



Análisis Forense Informático

TRABAJO FINAL DEL MÓDULO

18/05/2024

PEDRO MANUEL GARCÍA ÀLVAREZ | int.marisma@gmail.com

1.- Introducción	3
2.- Trabajo fin de Módulo Informática Forense.....	3
3.- Historia del caso Juan Pérez Caja rural	4
4.- Método de extracción de los archivos y ficheros proporcionados	5
4.1.- Proceso de Extracción de Memoria de una Máquina Virtual	5
4.1.1.- Paso 1: Asegúrate de que la Máquina Virtual está Corriendo	5
4.1.2.- Paso 2: Confirmar que la Máquina Virtual está Corriendo	5
4.1.3.- Paso 3: Volcar la Memoria de la Máquina Virtual	6
4.1.4.- Paso 4: Verificar el Volcado de Memoria	6
4.1.5.- Paso 5: Apagar la Máquina Virtual.....	7
4.1.6.- Paso 5.- Alternativa: Apagado Suave	7
4.2.- Proceso para Extraer la Imagen del Disco Duro	8
5.- Cuestionario de pregunta para resolver.	8
6.- Cuestionario de pregunta para resolver de Conrando.	9

1.- Introducción

En el marco de la presente actividad colaborativa, mi compañero Conrado y yo hemos participado en un intercambio de cuestionarios diseñados para explorar y resolver un caso particular. Esta metodología nos ha permitido abordar el caso desde diversas perspectivas y enriquecer nuestra comprensión mediante el intercambio de preguntas y respuestas.

El propósito de este documento es presentar los cuestionarios intercambiados y las respuestas proporcionadas por ambas partes. A través de este análisis, buscamos ofrecer una visión detallada del proceso de investigación y análisis que hemos llevado a cabo en relación con el caso en cuestión.

Sin más preámbulos, procedemos a compartir los cuestionarios intercambiados y las respuestas correspondientes, con el objetivo de profundizar en nuestra comprensión del caso y destacar los enfoques diversos que hemos empleado para su resolución.

2.- Trabajo fin de Módulo Informática Forense.

Vamos a realizar un pequeño reto parecido a los que hemos visto en clase. La idea es que cada uno de vosotros prepare el volcado de memoria y de disco de una máquina con unas características concretas a la que previamente se le habrán realizado una serie de acciones tales como borrado de ficheros, cambio de extensiones, encriptación y ocultación.

Las características de la máquina serán como mínimo:

- Sistema Operativo: Windows XP Home (ó similar).
- 2 Gb de Disco.
- 64 Mb de memoria RAM.

Posteriormente la información de la máquina debe ser analizada con Volatility y Autopsy.

Se debe entregar:

- Pequeño texto describiendo la situación en la que se ha encontrado la máquina y las técnicas usadas para la extracción de las imágenes. Una página como máximo.
- Imagen de disco.
- Imagen de memoria.
- Cuestionario con preguntas a resolver.

Finalmente, intercambiaremos los retos y cada alumno deberá resolver el reto propuesto por otro compañero.

3.- Historia del caso Juan Pérez Caja rural

La mañana del martes, mientras realizábamos una rutina de monitoreo de seguridad en el sistema de Caja Rural, detectamos actividades sospechosas en la estación de trabajo de un empleado reciente, Juan Pérez, que dejó la compañía hace aproximadamente dos meses. Juan era un empleado de confianza que trabajaba en el departamento de tecnología de la información de nuestro banco.

Tras una investigación inicial, descubrimos que Juan había estado accediendo de manera no autorizada a bases de datos sensibles de clientes durante las últimas semanas antes de su partida. Nuestro equipo de seguridad cibernética descubrió que, utilizando sus credenciales de administrador anteriores, Juan había descargado ilegalmente información confidencial de cuentas bancarias, incluyendo nombres de usuarios, contraseñas y datos personales de clientes.

Parece que Juan había ideado un plan para vender estos datos al mejor postor en el mercado negro. Para cubrir sus huellas, Juan había implementado varias técnicas de ocultamiento y encriptación en su estación de trabajo, una máquina VirtualBox con sistema operativo Windows XP SP3.

El equipo de seguridad actuó rápidamente para asegurar la estación de trabajo de Juan antes de que pudiera borrar o destruir evidencia incriminatoria. Ahora, nos encontramos frente a la tarea de extraer y analizar la información almacenada en su portátil para encontrar pruebas sólidas que respalden nuestras sospechas.

4.- Método de extracción de los archivos y ficheros proporcionados

En este ejercicio se entrega los ficheros siguientes:

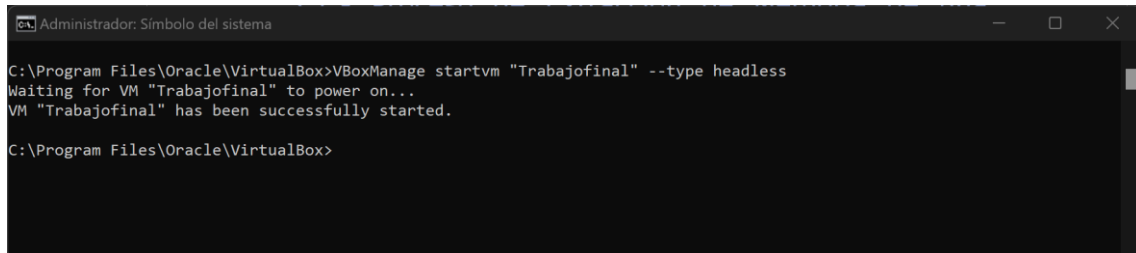
- trabajofinal.mem
- trabajofinal.raw

4.1.- Proceso de Extracción de Memoria de una Máquina Virtual

La extracción de memoria se ha realizado utilizando los siguientes comandos en modo administrador de cmd con VirtualBox. A continuación, se presentan los pasos detallados para asegurarse de que la máquina virtual esté en ejecución y para volcar su memoria correctamente:

4.1.1.- Paso 1: Asegúrate de que la Máquina Virtual está Corriendo

Primero, necesitas asegurarte de que tu máquina virtual esté en ejecución. Puedes iniciar la máquina virtual desde la línea de comandos con el siguiente comando:



```
Administrador: Símbolo del sistema
C:\Program Files\Oracle\VirtualBox>VBoxManage startvm "Trabajofinal" --type headless
Waiting for VM "Trabajofinal" to power on...
VM "Trabajofinal" has been successfully started.
C:\Program Files\Oracle\VirtualBox>
```

VBoxManage startvm "Trabajofinal" --type headless

Este comando iniciará la máquina virtual en modo headless, es decir, sin una interfaz gráfica de usuario.

4.1.2.- Paso 2: Confirmar que la Máquina Virtual está Corriendo

Verifica que la máquina virtual esté en ejecución usando el siguiente comando:

```
Administrador: Símbolo del sistema
C:\Program Files\Oracle\VirtualBox>VBoxManage list runningvms
"Trabajofinal" {4a0c9899-89e7-4f0a-8e27-c91f7798b068}
C:\Program Files\Oracle\VirtualBox>
```

VBoxManage list runningvms

Este comando te mostrará una lista de todas las máquinas virtuales que actualmente están en ejecución. Asegúrate de que "Trabajofinal" aparezca en la lista.

4.1.3.- Paso 3: Volcar la Memoria de la Máquina Virtual

Una vez que te asegures de que la máquina virtual esté corriendo, puedes volcar la memoria con el siguiente comando:

```
Administrador: Símbolo del sistema
C:\Program Files\Oracle\VirtualBox>VBoxManage debugvm "Trabajofinal" dumpvmcore --filename "C:\trabajofinal.mem"
C:\Program Files\Oracle\VirtualBox>
```

VBoxManage debugvm "Trabajofinal" dumpvmcore --filename "C:\trabajofinal.mem"

4.1.4.- Paso 4: Verificar el Volcado de Memoria

```
Administrador: Símbolo del sistema
C:\>dir
El volumen de la unidad C es OS
El número de serie del volumen es: A010-5262

Directorio de C:\
14/02/2024 01:07 <DIR> $WINDOWS.BT
10/05/2024 00:30 <DIR> bajadadevideos
07/03/2024 22:53 <DIR> descargarweb
14/02/2024 01:20 <DIR> ESD
15/11/2023 15:11 <DIR> eSupport
01/04/2024 23:48 <DIR> pedro
16/05/2024 21:53 <DIR> Program Files
31/03/2024 12:27 <DIR> Program Files (x86)
18/05/2024 18:32 87.946.936 trabajofinal.mem
09/04/2024 21:12 <DIR> ud 2 suricata
09/04/2024 21:15 9.370.644 ud 2 suricata.rar
29/12/2023 21:50 <DIR> Users
12/02/2024 22:40 <DIR> win-mb5100-1_1-n_mcd
14/05/2024 22:54 <DIR> windows
12/04/2024 01:29 <DIR> xampp
2 archivos 97.317.580 bytes
13 dirs 10.772.103.168 bytes libres
```

Después de ejecutar el comando, verifica que el archivo "C:\trabajofinal.mem" ha sido creado y tiene un tamaño que corresponde a la cantidad de RAM asignada a la máquina virtual.

Siguiendo estos pasos, puedes asegurar una correcta extracción de la memoria de tu máquina virtual.

4.1.5.- Paso 5: Apagar la Máquina Virtual

Una vez que hayas terminado de trabajar con la máquina virtual, puedes apagarla con el siguiente comando:

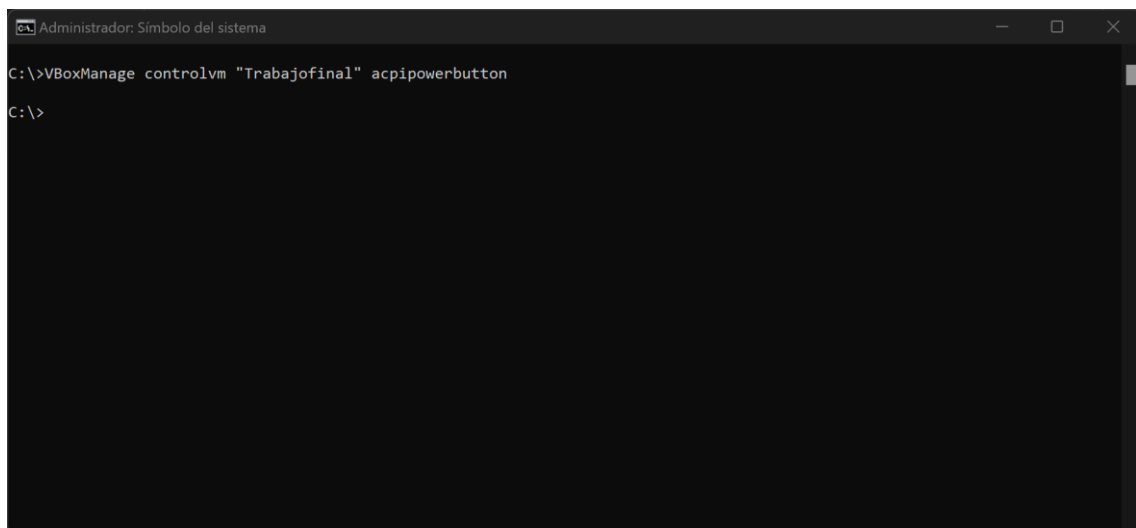
```
VBoxManage controlvm "Trabajofinal" poweroff
```

