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.

C	Physical Drive
С	Logical Drive
6	Image File
С	Contents of a Folder (logical file-level analysis only; excludes deleted, unallocated, etc.)

Se selecciona la ruta donde esta almacenada la imagen del sistema

μ	Browse

Debería verse de la siguiente forma



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

<u>File View M</u> ode <u>H</u> elp	
🏠 🏫 🚖 🔄 🖬 🖬 🗖 🚛 🛲 📟 🚥	🕅 🖸 🕄 🖸 🖬
Evidence Tree	File List
⊡ 💁 practica1.vmdk	Name
Partition 1 [3060MB]	🍶 [orphan]
Export Fles	
[unalloc] Export File Hash Li	st
	st ge (AD1)

Procedimiento de generación de firmas criptográficas en ejecución

🏫 🎎 🚖 🔄 🔂 🖬 🔂 🚛 💷 🛲	🚺 🔁 🕄 🗋 🗎 🖬 🔛 🗄
dence Tree	File List
g practica 1.vmdk	Name
	 [orphan] [root] [unallocated space] backup boot sector file system slack
Hashing Files	-2
Hashing files	
sto practica 1 ymdk\Partition 1 [3060MB]\NONAM	IF [NTES]\[root]\Archivos de

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]\\$Bac
d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfef95601890afd80709	practica1.vmdk\Partition 1 [3060MB]\NONAME [NTFS]\[root]\\$Bac
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
	f	

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.

?	The vendor of the processor(s) in this machine is not the same as the vendor of the processor(s) in the machine on which the snapshot was saved. You may attempt to resume this virtual machine, but doing so may result in unpredictable behavior. Do you wish to try to resume this virtual machine?
	Yes No
Mware	e Workstation
Restor	ing virtual machine state

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.

Dispositivos con almacenami	ento extraíble
Disco de 3½ (A:)	Unidad de CD (D;)
entas Ayuda	
V	\vee
adencrypt.dll 2.9.0.1385 ADEncrypt DLL	ADIsoDLL.dll
boost_date_time-vc90-mt-1_3.	boost_filesystem-vc90-mt-1_3
boost_regex-vc90-mt-1_39.dll	boost_system-vc90-mt-1_39.dll
boost_thread-vc90-mt-1_39.dll	cximage.dll 5.9.9.1 cximage
FTK Imager.exe FTK Imager AccessData Corporation	icudt40.dll 4.0.1.0 ICU Data DLL
icuuc40.dll 4.0.1.0 IBM ICU Common DLL	IsoBuster.dll 2.4.0.4 CD / DVD / Image File access
libeay32.dll 0.9.8.11 OpenSSL Shared Library	MD5Remote.dll

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

	ccessData FTK Imager 2.9.0.1385			_ 🗆 ×
Eile	View Mode Help			
	Add Evidence Item	逐		के देखें देखें 🤶
	Add All Attached Devices	×	File List	×
-	Remove Evidence Item		Name	Size Type
	Remove All Evidence Items			
٦	<u>C</u> reate Disk Image			
	Export Disk Image			
	Export Logical Image (AD1)			
1	Add to Custom Content Image (AD1)			
	Create Custom Content Image (AD1)	×		
-	Verify Drive/Image	5		
	Cap <u>t</u> ure Memory			
家	MetaCarve (Deep <u>S</u> can)			
	Obtain Protected Files	1		
9	Detect EFS Encryption	-	•	•
B	and the second se	nt	1	=

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

<u>File View Mode Help</u>		
	E & & = = = ¥ 6 4 D B B 4	ि रिक्षे रिक्षे
Evidence Tree	× File List	×
	Name	Size Type
Mem	ory Capture	X
Ente	r the path for the dumpfile:	
Level Level	Duranting 1	1
c:0	Practical browse	
Ente	r the filename for the dumpfiles	
	· che mename for che dampnie.	<u> 27</u>
mei	mdump.mem	
Custom Content Sources	24	
Evidence:File System Pa	Capture Memory Cancel	
•	F I	
	e till Greate Image	
Temore Izenove		•
Duesewhine Ulau Value T	pter Custom Content	
Propercies [nex value]	Interna Coston Concentral	in the second

Proceso de volcado de memoria en ejecución.

File View Mode Help		
		8.
	Name	Size Type
Memory Progress Destination: E:\Practica1\me Status: 102MB/536MB [Evidence:File System]]	emdump.mem [19%] Cancel	
New Edit Remove Remove All Greate Image Properties Hex Value Inter Custom Content Custom Content	<u>دا</u>	
For Help, press F1		NUM

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.

H HashCalc	
Data Format:	Data: D:\Tesis\Practico\Volcadomemoria1\memdump.mem
П НМАС	Key Format: Key:
MD5	1d11e56fefd0f59357b99c343d1fffbd
₩D4	34ce91a2327dc343e6170156b77d32ae
🔽 SHA1	ef3a03abc93fb248eb897a6bddca22dba35c1ceb
CRC32	a27b7927
□ eDonkey/ eMule	
<u>SlavaSo</u> ft	Calculate Close Help

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

- Source Drive Selecti	on Ibo following publi	able drives:	
C:\- [NTFS]	rie toliowing avai	able unves.	_

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.

mage Source C:\			
ct Image Destination			
mage Destination Folder			
E:\VL001			Browse
image Filename (Excluding E	Extension)		
dicoC001			
For Raw and E0:	Image Fragment Size (f 1 formats: 0 = do not fragm	4B) 1500 ent	
Compression (0=Nor	ne, 1=Fastest,, 9=Smalle	est) 0	<u></u>
	Use AD Encrypt	ion 🗖	

Creando la imagen

licoC001 Nage
licoC001 hage
Nage
0:00:07

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

🖂 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:

Тіро	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

Nombre	Nombre completo		
Administrador			
SAsistente de	Cuenta de asistente de A		
🛃 Invitado			

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.



	-	Nombre	Tipo	Datos
KB974112 KB974318 KB974318 KB974571 KB975025 KB975364-IE8 KB975467 KB976325 KB976325-IE8 MobileOptionPack Mozilla Firefox (3.5) MPlayer2 NLSDownlevelMapping OutlookExpress SchedulingAgent WinLiveSuite_Wave3		Nomore DisplayIcon DisplayName DisplayVersion ModifyPath Publisher UninstallString URLInfoAbout	REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ	Uacos (valor no establecido) "C:\WINDOWS\\$NtUnins TrueCrypt 6.3a "C:\WINDOWS\\$NtUnins TrueCrypt Foundation "C:\WINDOWS\\$NtUnins http://www.truecrypt.or
	-	•		

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.

