que hacer constar se finaliza la presente acta, en una hoja de papel bond tamaño oficio, utilizada únicamente de anverso, a la que se le adhiere un timbre notarial del valor 838,67 euros la cual se hace entrega al mismo interesado para los usos legales que le convengan. Leído que le fue lo escrito al requirente, enterado de su contenido, lo ratifica, acepta y firma de conformidad. Doy fe.

Firma: Ruben Mesquida Gomila.

Perito Informático

Firma: Juan García Pérez

Gerente Sitsa S.A

ANTE MÍ: Lic. Pablo Pérez Pérez.

Notario.



Ilustración 23. Acta notarial de presencia

8. FASE DE ANÁLISIS E INVESTIGACIÓN

En esta fase de análisis que es la fase principal de un caso donde pretendemos dar respuesta al cliente propuesto y a los objetivos establecidos en el trabajo. Iremos revisando las distintas imágenes analizando por etapas cada una de ellas.

8.1 ANÁLISIS DE MEMORIA

En esta primera etapa del análisis procederemos a analizar la imagen y la memoria que obtuvimos antes.

Este análisis será realizado con Volatility que es una herramienta open-source para el análisis de memoria, se ha elegido a esta herramienta por la madurez del proyecto y la gran cantidad de plugin que hay.

Hay otra herramienta llamada Rekall que es un fork de volatility, pero también admite la adquisición de la memoria.

8.1.1. VALIDACIÓN

Antes de empezar con el análisis de la memoria hay que validar las sumas de verificación, para comprobar que la imagen no ha sido modificada en el transcurso de su adquisición hasta que se procede a su análisis. Este paso, aunque sencillo, es importante realizarlo debido a que si no coincidieran las sumas estaríamos rompiendo la cadena de custodia.

```
C:\Users\MesQ\Desktop\TFM_RubenMesquidaGomila\Imagenes>fciv -md5 -sha1 USUARIO-PC-20191003-102619.dmp
// File Checksum Integrity Verifier version 2.05.
//          MD5           SHA-1
-----
4c7964abcccef792f0f3c49f96a1b006a 3d373b2cf20a54926b68b4902e30b306cf7eb8 usuario-pc-20191003-102619.dmp
C:\Users\MesQ\Desktop\TFM_RubenMesquidaGomila\Imagenes>
```

Ilustración 24. Validación Imagen RAM

En nuestro caso vemos que las sumas de verificación coinciden con las que obtuvimos al principio.

8.1.2. INFORMACIÓN DE LA IMAGEN

Validada la imagen de la memoria, como punto de partida se deberá identificar el sistema de la imagen, para ello se utilizará el argumento imageinfo que realizará una búsqueda en las estructuras de depuración del núcleo (KDBG) para identificar el sistema y darnos el perfil adecuado para poder realizar el análisis.

```
C:\Users\MesQ\Desktop\TFM_RubenMesquidaGomila\Imagenes>volatility_2.6_win64_standalone.exe -f USUARIO-PC-20191003-102619.dmp imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
```

Ilustración 25. Imageinfo 1



```
→ Suggested Profile(s) : Win8SP0x64, Win81UIx64, Win10x64_14393, Win10x64_10586, Win10x64, Win2012R2x64_18340, Win2012R2x64, Win2010x64_14393, Win2012x64, Win8SP1x64_18340, Win8SP1x64 (Instantiated with Win8SP1x64)
AS Layer1 : WindowsAM0x64PagedMemory (Kernel AS)
AS Layer2 : WindowsCrashDumpSpace64 (Unnamed AS)
AS Layer3 : WindowsAddressSpace (C:\Users\MesQ\Desktop\TFM_RubenMesquidaGomila\Imagenes\USUARIO-PC-20191003-102619.dmp)
PAE type : NO PAE
DTB : 0x1870000L
KDBG : 0xf000027f4000L
Number of Processors : 1
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0xfffff800027f5d00L
KUSER_SHARED_DATA : 0xfffff780000000000L
Image date and time : 2019-10-03 16:16:22 UTC+0000
Image local date and time : 2019-10-03 21:26:22 +0200
```

Ilustración 26. Imageinfo 2

De los perfiles anteriores propuestos, al final se utilizó Win7SP1x64 que es el que se identificó que funcionaba correctamente con la imagen obtenida.

8.1.3. PROCESOS ACTIVOS

Identificada la imagen, ejecutaremos volatility con el argumento pslist que nos muestra los procesos activos en el momento de la adquisición de la imagen. Este es útil para hacer un cribado inicial para buscar procesos desconocidos o procesos conocidos con un nombre ligeramente diferente como scvhost.exe.

En la imagen siguiente podemos ver la salida de pslist, donde podemos ver un proceso extraño qVhPAJWr.exe con PID 3204

Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0xfffffa80021aa040 System	4	0	78	536	-----	0	2019-10-02 15:33:36 UTC+0000	
0xfffffa800214f500 smss.exe	248	4	2	29	-----	0	2019-10-02 15:33:36 UTC+0000	
0xfffffa80028cb30 csrss.exe	320	312	10	523	0	0	2019-10-02 15:33:37 UTC+0000	
0xfffffa8002a04060 wininit.exe	368	312	3	73	0	0	2019-10-02 15:33:40 UTC+0000	
0xfffffa8002a04060 csrss.exe	370	360	9	401	1	0	2019-10-02 15:33:40 UTC+0000	
0xfffffa8002b06510 winlogon.exe	484	369	3	113	1	0	2019-10-02 15:33:43 UTC+0000	
0xfffffa8002b7c730 services.exe	468	368	9	197	0	0	2019-10-02 15:33:41 UTC+0000	
0xfffffa8002b13b30 lsass.exe	472	368	7	600	0	0	2019-10-02 15:33:41 UTC+0000	
0xfffffa8002b8a30 lsm.exe	480	368	10	153	0	0	2019-10-02 15:33:41 UTC+0000	
0xfffffa8002c4d060 svchost.exe	584	460	10	356	0	0	2019-10-02 15:33:42 UTC+0000	
0xfffffa8002c7c200 VBoxService.exe	644	460	12	137	0	0	2019-10-02 15:33:42 UTC+0000	
0xfffffa8002c7d000 svchost.exe	712	460	5	273	0	0	2019-10-02 15:33:44 UTC+0000	
0xfffffa8002cdd4f00 svchost.exe	804	469	19	405	0	0	2019-10-02 15:33:44 UTC+0000	
0xfffffa8002d43400 svchost.exe	864	468	16	372	0	0	2019-10-02 16:33:44 UTC+0000	
0xfffffa8002d5e300 svchost.exe	888	460	35	1205	0	0	2019-10-02 16:33:44 UTC+0000	
0xfffffa8002d5f600 svchost.exe	332	460	14	339	0	0	2019-10-02 16:33:45 UTC+0000	
0xfffffa8002e73610 svchost.exe	932	460	15	453	0	0	2019-10-02 16:33:45 UTC+0000	
0xfffffa8002f19060 spoolsv.exe	1152	460	12	281	0	0	2019-10-02 16:33:46 UTC+0000	
0xfffffa8002f46b90 svchost.exe	1180	460	17	297	0	0	2019-10-02 16:33:47 UTC+0000	
0xfffffa8002f46b90 armvcs.exe	1200	460	5	73	0	0	2019-10-02 16:33:47 UTC+0000	
0xfffffa8002f46b90 taskhost.exe	1328	469	15	243	0	0	2019-10-02 16:33:47 UTC+0000	
0xfffffa8002f46b90 taskhost.exe	1688	460	5	96	0	0	2019-10-02 16:33:47 UTC+0000	
0xfffffa8002f46b90 taskhost.exe	1992	460	9	287	1	0	2019-10-02 16:35:20 UTC+0000	
0xfffffa8002d5a740 dwm.exe	312	864	3	72	1	0	2019-10-02 16:35:20 UTC+0000	
0xfffffa8001b5e420 explorer.exe	528	1088	29	994	1	0	2019-10-02 16:35:20 UTC+0000	
0xfffffa8002a6fd00 VBoxTray.exe	1372	528	13	141	1	0	2019-10-02 16:35:21 UTC+0000	
0xfffffa8002a6fd00 VBoxTray.exe	1608	528	13	178	1	0	2019-10-02 16:35:21 UTC+0000	
0xfffffa8002d2060 SearchIndexer	1944	468	11	608	0	0	2019-10-02 16:35:27 UTC+0000	
0xfffffa8002b5c130 wmpnetwk.exe	2092	460	11	248	0	0	2019-10-02 16:35:27 UTC+0000	
0xfffffa8002cfb480 sppsvc.exe	2484	460	5	147	0	0	2019-10-02 16:35:30 UTC+0000	
0xfffffa8002d1b630 svchost.exe	2712	460	13	315	0	0	2019-10-02 16:35:48 UTC+0000	
0xfffffa8002d27060 thunderbird.exe	2338	528	42	717	1	0	2019-10-02 17:03:21 UTC+0000	
0xfffffa8001d9e060 chrome.exe	2844	528	25	741	1	0	2019-10-02 17:03:35 UTC+0000	
0xfffffa8001d9e060 chrome.exe	2948	528	2	55	1	0	2019-10-02 17:03:35 UTC+0000	
0xfffffa8001d9e060 chrome.exe	2188	2844	12	294	1	0	2019-10-02 17:03:35 UTC+0000	
0xfffffa8001d9e060 chrome.exe	2256	2844	12	264	1	0	2019-10-02 17:03:35 UTC+0000	
0xfffffa8001e29aa0 chrome.exe	2088	2844	12	179	1	0	2019-10-02 17:03:35 UTC+0000	
0xfffffa8001e36030 chrome.exe	1392	2844	8	175	1	0	2019-10-02 17:03:44 UTC+0000	
0xfffffa8001e3d030 chrome.exe	2188	584	6	201	0	0	2019-10-02 17:03:55 UTC+0000	
0xfffffa8002e2f4030 chrome.exe	3164	2844	11	161	1	0	2019-10-02 17:04:50 UTC+0000	
0xfffffa8002e2f4030 chrome.exe	3164	304	18	303	0	0	2019-10-02 17:04:50 UTC+0000	
0xfffffa8002e2f4030 wscript.exe	3304	304	4	128	1	1	2019-10-02 17:07:41 UTC+0000	
0xfffffa8002e2f4030 wscript.exe	3312	528	1	20	1	0	2019-10-02 17:09:51 UTC+0000	
0xfffffa80030a060 conhost.exe	3320	376	2	54	1	0	2019-10-02 17:09:58 UTC+0000	
0xfffffa8002e8060 audiodec.exe	3800	804	6	126	0	0	2019-10-03 10:26:06 UTC+0000	
0xfffffa8002d93060 SearchProtocol	2228	1944	8	315	0	0	2019-10-03 10:26:06 UTC+0000	
0xfffffa8002a12530 SearchFilterHo	3228	1944	5	80	0	0	2019-10-03 10:26:06 UTC+0000	
0xfffffa8002917060 DumpIt.exe	3460	3312	5	88	1	0	2019-10-03 10:26:19 UTC+0000	
0xfffffa8001e83506 WmiPrvSE.exe	3252	584	8	120	0	0	2019-10-03 10:26:22 UTC+0000	

Ilustración 27. RAM Lista procesos

A continuación, para saber el árbol de procesos utilizaremos pstree que utiliza la salida de pslist y los muestra con la relación padre-hijo, esto es muy útil cuando la lista de procesos es enorme y nos permite ver cualquier relación sospechosa entre procesos.

En la siguiente imagen tenemos la salida de pstree donde vemos que el proceso anterior PID 3204 tiene como padre wscript.exe con PID 304

Name	Pid	PPid	Thds	Hnds	Time
0xfffffa8002f19060 spoolsv.exe	1152	460	12	281	2019-10-02 16:33:46 UTC+0000
0xfffffa800303100 armsvc.exe	1280	460	4	73	2019-10-02 16:33:47 UTC+0000
0xfffffa8002a20600 SearchIndexer	1944	460	11	600	2019-10-02 16:35:27 UTC+0000
0xfffffa8002a12530 SearchFilterHo	3228	1944	5	80	2019-10-02 16:36:06 UTC+0000
0xfffffa8002d1b630 SearchFilterHo	3230	1944	8	91	2019-10-02 16:36:06 UTC+0000
0xfffffa8002994170 taskhost.exe	1688	460	5	98	2019-10-02 16:31:47 UTC+0000
0xfffffa8002c7c200 VBoxService.exe	644	460	12	137	2019-10-02 15:31:42 UTC+0000
0xfffffa8002f46b90 taskhost.exe	1180	460	17	297	2019-10-02 16:33:47 UTC+0000
0xfffffa8002d1b630 svchost.exe	804	460	19	405	2019-10-02 16:34:41 UTC+0000
0xfffffa8002d1b630 wmpnetwk.exe	3080	460	5	106	2019-10-02 16:34:41 UTC+0000
0xfffffa8002d1b630 svchost.exe	2712	460	13	315	2019-10-02 16:35:48 UTC+0000
0xfffffa8002d1b630 wmpnetwk.exe	2992	460	11	245	2019-10-02 16:35:27 UTC+0000
0xfffffa8002d1b630 svchost.exe	1328	460	15	241	2019-10-02 16:33:47 UTC+0000
0xfffffa8002c5e300 svchost.exe	712	460	9	273	2019-10-02 16:33:44 UTC+0000
0xfffffa8002d1b630 svchost.exe	1456	460	9	319	2019-10-02 16:33:44 UTC+0000
0xfffffa8002d1b630 svchost.exe	2484	460	5	147	2019-10-02 16:36:30 UTC+0000
0xfffffa8002d4a400 svchost.exe	864	460	16	372	2019-10-02 16:33:44 UTC+0000
0xfffffa8002d5a740 dwm.exe	312	864	3	72	2019-10-02 16:35:20 UTC+0000
0xfffffa8002d5a740 svchost.exe	3070	312	18	523	2019-10-02 15:33:40 UTC+0000
0xfffffa8002d5a740 svchost.exe	368	312	3	133	2019-10-02 15:33:40 UTC+0000
0xfffffa8002b7c300 wmpnetwk.exe	468	368	9	197	2019-10-02 15:31:41 UTC+0000
0xfffffa8002b7c300 services.exe	584	460	10	356	2019-10-02 15:31:42 UTC+0000
0xfffffa8002b7c300 services.exe	3252	584	8	120	2019-10-02 16:26:22 UTC+0000
0xfffffa8002b7c300 WmiPrvSE.exe	2160	584	6	201	2019-10-02 17:03:52 UTC+0000
0xfffffa8002b7c300 WmiPrvSE.exe	2232	460	14	314	2019-10-02 16:33:40 UTC+0000
0xfffffa8002d5e300 svchost.exe	888	460	35	1205	2019-10-02 16:31:44 UTC+0000
0xfffffa8002d5e300 svchost.exe	932	460	15	453	2019-10-02 16:31:45 UTC+0000
0xfffffa8002b373610 lsass.exe	472	368	7	600	2019-10-02 15:31:41 UTC+0000
0xfffffa8002b13b30 lsass.exe	3060	308	10	153	2019-10-02 15:33:41 UTC+0000
0xfffffa8002c5e300 svchost.exe	584	460	10	356	2019-10-02 15:33:42 UTC+0000
WARNING : volatility.debug : PID 584 PPID 460 has already been seen	932	460	15	453	2019-10-02 16:31:45 UTC+0000
WARNING : volatility.debug : PID 3204 PPID 460 has already been seen	332	460	14	339	2019-10-02 16:31:45 UTC+0000
WARNING : volatility.debug : PID 332 PPID 460 has already been seen	332	460	15	3205	2019-10-02 16:33:44 UTC+0000
WARNING : volatility.debug : PID 888 PPID 460 has already been seen	388	460	35	1205	2019-10-02 16:31:44 UTC+0000
WARNING : volatility.debug : PID 932 PPID 460 has already been seen	932	460	15	453	2019-10-02 16:33:44 UTC+0000
0xfffffa80018a400 System	4	0	78	536	2019-10-02 15:13:16 UTC+0000
0xfffffa80018a400 System	240	4	20	2019-10-02 15:13:25 UTC+0000	
0xfffffa8001b28e01b explorer.exe	528	1088	29	994	2019-10-02 16:36:20 UTC+0000
0xfffffa8002b76000 wordpad.exe	3704	208	3	162	2019-10-02 17:04:09 UTC+0000
0xfffffa8001e2904:cmd.exe	3312	528	1	20	2019-10-02 17:09:58 UTC+0000
0xfffffa8001e91700:DumpIt.exe	3460	3312	5	80	2019-10-03 10:26:19 UTC+0000
0xfffffa8002d20600 SearchIndexer	2336	528	42	472	2019-10-02 17:03:22 UTC+0000
0xfffffa8002d20600 SearchIndexer	3584	528	5	178	2019-10-02 17:03:21 UTC+0000
0xfffffa8002d20600 wscript.exe	3204	304	4	120	2019-10-02 17:07:41 UTC+0000
0xfffffa8001e09600 chrome.exe	2844	528	25	741	2019-10-02 17:03:45 UTC+0000
0xfffffa8001e09600 chrome.exe	1392	2844	8	175	2019-10-02 17:03:44 UTC+0000
0xfffffa8001e09600 chrome.exe	2060	2844	12	301	2019-10-02 17:03:44 UTC+0000
0xfffffa8001e09600 chrome.exe	2188	2844	12	294	2019-10-02 17:03:45 UTC+0000
0xfffffa8001d4b300 chrome.exe	2256	2844	12	264	2019-10-02 17:03:35 UTC+0000
0xfffffa8001d9e060 chrome.exe	2948	2844	2	55	2019-10-02 17:03:35 UTC+0000
0xfffffa8001d9e060 chrome.exe	2412	2844	7	73	2019-10-02 17:03:35 UTC+0000
0xfffffa8001d9e060 chrome.exe	3160	2844	11	141	2019-10-02 17:03:40 UTC+0000
0xfffffa8002b6fd00 VBoxTray.exe	1372	528	13	141	2019-10-02 16:35:21 UTC+0000
0xfffffa8002b6fd00 winlogon.exe	404	360	3	113	2019-10-02 15:33:41 UTC+0000
0xfffffa8002a03400:cssrss.exe	376	360	9	401	2019-10-02 15:33:40 UTC+0000

Ilustración 28. RAM Árbol procesos

A continuación, utilizaremos psscan, que muestra un listado de procesos como pslist, pero psscan muestra los procesos inactivos e incluso procesos ocultos que pueden ser utilizados por algún tipo de malware.

En este caso no se han encontrado ningún tipo de proceso inactivo u oculto

C:\Users\MesQ\Desktop\TFM_RubenMesquidaGomila\Imagenes>volatility_2.6_win64_standalone.exe -f USUARIO-PC-20191003-102619.dmp --profile=Win7SP1x64 psscan	Volatility Foundation Volatility Framework 2.6	Offset(P)	Name	PID	PPID	PDB	Time created	Time exited
<hr/>								
0x000000007e5a31d0 armsvc.exe		1280	460	0x0000000078fe2000	2019-10-02	16:33:47	UTC+0000	
0x000000007e5da060 conhost.exe		3320	376	0x000000004874a000	2019-10-02	17:09:58	UTC+0000	
0x000000007e7c7860 taskhost.exe		1992	460	0x0000000072194000	2019-10-02	16:35:20	UTC+0000	
0x000000007e813610 svchost.exe		932	460	0x000000006315000	2019-10-02	16:33:45	UTC+0000	
0x000000007e88fb30 audiogd.exe		2056	804	0x0000000050bcc000	2019-10-03	10:20:21	UTC+0000	2019-10-03 10:22:
24 UTC+0000								
0x000000007e894b30 chrome.exe		3164	2844	0x0000000050f60000	2019-10-02	17:03:56	UTC+0000	
0x000000007e898060 audiogd.exe		3800	804	0x000000003c641000	2019-10-03	10:26:06	UTC+0000	
0x000000007e8b9060 spoolsv.exe		1152	460	0x000000007ab6b000	2019-10-02	16:33:46	UTC+0000	
0x000000007e8d46c0 taskhost.exe		2548	460	0x000000003f040000	2019-10-03	10:20:00	UTC+0000	2019-10-03 10:22:
00 UTC+0000								
0x000000007e8dc060 qVPAJWr.exe		3204	304	0x0000000047cdd000	2019-10-02	17:07:41	UTC+0000	
0x000000007e8eb890 svchost.exe		1180	460	0x0000000079d57000	2019-10-02	16:33:47	UTC+0000	
0x000000007e957060 wordpad.exe		3704	528	0x000000004ae34000	2019-10-02	17:04:09	UTC+0000	
0x000000007e9ed060 svchost.exe		584	460	0x0000000010fc0000	2019-10-02	15:33:42	UTC+0000	
0x000000007ea1c2e0 VBoxService.exe		644	460	0x00000000ff640000	2019-10-02	15:33:42	UTC+0000	
0x000000007ea3eb30 svchost.exe		712	460	0x00000000f1bb0000	2019-10-02	16:33:44	UTC+0000	
0x000000007ea7d4f0 svchost.exe		804	460	0x00000000e0ec4000	2019-10-02	16:33:44	UTC+0000	
0x000000007ea9b8e0 sppsvc.exe		2484	460	0x000000006204b000	2019-10-02	16:35:30	UTC+0000	
0x000000007eabb630 svchost.exe		2712	460	0x00000000606a4000	2019-10-02	16:35:48	UTC+0000	
0x000000007eac7060 thunderbird.exe		2336	528	0x000000003707c000	2019-10-02	17:03:21	UTC+0000	
0x000000007eaea340 svchost.exe		864	460	0x000000000dfb5000	2019-10-02	16:33:44	UTC+0000	
0x000000007efafa470 dwm.exe		312	864	0x00000000722e8000	2019-10-02	16:35:20	UTC+0000	
0x000000007eafeb30 svchost.exe		888	460	0x00000000dc7c0000	2019-10-02	16:33:44	UTC+0000	
0x000000007ebe3360 SearchProtocol		2228	1944	0x000000003e62b000	2019-10-03	10:26:06	UTC+0000	
0x000000007eb9c560 svchost.exe		332	460	0x00000000a8c70000	2019-10-02	16:33:45	UTC+0000	
0x000000007eba3460 csrss.exe		376	360	0x000000001751a000	2019-10-02	15:33:40	UTC+0000	
0x000000007eba4060 wininit.exe		368	312	0x0000000001759d000	2019-10-02	15:33:40	UTC+0000	
0x000000007ebb2530 SearchFilterHo		3228	1944	0x000000003e5b0000	2019-10-03	10:26:06	UTC+0000	
0x000000007ec0f6d0 VboxTray.exe		1372	528	0x000000000fc0a000	2019-10-02	16:35:21	UTC+0000	
0x000000007ec18b30 wscript.exe		304	528	0x000000000fc257000	2019-10-02	16:35:21	UTC+0000	
0x000000007ec72060 SearchIndexer.		1944	460	0x0000000066ba0000	2019-10-02	16:35:27	UTC+0000	
0x000000007eca910 winlogon.exe		404	360	0x0000000016820000	2019-10-02	15:33:41	UTC+0000	
0x000000007ecbb30 lsass.exe		472	368	0x00000000151f0000	2019-10-02	15:33:41	UTC+0000	
0x000000007ecfc30 wmpnetwk.exe		2092	460	0x0000000064f40000	2019-10-02	16:35:27	UTC+0000	
0x000000007ed1c30 services.exe		460	368	0x00000000157ba000	2019-10-02	15:33:41	UTC+0000	
0x000000007ed2ab30 lsm.exe		480	368	0x0000000015482000	2019-10-02	15:33:41	UTC+0000	
0x000000007ee6bb30 csrss.exe		320	312	0x0000000025857000	2019-10-02	15:33:37	UTC+0000	
0x000000007eef7060 DumpIt.exe		3460	3312	0x0000000076095000	2019-10-03	10:26:19	UTC+0000	
0x000000007ef34170 svchost.exe		1688	460	0x0000000076462000	2019-10-02	16:33:47	UTC+0000	
0x000000007f687b30 svchost.exe		1328	460	0x0000000078189000	2019-10-02	16:33:47	UTC+0000	
0x000000007f6ef500 smss.exe		248	4	0x000000002be16000	2019-10-02	15:33:36	UTC+0000	
0x000000007f7c9aa0 chrome.exe		2088	2844	0x0000000045fcc000	2019-10-02	17:03:35	UTC+0000	
0x000000007f7ce290 cmd.exe		3312	528	0x000000009d05000	2019-10-02	17:09:58	UTC+0000	
0x000000007f7fdb30 chrome.exe		1392	2844	0x000000002118000	2019-10-02	17:03:44	UTC+0000	
0x000000007f7ddb30 WmiPrvSE.exe		2188	584	0x00000000333ec000	2019-10-02	17:03:55	UTC+0000	
0x000000007f8233de WmiPrvSE.exe		3252	584	0x00000000375df000	2019-10-03	10:26:22	UTC+0000	
0x000000007fabb630 chrome.exe		2412	2844	0x00000000698f000	2019-10-02	17:03:35	UTC+0000	
0x000000007fab2960 chrome.exe		2948	2844	0x000000004b327000	2019-10-02	17:03:35	UTC+0000	
0x000000007fb3e060 chrome.exe		2844	528	0x00000000715ff000	2019-10-02	17:03:35	UTC+0000	
0x000000007fb7d120 chrome.exe		2180	2844	0x0000000049924000	2019-10-02	17:03:35	UTC+0000	
0x000000007fb94b30 chrome.exe		2256	2844	0x000000004b14000	2019-10-02	17:03:35	UTC+0000	
0x000000007fcfea20 explorer.exe		528	1088	0x000000001713d000	2019-10-02	16:35:20	UTC+0000	
0x000000007ff09040 System		4	0	0x0000000000187000	2019-10-02	15:33:36	UTC+0000	

Ilustración 29. RAM Psscan

Para terminar la detección de procesos hemos utilizado psxview utiliza múltiples métodos para detectar procesos y enumera qué procesos son y cuáles no son detectados por cada método de detección. Esta comparación puede ayudar a identificar los procesos que están tratando de evitar la detección.

