ANEXO A

ANEXO A

PRÁCTICA 1. Análisis del sistema de un sospechoso de Ciber-acoso

Hasta el momento en todo este trabajo se ha dicho que el fin de la informática forense es conocer mediante un estudio exhaustivo la historia de un equipo informático que se encuentre o se sospeche que se encuentra comprometido dentro de un delito. El objetivo del análisis será encontrar las evidencias necesarias que certifiquen, que realmente existió un delito.

En este sentido a continuación presentamos un caso práctico, en donde se aplicará las técnicas forenses necesarias para poder llegar a esclarecer los hechos y atrapar al delincuente.

Esta práctica tratará directamente el tema del Ciberacoso o Cyberbullying, que es el uso de la información electrónica y medios de comunicación tales como correo electrónico, redes sociales, blogs, mensajería instantánea, mensajes de texto, celulares, y websites difamatorios, diseñados para acosar a una persona o a un grupo de personas. Este acoso puede constituir un delito penal, el ciberacoso puede también constituir o incluir amenazas, connotaciones sexuales, etiquetas despectivas, etc.

Comencemos con la descripción del escenario y la implementación de los entornos de análisis.

1.- Escenario

Gracias a una denuncia puesta en la Policía, específicamente en la unidad de delitos informáticos, se pretende llevar a cabo un análisis forense a un sistema propiedad de un sospechoso que tiene contacto con la victima de ciberacoso. Este análisis será realizado bajo la sospecha de

que se está realizando actos delictivos y judicializables, además se cree que el sospechoso distribuye contenido pedófilo a través de internet.

2.- Objetivos

El objetivo es realizar un análisis forense al equipo informático de la persona sospechosa, para ello se entrega a la unidad de delitos informáticos una imagen o snapshotdel sistema objetivo. Esta imagen podrá ser restaurada con el software de máquinas virtuales VMWare Server o VMWare Player, ambas aplicaciones de uso gratuito.

3.- Finalidad

La finalidad del análisis será llegar a determinar los siguientes puntos:

1. Antecedentes del Sistema/Escenario.
2. Recolección de datos.
3. Descripción de la evidencia.
4. Entorno del análisis/Descripción de las herramientas.
5. Análisis de la evidencia/Información del sistema analizado /Aplicaciones /Servicios.
6. Metodología.
7. Descripción de los hallazgos.
8. Huellas del comportamiento y de las actividades del sospechoso.
9. Cronología de las actividades del sospechoso.
10. Posibles víctimas del sospechoso.
11. Rastros del sospechoso.
12. Conclusiones.
13. Referencias.

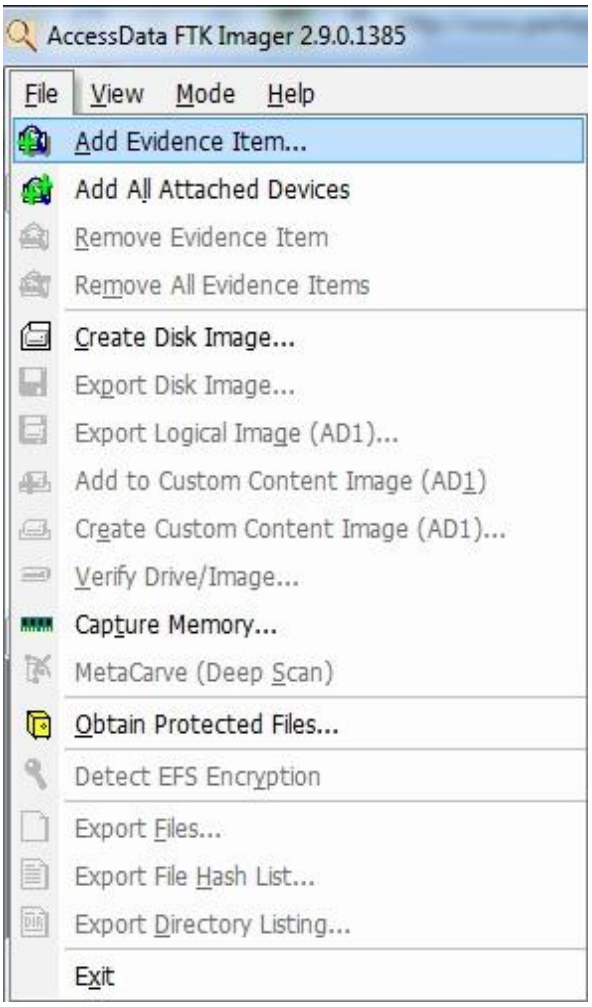
4.- Integridad de la evidencia

Una tarea indispensable en el análisis forense digital es el firmado criptográfico, que se tiene que hacer a cada una de las evidencias que se

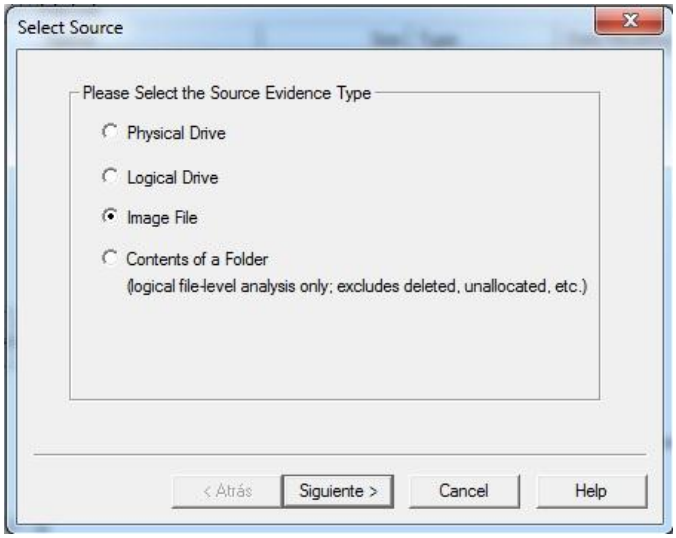
encuentren involucradas en el proceso, para ello se va a utilizar la herramienta FTKImager de Acces Data.

Se debe tener claro antes de iniciar que las funciones hash nos permiten identificar si un archivo ha sido modificado pero no nos dice en cuanto, por eso es necesario ir llenando la bitácora para saber quién ha tenido acceso a las evidencias.

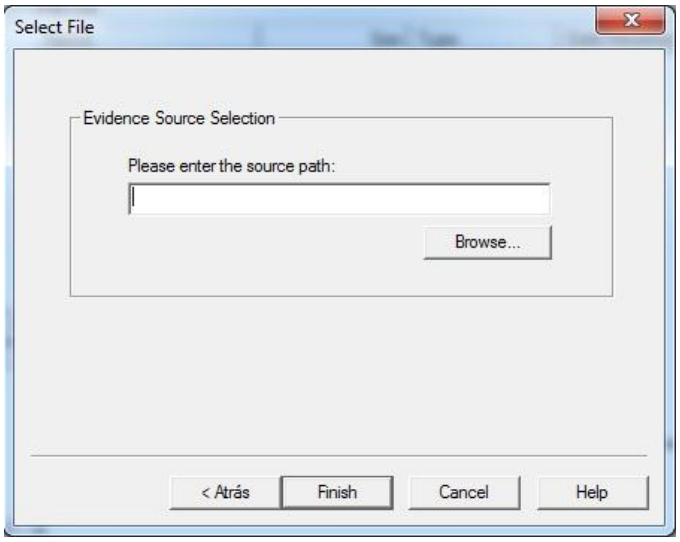
Se ejecuta la herramienta, seleccionamos File, AddEvidenceItem



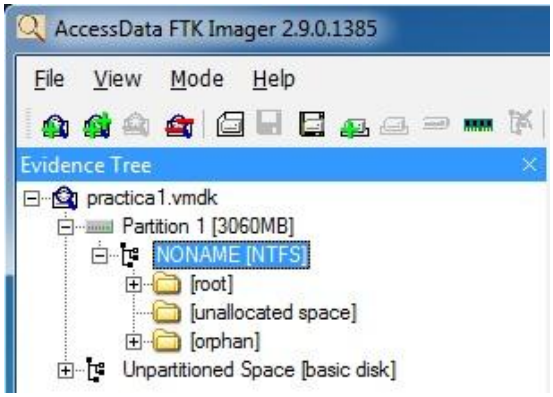
Luego seleccionamos el recurso a adjuntar como evidencia. Para nuestro caso Image File.



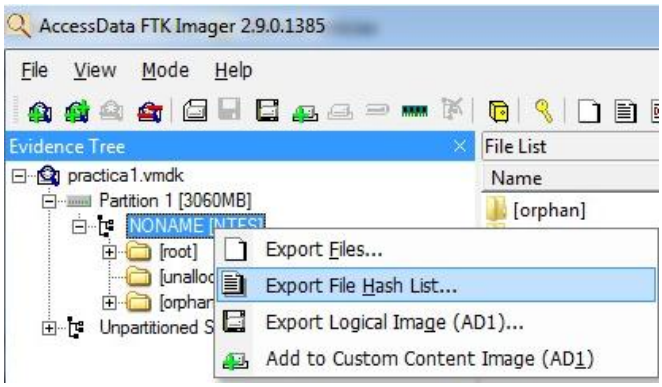
Se selecciona la ruta donde esta almacenada la imagen del sistema



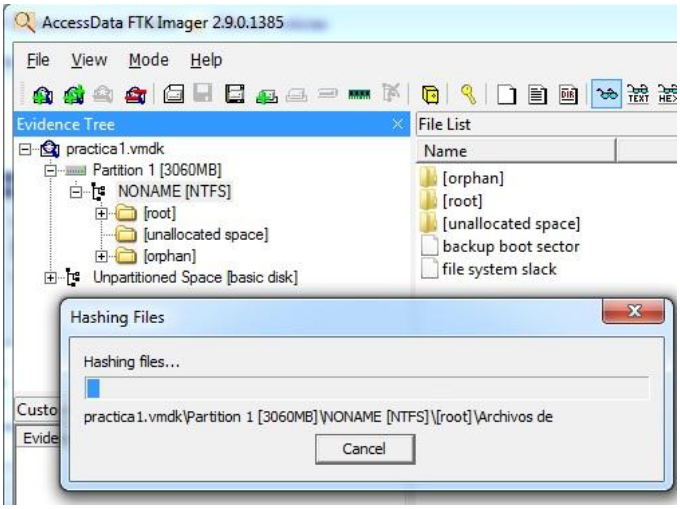
Debería verse de la siguiente forma



Ahora hacemos clic derecho sobre la evidencia y seleccionamos la opción Export File Hash List.



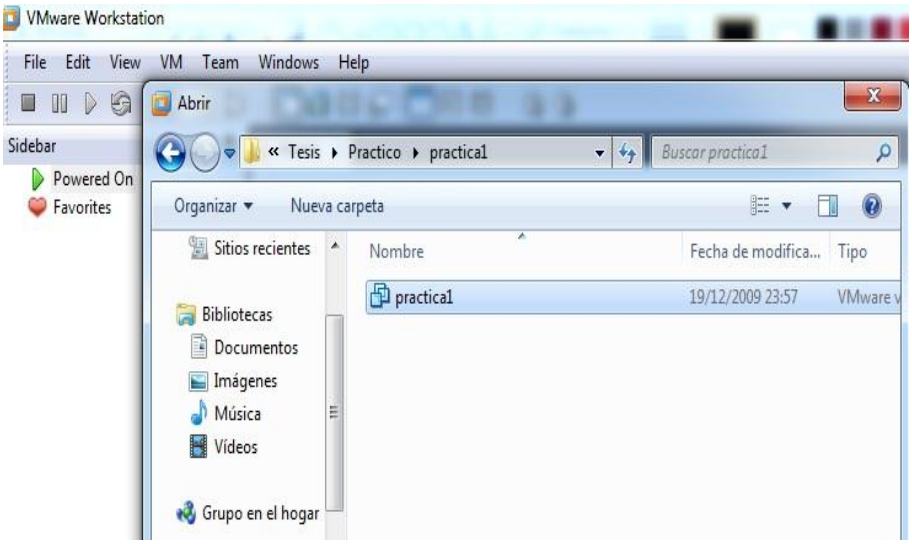
Procedimiento de generación de firmas criptográficas en ejecución



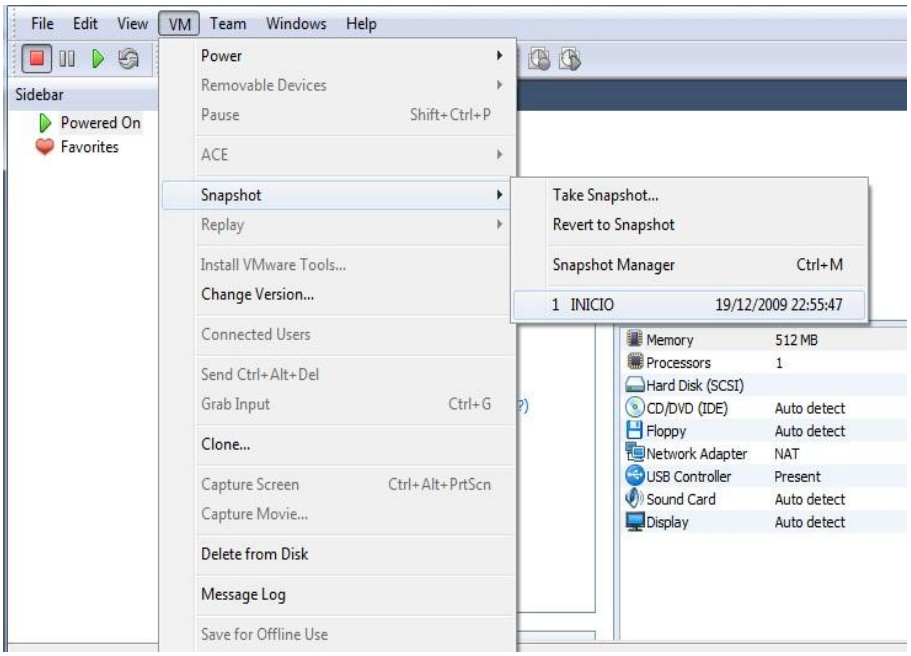
Finalmente tendremos un archivo CSV con la tabla de valores HASH para cada archivo. Esta firma está representada con los algoritmos MD5 y SHA1.

