

Índice:

Ejercicio 1	2
a) Análisis forense y uso de comandos o herramientas de análisis forense.....	2

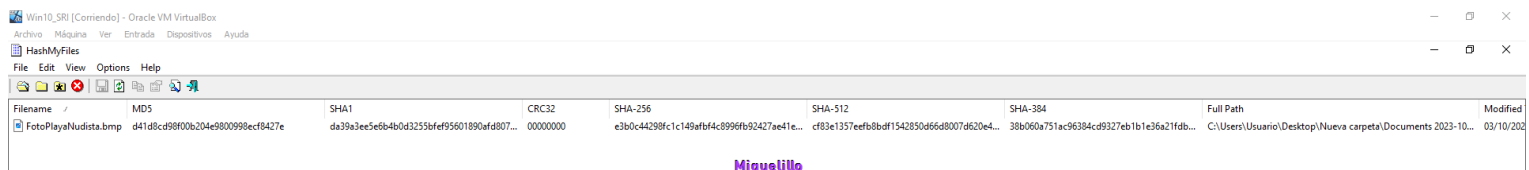
Ejercicio 1

a) Análisis forense y uso de comandos o herramientas de análisis forense.

Solución:

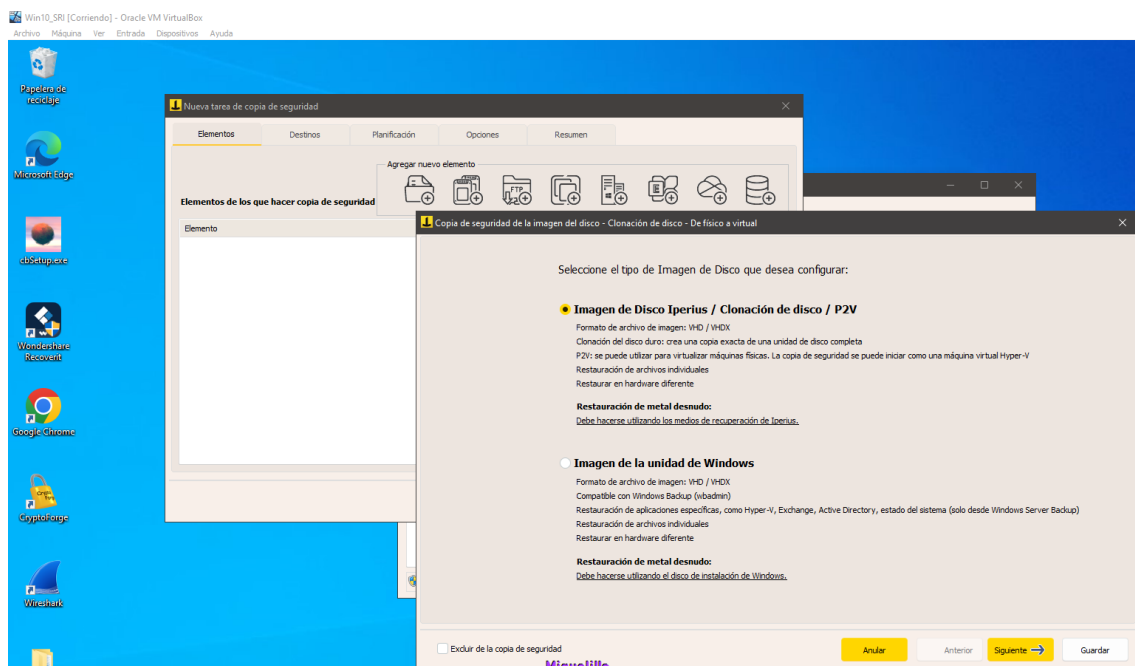
A la hora de realizar un análisis forense se utiliza un documento de cadena de custodia lo que indica que las evidencias que han sacado del dispositivo no han sido manipuladas y se pueden presentar como pruebas en un juicio para confirmar que no ha sido confirmado se saca la función Hash del documento

