TAREA 01

APLICACIÓN DE METODOLOGÍAS DE ANÁLISIS FORENSES

ANÁLISIS FORENSE INFORMÁTICO

ALBA MOREJÓN GARCÍA

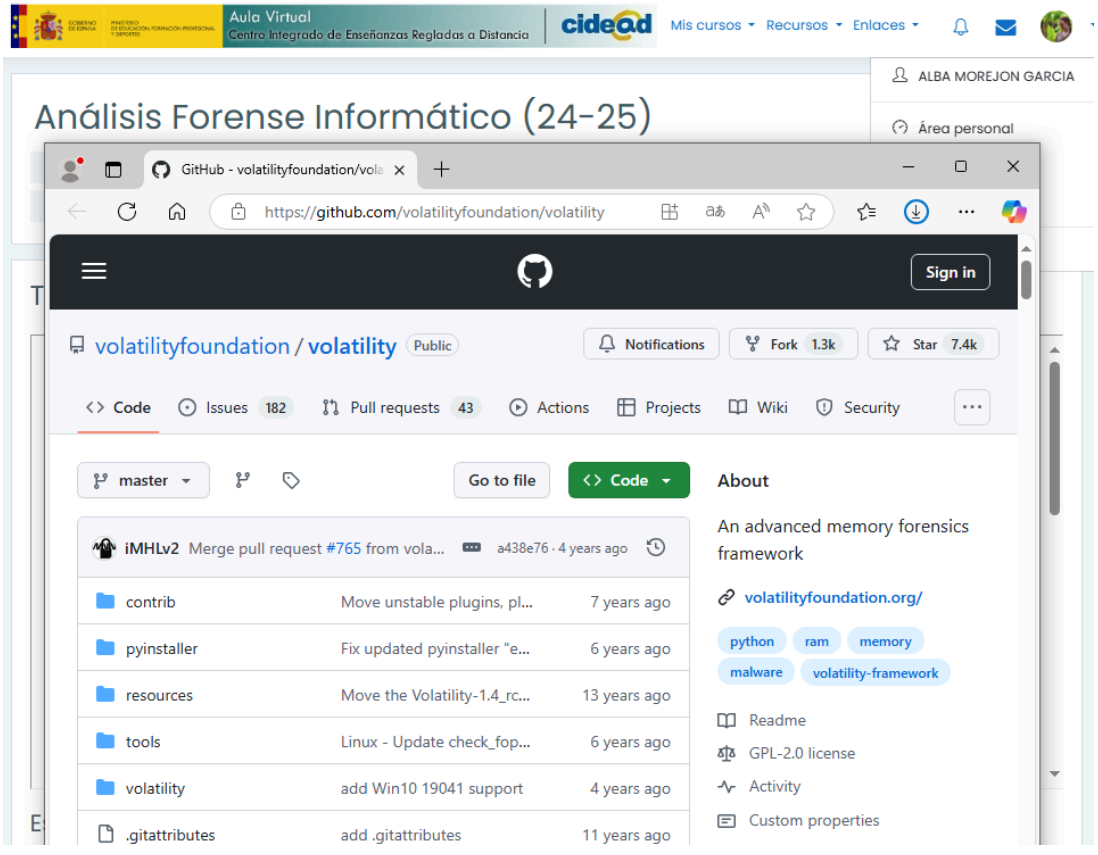
2024/2025

CETI - Ciberseguridad en Entornos de las Tecnologías de la Información

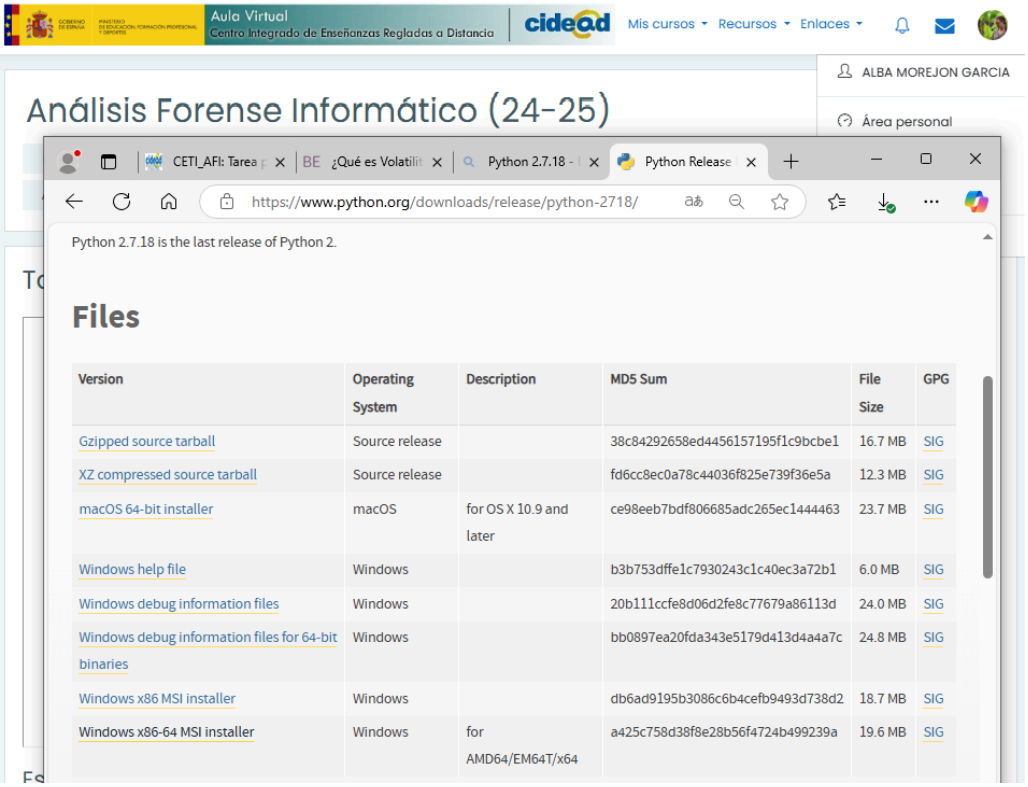
CASO PRÁCTICO
María está trabajando en un caso y ha recibido la imagen de memoria RAM de un servidor que ha tenido un comportamiento anómalo.
Un compañero sobre el terreno ha capturado la memoria RAM de la máquina antes de que la apagasen y se la ha enviado al laboratorio para ser analizada por María.
El coordinador de la investigación le ha hecho varias preguntas a María que deberá responder sobre la evidencia.

Apartado 1: Analiza la memoria RAM
Lo ideal es usar la herramienta Volatility (versión 2), la tienes disponible en Volatility
La memoria RAM está disponible en este enlace
(https://mega.co.nz/#!1UpjkTab!RP_QeooLaxA7bixLxkHLIqhWKfQ9G_0M58NSUchRn68)
Descomprime la memoria RAM
Debes de ejecutar Volatility desde consola ya sea en Windows o Linux
Tienes varias guías de vídeo que te pueden ayudar en el proceso:
https://www.youtube.com/watch?v=RFYbevw6hxI
https://www.youtube.com/watch?v=iU9mqB4h3Tg
Otras herramientas que te pueden ser útiles
Floss: https://github.com/mandiant/flare-floss

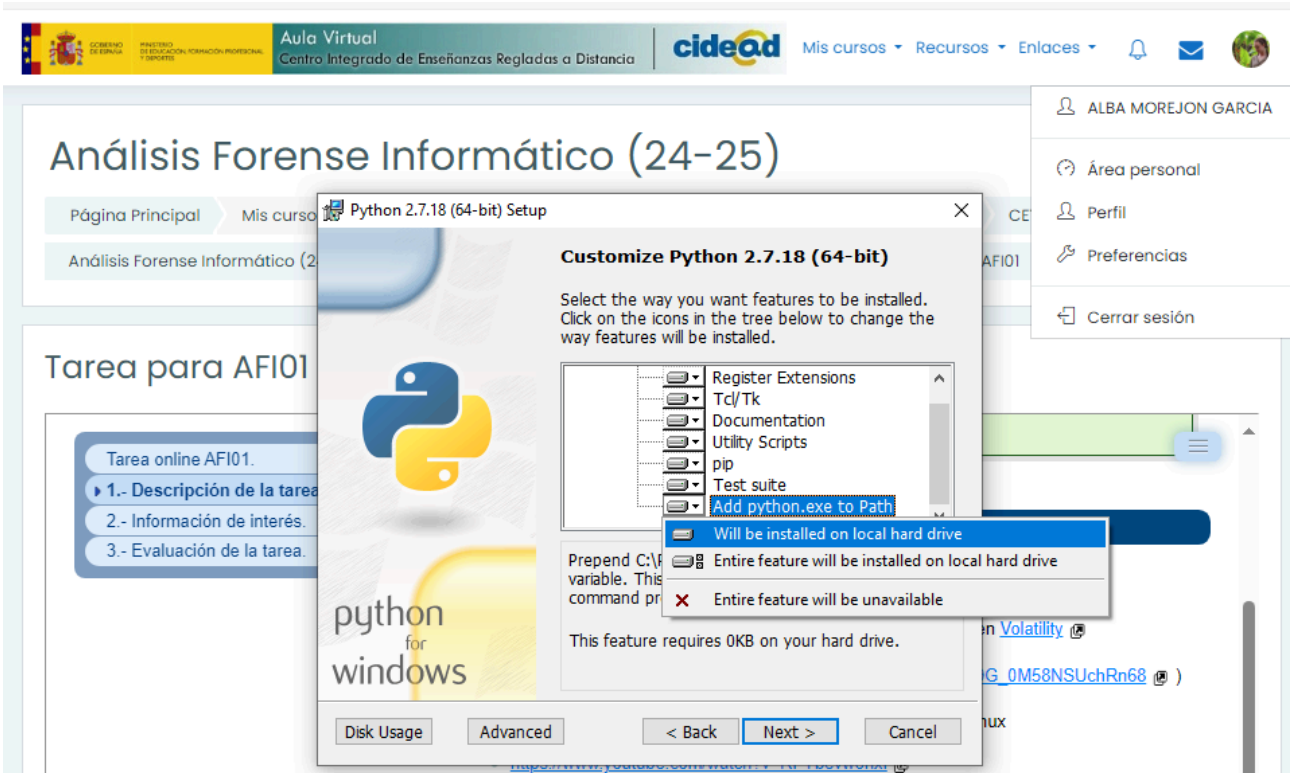
DESCARGAS E INSTALACIÖNES
Herramienta Volatility
Descargamos el .zip con los archivos .py (lenguaje python) de la pagina principal de volatility
https://volatilityfoundation.org/



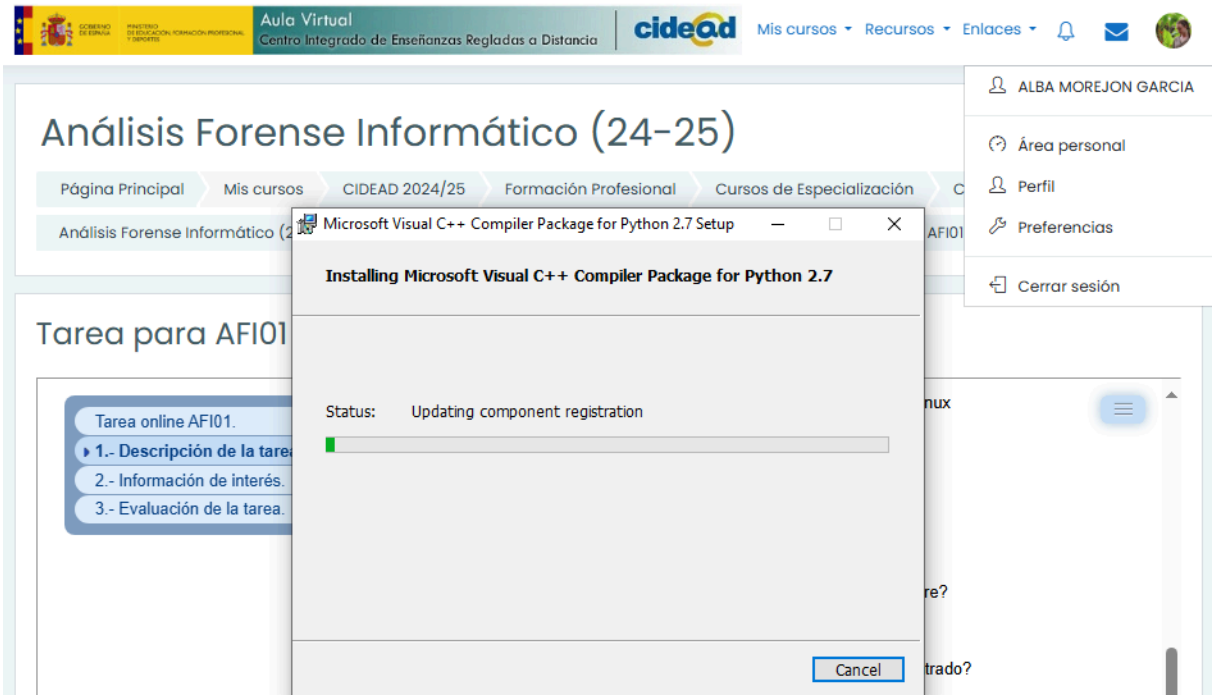
Volatility trabaja con la versión 2.7.18 de python por tanto vamos a la página principal y descargamos la versión para windows 64 desde https://www.python.org/downloads/release/python-2718/



Instalamos la versión de python descargada y cambiamos la ultima opcion para que se instale en el disco local

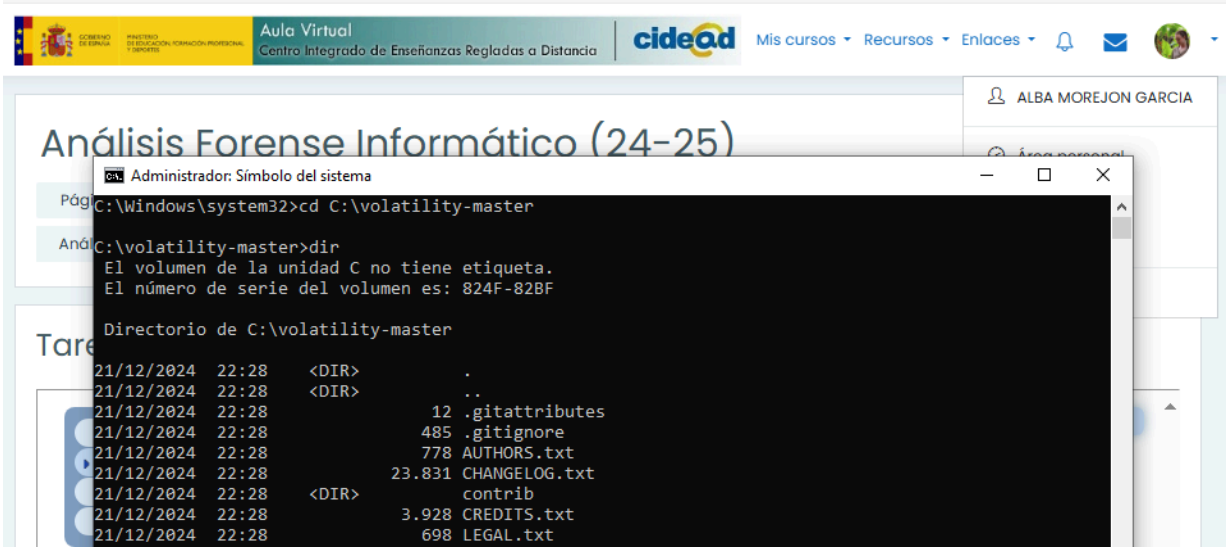


Descargamos C++ la versión compatible con el python instalado (v 2.7.18) https://archive.org/details/vcfor-python-27 y lo instalamos.