MD5	SHA1	FileNames
0c4708b0072054dd16531d1851ad0227	b2c43c79787926865ec5f0f36eb39d6a3f1b379d	practica1.vmdk\Partition 1 [3060MB]\NONAME [NTFS]\[root]\$I30
ad617ac3906958de35eacc3d90d31043	b49d7f48300701235231f6b6fc3d92a5630f9e70	practica1.vmdk\Partition 1 [3060MB]\NONAME [NTFS]\[root]\$Att
d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfef95601890afd80709	practica1.vmdk\Partition 1 [3060MB]\NONAME [NTFS]\[root]\$Bad
d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfef95601890afd80709	practica1.vmdk\Partition 1 [3060MB]\NONAME [NTFS]\[root]\$Bad
f4f8c73e639788d581f8c721e09ea092	d6358782e4d191ee165a19b2adc916a762d45558	practica1.vmdk\Partition 1 [3060MB]\NONAME [NTFS]\[root]\$Bit
6949975bae00d97ec8c65b1d5d9258bd	aed2fcd61ac47a715a015711197ec8f921b53fa6	practica1.vmdk\Partition 1 [3060MB]\NONAME [NTFS]\[root]\$Boo
5011746ae35d3a12b01fd61e72b109cb	a54828365fe73ace15d0f8e87b338f828efb93fc	practica1.vmdk\Partition 1 [3060MB]\NONAME [NTFS]\[root]\$Ext
420445dd74310d5967dbde6a36df05b8	d9d4fb71ee2f076782d3b8d3e7cfabd82812e5c0	practica1.vmdk\Partition 1 [3060MB]\NONAME [NTFS]\[root]\$Ext
6c768abe7517044afcd418e6c8a18a33	eef231ee80882665317ecbd819703425ca03d3ca	practica1.vmdk\Partition 1 [3060MB]\NONAME [NTFS]\[root]\$Ext
51f03672d2152c11f0ff3f399e272922	abb5dcb132358e0df5add93887379562af7e44a9	practica1.vmdk\Partition 1 [3060MB]\NONAME [NTFS]\[root]\$Ext
e3987337ab34ebbb2dd182c69a0d5d45	1114e6c02bd7314704e1cc6c5bf04e2c996685cc	practica1.vmdk\Partition 1 [3060MB]\NONAME [NTFS]\[root]\$Log
97e63078ef702e386b0a6e19121695c1	978db2cb8dc460162378fa61b70bed73944aed23	practica1.vmdk\Partition 1 [3060MB]\NONAME [NTFS]\[root]\$MF

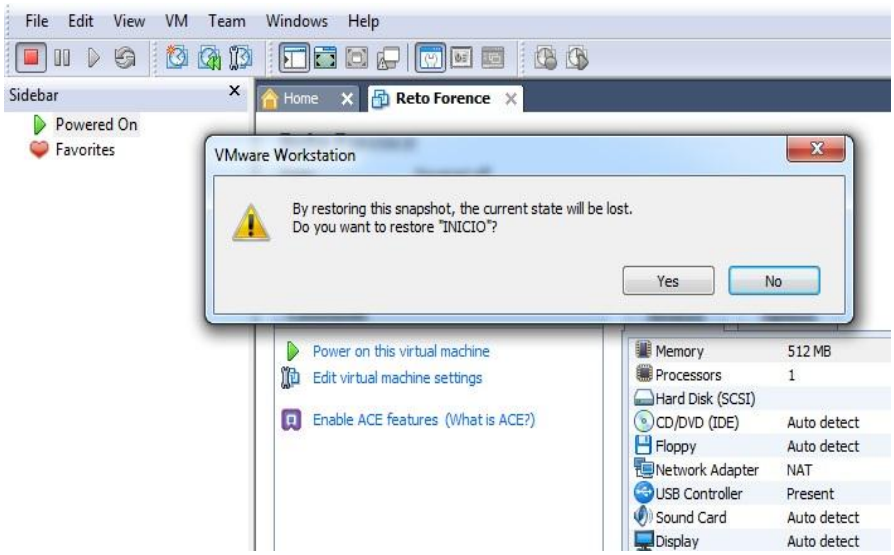
Una vez que se tenga listo el archivo de firmas criptográficas se procede a montar la imagen del sistema que fue entregada, en la máquina virtual, en este caso en concreto se usará VMWare Workstation, solo hace falta abrir el archivo con extensión vmx.



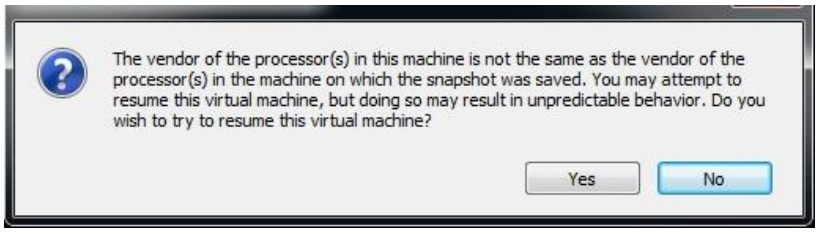
Luego desde el menú VM / Snapshot se restaura la instantánea denominada INICIO, se hará de esta forma porque permitirá simular el momento en que se llega a la escena, en donde se tendrá que recolectar todos los datos posibles del sistema.

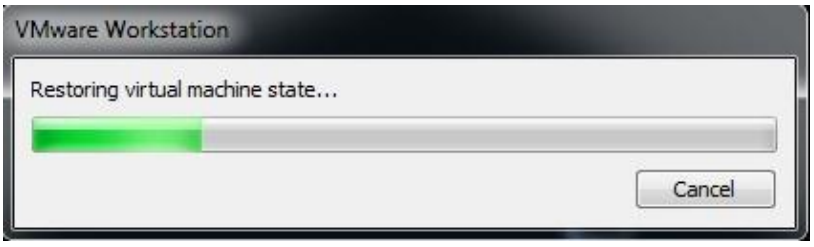


Saldrá un mensaje de advertencia sobre la restauración de la instantánea, en este caso interesa restaurarlo desde el momento en que se dieron los hechos.



Es muy probable que salga un mensaje de advertencia por el tipo de procesador que se usó para sacar la máquina virtual y el que tiene nuestra máquina actual, en este caso le decimos que si restaure.



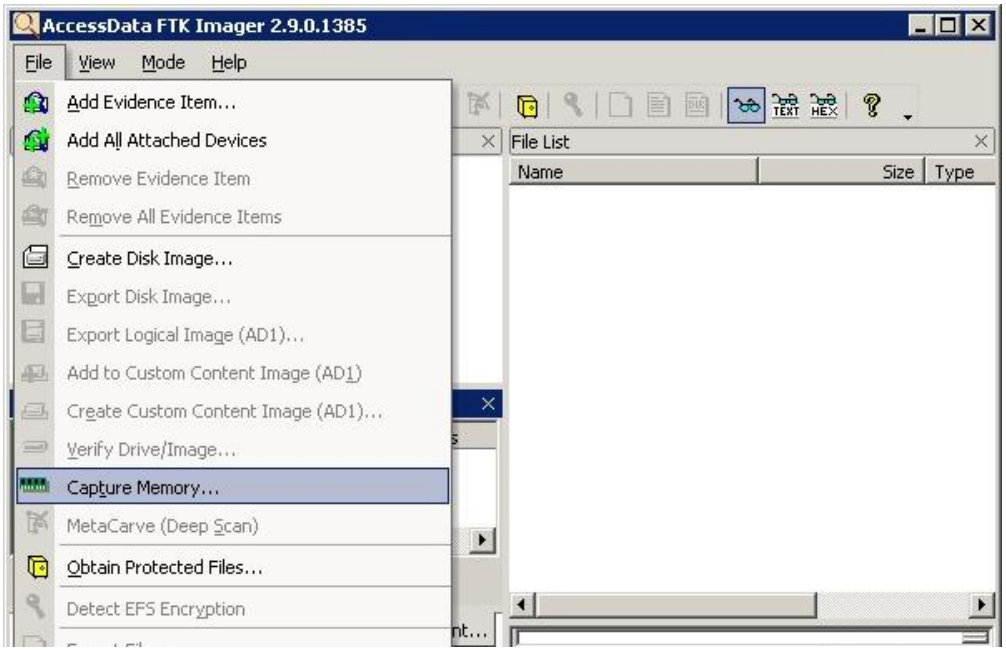


Con esto ya se tendrá implementado el entorno del sistema, el cual será objeto de estudio forense en los siguientes pasos.

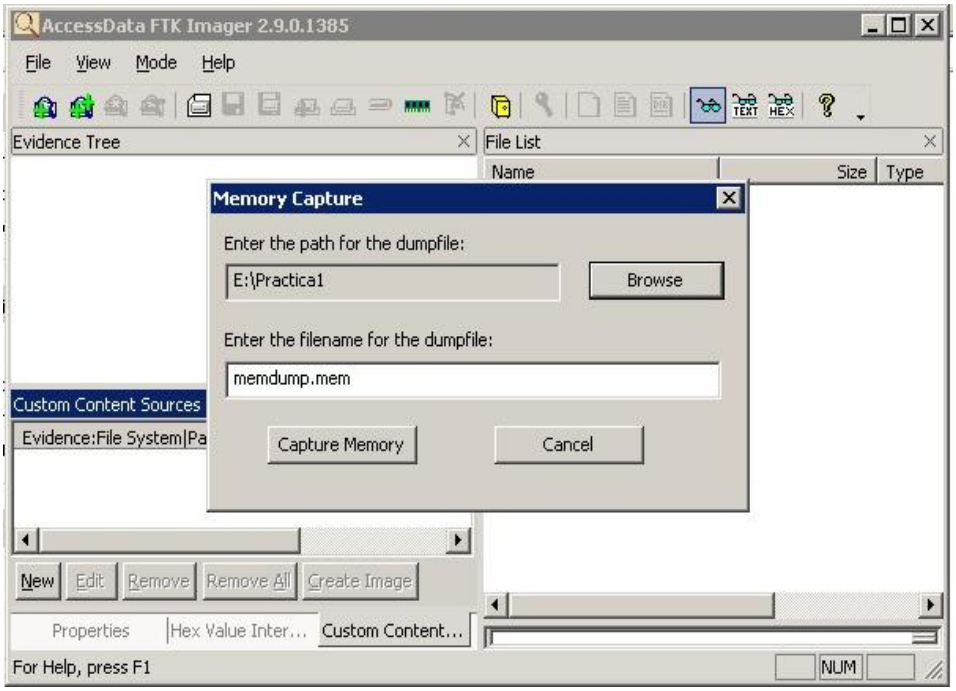
Como ya tenemos el sistema listo lo que tenemos que hacer primero es preservar los datos más volátiles, en este caso se hará un volcado de memoria, con el objetivo de recolectar información volátil que se encuentre alojada en la memoria, lo cual permitirá obtener datos importantes y que son altamente volátiles si no se realiza el volcado de la memoria antes de apagar o reiniciar el equipo en investigación.

Se conectará un dispositivo USB, el cual contiene la herramienta FTK Imager que permitirá realizar el volcado de memoria.

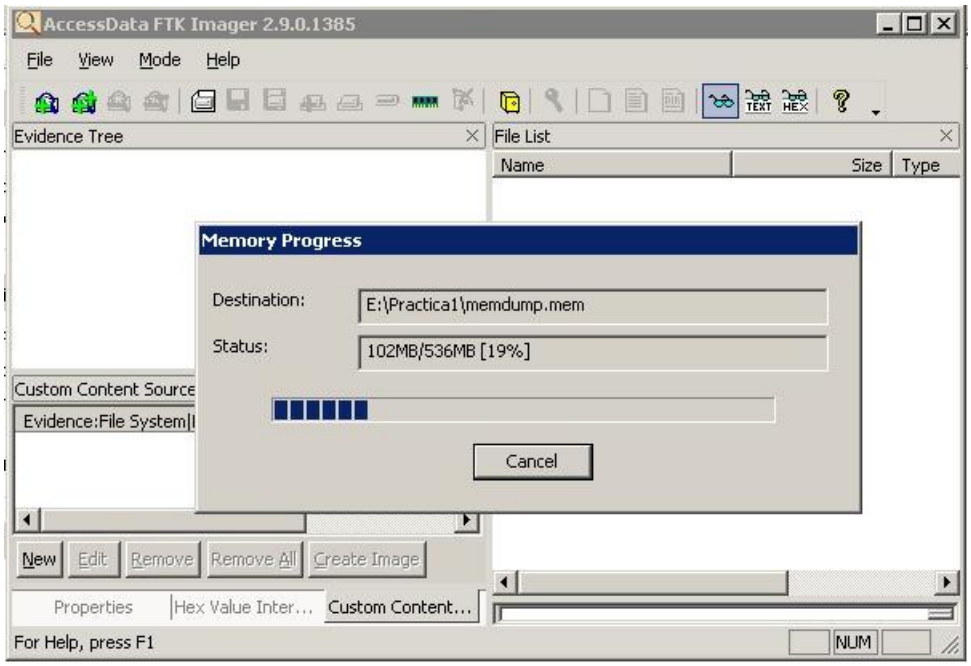
Se ejecuta el programa FTK Imager para empezar con el volcado de memoria.



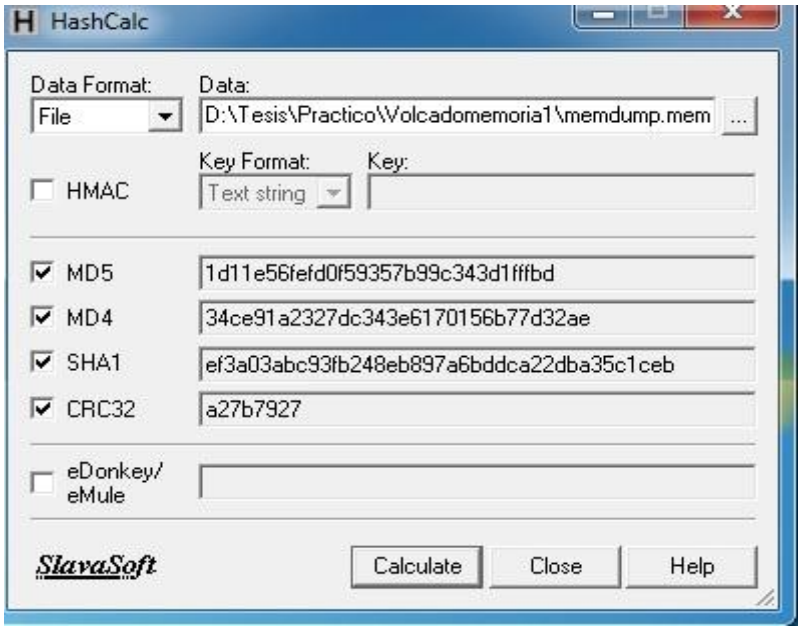
Luego de escoger la opción de captura de memoria, hay que especificar el lugar donde se quiere guardar dicha captura de memoria.



Proceso de volcado de memoria en ejecución.



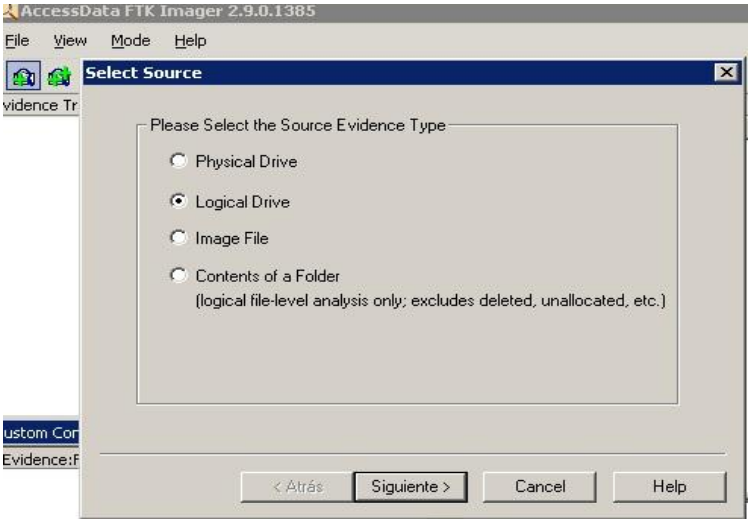
Cuando se termine con el volcado o extracción de información de la memoria, se saca la unidad de memoria USB y en otro equipo que no sea la máquina virtual se procede a generar las firmas digitales del archivo capturado.