Seleccione un elemento para ver su	Nombre 🛆
descripción.	Servicio de descubrimientos SSDP
	🖏 Servicio de Index Server
	🖏 Servicio de informe de errores
	🙀 Servicio de protocolo de autenticación extensible
	🎇 Servicio de puerta de enlace de capa de aplicación
	🎇 Servicio de restauración de sistema
	🍓 Servicio de transferencia inteligente en segundo plano
	🍓 Servicio de VMware Tools
	🍓 Servicio del administrador de discos lógicos
	🎇 Servicio del número de serie de medio portátil
	🍓 Servicios de cifrado
	🍓 Servicios de Terminal Server
	Servicios IPSEC
	🖏 Servidor
	🆓 Sistema de alimentación ininterrumpida
	🆓 Sistema de sucesos COM+
	🆏 Tarjeta inteligente
	🆓 Telefonía
	🖏 Telnet
	🖏 Temas
	TP AutoConnect Service
	TP VC Gateway Service
	🖏 Windows Installer

Servicios y procesos en ejecución

ex C:\WINDOWS\system32\cmd.exe				
Microsoft Windows XP [Ver (C) Copyright 1985-2001	rsión 5.1 Microsoft	L.2600] t Corp.		
C:\Documents and Setting:	s\Admini:	strador>tasklist		
Nombre de imagen	PID	Nombre de sesión	Núm. de =======	Uso de memor =======
System Idle Process	Ø	Console	0	28 KB
System	4	Console	Ø	244 KB
smss.exe	416	Console	0	352 KB
csrss.exe	652	Console	Ø	2.992 KB
winlogon.exe	676	Console	0	4.232 KB
services.exe	728	Console	Ø	2.932 KB
lsass.exe	740	Console	0	2.424 KB
vmacthlp.exe	912	Console	Ø	1.500 KB
svchost.exe	952	Console	0	3.900 KB
svchost.exe	1028	Console	Ø	3.164 KB
svchost.exe	1124	Console	0	30.084 KB
svchost.exe	1236	Console	Ø	3.016 KB
svchost.exe	1456	Console	0	3.300 KB
explorer.exe	1508	Console	Ø	25.100 KB
spoolsv.exe	1672	Console	0	4.108 KB
svchost.exe	1152	Console	Ø	3.112 KB
vmtoolsd.exe	1192	Console	0	6.012 KB
VMUpgradeHelper.exe	1804	Console	Ø	3.340 KB
UMwareTray.exe	1752	Console	0	3.252 KB
VMwareUser.exe	1440	Console	Ø	8.268 KB
ctfmon.exe	984	Console	0	3.332 KB
svchost.exe	2396	Console	Ø	3.084 KB
wuauclt.exe	2296	Console	Ø	13.160 KB
wuauclt.exe	3452	Console	Ø	4.584 KB
wmiprvse.exe	1224	Console	0	6.596 KB
cmd.exe	2368	Console	Ø	2.748 KB
tasklist.exe	2324	Console	Ø	4.392 KB

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.

Jtilidad de configura	ción del sistema	
eneral SYSTEM.INI \	WIN.INI BOOT.INI Servicios	Inicio Herramientas
Elemento de inicio	Comando	Ubicación
🖾 VMwareTray	"C:\Archivos de progra	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersi
VMwareUser	"C:\Archivos de progra	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersi
🗹 msnmsgr	"C:\Archivos de progra	HKCU\SOFTWARE\Microsoft\Windows\CurrentVers
🗹 GoogleUpdate	"C:\Documents and Se	HKCU\SOFTWARE\Microsoft\Windows\CurrentVers
🗹 ctfmon	C:\WINDOWS\system	HKCU\SOFTWARE\Microsoft\Windows\CurrentVers

Programas ejecutados en el sistema

🂐 Windows File Analyzer - [PA - Prefetch]				_ 8 ×
👻 File Windows Help					Minimizar
🚺 PA - Prefetch					
Prefetch Analysis Directory: C:WINDOWS\Prefetch Volume serial: F459-E600 Volume label:				ļ	Report
Application	Created	Written 🔺	Last Accessed	Embedded Date	Runs Fi
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_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
STG88.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 TrueCrypt¹ 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 Stream² (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.

¹TrueCrypt 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.

²Característica 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.

E:\lads>LADS c: /S	-
LADS - Freeware version 4.10 (C) Copyright 1998-2007 Frank Heyne Software (http://www.heysoft.de) This program lists files with alternate data streams (ADS) Use LADS on your own risk!	
Scanning directory C:\ with subdirectories	
size ADS in file	
Error 32 opening C:\Documents and Settings\Administrador\Configuracian local\Da os de programa\Microsoft\Windows\UsrClass.dat Error 32 opening C:\Documents and Settings\Administrador\Configuracian local\Da os de programa\Microsoft\Windows\UsrClass.dat.LOG 25214 C:\Documents and Settings\Administrador\Favoritos\Výnculos\Sitios s geridos.url:favicon 24 C:\Documents and Settings\Administrador\Mis documentos\Mi m·sica\La	t u
319488 C:\Documents and Settings\Administrador\Mis documentos\Mis imβgenes Scarface.jpg:oculto	1
Error 32 opening C:\Documents and Settings\Administrador\ntuser.dat.LOG Error 32 opening C:\Documents and Settings\LocalService\Configuracian local\Data s de programa\Microsoft\Windows\UsrClass.dat Error 32 opening C:\Documents and Settings\LocalService\Configuracian local\Data s de programa\Microsoft\Windows\UsrClass.dat.LOG Error 32 opening C:\Documents and Settings\LocalService\NTUSER.DAT Error 32 opening C:\Documents and Settings\LocalService\NTUSER.DAT Error 32 opening C:\Documents and Settings\LocalService\Configuracian local\Data Error 32 opening C:\Documents and Settings\LocalService\Configuracian local\Data Error 32 opening C:\Documents and Settings\LocalService\Configuracian local\D tos de programa\Microsoft\Windows\UsrClass.dat Error 32 opening C:\Documents and Settings\NetworkService\Configuracian local\D tos de programa\Microsoft\Windows\UsrClass.dat Error 32 opening C:\Documents and Settings\NetworkService\Configuracian local\D tos de programa\Microsoft\Windows\UsrClass.dat.LOG Error 32 opening C:\Documents and Settings\NetworkService\NTUSER.DAT Error 32 opening C:\Documents and Settings\NetworkService\NTUSER.DAT Error 32 opening C:\Documents and Settings\NetworkService\NTUSER.DAT Error 32 opening C:\Documents and Settings\NetworkService\ntuser.dat.LOG Error 32 opening C:\WINDOWS\system32\CatRoot2\edb.log Error 32 opening C:\WINDOWS\system32\CatRoot2\edb.log Error 32 opening C:\WINDOWS\system32\catRoot2\edb.mp.edb Error 32 opening C:\WINDOWS\system32\config\default.LOG Error 32 opening C:\WINDOWS\system32\config\SAM Error 32 opening C:\WINDOWS\system32\config\SAM Error 32 opening C:\WINDOWS\system32\config\SAM Error 32 opening C:\WINDOWS\system32\config\SECURITY Error 32 opening C:\WINDOWS\system32\config\SECURITY.LOG	o D a
Error 32 opening C:\WINDOWS\system32\config\software	-

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.