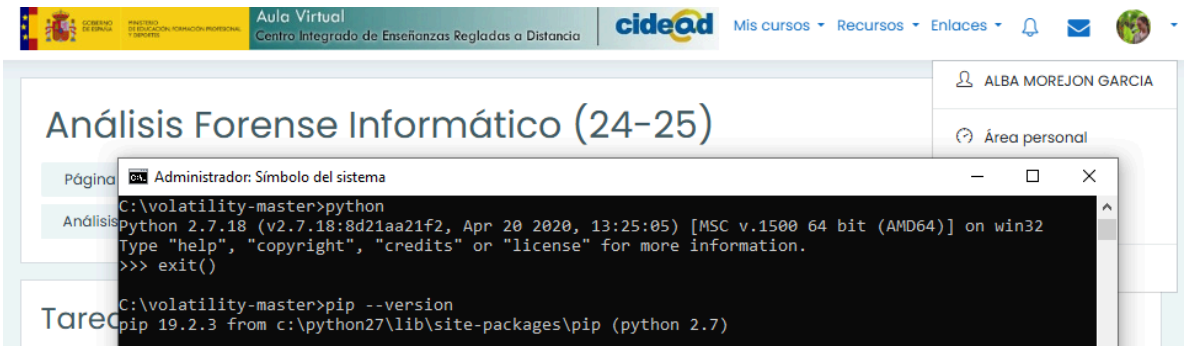
Dependencias recomendadas: https://github.com/volatilityfoundation/volatility/wiki/installation

Nos situamos en la carpeta donde hemos descomprimido el archivo de volatility

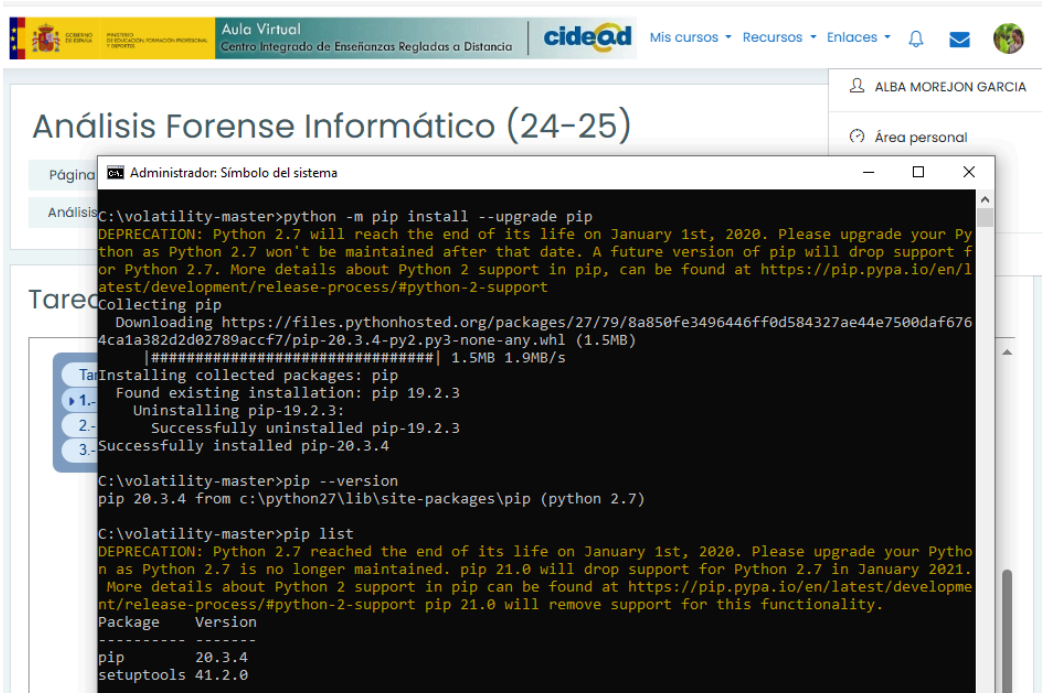


Revisamos la versión de python y la de pip:

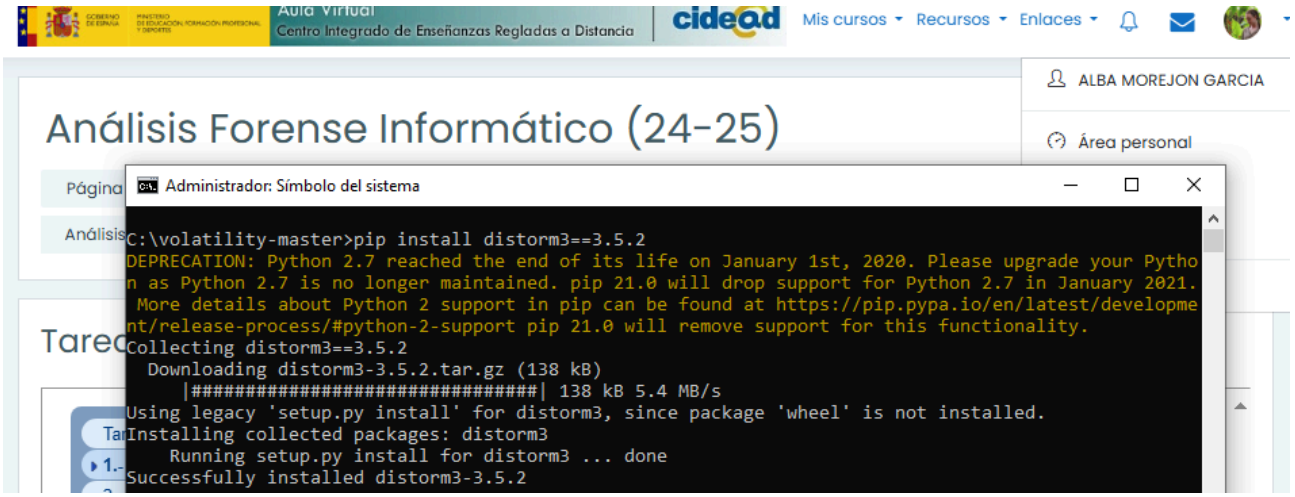
- Python 2.7.18
- PIP 19.2.3



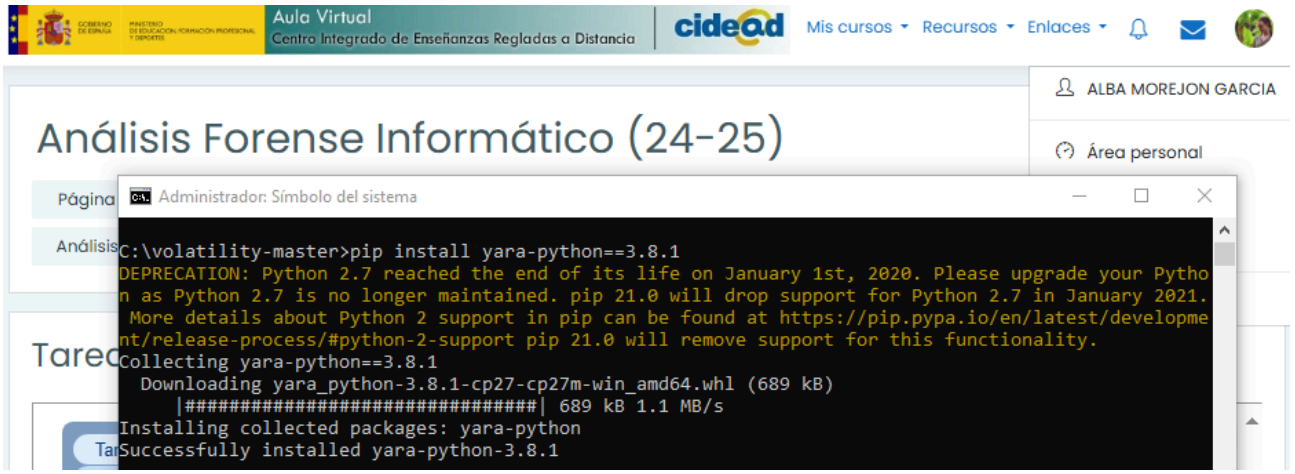
Debemos actualizar la versión de pip, utilizando el comando “python -m pip install --upgrade pip” y comprobamos que la versión actual es pip 20.3.4



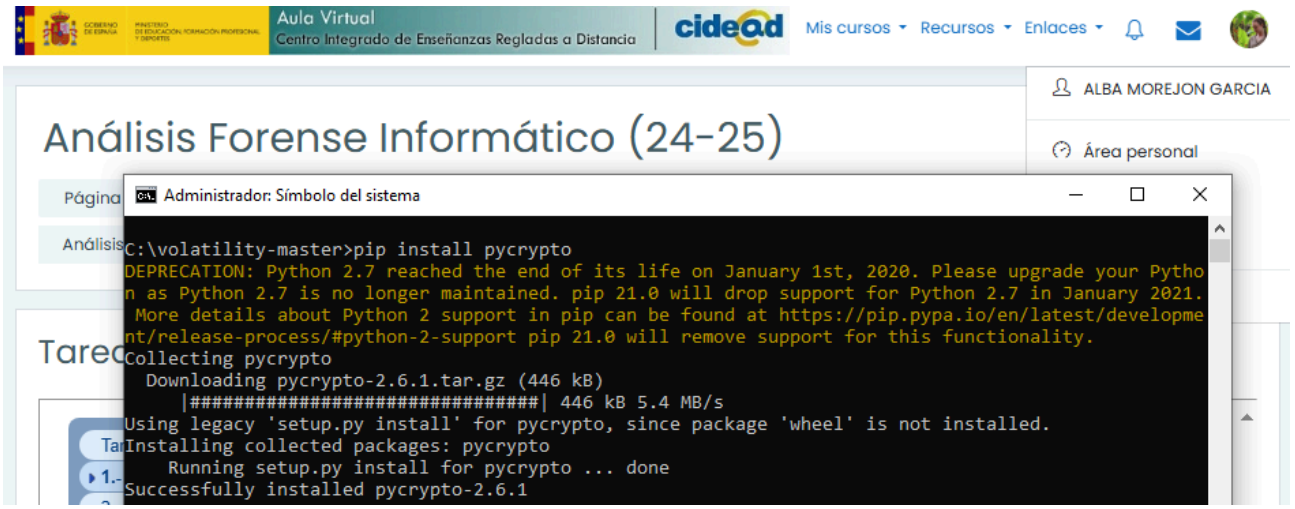
A continuación instalamos las dependencias requeridas:
Distorm3 3.5.2



