Casos prácticos

Análisis Forense de Sistemas Informáticos

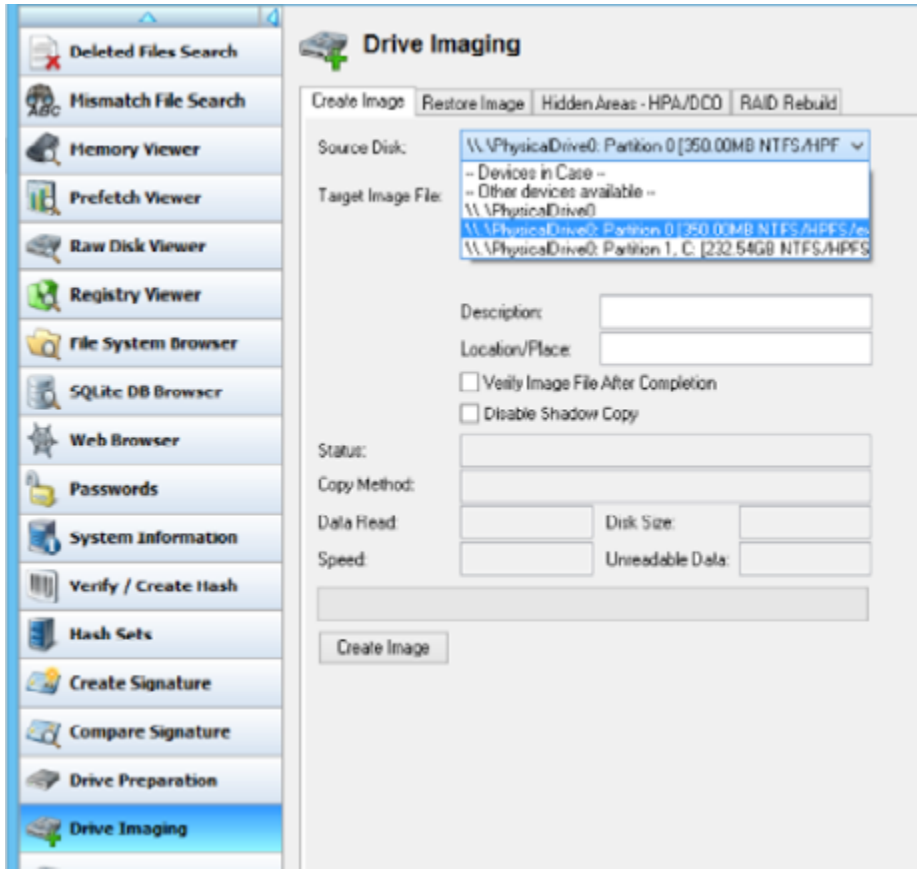
Telefónica EDUCACIÓN DIGITAL

Casos prácticos

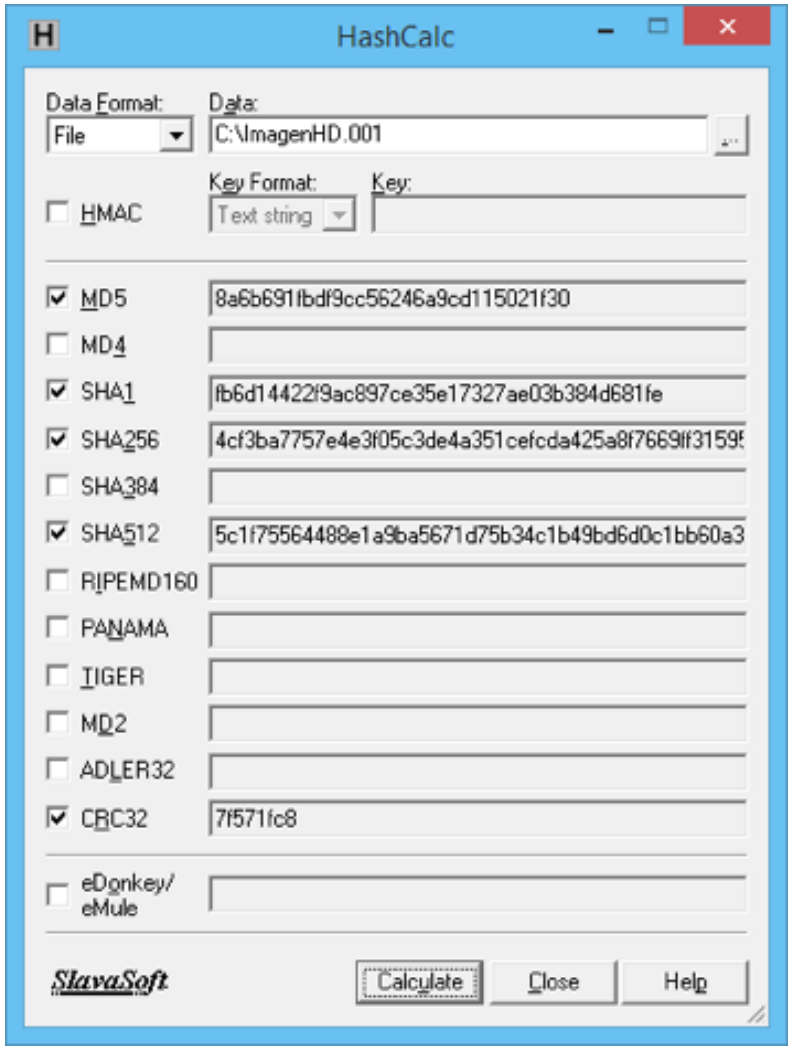
1 | Realizar la adquisición de un disco con sistema Windows mediante alguna de las herramientas vistas. Calcular el hash de la imagen obtenida.

A través de alguna de las distintas herramientas que hemos visto, podemos realizar la adquisición de un disco. Todo dependerá de si tenemos acceso físico o no al dispositivo o si, además, lo debemos realizar en vivo (en caliente) o no.

Podemos utilizar OSForensics como se muestra en la siguiente imagen.