En este caso he usado HashMyFiles

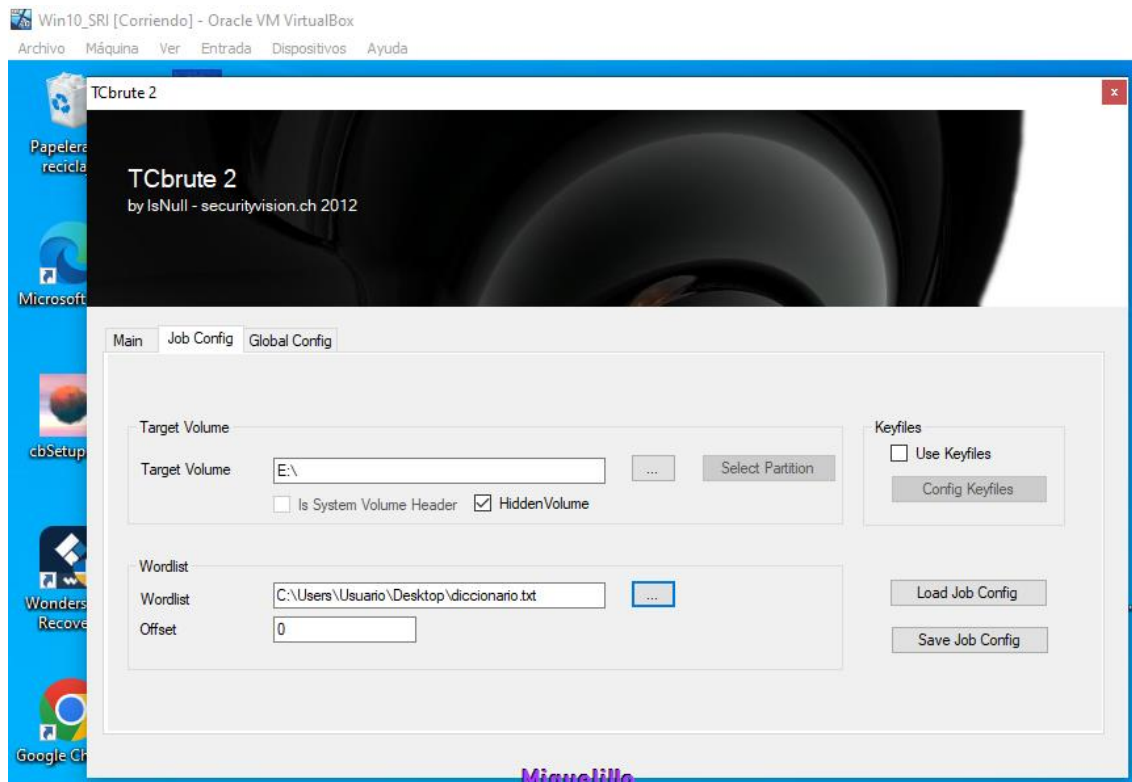


Filename	MD5	SHA1	CRC32	SHA-256	SHA-512	SHA-384	Full Path	Modified
FotoPlayaNudista.bmp	d41d8cd98f00b204e9800998ec8427e	da39a3ee5e6b4b0d3255bfef95601890afd807...	00000000	e3b0c44298fc1c149afbf4c8996fb92427ae41e...	cf83e1357effb8bdf1542850d66d8007d620e4...	38b0600751ac96384cd9327eb1b1e36a21fdb...	C:\Users\Usuario\Desktop\Nueva carpeta\Documents 2023-10...	03/10/2023

En un análisis forense se suele clonar el disco duro para mantener la integridad del original y se trabaja con el clonado. O bien con una clonadora de discos física con software dedicado como **Iperius Backup**

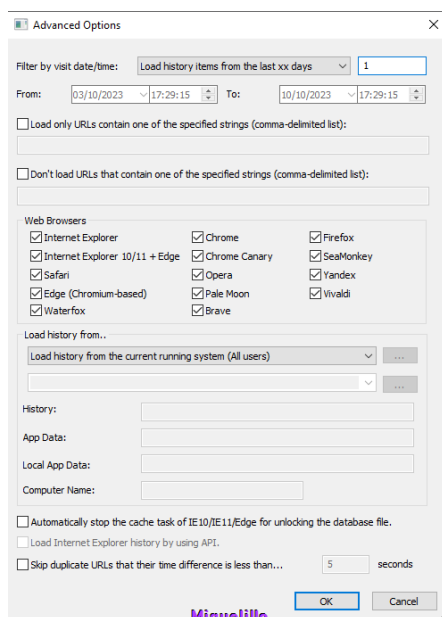


En caso de estar cifrado podemos hacer un ataque de fuerza bruta si tenemos una mínima idea de cómo es la contraseña podríamos no tardar mucho pero si no tenemos la mínima idea y la contraseña no es insegura o de diccionario podríamos tardar cientos de años. Voy a usar TCbrute