En este caso no se ha encontrado ningún otro proceso que no haya sido detectado con anterioridad.

```
C:\Users\MesQ\Desktop\TFM_RubenMesquidaGomila\Imagenes>volatility_2.6_win64_standalone.exe -f USUARIO-PC-20191003-102619.dmp --profile=Win7SP1x64 psxview
Volatility Foundation Volatility Framework 2.6

Offset(P)      Name          PID  plist  psscan  thrdproc  pscid  csrss  session  deskthrd  ExitTime
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
0x000000007fb7d120 chrome.exe        2180  True   True   True   True   True   True   True
0x000000007fb233d0 WmiPrvSE.exe    3252  True   True   True   True   True   True   True
0x000000007fc7860 taskhost.exe     1992  True   True   True   True   True   True   True
0x000000007eac7060 thunderbird.exe 2336  True   True   True   True   True   True   True
0x000000007ea9b8e0 sppsvc.exe      2484  True   True   True   True   True   True   True
0x000000007e8e0890 svchost.exe     1180  True   True   True   True   True   True   True
0x000000007fabc960 chrome.exe        2948  True   True   True   True   True   True   True
0x000000007ea9470 dwm.exe         312   True   True   True   True   True   True   True
0x000000007e94b30 chrome.exe        3164  True   True   True   True   True   True   True
0x000000007f087b30 svchost.exe     1328  True   True   True   True   True   True   True
0x000000007fc9aa0 chrome.exe        2088  True   True   True   True   True   True   True
0x000000007ec0f6d0 VBoxTray.exe    1372  True   True   True   True   True   True   True
0x000000007e957060 wordpad.exe     3704  True   True   True   True   True   True   True
0x000000007fcfe20 explorer.exe     528   True   True   True   True   True   True   True
0x000000007ecb3b0 lsass.exe       472   True   True   True   True   True   True   False
0x000000007ed2ab30 qVhPAJWr.exe   3204  True   True   True   True   True   True   True
0x000000007fd6b30 lsm.exe         480   True   True   True   True   True   True   False
0x000000007fca6910 winlogon.exe   1392  True   True   True   True   True   True   True
0x000000007ecfcbb0 wmpnetwk.exe   404   True   True   True   True   True   True   True
0x000000007e944260 SearchIndexer. 2992  True   True   True   True   True   True   True
0x000000007eb3860 SearchProtocol 1944  True   True   True   True   True   True   False
0x000000007eaee340 svchost.exe     2228  True   True   True   True   True   True   False
0x000000007e9ed060 svchost.exe     864   True   True   True   True   True   True   False
0x000000007e9ed060 svchost.exe     584   True   True   True   True   True   True   False
0x000000007eb9060 spoolsv.exe     1152  True   True   True   True   True   True   True
0x000000007e00b7060 DumpIt.exe     3460  True   True   True   True   True   True   True
0x000000007ea7d4f0 svchost.exe     804   True   True   True   True   True   True   True
0x000000007e898860 audiogd.exe    3880  True   True   True   True   True   True   True
0x000000007eb72530 SearchFilterHo 3228  True   True   True   True   True   True   True
0x000000007e5a31d0 armsvc.exe     1280  True   True   True   True   True   True   False
0x000000007esda60 conhost.exe     3320  True   True   True   True   True   True   True
0x000000007eabb630 svchost.exe     2712  True   True   True   True   True   True   False
0x000000007eac2e0 VBoxService.exe  644   True   True   True   True   True   True   False
0x000000007ec18b30 wscript.exe     304   True   True   True   True   True   True   True
0x000000007eba4060 wininit.exe    368   True   True   True   True   True   True   True
0x000000007e13610 svchost.exe     932   True   True   True   True   True   True   True
0x000000007fb3e060 chrome.exe      2844  True   True   True   True   True   True   True
0x000000007ed1cb30 services.exe    460   True   True   True   True   True   True   False
0x000000007ef34170 svchost.exe     1688  True   True   True   True   True   True   True
0x000000007eb9c560 svchost.exe     332   True   True   True   True   True   True   True
0x000000007fdbd30 WmiPrvSE.exe   2188  True   True   True   True   True   True   False
0x000000007ea3eb30 svchost.exe     712   True   True   True   True   True   True   True
0x000000007fb94b30 chrome.exe      2256  True   True   True   True   True   True   True
0x000000007fc2e90 cmd.exe         3312  True   True   True   True   True   True   True
0x000000007fab6b30 chrome.exe      2412  True   True   True   True   True   True   True
0x000000007eafeb30 svchost.exe     888   True   True   True   True   True   True   True
0x000000007fce5f00 smss.exe       248   True   True   True   False  False  False  False
0x000000007ff09040 System         4    True   True   True   False  False  False  False
0x000000007eba3460 csrss.exe      376   True   True   True   False  False  True   True
0x000000007ee6hb30 csrss.exe      320   True   True   True   False  True   True   True
0x000000007e8da6c0 taskhost.exe   2548  False  True   False  False  False  False  False  2019-10-03 10:22:00 UTC+0000
0x000000007e88fb30 audiogd.exe    2056  False  True   False  False  False  False  False  2019-10-03 10:25:24 UTC+0000
```

Ilustración 30. RAM Psxview

Acabada la detección, procederemos a analizar el proceso 3204, primero es importante saber qué DLLs son importadas en proceso. Una DLL contiene código ejecutable que puede proporcionar una funcionalidad específica a un proceso, de modo que si vemos qué DLLs incorpora un proceso puede darnos una idea de sus capacidades.

Las DLL detectadas en el proceso detectado son:

DLL	Características
ntdll	Es la librería que contiene las funciones del núcleo NT
Wow64	WOW64 es el emulador x86 que permite que las aplicaciones basadas en Windows de 32 bits se ejecuten sin problemas en Windows de 64 bits.
Wow64win	Wow64win es uno de las tres DLL utilizadas por Wow64 y proporciona los puntos de entrada apropiados para aplicaciones de 32 bits.
Wow64cpu	Wow64cpu es otra de las tres DLL utilizadas por Wow64 y se encarga de cambiar el procesador de 32 bits a 64 bits.

Tabla 2. DLLs Proceso 3204

```
C:\Users\MesQ\Desktop\TFM_RubenMesquidaGomila\Imagenes>volatility_2.6_win64_standalone.exe -f USUARIO-PC-20191003-102
619.dmp --profile=Win7SP1x64 dlllist -p 3204
Volatility Foundation Volatility Framework 2.6
*****
qVhPAJWr.exe pid: 3204
Command line : "C:\Users\usuario\AppData\Local\Temp\rad8B4D9.tmp\qVhPAJWr.exe"
Note: use ldrmodules for listing DLLs in Wow64 processes

Base           Size      LoadCount Path
-----
0x0000000000400000    0x16000          0xffff C:\Users\usuario\AppData\Local\Temp\rad8B4D9.tmp\qVhPAJWr.exe
0x0000000007724000    0x1a9000         0xffff C:\Windows\SYSTEM32\ntdll.dll
0x00000000074f1000    0x3f000           0x3 C:\Windows\SYSTEM32\wow64.dll
0x00000000074eb0000    0x5c000           0x1 C:\Windows\SYSTEM32\wow64win.dll
0x00000000074ea0000    0x8000            0x1 C:\Windows\SYSTEM32\wow64cpu.dll

C:\Users\MesQ\Desktop\TFM_RubenMesquidaGomila\Imagenes>.
```

Ilustración 31. Lista DLL PID 3204

A continuación, revisaremos los SID asociados al proceso, entre otras cosas, esto puede ayudar a identificar los procesos que tienen privilegios escalados de forma maliciosa. Para ello utilizaremos el comando getsids.

En este caso tenemos los siguientes SIDs asociados al proceso:

```
C:\Users\MesQ\Desktop\TFM_RubenMesquidaGomila\Imagenes>volatility_2.6_win64_standalone.exe -f USUARIO-PC-20191003-102
619.dmp --profile=Win7SP1x64 getsids -p 3204
Volatility Foundation Volatility Framework 2.6
qVhPAJWr.exe (3204): S-1-5-21-3975874985-624589505-3648474185-1000 (usuario)
qVhPAJWr.exe (3204): S-1-5-21-3975874985-624589505-3648474185-513 (Domain Users)
qVhPAJWr.exe (3204): S-1-1-0 (Everyone)
qVhPAJWr.exe (3204): S-1-5-32-544 (Administrators)
qVhPAJWr.exe (3204): S-1-5-32-545 (Users)
qVhPAJWr.exe (3204): S-1-5-4 (Interactive)
qVhPAJWr.exe (3204): S-1-2-1 (Console Logon (Users who are logged onto the physical console))
qVhPAJWr.exe (3204): S-1-5-11 (Authenticated Users)
qVhPAJWr.exe (3204): S-1-5-15 (This Organization)
qVhPAJWr.exe (3204): S-1-5-5-0-135945 (Logon Session)
qVhPAJWr.exe (3204): S-1-2-0 (Local (Users with the ability to log in locally))
qVhPAJWr.exe (3204): S-1-5-64-10 (NTLM Authentication)
qVhPAJWr.exe (3204): S-1-16-8192 (Medium Mandatory Level)
```

Ilustración 32. SIDs Proceso 3204

Con envars listaremos todas las variables de entorno del proceso que se estaban ejecutando en el momento de la adquisición.

```
C:\Users\MesQ\Desktop\TFM_RubenMesquidaGomila\Imagenes>volatility_2.6_win64_standalone.exe -f USUARIO-PC-20191003-102619.dmp --profile=Win7SP1x64 envars -p 3204
Volatility Foundation Volatility Framework 2.6
Pid Process Block Variable Value
3204 qVhPAJWr.exe 0x000000000031120 ALLUSERSPROFILE C:\ProgramData
3204 qVhPAJWr.exe 0x000000000031120 APPDATA C:\Users\usuario\AppData\Roaming
3204 qVhPAJWr.exe 0x000000000031120 CommonProgramFiles C:\Program Files\Common Files
3204 qVhPAJWr.exe 0x000000000031120 CommonProgramFiles(x86) C:\Program Files(x86)\Common Files
3204 qVhPAJWr.exe 0x000000000031120 COMPUTERNAME USUARIO-PC
3204 qVhPAJWr.exe 0x000000000031120 COMPUTERNAME=x86 USUARIO-PC
3204 qVhPAJWr.exe 0x000000000031120 CmdSpec NO
3204 qVhPAJWr.exe 0x000000000031120 CURRENTDIRECTORY C:
3204 qVhPAJWr.exe 0x000000000031120 HOMEPATH \Users\usuario
3204 qVhPAJWr.exe 0x000000000031120 HOMEPATH=C:\Users\usuario\AppData\Local\Temp\USUARIO-PC
3204 qVhPAJWr.exe 0x000000000031120 LOGONSERVER 1
3204 qVhPAJWr.exe 0x000000000031120 NUMBER_OF_PROCESSORS 1
3204 qVhPAJWr.exe 0x000000000031120 OS C:\Windows\NT
3204 qVhPAJWr.exe 0x000000000031120 Path C:\Windows\system32;C:\Windows;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\;CMD;BAT;CHD;VBS;.JS;.VBE;.WSF;.WSH;.MSC
3204 qVhPAJWr.exe 0x000000000031120 PROCESSOR_ARCHITECTURE AMD64
3204 qVhPAJWr.exe 0x000000000031120 PROCESSOR_IDENTIFIER Intel64 Family 6 Model 158 Stepping 10, GenuineIntel
3204 qVhPAJWr.exe 0x000000000031120 PROCESSOR_REVISION 9e0a
3204 qVhPAJWr.exe 0x000000000031120 ProgramData C:\ProgramData
3204 qVhPAJWr.exe 0x000000000031120 PUBLIC C:\Users\public
3204 qVhPAJWr.exe 0x000000000031120 SESSIONNAME Console
3204 qVhPAJWr.exe 0x000000000031120 SystemRoot C:\Windows
3204 qVhPAJWr.exe 0x000000000031120 TEMP C:\Users\usuario\AppData\Local\Temp\USUARIO-PC\Temp\USUARIO-PC\LocalTemp
3204 qVhPAJWr.exe 0x000000000031120 USERDOMAIN usuario
3204 qVhPAJWr.exe 0x000000000031120 USERNAME usuario
3204 qVhPAJWr.exe 0x000000000031120 USERPROFILE C:\Users\usuario
3204 qVhPAJWr.exe 0x000000000031120 windir C:\Windows
3204 qVhPAJWr.exe 0x000000000031120 windows_Tracing_Flags 1
3204 qVhPAJWr.exe 0x000000000031120 windows_Tracing_LogFile C:\BVBF\tests\installpackage\csilogfile.log

C:\Users\MesQ\Desktop\TFM_RubenMesquidaGomila\Imagenes>
```

Ilustración 33. RAM Variables entorno

8.1.3. SERVICIOS

Analizados los procesos procederemos a revisar los servicios en ejecución, volatility es el único framework de análisis de memoria con la capacidad de listar los servicios. Para listarlos ejecutaremos el plugin svcscan, es importante revisar los servicios por si algún tipo de malware se encuentra listado o relacionado con algún servicio de Windows.

En este caso no se ha detectado ningún servicio extraño

```
C:\Users\MesQ\Desktop\TFM_RubenMesquidaGomila\Imagenes>volatility_2.6_win64_standalone.exe -f  
619.dmp --profile=Win7SP1x64 svcscan  
Volatility Foundation Volatility Framework 2.6  
Offset: 0xc7eb30  
Order: 227  
Start: SERVICE_AUTO_START  
Process ID: 584  
Service Name: Power  
Display Name: Energía  
Service Type: SERVICE_WIN32_SHARE_PROCESS  
Service State: SERVICE_RUNNING  
Binary Path: C:\Windows\system32\svchost.exe -k DcomLaunch  
  
Offset: 0xc7ea40  
Order: 226  
Start: SERVICE_DEMAND_START  
Process ID: 1688  
Service Name: PolicyAgent  
Display Name: Agente de directiva IPsec  
Service Type: SERVICE_WIN32_SHARE_PROCESS  
Service State: SERVICE_RUNNING  
Binary Path: C:\Windows\system32\svchost.exe -k NetworkServiceNetworkRestricted  
  
Offset: 0xc7e950  
Order: 225  
Start: SERVICE_DEMAND_START  
Process ID: -  
Service Name: PNRPsvc  
Display Name: Protocolo de resolución de nombres de mismo nivel  
Service Type: SERVICE_WIN32_SHARE_PROCESS  
Service State: SERVICE_STOPPED  
Binary Path: -  
  
Offset: 0xc7e860  
Order: 224  
Start: SERVICE_DEMAND_START  
Process ID: -  
Service Name: PNRPAutoReg  
Display Name: Servicio de publicación de nombres de equipo PNRP  
Service Type: SERVICE_WIN32_SHARE_PROCESS  
Service State: SERVICE_STOPPED  
Binary Path: -  
  
Offset: 0xc7e680  
Order: 222  
Start: SERVICE_AUTO_START  
Process ID: 584  
Service Name: PlugPlay  
Display Name: Plug and Play  
Service Type: SERVICE_WIN32_SHARE_PROCESS  
Service State: SERVICE_RUNNING  
Binary Path: C:\Windows\system32\svchost.exe -k DcomLaunch  
  
Offset: 0xc80090  
Order: 221  
Start: SERVICE_DEMAND_START  
Process ID: -  
Service Name: pla  
Display Name: Registros y alertas de rendimiento  
Service Type: SERVICE_WIN32_SHARE_PROCESS  
Service State: SERVICE_STOPPED  
Binary Path: -
```

Ilustración 34. RAM Servicios

8.1.5. CONEXIONES

En este paso realizaremos una parte fundamental cuando se realiza un análisis que es la identificación de conexiones del equipo, aquí se buscaran conexiones extrañas que pueda haber. Para esto se utilizará el plugin netscan que buscara en la imagen la actividad de la red, este plugin es capaz de encontrar sesiones activas tanto como inactivas en el momento de la adquisición.

En este caso vemos que el proceso 3204 sospechoso que se había encontrado hay varias sesiones cerradas y una de establecida, esta va hacia la IP 192.168.1.165 hacia el puerto 4444, este puerto es utilizado por varios malware por lo que habrá que seguir mirando en los siguientes pasos.

Offset(P)	Proto	Local Address	Foreign Address	State	Pid	Owner	Created
0x7e61e6e0	UDPV6	fe80::7d4a:52fc:47aa:8b27:53680 *:	*.*	CLOSED	1328	svchost.exe	2019-10-03 10:20:03 UTC+0000
0x7e62c290	UDPV6	192.168.1.168:138	*.*	ESTABLISHED	4	System	2019-10-03 10:20:05 UTC+0000
0x7e833950	UDPV4	0.0.0.0:5355	*.*	CLOSED	932	svchost.exe	2019-10-03 10:25:04 UTC+0000
0x7e838bf0	UDPV4	0.0.0.0:5353	*.*	LISTENING	2844	chrome.exe	2019-10-03 10:20:11 UTC+0000
0x7e839c70	UDPV4	0.0.0.0:5353	*.*	LISTENING	2844	chrome.exe	2019-10-03 10:20:11 UTC+0000
0x7e839c70	UDPV6	:::5353	*.*	LISTENING	2844	chrome.exe	2019-10-03 10:20:11 UTC+0000
0x7e881480	UDPV4	0.0.0.0:0	*.*	CLOSED	932	svchost.exe	2019-10-03 10:20:05 UTC+0000
0x7e881480	UDPV6	:::0	*.*	CLOSED	932	svchost.exe	2019-10-03 10:20:05 UTC+0000
0x7e8a6910	UDPV4	0.0.0.0:3702	*.*	LISTENING	1328	svchost.exe	2019-10-03 10:20:08 UTC+0000
0x7e8a6910	UDPV6	:::3702	*.*	LISTENING	1328	svchost.exe	2019-10-03 10:20:08 UTC+0000
0x7e8acbf0	UDPV4	0.0.0.0:0	*.*	CLOSED	644	VBoxService.exe	2019-10-03 10:20:41 UTC+0000
0x7e8b1190	UDPV6	:::53681	*.*	LISTENING	1328	svchost.exe	2019-10-03 10:20:03 UTC+0000
0x7e8d3800	UDPV6	0.0.0.0:3702	*.*	LISTENING	1328	svchost.exe	2019-10-03 10:20:08 UTC+0000
0x7e8d3800	UDPV6	:::3702	*.*	LISTENING	1328	svchost.exe	2019-10-03 10:20:08 UTC+0000
0x7ea27640	UDPV4	0.0.0.0:0	*.*	CLOSED	49038752		2019-10-02 16:35:28 UTC+0000
0x7eb82810	UDPV4	0.0.0.0:0	*.*	CLOSED	644	VBoxService.exe	2019-10-03 10:26:41 UTC+0000
0x7ebb94f0	UDPV6	:::11900	*.*	LISTENING	1328	svchost.exe	2019-10-03 10:20:03 UTC+0000
0x7ec4c920	UDPV4	0.0.0.0:5355	*.*	LISTENING	932	svchost.exe	2019-10-03 10:25:04 UTC+0000
0x7ec4c920	UDPV6	:::5355	*.*	LISTENING	932	svchost.exe	2019-10-03 10:25:04 UTC+0000
0x7ec56ec0	UDPV4	127.0.0.1:53683	*.*	LISTENING	1328	svchost.exe	2019-10-03 10:20:03 UTC+0000
0x7eca4bf0	UDPV4	127.0.0.1:1900	*.*	LISTENING	1328	svchost.exe	2019-10-03 10:20:03 UTC+0000
0x7ee101e0	UDPV4	0.0.0.0:3702	*.*	LISTENING	1328	svchost.exe	2019-10-03 10:20:08 UTC+0000
0x7ee0d70	UDPV4	0.0.0.0:500	*.*	LISTENING	888	svchost.exe	2019-10-02 16:33:47 UTC+0000
0x7eec2010	UDPV4	0.0.0.0:4500	*.*	LISTENING	888	svchost.exe	2019-10-02 16:33:47 UTC+0000
0x7eec2bb0	UDPV4	0.0.0.0:500	*.*	LISTENING	888	svchost.exe	2019-10-02 16:33:47 UTC+0000
0x7eec2bb0	UDPV6	:::500	*.*	LISTENING	888	svchost.exe	2019-10-02 16:33:47 UTC+0000
0x7eec4730	UDPV4	0.0.0.0:0	*.*	LISTENING	888	svchost.exe	2019-10-02 16:33:47 UTC+0000
0x7eec72c0	UDPV4	0.0.0.0:0	*.*	LISTENING	888	svchost.exe	2019-10-02 16:33:47 UTC+0000
0x7eec72c0	UDPV6	:::0	*.*	LISTENING	888	svchost.exe	2019-10-02 16:33:47 UTC+0000
0x7eeaeac0	UDPV4	192.168.1.168:137	*.*	CLOSED	4	System	2019-10-03 10:20:05 UTC+0000
0x7e90b250	TCPV4	0.0.0.0:49154	0.0.0.0:0	LISTENING	888	svchost.exe	
0x7e90e390	TCPV4	0.0.0.0:49154	0.0.0.0:0	LISTENING	888	svchost.exe	
0x7e90e390	TCPV6	:::49154	:::0	LISTENING	888	svchost.exe	
0x7e9ac200	TCPV4	0.0.0.0:49156	0.0.0.0:0	LISTENING	1688	svchost.exe	
0x7eab6d80	TCPV4	0.0.0.0:135	0.0.0.0:0	LISTENING	712	svchost.exe	
0x7eabbae0	TCPV4	0.0.0.0:135	0.0.0.0:0	LISTENING	712	svchost.exe	
0x7eabbae0	TCPV6	:::135	:::0	LISTENING	712	svchost.exe	
0x7eabbd90	TCPV4	0.0.0.0:49152	0.0.0.0:0	LISTENING	368	wininit.exe	
0x7eac2ba0	TCPV4	0.0.0.0:49152	0.0.0.0:0	LISTENING	368	wininit.exe	
0x7eac2ba0	TCPV6	:::49152	:::0	LISTENING	368	wininit.exe	
0x7eb4a8e0	TCPV4	0.0.0.0:49153	0.0.0.0:0	LISTENING	894	svchost.exe	
0x7eb4e3e0	TCPV4	0.0.0.0:49153	0.0.0.0:0	LISTENING	894	svchost.exe	
0x7eb4e3e0	TCPV6	:::49153	:::0	LISTENING	894	svchost.exe	
0x7ec0f4a0	TCPV4	0.0.0.0:49158	0.0.0.0:0	LISTENING	472	lsass.exe	
0x7ecb53f0	TCPV4	0.0.0.0:49158	0.0.0.0:0	LISTENING	472	lsass.exe	
0x7ecb53f0	TCPV6	:::49158	:::0	LISTENING	472	lsass.exe	
0x7e825cf0	TCPV4	192.168.1.168:49227	192.168.1.165:4444	CLOSED	3204	qvhPAW.exe	
0x7eab2018	TCPV4	127.0.0.1:49180	127.0.0.1:49179	ESTABLISHED	2336	thunderbird.exe	
0x7eabc30	TCPv6	-:0	38eb:c902:80fa:ffff:38eb:c902:80fa:ffff:0	CLOSED	1	P??@?????	
0x7eb49770	TCPV6	-:0	f8d4:cd02:80fa:ffff:098:d02:80fa:ffff:0	CLOSED	1	P??@?????	
0x7ebb2990	TCPV4	192.168.1.168:49228	74.125.133.188:443	ESTABLISHED	2180	chrome.exe	
0x7ebbfb00	TCPV4	-:49219	192.168.1.1:443	CLOSED	2336	thunderbird.exe	
0x7ecb5cf0	TCPV6	-:0	383b:b102:80fa:ffff:383b:b102:80fa:ffff:0	CLOSED	932	svchost.exe	
0x7ef5a490	UDPV4	0.0.0.0:3702	*.*	CLOSED	1328	svchost.exe	2019-10-03 10:20:08 UTC+0000
0x7ef5b650	UDPV4	0.0.0.0:62255	*.*	CLOSED	1328	svchost.exe	2019-10-02 16:33:47 UTC+0000
0x7ef5d8e0	UDPV4	0.0.0.0:62256	*.*	CLOSED	1328	svchost.exe	2019-10-02 16:33:47 UTC+0000
0x7ef5d8e0	UDPV6	:::62256	*.*	CLOSED	1328	svchost.exe	2019-10-02 16:33:47 UTC+0000
0x7ef98010	UDPV6	fe80::7d4a:52fc:47aa:8b27:1900	*.*	CLOSED	1328	svchost.exe	2019-10-03 10:20:03 UTC+0000
0x7efdd7c0	UDPV4	0.0.0.0:0	*.*	CLOSED	1688	svchost.exe	2019-10-02 16:33:48 UTC+0000