Se procede rápidamente a ejecutar el archivo recuperado

Please enter the password required to open this document. Password:	winhex Recuperado.exe Steganos LockNot Steganos GmbH
OK Cancel	

Se encuentra que se trata de un programa denominado SteganosLockNote⁴, nuevamente si hacemos la consulta en Google dice

³Ejecutable 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.

rección 📄 Resultado de la búsqueda			💌 🔁 I
ıscar ×	Nombre	En la carpeta	Tamaño
k A	🔄 💽 La verdad.mp3	C:\Documents and Settings\Administrador\Mis docu	4.714 KB
ς Nuevo 🤣	NTUSER.DAT	C:\Documents and Settings\Administrador	1.024 KB
	🖬 🖬 favorito	C:\Documents and Settings\Administrador\Favoritos	5.120 KB
Discos duros locales (L:)	5.tmp	C:\Documents and Settings\Administrador\Temp	1.023 KB
	🕼 🕼 IconCache.db	C:\Documents and Settings\Administrador\Configur	2.617 KB
Buscar ahora Detener	👘 vmmsi.log_20091215_02	C:\Documents and Settings\Administrador\Configur	3.417 KB
Deciones de búsqueda 77	👫 IrfanView_Wallpaper.bmp	C:\Documents and Settings\Administrador\Datos d	1.407 KB
	Common.cab	C:\Documents and Settings\Administrador\Configur	1.460 KB
🗖 Fecha	👔 🛅 Help.cab	C:\Documents and Settings\Administrador\Configur	1.190 KB
🗖 Tipo	🚽 🚰 instmsi2k.exe	C:\Documents and Settings\Administrador\Configur	1.780 KB
✓ Tamaño	instmsiw.exe	C:\Documents and Settings\Administrador\Configur	2.526 KB
	Micros~1.cab	C:\Documents and Settings\Administrador\Configur	3.072 KB
al menos 🗾 1000 🚔 KB	🛛 👘 VMware Tools.msi	C:\Documents and Settings\Administrador\Configur	12.077 KB
🔽 Opeienes auanzadas	VMware Tools64.msi	C:\Documents and Settings\Administrador\Configur	17.984 KB
	explorer.exe	C:\WINDOWS	1.606 KB
Buscar en carpetas de sistema	SET3.tmp	C:\WINDOWS	1.218 KB
Buscar archivos y carpetas ocultos	SET4.tmp	C:\WINDOWS	1.064 KB
Russer en subezretas	🙀 🐭 xul. dll	C:\Archivos de programa\Mozilla Firefox	10.503 KB
I → Buscal en subcalpetas	📄 🦢 msoe.dll	C:\Archivos de programa\Outlook Express	1.285 KB
Distinguir mayúsculas de minúscula	🔛 🦢 msoeres.dll	C:\Archivos de programa\Outlook Express	2.457 KB
🗖 Buscar en cinta de copia de segur	🔯 wmnetmgr.dll	C:\WINDOWS\\$NtUninstallKB952069_WM9\$	1.029 KB
	wmvcore.dll	C:\WINDOWS\\$NtUninstallKB952069_WM9\$	2.060 KB
Los <u>servicios de Index Server</u> están	🔯 mstscax.dll	C:\WINDOWS\\$NtUninstallKB956744\$	2.014 KB
	🚽 🦢 kernel32.dll	C:\WINDOWS\\$NtUninstallKB959426\$	1.019 KB
3uscar otros elementos:	wmvcore.dll	C:\WINDOWS\\$NtUninstallKB968816_WM9\$	2.124 KB
Archivos o carpetas	wmvcore.dll.000	C:\WINDOW5\\$NtUninstallKB968816 WM9\$	2.124 KB

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.

AccessData FTK Imager 2.9.0.1385	_ Ø 2
File View Mode Help	
E Datos de programa	Name Size Type Date Modified
Entorno de red Escritorio Escritorio Formaticache ETIdCache IETIdCache	Sitios web de Microsoft 1 KB Directory 20/12/2009 0:1 Vínculos 1 KB Directory 20/12/2009 0:5 \$\vec{1}\$ \$130 4 KB NTFS Index Allo 20/12/2009 0:5 \$\vec{1}\$ Desktop.ini 1 KB Regular File 15/12/2009 7:4 \$\vec{1}\$ Pasktop.ini 1 KB Regular File 20/12/2009 2:5
Henú Inicio Henú Inicio Henú Inicio Henú Inicio Henú Inicio His documentos Pirvatlas Pirvatle Reciente For SendTo Henú Temp	
Custom Content Sources X	
Evidence:File System Path File Options	
	$ \begin{array}{c} 000010 & 01 & 56 & b2 & 27 & 36 & 91 & 10 & -43 & 7A & b1 & b6 & 2.56 & ct & bb & \sqrt{4} \times 74 \times $
New Edit Remove Remove All Greate Image	000060 FE 9D AA 3E 19 66 CD 56-D4 97 7E 1B 5E 9C 48 52 b·*> ffv0···· 000070 C6 FF 17 6A 68 93 BA AF-9D D4 28 C1 B1 7B 97 7B Æÿ-jh·°¯·Ô(Á= 000080 DA 30 AC CA 15 5D C4 5B-B8 29 93 98 8F 71 70 65 ÚO-Ê·JĂ[.)···
Properties Hex Value Inter Custom Content	Cursor pos = 0: clus = 322357: log sec = 2578856: pby sec = 2578912
VENUES OF THE PARTY OF THE PART	root//Documents and Sattings/Administrador/Eavoritos/Eavorito

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.

REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ	(valor no establecido) C:\WINDOWS\\$NtUninst C:\Documents and Settin C:\Documents and Settin Z:\sexy (1).jpg Z:\sexy (2).jpg xy (3).jpg xy (4).jpg xy (5).jpg
REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ	C:\WINDOWS\\$NtUninst C:\Documents and Settir C:\Documents and Settir Z:\sexy (1).jpg Z:\sexy (2).jpg ? X (3).jpg xy (4).jpg xy (5).jpg
REG_SZ REG_SZ REG_SZ REG_SZ	C:\Documents and Settir C:\Documents and Settir Z:\sexy (1).jpg Z:\sexy (2).jpg ? x (3).jpg xy (4).jpg xy (5).jpg
REG_SZ REG_SZ REG_SZ	C:\Documents and Setti Z:\sexy (1).jpg Z:\sexy (2).jpg ? x (3).jpg xy (4).jpg xy (5).jpg
REG_SZ REG_SZ	Z:\sexy (1).jpg Z:\sexy (2).jpg ? X xy (3).jpg xy (4).jpg xy (5).jpg
REG_SZ	Z:\sexy (2).jpg xy (3).jpg xy (4).jpg xy (5).jpg
	? × (3).jpg xy (4).jpg xy (5).jpg
	xy (4), jpg xy (5), jpg
	xy (5), jpg
	pcuments and Settir
	pcuments and Setti
	Hajbic
\$\spuninst\TrueCr	ypt.exe
Aceptar C	Jancelar
110 C.	
	\$\spuninst\TrueCr Aceptar C

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.



umes	System	Keyfiles	Tools Set	tings Help				Home	epag
orive M:	Volume				Siz	e Encryption	algorithm	Туре	1
N: O: P:									
Q: R: S:									
► 1: ►U: ►V:									
X: Y:									
Z:									
	Create Vo	olume	J	Volume	Properties		Wipe	Cache	
/olume	, 						Calari		
	<u>م</u>	Never sa	ve history		Volume T	ools	Select I	Device	
					- 12	-1284			-

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
📾 caBctuv2F0m3ImInV+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+UbIvZLlOCB4bjr930k2+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
PPf14mSRIIi3AW2khD89XlbrEQ4=	1 KB	Archivo	19/12/2009 21:19
📷 rqGksW+2F8wfzUh1HZlpBKE2Fam3k=	6 KB	Archivo	19/12/2009 21:19
🔤 UZqGVwSl7zIc5syYGmgiq4tGCyw=	2 KB	Archivo	19/12/2009 21:22
🔟 vye5j5XLS7iep8OnLR6O0tdukBU=	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.

+t72FMT	RoauaCqxZtpzSu	3QD0r	PM=															
istriert]	Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
+t72FN	00000000	FF	D8	FF	EO	00	10	4 A	46	49	46	00	01	01	01	00	60	ÿØÿà JFIF `
H:\Me	00000016	00	60	00	00	FF	DB	00	43	00	10	0B	0C	0E	0C	0A	10	`ÿÛ C
	00000032	0E	0D	0E	12	11	10	13	18	28	14	18	16	16	18	31	23	(1#
File Kill	00000048	25	1D	28	3A	33	3D	3C	39	33	38	37	40	48	5C	4E	40	% (:3=<9387@H\N@
?bytes	00000064	44	57	45	37	38	50	6D	51	57	5F	62	67	68	67	3E	4D	DWE78PmOW baha>M

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 *"leHistory"* que sirve para ver el historial de Internet Explorer.

dex.dat file location			
C:\Documents and Settings\Administrador\Configura	ación local\Archivos temporales de Interr	et\Content.IE5\	Browse

E History Manager 1.0	
File Edit View Help	
Address Bar Cookies URLs History Index.dat Au	utoComplete
URL	Last Modified
💊 https://ieonline.microsoft.com/favicon.ico	19/12/2009 19:55:10
🔍 http://www.microsoft.com/spain/windows/Framework/Controls/Windows	19/12/2009 19:55:13
💫 http://www.google.es/images/nav_logo7.png	19/12/2009 19:55:30
💫 http://www.google.com.co/images/dl_btn_left.gif	19/12/2009 21:08:44
💫 http://col.stb.s-msn.com/i/1E/592BCB98B8663F21E28E5BAC21232.png	19/12/2009 22:15:27
💫 http://www.gowindowslive.com/Messenger/Wave3MessengerHighlights	15/12/2009 3:51:40
💫 http://www.gowindowslive.com/Messenger/Wave3MessengerHighlights	15/12/2009 3:51:43
💫 http://img1.catalog.video.msn.com/image.aspx?uuid=5bb78ff8-2e35-4bb	19/12/2009 0:37:52
💫 http://www.microsoft.com/spain/windows/Framework/js/core.js	19/12/2009 19:55:07
ktp://www.fondosgratis.com.mx/archivos/items/th_1173403443_alienw	19/12/2009 23:22:08
$ ightarrow$ http://images.google.com.co/intl/es_co/images/logos/images_logo.gif	19/12/2009 21:08:54
💫 http://s2.imgsrc.ru/r/ranma/3/15232753VYS.jpg	19/12/2009 21:26:59
💫 http://img3.catalog.video.msn.com/image.aspx?uuid=e3510626-27f6-480	15/12/2009 9:32:03
💫 http://www.bing.com/partner/primedns.gif	19/12/2009 1:11:00
💫 http://db2.stc.s-msn.com/br/hp/v12/es-es/css/i/media_icon_msgboard	19/12/2009 1:11:15
💫 http://db2.stc.s-msn.com/br/hp/v12/es-es/css/i/rss.gif	19/12/2009 1:11:15
💫 http://pagead2.googlesyndication.com/pagead/js/graphics.js	19/12/2009 19:55:37
💫 http://www.fondosgratis.com.mx/archivos/items/th_1177455704_firefox1	19/12/2009 23:22:08
💫 http://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-49588056	19/12/2009 19:56:47
💫 res://ieframe.dll/noaddon.png	19/12/2009 19:54:34
💫 http://fpdownload2.macromedia.com/get/shockwave/cabs/flash/swflas	19/12/2009 21:04:00
http://ads1.msads.net/ads/94160/0000094160_000000000000006926	19/12/2009 21:05:22
ktp://i201.photobucket.com/albums/aa270/pbozzolo/beta-verde-azul2	19/12/2009 21:07:01
💫 http://images.google.com.co/images/nav_logo7.png	19/12/2009 21:08:54
A http://s3.imgsrc.ru/s/scarface123/1/16307291kFd.jpg?1261276595	19/12/2009 21:35:14
💫 http://col.stb.s-msn.com/i/D7/50E594E19ED8C6BB1AF379CB0F059.gif	19/12/2009 22:15:30

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:

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



Escandalo en High School Musical por fotos desnuda de Vanessa Hudgens





Un nuevo escándalo de ribetes sexuales sacude a la franquicia High School Musical: luego de que una participante de la selección para la versión argentina del telefilme fuera separada del casting por la aparición de un video porno suyo en Internet, ahora corre el rumor de que muy pronto se conocerían en todo el mundo unas fotos que Vanessa Hudgens se habría sacado para su novio Zac Efron en las que aparece sin ropa.