Este comando apagará la máquina virtual "Trabajofinal" de forma inmediata.

4.1.6.- Paso 5.- Alternativa: Apagado Suave

Si prefieres un apagado suave, que permite que el sistema operativo invitado cierre los programas de manera ordenada, puedes usar:

```
VBoxManage controlvm "Trabajofinal" acpipowerbutton
```



```
Administrador: Símbolo del sistema
C:\>VBoxManage controlvm "Trabajofinal" acpipowerbutton
C:\>
```

Este comando simula presionar el botón de encendido/apagado en una computadora física, enviando una señal ACPI al sistema operativo invitado para que realice un apagado controlado.

4.2.- Proceso para Extraer la Imagen del Disco Duro

```
Administrador: Símbolo del sistema
C:\>VBoxManage clonemedium disk "C:\Users\internet\Desktop\Instituto\A01.- AFI\Trabajo final\trabajofinal\trabajofinal.vdi"
"C:\Trabajofinal.raw" --format RAW
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
Clone medium created in format 'RAW'. UUID: 830e1165-04c1-4c3f-ae0c-f9d061ced568
C:\>
```

Para extraer la imagen del disco duro, utiliza el siguiente comando:

```
VBoxManage clonemedium disk
"C:\Users\internet\Desktop\Instituto\A01.- AFI\Trabajo
final\trabajofinal\Trabajofinal.vdi" "C:\Trabajofinal.raw" --format RAW
```

```
Administrador: Símbolo del sistema
C:\>dir
El volumen de la unidad C es OS
El número de serie del volumen es: A010-5262

Directorio de C:\
14/02/2024 01:07 <DIR> $WINDOWS~BT
10/05/2024 00:30 <DIR> bajadadevideos
07/03/2024 22:53 <DIR> descargarweb
14/02/2024 01:20 <DIR> ESD
15/11/2023 15:11 <DIR> eSupport
01/04/2024 23:48 <DIR> pedro
16/05/2024 21:53 <DIR> Program Files
31/03/2024 12:27 <DIR> Program Files (x86)
18/05/2024 18:32 87.946.936 trabajofinal.mem
18/05/2024 20:25 936.378.368 Trabajofinal.raw
09/04/2024 21:12 <DIR> ud 2 suricata
09/04/2024 21:15 9.370.644 ud 2 suricata.rar
29/12/2023 21:50 <DIR> Users
12/02/2024 22:40 <DIR> win-mb5100-1_1-n_mcd
14/05/2024 22:54 <DIR> Windows
12/04/2024 01:29 <DIR> xampp
3 archivos 1.033.695.948 bytes
13 dirs 7.919.333.376 bytes libres
C:\>
```

5.- Cuestionario de pregunta para resolver.

Cuestionario a resolver del caso de Juan Pérez ex empleado Caja Rural.

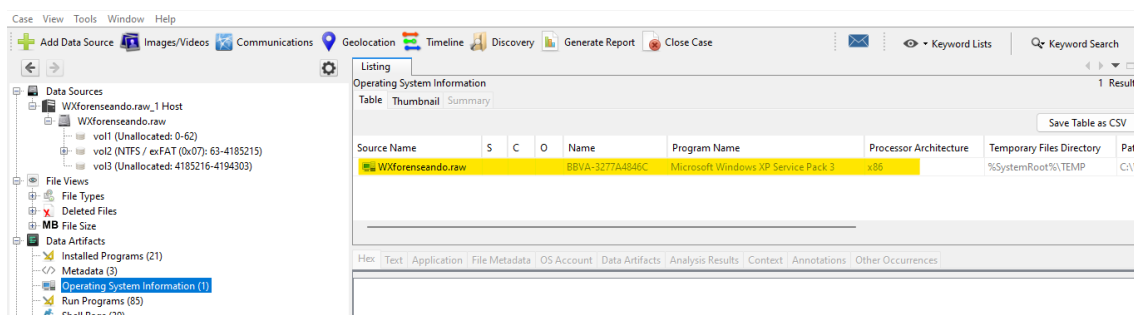
1.- ¿Cuál es el software específico que Juan Pérez empleó para cifrar el archivo de cuentas bancarias?

2.- ¿En qué archivo ha guardado Juan Díaz la contraseña para acceder al archivo que contiene las cuentas bancarias?

3. ¿Cuándo se creó el archivo oculto de la contraseña?
- 4.- ¿Qué procesos estaban activos en el sistema en el momento de la captura de la memoria?
5. ¿Dónde está almacenado el archivo encriptado base de datos de clientes?
6. ¿Cuándo se creó el archivo encriptado que contiene las bases de datos?
- 7.- ¿Cuál es el contenido del archivo de la base de datos?
- 8.- ¿Cuál es el nombre del dispositivo?
9. ¿Qué usuarios estaban autenticados en el sistema al momento de la captura de la memoria?
- 10.- ¿Cuál es el perfil del sistema operativo utilizado en el volcado de memoria 'trabajofinal.mem'?

