

Nombre :	Univ. Gonzalo Espinoza Chiri	Numero de practica
Materia	Informática Forense sis-939	3
Docente:	Ing. David Sossa L.	
Auxiliar :	Univ.	

PRACTICA DE RECOLECCION DE INFORMACION VOLATIL

Parte 1: Introducción

1.1. Antecedentes:

En un incidente de seguridad, donde se ha realizado una intrusión no permitida a un equipo de cómputo y se requiere buscar la causa o al culpable para que se haga justicia sobre los daños que fueron hechos, para ello se emplea los conocimientos y experiencia de los investigadores forenses en cómputo.

Uno de los primeros pasos que se realiza es congelar la escena del crimen con el fin de adquirir la información que puede llevarlo a encontrar las evidencias necesarias para identificar las causas del incidente. En los crímenes digitales la captura de información se convierte en un paso importante durante la investigación, ya que si no se siguen los pasos adecuados es fácil perder la información volátil del sistema, cuando el investigador llega a la escena del crimen puede encontrar el sistemas “vivo” (corriendo sus procesos en forma normal) o el sistemas apagado “muerto”, el caso de un sistema vivo, es difícil congelar la escena del crimen, ya que la evidencia es sensitiva al tiempo además de frágil, puede ser fácilmente alterada, dañada o destruida además al realizar la captura de información volátil y de memoria es fácil cometer errores que traigan consecuencias graves, ya que si se apaga el equipo antes de capturar la información, puede destruir la poca evidencia existente, en caso de que el sistema muere (se apaga) podemos decir que la información volátil se ha perdido. En este sentido se debe examinar cada elemento con cuidado.

Antecedentes caso ficticio: en una empresa de auditores se tiene las sospechas de que uno de los empleados está filtrando información a otra empresa de los reportes de auditoría, para ello se pide realizar un análisis forense de la computadora que se le asignó a dicho empleado, la computadora se encuentra encendida.

1.2. Objetivo

Poner en práctica los conocimientos de informática forense en la recolección de información volátil.

1.3. Datos del propietario del equipo.

Datos del propietario	Nombre del equipo	nombre de usuario	Descripción física del hardware
empresa CONT.srl	Portatil : HP	Marco Tejerina Ventura	Procesador : Intel Core i7-6500U
	Modelo: 450 Probook		Memoria Ram : 8 GB
	color: negro		Disco duro: 1 TB
			Adaptador wifi y Bluetooth
			puerto LAN

2. Tabla de hashes de todos los archivos recolectados (los cuales se citan a continuación)

3. INFORMACION INICIAL

n°	Tipo de Evidencias	Nombre del archivo	Hash	Hora y Fecha	Hora Inicio-final
1	volcado de memoria (volátil)	memdump.mem	si	07:49 p.m. -15/10/2018	07:46 - 20:00

Descripción: el volcado de memoria se lo realiza a la memoria RAM, con el programa AccessData FTK image v3.2.0.0, el programa generara un archivo llamado “memdump.mem” el cual contiene toda la información contenida en la memoria RAM.

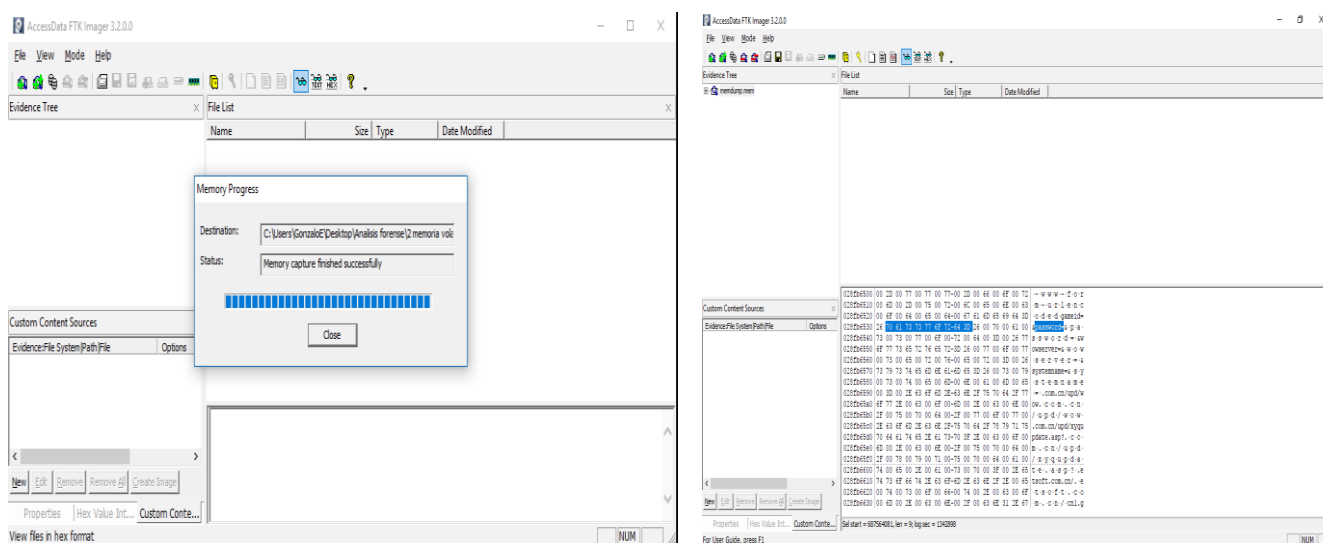
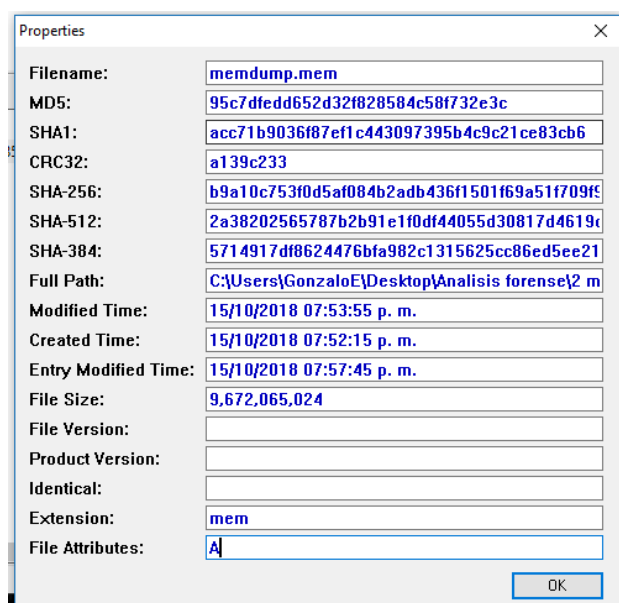


Tabla de hash del archivo memdump.men:



n°	Tipo de Evidencias	Nombre del archivo	Hash	Hora y Fecha	Hora Inicio-final
2	Exportación de registro entero(Windows)				

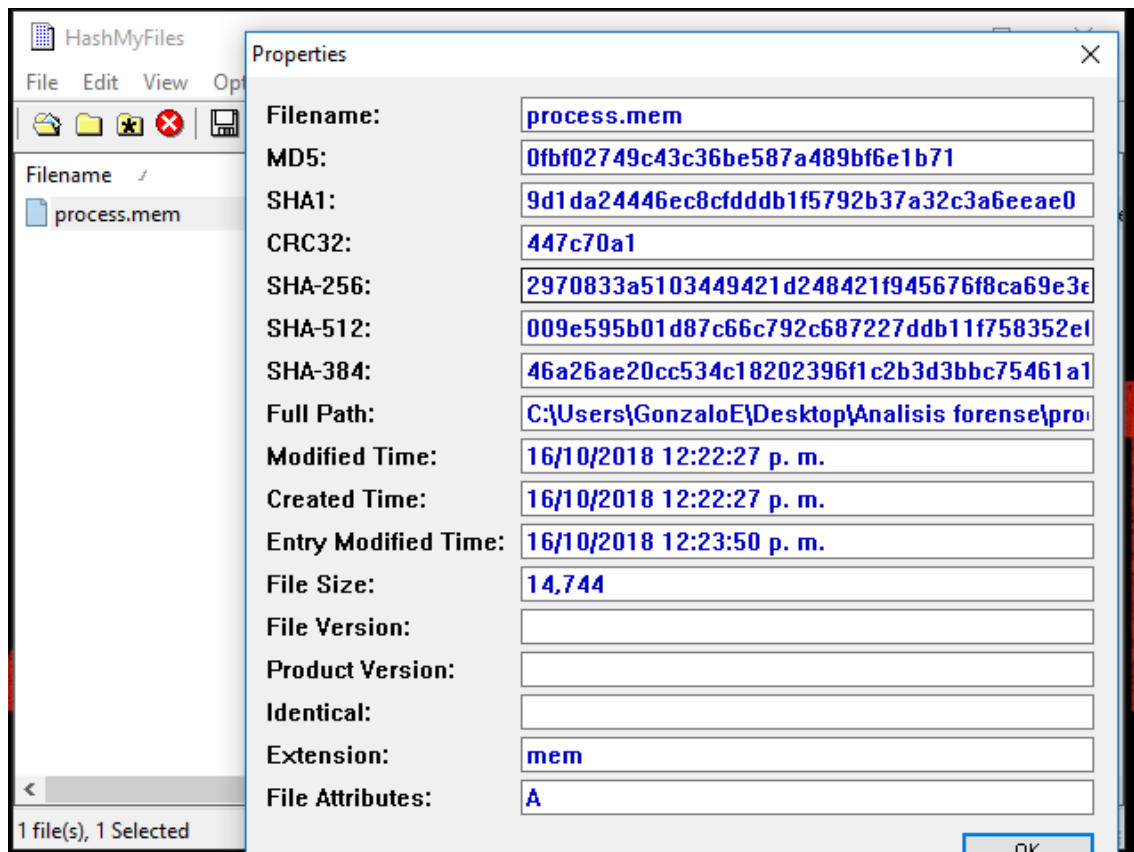
n°	Tipo de Evidencias	Nombre del archivo	Hash	Hora y Fecha	Hora Inicio-final
3	procesos en ejecucion	process.man	Si	12:32 p.m. -16/10/2018 GTM-4	12:00 - 12:35