Según informa el periódico sensacionalista estadounidense Nacional Enquirer, las imágenes muestran a "Gabrielle" autorretratándose con su teléfono celular frente a un espejo, solo ataviada con una cadena de oro alrededor de su cintura. Se suponía que sólo su novio y compañero de trabajo Zac las vería, pero al parecer cayeron en manos de una

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

🔇 💽 - C 🗙 🍙 🛐 🚺 http://in	ngsrc.ru/main/login.php 🏠 🚽 🚱 Google 🗸
🔊 Más visitados わ Comenzar a usar Firefox <u> </u> Últir	nas noticias
iMGSRC.RU Free photo hosting!	
iMGSRC.RU	login, upload your photos!
	join free search more users FAQ русский
Members login:	Not yet a member?
Username: Password: login register now FREE	Be a part of the 274000 users community - join iMGSRC.RU FREE right here, right now! It only takes a minute and requires a single working email - no registration ever was so easy. Register now to access all the fun stuff, simply fill form below.
 Cookies must be enabled. Password is CaSeSeNsItIvE. More help available in our FAQ. 	email:
Forgotten your password? Username or e-mail: remind me a password	email, because in case this email account is overloaded, blocked or is in any other way inaccessible by our mailer (eg. because of faulty spam protection), you will not be able to get your password to work with the iMGSRC.RU. We will not spam you so have no worries.
	Attention AOL users: AOL treats any iMGSRC.RU emails as spam, thus preventing you from receiving them.
	Login:
	Choose your username (login). Please use only english letters and numbers, from 4 to 16 characters.
	Check input and continue

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*".

🔇 💽 🗸 🟠 🥘 🦲 http://imgsrc.ru/main/user.php?user=scarface12 🗟 🏫 🕤 🔀 Google 💦											
🧕 Más visitados 🀢 Comenzar a usar Firefox 🔜 Últimas notici	as										
iMGSRC.RU albums of SCARFACE123 +											
iMGSRC.RU Albums of	iMGSRC.RU Albums of login, upload your										
SCARFACE123					photos!						
				r	join free search more users FAQ русский						
Email: hidden, contact via Registered on: 2009-12-20	comme	nts									
Albums of scarface123 (2) 🔊 🖸 SHARE :											
Albums of scarface123 (2) 🔊 🖸 SHARE : name 🛦 🔻 (show album previews)	photos	in section 🔺 🔻	pageviews*	comm	modified 🔺 🔻						
Albums of scarface123 (2) SHARE : name A V (show album previews) Princesa (password protected)	photos 4	in section ▲ ▼ nudity	pageviews* 5+138	comm 0	modified ▲ ▼ 2009-12-20 05:36:35						
Albums of scarface123 (2) SHARE : name ▲ ▼ (show album previews) Princesa (password protected) Otra Pendeja (password protected)	photos 4 5	in section ▲▼ nudity nudity	pageviews* 5+138 2+142	<u>comm</u> 0 0	modified ▲ ▼ 2009-12-20 05:36:35 2009-12-20 07:39:41						

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

🔇 🖂 C 🗙 🏠 🥘 🦳 http://imgsrc.ru/main/join.php?ema	ail=scarface1fisic 🏠 📲 🎖 Google 🛛 🧳
🖉 Más visitados 🌮 Comenzar a usar Firefox 🔊 Últimas noticias	
iMGSRC.RU Host your photos in no ti +	
iMGSRC.RU Host your photos in no	login, upload your
time!	photos!
Welcome to fast and completely FREE web photo hosting	join free search more users FAQ русский
iMGSRC.RU registration, step 1	
storage for your pictures, will be allowed to com registered and also will have all the fun of <u>free phot</u> email:	in get an <u>unimited</u> hosting imunicate with users already osharing.
This is <u>required</u> to be a valid email - iMGSRC.RU will send you a new password to login	1 and post your photos.
email: scaface fisica@hotmail. this email is already used on iMGSRC.RU. Only 1 a	account per email.
Please use a nice valid email, because in case this email account is overloaded, blocked or because of faulty spam protection), you will not be able to get your password to work w Attention AOL users: AOL treats any iMGSRC.RU emails as spam, thus preventing y	is in any other way inaccessible by our mailer (eg. rith the service. ou from receiving them.
Choose your username (login):	
Login name should be at least 4 characters long. Use <u>only</u> letters and numbers.	
Login: scafface123	

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.



iMGSRC.RU Princesa

login, upload your photos!



"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.

💱 IE History Manager 1.0
File Edit View Help
Address Bar Cookies URLs History Index.dat AutoComplete Befresh
URLjü
about:Home file:///C:/Documents%20and%20Settings/Administrador/Mis%20documentos/Mi%20m%FAsica/La%20verdad.mp3 file:///C:/Documents%20and%20Settings/Administrador/Mis%20documentos/Mis%20im%E1genes/lunar.jpg file:///C:/Documents%20and%20Settings/Administrador/Mis%20documentos/Mis%20im%E1genes/lunar.jpg file:///C:/Documents%20and%20Settings/Administrador/Mis%20documentos/Mis%20im%E1genes/pijamada1.jpg file:///C:/Documents%20and%20Settings/Administrador/Mis%20documentos/Mis%20im%E1genes/pijamada2.gif file:///C:/Documents%20and%20Settings/Administrador/Mis%20documentos/Mis%20im%E1genes/pijamada3.jpg file:///C:/Documents%20and%20Settings/Administrador/Mis%20documentos/Mis%20im%E1genes/pijamada3.jpg file:///C:/Documents%20and%20Settings/Administrador/Mis%20documentos/Mis%20im%E1genes/Scafface.jpg file:///C:/Documents%20and%20Settings/Administrador/Mis%20documentos/Mis%20im%E1genes/Scafface.jpg file:///C:/Documents%20and%20Settings/Administrador/Mis%20documentos/Mis%20im%E1genes/sexy%20[1].jpg file:///C:/Documents%20and%20Settings/Administrador/Mis%20documentos/Mis%20im%E1genes/sexy%20[2].jpg file:///C:/Documents%20and%20Settings/Administrador/Mis%20documentos/Mis%20im%E1genes/sexy%20[3].jpg file:///C:/Documents%20and%20Settings/Administrador/Mis%20documentos/Mis%20im%E1genes/sexy%20[4].jpg file:///C:/Documents%20and%20Settings/Administrador/Mis%20documentos/Mis%20im%E1genes/sexy%20[4].jpg file:///C:/Documents%20and%20Settings/Administrador/Mis%20documentos/Mis%20im%E1genes/sexy%20[6].jpg file:///C:/Documents%20and%20Settings/Administrador/Mis%20documentos/Mis%20im%E1genes/sexy%20[6].jpg file:///C:/Documents%20and%20Settings/Administrador/Mis%20documentos/Mis%20im%E1genes/sexy%20[6].jpg file:///C:/Documents%20and%20Settings/Administrador/Mis%20documentos/Mis%20im%E1genes/sexy%20[6].jpg file:///C:/Documents%20and%20Settings/Administrador/Mis%20documentos/Mis%20im%E1genes/sexy%20[6].jpg file:///C:/Documents%20and%20Settings/Administrador/Mis%20documentos/Mis%20im%E1genes/sexy%20[6].jpg file:///C:/Doc
http://mp3.hhgroups.com/Material/Maquetas/1524/08. Porta - Las ninas unas guarras pero los tios unos cerdos [con May] - ww http://mp3.hhgroups.com/Material/Maquetas/559/09. Porta - las ninyas de hoy en dia todas son unas www.HHGroups.com