6.- Cuestionario de pregunta para resolver de Conrando.

¿Cómo se llama el equipo intervenido? **BBVA-3277A4846C**

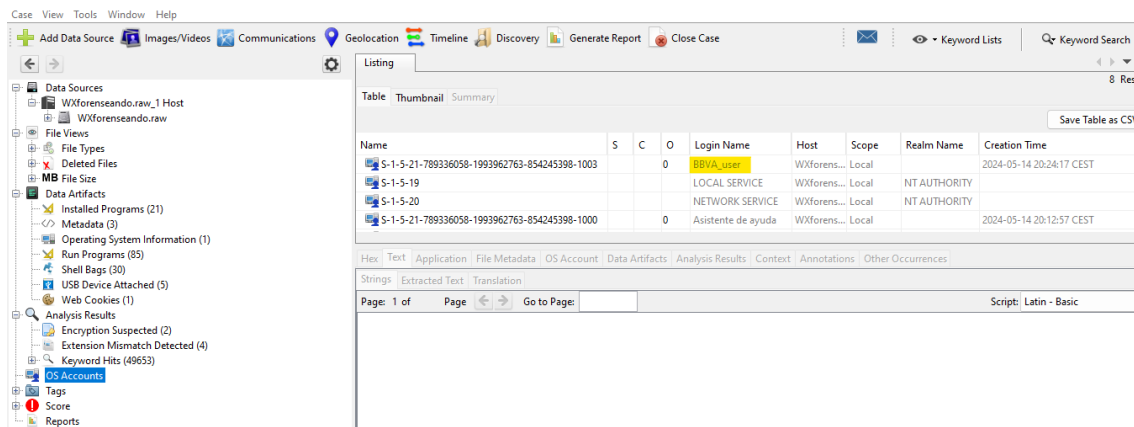


```
Administrador: Símbolo del sistema

C:\Users\internet\Desktop\Instituto\A01.- AFI\Trabajo final\conrado>volatility -f wxforenseandomemoria.raw --profile=WinXPSP3x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                PID  PPID  Thds  Hnds  Sess  Wow64  Start                Exit
-----
0x80e32d68 System              4    0     56   242   -----  0    0 2024-05-14 19:47:06 UTC+0000
0x80ce9da0 smss.exe           376  4     3    19   -----  0    0 2024-05-14 19:47:07 UTC+0000
0x80cd21d0 csrss.exe          532  376    11   335   0        0    0 2024-05-14 19:47:07 UTC+0000
0x80cacda0 winlogon.exe      624  376    21   529   0        0    0 2024-05-14 19:47:07 UTC+0000
0x80e426a8 services.exe    668  624    17   330   0        0    0 2024-05-14 19:47:07 UTC+0000
0x80d4dc08 lsass.exe         680  624    20   332   0        0    0 2024-05-14 19:47:07 UTC+0000
0x80cb4c20 VBoxService.exe 836  668     9   121   0        0    0 2024-05-14 19:47:08 UTC+0000
0x80cd1da0 svchost.exe    884  668    19   200   0        0    0 2024-05-14 19:47:08 UTC+0000
0x80cddda0 svchost.exe    972  668     9   221   0        0    0 2024-05-14 19:47:08 UTC+0000
0xffa7c2d8 svchost.exe   1064  668    54  1093   0        0    0 2024-05-14 19:47:08 UTC+0000
0xffa748d8 svchost.exe   1108  668     4    63   -----  0    0 2024-05-14 19:47:08 UTC+0000
0xffa6c020 svchost.exe   1140  668    14   197   0        0    0 2024-05-14 19:47:08 UTC+0000
0xffa95f8 spoolsv.exe    1320  668    11   107   0        0    0 2024-05-14 19:47:09 UTC+0000
0xffa004d0 VBoxTray.exe  1816 1636    11   116   0        0    0 2024-05-14 19:47:18 UTC+0000
0xff9fb20 ctfmon.exe       1824 1636     1    70   0        0    0 2024-05-14 19:47:18 UTC+0000
0xff99c290 alg.exe        1436  668     6   105   0        0    0 2024-05-14 19:47:30 UTC+0000
0xff991da0 wscntfy.exe   1460 1064     1    37   0        0    0 2024-05-14 19:47:30 UTC+0000
0xffa3e1b0 explorer.exe   1184  624    15   497   0        0    0 2024-05-14 19:49:58 UTC+0000
0x80d91da0 DumpIt.exe      196  1184     1    25   0        0    0 2024-05-14 21:26:38 UTC+0000

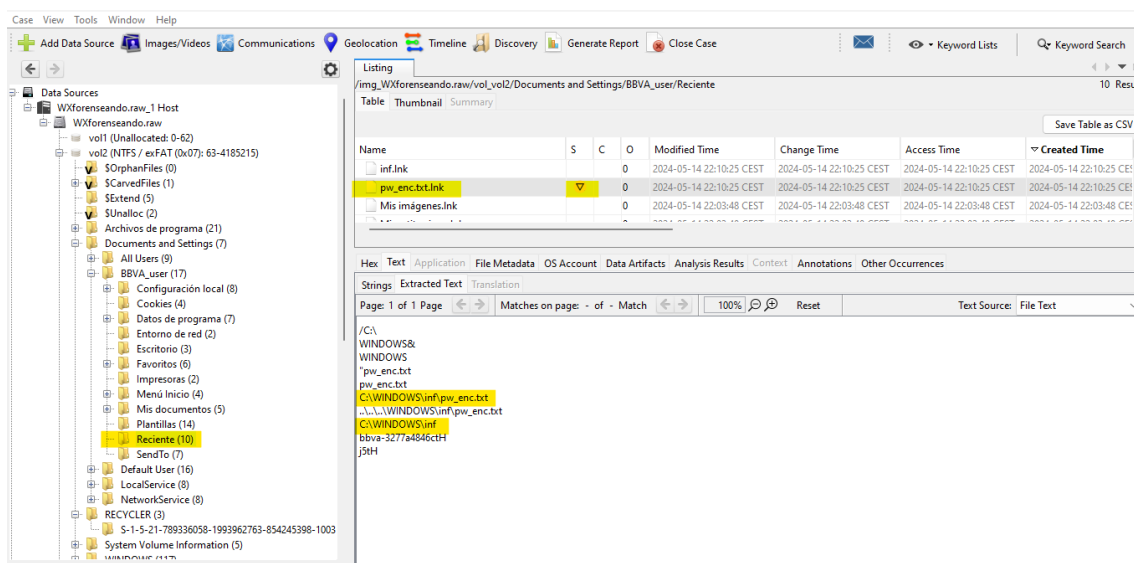
C:\Users\internet\Desktop\Instituto\A01.- AFI\Trabajo final\conrado>
```