Miguelillo

Herramienta para sacar el historial de los buscadores BrowsingHistory, en la configuración podemos seleccionar de cuantos días queremos los registros.



Miguelillo

Win10_SRI [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

BrowsingHistoryView

File Edit View Options Help

URL	Title	Visit Time	Visit Count	Visited From	Visit Type	Visit Duration	Web Browser	User Profile	Brows...
ms-gamingoverlay://...		10/10/2023 9:16:53	4				Internet Explorer 10/11 / ...	Usuario	
https://cifraronline.co...	Cifrar Online - Encriptar y desencrip...	10/10/2023 9:36:20	1		Typed URL	00:00:53.783	Chrome	Usuario	Defau...
https://www.google.c...	cifrar por sustitucion - Buscar con G...	10/10/2023 9:37:21	2		Generated	00:00:00.742	Chrome	Usuario	Defau...
https://www.google.c...	cifrar por sustitucion - Buscar con G...	10/10/2023 9:37:22	2	https://www.google.co...	Link	00:00:16.778	Chrome	Usuario	Defau...
https://www.gausian...	Criptografía: Cifrado por sustitució...	10/10/2023 9:37:30	1	https://www.google.co...	Link	00:15:23.204	Chrome	Usuario	Defau...
https://www.google.c...	cifrado por sustitucion online - Bus...	10/10/2023 9:37:39	2	https://www.google.co...	Form Submit	00:00:01.759	Chrome	Usuario	Defau...
https://www.google.c...	cifrado por sustitucion online - Bus...	10/10/2023 9:37:40	2	https://www.google.co...	Link	00:15:23.027	Chrome	Usuario	Defau...
https://es.planetcalc.c...	Calculadora en línea: Herramienta d...	10/10/2023 9:37:43	1	https://www.google.co...	Link	00:15:15.710	Chrome	Usuario	Defau...
https://brianur.info/c...	Cifrado Caesar - BrianUR	10/10/2023 9:37:47	3	https://www.google.co...	Link	00:00:17.570	Chrome	Usuario	Defau...
https://brianur.info/t...		10/10/2023 9:38:05	12	Miguel Lillo	Manual Subframe		Chrome	Usuario	Defau...

Herramienta para ver el caché de Chrome ChromeCacheView

Win10_SRI [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

ChromeCacheView C:\Users\Usuario\AppData\Local\Google\Chrome\User Data\Default\Cache_Data

File Edit View Options Help

Filename	URL	Content Type	File Size	Last Accessed	Server Time	Server Last Modified	Expire Time	Server Name	Server Response
xa=AKA0jsTh...	https://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js	image/gif	42	10/10/2023 19:44:09	10/10/2023 19:44:12	01/01/1601 1:00:00	01/01/1990 1:00:00	cafe	HTTP/1.1 200
xa=AKA0jsTh...	https://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js	image/gif	42	10/10/2023 19:44:09	10/10/2023 19:44:12	01/01/1601 1:00:00	01/01/1990 1:00:00	cafe	HTTP/1.1 200
xa=AKA0jsTh...	https://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js	image/gif	42	10/10/2023 19:44:09	10/10/2023 19:44:11	01/01/1601 1:00:00	01/01/1990 1:00:00	cafe	HTTP/1.1 200
dc_oe=ChM7ML...	https://ads.google.com/pagead/js/adsbygoogle.js	image/gif	42	10/10/2023 19:44:09	10/10/2023 19:44:11	01/01/1601 1:00:00	01/01/1990 1:00:00	cafe	HTTP/1.1 200
dc_oe=ChM7ML...	https://ads.google.com/pagead/js/adsbygoogle.js	image/gif	42	10/10/2023 19:43:57	10/10/2023 19:44:00	01/01/1601 1:00:00	01/01/1990 1:00:00	cafe	HTTP/1.1 200
xa=AKA0jsTh...	https://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js	image/gif	42	10/10/2023 19:42:47	10/10/2023 19:42:51	01/01/1601 1:00:00	01/01/1990 1:00:00	cafe	HTTP/1.1 200
xa=AKA0jsTh...	https://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js	image/gif	42	10/10/2023 19:42:47	10/10/2023 19:42:51	01/01/1601 1:00:00	01/01/1990 1:00:00	cafe	HTTP/1.1 200
xa=AKA0jsTh...	https://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js	image/gif	42	10/10/2023 19:42:47	10/10/2023 19:42:51	01/01/1601 1:00:00	01/01/1990 1:00:00	cafe	HTTP/1.1 200

