



Análisis Forense Windows Avanzado

Este va a ser un taller para obtener información de windows

Este va a ser un taller para obtener información de windows

Ver últimos archivos modificados

Lo primero será ejecutar una consola de Windows y el directorio con el comando:

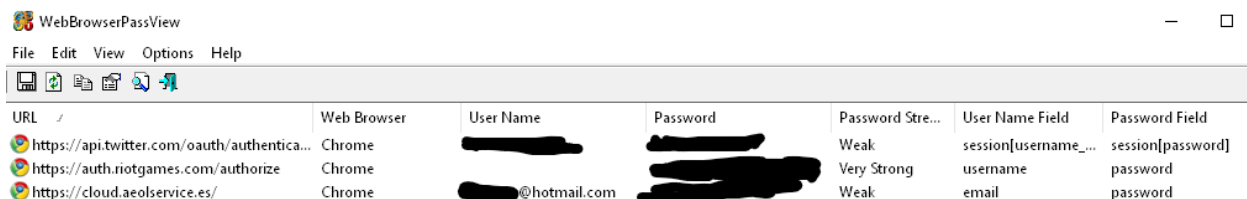
```
dir /t:w /a /s /o:d
```

```
Directorio de C:\Users\User\Desktop\cursos\datascience\Talleres\Caso_estudio_pandas
30/04/2023  22:40    <DIR>          .ipynb_checkpoints
30/04/2023  22:40             97.387 Practica1.ipynb
30/04/2023  22:40            107.572 Practica2.ipynb
30/04/2023  22:40    <DIR>          ..
30/04/2023  22:40    <DIR>          .
30/04/2023  22:40    <DIR>          datos
                2 archivos             204.959 bytes
```

Esto son archivos después de realizar un git pull

Ver contraseñas del buscador

Descargaremos WebPassView

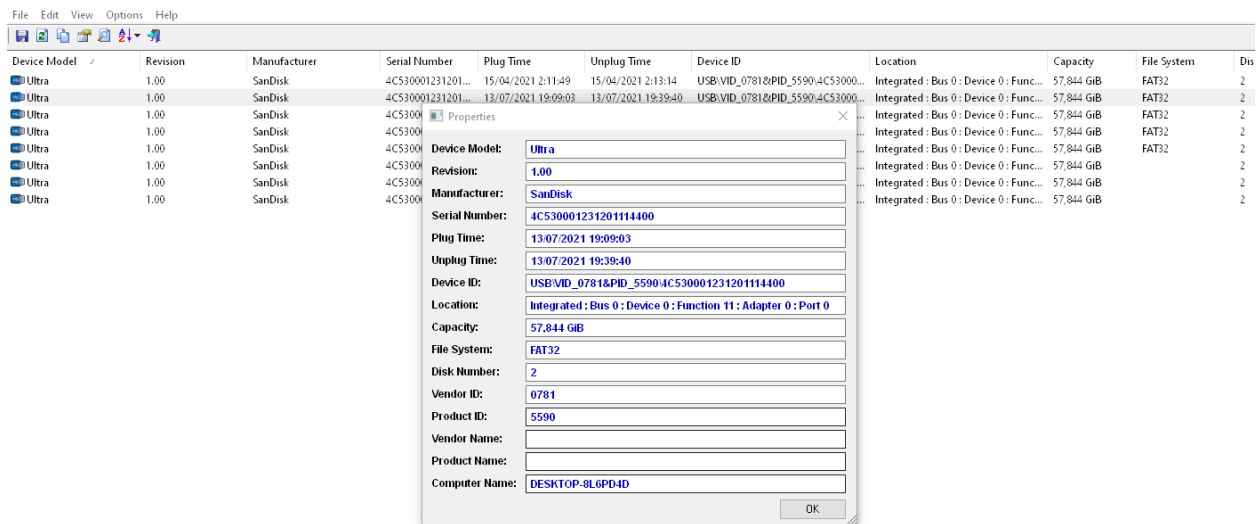


URL	Web Browser	User Name	Password	Password Stre...	User Name Field	Password Field
https://api.twitter.com/oauth/authentica...	Chrome	[REDACTED]	[REDACTED]	Weak	session[username_...	session[password]
https://auth.riotgames.com/authorize	Chrome	[REDACTED]	[REDACTED]	Very Strong	username	password
https://cloud.aeolservice.es/	Chrome	[REDACTED]@hotmail.com	[REDACTED]	Weak	email	password