Descripción: para mostrar los procesos en ejecución, se utilizó la consola de comandos de la máquina, (rasklist).

```
C:\Users\GonzaloE\Desktop\Analisis forense\procesos en ejecucion>tasklist

Nombre de imagen          PID Nombre de sesión Núm. de ses Uso de memor
=====
System Idle Process       0 Services          0          8 KB
System                    4 Services          0      11,580 KB
smss.exe                  400 Services          0       948 KB
csrss.exe                 612 Services          0      4,328 KB
wininit.exe               736 Services          0      4,768 KB
services.exe              808 Services          0      7,556 KB
lsass.exe                 816 Services          0     14,024 KB
svchost.exe               936 Services          0       2,832 KB
fontdrvhost.exe           952 Services          0       2,820 KB
svchost.exe               992 Services          0     22,156 KB
svchost.exe               372 Services          0     13,404 KB
svchost.exe               556 Services          0       6,056 KB
svchost.exe              1220 Services          0     13,424 KB
svchost.exe              1260 Services          0       9,152 KB
svchost.exe              1268 Services          0       7,004 KB
svchost.exe              1352 Services          0       7,804 KB
atiesrxx.exe             1476 Services          0       4,072 KB
svchost.exe              1548 Services          0     79,436 KB
svchost.exe              1556 Services          0       4,524 KB
Memory Compression       1620 Services          0    316,628 KB
svchost.exe              1696 Services          0     17,096 KB
svchost.exe              1704 Services          0       9,688 KB
svchost.exe              1720 Services          0     14,748 KB
svchost.exe              1728 Services          0       5,524 KB
svchost.exe              1880 Services          0       5,908 KB
igfxCUIService.exe       1928 Services          0       5,708 KB
svchost.exe              1964 Services          0       6,200 KB
svchost.exe              1972 Services          0       7,292 KB
svchost.exe              2008 Services          0       5,780 KB
svchost.exe              2072 Services          0       6,916 KB
svchost.exe              2196 Services          0     10,620 KB
svchost.exe              2220 Services          0     11,092 KB
svchost.exe              2320 Services          0       8,120 KB
svchost.exe              2336 Services          0     11,924 KB
svchost.exe              2436 Services          0       7,188 KB
svchost.exe              2460 Services          0     23,596 KB
svchost.exe              2644 Services          0     13,648 KB
svchost.exe              2668 Services          0       5,196 KB
svchost.exe              2676 Services          0       9,976 KB
svchost.exe              2856 Services          0     11,368 KB
```

Has del archivo generado (process.mam):



nº	Tipo de Evidencias	Nombre del archivo	Hash	Hora y Fecha	Hora Inicio-final
4	Servicios en ejecución	servicesEjecution.mem/txt	Si	17:20 p.m. -16/10/2018 GTM-4	17:20 - 17:35

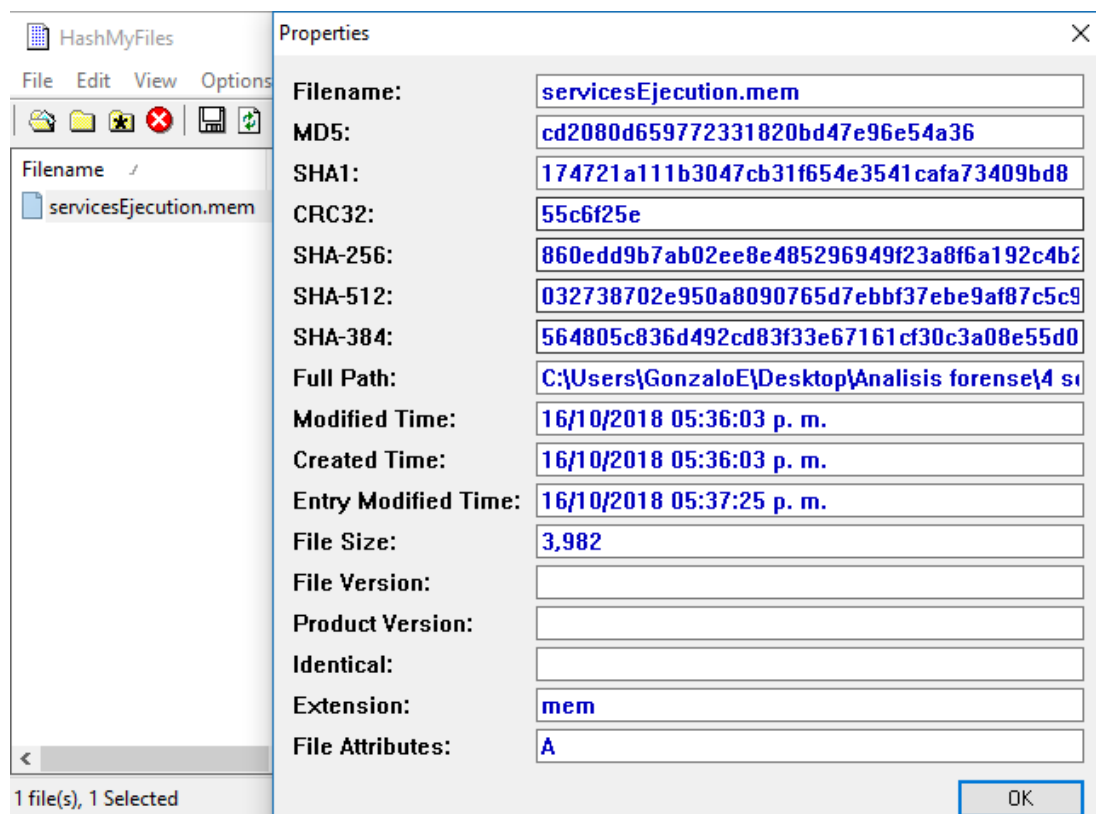
Descripción: para poder obtener una lista de los servicios en ejecución del sistema se empleó el comando de “**net start**”, la cual nos muestra una lista de todos los servicios en ejecución como se muestra:

```

Administrador: Símbolo del sistema
C:\Users\GonzaloE\Desktop\Análisis forense\4 servicios en ejecución>net start
Se han iniciado estos servicios de Windows:
Administrador de conexiones de acceso remoto
Administrador de conexiones de Windows
Administrador de credenciales
Administrador de cuentas de seguridad
Administrador de cuentas web
Administrador de sesión local
Administrador de usuarios
Adquisición de imágenes de Windows (WIA)
Agente de conexión de red
Agente de directiva IPsec
Agente de eventos de tiempo
Agente de eventos del sistema
Aislamiento de claves CNG
AMD External Events Utility
Aplicación auxiliar de NetBIOS sobre TCP/IP
Aplicación auxiliar IP
Asignador de extremos de RPC
Audio de Windows
BTDevManager
Cliente de seguimiento de vínculos distribuidos
Cliente DHCP
Cliente DNS
Cola de impresión
Compilador de extremo de audio de Windows
Configuración automática de dispositivos conectados a la red
Configuración automática de WLAN
Contenedor de Microsoft Passport
CoreMessaging
CxdmSvc
CXUtilSvc
Detección de hardware shell
Detección SSDP
Energía
Estación de trabajo
Firewall de Windows Defender
Geolocation Service
Host de proveedor de detección de función
Host del servicio de diagnóstico
HP CASL Framework Service

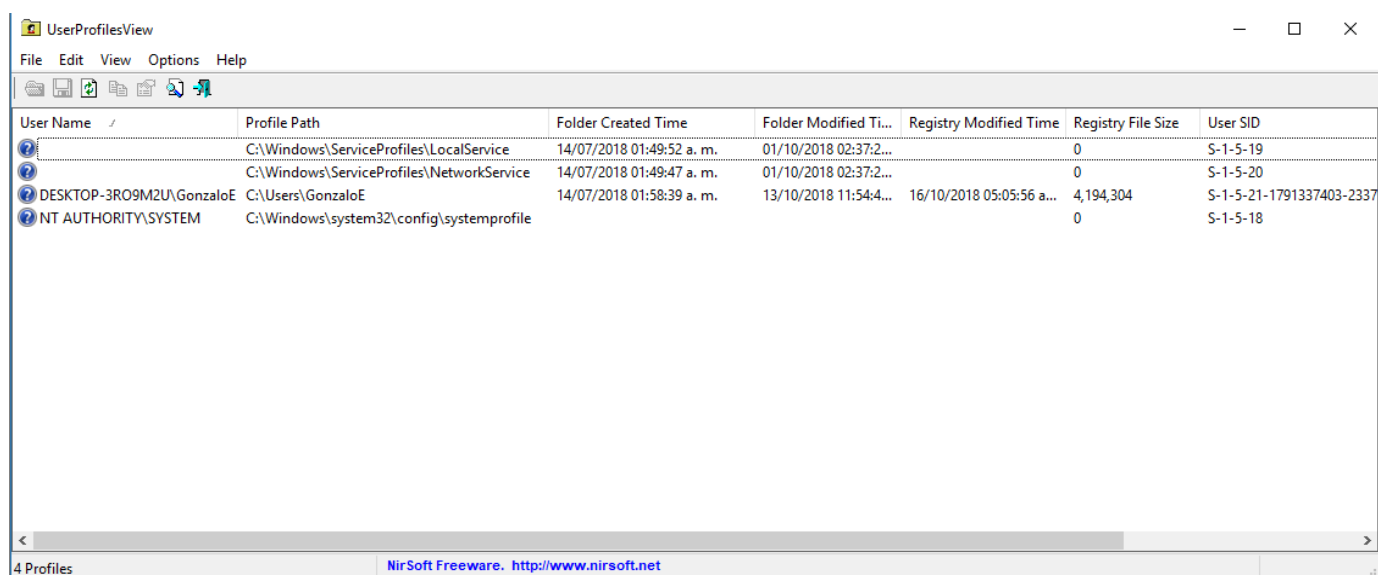
```