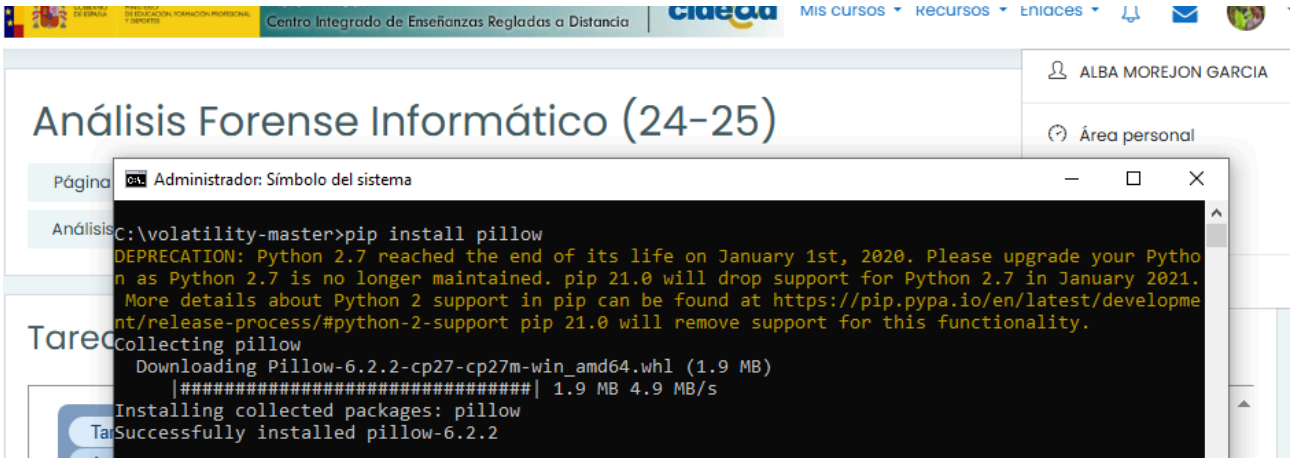
Yara-python 3.8.1



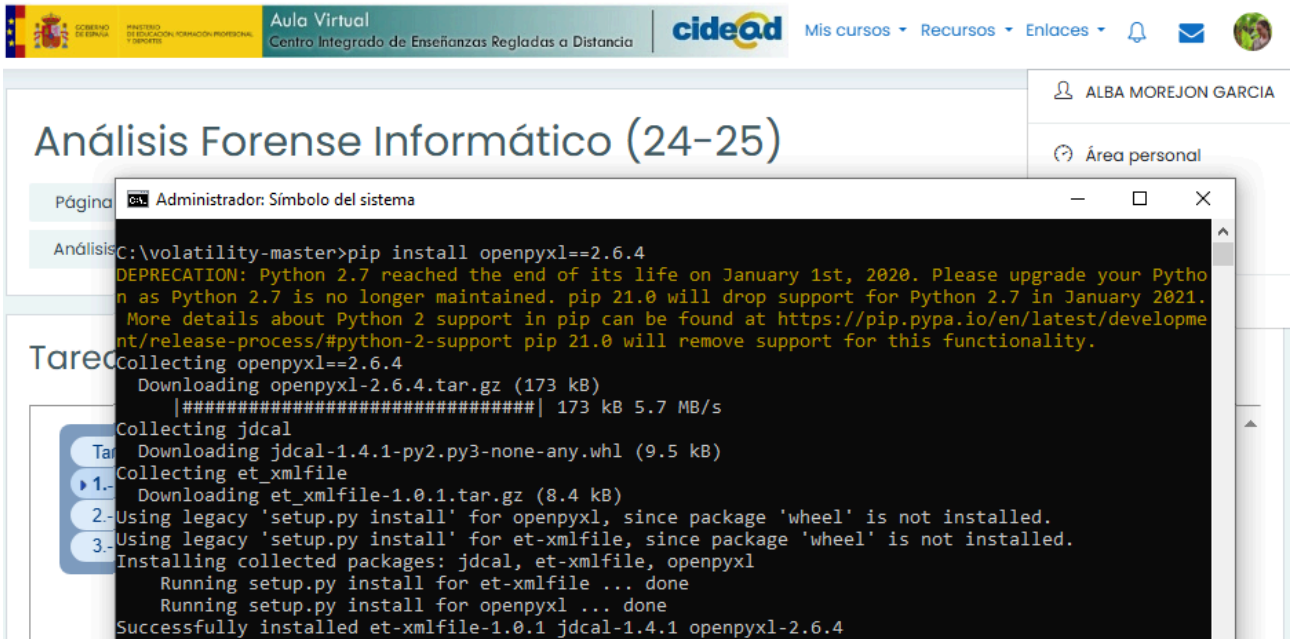
Pycrypto 2.6.1



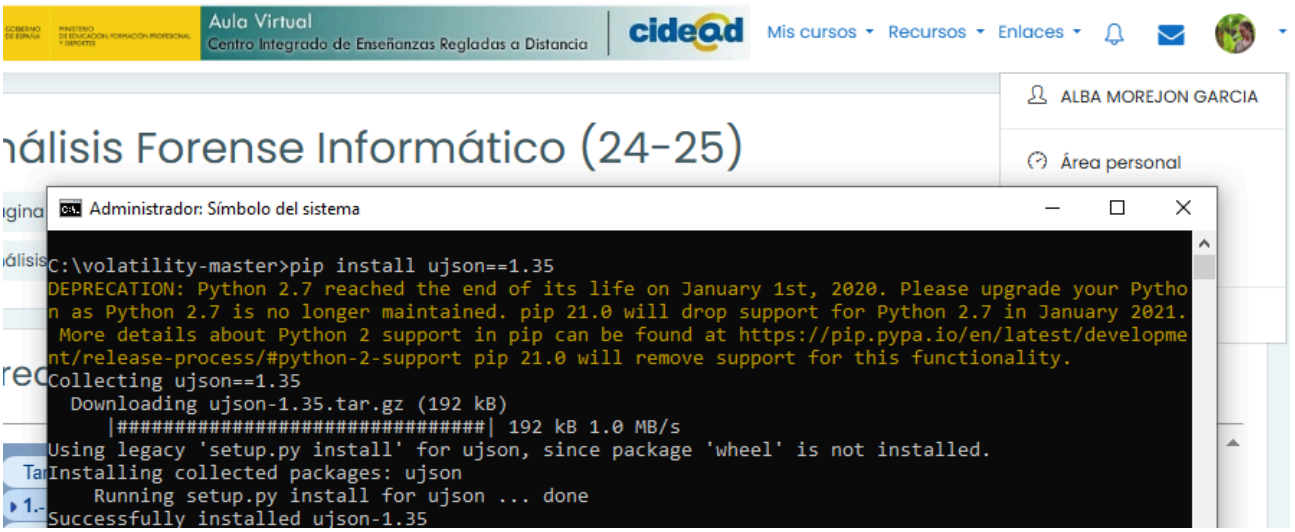
Pillow 6.2.2



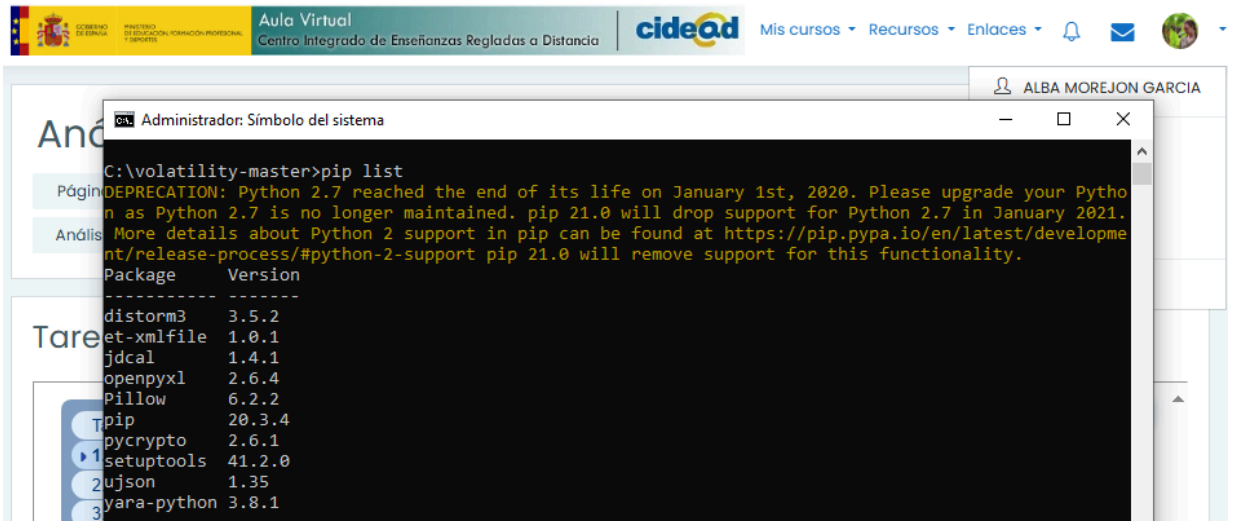
Openpyxl 2.6.4.



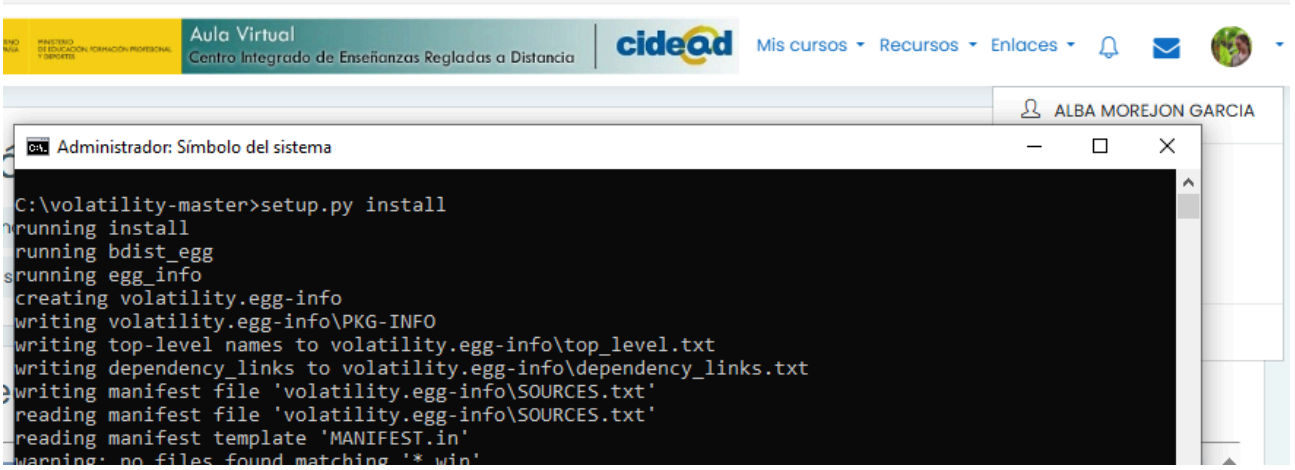
Ujson 1.35

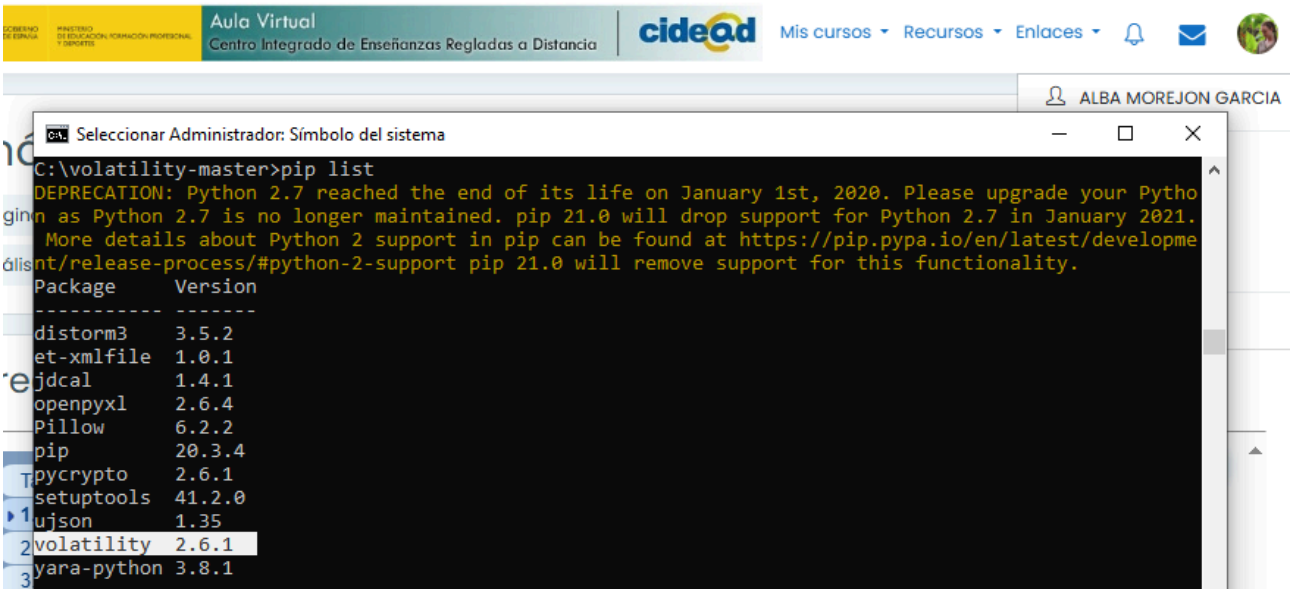


Comprobamos los paquetes que hemos instalado



Nos volvemos a situar en la carpeta donde descomprimimos volatility y ejecutamos el setup con el comando “setup.py install” y comprobamos que se haya instalado.





ANÁLISIS DE MEMORIA RAM

Hemos copiado la memoria ram descomprimida en la ruta C:\ram\, para llevar a cabo la tarea nos posicionamos en la carpeta donde descomprimimos volatility y ejecutamos el comando "python vol.py -f C:\RAM\memdump.mem imageinfo" en la que nos muestra los perfiles

Imageninfo es un comando que sirve para obtener información de la memoria ram capturada, como el sistema operativo, la arquitectura y otros detalles.

Los suggested profiles, son los perfiles de sistema operativo sugeridos para analizar, en este caso la memoria proviene de una maquina con Windows Vista o Windows Server de 32 bits las dos (x86)

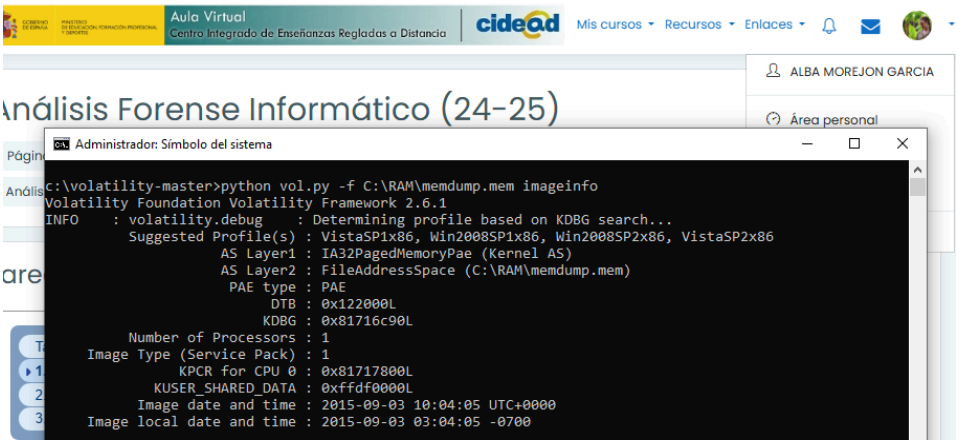
- VistaSP1x86
- Win2008SP1x86
- Win2008SP2x86
- VistaSP2x86

En este caso VistaSP2x86 sería el perfil inicial.

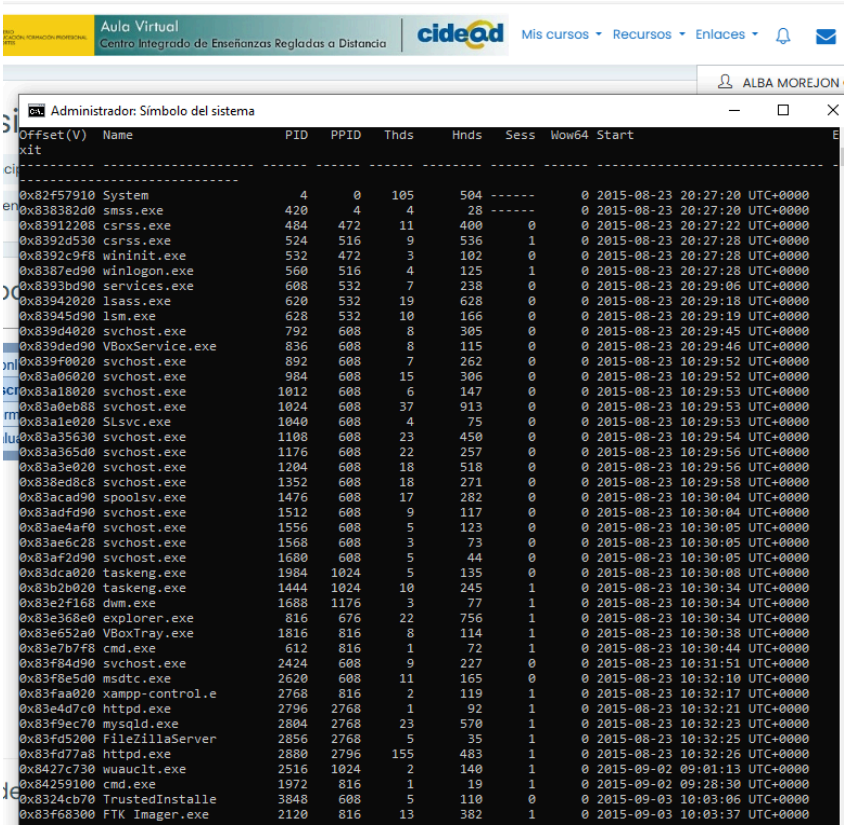
En Number of Precessors, el sistema tiene 1 procesador

En Image date and time nos muestra que la captura de la memoria ram se hizo el 2015/09/03