Para ver los registros del sistema FullEventView

Win10_SRI [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

FullEventLogView

File Edit View Options Help

Event Time	Record ID	Event ID	Level	Channel	Provider	Description	Opcode	Task	Keywords	Process ID
03/10/2023 20:00...	2459	1003	Information	Application	Microsoft-Windows-Security...	El servicio de protección de software compl...			Clásico	
03/10/2023 20:00...	2460	8198	Error	Application	Microsoft-Windows-Security...	Error de la activación de licencia (slui.exe) c...			Clásico	
03/10/2023 20:00...	1333	811	Information	Microsoft-Windows-Winlogon...	Microsoft-Windows-Winlogon	El suscriptor <Sens> a notificaciones de wi...	Iniciar (1)	811	0x400000000000...	628
03/10/2023 20:00...	1334	812	Information	Microsoft-Windows-Winlogon...	Microsoft-Windows-Winlogon	El suscriptor <Sens> a notificaciones de wi...	Detener (2)	811	0x400000000000...	628
03/10/2023 20:00...	1335	811	Information	Microsoft-Windows-Winlogon...	Microsoft-Windows-Winlogon	El suscriptor <TermSrv> a notificaciones de...	Iniciar (1)	811	0x400000000000...	628
03/10/2023 20:00...	1336	812	Information	Microsoft-Windows-Winlogon...	Microsoft-Windows-Winlogon	El suscriptor <TermSrv> a notificaciones de...	Detener (2)	811	0x400000000000...	628
03/10/2023 20:00...	3154	3	Information	System	Virtual Disk Service	Servicio iniciado.			Clásico	
03/10/2023 20:00...	450	1	Information	Microsoft-Windows-Universal...	Microsoft-Windows-Universal...	Se registró al inquilino P-ARIA-4bb4d6f7caf...		1	0x800000000000...	1320
03/10/2023 20:00...	2544	5857	Undefined	Microsoft-Windows-WMI-Act...	Microsoft-Windows-WMI-Act...	El proveedor WMIProv se inició con código...			0x400000000000...	5476
03/10/2023 20:00...	2545	5858	Error	Microsoft-Windows-WMI-Act...	Microsoft-Windows-WMI-Act...	Id = (00000000-0000-0000-0000-000000000000...			0x400000000000...	528
03/10/2023 20:00...	2546	5858	Error	Microsoft-Windows-WMI-Act...	Microsoft-Windows-WMI-Act...	Id = (00000000-0000-0000-0000-000000000000...			0x400000000000...	528
03/10/2023 20:00...	451	1	Information	Microsoft-Windows-Universal...	Microsoft-Windows-Universal...	Se registró al inquilino P-ARIA-5476d0c47...		1	0x800000000000...	1320
03/10/2023 20:00...	149	145	Information	Microsoft-Windows-WinRM/...	Microsoft-Windows-WinRM/...	La operación de WSMAN Enumeration se ini...	Iniciar (1)		llamada a la A...	528

Miguel Lillo

Para ver las redes a las que te has conectado y sus contraseñas WirelessKeyView

WirelessKeyView

File Edit View Options Help

Network Name...	Key Type	Key (Hex)	Key (Ascii)	Adapter Name	Adapter GUID	Authentication	Encryption
(00)						WPA2PSK	AES
(00)						WPA2PSK	AES
(00)						WPA2PSK	AES
(00) WLAN2ASIR	WPA2-PSK	3630363036303630363000	6060606060	Realtek RTL		WPA2PSK	AES