Ilustración 35. RAM Conexiones red 1

0x7ea62010	TCPv4	127.0.0.1:49180	127.0.0.1:49179	ESTABLISHED	2336	thunderbird.exe	
0x7eabcc30	TCPv6	-::0	38eb:c902:80fa:ffff:38eb:c902:80fa:ffff:0	CLOSED	1	P??B???	
0x7ebd49770	TCPv6	-::0	f8d4:c002:80fa:ffff:e098:002:80fa:ffff:0	CLOSED	1	P??B???	
0x7ebb2998	TCPv4	192.168.1.168:49228	74.125.133.188:443	ESTABLISHED	2180	chrome.exe	
0x7ebfb500	TCPv4	-:49219	192.168.1.1:443	CLOSED	2336	thunderbird.exe	
0x7ecb5cf0	TCPv6	-::0	383b:b102:80fa:ffff:383b:b102:80fa:ffff:0	CLOSED	932	svchost.exe	
0x7ef5a490	UDPv4	0.0.0.0:3702	*.*	1328	svchost.exe	2019-10-03 10:20:08 UTC+0000	
0x7ef5b650	UDPv4	0.0.0.0:62255	*.*	1328	svchost.exe	2019-10-02 16:33:47 UTC+0000	
0x7ef5d8e0	UDPv4	0.0.0.0:62256	*.*	1328	svchost.exe	2019-10-02 16:33:47 UTC+0000	
0x7ef5d8e0	UDPv6	:::62256	*.*	1328	svchost.exe	2019-10-02 16:33:47 UTC+0000	
0x7ef98010	UDPv6	fe80::7d4a:52fc:47aa:8b27:1900	*.*	1328	svchost.exe	2019-10-03 10:20:03 UTC+0000	
0x7effd7c0	UDPv4	0.0.0.0:0	*.*	1688	svchost.exe	2019-10-02 16:33:48 UTC+0000	
0x7effd7c0	UDPv6	:::0	*.*	1688	svchost.exe	2019-10-02 16:33:48 UTC+0000	
0x7effe63f0	UDPv4	192.168.1.168:53682	*.*	1328	svchost.exe	2019-10-02 10:20:03 UTC+0000	
0x7efff8288	UDPv4	0.0.0.0:0	*.*	1688	svchost.exe	2019-10-02 16:33:48 UTC+0000	
0x7f7a9b70	UDPv4	0.0.0.0:4500	*.*	888	svchost.exe	2019-10-02 16:33:47 UTC+0000	
0x7f7a9b70	UDPv6	:::4500	*.*	888	svchost.exe	2019-10-02 16:33:47 UTC+0000	
0x7ff8e690	UDPv4	192.168.1.168:1900	*.*	1328	svchost.exe	2019-10-03 10:20:03 UTC+0000	
0x7eff43978	TCPv4	0.0.0.0:5357	0.0.0.0:0	LISTENING	4	System	
0x7eff43978	TCPv6	:::5357	:::0	LISTENING	4	System	
0x7eff773e0	TCPv4	0.0.0.0:445	0.0.0.0:0	LISTENING	4	System	
0x7eff773e0	TCPv6	:::445	:::0	LISTENING	4	System	
0x7eff78010	TCPv4	0.0.0.0:49155	0.0.0.0:0	LISTENING	460	services.exe	
0x7eff82010	TCPv4	0.0.0.0:49155	0.0.0.0:0	LISTENING	460	services.exe	
0x7eff82010	TCPv6	:::49155	:::0	LISTENING	460	services.exe	
0x7eff9fef0	TCPv4	0.0.0.0:49156	0.0.0.0:0	LISTENING	1688	svchost.exe	
0x7eff9fef0	TCPv6	:::49156	:::0	LISTENING	1688	svchost.exe	
0x7ff85450	TCPv4	192.168.1.168:139	0.0.0.0:0	LISTENING	4	System	
0x7effca1f0	TCPv4	127.0.0.1:49179	127.0.0.1:49180	ESTABLISHED	2336	thunderbird.exe	
0x7ff869010	TCPv4	-:49218	192.228.79.201:443	CLOSED	2336	thunderbird.exe	
0x7fed3010	UDPv4	0.0.0.0:0	*.*	644	VBoxService.exe	2019-10-03 10:20:36 UTC+0000	
0x7ff840810	TCPv4	192.168.1.168:49216	192.168.1.165:4444	ESTABLISHED	3204	qVhPAJW.exe	
0x7fb92c10	TCPv4	-:49225	19.249.11.19:443	CLOSED	2336	thunderbird.exe	
0x7ffbad480	TCPv4	192.168.1.168:49227	192.168.1.165:4444	CLOSED	3204	qVhPAJW.exe	

Ilustración 36. RAM Conexiones red 2

8.2 ANÁLISIS DE IMAGEN DISCO DURO

Después de haber analizado la memoria, analizaremos la imagen tomada del disco duro, esta es una de las partes principales de un análisis forense. El objetivo de esta parte es conocer el sistema y buscar todas las evidencias posibles mediante diferentes herramientas.

8.2.1. VALIDACIÓN

Como se ha hecho en la imagen de la memoria RAM antes de empezar a analizar la imagen del disco duro se deben verificar las sumas de verificación y compararlas con las obtenidas en la fase de adquisición.

En este caso para hacerlo lo haremos mediante fciv y podremos ver como coinciden con las del principio.

```
C:\Users\MesQ\Desktop\TFM_RubenMesquidaGomila\Imagenes>fciv -md5 -sha1 d:\clonacionwin7.dd
// File Checksum Integrity Verifier version 2.05.
// 
      MD5           SHA-1
-----
93bbf050c944575865bde97ed815b09a 9b6f2e9e39b125a77d2ec672bbda4cc14411e839 d:\clonacionwin7.dd
C:\Users\MesQ\Desktop\TFM_RubenMesquidaGomila\Imagenes>
```

Ilustración 37. Validación imagen disco duro

8.2.2. CREACION CASO AUTOPSY

Después de validar la imagen procederemos a crear el caso en Autopsy, al abrir el programa crearemos el nuevo caso, donde introduciremos los datos y seleccionaremos la imagen o imágenes a analizar.



Ilustración 38. Creación Caso Autopsy 1

Primero se introducirá el nombre que queramos de caso, en este se ha puesto el número del caso.

A screenshot of the 'New Case Information' dialog box. The left sidebar shows 'Steps' with '1. Case Information' and '2. Optional Information' selected. The main area is titled 'Case Information'. It contains fields for 'Case Name' (IB07683811), 'Base Directory' (C:\Users\MesQ\Desktop\), a 'Browse' button, and 'Case Type' (radio buttons for 'Single-user' (selected) and 'Multi-user'). Below these, a note says 'Case data will be stored in the following directory:' followed by a text input field containing C:\Users\MesQ\Desktop\IB07683811. At the bottom are buttons for '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

Ilustración 39. Creación Caso Autopsy 2

Luego se introducirá el número del caso con los datos del perito o analista que realizará el análisis

New Case Information

Steps

1. Case Information
2. Optional Information

Optional Information

Case

Number: IB07683811

Examiner

Name: Ruben Mesquida Gomila

Phone:

Email: ruben.mesquida@perito.com

Notes:

Organization

Organization analysis is being done for: [redacted]

Manage Organizations

< Back Next > Finish Cancel Help

Ilustración 40. Creación caso Autopsy 2

Luego se deberá seleccionar el tipo de datos, en este caso una imagen de disco

Add Data Source

Steps

1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source

Select Type of Data Source To Add

Disk Image or VM File

Local Disk

Logical Files

Unallocated Space Image File

Autopsy Logical Imager Results

< Back Next > Finish Cancel Help

Ilustración 41. Creación caso Autopsy 3

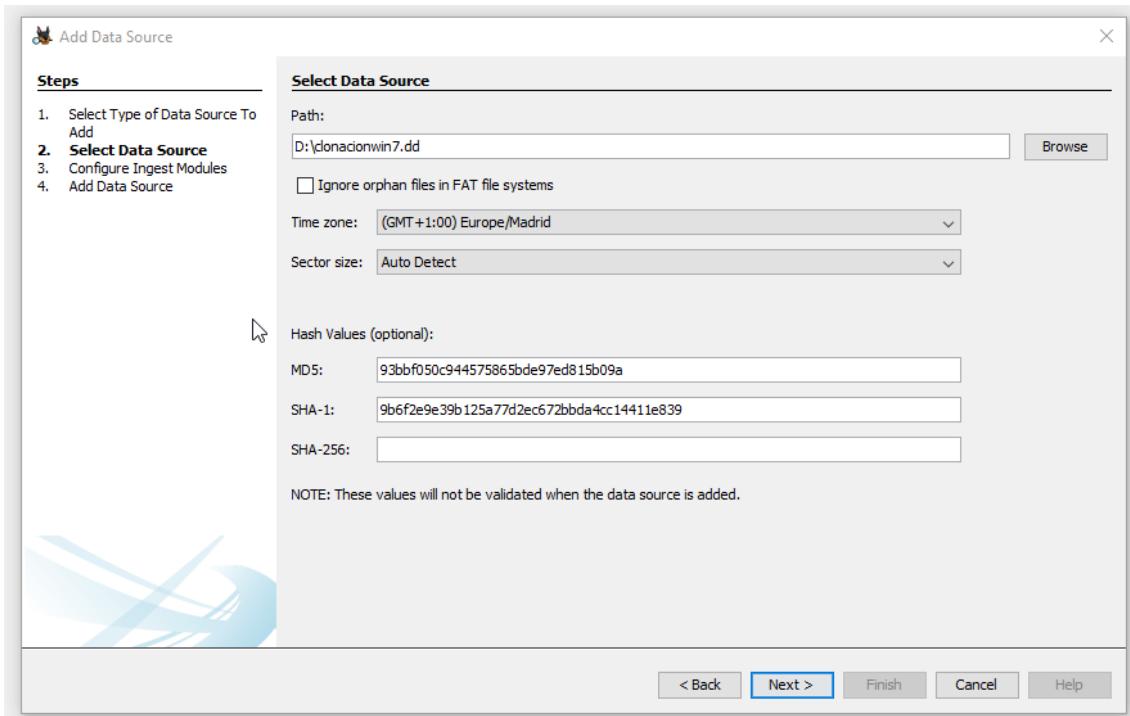


Ilustración 42. Creación caso Autopsy 4

Por último, se seleccionarán los módulos que se ejecutaron. Autopsy está formado por módulos analizan la información de la fuente de datos seleccionada, estos realizan todo el análisis de los archivos y analizan su contenido como pueden ser búsqueda de palabras clave, shellbags, historial de navegación, actividad reciente, etc.

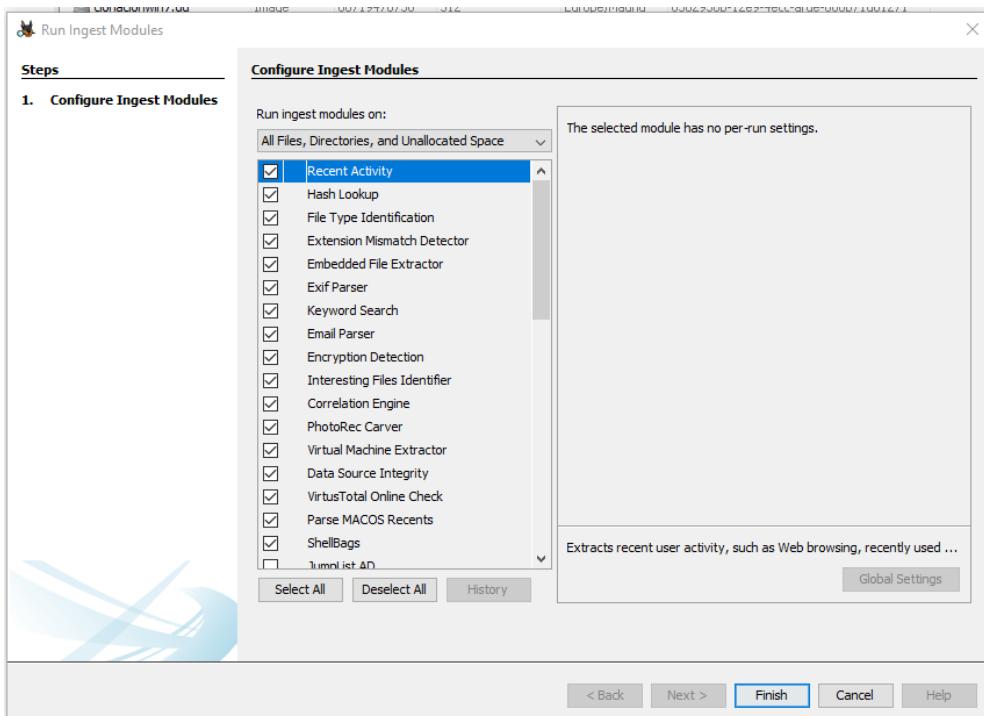


Ilustración 43. Creación caso Autopsy 4

8.2.3. ANALISIS DE MALWARE

Antes de empezar con el análisis con Autopsy, realizaremos un análisis de malware. Este análisis es importante realizarlo para obtener información adicional sobre el sistema, debido a que esto podría revelar información sobre archivos adicionales que en un análisis manual se nos podrían escapar y que podrían ser malware. Aunque hay que recordar que un análisis de malware con cualquier antivirus o herramienta, puede no siempre encontrar todos los archivos maliciosos o incluso a veces puede devolver falsos positivos.

Para proceder al análisis de malware primero deberemos montar la imagen para ello utilizaremos OSFMount que como hemos dicho es una herramienta que permite montar imágenes, como discos físicos o lógicos para su posterior análisis.

Con OSFMount seleccionaremos “Mount New” y seleccionaremos la imagen del disco que obtuvimos.

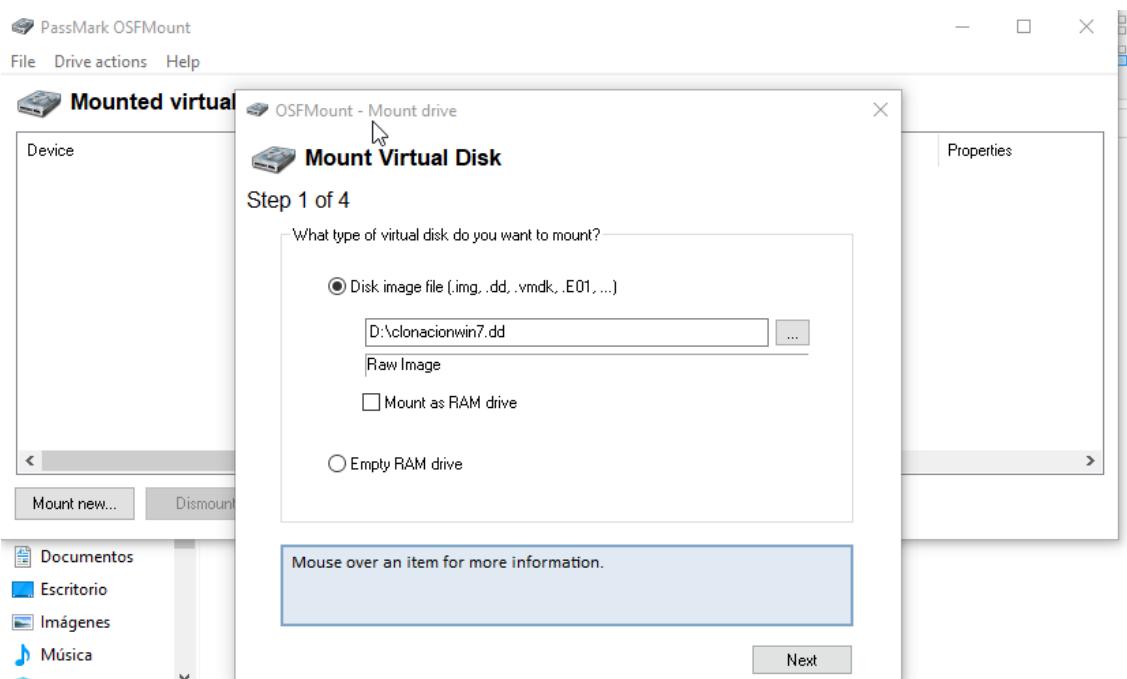


Ilustración 44. OSFMount 1

Se seleccionará el disco entero o solo una partición, en este caso hemos seleccionado la partición donde está instalado el sistema

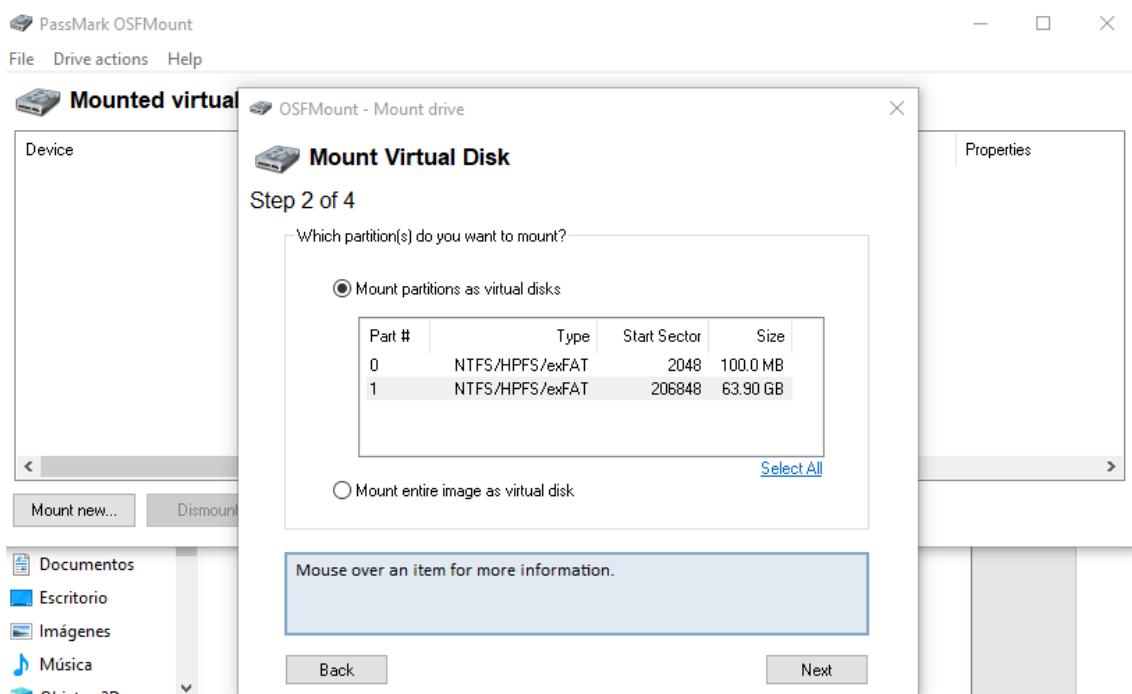


Ilustración 45. OSFMount 2

Seleccionada la partición, para no realizar cambios indebidos y romper la integridad y cadena de custodia, en la imagen nos deberemos asegurar que la opción de solo lectura este activada de esta forma evitaremos posibles cambios

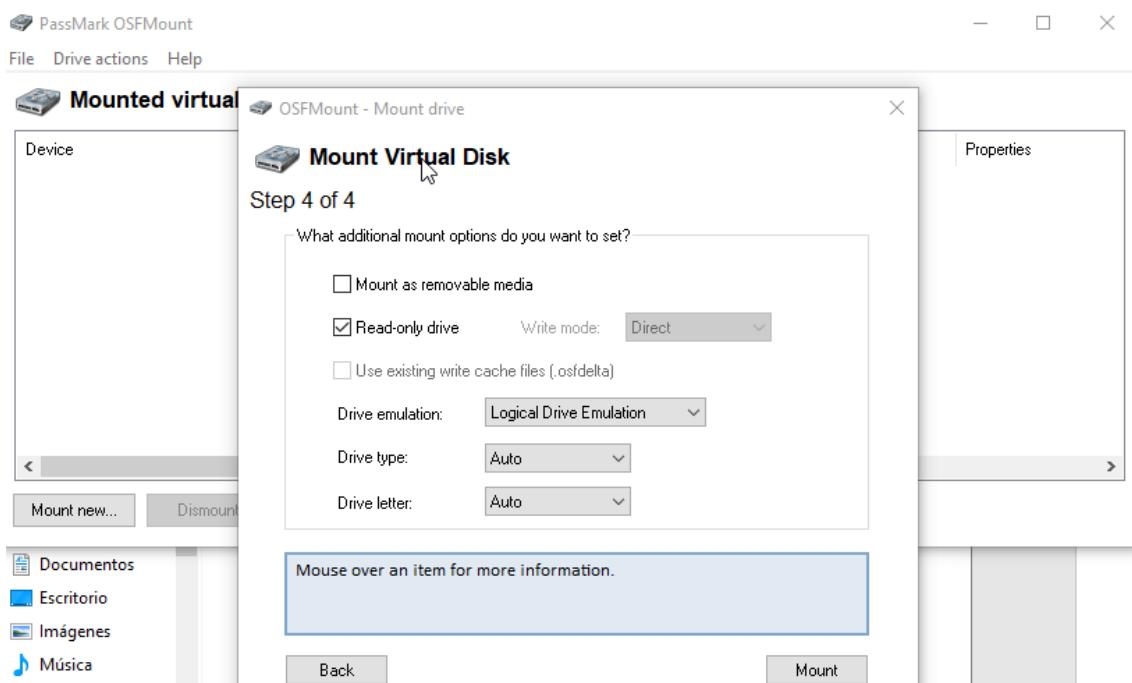


Ilustración 46. OSFMount 3

Hecho esto la imagen estará montada en nuestro equipo, luego desde una virtual hemos mapeado la imagen montada, en primer lugar, con el antivirus ClamAV que realizará un primer escaneo en busca de malware.

```
[root@parrot]~[/media]
└─# clamscan -r -i -l malware.log /media/sf_F_DRIVE/
/media/sf_F_DRIVE/ed01ebfb9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe: Win.R
nsomware.WannaCry-6313787-0 FOUND
WARNING: Can't open file /media/sf_F_DRIVE/pagefile.sys: Operation not permitted
```

Ilustración 47. Análisis ClamAV

Como resultado del análisis se ha encontrado un archivo infectado, detectado como un ransomware de la variante WannaCry. En la siguiente ilustración podemos ver la salida que se encuentra como anexo de este trabajo

```
-----  

/media/sf_F_DRIVE/ed01ebfb9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe: Win.Ransomware.WannaCry-6313787-0 FOUND  

----- SCAN SUMMARY -----  

Known viruses: 6361556  

Engine version: 0.101.4  

Scanned directories: 16252  

Scanned files: 80216  

Infected files: 1  

Total errors: 186  

Data scanned: 8090.37 MB  

Data read: 15970.25 MB (ratio 0.51:1)  

Time: 5819.145 sec (96 m 59 s)
```

Ilustración 48. Anexo 3 a Resultado ClamAV

Acabado el escaneo de ClamAV, realizaremos un análisis con Yara en búsqueda de otros posibles archivos infectados que no hayan sido detectados con ClamAV.

```
[root@parrot]~[/home/user/Desktop/YARA]
└─# yara -w -r malware_index.yar Exploit-Kits_index.yar Webshells_index.yar /media/sf_F_DRIVE/ > scanyara.txt
error scanning /media/sf_F_DRIVE//pagefile.sys: could not open file
```

Ilustración 49. Análisis Yara

Column1.1	Column1.2
2 Str_Win32_Winsock2_Library /media/sf_F_DRIVE	ed01ebfb9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
3 WannaDecryptor /media/sf_F_DRIVE	ed01ebfb9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
4 Wanna_Sample_84c2835a5d21bbcf75a61706d8ab549 /media/sf_F_DRIVE	ed01ebfb9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
5 ransom_telefonica /media/sf_F_DRIVE	ed01ebfb9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
6 Wanna_Cry_Ransomware_Generic /media/sf_F_DRIVE	ed01ebfb9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
7 WannaCry_Ransomware /media/sf_F_DRIVE	ed01ebfb9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
8 WannaCry_Ransomware_Dropper /media/sf_F_DRIVE	ed01ebfb9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
9 wannacry_static_ransom /media/sf_F_DRIVE	ed01ebfb9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
10 Str_Win32_Internet_API /media/sf_F_DRIVE	Program Files/Common Files/system/msadc/msadc.dll
11 Str_Win32_Http_API /media/sf_F_DRIVE	Program Files/Common Files/system/msadc/msadc.dll
12 Str_Win32_Wininet_Library /media/sf_F_DRIVE	Program Files/Common Files/system/wab32.dll
13 Str_Win32_Wininet_Library /media/sf_F_DRIVE	Program Files/Common Files/system/Ole DB/oledb32.dll
14 GlassesCode /media/sf_F_DRIVE	Program Files/DVD Maker/PipeTran.dll
15 Glasses /media/sf_F_DRIVE	Program Files/DVD Maker/PipeTran.dll
16 Str_Win32_Wininet_Library /media/sf_F_DRIVE	Program Files/Internet Explorer/hmmapi.dll
17 Str_Win32_Wininet_Library /media/sf_F_DRIVE	Program Files/Internet Explorer/ielowutil.exe
18 Str_Win32_Wininet_Library /media/sf_F_DRIVE	Program Files/Internet Explorer/jdebuggeride.dll
19 Str_Win32_Internet_API /media/sf_F_DRIVE	Program Files/Internet Explorer/jdebuggeride.dll
20 Str_Win32_Http_API /media/sf_F_DRIVE	Program Files/Internet Explorer/smapi.dll
21 Str_Win32_Wininet_Library /media/sf_F_DRIVE	Program Files/Internet Explorer/iedvtool.dll
22 Str_Win32_Http_API /media/sf_F_DRIVE	Program Files/Internet Explorer/iedvtool.dll

Ilustración 50. Anexo 3b Resultado Yara

Con los resultados anteriores y las evidencias encontradas en el análisis de memoria, se ha realizado la siguiente tabla de posibles evidencias.