En Image local date and time nos muestra la hora local del sistema

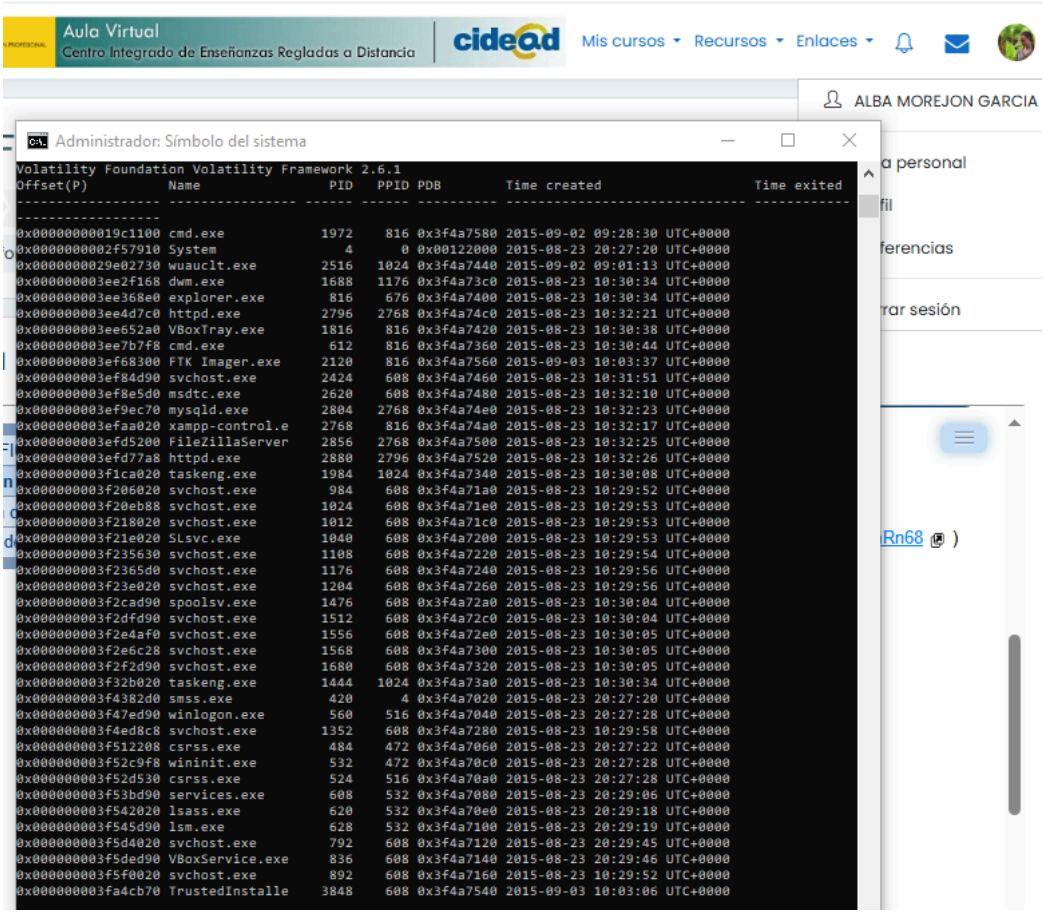


Listamos los procesos que estaban ejecutándose en el sistema capturado con el comando “python vol.py -f C:\RAM\memdump.mem --profile=VistaSP2x86 pslist”




```
Offset(V)  Name                PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- ---------- ------ ------ ------ -------- ------ ------ ------------------------------ ----------
0x82f57910 System                4      0    105      504 ------      0 2015-08-23 20:27:20 UTC+0000
0x838382d0 smss.exe            420      4      4       28 ------      0 2015-08-23 20:27:20 UTC+0000
0x83912208 csrss.exe           484    472     11      400      0      0 2015-08-23 20:27:22 UTC+0000
0x8392d530 csrss.exe           524    516      9      536      1      0 2015-08-23 20:27:28 UTC+0000
0x8392c9f8 wininit.exe         532    472      3      102      0      0 2015-08-23 20:27:28 UTC+0000
0x8387ed90 winlogon.exe        560    516      4      125      1      0 2015-08-23 20:27:28 UTC+0000
0x8393bd90 services.exe        608    532      7      238      0      0 2015-08-23 20:29:06 UTC+0000
0x83942020 lsass.exe           620    532     19      628      0      0 2015-08-23 20:29:18 UTC+0000
0x83945d90 lsm.exe             628    532     10      166      0      0 2015-08-23 20:29:19 UTC+0000
0x839d4020 svchost.exe         792    608      8      305      0      0 2015-08-23 20:29:45 UTC+0000
0x839ded90 VBoxService.exe     836    608      8      115      0      0 2015-08-23 20:29:46 UTC+0000
0x839f0020 svchost.exe         892    608      7      262      0      0 2015-08-23 10:29:52 UTC+0000
0x83a06020 svchost.exe         984    608     15      306      0      0 2015-08-23 10:29:52 UTC+0000
0x83a18020 svchost.exe        1012    608      6      147      0      0 2015-08-23 10:29:53 UTC+0000
0x83a0eb88 svchost.exe        1024    608     37      913      0      0 2015-08-23 10:29:53 UTC+0000
0x83a1e020 SLsvc.exe          1040    608      4       75      0      0 2015-08-23 10:29:53 UTC+0000
0x83a35630 svchost.exe        1108    608     23      450      0      0 2015-08-23 10:29:54 UTC+0000
0x83a365d0 svchost.exe        1176    608     22      257      0      0 2015-08-23 10:29:56 UTC+0000
0x83a3e020 svchost.exe        1204    608     18      518      0      0 2015-08-23 10:29:56 UTC+0000
0x838ed8c8 svchost.exe        1352    608     18      271      0      0 2015-08-23 10:29:58 UTC+0000
0x83acad90 spoolsv.exe        1476    608     17      282      0      0 2015-08-23 10:30:04 UTC+0000
0x83adfd90 svchost.exe        1512    608      9      117      0      0 2015-08-23 10:30:04 UTC+0000
0x83ae4af0 svchost.exe        1556    608      5      123      0      0 2015-08-23 10:30:05 UTC+0000
0x83ae6c28 svchost.exe        1568    608      3       73      0      0 2015-08-23 10:30:05 UTC+0000
0x83af2d90 svchost.exe        1680    608      5       44      0      0 2015-08-23 10:30:05 UTC+0000
0x83dca020 taskeng.exe        1984   1024      5      135      0      0 2015-08-23 10:30:08 UTC+0000
0x83b2b020 taskeng.exe        1444   1024     10      245      1      0 2015-08-23 10:30:34 UTC+0000
0x83e2f168 dwm.exe            1688   1176      3       77      1      0 2015-08-23 10:30:34 UTC+0000
0x83e368e0 explorer.exe        816    676     22      756      1      0 2015-08-23 10:30:34 UTC+0000
0x83e652a0 VBoxTray.exe       1816    816      8      114      1      0 2015-08-23 10:30:38 UTC+0000
0x83e7b7f8 cmd.exe             612    816      1       72      1      0 2015-08-23 10:30:44 UTC+0000
0x83f84d90 svchost.exe        2424    608      9      227      0      0 2015-08-23 10:31:51 UTC+0000
0x83f8e5d0 msdtc.exe          2620    608     11      165      0      0 2015-08-23 10:32:10 UTC+0000
0x83faa020 xampp-control.e    2768    816      2      119      1      0 2015-08-23 10:32:17 UTC+0000
0x83e4d7c0 httpd.exe          2796   2768      1       92      1      0 2015-08-23 10:32:21 UTC+0000
0x83f9ec70 mysqld.exe         2804   2768     23      570      1      0 2015-08-23 10:32:23 UTC+0000
0x83fd5200 FileZillaServer    2856   2768      5       35      1      0 2015-08-23 10:32:25 UTC+0000
0x83fd77a8 httpd.exe          2880   2796    155      483      1      0 2015-08-23 10:32:26 UTC+0000
0x8427c730 wuauclt.exe        2516   1024      2      140      1      0 2015-09-02 09:01:13 UTC+0000
0x84259100 cmd.exe            1972    816      1       19      1      0 2015-09-02 09:28:30 UTC+0000
0x8324cb70 TrustedInstalle    3848    608      5      110      0      0 2015-09-03 10:03:06 UTC+0000
0x83f68300 FTK Imager.exe     2120    816     13      382      1      0 2015-09-03 10:03:37 UTC+0000
```

Hacemos también una búsqueda más profunda de procesos que han existido (ocultos o terminados) “python vol.py -f C:\RAM\memdump.mem --profile=VistaSP2x86 psscan”




```
Volatility Foundation Volatility Framework 2.6.1
Offset(P)          Name                PID   PPID PDB        Time created                   Time exited
------------------ ---------------- ------ ------ ---------- ------------------------------ ------------------------------
0x000000000019c1100 cmd.exe            1972    816 0x3f4a7580 2015-09-02 09:28:30 UTC+0000
0x0000000002f57910 System                 4      0 0x00122000 2015-08-23 20:27:20 UTC+0000
0x0000000029e02730 wuauclt.exe         2516   1024 0x3f4a7440 2015-09-02 09:01:13 UTC+0000
0x000000003ee2f168 dwm.exe             1688   1176 0x3f4a73c0 2015-08-23 10:30:34 UTC+0000
0x000000003ee368e0 explorer.exe         816    676 0x3f4a7400 2015-08-23 10:30:34 UTC+0000
0x000000003ee4d7c0 httpd.exe           2796   2768 0x3f4a74c0 2015-08-23 10:32:21 UTC+0000
0x000000003ee652a0 VBoxTray.exe        1816    816 0x3f4a7420 2015-08-23 10:30:38 UTC+0000
0x000000003ee7b7f8 cmd.exe              612    816 0x3f4a7360 2015-08-23 10:30:44 UTC+0000
0x000000003ef68300 FTK Imager.exe      2120    816 0x3f4a7560 2015-09-03 10:03:37 UTC+0000
0x000000003ef84d90 svchost.exe         2424    608 0x3f4a7460 2015-08-23 10:31:51 UTC+0000
0x000000003ef8e5d0 msdtc.exe           2620    608 0x3f4a7480 2015-08-23 10:32:10 UTC+0000
0x000000003ef9ec70 mysqld.exe          2804   2768 0x3f4a74e0 2015-08-23 10:32:23 UTC+0000
0x000000003efaa020 xampp-control.e     2768    816 0x3f4a74a0 2015-08-23 10:32:17 UTC+0000
0x000000003efd5200 FileZillaServer     2856   2768 0x3f4a7500 2015-08-23 10:32:25 UTC+0000
0x000000003efd77a8 httpd.exe           2880   2796 0x3f4a7520 2015-08-23 10:32:26 UTC+0000
0x000000003f1ca020 taskeng.exe         1984   1024 0x3f4a7340 2015-08-23 10:30:08 UTC+0000
0x000000003f206020 svchost.exe          984    608 0x3f4a71a0 2015-08-23 10:29:52 UTC+0000
0x000000003f20eb88 svchost.exe         1024    608 0x3f4a71e0 2015-08-23 10:29:53 UTC+0000
0x000000003f218020 svchost.exe         1012    608 0x3f4a71c0 2015-08-23 10:29:53 UTC+0000
0x000000003f21e020 SLsvc.exe           1040    608 0x3f4a7200 2015-08-23 10:29:53 UTC+0000
0x000000003f235630 svchost.exe         1108    608 0x3f4a7220 2015-08-23 10:29:54 UTC+0000
0x000000003f2365d0 svchost.exe         1176    608 0x3f4a7240 2015-08-23 10:29:56 UTC+0000
0x000000003f23e020 svchost.exe         1204    608 0x3f4a7260 2015-08-23 10:29:56 UTC+0000
0x000000003f2cad90 spoolsv.exe         1476    608 0x3f4a72a0 2015-08-23 10:30:04 UTC+0000
0x000000003f2dfd90 svchost.exe         1512    608 0x3f4a72c0 2015-08-23 10:30:04 UTC+0000
0x000000003f2e4af0 svchost.exe         1556    608 0x3f4a72e0 2015-08-23 10:30:05 UTC+0000
0x000000003f2e6c28 svchost.exe         1568    608 0x3f4a7300 2015-08-23 10:30:05 UTC+0000
0x000000003f2f2d90 svchost.exe         1680    608 0x3f4a7320 2015-08-23 10:30:05 UTC+0000
0x000000003f32b020 taskeng.exe         1444   1024 0x3f4a73a0 2015-08-23 10:30:34 UTC+0000
0x000000003f4382d0 smss.exe             420      4 0x3f4a7020 2015-08-23 20:27:20 UTC+0000
0x000000003f47ed90 winlogon.exe         560    516 0x3f4a7040 2015-08-23 20:27:28 UTC+0000
0x000000003f4ed8c8 svchost.exe         1352    608 0x3f4a7280 2015-08-23 10:29:58 UTC+0000
0x000000003f512208 csrss.exe            484    472 0x3f4a7060 2015-08-23 20:27:22 UTC+0000
0x000000003f52c9f8 wininit.exe          532    472 0x3f4a70c0 2015-08-23 20:27:28 UTC+0000
0x000000003f52d530 csrss.exe            524    516 0x3f4a70a0 2015-08-23 20:27:28 UTC+0000
0x000000003f53bd90 services.exe         608    532 0x3f4a7080 2015-08-23 20:29:06 UTC+0000
0x000000003f542020 lsass.exe            620    532 0x3f4a70e0 2015-08-23 20:29:18 UTC+0000
0x000000003f545d90 lsm.exe              628    532 0x3f4a7100 2015-08-23 20:29:19 UTC+0000
0x000000003f5d4020 svchost.exe          792    608 0x3f4a7120 2015-08-23 20:29:45 UTC+0000
0x000000003f5ded90 VBoxService.exe      836    608 0x3f4a7140 2015-08-23 20:29:46 UTC+0000
0x000000003f5f0020 svchost.exe          892    608 0x3f4a7160 2015-08-23 10:29:52 UTC+0000
0x000000003fa4cb70 TrustedInstalle     3848    608 0x3f4a7540 2015-09-03 10:03:06 UTC+0000
```

Procesos de la lista relevantes en un sistema Windows en funcionamiento como por ejemplo:

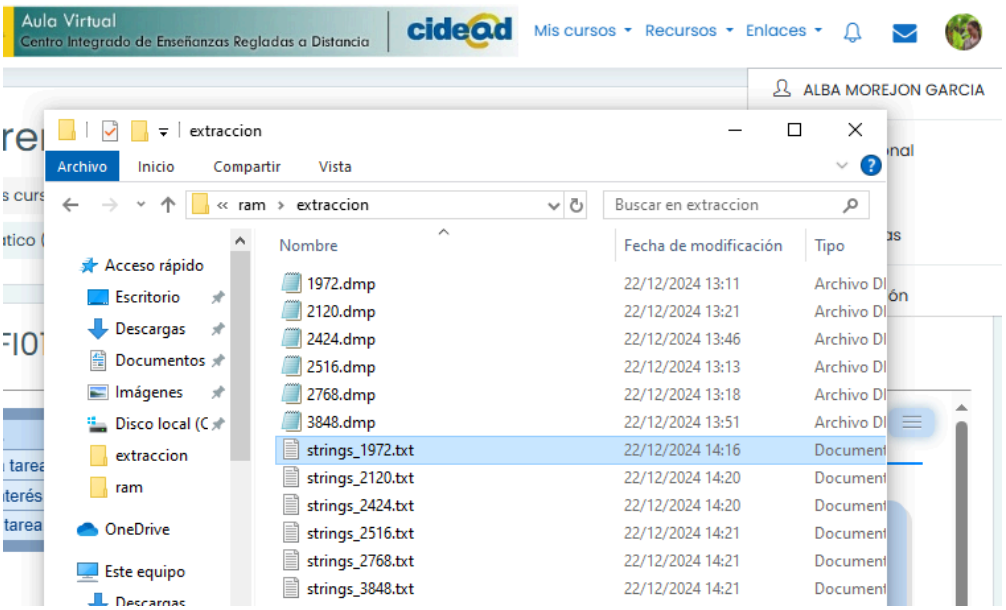
- System, proceso principal del sistema operativo
- smss.exe, csrss.exe, winlogon.exe, lsass.exe, svchost.exe … procesos estándar relacionados con la gestión se sesiones
- svchost.exe, ejecuta servicios del sistema operativo (se encuentra 12 veces este mismo proceso)
- explorer.exe, entorno gráfico parece iniciar correctamente
- VBoxTray.exe, VBoxService.exe, procesos relacionados con VirtualBox (esta memoria podría ser de una máquina virtual)
- xampp-control.e, httpd.exe, mysqld.exe, FileZillaServer, son procesos relacionados con Xampp (servidor apache, base de datos MySQL, servidor FTP)
- wuauclt.exe, es un proceso relacionado con las actualizaciones automáticas de windows
- cmd.exe, estaba ejecutada la consola de comandos
- TrustedInstalle, instalador de windows que se encarga de actualizaciones y cambios en el sistema, se estaba ejecutando antes de la captura de memoria
- FTK Imager.exe, es una herramienta forense, se estaba realizando un analisis antes de la captura

Ahora extraeremos la memoria de los procesos sospechosos y la analizaremos
"python vol.py -f C:\RAM\memdump.mem --profile=VistaSP2x86 memdump -p <PID> -D C:\ram\extraccion"

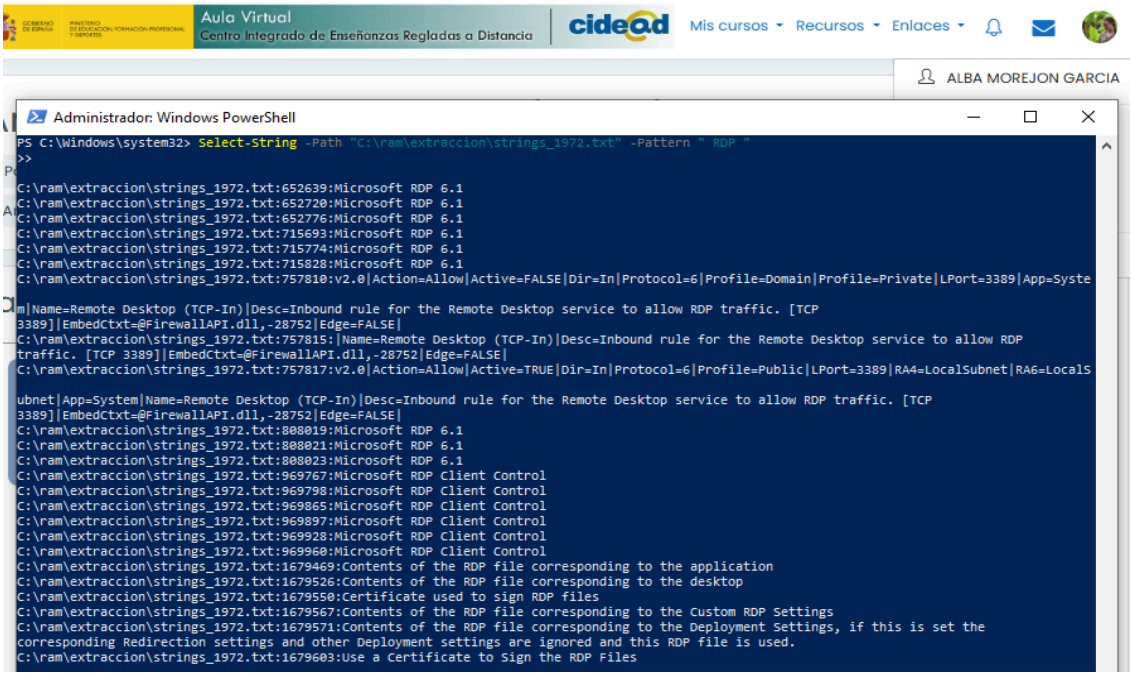
- cmd.exe (PID 1972)
- wuauclt.exe (PID 2516)
- xampp-console.e (PID 2768), httpd.exe (PID 2796), mysqld.exe (PID 2804), FileZillaServer (PID 2856)
- FTK Imager (PID 2120)
- svchost.exe (PID 2424)
- trustedInstaller (PID 3848)