Miguel Lillo

Para ver las cuentas y sus respectivas contraseñas CredentialFileView

CredentialFileView

File Edit View Options Help

Filename	Version	Decrypted...	Modified Time	Entry Type	Persist	Entry Name	User Name	Password	Full Path	File Size	File Modified Time	File C...
764CB232BCD7E661C8AA4EBF...	Vista/7/8/10	3342	19/10/2023 20:25:05	Generic	Local Machine	LegacyGenericTarget...	miguellillo2004@g...		C:\Users\Miguel\AppData\Local\Microsoft\Credentials\764CB232BCD7E661C8AA4EBF...	4,232	19/10/2023 20:25:05	03/10/2023 20:25:05
DFBE70A7E5CC19A398EBF1896...	Vista/7/8/10	11,272	09/10/2023 18:06:52	Generic	Local Machine	WindowsLiveTarget-vit...	02bannvisdbann		C:\Users\Miguel\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1896...	11,560	09/10/2023 18:06:52	25/07/2023 18:06:52
DFBE70A7E5CC19A398EBF1896...	Vista/7/8/10	11,256	25/07/2023 16:40:25	Generic	Local Machine	WindowsLiveTarget-vit...	02bannvisdbann		C:\Windows\system32\config\systemprofile\AppData\Local\Microsoft\Credentials\DFBE70A7...	11,544	25/07/2023 16:40:25	25/07/2023 16:40:25

Comandos de Windows para detectar si hay un intruso en la red

Netstat para ver el estado de los puertos y los protocolos

```

Simbolo del sistema - netstat -a

C:\Users\Miguel>netstat -a

Conexiones activas

Proto  Dirección local      Dirección remota      Estado
TCP    0.0.0.0:135           DESKTOP-3I954N4:0     LISTENING
TCP    0.0.0.0:445           DESKTOP-3I954N4:0     LISTENING
TCP    0.0.0.0:900           DESKTOP-3I954N4:0     LISTENING
TCP    0.0.0.0:912           DESKTOP-3I954N4:0     LISTENING
TCP    0.0.0.0:2156          DESKTOP-3I954N4:0     LISTENING
TCP    0.0.0.0:5040          DESKTOP-3I954N4:0     LISTENING
TCP    0.0.0.0:5357          DESKTOP-3I954N4:0     LISTENING
TCP    0.0.0.0:7680          DESKTOP-3I954N4:0     LISTENING
TCP    0.0.0.0:8834          DESKTOP-3I954N4:0     LISTENING
TCP    0.0.0.0:49664         DESKTOP-3I954N4:0     LISTENING
TCP    0.0.0.0:49665         DESKTOP-3I954N4:0     LISTENING
TCP    0.0.0.0:49666         DESKTOP-3I954N4:0     LISTENING
TCP    0.0.0.0:49667         DESKTOP-3I954N4:0     LISTENING
TCP    0.0.0.0:49668         DESKTOP-3I954N4:0     LISTENING
TCP    0.0.0.0:49669         DESKTOP-3I954N4:0     LISTENING
TCP    0.0.0.0:57621         DESKTOP-3I954N4:0     LISTENING
TCP    127.0.0.1:6463         DESKTOP-3I954N4:0     LISTENING
TCP    127.0.0.1:49695        DESKTOP-3I954N4:49695 ESTABLISHED
TCP    127.0.0.1:49696        DESKTOP-3I954N4:49695 ESTABLISHED
TCP    127.0.0.1:49699        DESKTOP-3I954N4:49700 ESTABLISHED
TCP    127.0.0.1:49700        DESKTOP-3I954N4:49699 ESTABLISHED
TCP    192.168.1.162:139      DESKTOP-3I954N4:0     LISTENING
TCP    192.168.1.162:2016    20.82.220.141:https   CLOSE_WAIT
TCP    192.168.1.162:2051    47:https               ESTABLISHED