Se ha detectado un archivo infectado con un RansomWare de la variante WannaCry y las posibles evidencias encontradas en el análisis de memoria, los resultados han sido inexactos por lo que se analizaran en la siguiente fase de análisis de archivos con Autopsy.

Archivo	Detección
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe	RansomWare Wannacry
qVhPAJWr.exe	Yara Str_Win32_Winsock2_Library Resultado: Inexacto, al analizarlo con Autopsy se extraerá para analizarlo correctamente

Tabla 3. Resultados Malware

8.2.4. DATOS BÁSICOS DEL EQUIPO

Con los análisis de malware realizados obtendremos los datos básicos del equipo a analizar. Con estos datos obtenemos una mayor información sobre el sistema a analizar, en etapas posteriores analizaremos las aplicaciones instaladas.

	Datos
Nombre equipo	Usuario-pc
Versión SO	Windows 7 Ultimate Service Pack 1 64 bits
Propietario	usuario
Organización	Sitsa

Tabla 4. Datos Equipo

Para obtener esta información, en los resultados después de haberse ejecutado los módulos en Operating System Information podremos obtener la información anterior

The screenshot shows the Autopsy 4.12.0 interface with the title bar "IB0763811 - Autopsy 4.12.0". The menu bar includes Case, View, Tools, Window, Help. The toolbar has buttons for Add Data Source, Images/Videos, Communications, Timeline, Close Case, and Generate Report. The main pane displays a hierarchical tree view of data sources, file types, deleted files, MB file size, and results. Under Results, Extracted Content is expanded, showing various file types like PDF, JPEG, and XML. A red box highlights the "Operating System Information (3)" node. Below it, Recent Documents (26) and SAM File (12) are listed. The bottom section shows a table titled "Operating System Information" with two rows: SYSTEM (Windows_NT, AMD64, %SystemRoot%\TEMP\donacionwin7.dd) and SYSTEM (Windows_NT, AMD64, %SystemRoot%\TEMP\donacionwin7.dd). A red box highlights the "SOFTWARE" row. At the bottom, there are tabs for Hex, Text, Application, Message, File Metadata, Results (which is selected), Annotations, and Other Occurrences.

Ilustración 51. Información Sistema

8.2.5. ANÁLISIS USUARIOS

Desde el archivo SAM del equipo podemos encontrar 3 usuarios:

- Usuario que es el propietario del equipo
- Y las cuentas Administrador e Invitado que son cuentas que vienen integradas en el sistema

The screenshot shows the Autopsy 4.12.0 interface with the title bar "IB0763811 - Autopsy 4.12.0". The menu bar includes Case, View, Tools, Window, Help. The toolbar has buttons for Add Data Source, Images/Videos, Communications, Timeline, Close Case, and Generate Report. The main pane displays a hierarchical tree view of data sources, file types, deleted files, MB file size, and results. Under Results, Extracted Content is expanded, showing various file types like PDF, JPEG, and XML. A red box highlights the "SAM File" node. Below it, Recent Documents (26) and SAM File (12) are listed. The bottom section shows a table titled "SAM File" with 12 results. The table includes columns: S, C, Username, Full_Name, Comment, Name, Internet_UserName, Password_Hint, Account_Type, Create_dt, Last_Logon_Date, Pwd_Reset_Dt. The table lists 12 entries, each corresponding to a user account. A red box highlights the last three entries, which are all "Administrator" accounts.

La cuenta de usuario tenemos que el ultimo inicio de sesión se trata de día 2019-09-24 12:13:44 cuando el usuario dejo el equipo el día 23

Account_Type	Default Admin User	SAMParse
Create_dtm	2019-09-24 10:12:01.030500	SAMParse
Last_Login_Date	2019-09-24 12:13:44	SAMParse
Pwd_Reset_Date	2019-09-24 11:12:01	SAMParse
Acct_Exp_Date		SAMParse
Pwd_Fail_Date	2019-09-29 16:54:20	SAMParse
User_rid	1000	SAMParse
User_ACB_FLAGS	532	SAMParse
User_failed_Count	1	SAMParse
User_login_count	2	SAMParse
user_acb_desc	Normal user account Password not required Comment does not apply	SAMParse

Ilustración 52. Datos Cuenta Usuario

De los usuarios Administrador e Invitado podemos ver que no se han detectado logins desde la instalación del sistema.

Type	Value	Source(s)
Full_Name		SAMParse
Comment	Cuenta integrada para la administración del equipo o dominio	SAMParse
Name		SAMParse
Internet_UserName		SAMParse
Password_Hint		SAMParse
Account_Type	Default Admin User	SAMParse
Create_dtm	2019-09-24 10:11:44.578125	SAMParse
Last_Login_Date	2019-11-21 04:47:20	SAMParse
Pwd_Reset_Date	2019-11-21 04:57:24	SAMParse
Acct_Exp_Date		SAMParse
Pwd_Fail_Date	No Fail Date	SAMParse
User_rid	500	SAMParse

Ilustración 53. Datos Cuenta Administrador

Result: 5 of 6		Result	Hex	Text	Application	Message	File Metadata	Results	Annotations	Other Occurrences	SAM File
Type	Value										Source(s)
Username	Invitado										SAMParse
Full_Name											SAMParse
Comment	Cuenta integrada para el acceso como invitado al equipo o dominio										SAMParse
Name											SAMParse
Internet_UserName											SAMParse
Password_Hint											SAMParse
Account_Type	Default Guest Acct										SAMParse
Create_dtm	2019-09-24 10:11:44.578125										SAMParse
Last_Login_Date	1970-01-01 01:00:00										SAMParse
Pwd_Reset_Date	1970-01-01 01:00:00										SAMParse
Acct_Exp_Date											SAMParse
Pwd_Fail_Date	No Fail Date										SAMParse

Ilustración 54. Datos Cuenta Invitado

8.2.6. ANÁLISIS LOGS SISTEMA

En esta etapa procederemos a analizar los logs y registros del sistema, los registros son una parte importante del sistema que se deba analizar debido a que se almacena información de importancia como pueden ser los registros de configuración del sistema, aplicaciones, dispositivos, etc.

REGISTRO DEL SISTEMA

Existen cuatro archivos de registro principales cada uno de estos contienen información diferente y se pueden encontrar en C:\windows\system32\config\

- System: Contiene toda la información referente al hardware del sistema
- Software: Contiene toda la información del software del sistema, parámetros de rendimiento y las configuraciones por defecto de Windows.
- Security: Contiene toda la información y parámetros de seguridad del sistema
- SAM: Contiene la información sobre el servicio de administración de cuentas del sistema y guarda las contraseñas de los usuarios registrados en el sistema

En la siguiente ilustración podemos ver la localización de estos

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(D)	Flags(Data)	Known	MDS
COMPONENTS			2019-09-29 18:16:59 CEST	2019-09-29 18:02:50 CEST	2019-09-29 18:02:50 CEST	2019-09-29 18:02:50 CEST	524088	Allocated	Allocated	unknown	0x07
DEFALT			2019-09-29 18:12:43 CEST	2019-09-29 18:12:43 CEST	2019-09-29 18:12:43 CEST	2019-09-29 18:12:43 CEST	524288	Allocated	Allocated	unknown	0x0d
DEFALT.LOG			2019-09-29 11:26:41 CEST	2019-09-29 13:09:32 CEST	2019-09-29 12:11:04 CEST	2019-09-29 12:11:04 CEST	1824	Allocated	Allocated	unknown	0x2f
DEFALT.LOG1			2019-09-29 10:13:40 CEST	2019-09-29 10:13:40 CEST	2019-07-14 04:04:08 CEST	2019-07-14 04:04:08 CEST	250880	Allocated	Allocated	unknown	0x06
DEFALT.LOG2			2019-09-29 10:13:40 CEST	2019-09-29 10:13:40 CEST	2019-07-14 04:04:08 CEST	2019-07-14 04:04:08 CEST	0	Allocated	Allocated	unknown	0x10
SAM			2019-09-29 18:12:43 CEST	2019-09-29 17:50:51 CEST	2019-09-29 18:12:43 CEST	2019-09-29 18:12:43 CEST	282144	Allocated	Allocated	unknown	0x20
SAM.LOG			2019-09-29 11:26:41 CEST	2019-09-29 13:09:32 CEST	2019-09-29 12:11:04 CEST	2019-09-29 12:11:04 CEST	1824	Allocated	Allocated	unknown	0x1a
SAM.LOG1			2019-09-29 10:13:40 CEST	2019-09-29 10:13:40 CEST	2019-07-14 04:04:08 CEST	2019-07-14 04:04:08 CEST	25600	Allocated	Allocated	unknown	0x2b
SAM.LOG2			2019-09-29 10:13:40 CEST	2019-09-29 10:13:40 CEST	2019-07-14 04:04:08 CEST	2019-07-14 04:04:08 CEST	0	Allocated	Allocated	unknown	0x1b
SECURITY			2019-09-29 18:12:43 CEST	2019-09-29 18:12:43 CEST	2019-09-29 18:12:43 CEST	2019-09-29 18:12:43 CEST	282144	Allocated	Allocated	unknown	0x4e
SECURITY.LOG			2019-09-29 11:26:41 CEST	2019-09-29 13:09:32 CEST	2019-09-29 12:11:04 CEST	2019-09-29 12:11:04 CEST	1824	Allocated	Allocated	unknown	0x1b
SECURITY.LOG1			2019-09-29 10:13:40 CEST	2019-09-29 10:13:40 CEST	2019-07-14 04:04:08 CEST	2019-07-14 04:04:08 CEST	21504	Allocated	Allocated	unknown	0x29
SECURITY.LOG2			2019-09-29 10:13:40 CEST	2019-09-29 10:13:40 CEST	2019-07-14 04:04:08 CEST	2019-07-14 04:04:08 CEST	0	Allocated	Allocated	unknown	0x1d
SOFTWARE			2019-09-29 18:12:43 CEST	2019-09-29 18:12:43 CEST	2019-09-29 18:12:43 CEST	2019-09-29 18:12:43 CEST	3988744	Allocated	Allocated	unknown	0x7d
SOFTWARE.LOG			2019-09-29 11:26:41 CEST	2019-09-29 13:09:32 CEST	2019-09-29 12:11:04 CEST	2019-09-29 12:11:04 CEST	1824	Allocated	Allocated	unknown	0x7e
SOFTWARE.LOG1			2019-09-29 10:13:40 CEST	2019-09-29 10:13:40 CEST	2019-07-14 04:04:08 CEST	2019-07-14 04:04:08 CEST	282144	Allocated	Allocated	unknown	0x49
SOFTWARE.LOG2			2019-09-29 10:13:40 CEST	2019-09-29 10:13:40 CEST	2019-07-14 04:04:08 CEST	2019-07-14 04:04:08 CEST	0	Allocated	Allocated	unknown	0x1d
SYSTEM			2019-09-29 18:12:43 CEST	2019-09-29 18:12:43 CEST	2019-09-29 18:12:43 CEST	2019-09-29 18:12:43 CEST	1022316	Allocated	Allocated	unknown	0x03
SYSTEM.LOG			2019-09-29 11:26:41 CEST	2019-09-29 13:09:32 CEST	2019-09-29 12:11:04 CEST	2019-09-29 12:11:04 CEST	1824	Allocated	Allocated	unknown	0x20
SYSTEM.LOG1			2019-09-29 10:13:40 CEST	2019-09-29 10:13:40 CEST	2019-07-14 04:04:08 CEST	2019-07-14 04:04:08 CEST	282144	Allocated	Allocated	unknown	0x2d
SYSTEM.LOG2			2019-09-29 10:13:40 CEST	2019-09-29 10:13:40 CEST	2019-07-14 04:04:08 CEST	2019-07-14 04:04:08 CEST	0	Allocated	Allocated	unknown	0x1d

Ilustración 55. Localización Archivos Registro

Los registros recomendados a buscar son:

- En esta primera clave se guardan las redes inalámbricas a la que se conectado el equipo. Este nos sirve para saber si el equipo se ha conectado a una red extraña o se ha conectado a otra red para otros hechos

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles

- En estas claves se guardan los documentos más usados recientemente cada clave puede contener hasta los últimos 10 documentos. Estos nos pueden servir para ver si se ha podido visualizar o robar algún tipo de información

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Rece ntDocs

- Esta clave nos servirá para ver si se ha introducido alguna URL extraña. Esto podría revelar donde se podría estar conectado algún malware, o puede revelar lo que el usuario estaba buscando/en.

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs

- Esta clave registra las IP que obtiene las interfaces del equipo. Sabiendo esto podríamos saber la IP que se estaba utilizando en el momento del incidente.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\Tcpip\Parameters\Interfaces

- Al hacer el análisis debemos revisar las claves más comunes donde se pueden guardar las aplicaciones o servicios que se podrían arrancar al iniciar el equipo. La clave más común es la que tenemos a continuación:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

- La siguiente es utilizada si solo se quiere que se ejecute una vez al arrancar.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

- En la siguiente clave muestra los servicios que se han configurado para se inicien al arrancar el sistema. Si está configurada en 2, el servicio se inicia automáticamente, si está configurada en 3 el servicio debe iniciarse manualmente, y si está configurada en 4 el servicio esta desactivado

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

- Para aplicación de 16 bits se encuentras en la siguiente clave

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\WOW

- En esta última clave se ejecutan las aplicaciones ejecutan cuando un usuario específico inicia sesión.

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Para el análisis se puede hacer con Autopsy debido a que podemos ver abajo en Application la estructura de los registros.

En nuestro caso las evidencias en el registro encontradas ha sido la siguiente:

En la clave HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run se ha encontrado la siguiente entrada que se ejecuta al arrancar el sistema donde lo analizaremos en profundidad en la siguiente fase de análisis de archivos

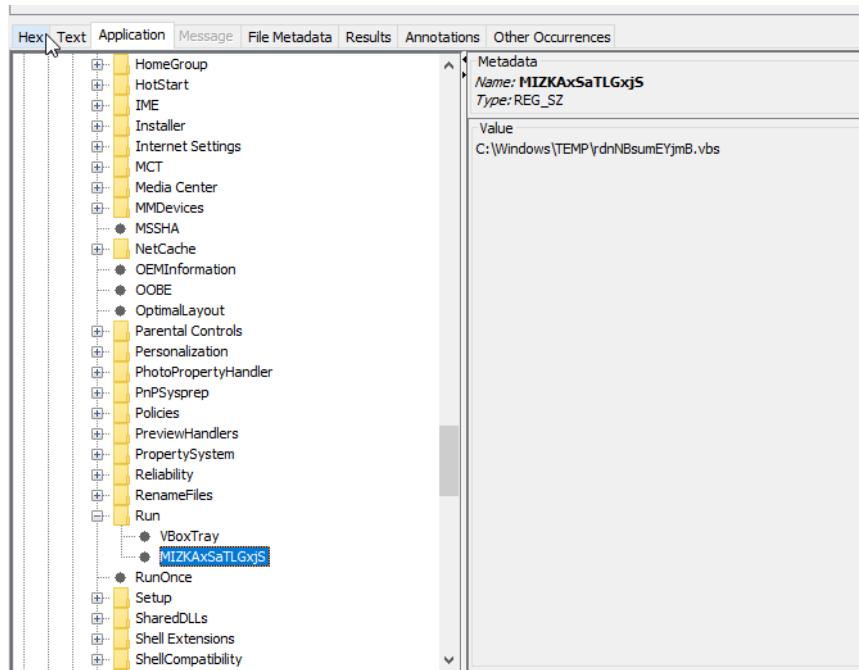


Ilustración 56. Evidencia Registro

EVENTOS DEL SISTEMA

Hecho el análisis del registro, se analizarán los eventos del sistema estos pueden proporcionarnos pistas debido a que registran los eventos del usuario en el equipo y son una fuente potencial donde poder encontrar evidencias

Estos archivos de eventos se encuentran en C:\System32\winevt\Logs\ para poder analizarlos con el botón derecho seleccionaremos “Extract Files” lo que extraerá los archivos de la imagen para poder analizar, para abrirlos se puede hacer con el Visor de Eventos de Windows

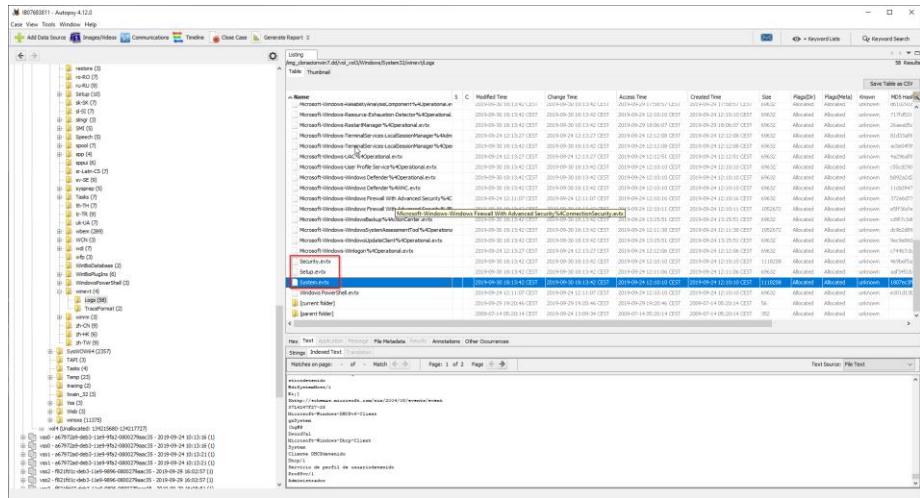


Ilustración 57. Localización archivos Eventos

En la siguiente ilustración podemos ver los archivos extraídos

TFM_RubenMesquidaGomila > IB07683811 > Export				
	Nombre	Fecha de modificación	Tipo	Tamaño
	86407-Application.evtx	06/10/2019 16:56	Registro de eventos	1.092 KB
↔	86409-HardwareEvents.evtx	06/10/2019 16:56	Registro de eventos	68 KB
	86456-Security.evtx	06/10/2019 16:56	Registro de eventos	1.092 KB
	86458-Setup.evtx	06/10/2019 16:56	Registro de eventos	68 KB
	86459-System.evtx	06/10/2019 16:56	Registro de eventos	1.092 KB

Ilustración 58. Archivos Eventos Extraídos

Empezamos analizando los eventos de Aplicaciones, que contiene todos los eventos relacionados con las aplicaciones instaladas en el sistema

En este primer archivo no se han encontrado evidencias a destacar.

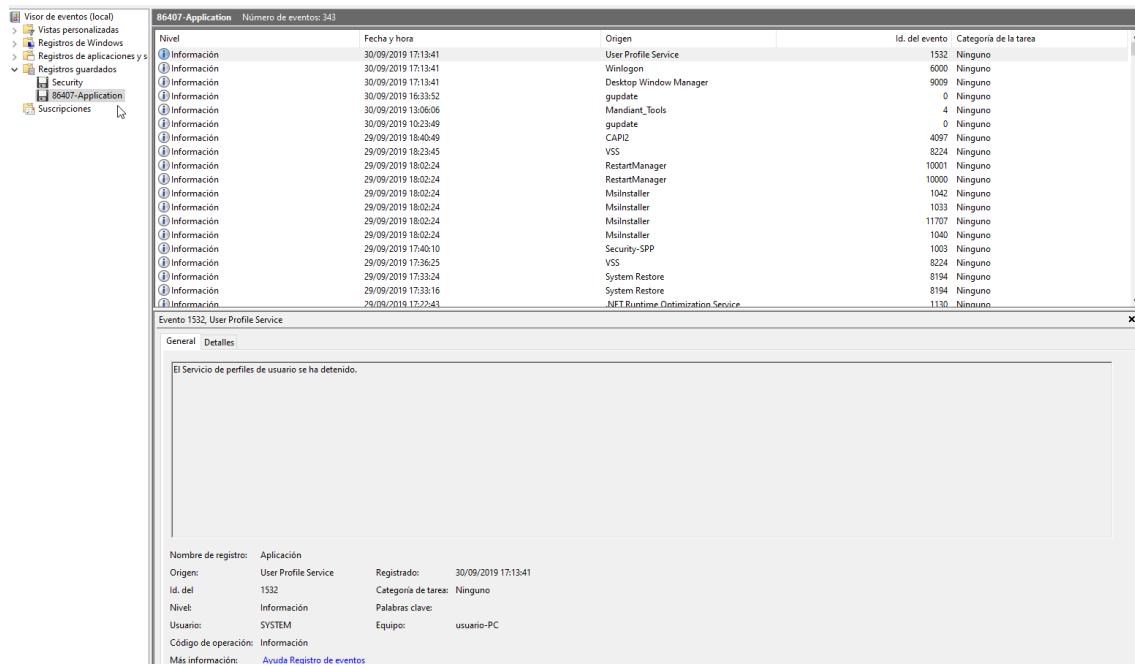


Ilustración 59. Eventos Aplicación

En los eventos de “Hardware Events” y Setup no se encontró nada destacable. Luego pasamos a analizar los eventos de System que contiene los eventos de componentes del sistema Windows, como controladores y otros servicios.