¿Cuál era el usuario de inicio de sesión? **bbva_user**



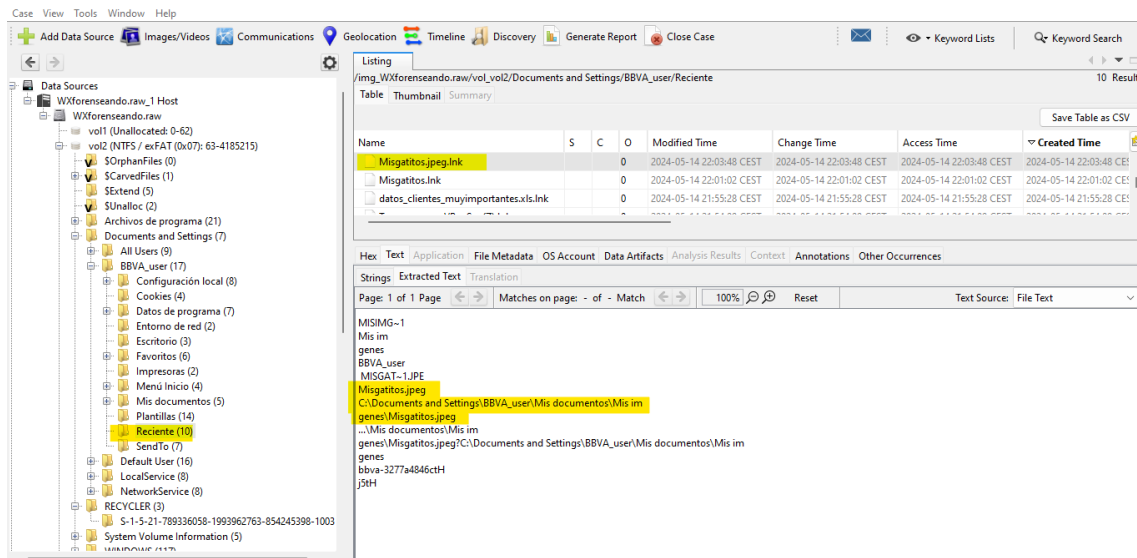
Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-21-789336058-1993962763-854245398-1003			0	BBVA_user	WXforens...	Local		2024-05-14 20:24:17 CEST
S-1-5-19				LOCAL SERVICE	WXforens...	Local	NT AUTHORITY	
S-1-5-20				NETWORK SERVICE	WXforens...	Local	NT AUTHORITY	
S-1-5-21-789336058-1993962763-854245398-1000			0	Asistente de ayuda	WXforens...	Local		2024-05-14 20:12:57 CEST

¿Has encontrado algún/algunos ficheros sospechosos en el equipo?
Sí, Misgatitos.jpeg y pw_enc.txt