Hash del archivo:

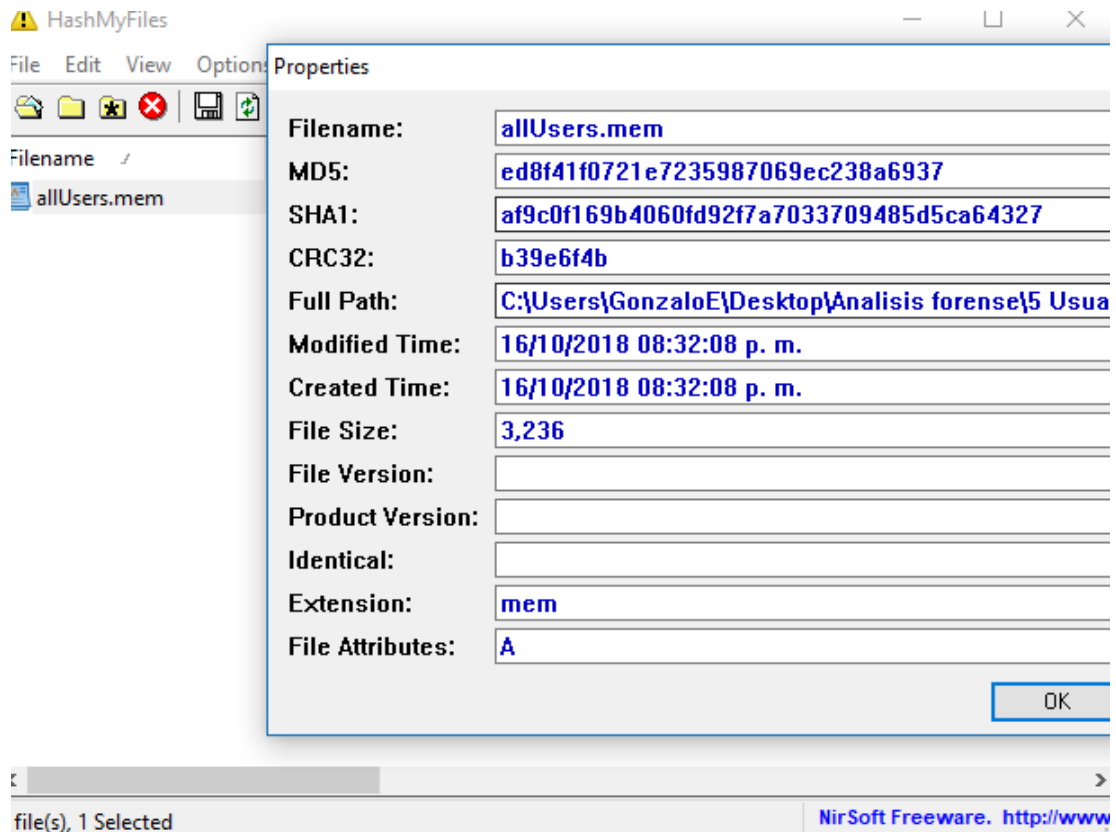


nº	Tipo de Evidencias	Nombre del archivo	Hash	Hora y Fecha	Hora Inicio-final
5	Usuarios que han iniciado sesión y listado de cuentas de usuario.	allUsers.mam	SI	20:35 p.m. -16/10/2018 GTM-4	20:35-20:40

Descripción: el programa que proporciona el sitio <http://www.nirsoft.net> "UserProfilesView.exe" nos permite ver listar todos los usuarios existentes en el sistema, dichos resultados son guardados en un archivo "allUsers.mem o allUsers.txt".



Hash de archivo:



4. INFORMACION DE RED

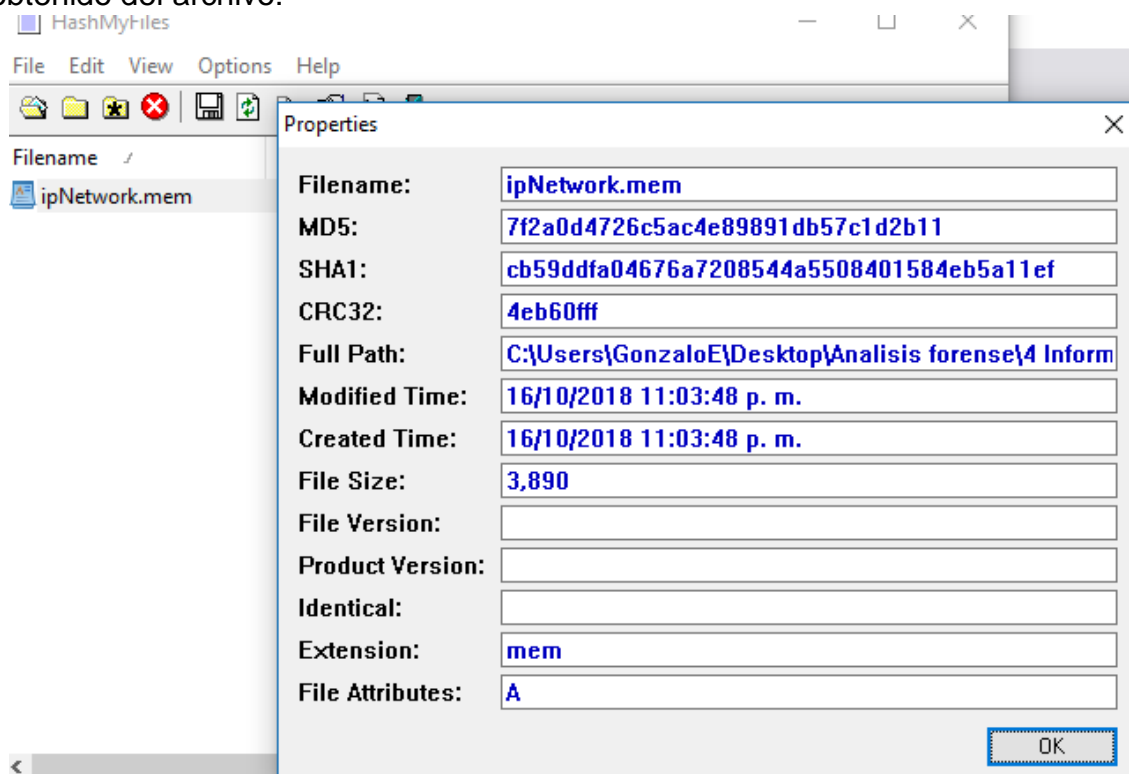
n°	Tipo de Evidencias	Nombre del archivo	Hash	Hora y Fecha	Hora Inicio-final
1	Configuracion de red (ip, dns, etc)	ipnetwork.mem	Si	23:00 p.m. -16/10/2018 GTM-4	23:00- 23:17

Descripción: en este punto se identifican la ip, el dns el dhcp, y otras características del captador de red, esta información es brindada por la aplicación “awatch.exe”, dicha información esta almacena con el nombre de ipNetwork.mem o txt. La información se muestra a continuación:

AdapterWatch				
File Edit View Options Help				
Network Adapters TCP/UDP Statistics IP Statistics ICMP Statistics General				
Entry Name	Realtek PCIe GBE Family Controller	VirtualBox Host-Only Ethernet Adapter	VirtualBox Host-Only Ethernet Adapter #2	VMware Virtual Ethernet Adap
Adapter Type	Ethernet	Ethernet	Ethernet	Ethernet
DHCP Enabled	Yes	Yes	No	Yes
IP Addresses	0.0.0.0 (0.0.0.0)	169.254.102.92 (255.255.0.0)	192.168.99.1 (255.255.255.0)	192.168.226.1 (255.255.255.0)
Default Gateway	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
DHCP Server	0.0.0.0	0.0.0.0		192.168.226.254
WINS Enabled	No	No	No	No
Primary WINS Server				
Secondary WINS Server				
DHCP Lease Obtained At	N/A	N/A	N/A	16/10/2018 11:02:34 p. m.
DHCP Lease Expires At	N/A	N/A	N/A	16/10/2018 11:32:34 p. m.
IP Address Auto-Configurati...	Enabled	Enabled	Enabled	Enabled
IP address auto-configured ...	No	Yes	No	No
DNS Servers				
Maximum Transmission Uni...	1500	1500	1500	1500
Interface Speed (Bits Per Sec...	0	100,000,000	100,000,000	100,000,000
Enabled/Disabled	Enabled	Enabled	Enabled	Enabled
Operational Status	Non Operational	Operational	Operational	Operational
Received Data	0 Bytes	0 Bytes	0 Bytes	28 Bytes
Sent Data	0 Bytes	3,019,379 Bytes	1,830,967 Bytes	894 Bytes