Este es un ejemplo de lo que podríamos encontrar

Historial de USB

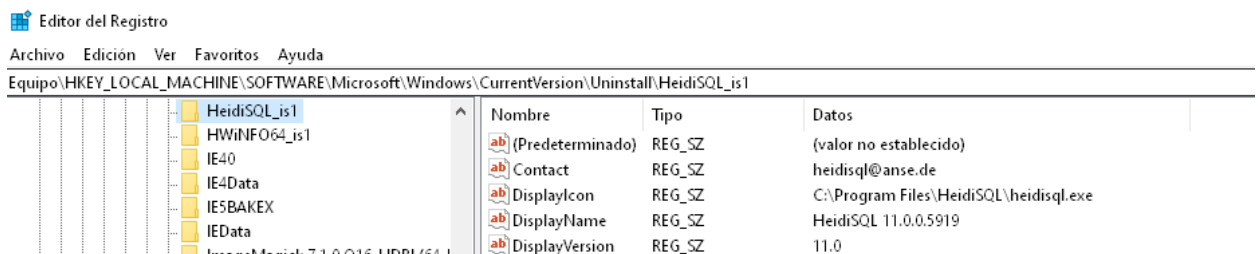
En este caso usé usbDriveLog



Registros de desinstalación

Accederemos al regedit.exe y entraremos a:

Equipo\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall



Veremos todas las aplicaciones desinstaladas

Trabajo con volcados de memoria

Instalaremos dumpIt

Y crearemos un volcado de memoria como el hecho en el curso de Análisis Forense Básico

Volatility

Una vez edscargado el volatility

Pondremos volatility.exe y nuestro volcado en un mismo directorio

Desde dentro de un cmd lanzaremos:

```
volatility.exe imageinfo -f "nombrevolcado".draw
```

```
Suggested Profile(s) : Win10x64_17134, Win10x64_10586, Win10x64_14393, Win10x64_16299, Win2016x64_14393, Win10x64_15063 (Instantiated with Win10x64_15063)
AS Layer1 : SkipDuplicatesAMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (/cases/memory/base-rd01-memory.img)
PAE type : No PAE
DTB : 0x1aa002L
KDBG : 0xf8012536c910L
Number of Processors : 2
Image Type (Service Pack) : 0
KPCR for CPU 0 : 0xfffff8012396e000L
KPCR for CPU 1 : 0xfffffe0816b440000L
```

Ahora para trabajar con uno de los perfiles usaremos

```
volatility.exe --profile="nombreperfil" pslist -f "nombrevolcado".raw
```

Para crear un archivo más legible podremos usar:

```
volatility.exe --profile="nombreperfil" svcscan -f "nombrevolcado".raw
```

Esto nos creará una carpeta con un html donde tendremos toda la información de ese volcado

662) Running Programs			
Name	Process ID	Memory	Description
cmd.exe	3888	1900KB	
cmd.exe	2244	2956KB	Windows Command Processor
conhost.exe	1816	2052KB	Console Window Host
conhost.exe	2528	4228KB	Console Window Host
conhost.exe	1868	4576KB	Console Window Host
csrss.exe	316	3060KB	Client Server Runtime Process
csrss.exe	368	5632KB	Client Server Runtime Process
csrss.exe	1656	3212KB	
DAWF.exe	1252	8768KB	DragonJAR Automatic Windows Forensic, una herramienta para automatizar el pro de extracción de información forense en entornos Windows.
dm.exe	1744	4616KB	Desktop Window Manager
explorer.exe	1848	6520KB	Windows Explorer
GoogleCrashHandler.exe	2160	532KB	Google Crash Handler
lsass.exe	480	778KB	Local Security Authority Process
lsass.exe	488	2736KB	Local Session Manager Service
SearchFilterHost.exe	3968	5752KB	Microsoft Windows Search Filter Host
SearchIndexer.exe	2576	46896KB	Microsoft Windows Search Indexer
SearchProtocolHost.exe	2240	5472KB	Microsoft Windows Search Protocol Host
services.exe	472	5500KB	Services and Controller app
smss.exe	236	736KB	
spoolsv.exe	1232	7612KB	Spooler SubSystem App
spssvc.exe	536	8896KB	Microsoft Software Protection Platform S