En System es útil buscar los siguientes eventos:

ID Evento XP o Anterior	ID Evento Vista o Posterior	Descripción
2934	7030	Error de creación de servicios
2944	7040	El servicio cambio de automático a deshabilitado
2949	7045	Creación de un servicio

Tabla 5. Eventos útiles System

En System tampoco se encontraron evidencias a destacar.

Por último, se analizará Security aquí encontraremos todos los eventos relacionados con la seguridad, como los intentos de inicio de sesión o el acceso a recursos.

ID Evento XP o Anterior	ID Evento Vista o Posterior	Descripción
528	4624	Inicio de sesión correcto
529	4625	Inicio de sesión incorrecto
680	4776	Validación de credenciales con autenticación NTLM tanto correctas como incorrectas
624	4720	Usuario creado
636	4732	Usuario añadido a un grupo de seguridad local
632	4728	Usuario añadido a un grupo de seguridad global

Tabla 6. Eventos útiles Security

En el evento de un inicio de sesión correcto podemos diferenciar distintos

ID	Tipo	Descripción
2	Interactivo	Un usuario ha iniciado sesión en el equipo.
3	Red	Un usuario o equipo conectado al equipo desde la red.
4	Batch	Un usuario es iniciado mediante un proceso del equipo
5	Servicio	Un usuario fue iniciado desde un servicio del equipo
7	Desbloqueo	El equipo se ha desbloqueado
8	NetworkCleartext	Un usuario conectado a este ordenador desde la red. La contraseña del usuario se pasó al paquete de autenticación en texto plano

Tabla 7. Tipos de inicio de sesión

En nuestro caso se han encontrado distintos inicios de sesión después de que el día 23 el usuario dejara de utilizar el equipo. Se detectó el día 24 a las 12:13 que también fue detectado en archivo SAM del equipo.

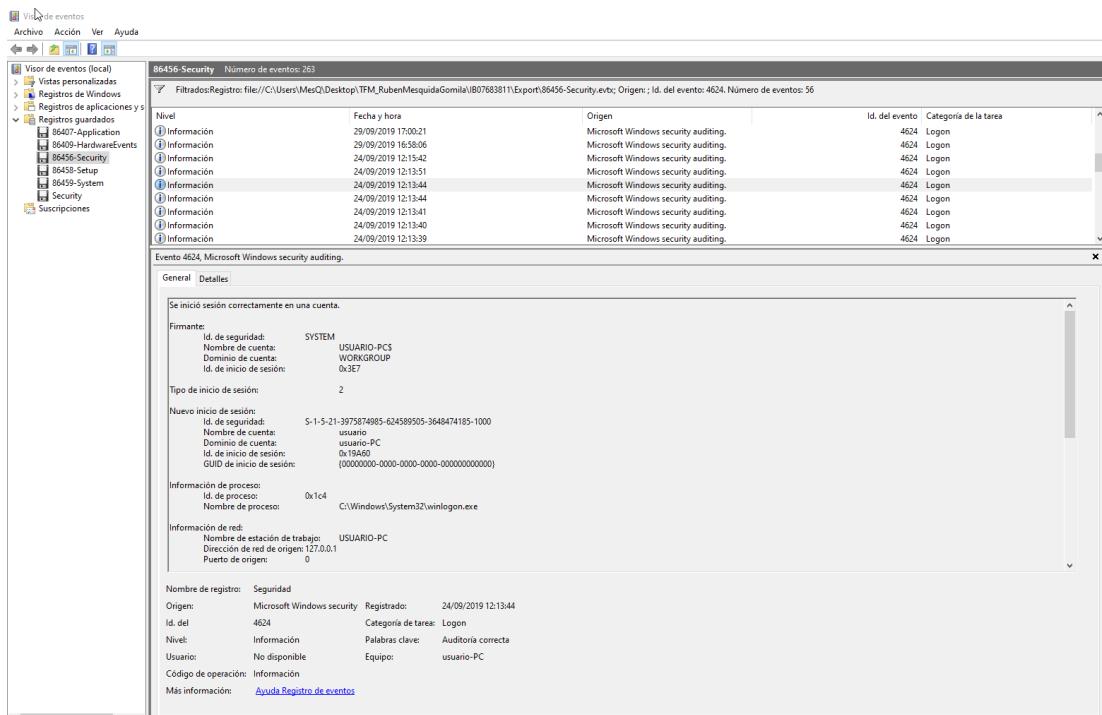


Ilustración 60. Inicios de sesión día 24

Otros datos interesantes a analizar son los dispositivos que han sido conectados al sistema, esto nos puede ser de gran ayuda si por ejemplo los datos hubieran robados en un USB en algún descuido del usuario.

DISPOSITIVOS USB

Desde Autopsy encontramos un módulo “USB Device Attached” que nos mostrara el historial de los dispositivos conectado. En este caso no hemos encontrado datos de interés.

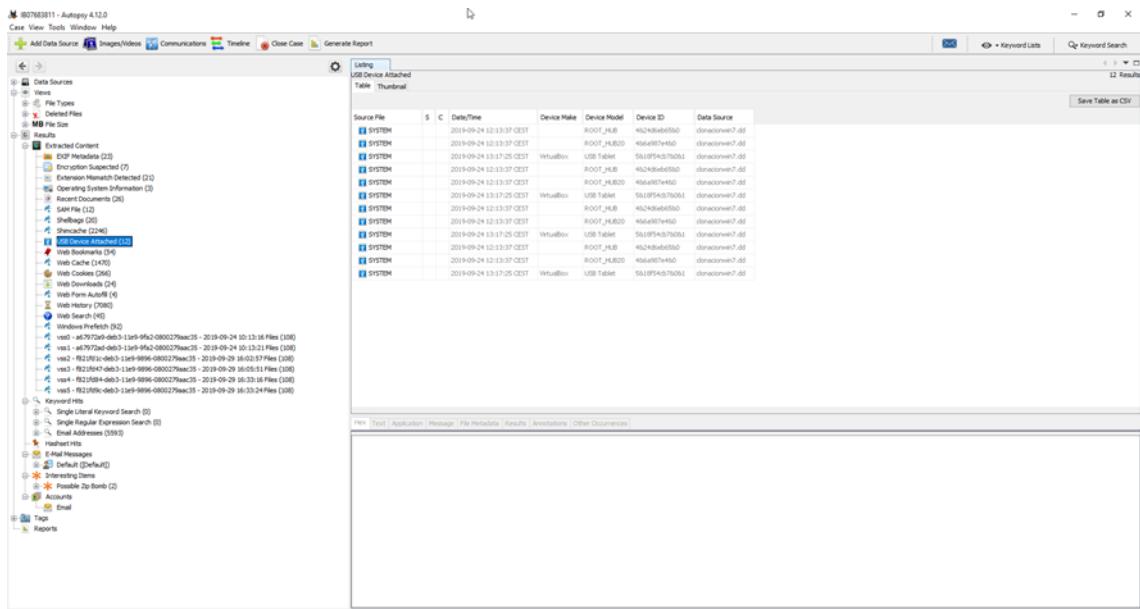


Ilustración 61. Dispositivos USB

WINDOWS PREFETCH

Después hemos analizado los archivos Prefetch que son archivos importantes al analizar un sistema, debido a que Windows crea un archivo de estos cuando se ejecuta una aplicación por primera vez esto hace que sean archivos importantes y a tener en cuenta a la hora de analizar un sistema, debido a que se puede probar que un programa se ejecutó y en la hora en la que se hizo. Incluso si el programa ha sido eliminado, es posible que aún exista un archivo Prefetch en el sistema.

No se encontró ningún archivo Prefetch destacable.

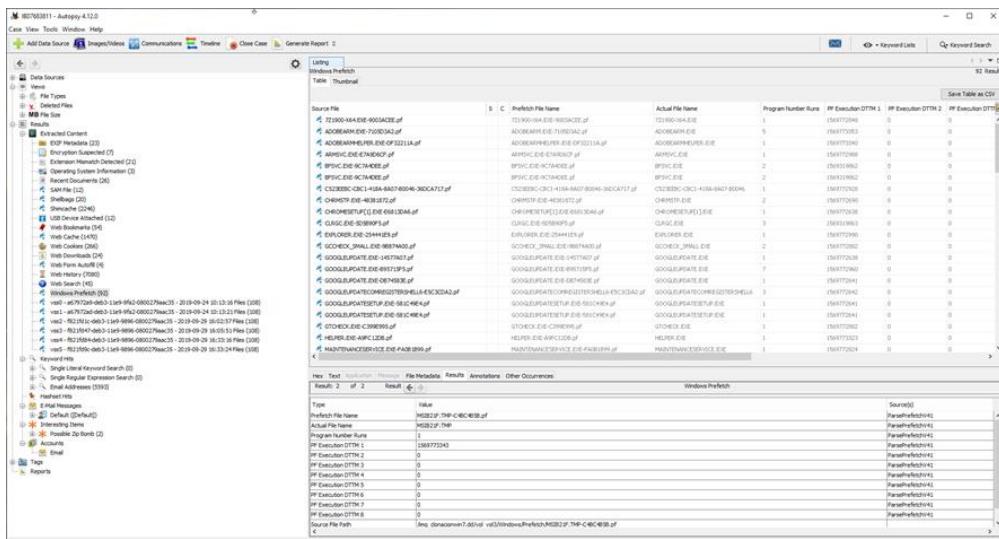


Ilustración 62. Windows Prefetch

WINDOWS SHELLBAGS

Los Shellbags son los registros de las vistas, tamaños y posiciones de una ventana de carpetas cuando se visualizan a través del Explorador de Windows. Esto nos proporciona un historial de exploración y los detalles de cualquier en un sistema incluso si ha sido borrada.

En la cuenta del propietario del equipo, encontramos distintas pruebas que, la última escritura en esas carpetas fue el día 24 y la última modificación se trata de día 29

NTUSER.DAT	09/24/2019 10:13:25	/img_clonacionwin7.dd/vol_vol3/Users/usuario/NTUSER.DAT	09/29/2019 16:07:20	01/01/1970 00:00:00	01/01/1970 00:00:00	\Contratos
NTUSER.DAT	09/24/2019 10:13:25	/img_clonacionwin7.dd/vol_vol3/Users/usuario/NTUSER.DAT	09/29/2019 16:07:20	01/01/1970 00:00:00	01/01/1970 00:00:00	\Planes
NTUSER.DAT	09/24/2019 10:13:25	/img_clonacionwin7.dd/vol_vol3/Users/usuario/NTUSER.DAT	09/29/2019 16:07:49	01/01/1970 00:00:00	01/01/1970 00:00:00	\Planes
NTUSER.DAT	09/24/2019 10:13:25	/img_clonacionwin7.dd/vol_vol3/Users/usuario/NTUSER.DAT	09/29/2019 16:07:48	01/01/1970 00:00:00	01/01/1970 00:00:00	\Planes
NTUSER.DAT	09/24/2019 10:13:25	/img_clonacionwin7.dd/vol_vol3/Users/usuario/NTUSER.DAT	09/29/2019 16:07:56	01/01/1970 00:00:00	01/01/1970 00:00:00	\Diseños
NTUSER.DAT	09/24/2019 10:13:25	/img_clonacionwin7.dd/vol_vol3/Users/usuario/NTUSER.DAT	09/29/2019 16:12:10	01/01/1970 00:00:00	01/01/1970 00:00:00	\Password Importante.txt
NTUSER.DAT	09/24/2019 10:13:25	/img_clonacionwin7.dd/vol_vol3/Users/usuario/NTUSER.DAT	09/29/2019 16:12:10	01/01/1970 00:00:00	01/01/1970 00:00:00	\Password Importante.txt
NTUSER.DAT	09/24/2019 10:13:25	/img_clonacionwin7.dd/vol_vol3/Users/usuario/NTUSER.DAT	09/29/2019 16:15:06	01/01/1970 00:00:00	01/01/1970 00:00:00	\Facturación
NTUSER.DAT	09/24/2019 10:13:25	/img_clonacionwin7.dd/vol_vol3/Users/usuario/NTUSER.DAT	09/29/2019 16:15:06	01/01/1970 00:00:00	01/01/1970 00:00:00	\Facturación
NTUSER.DAT	09/24/2019 10:13:25	/img_clonacionwin7.dd/vol_vol3/Users/usuario/NTUSER.DAT	09/30/2019 12:10:10	01/01/1970 00:00:00	01/01/1970 00:00:00	\Presupuestos
NTUSER.DAT	09/24/2019 10:13:25	/img_clonacionwin7.dd/vol_vol3/Users/usuario/NTUSER.DAT	09/30/2019 12:10:10	01/01/1970 00:00:00	01/01/1970 00:00:00	\Presupuestos

Ilustración 63. Shellbags

8.2.7. ANÁLISIS ARCHIVOS Y DATOS BORRADOS

En esta fase realizaremos el análisis del sistema, en primer lugar, realizaremos un timeline para tener una idea preliminar del sistema y después se revisarán los archivos pertinentes mediante Autopsy

TIMELINE

Un timeline contiene gran cantidad de registros y consiste el conjunto de archivos de sistema con la ubicación de este las marcas de tiempo fecha de creación, modificación, acceso, etc.

Con el timeline y teniendo esto en cuenta es recomendable que busquemos en lugares donde se suelen almacenar malware, estas ubicaciones son:

- %APPDATA%
- %TEMP%
- %WINDIR%

En estas ubicaciones se deben buscar archivos ejecutables sospechosos o archivos modificados que puedan haber sido alterados por el posible malware o la posible incidencia. Aunque también hay que tener en cuenta se pueden ocultar en otras ubicaciones, sector de arranque, particiones ocultas, etc.

Para empezar la creación del timeline utilizaremos la herramienta log2timeline, que será la encargada de generarnos el timeline de la imagen. Para ello desde una terminal ejecutaremos la herramienta indicando la salida del archivo y la ubicación de la imagen.

Como nota dependiendo del tamaño de la imagen esta operación puede tardar un buen tiempo.

```
Log2timeline.exe archivo_salida archivo_origen
```

```

C:\Users\MesQ\Desktop\TFM_RubenMesquidaGomila\Hrramientas\plaso-20190708.py3.7-amd64>log2Timeline.exe "D:\timeline.plaso" "D:\clonacionwin7.dd"
2019-10-07 13:02:31,459 [INFO] (MainProcess) PID:11924 <date location> Determined location: C:\Users\MesQ\Desktop\TFM_RubenMesquidaGomila\Hrramientas\plaso-20190708-py3.7-amd64\data
2019-10-07 13:02:31,476 [INFO] (MainProcess) PID:11924 <artifact_definitions> Determined artifact definitions path: C:\Users\MesQ\Desktop\TFM_RubenMesquidaGomila\Hrramientas\plaso-20190708-py3.7-amd64\artifacts
Checking availability and versions of dependencies.
[OPTIONAL] missing: 124.
[OK]

The following partitions were found:
Identifier Offset (in bytes) Size (in bytes)
p1 1048576 (0x00100000) 100.0MB / 104.9MB (1048576000 B)
p2 105906176 (0x0e500000) 63.9GB / 68.6GB (68612521984 B)

Please specify the identifier of the partition that should be processed. All partitions can be defined as: "all". Note that you can abort with Ctrl-C.

Partition identifiers: p2
The following Volume Shadow Snapshots (VSS) were found:
Identifier Creation Time
vss1 2019-09-24 10:13:16.0402656
vss2 2019-09-24 10:13:21.0715156
vss3 2019-09-29 16:52:57.2166571
vss4 2019-09-29 16:05:53.9769989
vss5 2019-09-29 16:13:16.4481869
vss6 2019-09-29 16:33:24.0536533

Please specify the identifier(s) of the VSS that should be processed:
Please note that VSS identifiers are 1..n. Multiple stores can be defined as: 1..3..5 (a list of comma separated values). Ranges and lists can also be combined as: 1..3..5.. The first store is 1. All stores can be defined as "all". If no stores are specified none will be processed. You can abort with Ctrl-C.

VSS Identifiers: 1..6
Source path : D:\clonacionwin7.dd
Source type : storage media image
Processing time : 00:00:00

Processing started.

```

Ilustración 64. Log2Timeline

Terminado el primer proceso tendremos creado un archivo .plaso, este archivo lo convertiremos en un archivo Excel para una mayor facilidad de uso, para eso utilizaremos la herramienta psort que viene incluida al descargar la herramienta anterior

Psort.exe -z Zona_Horaria -o formato_archivo_origen -w archivo_salida

Esta operación también puede tardar un poco dependiendo del tamaño del archivo generado.

```
c:\Users\MesQ\Desktop\TFM_RubenMesquidaGomila\Hrramientas\plaso-20190708-py3.7-amd64>psort.exe -z Europe/Madrid -o xlsx d:\timeline.plaso -w d:\timeline.xlsx
```

Ilustración 65. Timeline a Excel

Acabado este último proceso tendremos un archivo Excel que contendrá los archivos del sistema con sus diferentes “timestamps”, de esta forma podemos hacer un primer análisis de los archivos que contiene la imagen.

Año	Mes	Día	Hora	Minuto	Segundo	Timestamp	Formato	Nombre	Path	Formato	Nombre	Path
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V554T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V554T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Last Access Time	FILE	NTFS Last Access Time	V554T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V554T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Create Time	FILE	NTFS Create Time	V554T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V554T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Access Time	FILE	NTFS Last Access Time	V554T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V555T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V555T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V555T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V555T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V555T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V555T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V555T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V555T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V555T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V555T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Creation Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat			V556T5K\Windows\System32\DriverStore\FileRepository\ntf_31bf3bf5de\filestat		
2009	07	31	21:59:31.932	Creation Time	FILE	NTFS Last Access Time	V556T5K\Windows\Volume\amrnd_nv_h\ntf_31bf3bf5de\filestat	</td				

ARCHIVOS

Visualizado el timeline, teniendo en cuenta la informacion recopilada del cliente y lo que hemos descubierto hasta ahora. En el escritorio de usuario estan disponibles las distintas carpetas con los archivos relacionado con la filtracion, las diferentes rutas de losa archivos sospechos encontrados, ademas de revisar otros posibles archivos maliciosos.

Tipo	Nombre	Ruta	Modificacion	Último Acceso	Tamaño (bytes)	MD5
Carpeta	Presupuestos	C:/Users/usuario/Desktop/Presupuesto	2019-09-30 14:10:09 CEST	2019-09-30 14:10:09 CEST	¿?	N/C
Carpeta	Planos	C:/Users/usuario/Desktop/Planos	2019-09-29 18:07:47 CEST	2019-09-29 18:07:47 CEST	¿?	N/C
Carpeta	Facturacion	C:/Users/usuario/Desktop/Facturacion	2019-09-29 18:15:05 CEST	2019-09-29 18:15:05 CEST	¿?	N/C
Carpeta	Diseños	C:/Users/usuario/Desktop/Diseños	2019-09-29 18:07:54 CES	2019-09-29 18:07:54 CES	¿?	N/C
Carpeta	Contratos	C:/Users/usuario/Desktop/Contratos	2019-09-29 18:07:19 CEST	2019-09-29 18:07:19 CEST	¿?	N/C
Archivo	Password Importante.txt	C:/Users/usuario/Desktop/Password Importante.txt	2019-09-29 18:12:09 CEST	2019-09-29 18:09:41 CEST	208	4f2b9304ae2260f541ac147f39fb907a
Archivo	ejemplo-de-presupuesto-operativo.xls	C:/Users/usuario/Desktop/Presupuestos/ejemplo-de-presupuesto-operativo.xls	2019-09-29 18:06:34 CEST	2019-09-29 18:06:34 CEST	38912	f69bb3712c4df902ccf028ac289945f5
Archivo	formato-presupuesto (1).xlsx	C:/Users/usuario/Desktop/Presupuestos/formato-presupuesto (1).xlsx	2019-09-29 18:06:34 CEST	2019-09-29 18:06:34 CEST	17004	a316760ccf7846febcca6fad2c52df3
Archivo	iphone-6-plano.webp	C:/Users/usuario/Desktop/Planos /iphone-6-plano.webp	2019-09-29 18:06:34 CEST	2019-09-29 18:06:34 CEST	36154	3e41c58ff2bd6656be41b3f2281a6982

Archivo	new_iphone1-1-e1338410471243.jpg	C:/Users/usuario/Desktop/Planos/new_iphone1-1-e1338410471243.jpg	2019-09-29 18:06:34 CEST	2019-09-29 18:06:34 CEST	93784	e2b4de2c2333c6797b6e6f376dfa f55d
Archivo	12081156362-ejemplofactura.xls	C:/Users/usuario/Desktop/Facturacion/12081156362-ejemplofactura.xls	2019-09-29 18:15:05 CEST	2019-09-29 18:15:05 CEST	15872	7af044c5243f725fa5db5143105ad7a
Archivo	factura-gasolinera.docx	C:/Users/usuario/Desktop/Facturacion/factura-gasolinera.docx	2019-09-29 18:15:05 CEST	2019-09-29 18:15:05 CEST	17736	c951fbe488ca7ce07719c1d4e13d6f41
Archivo	factura-gasolinera.pdf	C:/Users/usuario/Desktop/Facturacion/factura-gasolinera.pdf	2019-09-29 18:15:05 CEST	2019-09-29 18:15:05 CEST	384911	127b99d4166b7f524e1fb54d08aebf52
Archivo	factura-gasolinera.xlsx	C:/Users/usuario/Desktop/Facturacion/factura-gasolinera.xlsx	2019-09-29 18:15:05 CEST	2019-09-29 18:15:05 CEST	31237	edff2d51866a60a9f4744d7ccc6773ee
Archivo	D3rK03RUEAA2g7c-640x360.jpg	C:/Users/usuario/Desktop/Diseños/D3rK03RUEAA2g7c-640x360.jpg	2019-09-29 18:06:34 CEST	2019-09-29 18:06:34 CEST	16579	c2a877d624076a4113819dd5314116b0
Archivo	descarga (1).jpg	C:/Users/usuario/Desktop/Diseños/descarga (1).jpg	2019-09-29 18:06:34 CEST	2019-09-29 18:06:34 CEST	4322	a3016f0e76b1a21fd4544cf5200bf998
Archivo	iPhone-7-Mock-Ups.jpg	C:/Users/usuario/Desktop/Diseños/iPhone-7-Mock-Ups.jpg	2019-09-29 18:06:34 CEST	2019-09-29 18:06:34 CEST	193967	a4ec1dec4dc2c65e759afc3fce3bd0d
Archivo	iphone-7-rojo-830x400.jpg	C:/Users/usuario/Desktop/Diseños/iphone-7-rojo-830x400.jpg	2019-09-29 18:07:34 CEST	2019-09-29 18:07:34 CEST	30257	e4b61f01cef967f5117514a9bc06f611
Archivo	contrato-de-obras-de-construccion.docx	C:/Users/usuario/Desktop/Contratos/contrato-de-obras-de-construccion.docx	2019-09-29 18:06:34 CEST	2019-09-29 18:06:34 CEST	391254	31b49a38dc72fd0721df39276e29bb5f
Archivo	contrato-de-obras-de-construccion.pdf	C:/Users/usuario/Desktop/Contratos/contrato-de-obras-de-construccion.pdf	2019-09-29 18:06:34 CEST	2019-09-29 18:06:34 CEST	439015	7b807998fbd61c1dd42d5a54402694ce
Archivo	contrato-de-prestamo-mercantil.docx	C:/Users/usuario/Desktop/Contratos/contrato-de-prestamo-mercantil.docx	2019-09-29 18:06:34 CEST	2019-09-29 18:06:34 CEST	17393	4e033188ff03cd4e7507fb04f383d17

Tabla 8. Documentos

Después de revisar y analizar los archivos podemos ver que la gran mayoría han sido accedidos y modificado por última vez el día 29, la empresa Sitsa detecto la filtración el día 30.

Este equipo analizado se dejó de utilizar el día 23 por lo que no han sido accedido por la persona normal que utiliza el equipo.

ANÁLISIS ARCHIVOS SOSPECHOSOS

Revisados los documentos, hemos procedido a revisar los archivos sospechosos encontrados hasta ahora.