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.

	🗢 🙋 C:\Do	ocuments and	Settings\Adminis	strador\Configuració	ón local\Arct 💌 😏 🗙 🧯
Archivo	Edición Ver	Favoritos	Herramientas	Ayuda	
🔆 Favor	ritos 🛛 🝰 🏉	Sitios sugerio	los 🔹 🙋 Galeri	ia de Web Slice 🝷	
🤏 iMGSI	RC.RU Princesa	on .iMGSRC.R	U		🏠 • 🗟 • 🖻

Информация об альбоме:

Name:	Princesa
Password:	scarface
Comments:	only allow iMGSRC.RU registered users with photos to
In section:	nudity
Preword (description):	pendejita que me envio sus fotos pensando que ese lunar tenia cancer jejejeje
Comma separated tags:	
Download whole album:	Only available for albums with 12+ photos.
	Save album information

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.

iMGSRC.RU Otra Pendeja

login, upl



iMGSRC.RU Princesa



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.

scartace1fisica@hotm	
Band. entrada (1)	Responder Responder a todos Reenviar 🎩 🏠
Correo no deseado Borradores Enviados Eliminados Administrar carpetas Agregar una cuenta de correo electrónico	iMGSRC.RU registration De: iMGSRC.RU (admin@iMGSRC.RU) Es posible que no conozcas a este remitente. Marcar como seguro Marcar como correo no deseado Enviado: sábado, 19 de diciembre de 2009 09:30:02 p.m. Para: scarface123 (scarface1fisica@hotmail.com)
Lugares relacionados Hoy Lista de contactos	iMGSRC.RU registration data: login: scarface123 password: J9FVB779

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.

36

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

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

0446281760 0000; ">pues en esta foto no aparece muy bien el lunar</Text></Message><Message 0446281840 Date="19/12/2009" Time="21:20:44" DateTime="2009-12-20T02:20:44.4422" SessionID= 0446281920 "2"><From><User FriendlyName="Scarface"/></From><To><User FriendlyName="Natalia" 0446282000 /></To><Text Style="font-family:Segoe UI; color:#000000; ">no puedo ver el conto 0446282080 | rno</Text></Message><Message Date="19/12/2009" Time="21:20:52" DateTime="2009-12 0446282160 -20T02:20:52.833Z" SessionID="2"><From><User FriendlyName="Scarface"/></From><To

0446277840 | font-family:Segoe UI; color:#000000; ">pueden ser peligroso</Text></Message><Mes 0446277920 | sage Date="19/12/2009" Time="21:16:08" DateTime="2009-12-20T02:16:08.8952" Sessi 0446278000 onID="2"><From><User FriendlyName="Scarface"/></From><To><User FriendlyName="Nat 0446278080 alia"/></To><Text Style="font-family:Segoe UI; color:#000000; ">podria ser cance 0446278160 r</Text></Message><Message Date="19/12/2009" Time="21:16:15" DateTime="2009-12-2" 0446278240 0T02:16:15.3332" SessionID="2"><From><User FriendlyName="Natalia"/></From><To><U 0446278320 ser FriendlyName="Scarface"/></To><Text Style="font-family:Segoe UI; color:#0000 0446278400 00; ">SI?????</Text></Message><Message Date="19/12/2009" Time="21:16:22" DateTim 0446278480 e="2009-12-20T02:16:22.833Z" SessionID="2"><From><User FriendlyName="Natalia"/>< 0446278560 /From><To><User FriendlyName="Scarface"/></To><Text Style="font-family:Segoe UI; 0446278640 color:#000000; ">que miedo</Text></Message><Message Date="19/12/2009" Time="21: 0446278720 16:29" DateTime="2009-12-20T02:16:29.8642" SessionID="2"><</pre>From><User FriendlyNam 0446278800 | e="Natalia"/></From><To><User FriendlyName="Scarface"/></To><Text Style="font-fa 0446278880 mily:Segoe UI; color:#000000; ">: (</Text></Message><Message Date="19/12/2009" Ti 0446278960 me="21:16:49" DateTime="2009-12-20T02:16:49.7392" SessionID="2"><From><User Frie 0446279040 ndlyName="Scarface"/></From><To><User FriendlyName="Natalia"/></To><Text Style=" 0446279120 font-family:Segoe UI; color:#000000; ">si, un tipo de cancer de piel, que da por 0446279200 | la exposicion a los rayos del sol</Text></Message><Message Date="19/12/2009" Ti 0446279280 me="21:17:04" DateTime="2009-12-20T02:17:04.348Z" SessionID="2"><From><User Frie 0446279360 ndlyName="Scarface"/></From><To><User FriendlyName="Natalia"/></To><Text Style="