```

Netstat -b para ver el trafico por proceso

```

Administrador: Símbolo del sistema

TCP    192.168.1.162:2051    47:https               ESTABLISHED
[Discord.exe]
TCP    192.168.1.162:2178    124:4070               ESTABLISHED
[Spotify.exe]
TCP    192.168.1.162:2188    40:https               ESTABLISHED
[Spotify.exe]
TCP    192.168.1.162:2217    40:https               ESTABLISHED
[Spotify.exe]
TCP    192.168.1.162:2317    wr-in-f188:5228        ESTABLISHED
[chrome.exe]
TCP    192.168.1.162:2458    wo-in-f188:5228        ESTABLISHED
[chrome.exe]
TCP    192.168.1.162:2478    ec2-52-211-204-154:https ESTABLISHED
[chrome.exe]
TCP    192.168.1.162:2534    whatsapp-cdn-shv-01-mad1:https ESTABLISHED
[chrome.exe]
TCP    192.168.1.162:3471    185.183.113.100:https  ESTABLISHED
[chrome.exe]
TCP    192.168.1.162:3731    89.107.245.133:https   ESTABLISHED
[chrome.exe]
TCP    192.168.1.162:8805    edge-dgw-shv-01-mad1:https ESTABLISHED
[chrome.exe]
TCP    192.168.1.162:8814    20.54.36.229:https     ESTABLISHED
[VirtualBoxVM.exe]
TCP    192.168.1.162:10963   ec2-52-57-17-240:https ESTABLISHED
[chrome.exe]
TCP    192.168.1.162:13425   162.159.129.235:https  ESTABLISHED
[Discord.exe]
TCP    192.168.1.162:13456   25:https               TIME_WAIT
TCP    192.168.1.162:13504   server-52-84-66-101:https ESTABLISHED

```

Netstat -es para ver las estadísticas de las conexiones

```

C:\Windows\system32>netstat -es
Estadísticas de interfaz

                Recibidos                Enviados
Bytes           940021248                1706109494
Paquetes de unidifusión  13432984                9230556
Paquetes no de unidifusión  366176                45738
Descartados      0                        0
Errores          0                        0
Protocolos desconocidos  0

Estadísticas de IPv4

Paquetes recibidos           = 3038368
Errores de encabezado recibidos = 0
Errores de dirección recibidos = 14133
Datagramas reenviados        = 0
Protocolos desconocidos recibidos = 0
Paquetes recibidos descartados = 57489
Paquetes recibidos procesados = 3041715
Solicitudes de salida        = 2018926

Estadísticas de TCP para IPv6

Activos abiertos             = 140
Pasivos abiertos             = 90
Intentos de conexión erróneos = 1546
Conexiones restablecidas     = 1
Conexiones actuales          = 0
Segmentos recibidos          = 9890
Segmentos enviados           = 9780
Segmentos retransmitidos     = 112

Estadísticas UDP para IPv4

Datagramas recibidos         = 1105840
Sin puerto                   = 19956
Errores de recepción         = 44256
Datagramas enviados          = 709723

Estadísticas UDP para IPv6

Datagramas recibidos         = 72367
Sin puerto                   = 4
Errores de recepción         = 8034
Datagramas enviados          = 9724

C:\Windows\system32>netstat -es

```

Para ver conexiones por NetBIOS nbtstat -r

```

C:\Windows\system32>nbtstat -r

Estadísticas de resolución y registro de nombres NetBIOS
-----

Resueltos por difusión           = 0
Resueltos por el servidor de nombres = 0

Registrados por difusión         = 78
Registrados por el servidor de nombres = 0