Tipo	Nombre	Ruta	Modificacion	Ultimo Acceso	Tamaño (bytes)	MD5
Archivo	ed01ebfb9eb5 bbea545af4d01 bf5f107166184 0480439c6e5ba be8e080e41aa. .exe	C:/ ed01ebfb9eb5bbea545af4d01bf 5f1071661840480439c6e5babe8 e080e41aa.exe	2019-09-29 13:45:25 CEST	2019-09-29 13:45:25 CEST	3514368	84c82835a 5d21bbcf75 a61706d8a b549
Archivo	rdnNBsumEYjm B.vbs	C:/Windows/Temp/rdnNBsumEYj mB.vbs	2019-09-21 18:06:52 CEST	2019-09-21 18:06:52 CEST	99597	e80c37bf73 cbe40f74dc 4140b9b9cf cd
Archivo	qVhPAJWr.exe	C:/Windows/Temp/rad6F67A.tm p/qVhPAJWr.exe	2019-09-30 13:39:29 CEST	2019-09-30 13:39:29 CEST	73802	1c58a3839 affecb936e 108fe40a3f 74e

Tabla 9. Archivos Sospechosos

Los archivos anteriores hemos procedido a extraerlos y a reanalizarlos de nuevo con VirusTotal, el primer archivo analizado ha sido rdnNBsumEYjmB.vbs y lo detectado 37 antivirus como un Dropper. Este archivo probablemente sea el que descargue el malware utilizado para el acceso

3682453bab8ae736b785211c819e200491e2a3dc774e

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
Ad-Aware	① VB:Trojan.VBS.Dropper.AG	AegisLab	① Trojan.Win32.Generic.4!c
ALYac	① VB:Trojan.VBS.Dropper.AG	Arcabit	① VB:Trojan.VBS.Dropper.AG
Avast	① BV:Dowloader-A [Trj]	AVG	① BV:Dowloader-A [Trj]
Avira (no cloud)	① HTML/ExpKit.Gen2	Baidu	① JS.Trojan-Downloader.Agent.xk
BitDefender	① VB:Trojan.VBS.Dropper.AG	CAT-QuickHeal	① Trojan.VBS.33100
Comodo	① TrojWare.VBS.TrojanDropper.Agent.NJA...	Cyren	① JS/Agent.ADPIEldorado
DrWeb	① JS.Muldrop.457	Emsisoft	① VB:Trojan.VBS.Dropper.AG (B)
eScan	① VB:Trojan.VBS.Dropper.AG	ESET-NOD32	① VBS/TrojanDropper.Agent.NJA
F-Prot	① JS/Agent.ADPIEldorado	F-Secure	① Malware.HTML/ExpKit.Gen2
FireEye	① VB:Trojan.VBS.Dropper.AG	Fortinet	① VBS/Agent.NJA!tr
GData	① VB:Trojan.VBS.Dropper.AG	Ikarus	① Trojan.Win32.Sworf

Ilustración 67. Archivo vbs analizado

El segundo archivo analizado ha sido qVhPAJWr.exe que es detectado por 54 antivirus como un Troyano, por fechas de creación de los archivos donde este se crea segundo después del vbs detectado como un dropper, y las conexiones que hemos visto en el análisis de la memoria RAM suponemos que este es el malware utilizado para acceder al equipo

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
Acronis	① Suspicious	Ad-Aware	① Trojan.CryptZ.Gen
AhnLab-V3	① Trojan.Win32.Shell.R1283	ALYac	① Trojan.CryptZ.Gen
Antiy-AVL	① Trojan/Win32.Rozena.ed	SecureAge APEX	① Malicious
Arcabit	① Trojan.CryptZ.Gen	Avast	① Win32-SwPatch [Wrm]
AVG	① Win32-SwPatch [Wrm]	Avira (no cloud)	① TR/CryptEPACK.Gen2
BitDefender	① Trojan.CryptZ.Gen	Bkav	① W32.FamVT.RorenNhc.Trojan
CAT-QuickHeal	① Trojan.Sworf.A	ClamAV	① Win.Trojan.MSShellcode-7
Comodo	① TrojWare.Win32.Rozena.A@4jwdor	CrowdStrike Falcon	① Win/malicious_confidence_100% (D)
Cybereason	① Malicious.39affe	Cylance	① Unsafe
Cyren	① W32/Sworf.A.gen!Eldorado	DrWeb	① Trojan.Sworf.1
eGambit	① Trojan.Generic	Emsisoft	① Trojan.CryptZ.Gen (B)

Ilustración 68. Troyano Analizado

Y el tercer archivo analizado, detectado por 64 antivirus y como habíamos visto en el primer análisis de malware realizo con ClamAV y Yara se trata de un Ransomware WannaCry. Suponemos que la intención era ejecutarlo después de filtrar los datos para dejar inutilizado el equipo o simplemente para pedir el rescate.

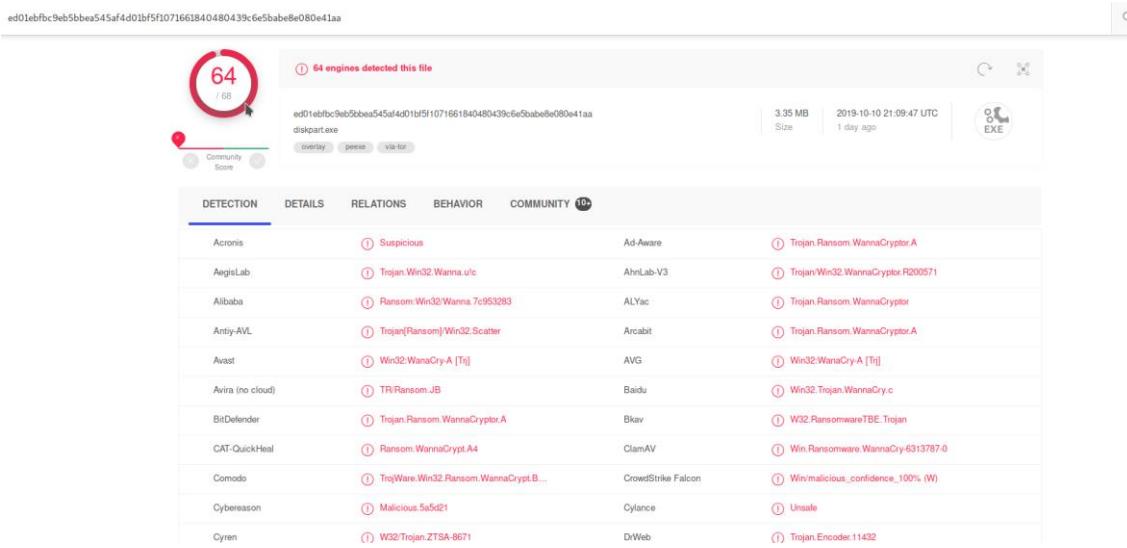


Ilustración 69. Ransomware WannaCry Analizado

ARCHIVOS BORRADOS, HUERFANOS Y FILE CARVING

A parte de haber analizado y revisado los archivos, también se han revisados los archivos borrados en el sistema, es importante revisar estos archivos borrados porque los atacantes la gran mayoría de veces borrarán archivos utilizados para no ser detectados, y hasta que el sistema no los sobrescriba se podrán recuperar.

Se han detectado 10724 archivos borrados, la gran mayoría son archivos del sistema, pero se han encontrados copias de los archivos filtrados borrados, además de algunos instaladores de programas.

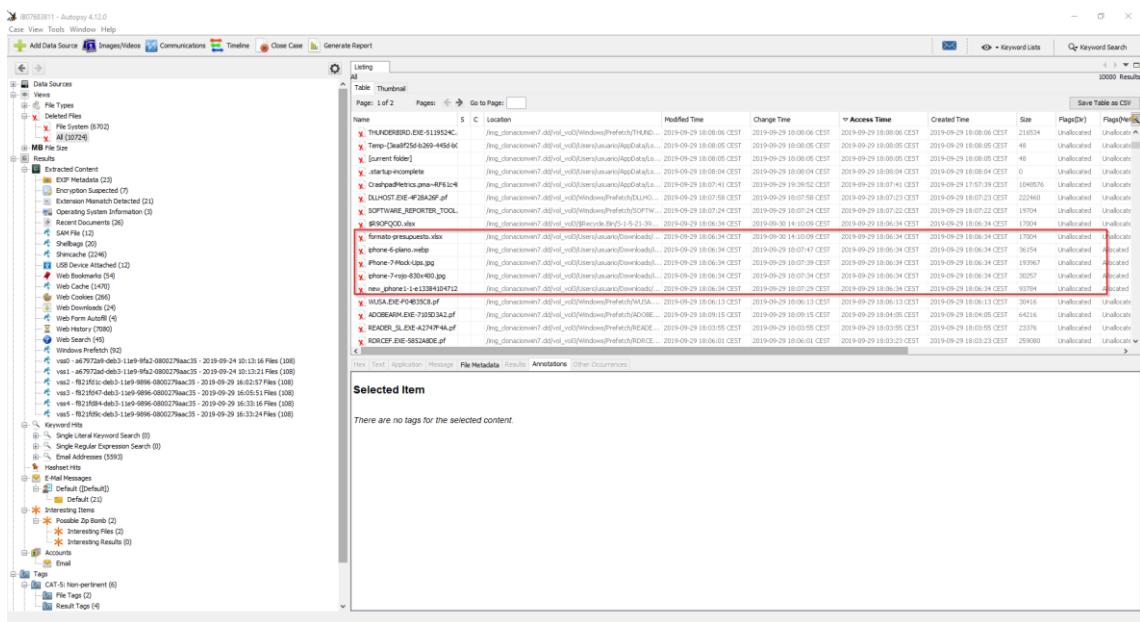


Ilustración 70. Archivos Borrados

No se han detectado archivos huérfanos, estos son archivos borrados que todavía tienen metadatos en el sistema de archivos, pero que no pueden ser accedidos desde el directorio raíz.

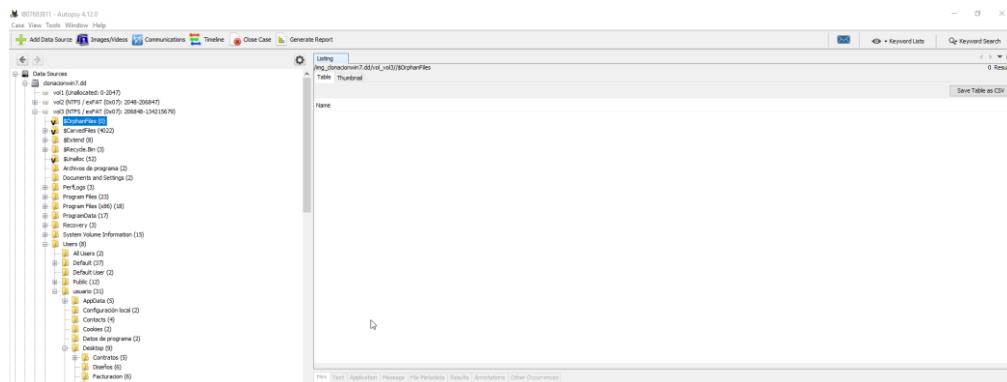


Ilustración 71. Archivos huérfanos

Los “carved files” son archivos borrado que han sido reconstruidos a partir de una cantidad de datos en bruto. Estos son recuperados de la zona no reservada del disco es decir del área de disco donde no hay nada almacenado. Es recomendable revisarlos en búsqueda de evidencias que nos puedan ayudar en la investigación

Se han encontrado 4022 “carved files”, pero no se detectaron archivos que puedan ser de interés.

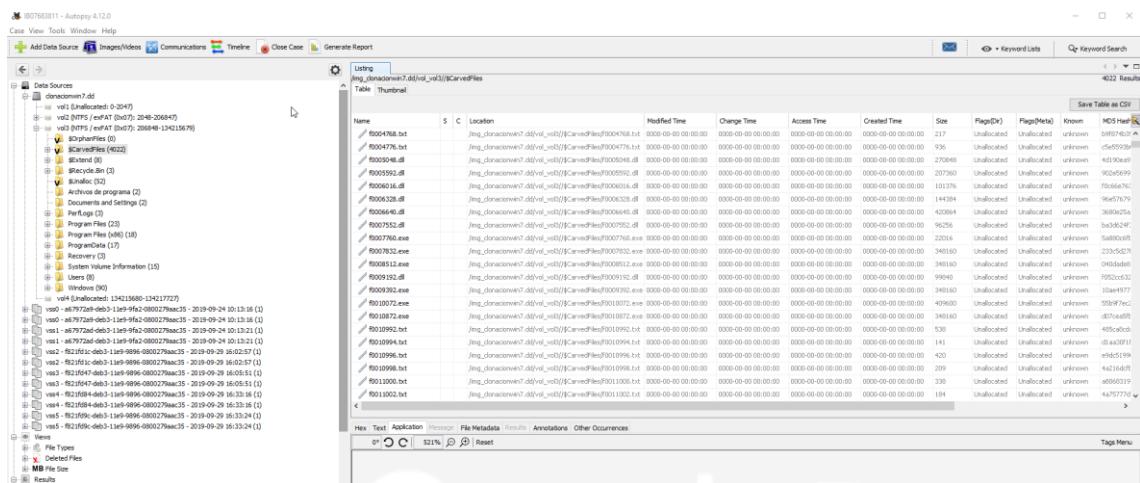


Ilustración 72. Carved Files

En esta fase como ultimo paso hemos revisado los archivos del espacio no asignando que son trozos del sistema de archivos que actualmente no se utilizan para nada. Este espacio puede almacenar archivos borrados y otros artefactos interesantes.

8.2.8. ANÁLISIS DATOS (ACTIVIDAD RECIENTE, COOKIES, HISTORIAL WEB, ETC.)

Finalizado el análisis de los archivos, procederemos a analizar los datos del sistema como pueden ser documentos recientes y toda la actividad web. De esta forma podemos obtener y añadir más información al caso.

DOCUMENTOS RECIENTES

En primer lugar, revisaremos los documentos recientes, de esta forma podemos ver la actividad que ha tenido el usuario.

En los documentos recientes podemos como hemos visto en el análisis de archivos que se han abierto los documentos el día 29 cuando ya el equipo no se estaba utilizando y justo un día antes de la filtración de la información.

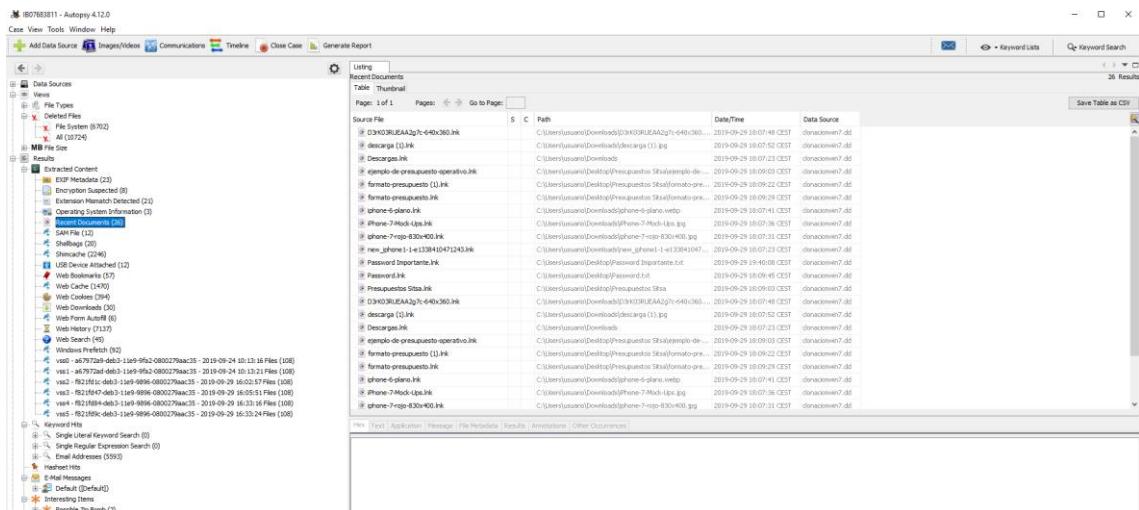


Ilustración 73. Documentos Recientes

DESCARGAS WEB

Los siguiente ha sido analizar las descargas web que se han hecho, es importante revisarlo en búsqueda de archivos sospechosos o alguna descarga que haya podido hacer el atacante.

En nuestro caso se han detectado distintas descargas, pero todas estas son de instaladores de programas de URLs de desarrolladores de confianza, por lo tanto, no se detectaron archivos sospechosos.

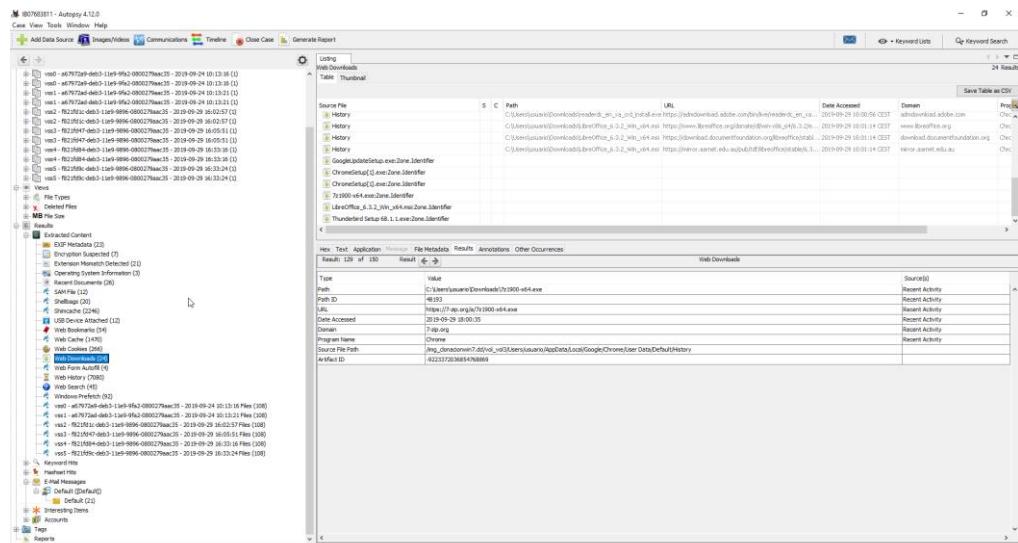


Ilustración 74. Descargas web

MARCADORES

Analizadas las descargas, se han revisado los marcadores o favoritos, en búsqueda de alguna web extraña, se detectaron un total de 57 marcadores, pero no se encontró que ninguno de ellos fueran sospechosos.

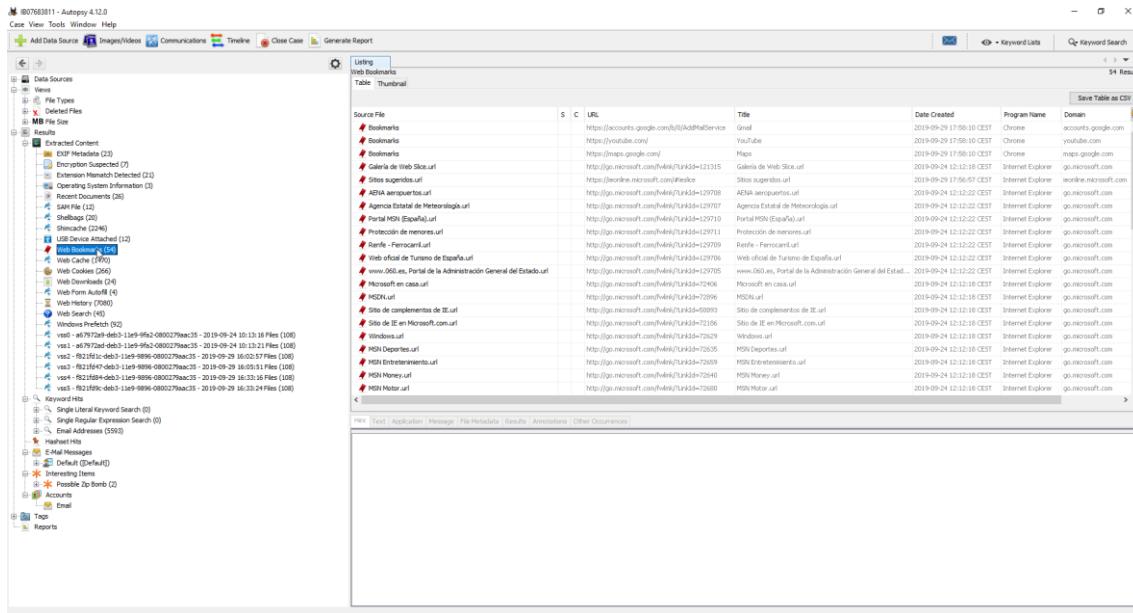


Ilustración 75. Marcadores

BÚSQUEDAS WEB

Se han revisado las b usquedas realizadas en el equipo, es importante revisarlo en busca de b usquedas extra nias que se hayan hecho y que nos complemente en la informaci on recopilada hasta ahora.

En este caso se encontró una búsqueda extraña a “pastebin” que es un sitio web que permite subir texto para que estén públicamente visibles. Se encontrado una búsqueda realizada el día 29-09-19 a las 19:39

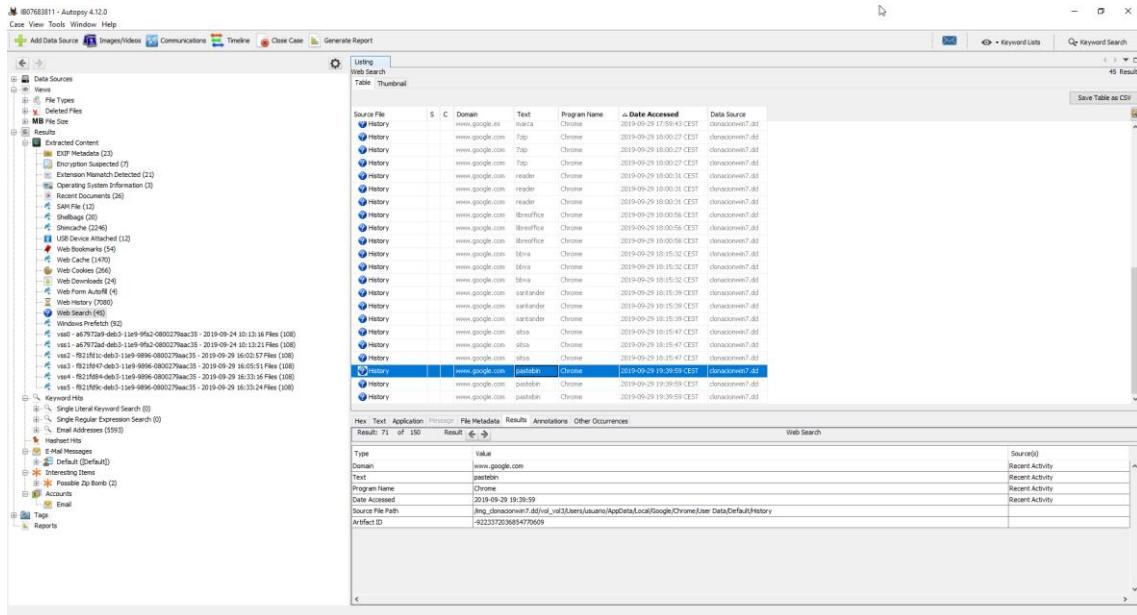


Ilustración 76. Búsqueda Pastebin

COOKIES

En el análisis de cookies se detectaron 394 cookies, con este análisis podemos hacer un seguimiento y obtener información sobre si el usuario tuvo una sesión activa, desde donde se encontró el sitio, etc.

Con el análisis de las cookies, podemos confirmar que se accedió a la web de pastebin debido a que se creó una sesión en dicha web, la sesión creada la encontramos a las 19:40:46 del día 29.