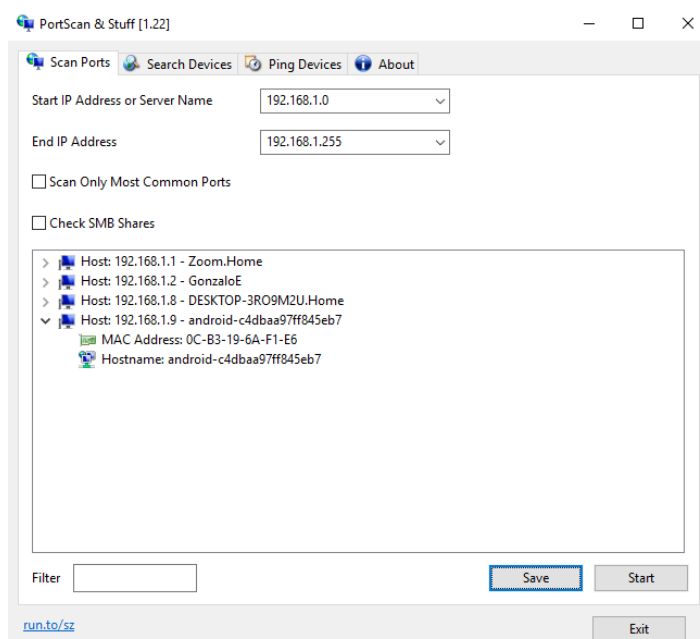
10 Adapter(s)

Hash obtenido del archivo:

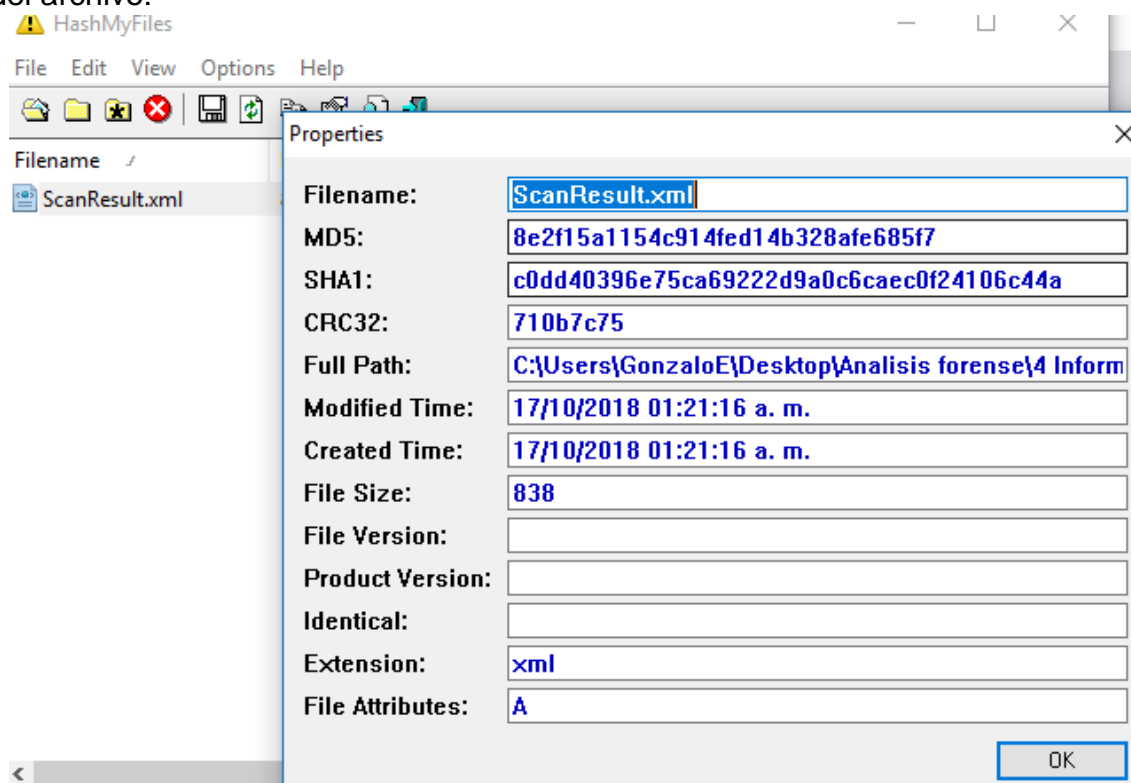


nº	Tipo de Evidencias	Nombre del archivo	Hash	Hora y Fecha	Hora Inicio-final
2	Estado de la red	ScanResult.xml	Si	01:26.p.m. -17/10/2018 GTM-4	01:20 - 01:27

Descripción: para identificar el estado de la red se emple el programa de portScant, este programa escanea los dispositivos que están conectados a la red, y permite ver su estado.



Hash del archivo:



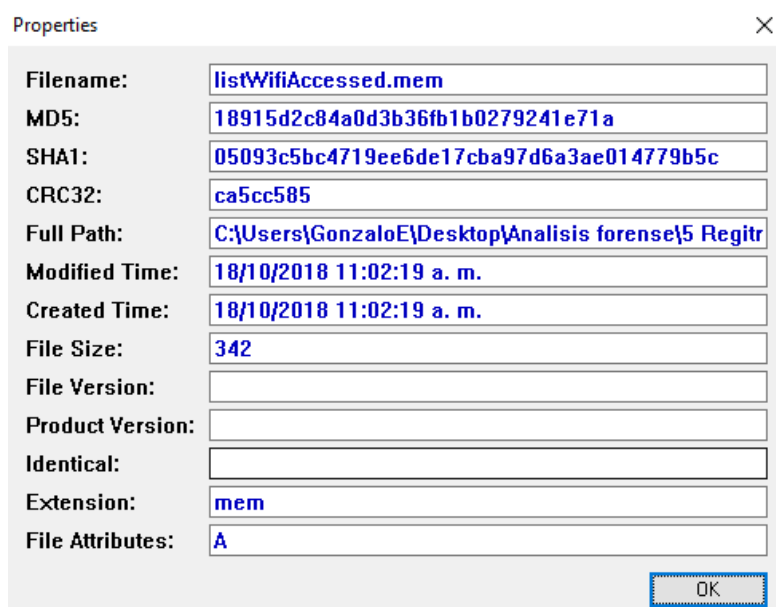
5. Registros de Windows.

n°	Tipo de Evidencias	Nombre del archivo	Hash	Hora y Fecha	Hora Inicio-final
1	Listado de redes WIFI a las que se ha conectado un equipo	listWifiAccessed.mem	Si	11:18p.m. -16/10/2018 GTM-4	11:18- 11:20

Descripción: El archivo obtenido muestra todas las conexiones wi-fi a las que se accedió, para ello se empleó el comando “**netsh wlan show profile**”, el resultado se muestra en la imagen:

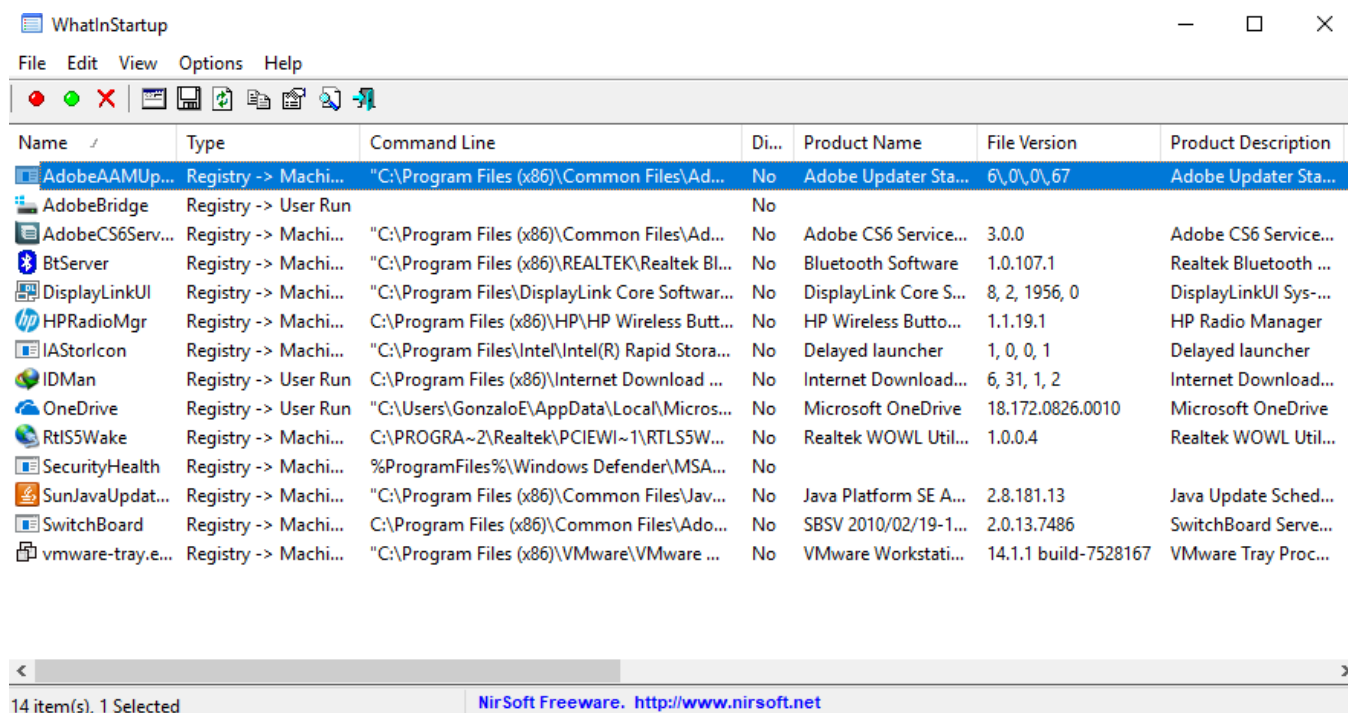
```
c:\Users\GonzaloE\Desktop\Análisis forense\5 Registro de Windows_\1 lista de redes wifi a las que se conectado un equipo>netsh wlan show profile
Perfiles en la interfaz Wi-Fi:
Perfiles de directiva de grupo (solo lectura)
-----
<Ninguno>
Perfiles de usuario
-----
Perfil de todos los usuarios : SaMiAn
Perfil de todos los usuarios : Wifi-Espinoza
Perfil de todos los usuarios : GonzaloE
```