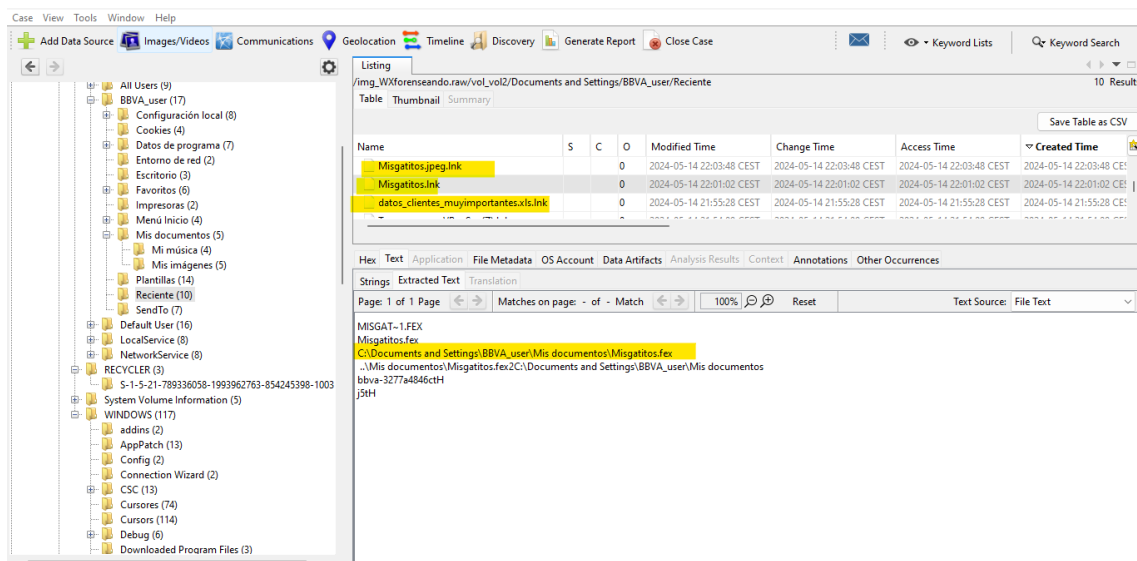
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
inf.lnk			0	2024-05-14 22:10:25 CEST	2024-05-14 22:10:25 CEST	2024-05-14 22:10:25 CEST	2024-05-14 22:10:25 CEST
pw_enc.txt			0	2024-05-14 22:10:25 CEST	2024-05-14 22:10:25 CEST	2024-05-14 22:10:25 CEST	2024-05-14 22:10:25 CEST
Mis imágenes.lnk			0	2024-05-14 22:03:48 CEST	2024-05-14 22:03:48 CEST	2024-05-14 22:03:48 CEST	2024-05-14 22:03:48 CEST

Strings: /C:/WINDOWS/inf/pw_enc.txt, C:\WINDOWS\inf\pw_enc.txt, \.\.\WINDOWS\inf\pw_enc.txt, C:\WINDOWS\inf\bbva-3277a4846cctH\jsh



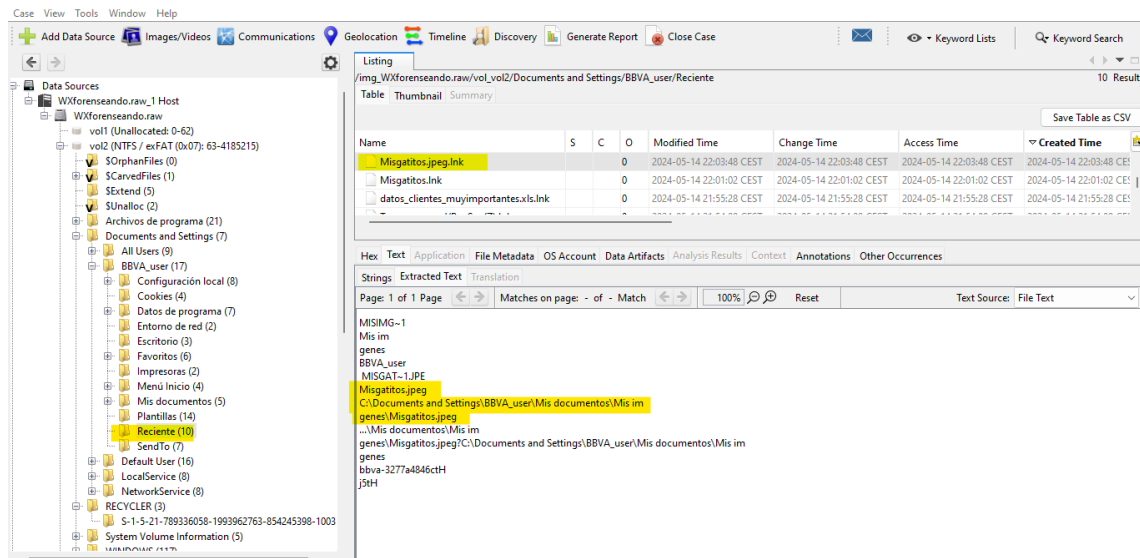
¿En qué basas tus sospechas? Misgatitos.jpeg, tiene extensión de imagen, pero no se puede visualizar y pw_enc.txt tiene información en su interior extraña.

¿Se ha utilizado alguna artimaña de ocultación en el disco duro? Sí, cambió de nombre encriptado a Misgatitos.jpeg.