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

1651909920 o· ·p·a·r·a· ·q·u·e· ·s·e·p·a·s· ·q·u·i·e·n· ·s·o·y···C·a·m·i·l·a· ·d·i·c·e·:··· 1651910000 üÿQ·U·I·E·N· ·L·E· ·D·I·O· ·E·S·A· ·F·O·T·O·!·!·!···üÿe·s·o· ·e·s· ·p·r·i·v·a·d· 1651910080 o···üÿd·e· ·u·n·a· ·p·i·j·a·m·a·d·a· ·e·n· ·l·a· ·c·a·s·a· ·d·e· ·m·i· ·a·m·i·g· 1651910160 a···üÿ!·!·!·!·!·!·!·!·!·!·!·!·!·!·!·!·····D·I·G·A·M·E· ·Y·A·!·!·!·!·!·!·!·!·!·!·!·!·!·!·!·! 1651910320 p.u.e.s. .q.u.e. .e.r.a. .u.n. .e.s.t.u.p.i.d.o.?...C.a.m.i.l.a. .d.i.c.e.:...üÿ 1651910480 e-r-e-s- -q-u-e- -l-e- -e-n-v-i-e- -e-s-a- -f-o-t-o- -a- -t-o-d-o-s- -t-u-s- -c-1651910560 o·n·t·a·c·t·o·s· ·e·n· ·e·l· ·m·e·s·s·e·n·g·e·r· ·y· ·f·a·c·e·b·o·o·k· ·e·s· ·m· 1651910640 e-j-o-r- -q-u-e- -s-e-a- -M-U-Y- -A-M-I-G-A-B-L-E---C-a-m-i-l-a- -d-i-c-e-:---üÿ 1651910800 a•n•d•a•r•l•e• •e•s•a• •f•o•t•o• •a• •N•A•D•I•E•!•!•!•!••üÿN•A•D•I•E•!•!•!• 1651910880 c.a.r.f.a.c.e. .d.i.c.e.:...üÿp.o.r. .q.u.e. .t.e. .q.u.e.d.a.s. .c.a.l.l.a.d.a. 1651910960 ···C·a·m·i·l·a· ·d·i·c·e·:···ūÿy·a· ·v·a·s· ·a· ·v·e·r·,· ·e·s·t·o·y· ·h·a·c·i·e· 1651911040 n.d.o. .t.o.d.o. .p.a.r.a. .q.u.e. .t.e. .m.e.t.a.n. .a. .l.a. .c.a.r.c.e.l.!.!. 1651911120 /·····S·c·a·r·f·a·c·e· ·d·i·c·e·:···üÿj·a·j·a·j·a·j·a·j·a··üÿn·a·d·i·e· ·m·e· · 1651911200 c.o.n.o.c.e...üÿn.i.s.i.q.u.i.e.r.a. .U.s.t.e.d...C.a.m.i.l.a. .d.i.c.e.:...üÿy. 1651911360 :····üÿs·a·b·e·s· ·q·u·i·e·n· ·e·s· ·c·a·m·i·l·o·2·3·2·0·h·o·t·m·a·i·l·.·c·o·m·?·

1883631600	ϔάὄϔϔϤὄϔϔϤὄϔϔϤϔ;· \a·s·i···üϔe·s· ·m·a·s· ·y·o· ·t·e·n·g·o· ·a·l·g·u·n·a·s·,· ·
1883631680	p.a.r.a.+.L.e.r.x.b.(üb.i.e.ne.lc.u.e.r.p.oN.a.t.a.l.i.ad.i.T.T.:
1883631760	x.b. (ub-p.o.rq.u.ea.v.e.c.e.su.n.an.oa.l.c.a.n.s.aav.e.r.s.
1883631840	e· ·t·o·d·a···üÿm·e· ·h·a· ·p·a·s·a·d·o···üÿt·a·m·b·i·e·n· ·t·e·n·g·o· ·a·l·g·u·
1883631920	n·a·s· ·f·o·t·o·s· ·üÿ··üÿd·e· ·u·n·a· ·p·i·j·a·m·a·d·a· ·c·o·n· ·m·i·s· ·a·m·i·
1883632000	g.a.sS.c.a.r.f.a.c.ed.i.c.e.:üÿq.u.eb.i.e.n., .yt.ee.n.c.o.n.
1883632080	t·r·a·s·t·e· ·a·l·g·o· ·r·a·r·o·?···N·a·t·a·l·i·a· ·d·i·c·e·:···üÿs·i·,· ·m·e· ·
1883632160	e·n·c·o·n·t·r·e· ·u·n· ·l·u·n·a·r· ·n·e·g·r·o· ·e·n· ·l·a· ·e·s·p·a·l·d·a···üÿq·
1883632240	u·e· ·n·o· ·s·a·b·i·a· ·q·u·e· ·t·e·n·i·a···S·c·a·r·f·a·c·e· ·d·i·c·e·:···üÿc·u·
1883632320	i.d.a.d.oc.o.ne.s.o.sl.u.n.a.r.e.süÿp.u.e.d.e.ns.e.rp.e.l.i.g.
1883632400	r.o.s.oüÿp.o.d.r.i.as.e.rc.a.n.c.e.rN.a.t.a.l.i.ad.i.c.e.:üÿs.
1883632480	I.?.?.?.?.?
1883632560	·u·n· ·t·i·p·o· ·d·e· ·c·a·n·c·e·r· ·d·e· ·p·i·e·l·, ·q·u·e· ·d·a· ·p·o·r· ·l·
1883632640	$a\cdot \cdot e\cdot x\cdot p\cdot o\cdot s\cdot i\cdot c\cdot i\cdot o\cdot n\cdot \cdot \cdot a\cdot \cdot l\cdot o\cdot s\cdot \cdot r\cdot a\cdot y\cdot o\cdot s\cdot \cdot d\cdot e\cdot l\cdot \cdot s\cdot o\cdot l\cdot \cdot \cdot \ddot{u}\ddot{y}p\cdot e\cdot r\cdot o\cdot \cdot n\cdot$
1883632720	$\circ \cdot \cdot t \circ \cdot d \cdot \circ \cdot s \cdot \cdot 1 \cdot \circ \cdot s \cdot \cdot 1 \cdot u \cdot n \cdot a \cdot r \cdot e \cdot s \cdot \cdot s \cdot \circ \cdot n \cdot \cdot p \cdot e \cdot 1 \cdot i \cdot g \cdot r \cdot \circ \cdot s \cdot \circ \cdot s \cdot \cdot \cdot N \cdot a \cdot t \cdot a \cdot 1 \cdot u \cdot n \cdot a \cdot r \cdot e \cdot s \cdot \cdot s \cdot \circ \cdot n \cdot a \cdot t \cdot a \cdot 1 \cdot u \cdot n \cdot a \cdot r \cdot e \cdot s \cdot \cdot s \cdot \circ \cdot n \cdot a \cdot r \cdot a \cdot 1 \cdot u \cdot n \cdot a \cdot r \cdot e \cdot s \cdot \cdot s \cdot \circ \cdot n \cdot a \cdot r \cdot a \cdot 1 \cdot u \cdot n \cdot a \cdot r \cdot e \cdot s \cdot \cdot s \cdot \circ \cdot n \cdot a \cdot r \cdot a \cdot 1 \cdot u \cdot n \cdot a \cdot r \cdot e \cdot s \cdot \cdot s \cdot o \cdot n \cdot a \cdot r \cdot a \cdot 1 \cdot u \cdot n \cdot a \cdot r \cdot e \cdot s \cdot \cdot s \cdot \circ \cdot n \cdot a \cdot r \cdot a \cdot 1 \cdot u \cdot n \cdot a \cdot r \cdot e \cdot s \cdot \cdot n \cdot a \cdot r \cdot a \cdot 1 \cdot u \cdot n \cdot a \cdot n \cdot a \cdot r \cdot a \cdot 1 \cdot u \cdot n \cdot a \cdot n \cdot n$
1883632800	i.ad.i.c.e.:üÿyc.o.m.os.es.ie.lm.i.oe.sp.e.l.i.g.r.o.
1883632880	s.oS.c.a.r.f.a.c.ed.i.c.e.:üÿy.ot.e.n.g.oe.x.p.e.r.i.e.n.c.i.a
1883632960	e.ne.s.et.i.p.od.ec.a.n.c.e.rd.ep.i.e.l., .p.o.rq.u.em.
1883633040	e· ·d·i·o· ·e·n· ·u·n· ·b·r·a·z·o·,· ·s·i· ·q·u·i·e·r·e·s· ·m·e· ·m·a·n·d·a·s· ·
1883633120	l.af.o.t.oyt.ed.i.g.os.ie.sd.el.o.sm.a.l.o.son.
1883633200	o···N·a·t·a·l·i·a· ·d·i·c·e·:···üÿm·m·m·,· ·b·u·e·n·o· ·y·a· ·t·e· ·l·a· ·m·a·n·
1883633280	d·o···S·c·a·r·f·a·c·e· ·d·i·c·e·:···üÿh·u·y·,· ·e·r·e·s· ·p·r·e·c·i·o·s·a····üÿy·
1883633360	·t·i·e·n·e·s· ·u·n· ·c·u·e·r·p·o· ·m·u·y· ·l·i·n·d·o····N·a·t·a·l·i·a· ·d·i·c·e·
1883633440	:···üÿb·o·b·o·,· ·m·i·r·a· ·e·l· ·l·u·n·a·r·,· ·e·l· ·l·u·n·a·r·!·!·!··S·c·a·r·
1883633520	f.a.c.ed.i.c.e.:üğj.e.j.e.j., .b.u.e.n.oüğp.u.e.se.ne.s.t.af.
1883633600	$\circ \cdot \cdot \circ \cdot \circ$
Cursor pos = 18	383631620; clus = 459871; log sec = 3678968