Hash del archivo:

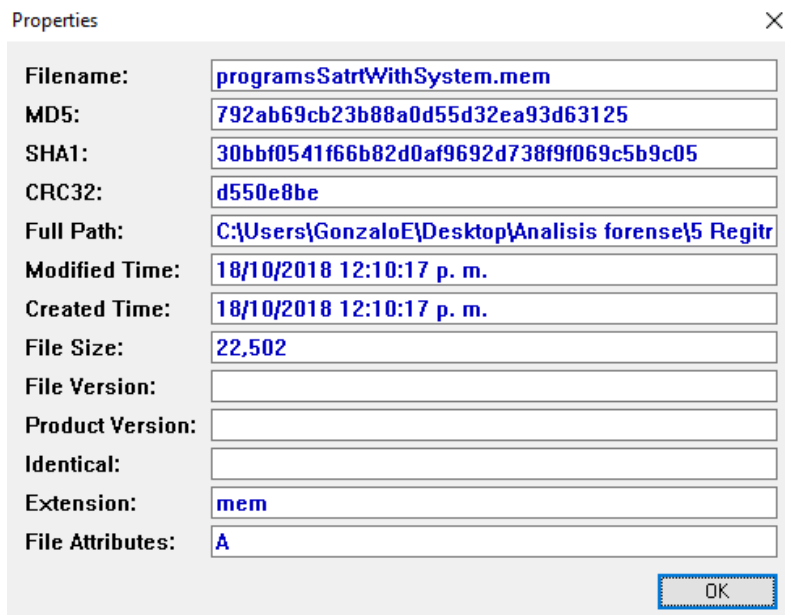


n°	Tipo de Evidencias	Nombre del archivo	Hash	Hora y Fecha	Hora Inicio-final
3	Programas que se ejecutan al iniciar el sistema operativo.	programsSatrtWithSystem.mem	Si	12:10p.m. -16/10/2018 GTM-4	12:10- 12:28

Descripción: “WhatInStartup.exe” esta herramienta muestra todos los programas que inician con el sistema, como se muestra en la imagen:

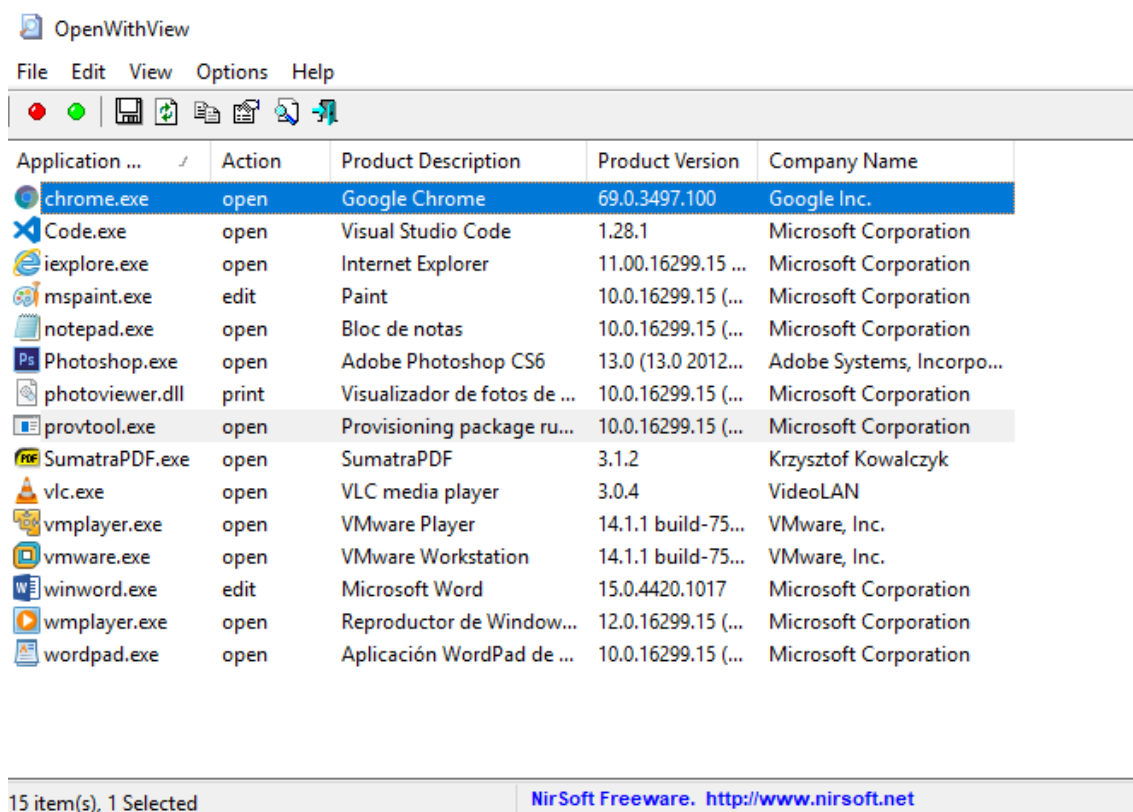


Hash del archivo generado:



nº	Tipo de Evidencias	Nombre del archivo	Hash	Hora y Fecha	Hora Inicio-final
4	Extensiones de ficheros y programas asociados para abrirlos.	OpenWithView.mem	Si	12:30p.m. -18/10/2018 GTM-4	12:30- 12:38

Descripción: “OpenWithView.exe” esta aplicación permite ver los programas asociados a los ficheros que puede abrirlos, como se muestra a continuación:



Hash asociado al archivo resultante:

Properties

Filename: OpenWithView.mem

MD5: ceeaa03f4d3ecedc3b745a1eb492967a

SHA1: a2ad0e94a3e640e3a11b096067573d78bab9859d

CRC32: b6312141

Full Path: C:\Users\GonzaloE\Desktop\Análisis forense\5 Regitr

Modified Time: 18/10/2018 12:34:13 p. m.

Created Time: 18/10/2018 12:34:13 p. m.

File Size: 8,870

File Version:

Product Version:

Identical:

Extension: mem

File Attributes: A

OK

n°	Tipo de Evidencias	Nombre del archivo	Hash	Hora y Fecha	Hora Inicio-final
5	Ficheros abiertos recientemente	RecentDocs-20181018-1634.reg	Si	16:30p.m. - 18/10/2018 GTM-4	16:30- 16:38

Descripción: el archivo archivos_recientes.bat permite mostrara todos los ficheros abiertos recientemente, el archivo generado es:

archivos_recientes.bat	18/10/2018 09:53 ...	Archivo por lotes ...	1 KB
hash-RecentDocs-Captura.PNG	18/10/2018 10:23 ...	Archivo PNG	10 KB
RecentDocs-20181018-1634.reg	18/10/2018 04:34 ...	Entradas de registro	553 KB
RecentDocs-20181018-2153.txt	18/10/2018 09:53 ...	Documento de tex...	555 KB

Hash del archivo generado:

Properties

Filename: RecentDocs-20181018-1634.reg

MD5: 1590fe53c0f5a35342be4177e5037057

SHA1: fe319caf0a5e02ae542422d0f1df55d48ad05616

CRC32: 7cb3eebd

Full Path: C:\Users\GonzaloE\Desktop\Análisis forense\5 Regitr

Modified Time: 18/10/2018 04:34:18 p. m.

Created Time: 18/10/2018 04:34:18 p. m.