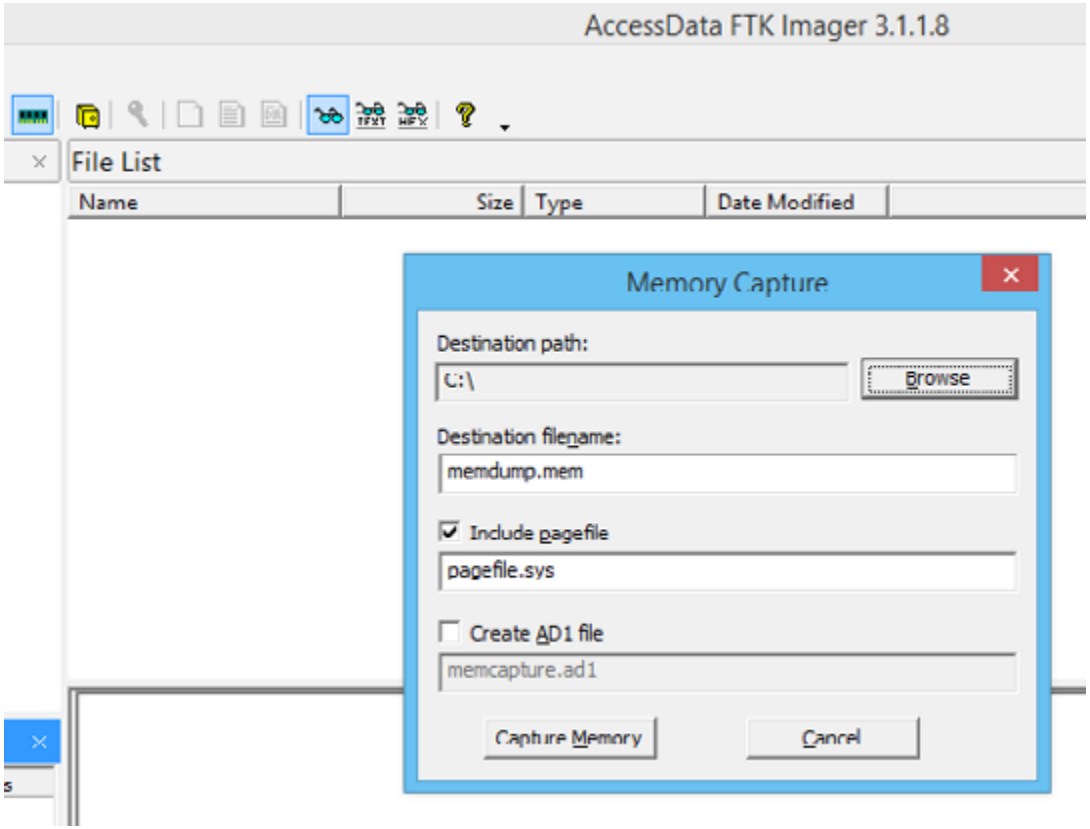


Para el cálculo del hash, podemos utilizar la misma herramienta que viene con OSForensics o utilizar una externa como HashCalc.



2 | Realizar el volcado de la memoria RAM con alguna de las herramientas vistas.

Podemos utilizar FTK Imager para poder realizar el volcado de memoria de una máquina como se muestra a continuación:

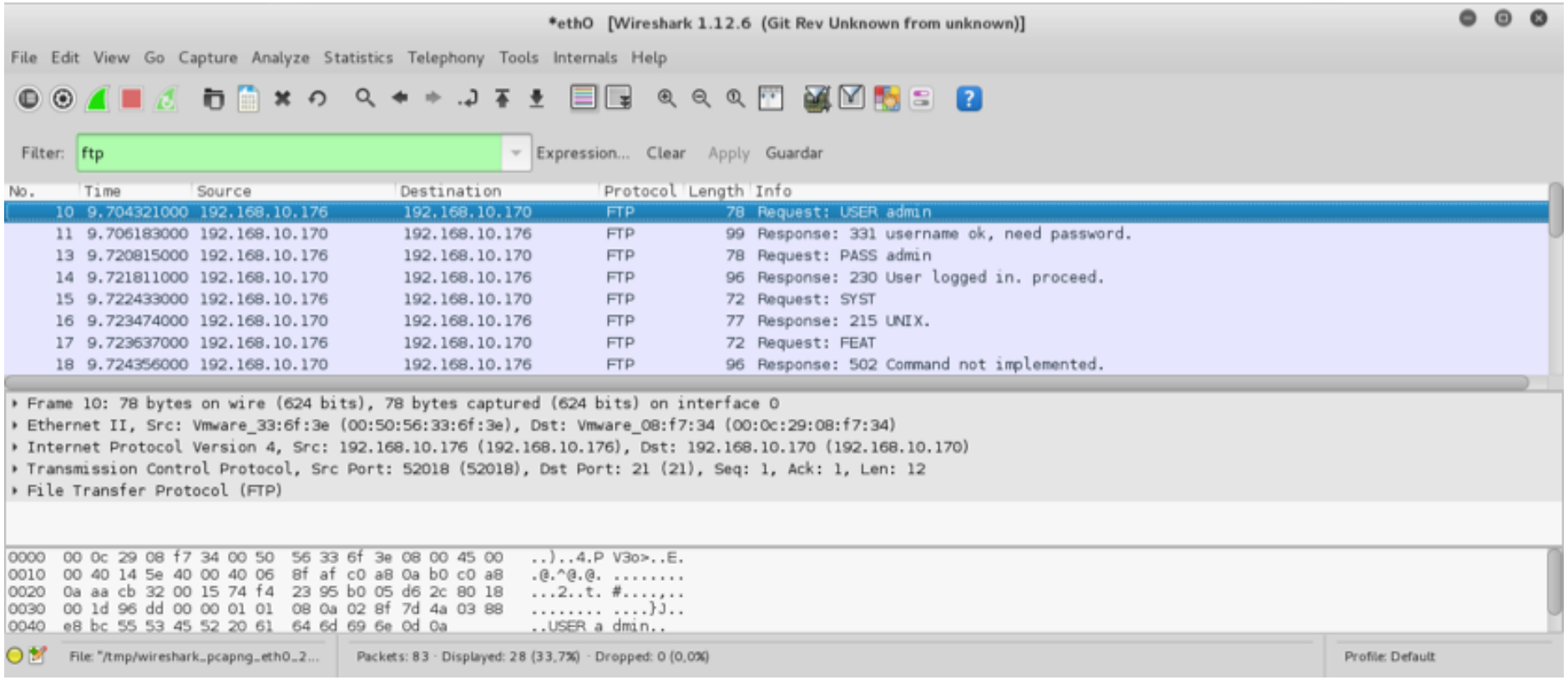


Como observamos en la imagen nos da la posibilidad de realizar el volcado de pagefile.sys, que es lo que conocemos como memoria virtual. Por lo que sería muy interesante realizar también su captura.

3 | Realizar la captura de tráfico de vuestra red para ver si obtenéis alguna credencial en plano de algún servicio que utilicéis (ftp, ssh, http, https, ...).

Para poder realizar el ejercicio necesitamos utilizar Wireshark y realizar la captura del tráfico de la red. Navegar por distintas web, utilizar el servicio ftp gratuito y/o utilizar el servicio ssh de Kali Linux.

Desde la captura de Wireshark utilizar los distintos filtros y búsquedas para ver si observáis texto en plano, así como las credenciales de algún servicio de Internet.



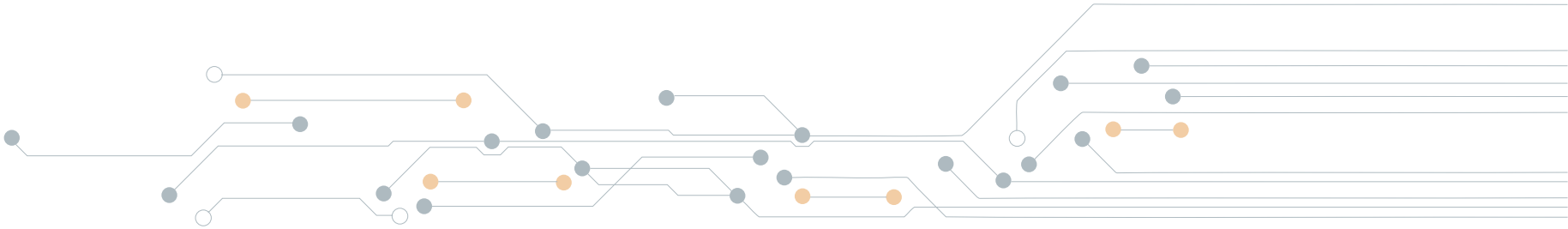
4 | Descargar la cabecera de un email y realizar su trazado con las herramientas online disponibles. ¿Qué habéis conseguido?

Lo primero sería almacenar el correo en formato estándar .eml para su posterior subida a la aplicación o servicio de tracking, o en su defecto, algunos lo que solicitan es una "copia" de esa cabecera, con lo que copiar y pegar sería suficiente. Sería interesante que os descargaseis Email Tracker Pro (versión de prueba http://www.emailtrackerpro.com/) y consultarais toda la información disponible.