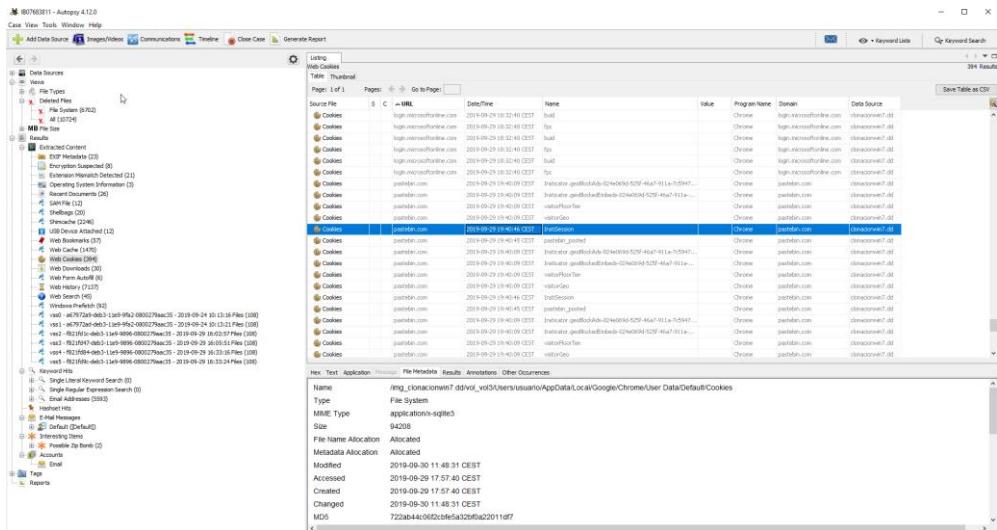


Ilustración 77. Análisis cookies

HISTORIAL

El análisis del historial web es una parte importante, debido a que nos da mucha información sobre el usuario y sobre sus hábitos. Conociendo los hábitos del usuario podemos diferenciar búsquedas extrañas o que el usuario no haya podido realizar.

En nuestro caso tenemos 7137 entradas en el historial. En el historial del usuario vemos páginas típicas como pueden ser periódicos, banca, etc. Pero como hemos visto en las cookies se ha accedido a pastebin; esta búsqueda de pastebin es una búsqueda extraña que cuadra con los hábitos del usuario.

A las 2019-09-29 19:40:45 encontramos que se accedió a la siguiente URL

<https://pastebin.com/post.php> que la pagina que procesa la subida de información a la web justo en el mismo monteo se detecta la siguiente URL

<https://pastebin.com/c6WQr4SU>

Ilustración 78. Análisis Historial

Si accedemos a esta página encontrada en el historial, vemos que se trata de una filtración de información personal del usuario, junto con información personal de la empresa. Por lo tanto, podemos suponer que esta información se filtró del propio equipo.

The screenshot shows a web browser window with the URL pastebin.com/c6WQr4SU. The page title is "PASTEBIN". The main content is a paste titled "Master Ciberseguridad PRUEBA" by "A GUEST" posted on "SEP 29TH, 2019" at "11:00 NEVER". A message encourages users to "Sign Up" to unlock features. The paste content is a list of 15 items, each numbered from 1 to 15:

1. Correo
2. sitsamaster@gmail.com 1A2B3C4d
- 3.
4. usuario empresa
- 5.
6. d.gonzalez@sitsa.com 1000.SITSA
- 7.
8. direccion@sitsa.com Gusano77
- 9.
10. Banco
11. 45365894h 746531
- 12.
13. PIN TARJETA
- 14.
15. 5300 4165 8532 4562 cvv 041 pin 5245

Below the paste, there are links for "RAW", "DATA", and "PLAIN".

Ilustración 79. Web Pastebin

8.2.9. ANÁLISIS EMAIL

Una vez terminado el análisis de los datos del sistema, vemos que Autopsy ha detectado emails que se van a proceder a analizar. Es interesante el análisis de emails debido a que se ha convertido en una de las formas de comunicación más utilizadas a nivel mundial, por eso puede ser objetivo de ataque por parte de actores malintencionados desde spam, phishing, pasando por acoso etc. De este modo analizando los emails se podrían descubrir importantes evidencias que ayudarían a un análisis.

Se han detectado 21 correos en total, en uno de esos correos de día 29 de septiembre a las 12:00:47, se ha detectado un correo sospechoso de phishing

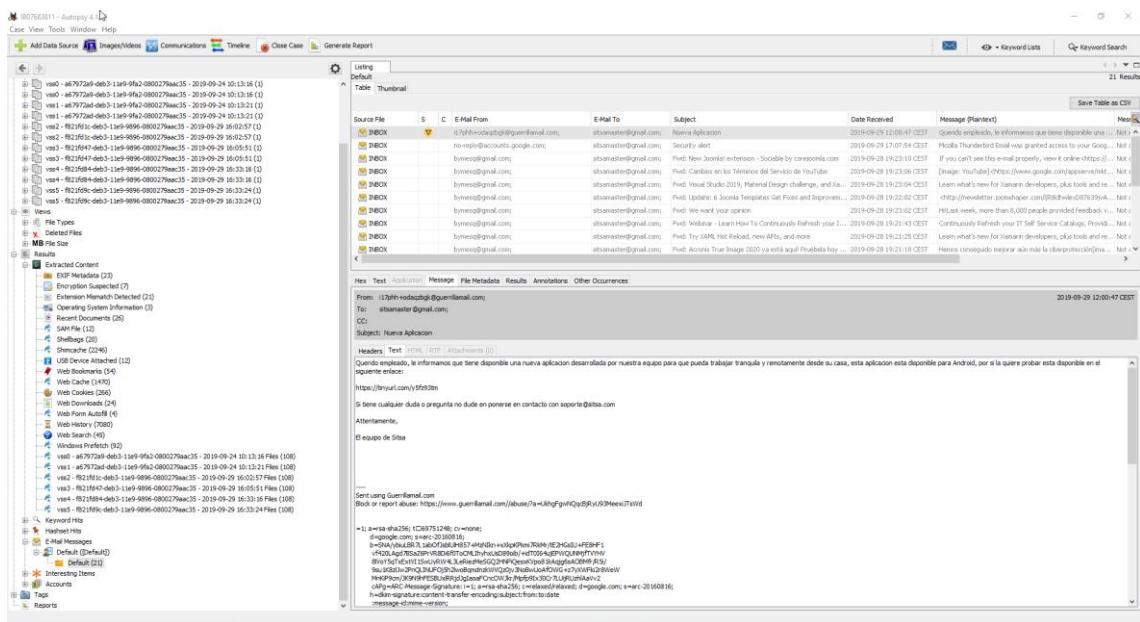


Ilustración 80. Email extraño

Leyendo el mensaje, vemos que dice el mensaje tiene disponible una nueva aplicación para Android, dirigiéndonos al mensaje vemos que nos descarga una APK. Analizando esta APK vemos que es detectada por 28 antivirus como malware como una Shell de meterpreter

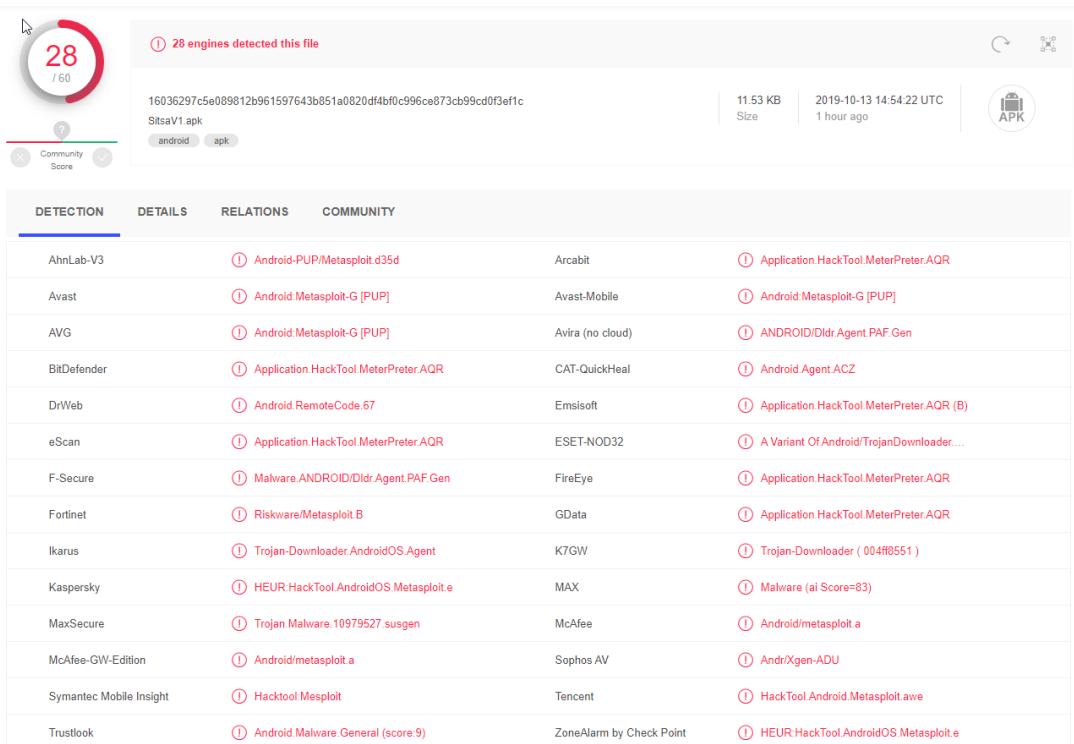


Ilustración 81. Análisis APK

Siguiendo el análisis del dicho correo, en las cabeceras del correo vemos que el remitente es 17phh+odaqzbhk@guerrillamail.com una cuenta bastante extraña

```
> dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=guerrillamail.com
Return-Path: <17phh+odaqzbhk@guerrillamail.com>
Received: from mail.guerrillamail.com ([2607:5300:60:689e::])
    by mx.google.com with ESMTPS id q39si9896345qtk.133.2019.09.29.03.00.48
    for <sitsmaster@gmail.com>
    (version=TLS_1_3 cipher=TLS_AES_256_GCM_SHA384 bits=6/256);
Sun, 29 Sep 2019 03:00:48 -0700 (PDT)
Received-SPF: pass (google.com: domain of 17phh+odaqzbhk@guerrillamail.com designates 2607:5300:60:689e:: as permitted sender) client-ip=2607:5300:60:689e::;
Authentication-Results: mx.google.com;
dkim=pass header.i=@guerrillamail.com header.s=highgrade header.b=JV6WW3a3;
spf=pass (google.com: domain of 17phh+odaqzbhk@guerrillamail.com designates 2607:5300:60:689e:: as permitted sender) smtp.mailfrom=17phh+odaqzbhk@guerrillamail.com;
dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=guerrillamail.com
Received: by 167.114.101.158 with HTTP; Sun, 29 Sep 2019 10:00:47 +0000
MIME-Version: 1.0
Message-ID: <51e46b0e8a3a84fbef18872e7bb652d977@guerrillamail.com>
Date: Sun, 29 Sep 2019 10:00:47 +0000
To: <sitsmaster@gmail.com> <sitsmaster@gmail.com>
From: <17phh+odaqzbhk@guerrillamail.com>
Subject: Nueva Aplicacion
X-Originating-IP: [185.142.15.222]
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: quoted-printable
X-Domain-Signer: PHP mailDomainSigner 0.2-20110415 <http://code.google.com/p/php-mail-domain-signer/>
DKIM-Signature: v=1; a=rsa-sha256; s=highgrade; d=guerrillamail.com; b=;
t=69751248; c=relaxed/relaxed; h=to:from:subject;
bh=wHYYoxX9EzcVyuN58u8zdbiulvKcAYO6HJLtxY5CUA=;
b=JV6WW3a357aoTPd8y/d2xv9hQoAkhfk7kt6dT6zeQPHiskRDyqFI7uVX7i4bmSa+Bf+GvYWHM
ZeEXfz2RLHTnnIV0wbq07Y1CaZPjpsDib3Pdu8VzgV2Sj+DTrClmvTfUqj3OJGm5DsCdl/_7dyh
GyHXK3vcvK31hdFistqnBtA36m/E3ryYClkdjn76cPf7xoGPrkolRxxr4Z8LjopANEsMqA/uu
0jZO9i+TF1LYzbJbe5gfYxuFJDItEMxKK+lwMe9eNmzGZeD0nm78gL0VkoPHr+uGRNRFgWBhG
UKCc/wxUdeYqX7zwhmSBP11k4EcbsdBkHzieLA=
Querido empleado, le informamos que tiene disponible una n
```

Ilustración 82. Cabecera correo electrónico

Si indagamos en el dominio guerrillamail vemos que se trata de un servicio de correo electrónico temporal, lo que confirma que probablemente se trata de un correo malicioso.

Lo analizado hasta ahora nos hace pensar que se puede deber a un APT dirigido a esta empresa.

8.2.10. ANÁLISIS OTRAS APLICACIONES

En todo análisis forense se deberían revisar si existen otras aplicaciones instaladas en el sistema susceptibles de ser atacadas y por lo tanto también deberían ser analizadas

Para la detección de los programas instalados se podría hacer desde Autopsy buscando manualmente en sitio como c:\Program Files, c:\Program Files (x86) o en el registro de Windows

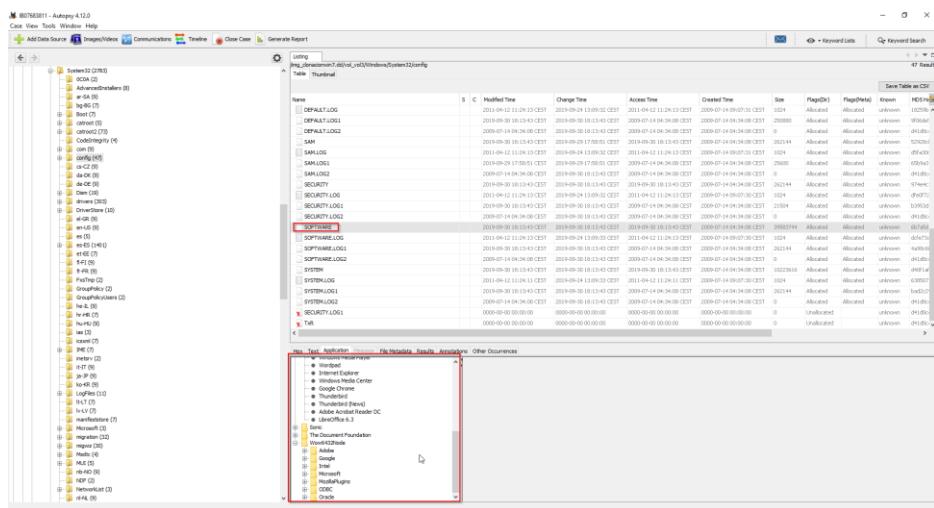


Ilustración 83. Programas Registro

Name	S	C	Modified Time	Change Time	Access Time	Access
[current folder]			2019-09-29 18:06:10 CEST	2019-09-29 18:06:10 CEST	2019-09-29 18:06:10 CEST	2019-0
[parent folder]			2019-09-30 13:45:22 CEST	2019-09-30 13:45:22 CEST	2019-09-30 13:45:22 CEST	2019-0
7-Zip			2019-09-29 18:00:49 CEST	2019-09-29 18:00:49 CEST	2019-09-29 18:00:49 CEST	2019-0
Archivos comunes			2019-09-24 12:12:01 CEST	2019-09-24 12:12:01 CEST	2019-09-24 12:12:01 CEST	2019-0
Common Files			2009-07-14 05:20:08 CEST	2019-09-24 13:09:34 CEST	2019-09-24 13:09:34 CEST	2009-0
DM Meker			2011-04-12 11:21:07 CEST	2019-09-24 13:09:34 CEST	2011-0	
Internet Explorer			2011-04-12 11:10:05 CEST	2019-09-24 13:09:34 CEST	2011-0	
LibreOffice			2019-09-29 18:06:23 CEST	2019-09-29 18:06:23 CEST	2019-09-29 18:06:23 CEST	2019-0
Microsoft Games			2011-04-12 11:21:05 CEST	2019-09-24 13:09:34 CEST	2019-09-24 13:09:34 CEST	2011-0
Mozilla Thunderbird			2019-09-29 18:00:23 CEST	2019-09-29 18:00:23 CEST	2019-09-29 18:00:23 CEST	2019-0
MSBuild			2009-07-14 07:32:38 CEST	2019-09-24 13:09:34 CEST	2019-09-24 13:09:34 CEST	2009-0
Oracle			2019-09-24 12:13:08 CEST	2019-09-24 12:13:08 CEST	2019-09-24 12:13:08 CEST	2019-0
Reference Assemblies			2009-07-14 07:32:38 CEST	2019-09-24 13:09:34 CEST	2019-09-24 13:09:34 CEST	2009-0
Uninstall Information			2009-07-14 07:09:26 CEST	2019-09-24 13:09:34 CEST	2019-09-24 13:09:34 CEST	2009-0
Windows Defender			2011-04-12 11:10:05 CEST	2019-09-24 13:09:34 CEST	2019-09-24 13:09:34 CEST	2011-0
Windows Journal			2011-04-12 11:21:05 CEST	2019-09-24 13:09:34 CEST	2011-0	
Windows Mail			2011-04-12 11:10:05 CEST	2019-09-24 13:09:34 CEST	2011-0	
Windows Media Player			2011-04-12 11:10:05 CEST	2019-09-24 13:09:34 CEST	2011-0	
Windows NT			2019-09-24 12:12:01 CEST	2019-09-24 12:12:01 CEST	2019-09-24 12:12:01 CEST	2019-0
Windows Photo Viewer			2011-04-12 11:10:05 CEST	2019-09-24 13:09:34 CEST	2011-0	
Windows Portable Devices			2010-11-21 04:31:34 CET	2019-09-24 13:09:34 CEST	2010-1	
Windows Sidebar			2011-04-12 11:10:05 CEST	2019-09-24 13:09:34 CEST	2011-0	
desktop.ini			2009-07-14 06:54:24 CEST	2019-09-24 13:07:54 CEST	2009-0	

Ilustración 84. Program Files

En total se han detectado los siguientes programas instalados:

Nombre Programa	
7-ZIP	
LibreOffice	

Mozilla Thunderbird
Adobe Reader
Google Chrome

En este caso no se detectaron evidencias en las aplicaciones listadas. Como nota es interesante revisar la ruta de instalación de extensiones de Google Chrome en búsqueda de alguna extensión maliciosa

C:/Users/usuario/AppData/Local/Google/Chrome/User Data/Default/Extensions/

9. FASE FINAL

Terminada toda la parte de análisis e investigación se procederá a enumerar las evidencias encontradas durante el análisis, y las conclusiones con las relaciones de dichas evidencias.

9.1 HALLAZGOS EVIDENCIAS

Durante el análisis y como resumen se encontraron las siguientes evidencias:

ID	Descripción
1	En el análisis de la memoria RAM se encontró el proceso 3204 qVhPAJWr.exe en ejecución
2	El proceso 3204 se estaba conectando hacia un equipo al puerto 4444
3	Se detecto en el sistema el archivo ed01ebfb9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe en la ruta c:\ que después del análisis de malware se evidencio que trataba de un Ransomware de la variante WannaCry
4	Se encontró que el archivo rdnNBsumEYjmB.vbs estaba configurado que se ejecutara al arrancar el sistema. Dentro del registro HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\
5	Se encontraron archivos acceditos después del 23 de septiembre que el usuario dejo de utilizar el equipo
6	Se detectaron inicios de sesión después de día 23 que el usuario dejo de utilizar el equipo.

7	Se encontraron archivos de la filtración borrados en el sistema
8	Se detecto que el archivo rdnNBsumEYjmB.vbs es un malware, en concreto un dropper que descarga el archivo qVhPAJWr.exe
9	Se detecto que el archivo qVhPAJWr.exe es un malware en concreto un troyano, probablemente utilizado como acceso al equipo
10	Se encontró una evidencia de un enlace en PasteBin el día 2019-09-29 19:40:45 https://pastebin.com/c6WQr4SU En el cual se evidencia información filtrada del usuario afectado
11	El día 29 de septiembre a las 12:00:47, se ha detectado un correo malicioso el cual contenía una aplicación infectada Android infectada.

Tabla 10. Hallazgos encontrados

9.2 CONCLUSIONES

Listados los hallazgos anteriores se han llegado a las siguientes conclusiones:

Se detecto un malware utilizado para la conexión al equipo llamado qVhPAJWr.exe en la ruta C:\Windows\Temp\rad6F67A.tmp, este malware se vio activo en la captura de la memoria RAM haciendo conexión hacia un equipo de la misma red hacia el puerto 4444 que es comúnmente utilizado por un software de pentesting altamente utilizado llamado Metasploit.

Aparte se encontró un ransomware dentro el equipo en la ruta C:\ed01ebfb9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe que no se llegó a ejecutar debido a que no se encontraron archivo cifrados en el equipo.

Además, se encontraron accesos a los archivos citados después de que el usuario dejara el equipo el día 23 de septiembre, y justo un día antes (el 29 de septiembre) de que se produjera la filtración de la información el día 30 de septiembre, junto a estos se detectaron varios inicios de sesión ese mismo día

En el historial web analizado se detectó un acceso a PasteBin el día 2019-09-29 19:40:45 donde probablemente se filtró la información del usuario <https://pastebin.com/c6WQr4SU>

Ese mismo día 29 de septiembre a las 12:00:47, se detectó un email phishing desde una cuenta de email temporal del servicio GuerrillaMail, este contenía un enlace de descarga, donde se descargaba una aplicación para Android que fue detectada como malware

Teniendo en cuenta todo lo anterior y con los hallazgos encontrados, podemos determinar que se encuentran evidencias suficientes para decir que el equipo ha sido vulnerado.

Hechas las conclusiones se elaboró el Informe Pericial anexo, que en caso de necesitarlo dicho informe podría ser ratificado en sede judicial



INFORME PERICIAL SITSA

CASO N.º IB07683811

Ruben Mesquida Gomila
N.º COL 07760

Ilustración 85. Anexo 11 Informe pericial

Tabla de contenido

Declaración o Juramento de Promesa	3
Declaración de imparcialidad	3
Confidencialidad	4
Derechos previos sobre la información	4
Derechos de propiedad	4
Protección de datos	4
Introducción	5
Descripción del equipo	5
Objetivo	5
Metodología	5
Procedimiento	6
Conclusiones	7

Ilustración 86. Contenido Informe Pericial

10. ANEXOS

Anexo 1 Acuerdo de Confidencialidad



ACUERDO DE CONFIDENCIALIDAD Y SECRETO

Menorca, 1 de octubre de 2019

REUNIDOS

D. Ruben Mesquida Gomila, mayor de edad y con domicilio en Menorca, con DNI 417452523Q, Perito Judicial Informática Forense con N.º de colegiado 07760.

D. Juan García Pérez mayor de edad y con DNI. 45875365H en nombre y representación de la empresa Servicios Integrales Tecnológicos S.A con CIF A07818501

EXPONEN

- Que ambas partes de reconocen capacidad suficiente para suscribir el presente contrato.
- Que durante el tiempo de relación las partes intercambiarán o crearán información, la cual están interesadas en regular la confidencialidad y secreto mediante las siguientes:

CONDICIONES

Objeto

Con el presente contrato las partes fijan formalmente y por escrito los términos y las condiciones bajo las que mantendrán la confidencialidad de la información suministrada y creada entre ellos.

A los efectos de este acuerdo, tendrá la consideración de información confidencial, toda la información susceptible de ser revelada por escrito, de palabra o por cualquier otro medio o soporte. Este acuerdo obliga a las partes a adoptar las medidas oportunas para asegurar el tratamiento confidencial de la información.

Duración

Este acuerdo tendrá una duración indefinida desde el momento de su firma. En caso de que no se renueve el contrato, ambas partes deberán devolver a la otra toda la información remitida entre sí, comprometiéndose a la destrucción de la misma.

Cada parte se compromete a mantener el compromiso de confidencialidad respecto a la información y material intercambiado entre las partes, de forma indefinida tras la finalización de este acuerdo.

Confidencialidad

Las partes se obligan a entregarse todo el material que sea necesario, y en el caso de ser este confidencial se comprometen a:

- a. Utilizar dicha información de forma reservada.
- b. No divulgar ni comunicar la información facilitada por la otra parte.
- c. Impedir la copia o revelación de esa información a terceros, salvo que gocen de aprobación escrita de la otra parte.
- d. Restringir el acceso a la información a sus empleados y subcontratados, en la medida en que razonablemente puedan necesitarla para el cumplimiento de sus tareas acordadas.