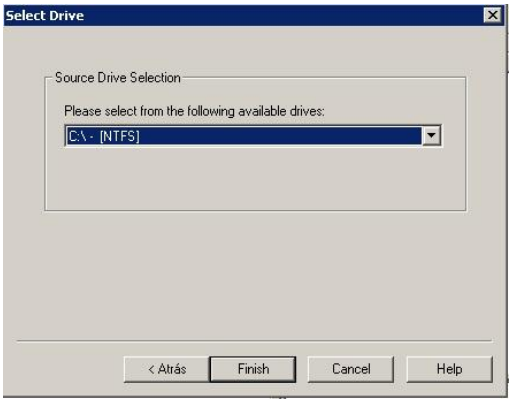
Ahora el siguiente paso es sacar varias copias completas del sistema, con el fin de preservar la evidencia, para esto se utiliza la misma

herramienta que se utilizó para realizar el volcado de memoria, FTK Imager.

En este caso se hará una copia de Drive Lógico.

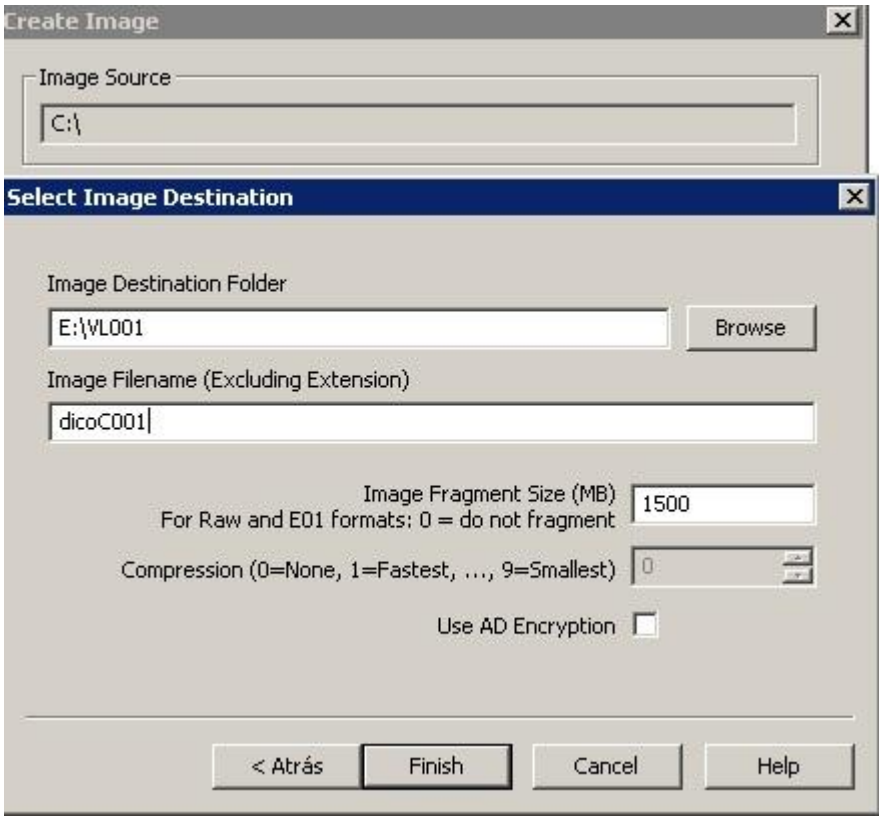


Se escoge el drive fuente

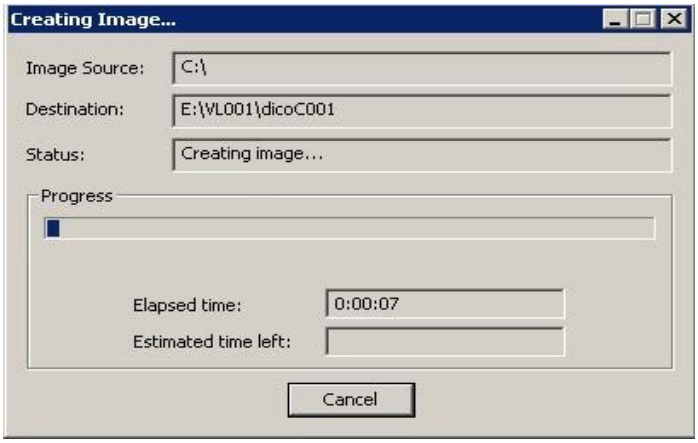


Se exporta la imagen a la memoria USB que se había montado en un paso previo.

Tipo de imagen a la que se desea exportar, en este caso se escogió Raw (dd), que lo que me hace es sacar un backup de la partición del disco seleccionado, se ingresa la información referente al caso y el código de la evidencia.



Creando la imagen



Cuando termina sale la verificación automática de la integridad de los datos copiados.

Drive/Image Verify Results

General	
Name	dsicoC001.001
Sector count	6268864
MD5 Hash	
Computed hash	b64ed31f7afa0d1209ebfe9d671ef6dd
Report Hash	b64ed31f7afa0d1209ebfe9d671ef6dd
Verify result	Match
SHA1 Hash	
Computed hash	2e04ef6981b774604295f4dc6aaae738bdb13465
Report Hash	2e04ef6981b774604295f4dc6aaae738bdb13465
Verify result	Match
Bad Sector List	
Bad sector(s)	No bad sectors found

Si se quiere hacer un copiado de disco físico se hace exactamente igual, solo se modifica la elección en la primera pantalla, de preferencia se debe hacer los dos tipos de copiado, el físico y el lógico.

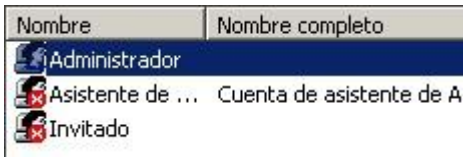
Identificación de la evidencia

Las características del sistema operativo son:

Tipo	Valor
Nombre	Microsoft Windows XP
Edición	Profesional
Fecha de instalación	2009-12-15
Producto ID	55274-640-0263172-23550
Propietario	Scarface
Buildnumber	2600
Service Pack	Service Pack 3

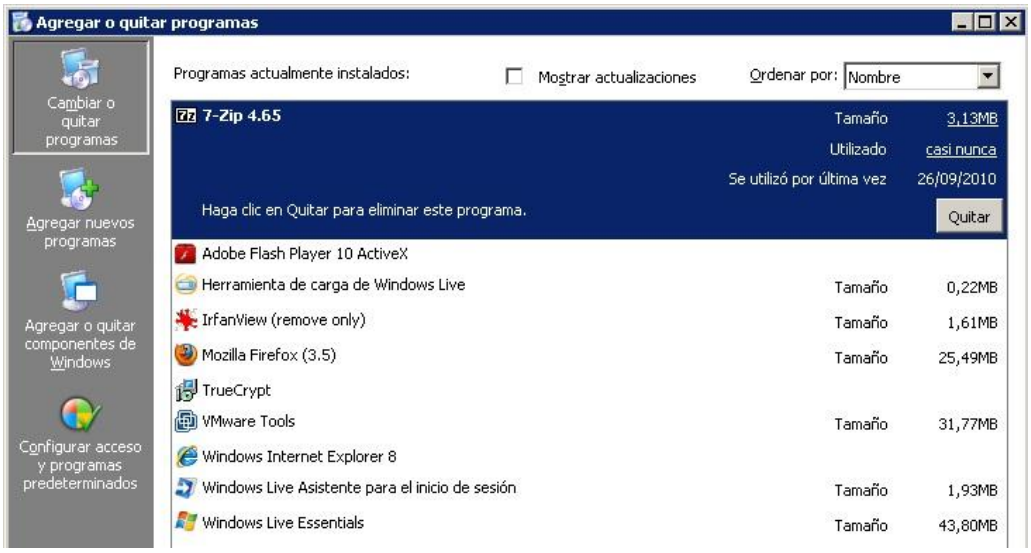
El huso horario configurado es el de EEUU – Canadá, la hora que marca en el sistema es 23:07 y la hora local es 21:06, por lo tanto existe una diferencia de 2 horas entre el sistema que se investiga y el sistema con el que se busca la evidencia.

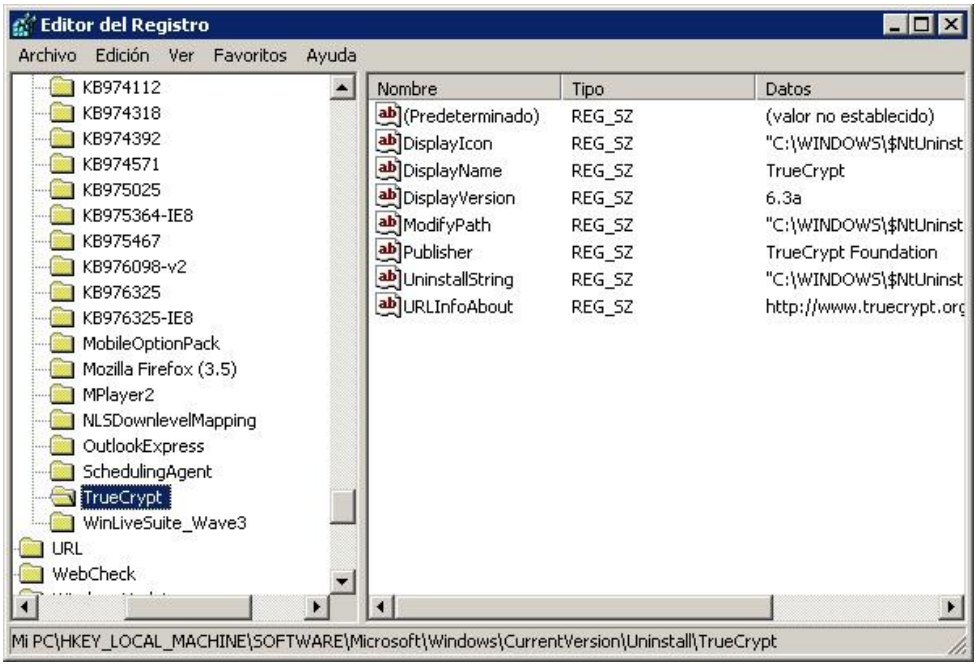
Solo existe un usuario, y este no tiene contraseña



Software Instalado

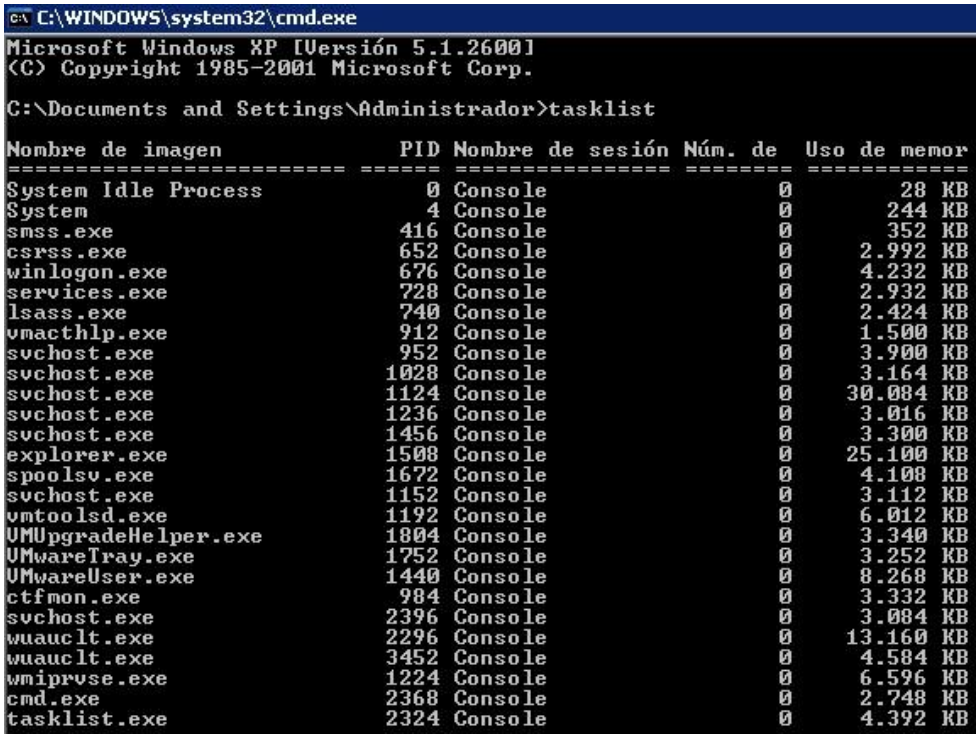
Se busca el software instalado de dos maneras, la una mediante la herramienta agregar o quitar programas del sistema y la otra mediante la búsqueda en el regedit.





En esta parte se logra detectar que existe un software llamado Truecrypt, el cual sirve para cifrar datos, según esto queda la posibilidad de que exista algún dato o disco duro cifrado.