Herramientas online:

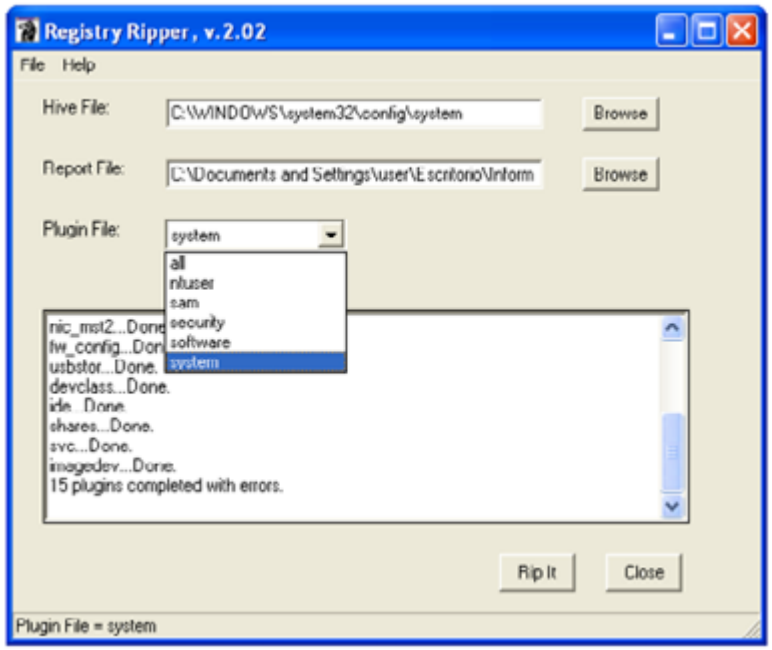
http://www.cyberforensics.in/OnlineEmailTracer/index.aspx