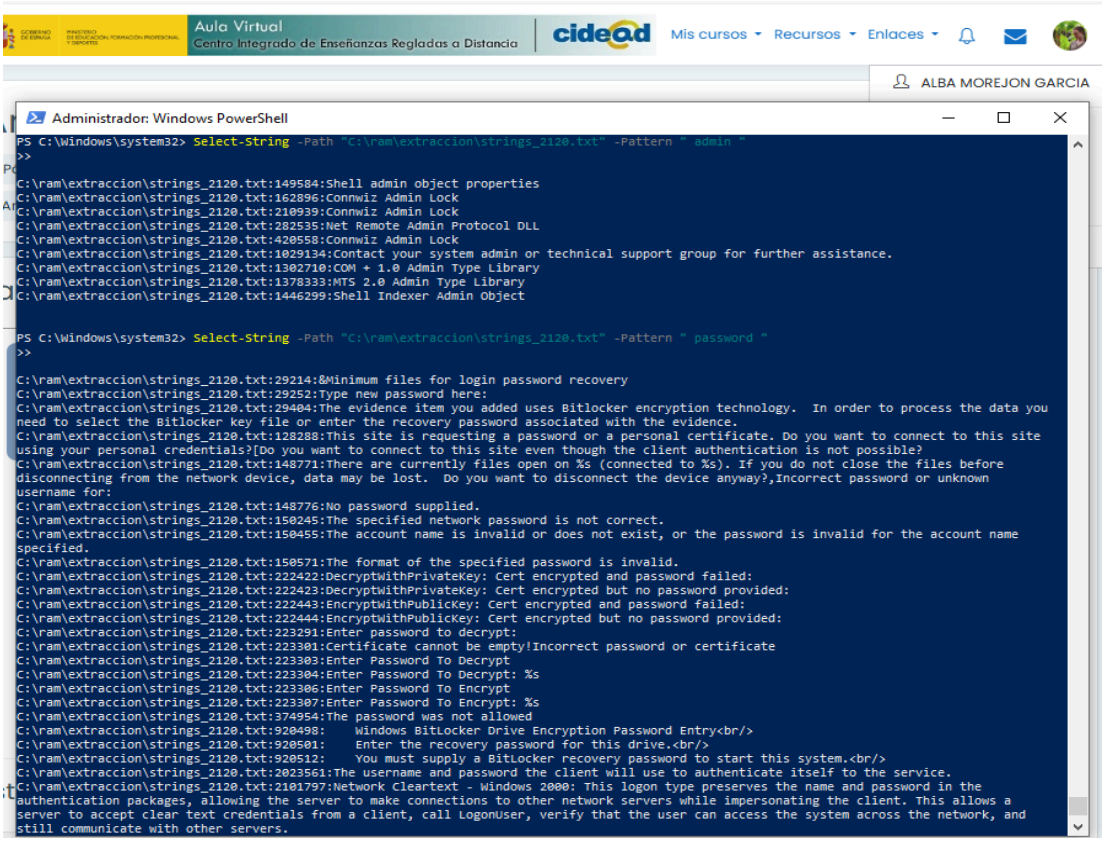
Vamos a analizar las cadenas de texto
Descargamos Sysinternals Suite desde la página https://learn.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite y extraemos los archivos en la carpeta c:\sysinternals ejecutamos el archivo string.exe
Situándonos en la carpeta recien creada y con el comando
"strings.exe C:\ram\extraccion\1972.dmp > C:\ram\extraccion\strings_1972.txt"
Extraemos en cadenas de texto la información almacenada

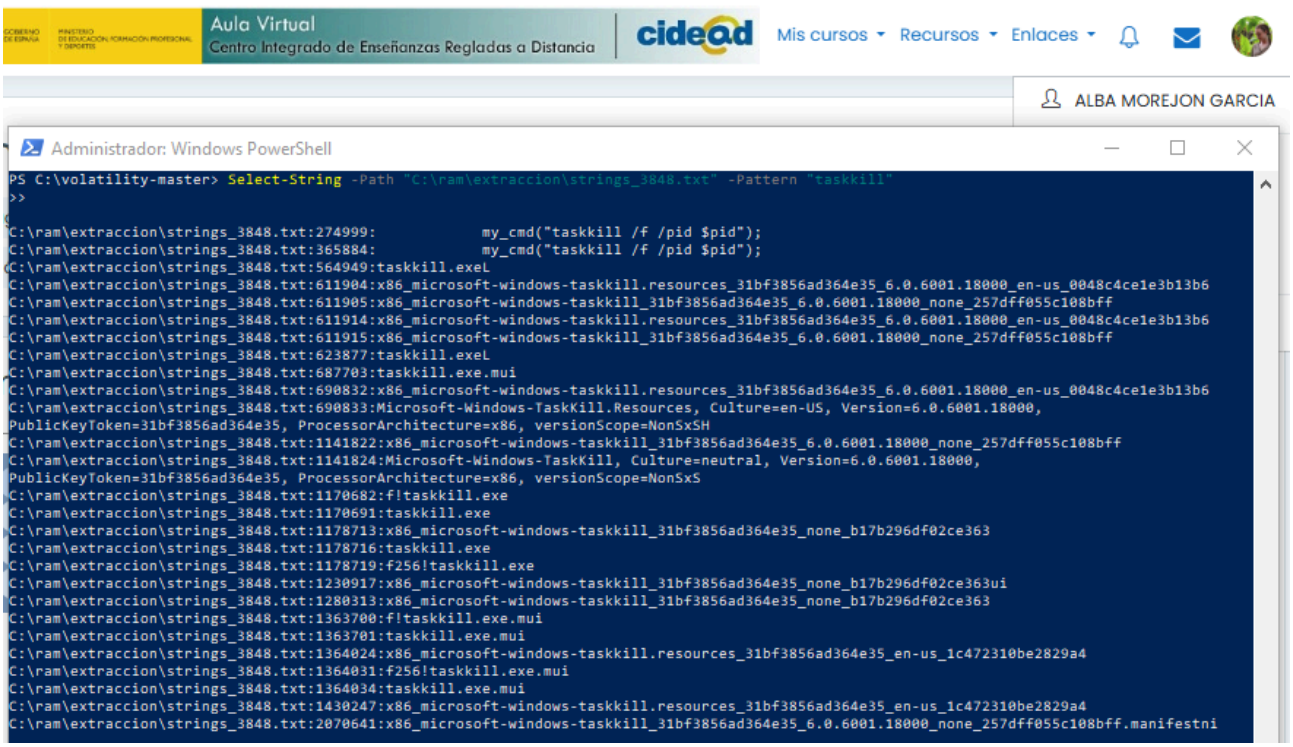
Queda así más o menos:



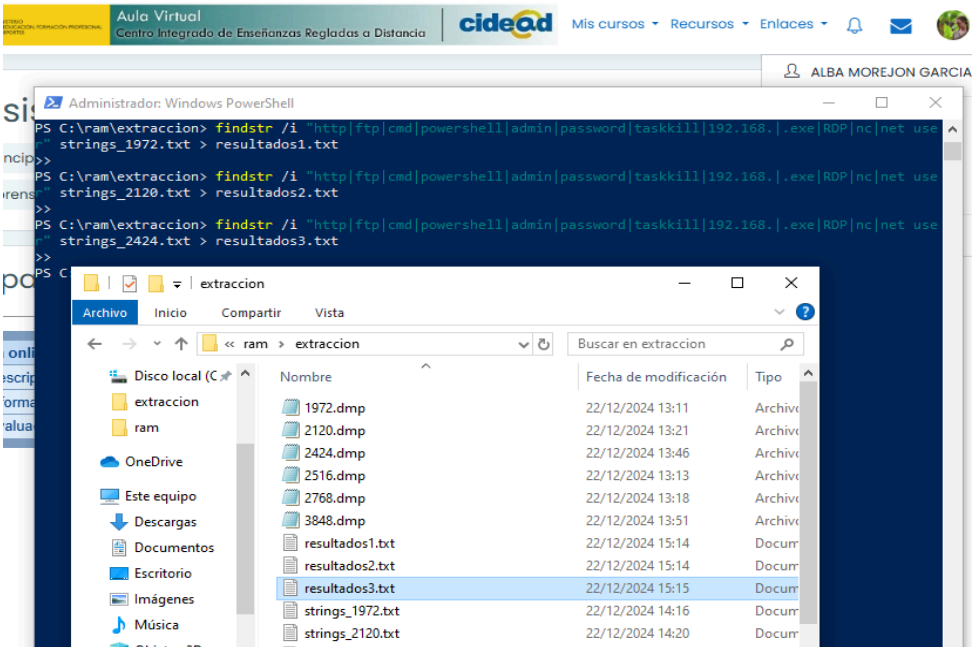
Analizamos uno por uno los archivos utilizando PowerShell y haciendo una búsqueda de palabras clave como: http, ftp,nc, password, admin, nc, RDP, PsTools, https://, .exe,.bat, net user, 192.168., taskkill…
"Select-String -Path "C:\ram\extraccion\strings_XXXX.txt" -Pattern "palabra_a_buscar"
Esto generará un archivo de texto con todas las cadenas legibles dentro de la memoria del proceso.
Buscaremos patrones sospechosos como direcciones IP, rutas de archivos extrañas, nombres de procesos, o cadenas relacionadas con actividades maliciosas.
Salen muchos resultados pero no sacamos nada en claro, podemos ver que se estaba ejecutando cambios de contraseña, conexiones con mysql, inicios en una base de datos en la que han intentado resetear la contraseña, accesos en remoto…



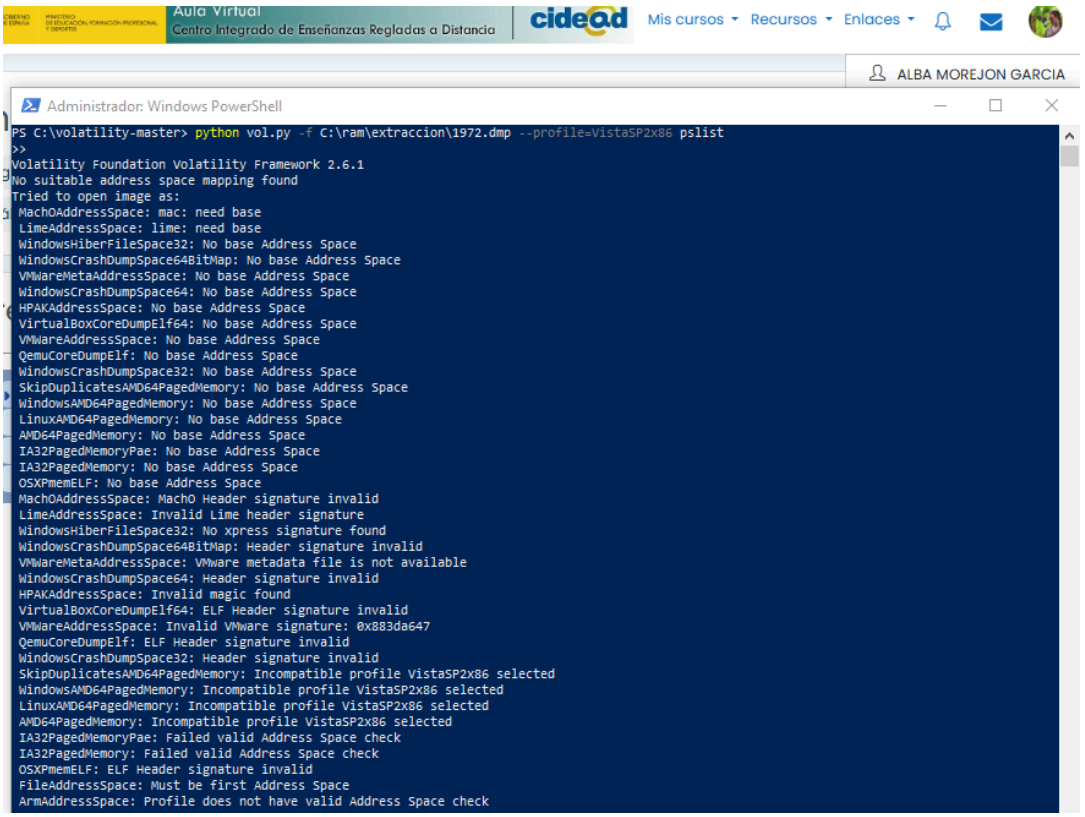

Aula Virtual
Centro Integrado de Enseñanzas Regladas a Distancia
cidead
Mis cursos
Recursos
Enlaces
ALBA MOREJON GARCIA
Administrador: Windows PowerShell
PS C:\Windows\system32> Select-String -Path "C:\ram\extraccion\strings_2120.txt" -Pattern " admin "
>>
C:\ram\extraccion\strings_2120.txt:149584:Shell admin object properties
C:\ram\extraccion\strings_2120.txt:162896:Connwiz Admin Lock
C:\ram\extraccion\strings_2120.txt:210939:Connwiz Admin Lock
C:\ram\extraccion\strings_2120.txt:282535:Net Remote Admin Protocol DLL
C:\ram\extraccion\strings_2120.txt:420558:Connwiz Admin Lock
C:\ram\extraccion\strings_2120.txt:1029134:Contact your system admin or technical support group for further assistance.
C:\ram\extraccion\strings_2120.txt:1302710:COM + 1.0 Admin Type Library
C:\ram\extraccion\strings_2120.txt:1378333:MTS 2.0 Admin Type Library
C:\ram\extraccion\strings_2120.txt:1446299:Shell Indexer Admin Object
PS C:\Windows\system32> Select-String -Path "C:\ram\extraccion\strings_2120.txt" -Pattern " password "
>>
C:\ram\extraccion\strings_2120.txt:29214:&Minimum files for login password recovery
C:\ram\extraccion\strings_2120.txt:29252:Type new password here:
C:\ram\extraccion\strings_2120.txt:29404:The evidence item you added uses Bitlocker encryption technology. In order to process the data you need to select the Bitlocker key file or enter the recovery password associated with the evidence.
C:\ram\extraccion\strings_2120.txt:128288:This site is requesting a password or a personal certificate. Do you want to connect to this site using your personal credentials?[Do you want to connect to this site even though the client authentication is not possible?
C:\ram\extraccion\strings_2120.txt:148771:There are currently files open on %s (connected to %s). If you do not close the files before disconnecting from the network device, data may be lost. Do you want to disconnect the device anyway?,Incorrect password or unknown username for:
C:\ram\extraccion\strings_2120.txt:148776:No password supplied.
C:\ram\extraccion\strings_2120.txt:150245:The specified network password is not correct.
C:\ram\extraccion\strings_2120.txt:150455:The account name is invalid or does not exist, or the password is invalid for the account name specified.
C:\ram\extraccion\strings_2120.txt:150571:The format of the specified password is invalid.
C:\ram\extraccion\strings_2120.txt:222422:DecryptWithPrivateKey: Cert encrypted and password failed:
C:\ram\extraccion\strings_2120.txt:222423:DecryptWithPrivateKey: Cert encrypted but no password provided:
C:\ram\extraccion\strings_2120.txt:222443:EncryptWithPublicKey: Cert encrypted and password failed:
C:\ram\extraccion\strings_2120.txt:222444:EncryptWithPublicKey: Cert encrypted but no password provided:
C:\ram\extraccion\strings_2120.txt:223291:Enter password to decrypt:
C:\ram\extraccion\strings_2120.txt:223301:Certificate cannot be empty!Incorrect password or certificate
C:\ram\extraccion\strings_2120.txt:223303:Enter Password To Decrypt
C:\ram\extraccion\strings_2120.txt:223304:Enter Password To Decrypt: %s
C:\ram\extraccion\strings_2120.txt:223306:Enter Password To Encrypt
C:\ram\extraccion\strings_2120.txt:223307:Enter Password To Encrypt: %s
C:\ram\extraccion\strings_2120.txt:374954:The password was not allowed
C:\ram\extraccion\strings_2120.txt:920498: Windows BitLocker Drive Encryption Password Entry
C:\ram\extraccion\strings_2120.txt:920501: Enter the recovery password for this drive.
C:\ram\extraccion\strings_2120.txt:920512: You must supply a BitLocker recovery password to start this system.
C:\ram\extraccion\strings_2120.txt:2023561:The username and password the client will use to authenticate itself to the service.
C:\ram\extraccion\strings_2120.txt:2101797:Network Cleartext - Windows 2000: This logon type preserves the name and password in the authentication packages, allowing the server to make connections to other network servers while impersonating the client. This allows a server to accept clear text credentials from a client, call LogonUser, verify that the user can access the system across the network, and still communicate with other servers.