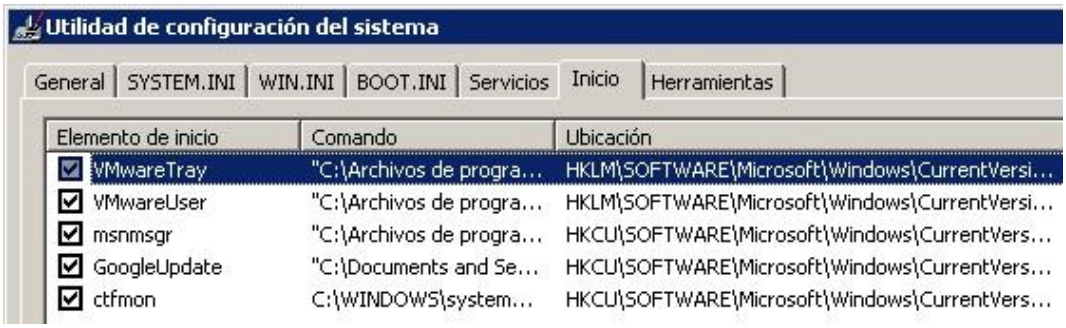
Servicios y procesos en ejecución



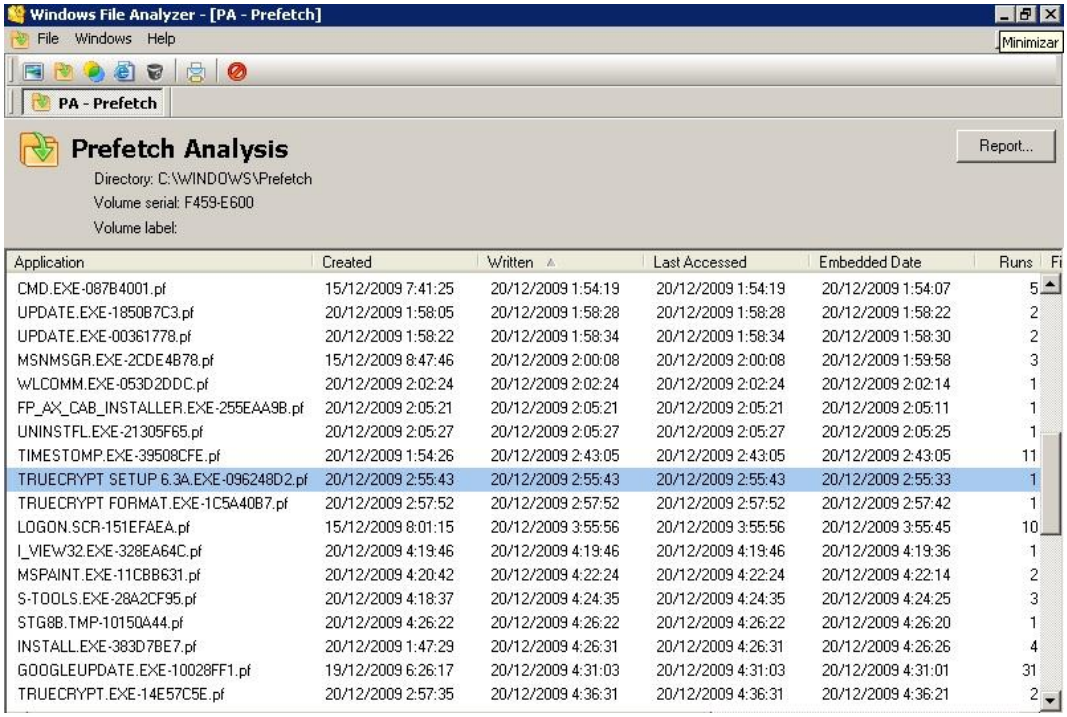
Hasta aquí no se logra advertir nada extraño o fuera de lo común

Programas que se inician con el arranque del sistema

Para esto se utiliza msconfig, y aparentemente no hay nada interesante o fuera de lo normal.



Programas ejecutados en el sistema



Application	Created	Written	Last Accessed	Embedded Date	Runs
CMD.EXE-087B4001.pf	15/12/2009 7:41:25	20/12/2009 1:54:19	20/12/2009 1:54:19	20/12/2009 1:54:07	5
UPDATE.EXE-1850B7C3.pf	20/12/2009 1:58:05	20/12/2009 1:58:28	20/12/2009 1:58:28	20/12/2009 1:58:22	2
UPDATE.EXE-00361778.pf	20/12/2009 1:58:22	20/12/2009 1:58:34	20/12/2009 1:58:34	20/12/2009 1:58:30	2
MSNMSGR.EXE-2CDE4B78.pf	15/12/2009 8:47:46	20/12/2009 2:00:08	20/12/2009 2:00:08	20/12/2009 1:59:58	3
WLCOMM.EXE-053D2DDC.pf	20/12/2009 2:02:24	20/12/2009 2:02:24	20/12/2009 2:02:24	20/12/2009 2:02:14	1
FP_AX_CAB_INSTALLER.EXE-255EAA9B.pf	20/12/2009 2:05:21	20/12/2009 2:05:21	20/12/2009 2:05:21	20/12/2009 2:05:11	1
UNINSTFL.EXE-21305F65.pf	20/12/2009 2:05:27	20/12/2009 2:05:27	20/12/2009 2:05:27	20/12/2009 2:05:25	1
TIMESTOMP.EXE-39508CFE.pf	20/12/2009 1:54:26	20/12/2009 2:43:05	20/12/2009 2:43:05	20/12/2009 2:43:05	11
TRUECRYPT SETUP 6.3A.EXE-096248D2.pf	20/12/2009 2:55:43	20/12/2009 2:55:43	20/12/2009 2:55:43	20/12/2009 2:55:33	1
TRUECRYPT FORMAT.EXE-1C5A40B7.pf	20/12/2009 2:57:52	20/12/2009 2:57:52	20/12/2009 2:57:52	20/12/2009 2:57:42	1
LOGON.SCR-151EFAEA.pf	15/12/2009 8:01:15	20/12/2009 3:55:56	20/12/2009 3:55:56	20/12/2009 3:55:45	10
I_VIEW32.EXE-328EA64C.pf	20/12/2009 4:19:46	20/12/2009 4:19:46	20/12/2009 4:19:46	20/12/2009 4:19:36	1
MSPAINT.EXE-11CBB631.pf	20/12/2009 4:20:42	20/12/2009 4:22:24	20/12/2009 4:22:24	20/12/2009 4:22:14	2
S-TOOLS.EXE-28A2CF95.pf	20/12/2009 4:18:37	20/12/2009 4:24:35	20/12/2009 4:24:35	20/12/2009 4:24:25	3
STG8B.TMP-10150A44.pf	20/12/2009 4:26:22	20/12/2009 4:26:22	20/12/2009 4:26:22	20/12/2009 4:26:20	1
INSTALL.EXE-383D7BE7.pf	20/12/2009 1:47:29	20/12/2009 4:26:31	20/12/2009 4:26:31	20/12/2009 4:26:26	4
GOOGLEUPDATE.EXE-10028FF1.pf	19/12/2009 6:26:17	20/12/2009 4:31:03	20/12/2009 4:31:03	20/12/2009 4:31:01	31
TRUECRYPT.EXE-14E57C5E.pf	20/12/2009 2:57:35	20/12/2009 4:36:31	20/12/2009 4:36:31	20/12/2009 4:36:21	2

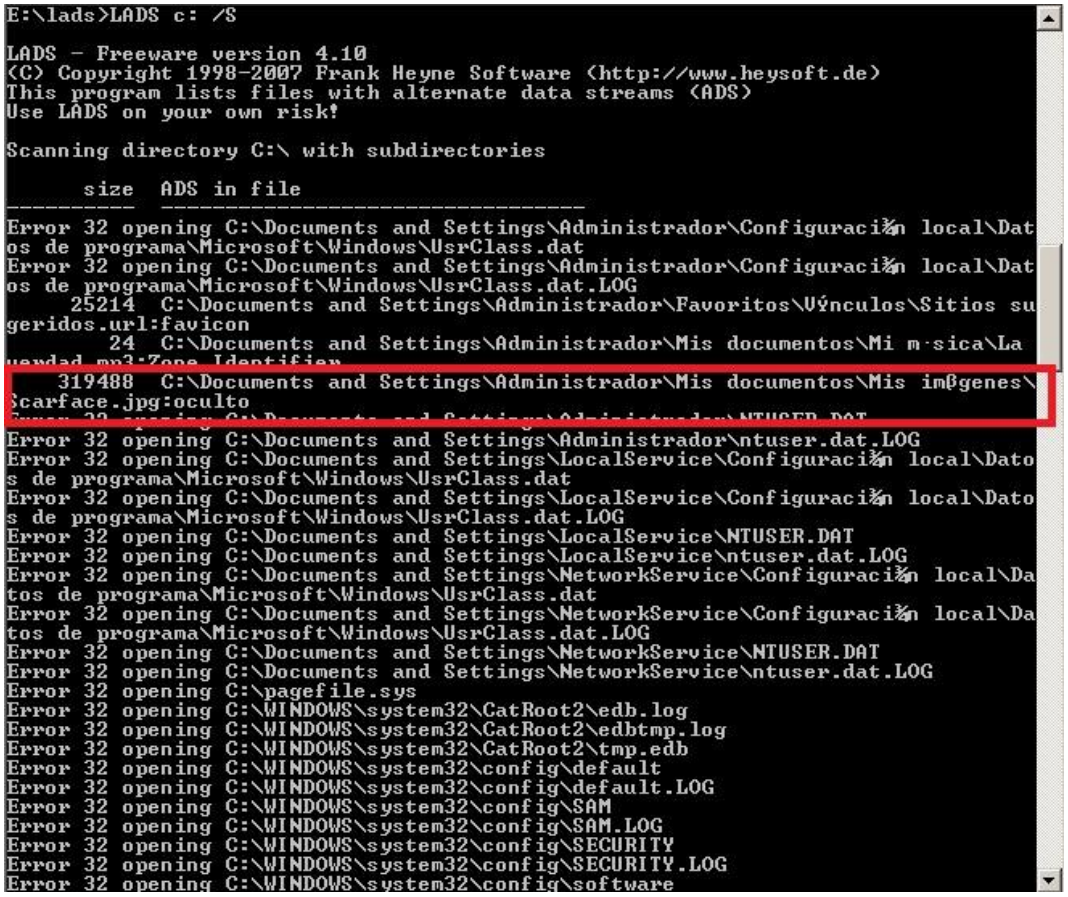
Nuevamente aquí se puede advertir que el programa TrueCrypt[1] se está ejecutando 2 veces.

Ahora que se tiene una idea de que es lo que se ejecuta y con qué tipo de sistema operativo se está trabajando, la pregunta es, ¿cuál es el siguiente paso?

Como se trata de un sistema operativo con un sistema de archivos NTFS, puede ser que el criminal haya creado un Alternate Data Stream[2] (ADS), que es una característica de este tipo de sistema de archivos que sirve para guardar información o streams, como por ejemplo nivel de acceso, directivas, permisos, si es un acceso directo, etc., es decir información que le sirva al sistema operativo para poder abrir el archivo, pero que puede ser usada también para ocultar información.

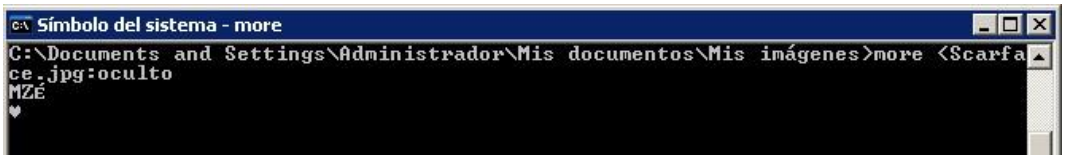
[1]TrueCrypt es una aplicación para cifrar y ocultar en el computador datos que el usuario considere reservados empleando para ello diferentes algoritmos de cifrado como AES, Serpent y Twofish o una combinación de los mismos. Permite crear un volumen virtual cifrado en un archivo de forma rápida y transparente.
[2]Característica de los sistemas NTFS en los que se oculta un archivo dentro de otro. (ADS)

En este caso se utilizará la herramienta “Lads” que sirve para encontrar este tipo de archivos.



Efectivamente se encuentra un archivo denominado Scarface.jpg: oculto, veamos que tiene la imagen.

El siguiente paso es ver qué tipo de archivo es el que está ocultando, para esto se utiliza el comando more.



Si se busca en Google a qué tipo de archivo pertenece **MZ**[3], se verifica que se trata de un archivo ejecutable.

Como las cosas se ponen interesantes lo siguiente es ver qué es lo que ejecuta, para esto utilizaremos el comando cat que permitirá extraer el ejecutable.

```
C:\>E:

E:\>cd UnxUtils

E:\UnxUtils>cd usr

E:\UnxUtils\usr>cd local

E:\UnxUtils\usr\local>cd wbin

E:\UnxUtils\usr\local\wbin>cat "C:\Documents and Settings\Administrador\Mis docu
mentos\Mis imágenes\Scarface.jpg:oculto">"Recuperado.exe"
```

Se procede rápidamente a ejecutar el archivo recuperado

Se encuentra que se trata de un programa denominado SteganosLockNote[4], nuevamente si hacemos la consulta en Google dice

[3] **Ejecutable de DOS:** Fue introducido con DOS 2.0, y puede ser identificado con los caracteres ASCII "MZ" o en forma hexadecimal *4D 5A* al comienzo del archivo (el llamado Número Mágico). Este ejecutable puede ser corrido tanto en DOS como en Windows. "MZ" son las iniciales de Mark Zbikowski, uno de los programadores de MS-DOS.

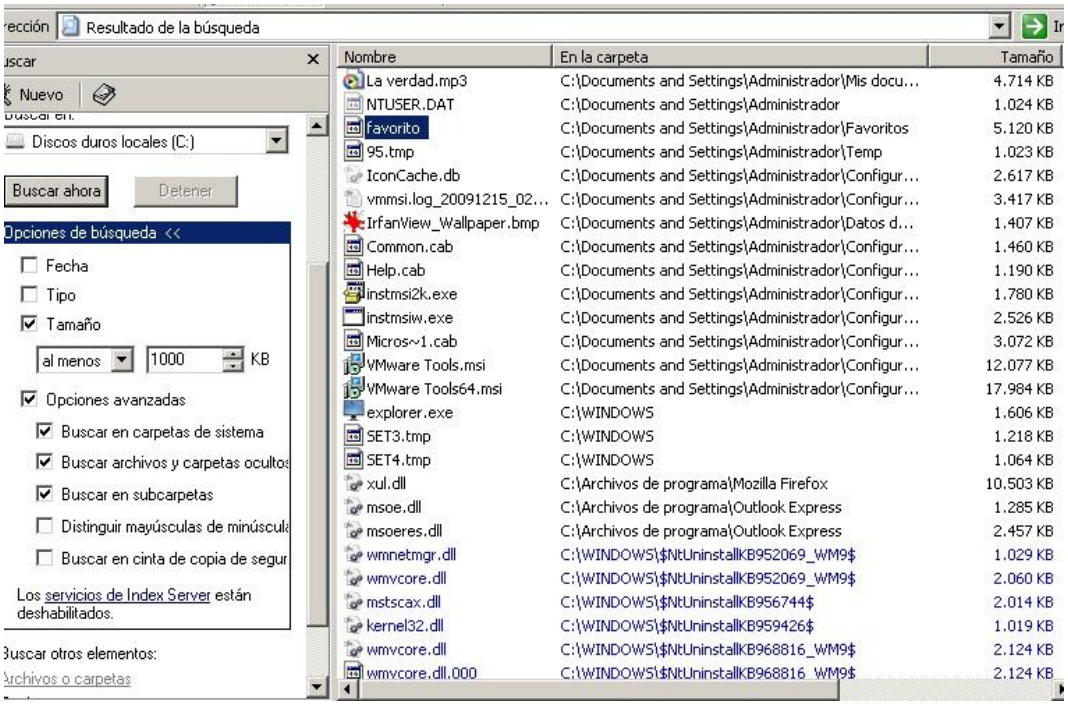
[4] Una pequeña utilidad similar al bloc de notas en la cual se puede codificar textos de una forma sencilla y fiable, utiliza el algoritmo AES de 256 bits.

que se trata de un programa que sirve para guardar con contraseña ciertos documentos.