http://whatismyipaddress.com/trace-email

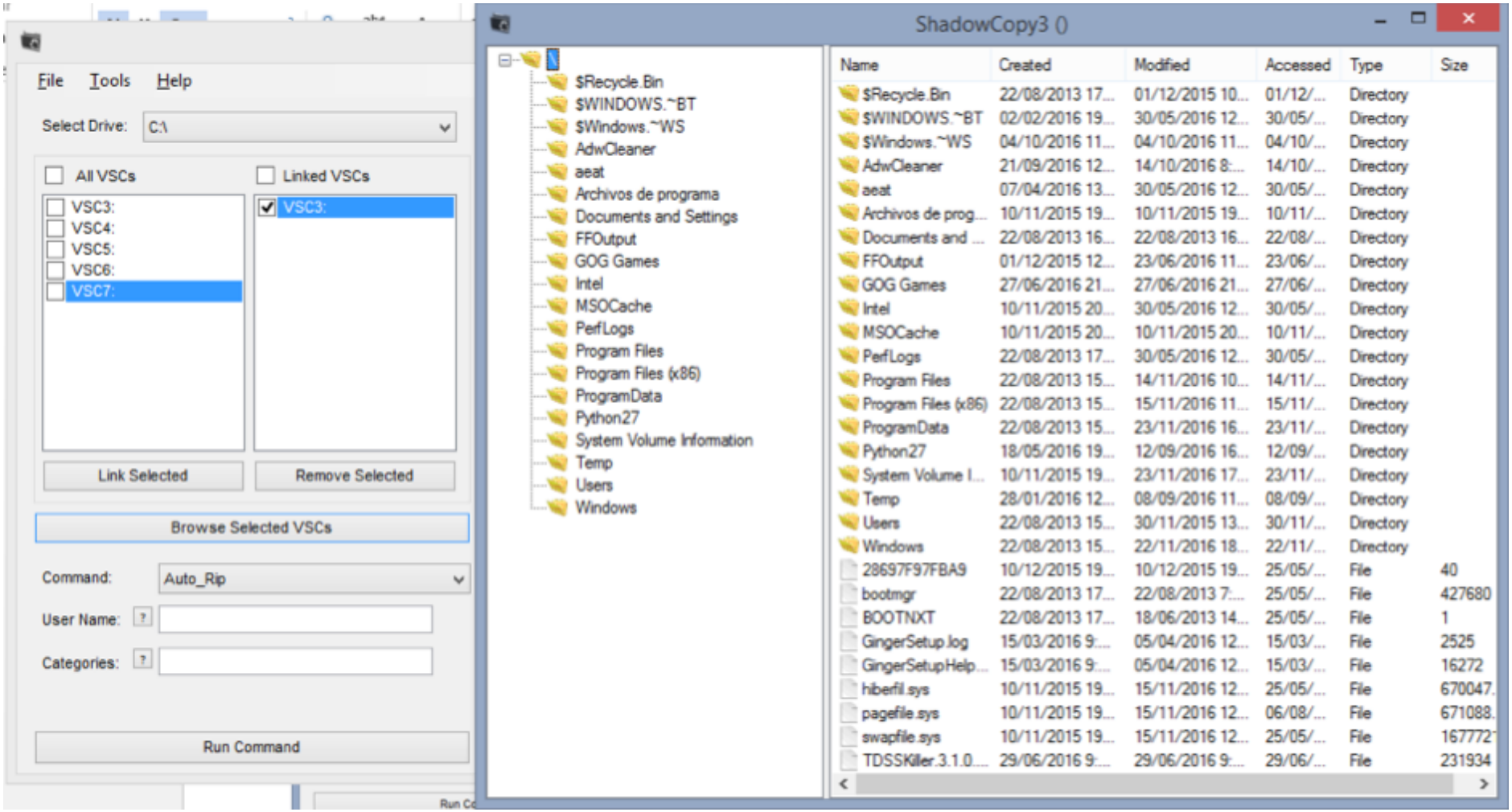


5 | Sobre la copia del disco duro realizada en el caso práctico 1, extraer la información más relevante con RegRipper. Con VSC Toolset comprobar en la máquina si existen copias ocultas para restaurar y obtener un archivo que ya no existe en la máquina, pero que está en la copia VSC.

Para la primera parte del caso práctico necesitamos localizar de la imagen del disco los archivos SAM/ SYSTEM/... para ello con FTKImager podemos cargar la imagen y extraer los ficheros que necesitamos (repasar la teoría para ver donde se encuentran cada uno de ellos). Una vez extraídos utilizamos RegRipper para extraer información valiosa, como la fecha en la que se instaló el sistema operativo, así como los usuarios que hay, entre otros. Consultar la máxima información posible.



Para la segunda parte del caso práctico, iniciamos VSC Toolset como administrador y comprobamos si existen copias de respaldo, en caso afirmativo, buscamos a través del browser de archivos algún archivo (imagen, documento, ...) que actualmente no esté, por ejemplo, en el escritorio.