File Size: 565,628

File Version:

Product Version:

Identical:

Extension: reg

File Attributes: A

OK

n°	Tipo de Evidencias	Nombre del archivo	Hash	Hora y Fecha	Hora Inicio-final
6	Software instalado.	SoftwareInstalado-20181018-2257.reg	Si	23:00p.m. -18/10/2018 GTM-4	23:00- 23:07

Descripción: la aplicación software instalado.bat permite mostrar todo el software que está instalado, al ejecutarlo la aplicación genera un archivo con una lista de todas las aplicaciones instaladas en un archivo llamado *SoftwareInstalado-20181018-2257.reg* como se muestra:

```
GonzaloE@DESKTOP-3R09M2U MINGW64 ~/Desktop/Análisis forense/5 Registro de windows_/6 Software instalado
$ cat SoftwareInstalado-20181018-2257.reg
cat Software Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\Software\Microsoft\windows\CurrentVersion\uninstall]

[HKEY_LOCAL_MACHINE\Software\Microsoft\windows\CurrentVersion\uninstall\AddressBook]

[HKEY_LOCAL_MACHINE\Software\Microsoft\windows\CurrentVersion\uninstall\AMD Catalyst Install Manager]
"InstallDir"="C:\\Program Files\\AMD\\CIM"
"EstimatedSize"=dword:00012d1b
"InstallDate"=""
"InstallLocation"="C:\\Program Files\\AMD\\CIM\\BIN64"
"InstallSource"=""
"Readme"=""
"Size"=""
"URLUpdateInfo"=""
"NoModify"=dword:00000000
"Version"=dword:08000394
"Language"=dword:00000000
"DisplayName"="AMD Software"
"Publisher"="Advanced Micro Devices, Inc."
"HelpLink"="http://www.amd.com"
"URLInfoAbout"="http://support.amd.com"
"AuthorizedCDFPrefix"=""
"Comments"=""
"Contact"="AMD Customer Support"
"HelpTelephone"="905-882-2600"
"DisplayVersion"="17.12"
"DisplayIcon"="C:\\Program Files\\AMD\\CIM\\BIN64\\RadeonInstaller.exe "
"UninstallString"="C:\\Program Files\\AMD\\CIM\\BIN64\\RadeonInstaller.exe /EXPRESS_UNINSTALL /IGNORE_UPGRADE /ON_REBOOT_MESSAGE:NO"
"ModifyPath"="C:\\Program Files\\AMD\\CIM\\BIN64\\RadeonInstaller.exe /CUSTOM_UNINSTALL /IGNORE_UPGRADE /ON_REBOOT_MESSAGE:NO"

[HKEY_LOCAL_MACHINE\Software\Microsoft\windows\CurrentVersion\uninstall\Android Studio]
"DisplayName"="Android Studio"
"DisplayVersion"="1.0"
"Publisher"="Google Inc."
```

Hash del archivo generado:

Properties

Filename:

SoftwareInstalado-20181018-2257.reg

MD5:

ea0fba05e7af721c8275694a11bdfa76

SHA1:

84fb893505438147d018d176c822edd4c189dad8

CRC32:

09e2b237

Full Path:

C:\Users\GonzaloE\Desktop\Análisis forense\5 Registr

Modified Time:

18/10/2018 10:57:45 p. m.

Created Time:

18/10/2018 10:57:45 p. m.

File Size:

123,798

File Version:

Product Version:

Identical:

Extension:

reg

File Attributes:

A

OK

6. Datos más relevantes

n°	Tipo de Evidencias	Nombre del archivo	Hash	Hora y Fecha	Hora Inicio-final
1	Contraseñas	ResulPassword.txt	SI	00:00 p.m. -16/10/2018 GTM-4	00:00-00:05

Descripción: la aplicación “NetUsers.exe” permite ver todas las contraseñas utilizadas en el sistema.

```
C:\Users\GonzaloE\Desktop\Análisis forense\6 Datos más relevantes_\1 Contraseñas>NetUsers.exe

-----
Current users logged on locally at DESKTOP-3R09M2U:
-----

The command completed successfully.
```

Hash del archivo generado:

Properties

Filename:

ResulPassword.mem

MD5:

283edff82746a2b5de0cca62ea36e30f

SHA1:

1a1accdc516b0045df7497092b8d2a9d32deabc4

CRC32:

fd10f566

Full Path:

C:\Users\GonzaloE\Desktop\Análisis forense\6 Datos

Modified Time:

18/10/2018 11:56:30 p. m.

Created Time:

18/10/2018 11:56:13 p. m.

File Size:

339

File Version:

Product Version:

Identical:

Extension:

mem

File Attributes:

A

OK

n°	Tipo de Evidencias	Nombre del archivo	Hash	Hora y Fecha	Hora Inicio-final
2	Dispositivos USB conectados.	usbHistory.txt/ USBDevview.txt	SI	00:58 p.m. -16/10/2018 GTM-4	00:58-00:59
2.1			Si	00:58 p.m. -17/10/2018 GTM-4	00:58-00:59

Descripción: la aplicación “usbHistory.exe” ejecutada desde la consola de comandos de Windows permite ver todos los dispositivos que se conectaron a la laptop.

```

C:\Users\GonzaloE\Desktop\Análisis forense\6 Datos más relevantes_\2 Dispositivos USB conectados>usbHistory.exe
USB History Dump
by naby (c)2008

(1) --- hp c350o USB Device
      instanceID: B1303110001840&0
      ParentIDPrefix:
      Driver:{4d36e967-e325-11ce-bfc1-08002be10318}\0001
      Disk Stamp: 07/13/2018 21:49
      Volume Stamp: 08/31/2018 18:05

(2) --- hp v165w USB Device
      instanceID: AA00000000001179&0
      ParentIDPrefix:
      Driver:{4d36e967-e325-11ce-bfc1-08002be10318}\0007
      Disk Stamp: 09/30/2018 20:19
      Volume Stamp: 08/31/2018 18:05

(3) --- hp v221w USB Device
      instanceID: 0524900000006418&0
      ParentIDPrefix:
      Driver:{4d36e967-e325-11ce-bfc1-08002be10318}\0004
      Disk Stamp: 07/24/2018 14:29
      Volume Stamp: 08/31/2018 18:05

(4) --- Linux File-CD Gadget USB Device
      instanceID: 7PH6CYQCUG5TZHSK&0
      ParentIDPrefix:
      Driver:{4d36e967-e325-11ce-bfc1-08002be10318}\0006
      Disk Stamp: 08/24/2018 10:26
      Volume Stamp: 08/31/2018 18:05

(5) --- Mass Storage Device USB Device

```

Hash del archivo generado:

Properties

Filename:	usbHistory.txt
MD5:	8b22fb78ede768929bba9896deabda41
SHA1:	b0329825d6f92070a9711393cdf848830b556519
CRC32:	8dd00778
Full Path:	C:\Users\GonzaloE\Desktop\Análisis forense\6 Datos
Modified Time:	19/10/2018 12:56:07 a. m.
Created Time:	19/10/2018 12:56:07 a. m.
File Size:	1,534
File Version:	
Product Version:	
Identical:	
Extension:	.txt
File Attributes:	A

OK

Descripción 2.1: el programa “*USBDeview.exe*” muestra todos los dispositivos USB conectados actualmente. Como se muestra a continuación:

USBDeview

File Edit View Options Help

Device Name	Description	Device Type	Connected	Safe To Unpl...	D...	USB Hub
0000.0014.0000.004.00...	SM-J730G	Unknown	No	Yes	No	No
0000.0014.0000.004.00...	Dispositivo serie USB	Communication	No	Yes	No	No
0000.0014.0000.004.00...	ADB Device	Vendor Specific	No	No	No	No
0000.0014.0000.005.00...	SM-G532M	Unknown	No	Yes	No	No
0000.0014.0000.005.00...	Dispositivo serie USB	Communication	No	Yes	No	No
0000.0014.0000.005.00...	ADB Device	Vendor Specific	No	No	No	No
0000.0014.0000.006.00...	USB Video Device	Video	Yes	Yes	No	No
0000.0014.0000.006.00...	hp c350o USB Device	Mass Storage	Yes	Yes	No	No
Port_#0004.Hub_#0001	hp v165w USB Device	Mass Storage	No	Yes	No	No
Port_#0004.Hub_#0001	USB Composite Device	Unknown	No	Yes	No	No
Port_#0004.Hub_#0001	USB Input Device	HID (Human Interface D...	No	Yes	No	No
Port_#0005.Hub_#0001	Unknown USB Device (Device ...	Unknown	No	No	No	No
Port_#0005.Hub_#0001	hp v221w USB Device	Mass Storage	No	Yes	No	No
Port_#0005.Hub_#0001	USB Composite Device	Unknown	No	Yes	No	No
Port_#0005.Hub_#0001	Linux File-CD Gadget USB Dev...	Mass Storage	No	Yes	No	No
Port_#0005.Hub_#0001	Mass Storage Device USB Devi...	Mass Storage	No	Yes	No	No
Port_#0006.Hub_#0001	USB Composite Device	Unknown	Yes	Yes	No	No

21 item(s), 1 Selected

NirSoft Freeware. <http://www.nirsoft.net> usb.ids is not loaded

Hash del archivo generado:

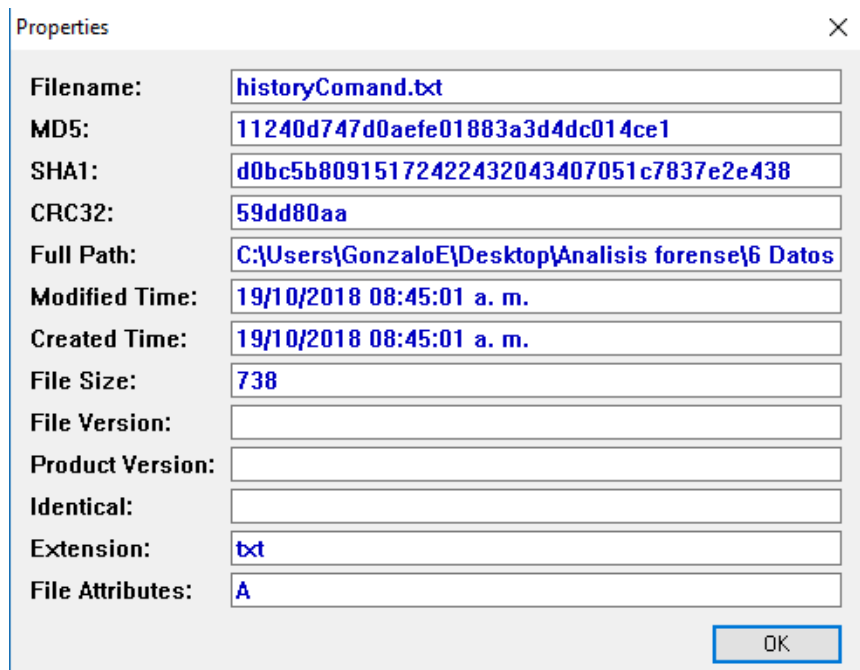
Filename:	USBDeview.txt
MD5:	0636c341e9ee97fb98639054b6abddc1
SHA1:	d973249c51d2eb4b12439f53091db69ac1a274c3
CRC32:	de16f1a4
Full Path:	C:\Users\GonzaloE\Desktop\Análisis forense\6 Datos
Modified Time:	19/10/2018 07:37:10 a. m.
Created Time:	19/10/2018 07:37:10 a. m.
File Size:	1,295
File Version:	
Product Version:	
Identical:	
Extension:	txt
File Attributes:	A
OK	

n°	Tipo de Evidencias	Nombre del archivo	Hash	Hora y Fecha	Hora Inicio-final
3	Histórico del intérprete de comandos	historyComand.txt	Si	08:47 p.m. -19/10/2018 GTM-4	08:40-08:49

Descripción: el comando “*doskey /history*” muestra el historial de comando de cmd como se muestra en la imagen.