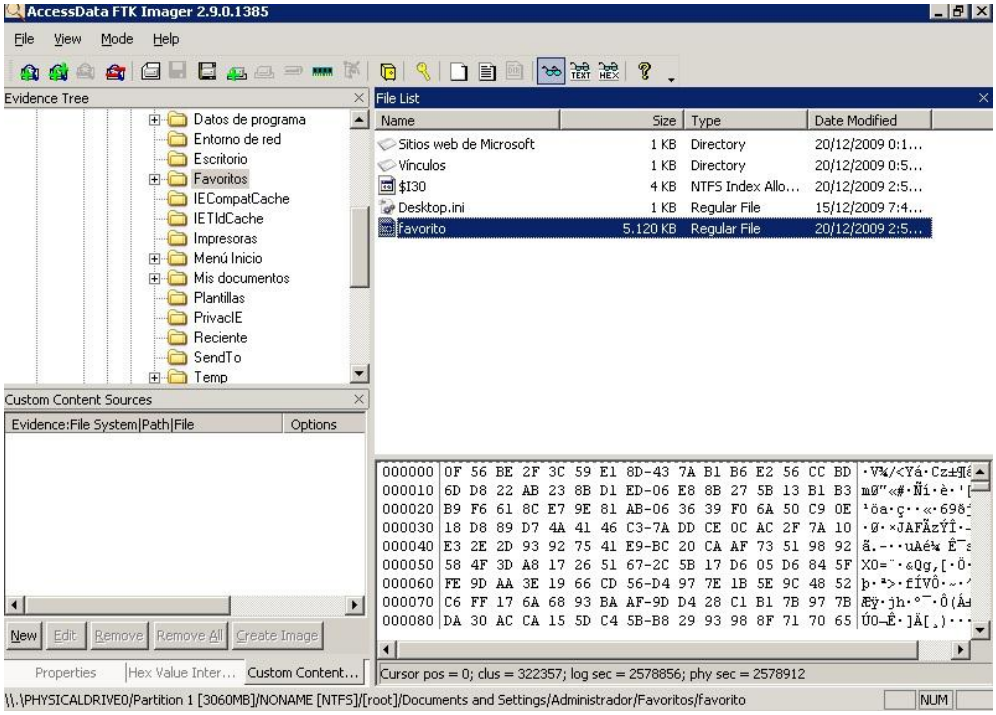
Este programa nos pide una contraseña, la cual veremos si se puede encontrar en algún rastro dejado en la computadora, o si forzosamente se tendrá que utilizar fuerza bruta para obtener la contraseña.

Búsqueda de contenido cifrado con Truecrypt

Para comenzar con lo más simple se procede con una búsqueda en el disco duro, de archivos sin extensión y que sean mayores a 1000 Kbytes, luego con el resultado se procederá a buscar los archivos y catalogar cuales se considerarán como sospechosos.



Justamente lo que se esperaba, se encuentra un archivo llamado favorito de un tamaño considerable y sin extensión, inmediatamente se procede a ver el contenido del archivo.

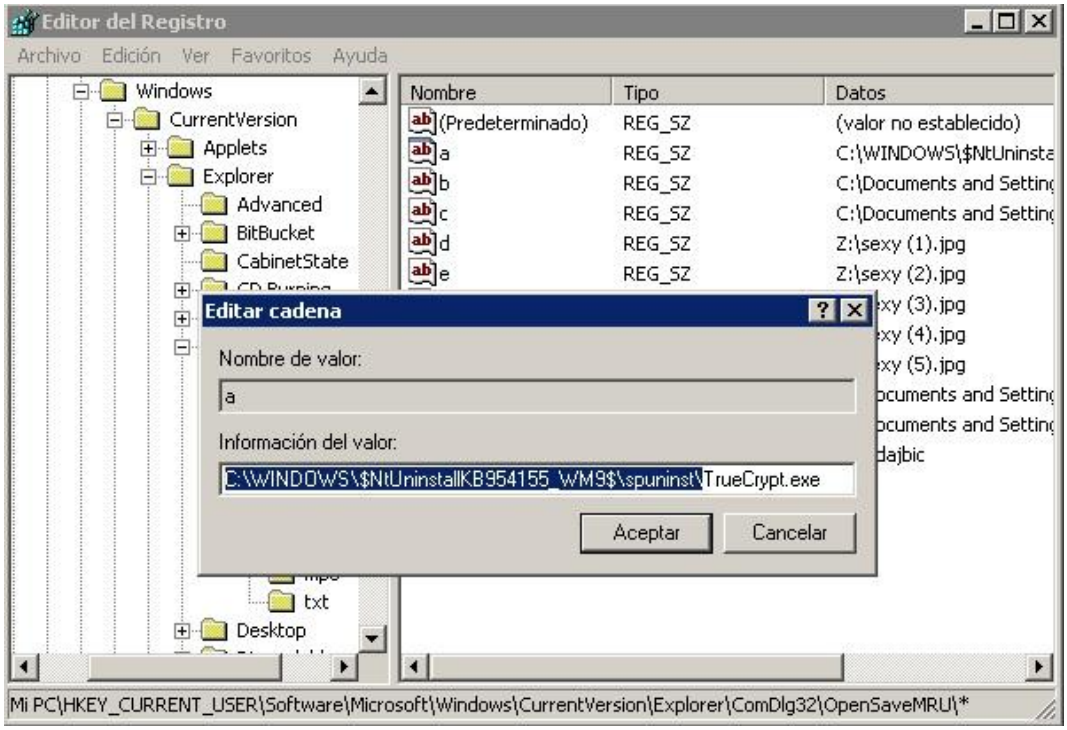


Se trata de un contenido ilegible, por lo tanto puede tratarse de un archivo o volumen previamente cifrado.

Ejecutando TrueCrypt

El siguiente paso lógico es ejecutar el programa TrueCrypt para verificar si el archivo es un volumen cifrado, pero como se dijo en puntos anteriores el programa TrueCrypt está instalado y ejecutándose pero no se encuentra en la carpeta predefinida para la instalación.

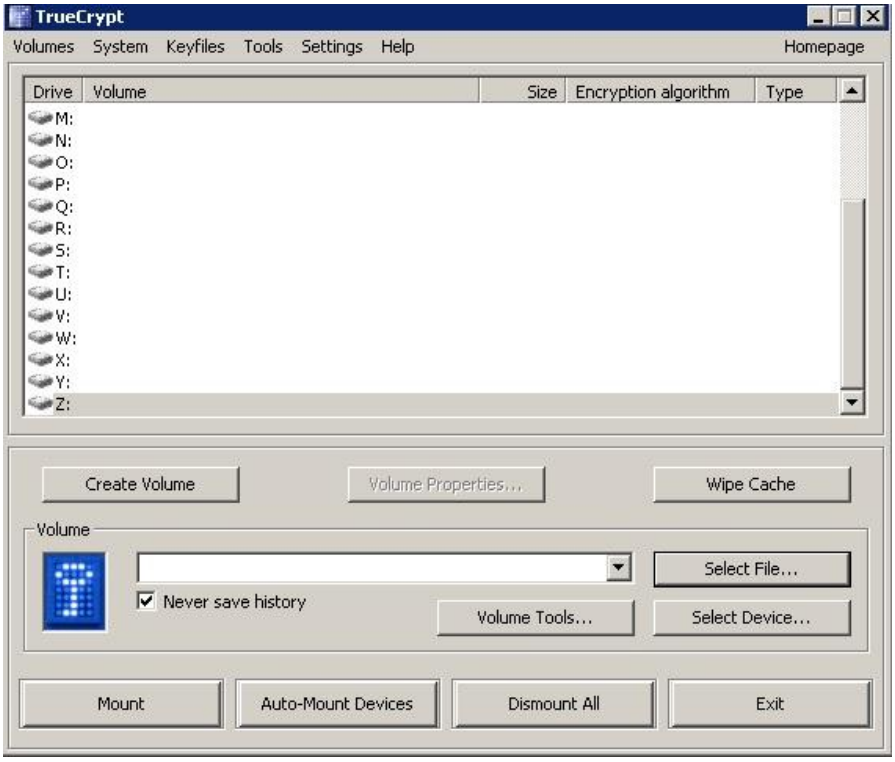
Se intenta hacer la búsqueda habilitando la casilla de mostrar documentos ocultos, pero no da ningún resultado. Por último se hace una búsqueda en el regedit y se obtiene un resultado.



Se puede notar claramente que alguien modifico la ruta normal del ejecutable y ahora se encuentra en:

"**C:\WINDOWS\$NtUninstallKB954155_WM9$\spuninst**".

Inmediatamente se verifica si la ruta existe y se comprueba la integridad del programa.



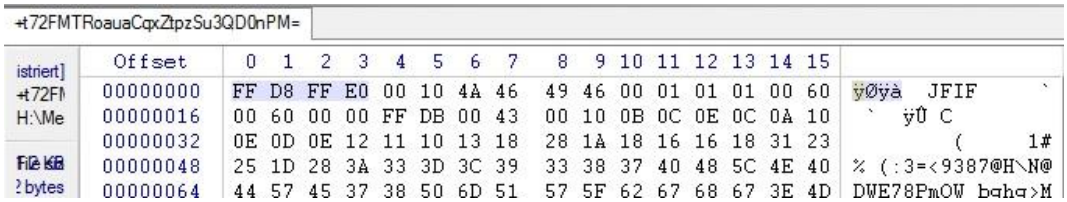
Archivos temporales de Internet

Buscando en los temporales de internet se encontró la siguiente carpeta:

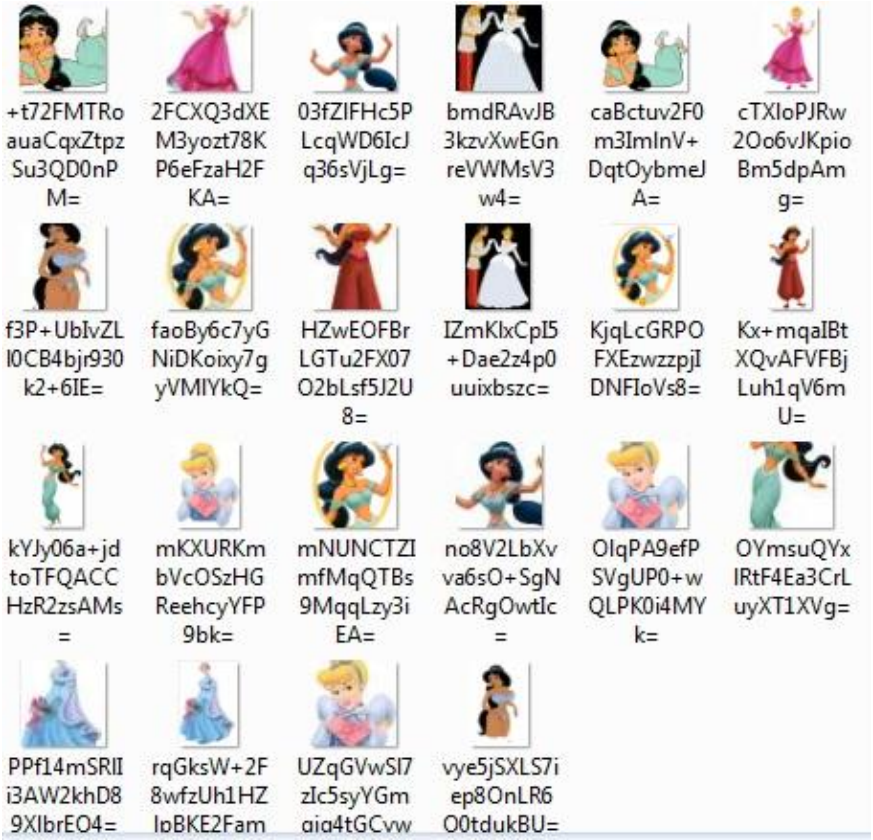
C:\Documents and Settings\Administrador\Temp\MessengerCache

Nombre	Ta...	Tipo	Fecha de modifi...
Sounds		Carpeta de archivos	15/12/2009 3:51
+t72FMTRoauaCqxZtpzSu3QD0nPM=	2 KB	Archivo	19/12/2009 23:09
2FCXQ3dXEM3yozt78KP6eFzaH2FKA=	2 KB	Archivo	19/12/2009 21:22
03fZlFHc5PLcqWD6IcJq36sVjLg=	12 KB	Archivo	19/12/2009 23:10
bmdRAvJB3kzvXwEGnreVWMsV3w4=	2 KB	Archivo	19/12/2009 21:22
caBctuv2F0m3ImlnV+DqtOybmeJA=	20 KB	Archivo	19/12/2009 23:09
cTXloPJRw2Oo6vJKpioBm5dpAmg=	11 KB	Archivo	19/12/2009 21:22
ErrorResponse.xml	3 KB	Documento XML	19/12/2009 21:03
f3P+UbIvZLl0CB4bjr930k2+6IE=	2 KB	Archivo	19/12/2009 23:09
faoBy6c7yGNiDKoixy7gyVMlYkQ=	2 KB	Archivo	19/12/2009 23:09
HZwEOFBrLGTu2FX07O2bLsf5J2U8=	2 KB	Archivo	19/12/2009 23:09
IZmKlxCpI5+Dae2z4p0uuixbszc=	17 KB	Archivo	19/12/2009 21:22
KjqLcGRPOFXEzwzzpjIDNFIoVs8=	23 KB	Archivo	19/12/2009 23:11
Kx+mqaIBtXQvAFVFBjLuh1qV6mU=	14 KB	Archivo	19/12/2009 23:09
kYJy06a+jdtoTFQACCHzR2zsAMs=	13 KB	Archivo	19/12/2009 23:09
mKXURKmbVcOSzHGReehcyYFP9bk=	9 KB	Archivo	19/12/2009 21:22
mNUNCTZImfMqQTBs9MqqLzy3iEA=	21 KB	Archivo	19/12/2009 22:25
no8V2LbXvva6sO+SgNAcRgOwtIc=	2 KB	Archivo	19/12/2009 23:09
OlqPA9efPSVgUP0+wQLPK0i4MYk=	20 KB	Archivo	19/12/2009 21:05
OYmsuQYxlRtF4Ea3CrLuyXT1XVg=	2 KB	Archivo	19/12/2009 23:09
PPf14mSRlIi3AW2khD89XlbrEQ4=	1 KB	Archivo	19/12/2009 21:19
rqGksW+2F8wfzUh1HZlpBKE2Fam3k=	6 KB	Archivo	19/12/2009 21:19
UZqGWwSl7zIc5syYGmgiq4tGCyw=	2 KB	Archivo	19/12/2009 21:22
vye5jSXLS7iep8OnLR6O0tdukBU=	16 KB	Archivo	19/12/2009 23:09

Estos archivos no tienen extensión, por tanto se decide abrirlos con un editor hexadecimal para tratar de descifrar el tipo de archivo.