Aula Virtual
Centro Integrado de Enseñanzas Regladas a Distancia
cidead
Mis cursos
Recursos
Enlaces
ALBA MOREJON GARCIA
Administrador: Windows PowerShell
PS C:\volatility-master> Select-String -Path "C:\ram\extraccion\strings_3848.txt" -Pattern "taskkill"
>>
C:\ram\extraccion\strings_3848.txt:274999: my_cmd("taskkill /f /pid $pid");
C:\ram\extraccion\strings_3848.txt:365884: my_cmd("taskkill /f /pid $pid");
C:\ram\extraccion\strings_3848.txt:564949:taskkill.exeL
C:\ram\extraccion\strings_3848.txt:611904:x86_microsoft-windows-taskkill.resources_31bf3856ad364e35_6.0.6001.18000_en-us_0048c4ce1e3b13b6
C:\ram\extraccion\strings_3848.txt:611905:x86_microsoft-windows-taskkill_31bf3856ad364e35_6.0.6001.18000_none_257dff055c108bff
C:\ram\extraccion\strings_3848.txt:611914:x86_microsoft-windows-taskkill.resources_31bf3856ad364e35_6.0.6001.18000_en-us_0048c4ce1e3b13b6
C:\ram\extraccion\strings_3848.txt:611915:x86_microsoft-windows-taskkill_31bf3856ad364e35_6.0.6001.18000_none_257dff055c108bff
C:\ram\extraccion\strings_3848.txt:623877:taskkill.exeL
C:\ram\extraccion\strings_3848.txt:687703:taskkill.exe.mui
C:\ram\extraccion\strings_3848.txt:690832:x86_microsoft-windows-taskkill.resources_31bf3856ad364e35_6.0.6001.18000_en-us_0048c4ce1e3b13b6
C:\ram\extraccion\strings_3848.txt:690833:Microsoft-Windows-TaskKill.Resources, Culture=en-US, Version=6.0.6001.18000, PublicKeyToken=31bf3856ad364e35, ProcessorArchitecture=x86, versionScope=NonSxSH
C:\ram\extraccion\strings_3848.txt:1141822:x86_microsoft-windows-taskkill_31bf3856ad364e35_6.0.6001.18000_none_257dff055c108bff
C:\ram\extraccion\strings_3848.txt:1141824:Microsoft-Windows-TaskKill, Culture=neutral, Version=6.0.6001.18000, PublicKeyToken=31bf3856ad364e35, ProcessorArchitecture=x86, versionScope=NonSxS
C:\ram\extraccion\strings_3848.txt:1170682:f!taskkill.exe
C:\ram\extraccion\strings_3848.txt:1170691:taskkill.exe
C:\ram\extraccion\strings_3848.txt:1178713:x86_microsoft-windows-taskkill_31bf3856ad364e35_none_b17b296df02ce363
C:\ram\extraccion\strings_3848.txt:1178716:taskkill.exe
C:\ram\extraccion\strings_3848.txt:1178719:f256!taskkill.exe
C:\ram\extraccion\strings_3848.txt:1230917:x86_microsoft-windows-taskkill_31bf3856ad364e35_none_b17b296df02ce363ui
C:\ram\extraccion\strings_3848.txt:1280313:x86_microsoft-windows-taskkill_31bf3856ad364e35_none_b17b296df02ce363
C:\ram\extraccion\strings_3848.txt:1363700:f!taskkill.exe.mui
C:\ram\extraccion\strings_3848.txt:1363701:taskkill.exe.mui
C:\ram\extraccion\strings_3848.txt:1364024:x86_microsoft-windows-taskkill.resources_31bf3856ad364e35_en-us_1c472310be2829a4
C:\ram\extraccion\strings_3848.txt:1364031:f256!taskkill.exe.mui
C:\ram\extraccion\strings_3848.txt:1364034:taskkill.exe.mui
C:\ram\extraccion\strings_3848.txt:1430247:x86_microsoft-windows-taskkill.resources_31bf3856ad364e35_en-us_1c472310be2829a4
C:\ram\extraccion\strings_3848.txt:2070641:x86_microsoft-windows-taskkill_31bf3856ad364e35_6.0.6001.18000_none_257dff055c108bff.manifestni

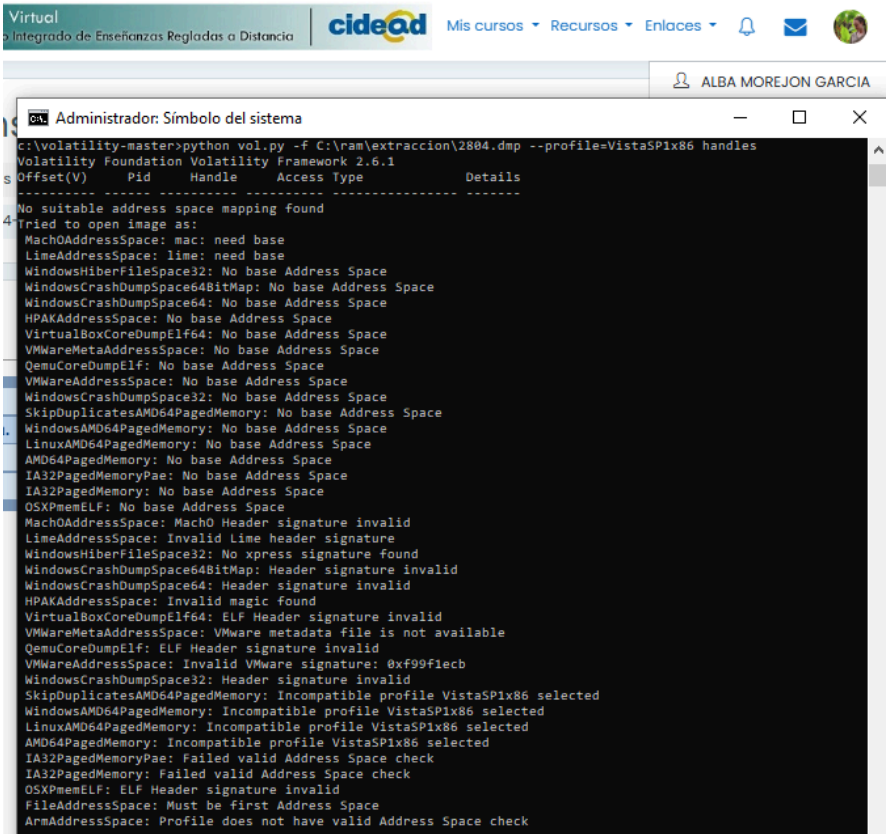
Hemos creado también archivos con las palabras clave que contenían algunos de los procesos para poder analizarlo mejor:
“findstr /i "http|ftp|cmd|powershell|admin|password|taskkill|192.168.|.exe|RDP|nc|net user" strings_1972.txt > resultados1.txt”



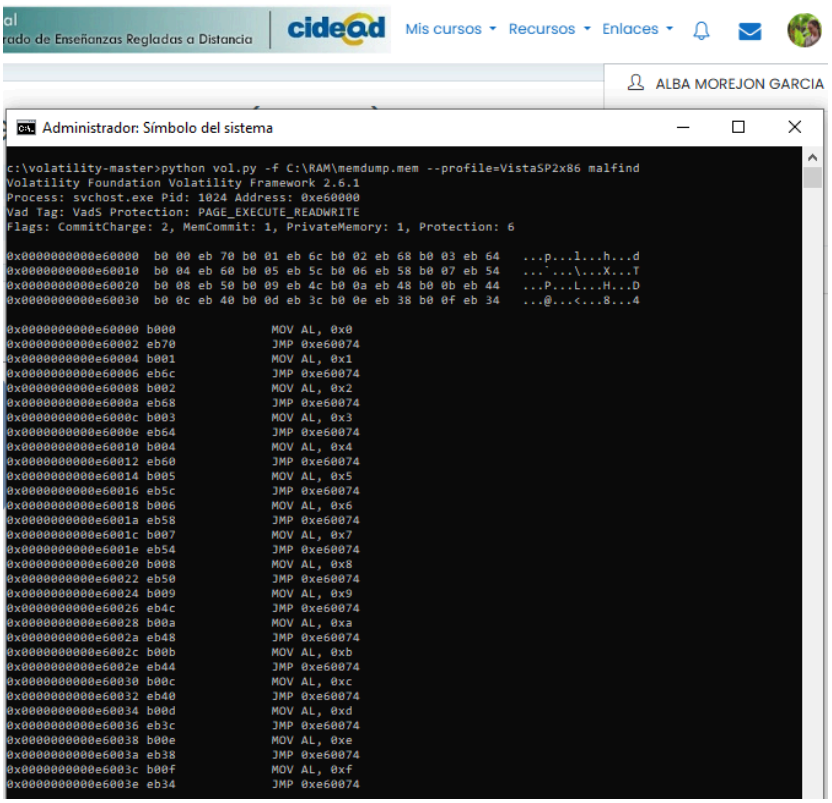
Vamos a pasar a ver más información sobre los procesos y sus propiedades:
“python vol.py -f C:\ram\extraccion\XXXX.dmp --profile=VistaSP2x86 pslist”
Nos sale este mismo resultado con todos los procesos



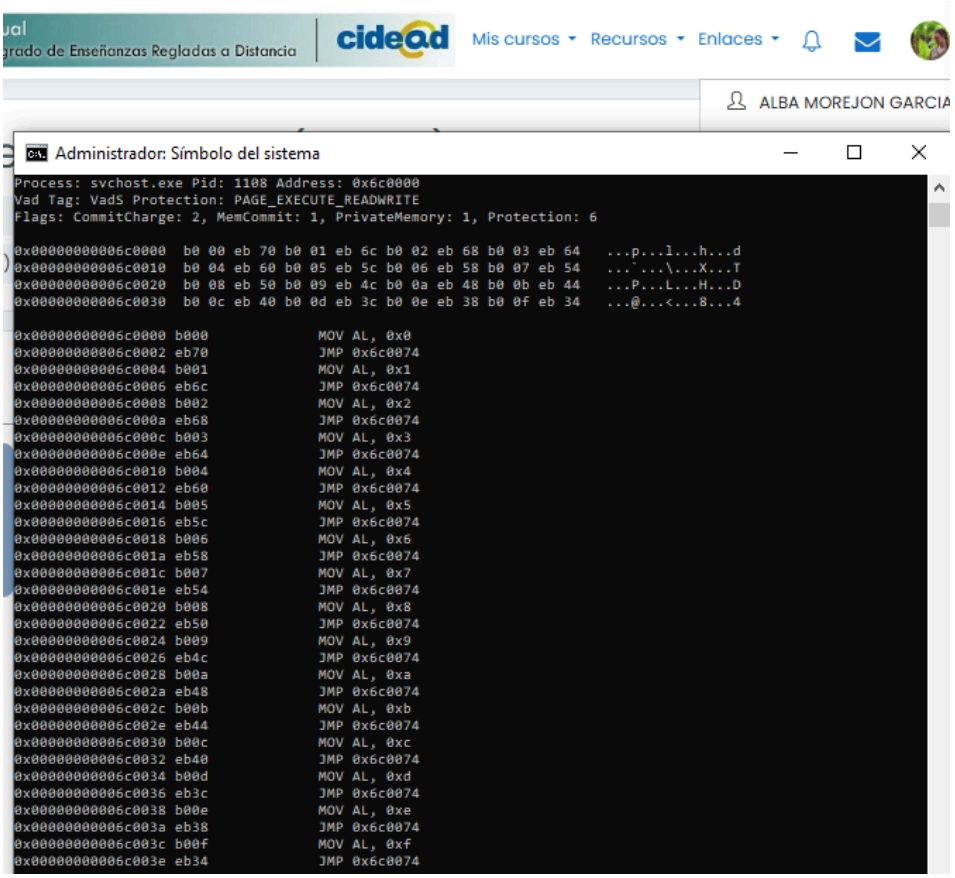
Nos aparece este mismo resultado con netscan, filescan, pslistcls, malfind y handles
Y probando los diferentes sistemas de la memoria VistaSP1x86, Win2008SP2x86 también pasa igual



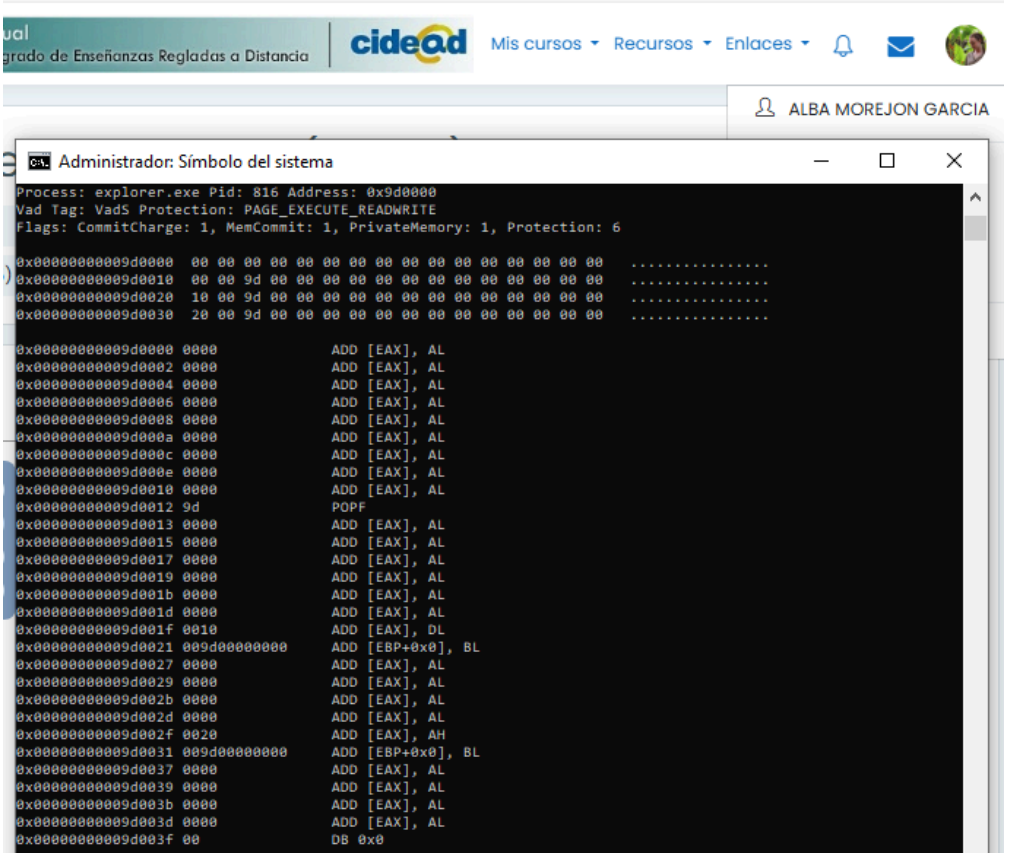
Ahora analizamos la memoria y encontramos información sobre la memoria, que podría estar relacionadas con código malicioso o inyectado. Nos muestra varios procesos:
“python vol.py -f C:\RAM\memdump.mem --profile=VistaSP2x86 malfind”
svchost.exe (PID 1024)