```

Con route PRINT podemos ver las tablas de enrutamiento en IPv4 y en IPv6

```

C:\Windows\system32>route PRINT
=====
Lista de interfaces
13...0a 00 27 00 00 0d .....VirtualBox Host-Only Ethernet Adapter
17...52 c2 e8 8e 2d 6b .....Microsoft Wi-Fi Direct Virtual Adapter
21...d2 c2 e8 8e 2d 6b .....Microsoft Wi-Fi Direct Virtual Adapter #2
5...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
11...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
3...50 c2 e8 8e 2d 6b .....Realtek RTL8822CE 802.11ac PCIe Adapter
15...50 c2 e8 8e 2d 6c .....Bluetooth Device (Personal Area Network)
1.....Software Loopback Interface 1
=====

IPv4 Tabla de enrutamiento
=====
Rutas activas:
Destino de red      Máscara de red      Puerta de enlace      Interfaz      Métrica
0.0.0.0             0.0.0.0             192.168.1.1           192.168.1.162  40
127.0.0.0           255.0.0.0           En vínculo            127.0.0.1      331
127.0.0.1           255.255.255.255     En vínculo            127.0.0.1      331
127.255.255.255     255.255.255.255     En vínculo            127.0.0.1      331
192.168.1.0         255.255.255.0       En vínculo            192.168.1.162  296
192.168.1.162       255.255.255.255     En vínculo            192.168.1.162  296
192.168.1.255       255.255.255.255     En vínculo            192.168.1.162  296
192.168.29.0        255.255.255.0       En vínculo            192.168.29.1   291
192.168.29.1        255.255.255.255     En vínculo            192.168.29.1   291
192.168.29.255      255.255.255.255     En vínculo            192.168.29.1   291
192.168.56.0        255.255.255.0       En vínculo            192.168.56.1   281
192.168.56.1        255.255.255.255     En vínculo            192.168.56.1   281
192.168.56.255      255.255.255.255     En vínculo            192.168.56.1   281
192.168.211.0       255.255.255.0       En vínculo            192.168.211.1  291
192.168.211.1       255.255.255.255     En vínculo            192.168.211.1  291
192.168.211.255     255.255.255.255     En vínculo            192.168.211.1  291
224.0.0.0           240.0.0.0           En vínculo            127.0.0.1      331
224.0.0.0           240.0.0.0           En vínculo            192.168.56.1   281
224.0.0.0           240.0.0.0           En vínculo            192.168.1.162  296
224.0.0.0           240.0.0.0           En vínculo            192.168.211.1  291
224.0.0.0           240.0.0.0           En vínculo            192.168.29.1   291
255.255.255.255     255.255.255.255     En vínculo            127.0.0.1      331
255.255.255.255     255.255.255.255     En vínculo            192.168.56.1   281
255.255.255.255     255.255.255.255     En vínculo            192.168.1.162  296
255.255.255.255     255.255.255.255     En vínculo            192.168.211.1  291
255.255.255.255     255.255.255.255     En vínculo            192.168.29.1   291

```

Para ver los recursos compartidos de la red **net share**

```

C:\Windows\system32>net SHARE

Nombre      Recurso      Descripción
-----
C$          C:\          Recurso predeterminado
IPC$        IPC remota
ADMIN$      C:\Windows  Admin remota
Se ha completado el comando correctamente.

```

Para ver los usuarios de net bios **nbtstat -n**

```

C:\Windows\system32>nbtstat -n

Ethernet:
Dirección IP del nodo: [192.168.56.1] Id. de ámbito : []

Tabla de nombres locales NetBIOS

Nombre                Tipo        Estado
-----
DESKTOP-3I954N4<20>   Único      Registrado
DESKTOP-3I954N4<00>   Único      Registrado
WORKGROUP              <00>      Grupo      Registrado

```

Para ver los usuarios de los recursos compartidos net users

```

C:\Windows\system32>net users

Cuentas de usuario de \\DESKTOP-3I954N4

-----
Administrador          DefaultAccount         Invitado
Miguel                 WDAGUtilityAccount
Se ha completado el comando correctamente.

```

Con la utilidad de mdd copiamos la RAM a un archivo y con Volatility -f interpretamos el archivo

```

Administrador: Windows PowerShell

PS C:\mdd_1.3\mdd>
PS C:\mdd_1.3\mdd> .\mdd_1.3.exe -o ram.img
-> mdd
-> ManTech Physical Memory Dump Utility
Copyright (C) 2008 ManTech Security & Mission Assurance

-> This program comes with ABSOLUTELY NO WARRANTY; for details use option '-w'
This is free software, and you are welcome to redistribute it
under certain conditions; use option '-c' for details.

```

Podemos desde propiedades obtener metadatos, aunque los archivos estén cifrados