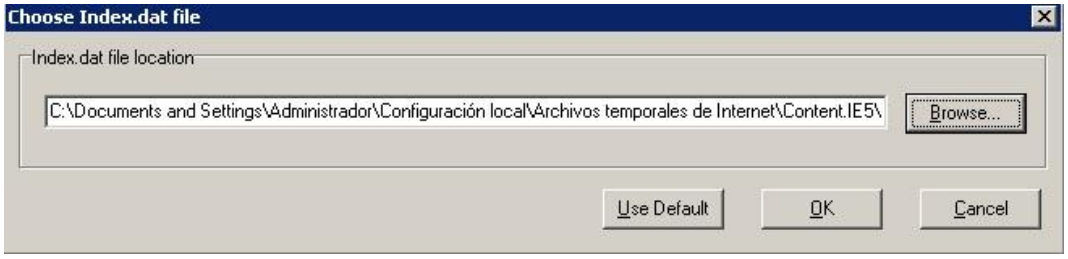


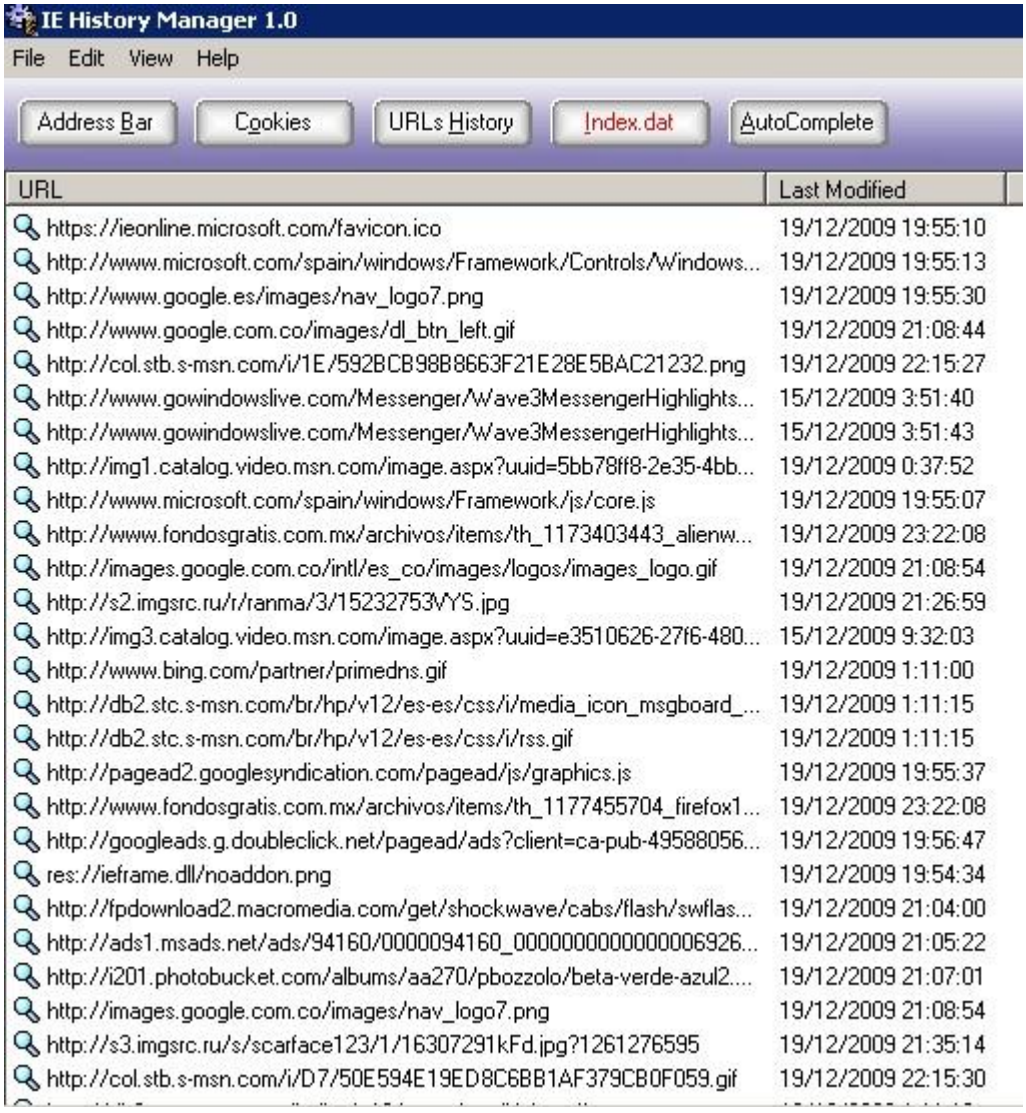
Haciendo una breve consulta en internet se puede encontrar que la cabecera FF D8 FF E0 corresponde a un archivo JPG, por tanto todos los archivos de esta carpeta son imágenes, ahora solo se les coloca la extensión jpg y ya se puede visualizar las imágenes.



Búsqueda de URL's

Lo siguiente es hacer un análisis de las páginas de internet en las cuales navegó el sospechoso. Para esto se utilizó la herramienta "*IeHistory*" que sirve para ver el historial de Internet Explorer.





La información que saca el programa es abundante, por eso es necesario hacer un análisis y en base a la experiencia definir cuáles serían las direcciones de mayor interés, en este caso se detallan las siguientes:

1. http://mp3.hhgroups.com/Material/Maquetas/559/09.%20Porta%20-%20las%20ninyas%20de%20hoy%20en%20dia%20todas%20son%20unas…%20-%20www.HHGroups.com.mp3
2. http://www.google.com.co/search?hl=es&q=high+school+musical+sexo&meta=&aq=f&oq=
3. http://politolia.wordpress.com/2007/09/06/escandalo-en-high-school-musical-por-fotos-desnuda-de-vanessa-hudgens
4. http://imgsrc.ru/main/login.php
5. http://imgsrc.ru/main/user.php?user=scarface123
6. http://imgsrc.ru/main/join2.php?email=scarface1fisica@hotmail.com&login=scarface123&finally=yeah

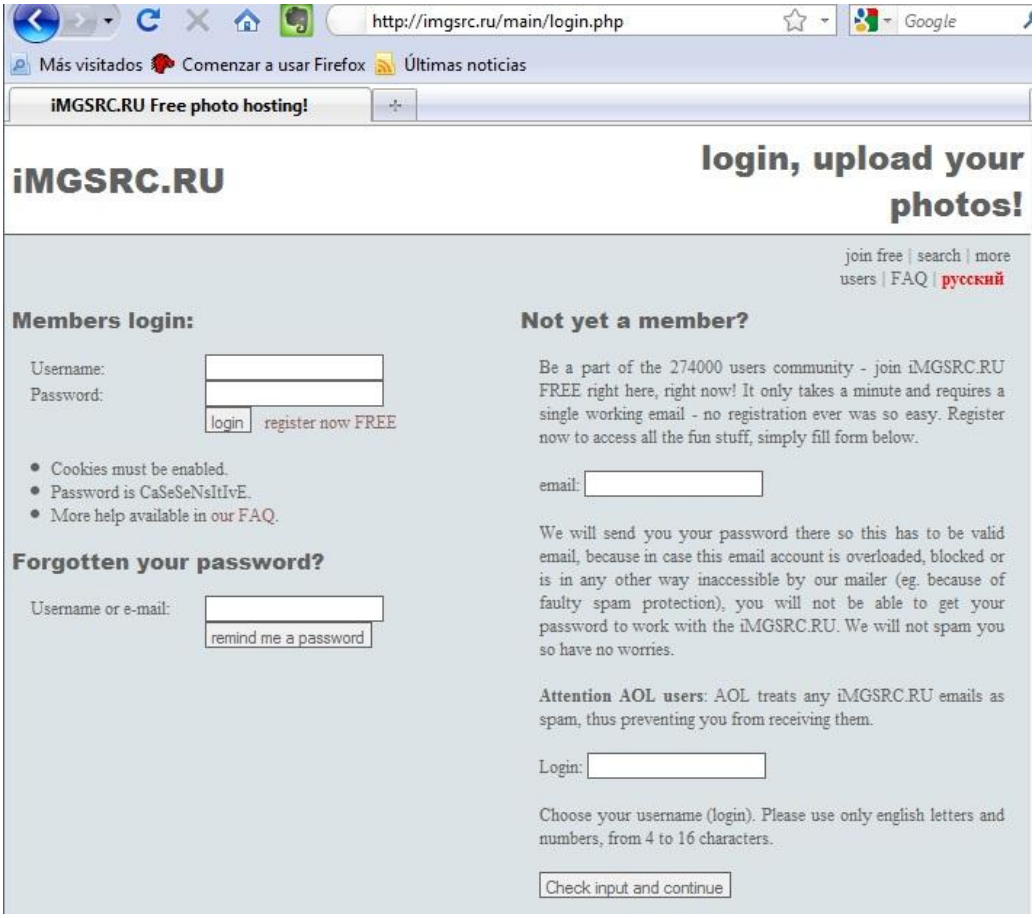
Análisis de cada URL

La primera dirección apunta al dominio "*hhgroups.com*", y se puede evidenciar que hizo una búsqueda con el texto *"Porta-las ninyas de hoy en dia todas son unas*", nuevamente haciendo una búsqueda rápida en internet, se encuentra que se trata de una canción del grupo Porta y que habla sobre las adolescentes de hoy y cuya letra se podría catalogar como ofensiva.

El segundo enlace hace una búsqueda en Google con el texto "*highschool musical sexo*", esta búsqueda lleva directamente a la tercera dirección, que es el primer resultado de la búsqueda.

Las tres últimas direcciones al parecer son importantes porque se refieren al mismo dominio y solicitan usuario y password.

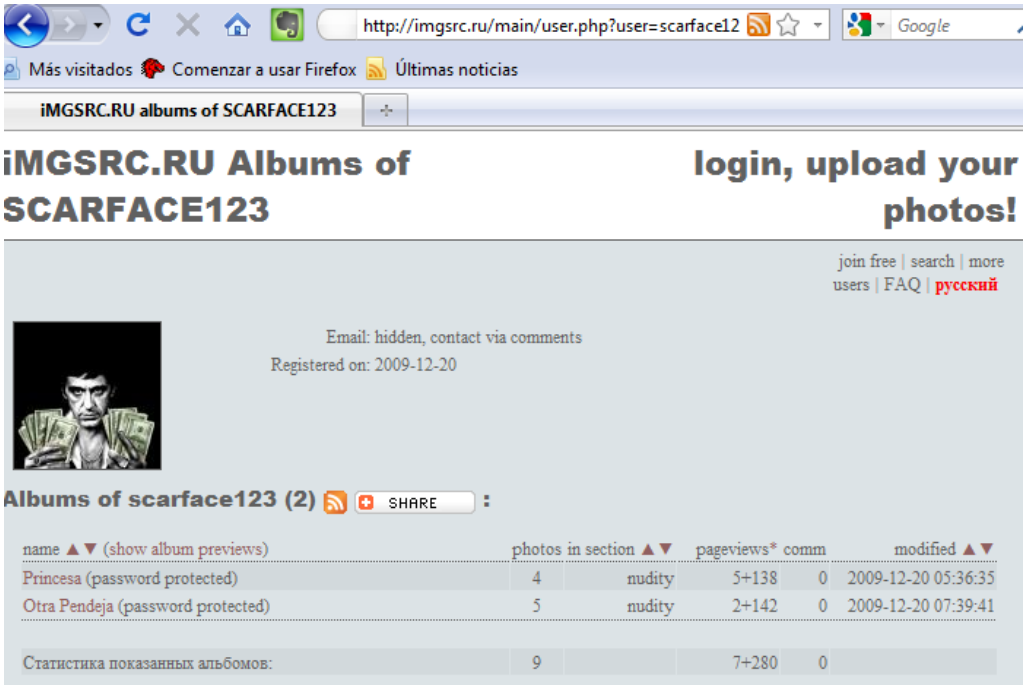
http://imgsrc.ru/main/login.php



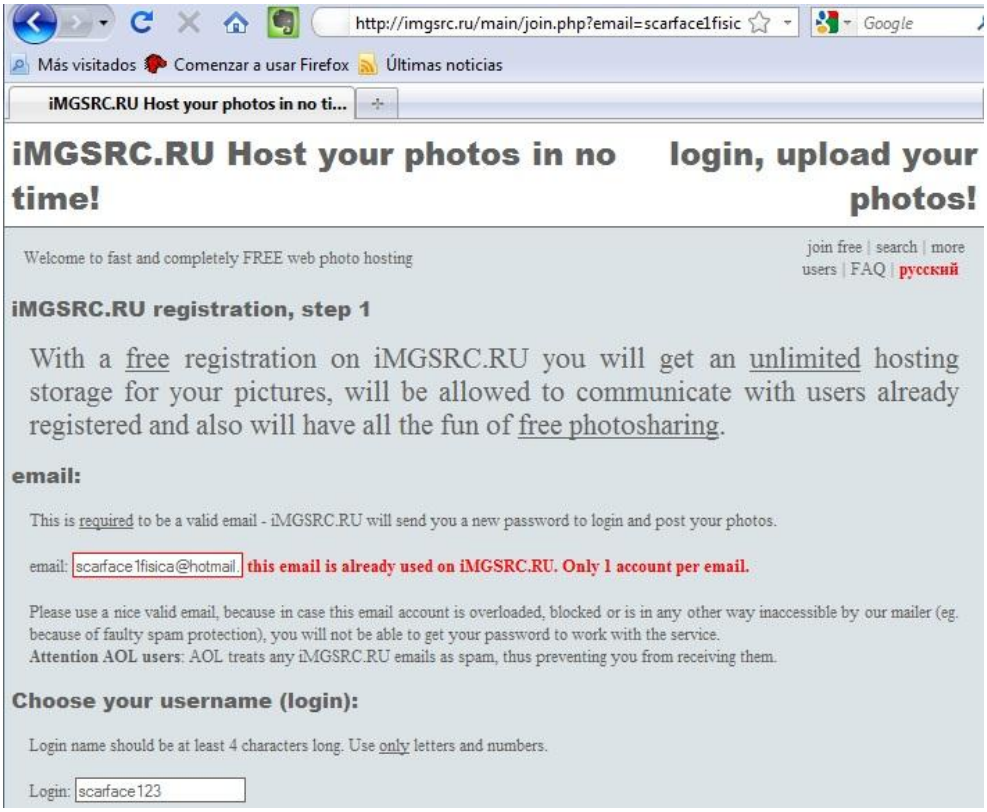
Como se comentó antes en esta página es necesario ingresar con un password y además de eso es una página rusa y por la fama de estos

enlaces rusos es casi seguro que este dominio acepte imágenes relacionadas con la pornografía.

http://imgsrc.ru/main/user.php?user=scarface123, esta dirección conduce al directorio del usuario scarface123, el cual es el posible sospechoso, por el momento se puede evidenciar que tiene 2 álbumes, uno denominado "*Princesa*" y el siguiente "*Otra pendeja*".