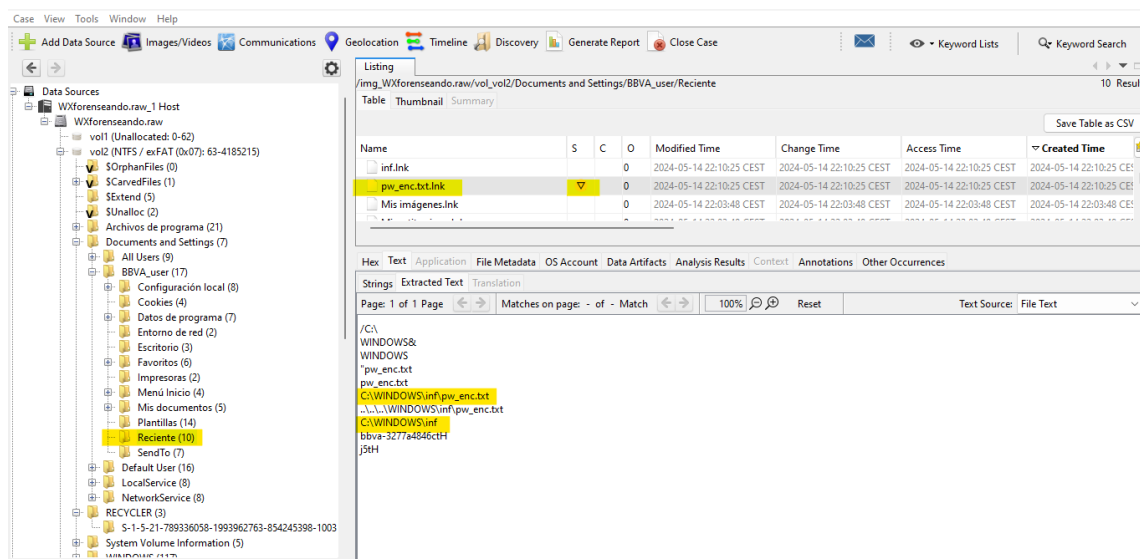


¿Dónde se encuentra el fichero o los ficheros sospechosos?

- Misgatitos.jpeg en C:/Documents and Settings\BBVA_user\Mis documentos\Mis imágenes