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.

Steganos LockNote	×	📄 Recuperado - Steganos Lock	Note 💶 🗵 🗙
T		File Edit Help	
Please enter the password required to	open this document.	http://ingsrc.ru/ Scarface1980 J9FVB779	4
Password: •••••	•••••		-
			11
	OK Cancel		
		1	
🗄 🔝 UnxUtils			
	Recuperado.exe		
	Stedabos LockMon	8	

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.

lumes	System	Keyfiles	Tools	Settings	Help				Home	enad
James	System	Reynies	10013	bottings	Theip	04			Home	spag
Drive	Volume					Siz	e Encrypt	tion algorithm	Туре	-
<₽M:										
🥯 N:										
••O:										
See 19										
Q;										
- R:										
14# T:										
₩U: :>:U:										
- U										
œ₩: œv:										
≪W: ≪X: ≪Y:										
W: X: Y: Z:	C:\Docu	ments and	Setting	s\Administ	r\favor	ito 4.8 №	IB Twofish	n-Serpent	Normal	-
W: X: Y: Z:	C:\Docu	ments and	Setting	s\Administ	r\favor	ito 4.8 M	IB Twofish	n-Serpent	Normal	
₩: X: Y: Z:	C:\Docu	ments and	Setting	s\Administ	r\favor	ito 4.8 M	IB Twofish	n-Serpent	Normal	
W: X: Y: Z:	C:\Docu	ments and	Setting	s\Administ	r\favor	ito 4.8 M	B Twofish	n-Serpent	Normal	_
W: X: Y: Z:	C:\Docu Create Vo	ments and	Setting:	s\Administ	r\favor Volume P	ito 4,8 M roperties	IB Twofish	n-Serpent	Normal : Cache	_
W: X: Y: Z:	C:\Docu Create Vo	ments and	Setting:	s\Administ	r\favor Volume P	ito 4,8 M roperties	IB Twofish	n-Serpent	Normal : Cache	_
W: X: Y: Z:	C:\Docu Create Vo	ments and		s\Administ	r\favor Volume P	ito 4,8 M roperties	IB Twofish	n-Serpent	Normal : Cache	
W: X: Y: Z:	C:\Docu Create Vo e	ments and blume :\Documer	Setting:	s\Administ	r\favor Volume P dministra	ito 4.8 M roperties dor\Favoritos\	B Twofish	n-Serpent	Normal Cache	
V: Y: Z: Volume	C:\Docu Create Vo e	ments and olume :\Documer	Setting:	s\Administ	r\favor Volume P dministra	ito 4.8 M roperties dor\Favoritos\	B Twofish	-Serpent	Normal Cache t File	
Volume	C:\Docu Create V(e Create V	ments and blume :\Documer Never sa	Setting:	s\Administ	r\favor Volume P dministra	ito 4.8 M roperties dor\Favoritos\ Volume T	B Twofish	-Serpent Wipe	Normal Cache t File	
Volume	C:\Docu Create Vi e	ments and olume :\Documer Never sa	Setting:	s\Administ 	r\favor Volume P dministra	ito 4.8 M roperties dor\Favoritos\ Volume T	B Twofish	n-Serpent Wipe	Normal : Cache :t File Device	
Volume	C:\Docu Create Vi e	ments and olume :\Documer Never sa	Setting:	s\Administ	r\favor Volume P dministra	ito 4.8 M roperties dor\Favoritos\ Volume T	B Twofish	-Serpent Wipe Select	Normal Cache t File Device	· · · · · · · · · · · · · · · · · · ·

C:\WINDOWS\\$NtUninstallKB954155_WM9\$\spuninst

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
 - o 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.

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

Herramientas Utilizadas

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/