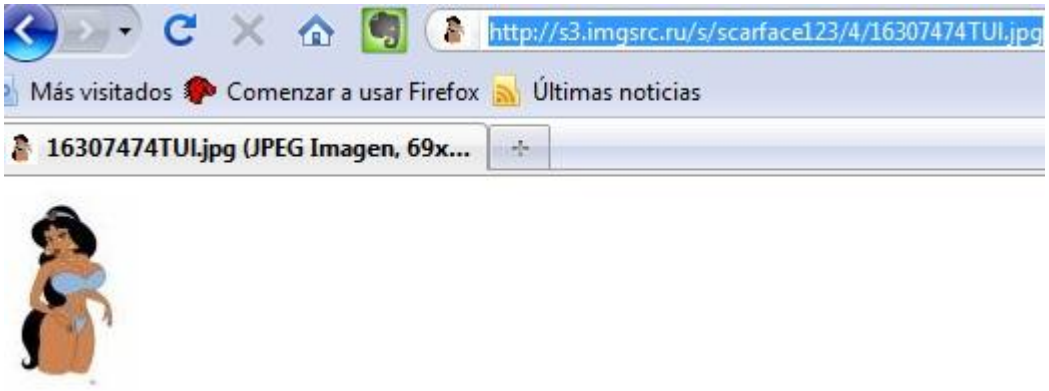
Y el último conduce al registro del sospechoso como usuario scarface123.



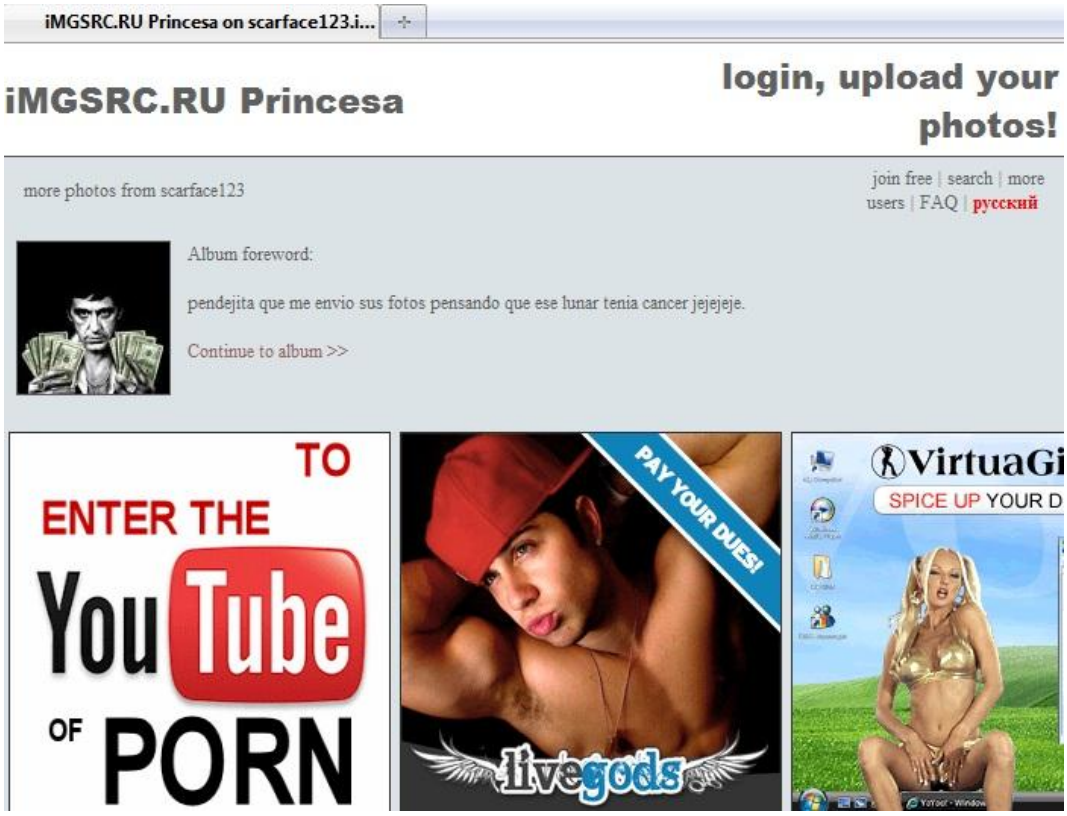
Este último enlace es interesante porque nos brinda los siguientes datos:

- E-mail: scarface1fisica@hotmail.com
- Usuario: scarface123
- Fecha: 19/12/2009 21:27:56

Existen rastros de que estas carpetas tienen contenido pedófilo



Cuando se trata de ingresar a uno de los álbumes pide contraseña pero muestra un mensaje de bienvenida interesante.

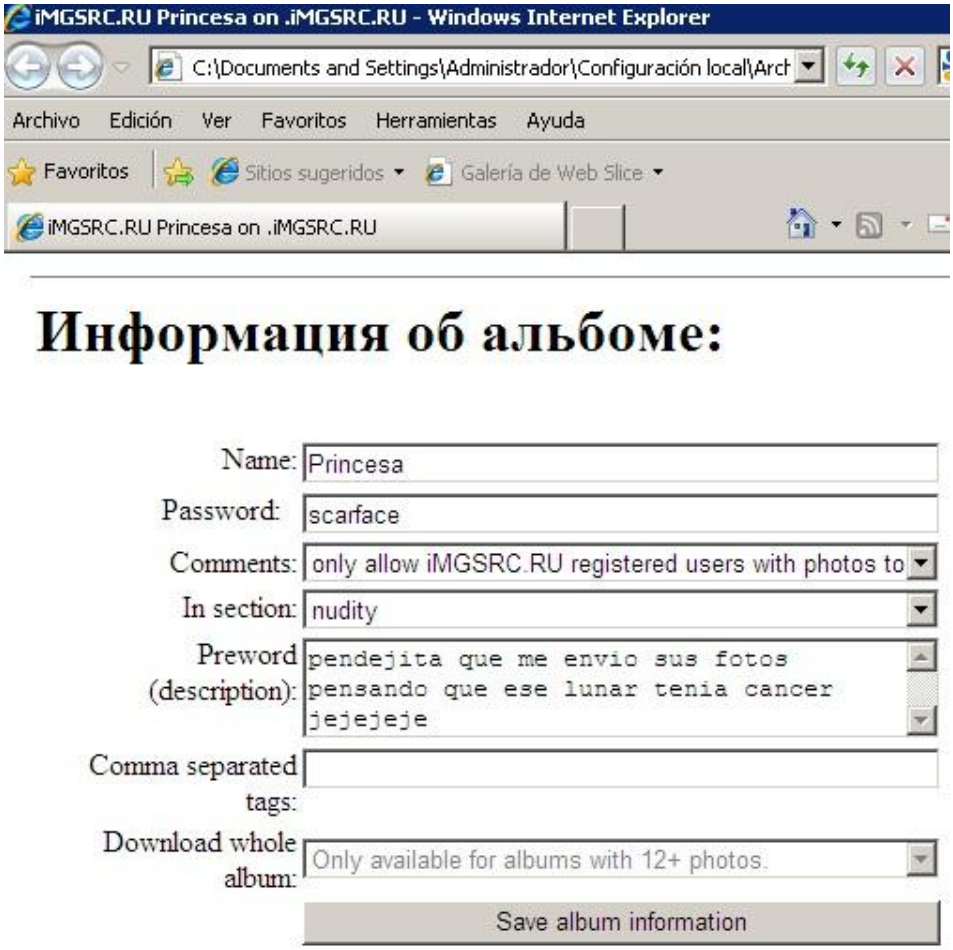


"*pendejita que me envió sus fotos pensando que ese lunar tenia cancerjejejeje.";* también se puede verificar que el hosting ruso si permite contenido pornográfico.

Si nuevamente revisamos el historial de la URL se puede encontrar que imágenes fueron las que se subieron presumiblemente a este hosting ruso.

La imagen que más llama la atención es lunar.jpg, esto porque está relacionado con el mensaje que se encontró en el ingreso a uno de los álbumes.

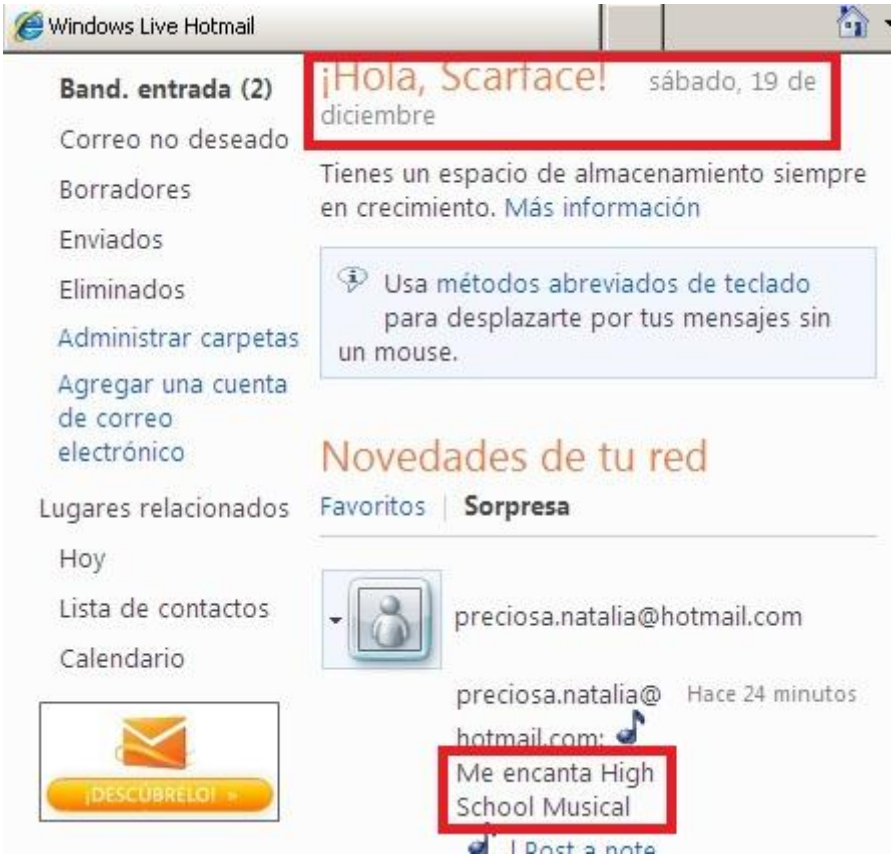
Siguiendo con el análisis de las direcciones encontradas, se encuentra una página muy interesante que muestra el mensaje mencionado anteriormente y también nos muestra un password, que puede ser el que se utiliza para entrar a los álbumes.



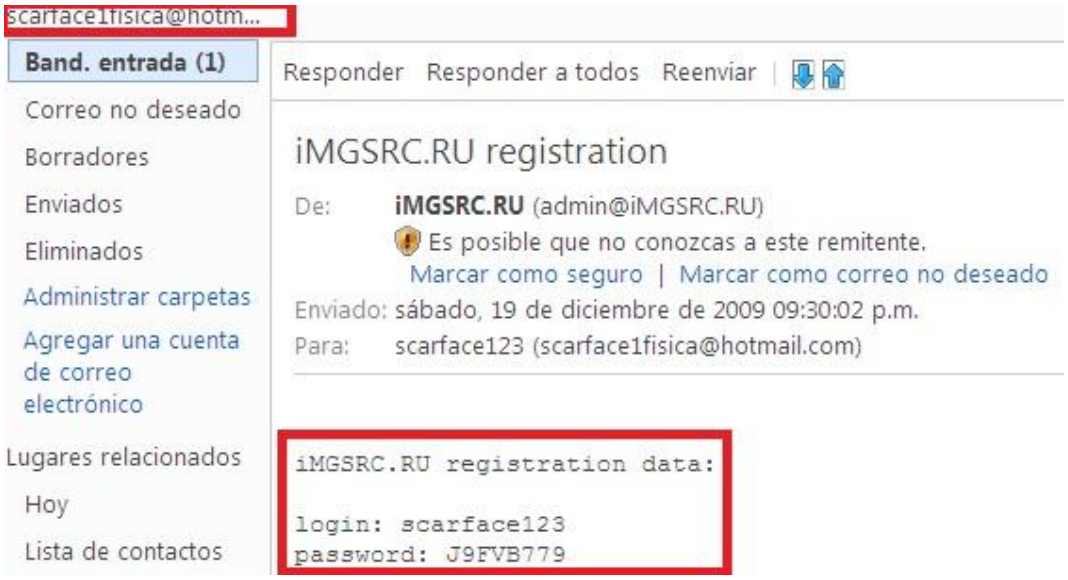
Probamos si es la clave correcta e ingresamos a los álbumes, en efecto es la clave correcta pero no se encuentra ninguna foto que contenga contenido pedófilo.

Pero si se puede advertir que en este sitio o en estos álbumes existieron fotos que fueron eliminadas.

También se puede encontrar rastros de acceso a Hotmail, se aprecia que tiene asignado un contacto denominado “precios.natalia@hotmail.com”, se puede apreciar que este correo está dentro del grupo “Me encanta High School Musical”.

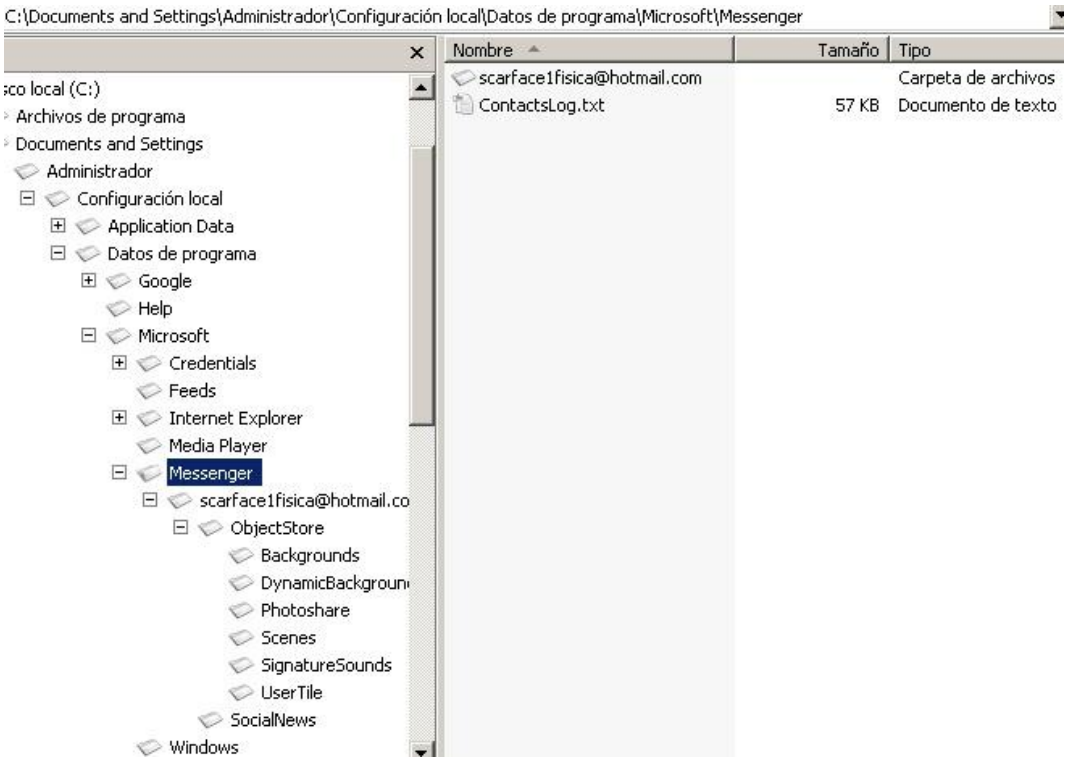


También se obtienen datos importantes que pueden servir como usuarios y contraseñas.