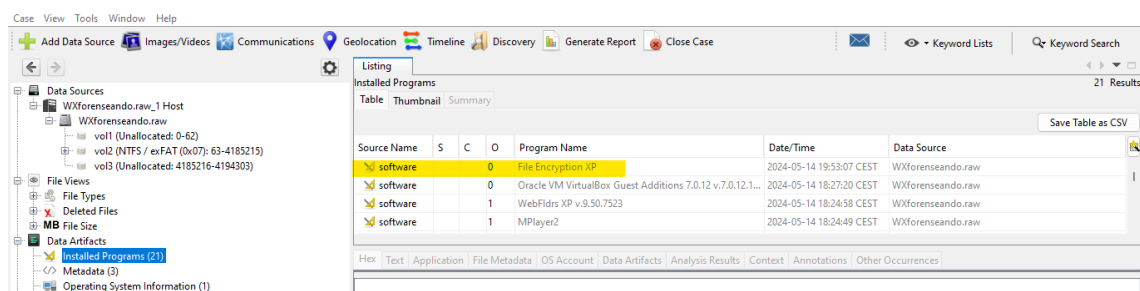


- pw_enc.txt en c:\WINDOWS\inf

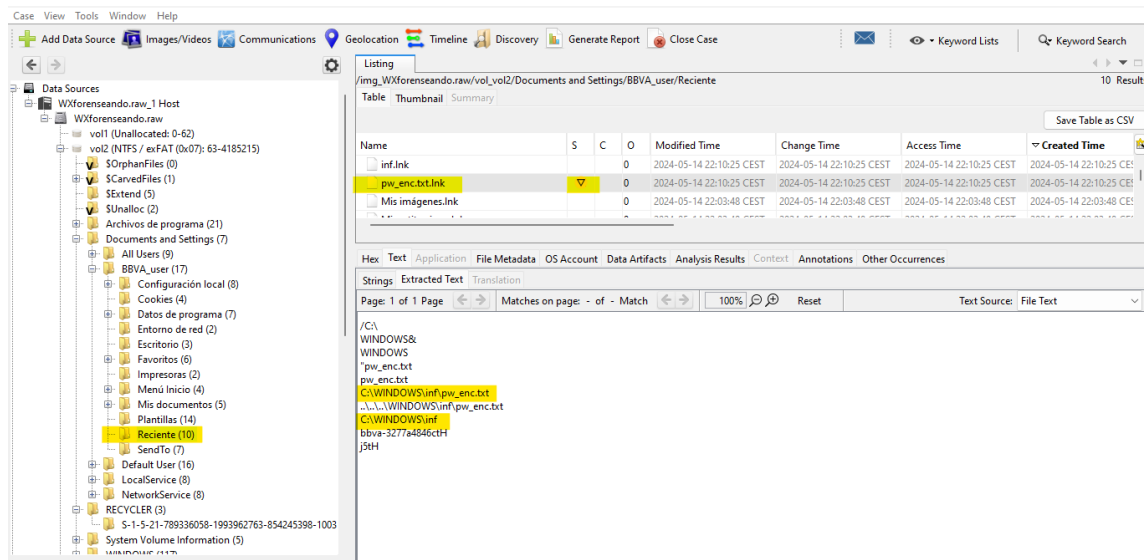


¿Has detectado si hay algún software de encriptación? **Sí**

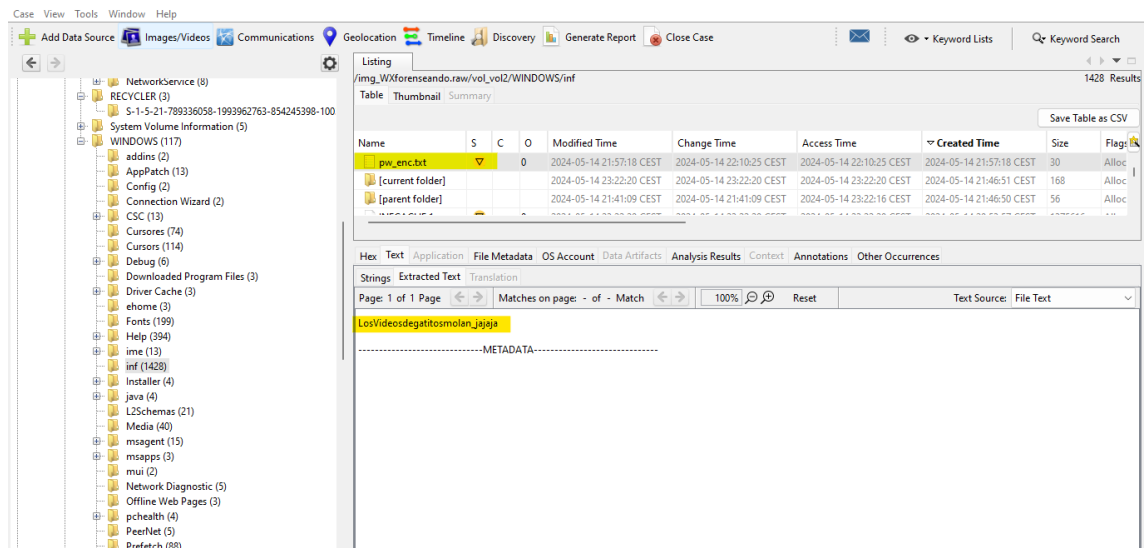
¿Sabrías identificar cuál? **File Encryption XP**



¿Has localizado la clave de descryptado? **Sí**



¿Dónde se encontraba la clave de descryptado? En un fichero de texto escondido llamado pw_enc.txt



¿Cuál era la clave de descifrado? LosVideosdegatitosmolan_jajaja

Finalmente ¿Qué contiene el fichero encriptado? Un fichero de Excel con el listado de clientes del banco, sus credenciales y número de cuenta.

datos_clientes_muyimportantes.xls [Modo de compatibilidad] - Excel

Archivo Inicio Insertar Diseño de página Fórmulas Datos Revisar Vista ¿Qué desea hacer?

Portapapeles Fuente Alineación Número Estilos

Calibri 11 A⁺ A⁻ N K S Fuente Alineación Número Estilos

A1 Nombre

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Nombre	Apellido	DNI	IBAN	Usuario	Contraseña								
2	Gracia	Yuste	62860711	ES1835955	molinerar	Xt8!l+Ko!^								
3	Julio	Solsona	97259946	ES6171592	nestor96	KS(%3IrcwK								
4	Sebastián	Mármol	26556960	ES7476802	emma90	B*39XYzF4								
5	Amancio	Niño	77303298	ES5672427	telmo80	017lFID3@H								
6	Silvia	Casals	47972839	ES5230830	severorod	^5L6p+JAcv								
7	Antonio	Calzada	47899398	ES2536030	pinillabali	HZ95Nfr5D@								
8	Jose Anto	Barragán	61292507	ES5540135	ymoliner	_&F1WQ\$X2o								
9	Pascual	Miguel	97354586	ES0929786	carlotaagu	_c%vwJhP14								
10	Bonifacio	Vendrell	68529196	ES0404197	scarpio	T2Re9fwW*g								
11	Clímaco	Minguez	67919216	ES6957624	sserra	F1^9!Twv^x								
12	Sosimo	Marqués	37103608	ES2461628	joaquinaes	j4\$JAdyN)9								
13	Herminia	Bueno	29379437	ES8331502	jorge89	!8PHL9p^lU								
14	Leonor	Benavent	37269860	ES9288690	wmanso	\$RWnFz9FA1								

Índice Alfabético

A

ACPI.....	7
actividad.....	3
actividades.....	4
anteriores.....	4
apagarla.....	7
Autopsy.....	3

B

bancarias.....	4, 8
bases.....	4, 9
BBVA.....	9, 11

C

cantidad.....	7
características.....	3
cibernética.....	4
comandos.....	5
comprensión.....	3
Conrado.....	3
Conrado.....	9
Corriendo.....	5
cuentas.....	4, 8
cuestión.....	3
cuestionarios.....	3

D

departamento.....	4
documento.....	3
Documents.....	11

E

ejecución.....	5, 6
ejercicio.....	5
encriptación.....	3, 4, 12
Encription.....	12
enfoques.....	3
estación.....	4
evidencia.....	4
Excel.....	13
extensiones.....	3
extracción.....	4, 5, 7

F

física.....	7
-------------	---

G

gráfica.....	5
--------------	---

H

Historia.....	4
huellas.....	4

I

imágenes.....	4, 11
incriminatoria.....	4
información.....	3, 4, 11
Informática.....	3
inicio.....	10
inmediata.....	7
intercambio.....	3
interfaz.....	5
investigación.....	3, 4

L

lista.....	6
------------	---

M

máquina.....	3, 4, 5, 6, 7
máquinas.....	6
martes.....	4
Módulo.....	3

N

nombres.....	4
--------------	---

O

ocultación.....	3, 11
ocultamiento.....	4

P

página.....	4
postor.....	4
preámbulos	3
preguntas	3, 4
propuesto.....	4
Puedes.....	5

R

RAM	3, 7
RAW	8
relación	3
resolución.....	3
respuestas.....	3
rutina.....	4

S

seguridad	4
sesión	10
situación.....	4
sospechosas	4

sospechosos	10, 11
-------------------	--------

T

técnicas	4
Trabajofinal	5, 6, 7

U

usuarios.....	4, 9
---------------	------

V

VBoxManage	5, 6, 7
VirtualBox	4, 5
visión.....	3
visto	3
Volatility.....	3

W

Windows	3, 4
---------------	------