Anexo 2 Formulario solicitud de Servicio

 <h3 style="text-align: center;">Formulario Solicitud de Servicio</h3>				N.º Caso:
				IB07683811
Información del Cliente				
Fecha: 01/10/2019	Nombre: Juan	Apellidos: García Pérez (SITSA)		NIF / CIF: CIF A07818501
País: España		Correo electrónico: j.garcia@sitsa.com	N.º Teléfono: 605 26 57 85	
Dirección: Av. Jaime el Conquistador 3		Código Postal: 07760	Provincia: Baleares	
Información del Caso				
Nombre Caso: Sitsa / IB07683811		Tipo Caso: Filtración información		
Impacto: <input checked="" type="checkbox"/> Alto <input type="checkbox"/> Medio <input type="checkbox"/> Bajo	Proceso Judicializado: <input checked="" type="checkbox"/> Sí <input type="checkbox"/> no	Valoración: Se valora con un impacto medio debido a que la filtración de la información puede acarrear perdidas a la empresa, pero no significa que esta empresa vaya a cerrar o para su habitual funcionamiento.		
Perito responsable: Ruben Mesquida Gomila			N.º Colegiado: 07760	
Correo Electrónico del perito: ruben.mesquida@perito.com			N.º Teléfono perito: 600 60 50 40	
Firma Cliente: 	Firmando usted acepta la información presentada es correcta para la realización del análisis forense. Este formulario debe ser entregado antes con máximo de 45 días después de la fecha especificada			Firma Perito: 
Más Información				
Sistema Operativo/s: <input checked="" type="checkbox"/> Windows <input type="checkbox"/> Apple / Mac <input type="checkbox"/> Linux / Unix <input checked="" type="checkbox"/> Android <input type="checkbox"/> Otros				
Ha sido analizado antes: <input checked="" type="checkbox"/> Si <input type="checkbox"/> No	En caso afirmativo indique el resultado y por quien se realizó:			
Contienen información sensible: <input checked="" type="checkbox"/> Si <input type="checkbox"/> No	En caso afirmativo indíquelo: Contiene distintos diseños de dispositivos y patentes de la empresa			
Requiere un manejo o cuidado especial: <input checked="" type="checkbox"/> Si <input type="checkbox"/> No	En caso afirmativo indíquelo:			
Servicios Demandados:	Por favor, enumere cada dispositivo con sus números de serie. Describa EN DETALLE el problema y el servicio que solicita; consulte la página 2 para obtener más información. Si usted tiene documentos suplementarios que pueden ayudar en el análisis, adjúntelos a esta solicitud.			
<p>El pasado 30 de septiembre detectamos una filtración de distintos diseños y planos de nuestros nuevos dispositivos que tenían que salir al mercado en breve. Esto nos puede provocar problemas en el lanzamiento lo que provocaría perdidas para la empresa.</p> <p>Después de investigar internamente el suceso, se descubrió que los dispositivos afectados fueron los de uno de los directores, estos dispositivos son los siguientes:</p> <ul style="list-style-type: none"> • Ordenador portátil Dell XPS con sistema Windows 7 y número de serie 0417852369 El usuario dejó de utilizar el ordenador el 23 debido a que empezó vacaciones. <p>Por eso pedimos que se analicen estos dispositivos en busca de malware, algún acceso remoto, y en búsqueda de información que haya sido sustraída o accedida sin el consentimiento de la empresa. Dependiendo del resultado nos gustaría que se judicializara el proceso.</p>				
<p>Si se produce la aceptación de su caso se le proporcionará un nuevo documento con su presupuesto y la información relativa.</p>				

Anexo 3 Presupuesto



Presupuesto

Menorca, 1 de octubre de 2019

REUNIDOS

D. **Ruben Mesquida Gomila**, mayor de edad y con domicilio en Menorca, con **DNI 417452523Q**, Perito Judicial Informática Forense con N.^º de colegiado **07760**.

D. **Juan García Pérez** mayor de edad y con DNI. **45875365H** en nombre y representación de la empresa **Servicios Integrales Tecnológicos S.A** con **CIF A07818501**

EXPONEN

Que ambas partes de reconocen capacidad suficiente para suscribir el presente contrato.

SERVICIOS SOLICITADOS

El cliente solicita los servicios para que se realice un informe pericial de los siguientes dispositivos que pertenecen a susodicha empresa

Los dispositivos incluidos en el caso son los siguientes:

- Ordenador portátil Dell XPS con sistema Windows 7 y número de serie **0417852369**

Donde se analizarán en búsqueda de malware, algún acceso remoto, y en búsqueda información que haya sido sustraída o accedida sin el consentimiento de la empresa

ACEPTACIÓN DEL CASO

El Perito **Ruben Mesquida Gomila**, acepta el caso que se abrió con código **IB07683811** por parte de la empresa **Servicios Integrales Tecnológicos S.A** con **CIF A07818501**, y este, por parte de satisfacer la correspondiente minuta de honorarios por el trabajo a realizar de análisis forense se determinan los siguientes honorarios descritos a continuación.

HONORARIOS

Los honorarios serán determinados, conforme a los usos y normas de la informática forense, atendiendo al asunto, su complejidad de su desarrollo, esfuerzo profesional, éxito o fracaso de las pretensiones del cliente, incidencias habidas en su tramitación, etc.

El Perito Informático fijará su minuta, atendiendo las circunstancias antes expresadas o cualesquiera otras que considere dignas de ser tenidas en cuenta.

Salidas del despacho, laboratorio, recursos, incidencias, dietas, viajes, etc., serán honorarios con independencia del asunto principal.

METODO DE PAGO

El cliente **Servicios Integrales Tecnológicos S.A** con **CIF A07818501**, realizará el pago en 2 plazos personalmente o de manera telemática la cantidad de **3561,83 euros**, correspondientes al 50% de la cuantía mínima calculada, importe total estimado del peritaje es de **7123,66 euros**

Anexo 4 Cadena de Custodia Imagen Disco

Evidencia



Caso N.º **IB07683811**

Evidencia N.º **02**

Sección A: Evidencia Recogida



Fecha 01/10/2019
14:33

Realizado por Ruben Mesquida Gomila

Dirección Av. Constitución 3, Ciutadella de Menorca

Sección B: Detalles Evidencia

Fecha 01/10/2019
14:33

Localización Ciutadella de Menorca,

Tipo de Dispositivo Portátil

Capacidad 64GB

Marca Dell

Modelo XPS 15 2019

N.º Serie 0417852369

Información Adicional...

No se han detectado arañazos ni desperfectos en el equipo

Imagen tomada

Si

No

Detallar daños, desperfectos o arañazos

Sección C: Detalles Imagen

Fecha 01/10/2019
15:33

Realizada por Ruben Mesquida Gomila

Localización Ciutadella de Menorca

Nombre archivo clonacionwin7.dd

Tamaño Imagen 64

(GB)

MD5 93bbf050c944575865bde97ed815b09a

SHA-1 9b6f2e9e39b125a77d2ec672bbda4cc14411e839

Información Adicional...

Esta segunda evidencia se trata de la imagen del disco duro del equipo.

Este formulario se utiliza para recoger un dispositivo de hardware que contiene datos que pueden ser de interés en un caso. Directrices:

- Asegurarse de que este formulario sólo se refiere a un elemento de prueba y de que se cumplimente uno para cada elemento de prueba.
- Este formulario debe ir acompañado de formularios de Cadena de Custodia que detallan los individuos que han manejado la evidencia.
- En la Sección D se pueden encontrar otras observaciones al dorso: Observaciones
- Es importante que estos formularios se mantengan junto con las pruebas en todo momento.

Anexo 5 Cadena de Custodia Imagen RAM

Evidencia



Caso N.º IB07683811

Evidencia N.º 01

Sección A: Evidencia Recogida

Fecha 01/10/2019 14:33	Realizado por Ruben Mesquida Gomila
---------------------------	-------------------------------------

Dirección Av. Constitución 3, Ciutadella de Menorca

Sección B: Detalles Evidencia

Fecha 01/10/2019
14:33

Localización Ciutadella de Menorca,

Tipo de Dispositivo Portátil Capacidad 64GB

Marca Dell Modelo XPS 15 2019

N.º Serie 0417852369

Información Adicional...

No se han detectado arañazos ni desperfectos en el equipo

Imagen tomada Si No

Detallar daños, desperfectos o arañazos

Sección C: Detalles Imagen

Fecha 01/10/2019 14:33	Realizada por Ruben Mesquida Gomila
---------------------------	-------------------------------------

Localización Ciutadella de Menorca

Nombre archivo win7-ram.aff4 Tamaño Imagen 2.4 (GB)

MD5 3e73b9992aebe3184dc5fc80dd45f34c

SHA-1 3488d8761bc0473e2f77c352f70c32d9b1662b04

Información Adicional...

Esta primera evidencia se trata de la adquisición de la memoria RAM del equipo.

Este formulario se utiliza para recoger un dispositivo de hardware que contiene datos que pueden ser de interés en un caso. Directrices:

- Asegurarse de que este formulario sólo se refiere a un elemento de prueba y de que se cumple uno para cada elemento de prueba.
- Este formulario debe ir acompañado de formularios de Cadena de Custodia que detallan los individuos que han manejado la evidencia.
- En la Sección D se pueden encontrar otras observaciones al dorso: Observaciones
- Es importante que estos formularios se mantengan junto con las pruebas en todo momento.

Anexo 6 Acta Notarial de presencia



ACTA NOTARIAL DE PRESENCIA

En la ciudad de Ciutadella de Menorca, a 1 de octubre del año 2019 siendo las doce horas, YO: PABLO PÉREZ PÉREZ, Notario, constituido en la Avenida Constitución N.º 3 de esta ciudad, a requerimiento del señor RUBEN MESQUIDA GOMILA con JUAN GARCIA PEREZ Gerente de Sitsa SA, a quien juramento de la manera siguiente: ¿Prometéis bajo juramento decir verdad en lo que fuereis preguntado?

CONTESTAN: Sí, bajo juramento prometemos decir verdad en lo que se nos pregunté, por lo que acto seguido les hice saber lo relativo al delito de Perjurio y pena consiguiente, de lo cual me dicen estar perfectamente enterados y seguidamente dicen llamarse Ruben Mesquida Gomila con número de identificación 41745223 y Perito N.º Colegiado 07760, y JUAN GARCIA PEREZ Gerente de Sitsa SA y en representación de esta con número de identificación 45875365H. Con el objeto de asentar la presente acta notarial, para el efecto procedo de la manera siguiente:

PRIMERO: El requirente Ruben Mesquida Gomila en este acto procede a la adquisición de las distintas imágenes de los equipos del señor Juan García Pérez Ordenador portátil Dell XPS con sistema Windows 7 y número de serie 0417852369 y Google Pixel 3 con sistema Android 8.1 con número de serie 369258147, se obtienen las distintas imágenes con las siguientes sumas de verificación:

- Imagen RAM Ordenador portátil: MD5: 4c7964abcef792f0f3c49f96a1b006a SHA1: 3d373b2cf20a54926b68b4902e30b306cf7eb8
- Imagen Disco Ordenador portátil: MD5: 93bbf050c944575865bde97ed815b09a SHA1: 9b6f2e9e39b125a77d2ec672bbda4cc14411e839

SEGUNDO: No habiendo más que hacer constar se finaliza la presente acta, en una hoja de papel bond tamaño oficio, utilizada únicamente de anverso, a la que se le adhiere un timbre notarial del valor 838,67 euros la cual se hace entrega al mismo interesado para los usos legales que le convengan. Leído que le fue lo escrito al requirente, enterado de su contenido, lo ratifica, acepta y firma de conformidad. Doy fe.

Firma: Ruben Mesquida Gomila.

Perito Informático

Firma: Juan García Pérez

Gerente Sitsa S.A

ANTE MÍ: Lic. Pablo Pérez Pérez.

Notario.



Anexo 7 Salida ClamAV malware

```
/media/sf_F_DRIVE/ed01ebfb9e5bbea545af4d01bf5f1071661840480439c6e5bab8e080e41aa.exe: Win.Ransomware.WannaCry-6313787-0 FOUND

----- SCAN SUMMARY -----
Known viruses: 6361556
Engine version: 0.101.4
Scanned directories: 16252
Scanned files: 80216
Infected files: 1
Total errors: 186
Data scanned: 8090.37 MB
Data read: 15970.25 MB (ratio 0.51:1)
Time: 5819.145 sec (96 m 59 s)
```

Anexo 8 Salida análisis Yara Scan

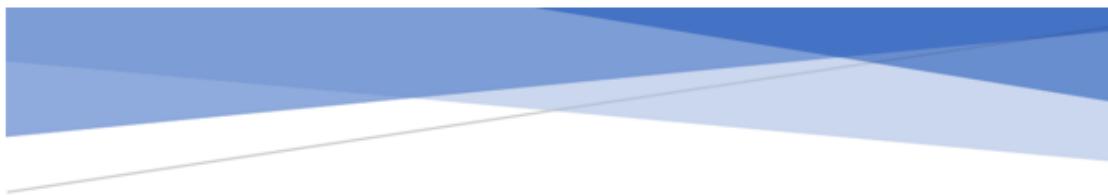
Column1.1	Column1.2
Str_Win32_Winsoc2_Library /media/sf_F_DRIVE	ed01ebfb9e5bbe45a4fd01bf5f1071661804080439c6e5bab8e080e41aa.exe
WannaDecryptor /media/sf_F_DRIVE	ed01ebfb9e5bbe45a4fd01bf5f1071661804080439c6e5bab8e080e41aa.exe
Wanna_Sample_04c32835a5d21bbc7fa5e17076d8ab549 /media/sf_F_DRIVE	ed01ebfb9e5bbe45a4fd01bf5f1071661804080439c6e5bab8e080e41aa.exe
ransom_telefonia /media/sf_F_DRIVE	ed01ebfb9e5bbe45a4fd01bf5f1071661804080439c6e5bab8e080e41aa.exe
WannaCry_Ransomware_Generic /media/sf_F_DRIVE	ed01ebfb9e5bbe45a4fd01bf5f1071661804080439c6e5bab8e080e41aa.exe
WannaCry_Ransomware /media/sf_F_DRIVE	ed01ebfb9e5bbe45a4fd01bf5f1071661804080439c6e5bab8e080e41aa.exe
WannaCry_Ransomware_Dropper /media/sf_F_DRIVE	ed01ebfb9e5bbe45a4fd01bf5f1071661804080439c6e5bab8e080e41aa.exe
wannacry_stc_random /media/sf_F_DRIVE	ed01ebfb9e5bbe45a4fd01bf5f1071661804080439c6e5bab8e080e41aa.exe
Str_Win32_Internet_API /media/sf_F_DRIVE	Program Files/Common Files/System/msadc/msadc.dll
Str_Win32_Http_API /media/sf_F_DRIVE	Program Files/Common Files/System/msadc/msadc.dll
Str_Win32_Wininet_Library /media/sf_F_DRIVE	Program Files/Common Files/system/wab32.dll
Str_Win32_Wininet_Library /media/sf_F_DRIVE	Program Files/Common Files/System/Ole DB/oledb32.dll
GlassesCode /media/sf_F_DRIVE	Program Files/DVD Maker/PipeTran.dll
Glasses /media/sf_F_DRIVE	Program Files/DVD Maker/PipeTran.dll
Str_Win32_Wininet_Library /media/sf_F_DRIVE	Program Files/Internet Explorer/hmmapi.dll
Str_Win32_Wininet_Library /media/sf_F_DRIVE	Program Files/Internet Explorer/ielowutil.exe
Str_Win32_Wininet_Library /media/sf_F_DRIVE	Program Files/Internet Explorer/jsdebuggeride.dll
Str_Win32_Internet_API /media/sf_F_DRIVE	Program Files/Internet Explorer/jsdebuggeride.dll
Str_Win32_Http_API /media/sf_F_DRIVE	Program Files/Internet Explorer/smapi.dll
Str_Win32_Wininet_Library /media/sf_F_DRIVE	Program Files/Internet Explorer/ledtool.dll
Str_Win32_Http_API /media/sf_F_DRIVE	Program Files/Internet Explorer/ledtool.dll
GlassesCode /media/sf_F_DRIVE	Program Files/DVD Maker/OmdProject.dll
Glasses /media/sf_F_DRIVE	Program Files/DVD Maker/OmdProject.dll
PM_Zig_with_js /media/sf_F_DRIVE	Program Files/LibreOffice/program/classes/ScriptProviderForJavaScript.jar
Str_Win32_Winsoc2_Library /media/sf_F_DRIVE	Program Files/LibreOffice/program/pgpmpp.dll
Str_Win32_Winsoc2_Library /media/sf_F_DRIVE	Program Files/LibreOffice/program/lcurl.dll
GlassesCode /media/sf_F_DRIVE	Program Files/LibreOffice/program/hwplo.dll
Glasses /media/sf_F_DRIVE	Program Files/LibreOffice/program/hwplo.dll
Str_Win32_Winsoc2_Library /media/sf_F_DRIVE	Program Files/LibreOffice/program/neon.dll
Str_Win32_Winsoc2_Library /media/sf_F_DRIVE	Program Files/LibreOffice/program/spr4.dll
Str_Win32_Winsoc2_Library /media/sf_F_DRIVE	Program Files/LibreOffice/program/mysqld.dll
Str_Win32_Winsoc2_Library /media/sf_F_DRIVE	Program Files/LibreOffice/program/lbxm12.dll
Str_Win32_Winsoc2_Library /media/sf_F_DRIVE	Program Files/LibreOffice/program/lfbclient.dll
Str_Win32_Winsoc2_Library /media/sf_F_DRIVE	Program Files/LibreOffice/program/libeasy32.dll
Str_Win32_Winsoc2_Library /media/sf_F_DRIVE	Program Files/LibreOffice/program/postgresql-sdbc-impl0.dll
Str_Win32_Winsoc2_Library /media/sf_F_DRIVE	Program Files/LibreOffice/program/python-core-3.5.7/lib/select.pyd

Anexo 9 Timeline archivos

Anexo 10 Aplicación Sitsa.apk

Aplicación archivo Sitsa.apk

Anexo 11 Informe Pericial



I

INFORME PERICIAL SITSA

CASO N.º IB07683811

Ruben Mesquida Gomila
N.º COL 07760

A

APK: Un APK es el formato de archivo utilizado para distribuir aplicaciones para el sistema operativo Android.

APT: Es un tipo de ataque o amenaza de forma persistente dirigida a atacar la seguridad una organización específica.

D

Dropper: Es un tipo de malware diseñado para ejecutarse en un equipo y una vez ejecutado automáticamente descargara el código o archivo malicioso.

E

Evidencia: es el tipo de prueba que se obtiene al realizar un análisis forense y que sostiene una hipótesis o verifica un hecho.

F

Fork: un fork es la creación de un nuevo proyecto que parte de la base de un proyecto ya existente.

Framework: es un conjunto estructurado de software, que facilita la realización de una tarea.

I

Imagen Forense: Es una copia exacta realizada de un disco o memoria, que permite ser analizada sin necesidad de modificar el dispositivo original del cual se ha extraído dicha imagen.

M

Malware: es un software malicioso que puede afectar a distintos tipos de dispositivo. El objetivo de este es el control remoto, robo de información, secuestro del equipo, etc.

MD5: es un algoritmo criptográfico de 128bits que principalmente se utiliza para comprobar la integridad de un archivo.

Metasploit: es un framework orientado a la seguridad informática utilizado para desarrollar, lanzar exploits y otras funciones que facilitan el trabajo de un pentester o analista.

Meterpreter: es un payload de Metasploit que se ejecuta después de haber explotado una vulnerabilidad.

O

Open source: es un tipo de software al cual se tiene acceso al código fuente para poder ser estudiado, mejorado o modificado.

P

PasteBin: es un servicio web que permite a usuarios subir trozos de código, textos, para sean públicos, estos se pueden subir de forma anónima o no

Perito: es una persona experta en un campo determinado capaz de analizar de forma objetiva un suceso , dispositivo, etc.

R

Ransomware: es un tipo de malware cuyo objetivo es el secuestro del equipo encriptando los archivos, a cambio para la recuperación de Iso archivos suelen pedir un rescate.

Rekall: es un fork de Volatility y es una herramienta utilizada para la adquisición , el análisis de memoria y extracción de posibles evidencias.

S

SHA1: es un algoritmo criptográfico que principalmente se utiliza para comprobar la integridad de un archivo. Se diferencia con MD5 en que SHA1 es mas seguro que MD5 y utilizada 160 bits en vez de 128.

Shell: es un interprete de ordenes que sirve para acceder a los programas, servicios ya archivos en un sistema.

T

Terminal: es un interprete de ordenes que sirve para acceder a los programas, servicios ya archivos en un sistema.

V

VBS: es un formato de archivo utilizado por el lenguaje de VBScript diseñado por Microsoft.

W

Wannacry: es un tipo de ransomware que tuvo gran repercusiones en 2017 afectando grandes empresas en el mundo.

12. BIBLIOGRAFÍA Y REFERENCIAS

- Statista, J. Clement, J.C (2019, 09 julio). Amount of monetary damage caused by reported cyber crime to the IC3 from 2001 to 2018 (in million U.S. dollars). Recuperado de <https://www.statista.com/statistics/267132/total-damage-caused-by-cyber-crime-in-the-us/>
- AV-Test, (2019, 24 septiembre) Total Malware. Recuperado de <https://www.av-test.org/en/statistics/malware/>
- RootedCon, José Miguel Holguín Aparicio y Marc Salinas Fernández, J.M.H. y M.S.F. (2019, 29 marzo). Taller de análisis de memoria RAM en sistemas Windows. Recuperado de <https://www.rootedcon.com/archive/rooted2019#session-153>
- European Union Agency for Network and Information Security, ENISA (2016, diciembre). Forensic Analysis Local Incident Response Handbook, Document for teachers. Recuperado de https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/2016-resources/exe1_forensic_analysis_i-handbook
- Javier Rubio Alamillo, J.R.A. (2018, 25 febrero). Diferencia entre un acta notarial de presencia y un peritaje informático. Recuperado de <https://peritoinformaticocolegiado.es/blog/diferencia-entre-un-acta-notarial-de-presencia-y-un-peritaje-informatico/>
- SANS Institute, Chad Tilbury, C.T. (s.f.). Memory Forensics Cheat Sheet 2.0 . Recuperado de <https://digital-forensics.sans.org/media/volatility-memory-forensics-cheat-sheet.pdf>
- Andrea Fortuna, A.F. (2017, 20 octubre). Windows evento logs in forensic analysis. Recuperado de <https://www.andreafortuna.org/2017/10/20/windows-event-logs-in-forensic-analysis/>
- SANS Institute, Kiel Wadner, K.W. (2014, 10 octubre). An analysis of Meterpreter during Post-Exploitation. Recuperado de <https://www.sans.org/reading-room/whitepapers/forensics/analysis-meterpreter-post-exploitation-35537>
- SANS Institute, Kristinn Gudjonsson, K.G. (2010, 29 junio). Mastering the super timeline with log2timeline. Recuperado de <https://www.sans.org/reading-room/whitepapers/logging/mastering-super-timeline-log2timeline-33438>
- BlackBag Training Team (2016, 09 junio). Windows Memory forensics 2. Recuperado de <https://www.blackbagtech.com/blog/windows-memory-forensics-part-2/>

- Forward Defense, Steve Anson, S.A. (2017, 16 noviembre). Windows memory analysis with Volatility. Recuperado de <https://www.forwarddefense.com/pdfs/Memory-Analysis-with-Volatility.pdf>
- Javier Maques, J.M. (2012, 01 septiembre) Peritaje judicial tecnológico: aspectos técnicos, legales y casos de estudio. Recuperado de https://javiermarques.es/wp-content/uploads/2016/11/Memoria_Marques_FranciscoJavier.pdf
- Forensic Focus, Derrick J. Farmer, D.J.F. (s.f.). A forensic analysis of the Windows registry. Recuperado de <https://www.forensicfocus.com/a-forensic-analysis-of-the-windows-registry>
- Magnet Forensics, Jaime McQuaid, J.M. (2014, 06 agosto). Forensic Analysis of Prefetch files in Windows. Recuperado de <https://www.magnetforensics.com/blog/forensic-analysis-of-prefetch-files-in-windows/>
- Magnet Forensics, Jaime McQuaid, J.M. (2014, 07 agosto). Forensic Analysis of Prefetch files in Windows. Recuperado de <https://www.magnetforensics.com/blog/forensic-analysis-of-windows-shellbags/>
- SANS Institute, Vincent Lo, V.L. (2014, 19 noviembre). Windows ShellBag forensics in depth. Recuperado de <https://www.sans.org/reading-room/whitepapers/forensics/windows-shellbag-forensics-in-depth-34545>
- The Sleuth Kit, (s.f.) Orphan Files. Recuperado de https://wiki.sleuthkit.org/index.php?title=Orphan_Files
- Infosec Institute, (s.f.) Computer Forensics: Web, email and messaging forensics. Recuperado de <https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/application-forensics/web-email-and-messaging-forensics/>