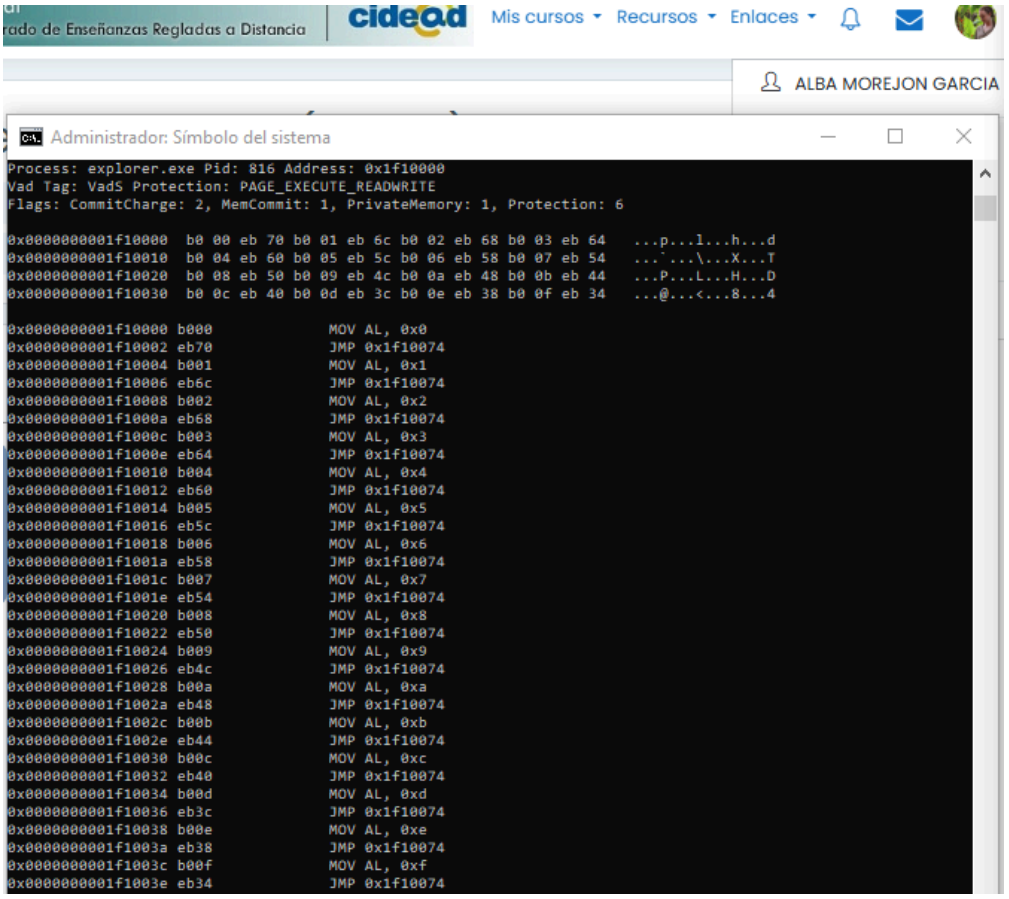


svchost.exe (PID 1108)

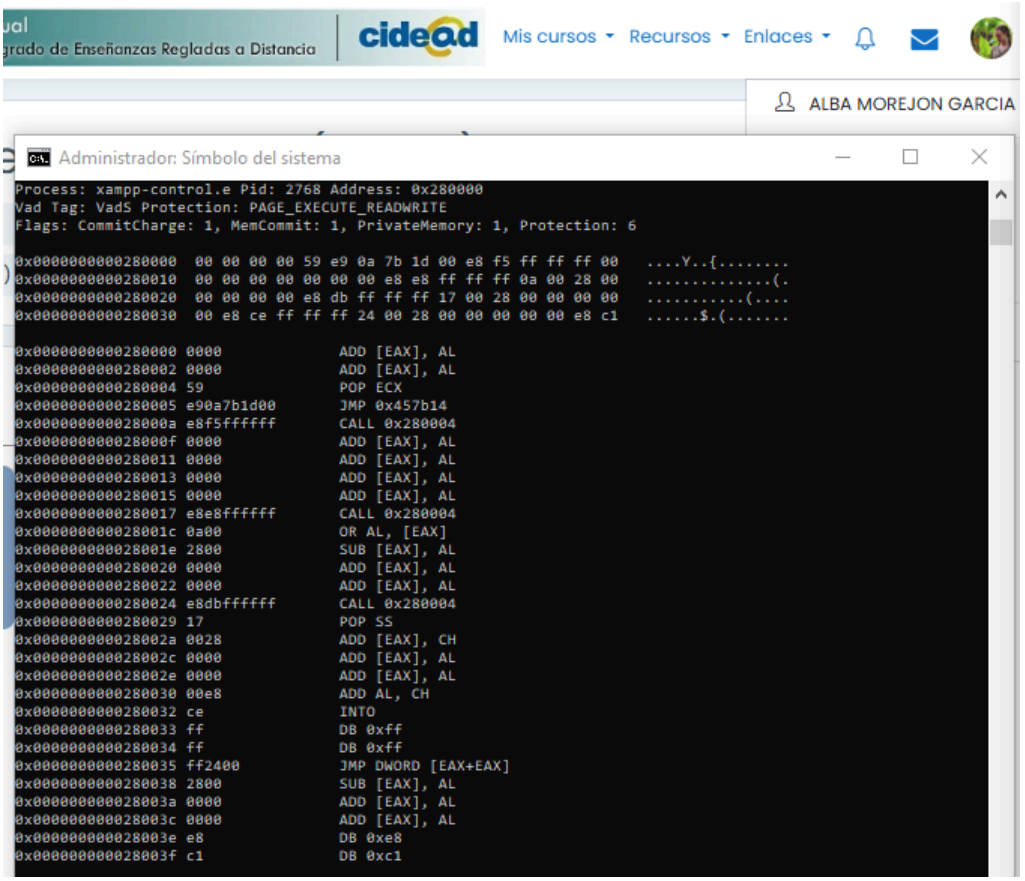


explorer.exe (PID 816)

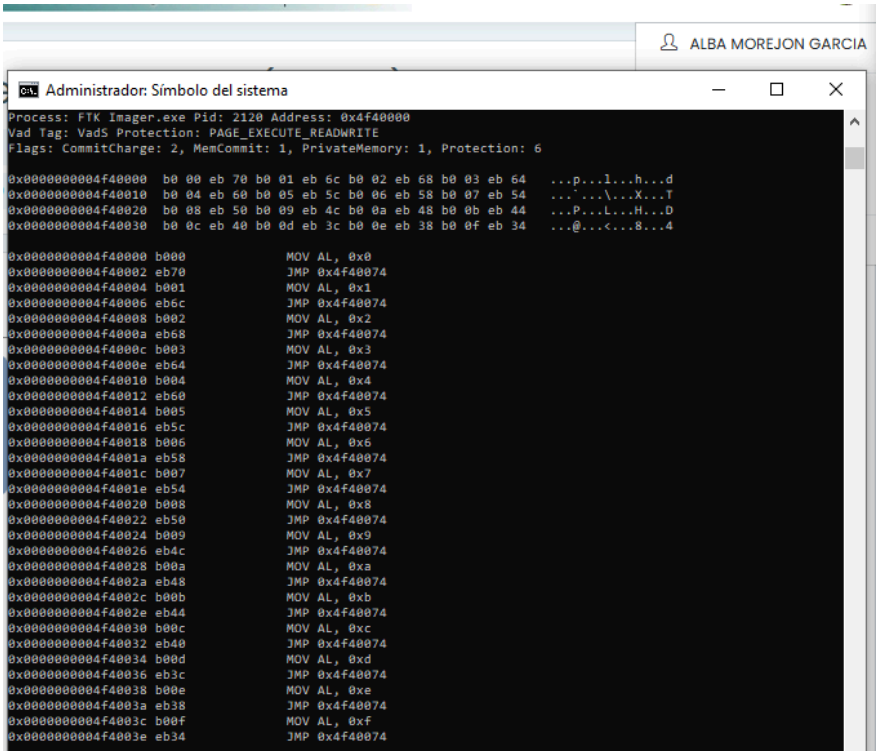




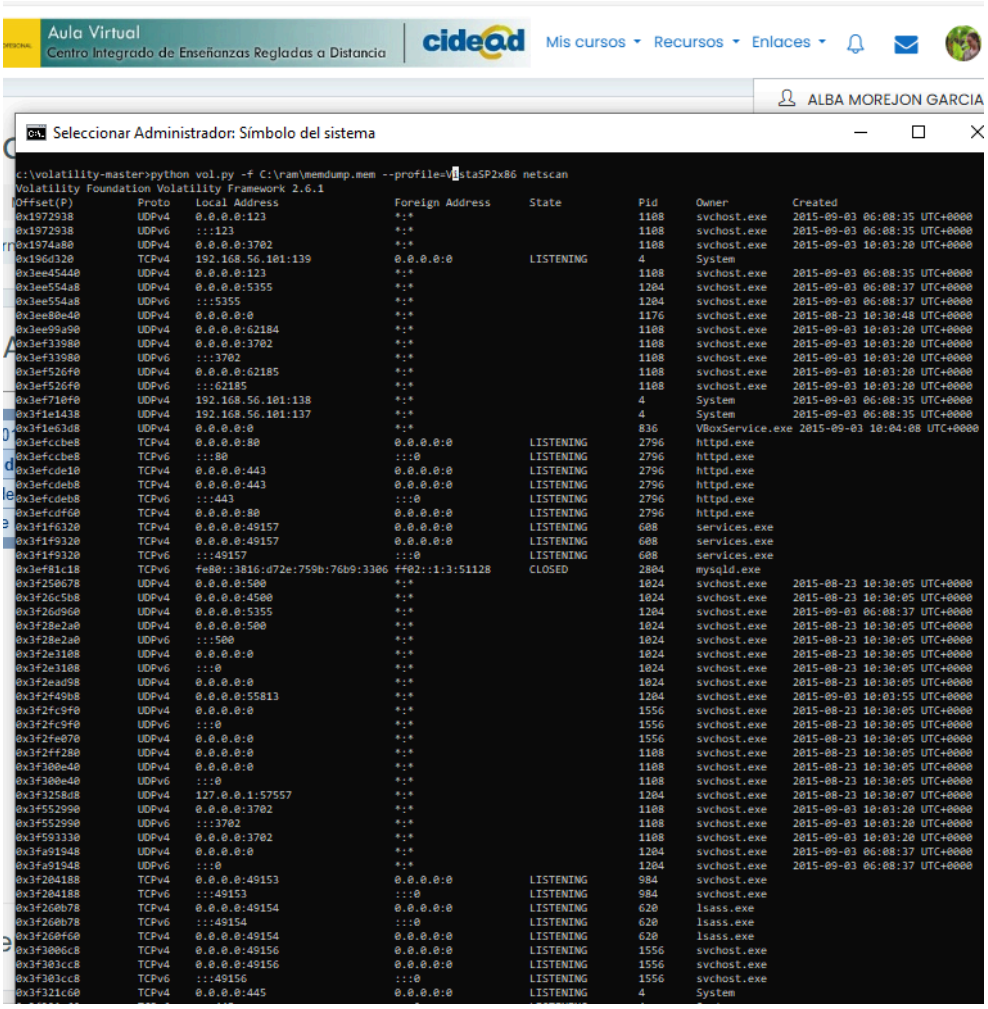
xampp-control.e (PID 2768)

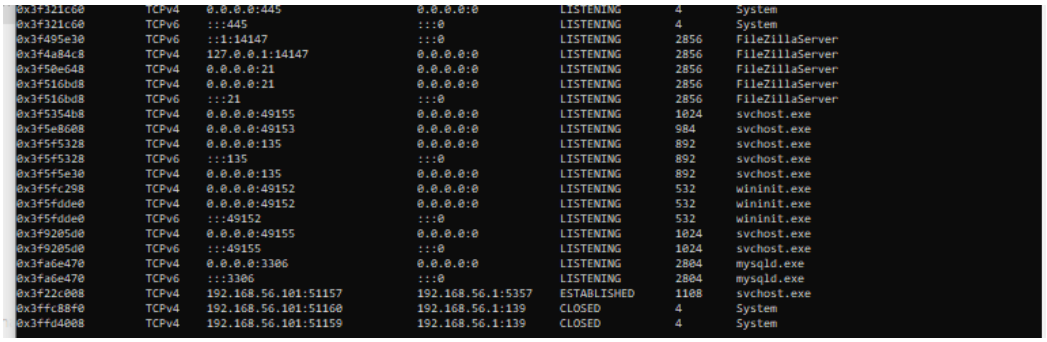


FTK Imager.exe (PID 2120)



Realizamos un escaneo de redes y conexiones de red activas en la memoria del sistema: "python vol.py -f C:\ram\memdump.mem --profile=VistaSP2x86 netscan"





0x3f321c60	TCPv4	0.0.0.0:445	0.0.0.0:0	LISTENING	4	System
0x3f321c60	TCPv6	:::445	:::0	LISTENING	4	System
0x3f495e30	TCPv6	::1:14147	:::0	LISTENING	2856	FileZillaServer
0x3f4a84c8	TCPv4	127.0.0.1:14147	0.0.0.0:0	LISTENING	2856	FileZillaServer
0x3f50e648	TCPv4	0.0.0.0:21	0.0.0.0:0	LISTENING	2856	FileZillaServer
0x3f516bd8	TCPv4	0.0.0.0:21	0.0.0.0:0	LISTENING	2856	FileZillaServer
0x3f516bd8	TCPv6	:::21	:::0	LISTENING	2856	FileZillaServer
0x3f5354b8	TCPv4	0.0.0.0:49155	0.0.0.0:0	LISTENING	1024	svchost.exe
0x3f5e8608	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING	984	svchost.exe
0x3f5f5328	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING	892	svchost.exe
0x3f5f5328	TCPv6	:::135	:::0	LISTENING	892	svchost.exe
0x3f5fe30	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING	892	svchost.exe
0x3f5fc298	TCPv4	0.0.0.0:49152	0.0.0.0:0	LISTENING	532	wininit.exe
0x3f5fdde0	TCPv4	0.0.0.0:49152	0.0.0.0:0	LISTENING	532	wininit.exe
0x3f5fdde0	TCPv6	:::49152	:::0	LISTENING	532	wininit.exe
0x3f9205d0	TCPv4	0.0.0.0:49155	0.0.0.0:0	LISTENING	1024	svchost.exe
0x3f9205d0	TCPv6	:::49155	:::0	LISTENING	1024	svchost.exe
0x3fa6e470	TCPv4	0.0.0.0:3306	0.0.0.0:0	LISTENING	2804	mysqld.exe
0x3fa6e470	TCPv6	:::3306	:::0	LISTENING	2804	mysqld.exe
0x3f22c008	TCPv4	192.168.56.101:51157	192.168.56.1:5357	ESTABLISHED	1108	svchost.exe
0x3ffc88f0	TCPv4	192.168.56.101:51160	192.168.56.1:139	CLOSED	4	System
0x3ffd4008	TCPv4	192.168.56.101:51159	192.168.56.1:139	CLOSED	4	System

- httpd.exe esta escuchando los puertos 80 y 443
- mysqld.exe esta escuchando el puerto 3306
- Hay tres conexiones en estado closed, lo que indica que hubo actividad previa en el puerto 139 (podría ser un intento de acceso compartido a la red)

192.168.56.101:51160

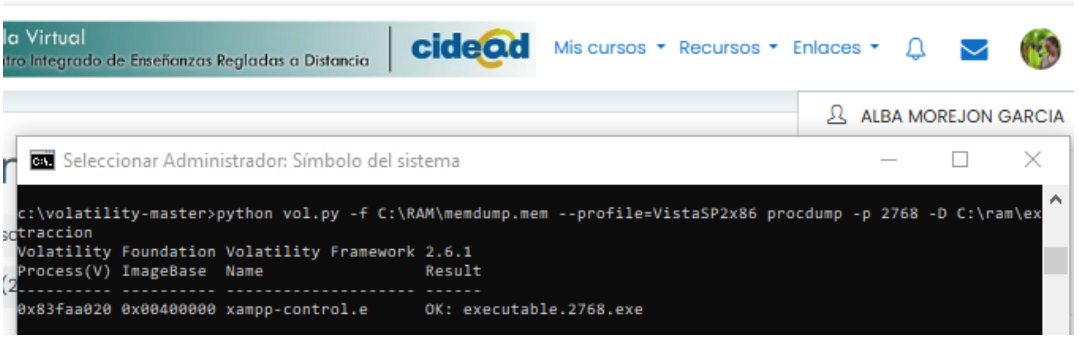
192.168.56.101:51159 a 192.168.56.1:139

- Conexión establecida a través del puerto 5357 (servicio web for devices)