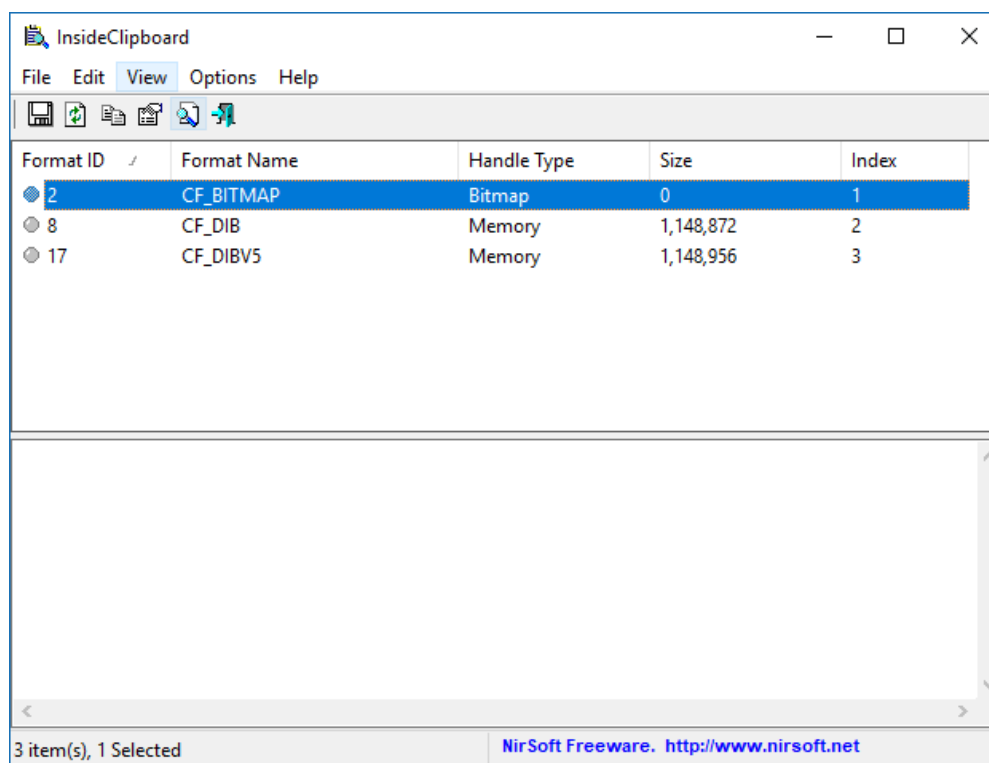
```
C:\Users\GonzaloE\Desktop\Análisis forense\6 Datos más relevantes__\3 Histórico del intérprete de comandos>doskey /history
dir
cd ..
dir
cd "6 Software instalado"
cls
dir
cd ..
dir
cd 6
cd "6 Datos más relevantes__"
dir
"1 Contraseñas"
cd "1 Contraseñas"
die
dir
NetUsers.exe
cls
NetUsers.exe
cat NetUsers.exe
cat NetUsers.exe >> ResulPassword.mem
NetUsers.exe >> ResulPassword.mem
clear
cls
NetUsers.exe >> ResulPassword.txt
NetUsers.exe
cd ..
dir
cd 2
cd "2 Dispositivos USB conectados"
dir
cls
dir
usbHistory.exe
cls
usbHistory.exe >> usbHistory.txt
usbHistory.exe >> usbHistory.mem
usbHistory.exe
```

Hash del archivo generado:

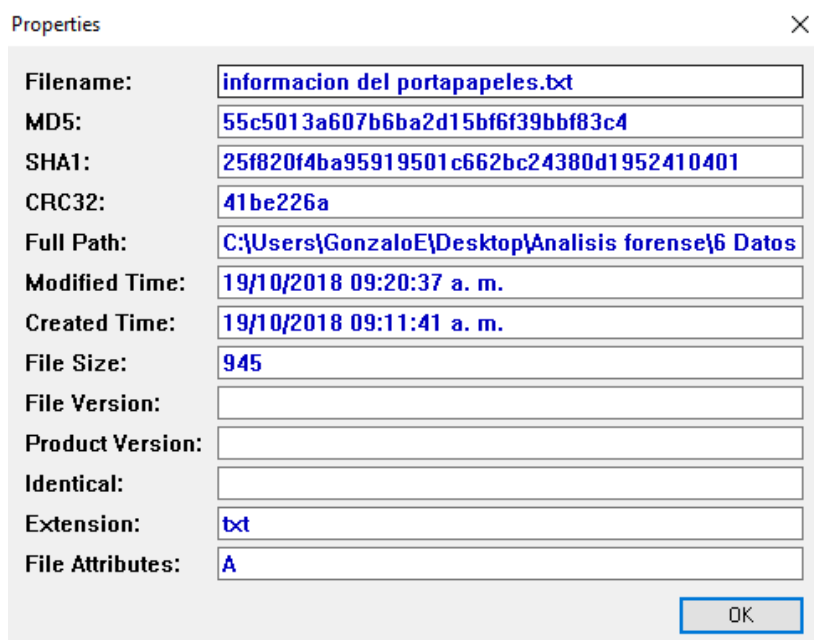


n°	Tipo de Evidencias	Nombre del archivo	Hash	Hora y Fecha	Hora Inicio-final
4	Información del portapapeles	informacion del portapapeles.txt	SI	09:10 p.m. -19/10/2018 GTM-4	09:10-09:14

Descripción: el aplicativo “InsideClipboard.exe” permite ver la información del portapapeles:

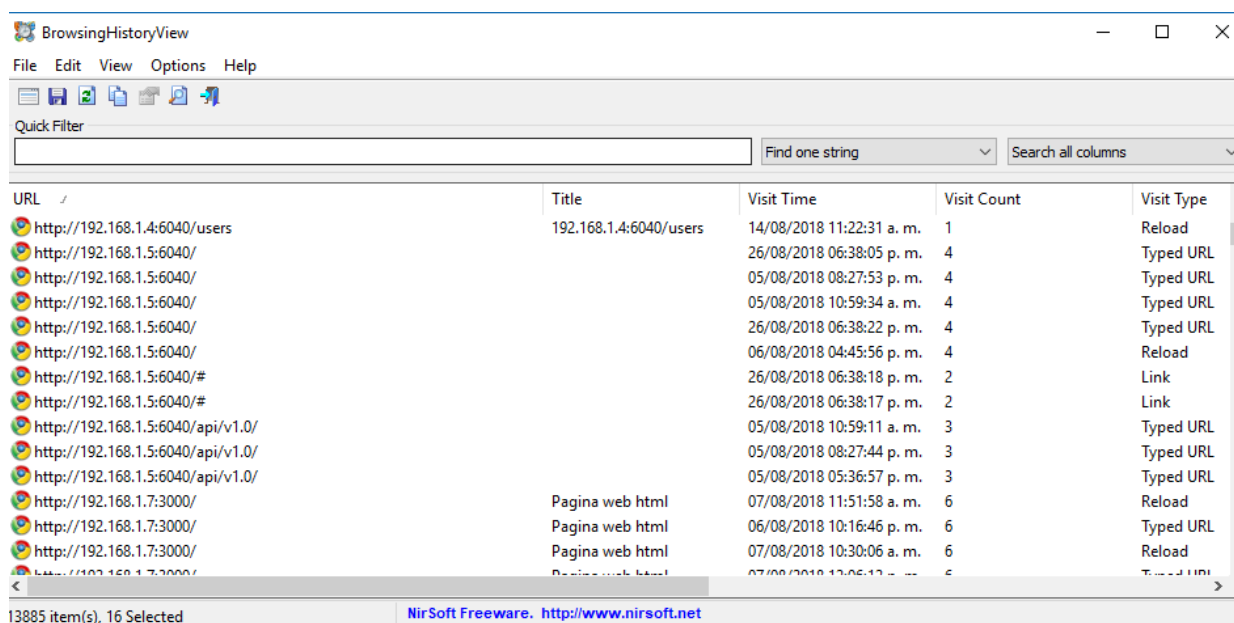


Hash del archivo generado:

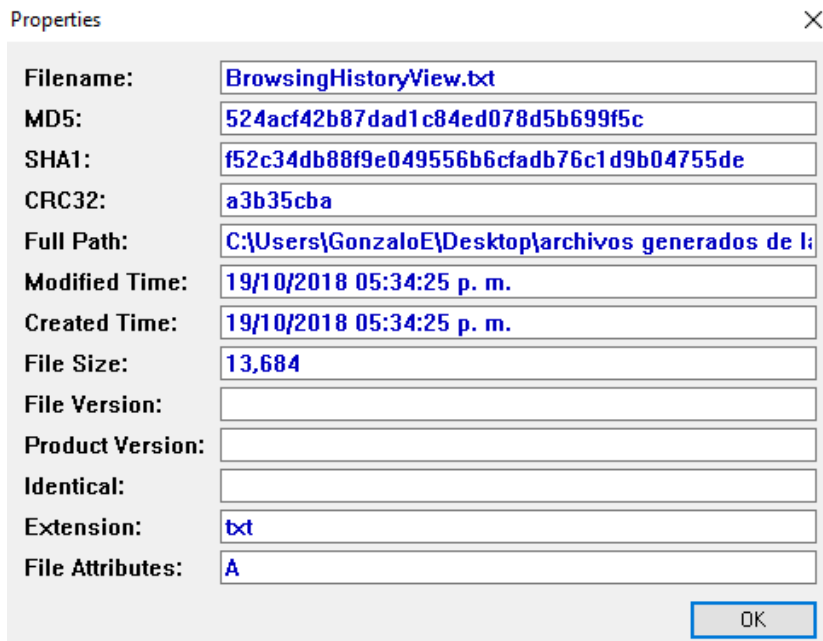


n°	Tipo de Evidencias	Nombre del archivo	Hash	Hora y Fecha	Hora Inicio-final
5	Historial de internet	BrowsingHistoryView.txt	SI	17:39 P.m. -19/10/2018 GTM-4	17:40-17:40

Descripción: las aplicación “BrowsingHistoryView.exe” es una utilidad que lee los datos históricos de 4 diferentes navegadores web (Internet Explorer, Mozilla Firefox, Google Chrome y Safari) y muestra el historial de navegación de todas estas páginas web. Los navegadores en una tabla. La tabla de historial de navegación incluye lo siguiente Información: URL visitada, título, tiempo de visita, recuento de visitas, navegador web y Perfiles de los usuarios.

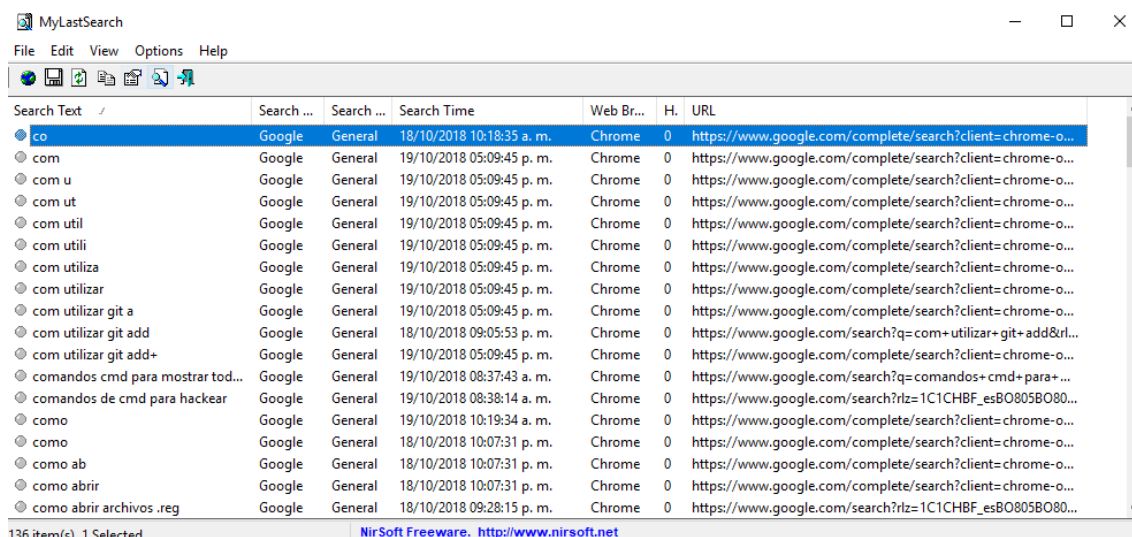


Hash del archivo generado:

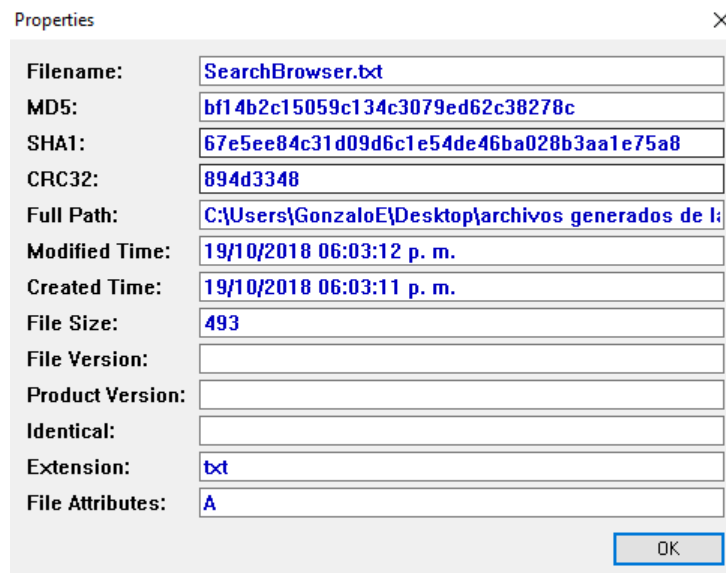


n°	Tipo de Evidencias	Nombre del archivo	Hash	Hora y Fecha	Hora Inicio-final
6	Últimas búsquedas	SearchBrowser.txt	Si	17:54 P.m. -19/10/2018 GTM-4	17:54-17:55

Descripción: La utilidad MyLastSearch escanea el caché y los archivos históricos de su Web navegador, y busque todas las consultas de búsqueda que haya realizado con más buscadores populares (Google, Yahoo y MSN) y con redes sociales populares Sitios de redes (Twitter, Facebook, MySpace). Las consultas de búsqueda que usted hizo se muestran en una tabla con las siguientes columnas: Buscar Texto, Motor de búsqueda, Tiempo de búsqueda, Tipo de búsqueda (General, Video, Imágenes)...Etc.

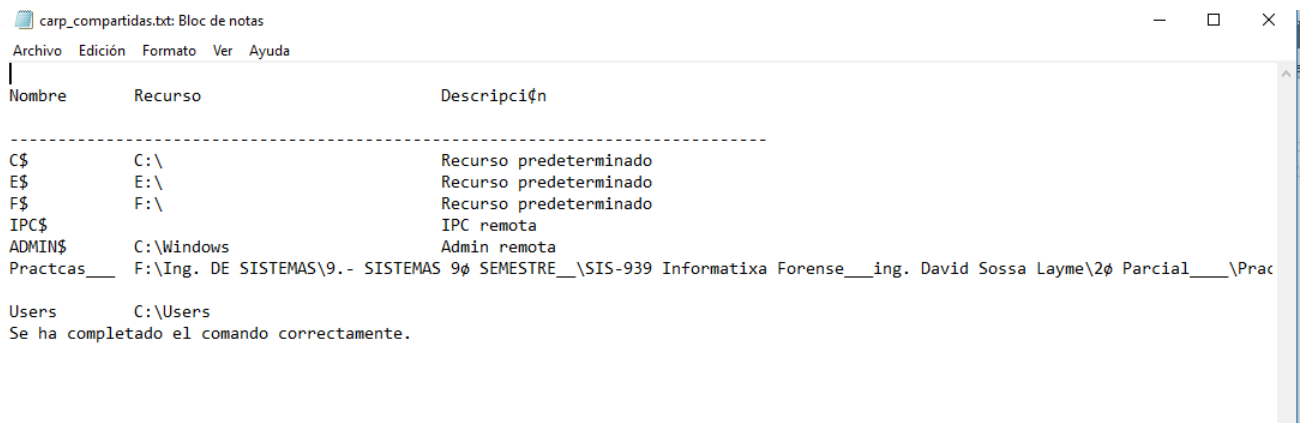


Hash del archivo generado:



nº	Tipo de Evidencias	Nombre del archivo	Hash	Hora y Fecha	Hora Inicio-final
8	Carpetas compartidas	carp_compartidas.txt	Si	09:34 a.m-19/10/2018 GTM-4	09.34-09:35

Descripción: la aplicación de línea de comandos **“carpetas_compartidas.bat”** nuestra todas las carpetas compartidas y los almacena en un archivo de texto para su posterior análisis, como se muestra en la imagen:



Hash del archivo generado:

Properties



Filename:	carp_compartidas.txt
MD5:	47acabd0b0ec600fc6e3f3d1a4fdadac
SHA1:	b5cb8b74958b694d5ab88aa26bfbf8cd52aa2bad
CRC32:	72d13d99
Full Path:	C:\Users\GonzaloE\Desktop\Análisis forense\8 carpel
Modified Time:	19/10/2018 09:28:36 a. m.
Created Time:	19/10/2018 09:28:36 a. m.
File Size:	829
File Version:	
Product Version:	
Identical:	
Extension:	.txt
File Attributes:	A

OK