Historial de mensajería instantánea

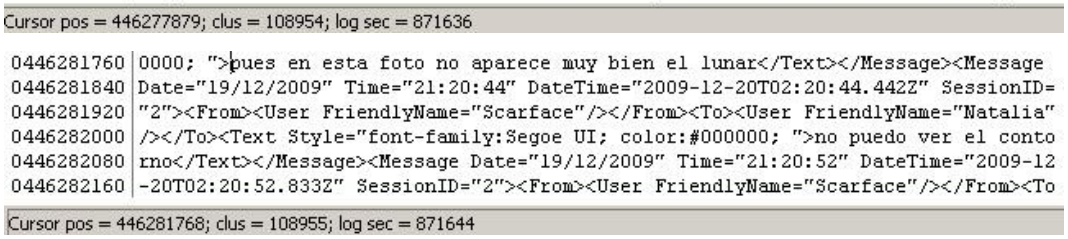
En esta parte se pretende hacer una búsqueda sobre los historiales de Messenger, para esto primero se revisará la carpeta donde este software acostumbra guardar los logs, "*C:\Documents and Settings\Administrador\Configuración local\Datos de programa\Microsoft\Messenger*", en esta ruta se encuentra la cuenta de Hotmail del sospechoso pero no se encuentra ningún log de conversaciones.



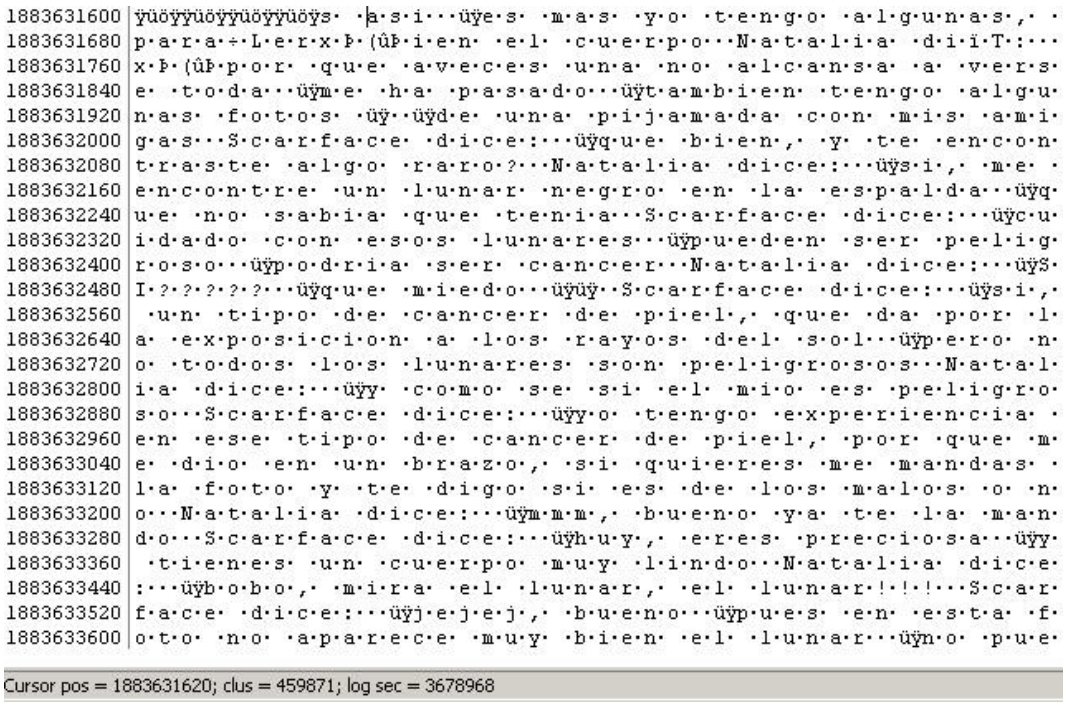
Revisando con más detenimiento en el disco duro se puede encontrar dos conversaciones, una con "*Camila*" y otra con "*Natalia*", a *Camila* la amenazan y le piden que envíe unas fotos y que ponga una cámara web, y a *Natalia* con la excusa de que pudiera tener una enfermedad le piden unas fotos para poder valorarla.

Cursor pos = 1651911284; clus = 403298; log sec = 3226389

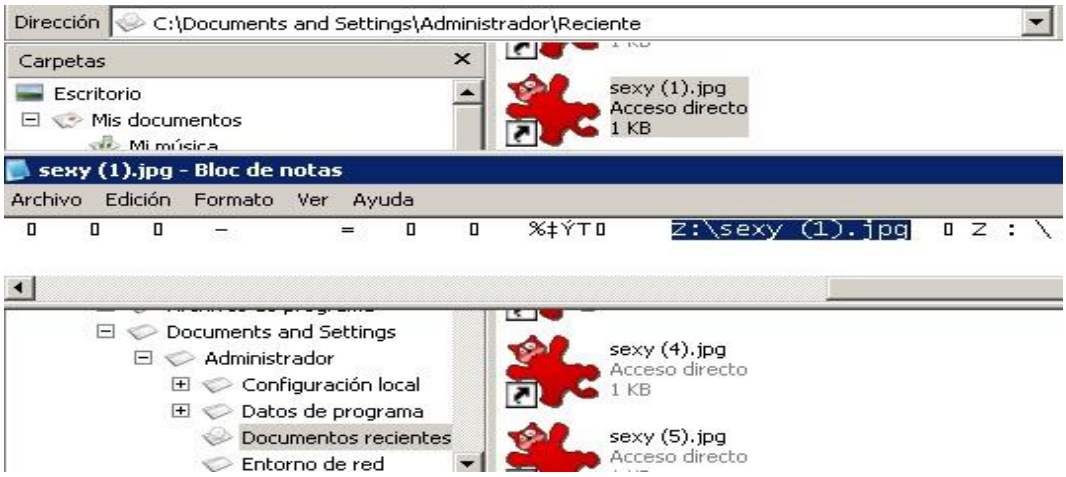
Cursor pos = 446277879; clus = 108954; log sec = 871636



Cursor pos = 446281768; clus = 108955; log sec = 871644



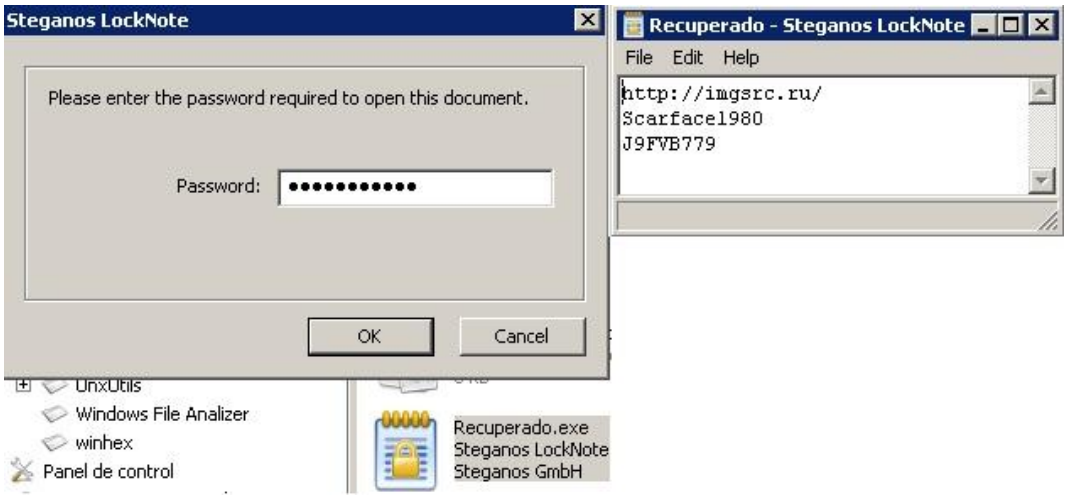
Por último se puede determinar que la mayoría de los últimos archivos abiertos son imágenes y estas imágenes fueron abiertas desde la unidad “Z” y en otros casos de la carpeta “Mis Imagenes”.



Hallazgo

Luego de buscar toda la cantidad de información posible, se puede empezar a hacer una descripción y un estudio más detallado.

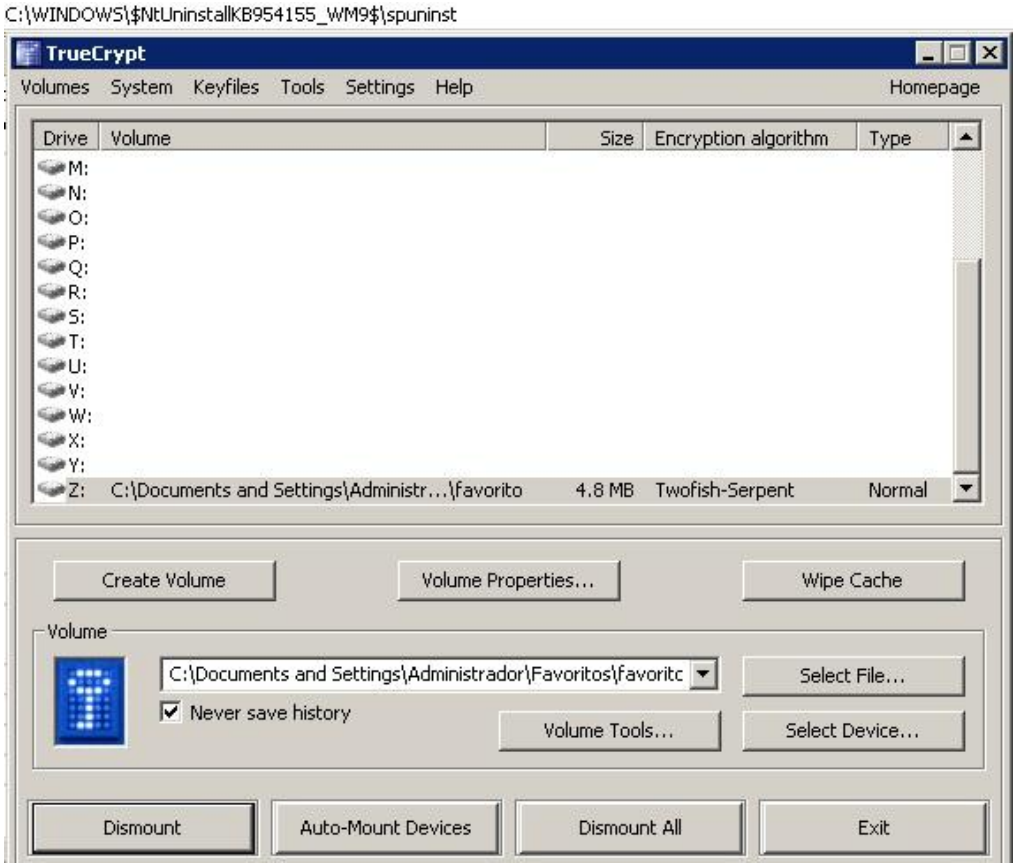
Lo primero es ejecutar nuevamente el programa “SteganosLockNote” que como se puede recordar fue oculto con la técnica ADS, ahora se prueba con las contraseñas encontradas.



La clave es “scarface123” y el ejecutable retorna datos que pueden ser usados como claves y el dominio “imgsrc.ru” que ya se había encontrado con anterioridad.

En este punto con toda la evidencia recolectada lo único que nos queda es buscar que contiene la unidad “Z”, para esto se debe ejecutar la aplicación “TrueCrypt” que como encontramos en un punto anterior se encuentra en la ruta "C:\WINDOWS\$NtUninstallKB954155_WM9$\spuninst", que no es la ruta por defecto y se encuentra ahí con la clara intención de ocultarla.

Se procede a montar la unidad con el archivo denominado “favorito” y que en un apartado anterior se había dicho que se trata de un archivo cifrado.



Al buscar en la ruta se encuentran las imágenes que habían sido borradas y de las cuales solo se contaba con el acceso directo.

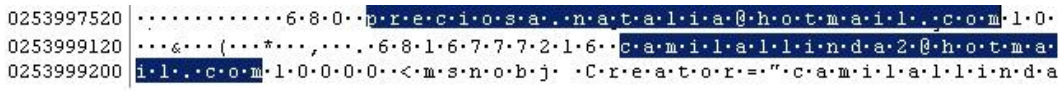
Rastros del sospechoso

Durante la investigación se pudo determinar que las huellas dejadas por el sospechoso y la evidencia determinante fue encontrada en:

- Historiales de navegación en Internet Explorer
  - Obtención de contraseñas y actividad en internet.
- Historiales del programa Messenger
  - Obtención de conversaciones y fotografías pedófilas solicitadas a sus víctimas.
- Historial de archivos abiertos recientemente
  - Rastros de ubicaciones donde se guardaban las fotografías.

Posibles victimas

Como se determinó que el modus operandi del sospechoso es buscar a sus víctimas mediante Messenger buscamos direcciones con la clave "@hotmail".



Natalia	preciosa.natalia@hotmail.com
Camila	camilalinda2@hotmail.com

Conclusiones

A continuación se detallan las siguientes conclusiones basadas en toda la evidencia que se ha encontrado y en las que se ha hecho referencia durante todo el informe.

El sospechoso buscó información en internet sobre "High School Musical", para luego utilizarla como enganche para sus posibles víctimas.

El sospechoso trato de ocultar toda información que lo pudiera incriminar.

El sospechoso utilizó herramientas para cifrar datos con el fin de ocultar información y ejecutar la aplicación que la contenía.

El sospechoso mantenía fotografías con contenido pedófilo en el disco duro, en el volumen cifrado y en un hosting de internet.

Dichas fotografías fueron solicitadas por el sospechoso a manera de engaños y amenazas a las usuarias de internet “Camila” y “Natalia”.

Como ya se mencionó antes el sospechoso mantenía y distribuía en internet las fotografías solicitadas a sus víctimas.

Herramientas Utilizadas

Aplicación	Funcionalidad	Licencia
Vmware WorkStation	Emular máquinas virtuales	Comercial
FTK Imager	Adquisición de imágenes de disco que luego serán usadas para análisis forense.	Free
Lads	Búsqueda de Alternate Data Stream (ADS)	Free
Cat	Extraer archivos de otros con ADS.	Free
deft_extra	Utilidades forenses	Free

Referencias

Aplicación	Dirección
VmwareWorkStation	http://www.vmware.com
FTKImager	http://www.accessdata.com/
Lads	http://www.heysoft.de
Cat	http://unxutils.sourceforge.net/
deft_extra	http://www.deftlinux.net/