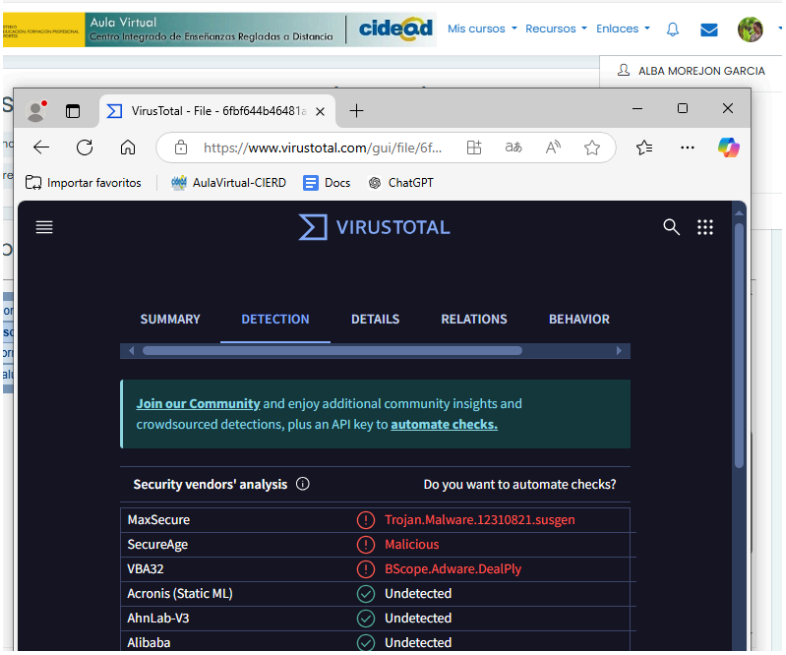
192.168.56.101:51157 a 192.168.56.1:5357

- El proceso svchost.exe se esta ejecutando de manera repetida en los puertos UDP 3702, 5355, 500, 4500 y TCP entre 49152 y 49157
- EL proceso VBoxService tiene una creación tardía en comparación con otros procesos

Nos centramos en el proceso 2768 y extraemos un volcado del proceso en específico (xampp-console.e) “python vol.py -f C:\RAM\memdump.mem --profile=VistaSP2x86 procdump -p 2768 -D C:\ram\extraccion”

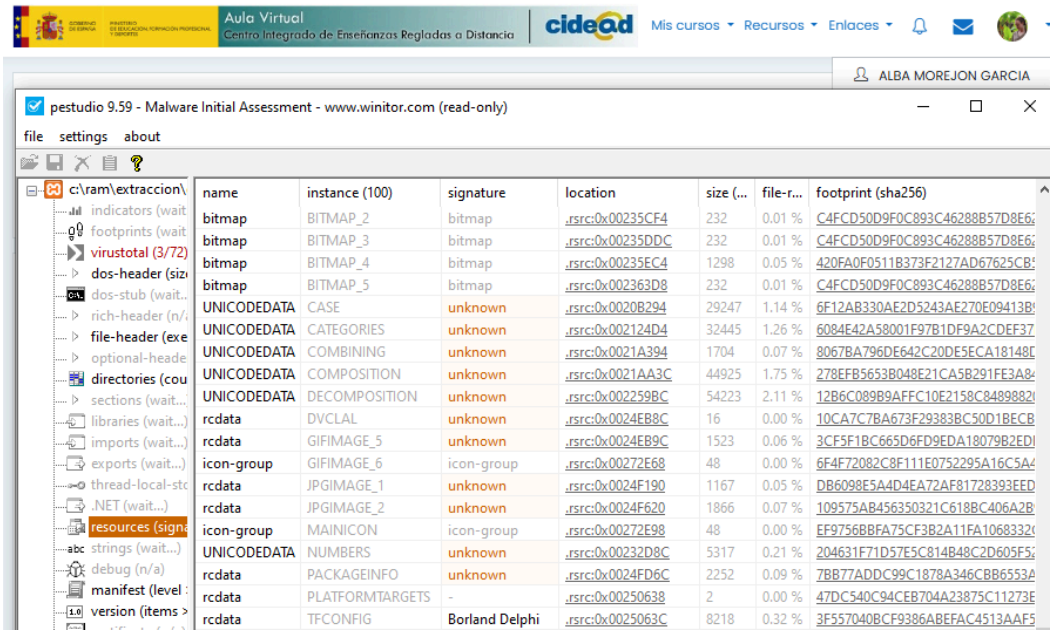


Se crea el archivo “executable.2768.exe”



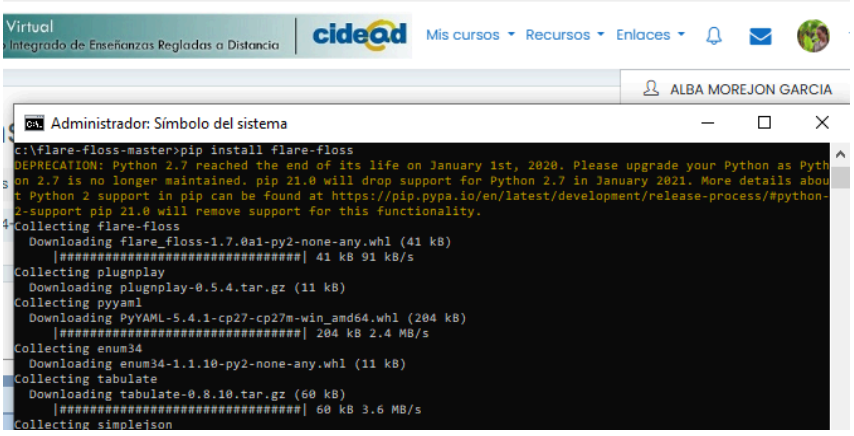
VirusTotal ha identificado que es un software malicioso, lo ha marcado como un troyano y como adware, esto sugiere que el archivo podría tener comportamientos tanto dañinos, como invasivos (robo de datos, control remoto, redireccionamiento de datos..)

Descargamos PEStudio en https://www.winitor.com/download2 y ejecutamos el ejecutable.

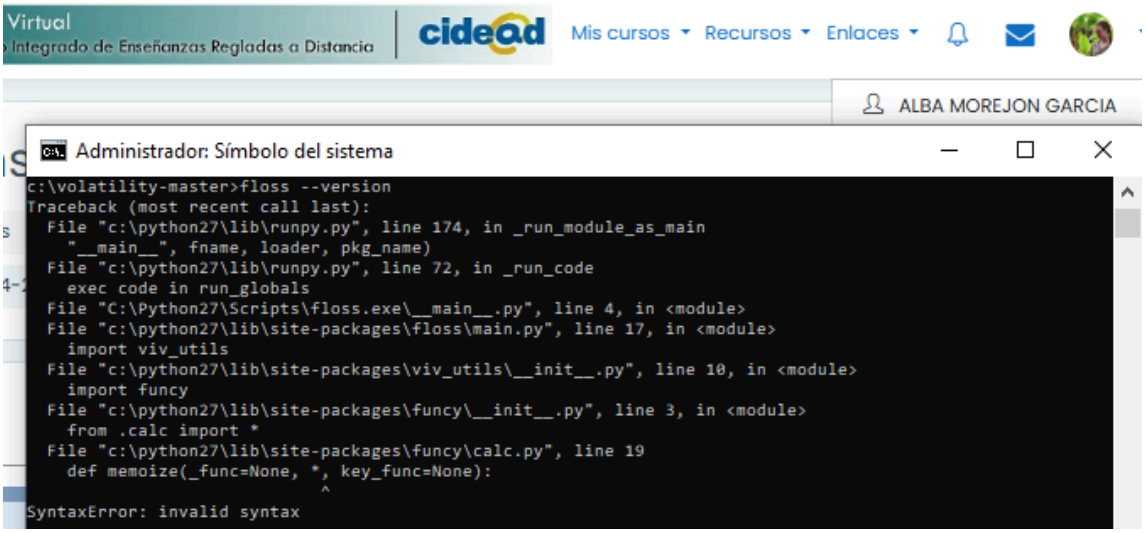


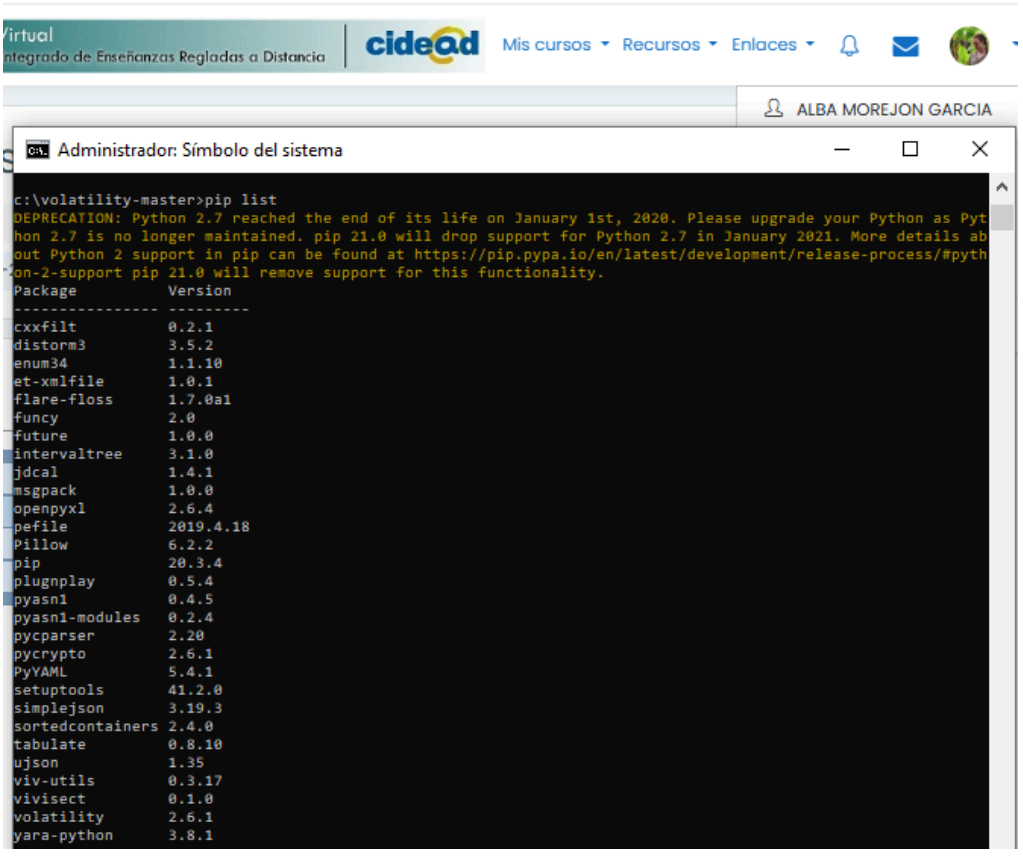
Algunos resultados que hemos obtenido con los datos de esta aplicación:
Los datos de resources son recursos incrustados en archivos ejecutables, la información unicode parece ser aleatoria o desconocida lo cual es común en malwares para ofuscarse. Los recursos como gifs y jpg incrustados suelen ser utilizados para camuflar datos maliciosos o engañar a la víctima mientras se ejecuta código dañino. El archivo hace uso de diversas funciones como GetclipboardData, OpenClipboard entre otras que son comúnmente utilizadas para robar información (contraseñas o información copiada). Además vemos que hay funciones relacionadas con la manipulación de tokens de acceso (OpenThreadToken) el malware podría estar tratando de elevar sus privilegios o ejecutar código de manera oculta. El uso de librerías como user32.dell, kernel32.dll o wtsapi32.dll es común en los malware que intentan interactuar con la interfaz de usuario o manipular procesos. La presencia de VirtualAlloc o VirtualQueryEx también sugiere que estan intentando inyectar código en otros procesos.
Las cadenas relacionadas con xampp_control podrían indicar que el malware se disfraza como software legitimo (XAMPP).

Descargamos el fichero comprimido de floss https://github.com/mandiant/flare-floss y lo descomprimimos en c:\ y lo instalamos con “pip install flare-floss”



No lo detecta (aun habiendo instalado python 3)





Apartado 2: Contestando a las preguntas
¿Qué pasaría si se hubiera apagado este servidor?
¿Qué tipo de comandos ha ejecutado el cibercriminal? ¿Qué sugiere?
¿Cómo se han ejecutado los comandos?
¿Qué actividad maliciosa has visto?
¿Puedes identificar desde qué IP vino el ataque?
¿Qué tipo de ataque pudo ser? ¿Qué tipo de malware se ha encontrado?

Si el software comprometido se hubiese apagado pudiera haberse detenido temporalmente, pero dependiendo de la naturaleza del software:

- Podría haberse vuelto a ejecutar automáticamente tras el reinicio, si tuviese técnicas de persistencia implementada, como creación de tareas programadas, modificación de recursos del sistema, técnicas de inyección
- Si estuviese en proceso de exfiltrar datos (del portapapeles por ejemplo) podría haberse detenido temporalmente, pero si ya había realizado una transmisión, los datos ya habrían sido filtrados.
- Si el malware estuviese esperando algún tipo de conexión (con un servidor) podría haberse detenido temporalmente pero el atacante podría haber restablecido la conexión tras el reinicio.
- Si el software estaba ejecutándose en segundo plano o estaba oculto, al apagarse el servidor podría haber desaparecido temporalmente, y volver a reactivarse tras el reinicio.

Basándonos en el resultado del analisis en Pestudio, el malware ha tenido

- Interacción con el portapapeles (por los comandos GetClipboardData, SetClipboardData) estos comandos permiten al atacante leer y modificar el contenido del portapapeles, buscando información sensible como contraseñas, claves…
- Manipulación de procesos y memoria (VirtualAlloc, VirtualQuery) estos comandos se utilizan para inyectar código en otros procesos y manipular la memoria del sistema. Esto indica que el atacante podría estar tratando de ocultarse dentro de otros procesos o ejecutarse en segundo plano.
- Accesos a recursos del sistema (OpenTheadToken, OpenProcessToken), estas funciones permiten la manipulación de tokens de acceso, sugieren que el atacante podría estar intentando escalar privilegios.
- Conexión con procesos (EnumThreadWindows, EnumDisplayMonitors) Pueden ser utilizados para realizar capturas o controlar la interfaz de usuario.

Estos comandos de forma general sugieren que el atacante está buscando información sensible y tratando de tomar el control total del sistema.

Los comandos han sido ejecutados por el malware en el sistema mediante inyección de código en procesos legítimos para ocultar su presencia, con manipulación de procesos, alterando tokens de acceso para escalar privilegios y accediendo al portapapeles, robando datos sensibles.
Estas acciones indican que el malware está interactuando con el sistema de manera sofisticada, con el objetivo de robar datos y obtener el control sobre el servidor.

La actividad maliciosa que hemos detectado ha sido el robo de información del portapapeles, escalada de privilegios, inyección de código en otros procesos, evasión y persistencia interactuando con la interfaz del usuario.

Debido a los errores encontrados y que no he podido resolver, no se la ip desde la que se atacó, pero se hubiera hecho con la herramienta floss analizando los logs de red para analizar la comunicación entre los servidores instalando floss y ejecutando el comando floss para analizar el proceso de xampp (apache).

Según la información recopilada el tipo de ataque parece un ataque de malware avanzado con capacidad de reconocimiento, exfiltración de datos, escalada de privilegios y persistencia, viendo las características puede ser un ataque de:

- Troyano, permiten al atacante tomar el control total de un sistema comprometido, robar datos y realizar actividades maliciosas.
- Adware, podría ser de este tipo por los componentes adicionales que muestran anuncios no deseados o interfieren en el comportamiento del sistema.
- Malware de escala de privilegios, por el uso de técnicas de manipulación de procesos y tokens, parece estar buscando elevar privilegios para tomar el control.

En resumen, el malware encontrado parece ser un troyano con capacidades de adware y escalada de privilegios, utilizado para robar datos sensibles y mantener el acceso al sistema.