File Tools Help
Select Drive: C:\
All VSCs
Linked VSCs
VSC3:
VSC4:
VSC5:
VSC6:
VSC7:
VSC3:
Link Selected
Remove Selected
Browse Selected VSCs
Command: Auto_Rip
User Name:
Categories:
Run Command
ShadowCopy3 ()
$Recycle.Bin
$WINDOWS.~BT
$Windows.~WS
AdwCleaner
aeat
Archivos de programa
Documents and Settings
FFOutput
GOG Games
Intel
MSOCache
PerfLogs
Program Files
Program Files (x86)
ProgramData
Python27
System Volume Information
Temp
Users
Windows
Name Created Modified Accessed Type Size
28697F97FBA9 10/12/2015 19... 10/12/2015 19... 25/05/... File 40
bootmgr 22/08/2013 17... 22/08/2013 7:... 25/05/... File 427680
BOOTNXT 22/08/2013 17... 18/06/2013 14... 25/05/... File 1
GingerSetup.log 15/03/2016 9:... 05/04/2016 12... 15/03/... File 2525
GingerSetupHelp... 15/03/2016 9:... 05/04/2016 12... 15/03/... File 16272
hiberfil.sys 10/11/2015 19... 15/11/2016 12... 25/05/... File 670047...
pagefile.sys 10/11/2015 19... 15/11/2016 12... 06/08/... File 671088...
swapfile.sys 10/11/2015 19... 15/11/2016 12... 25/05/... File 167772...
TDSSKiller.3.1.0.... 29/06/2016 9:... 29/06/2016 9:... 29/06/... File 231934

Telefónica EDUCACIÓN DIGITAL