

The background of the cover features abstract geometric shapes in shades of gold and yellow. In the top-left corner, there are several overlapping chevron and rectangular shapes pointing towards the center. In the bottom-right corner, there are more overlapping geometric shapes, including a large chevron pointing downwards and to the right, and several rectangular blocks of varying sizes.

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=RFYbev6hxI>

<https://www.youtube.com/watch?v=iU9mqB4h3Tg>

Otras herramientas que te pueden ser útiles

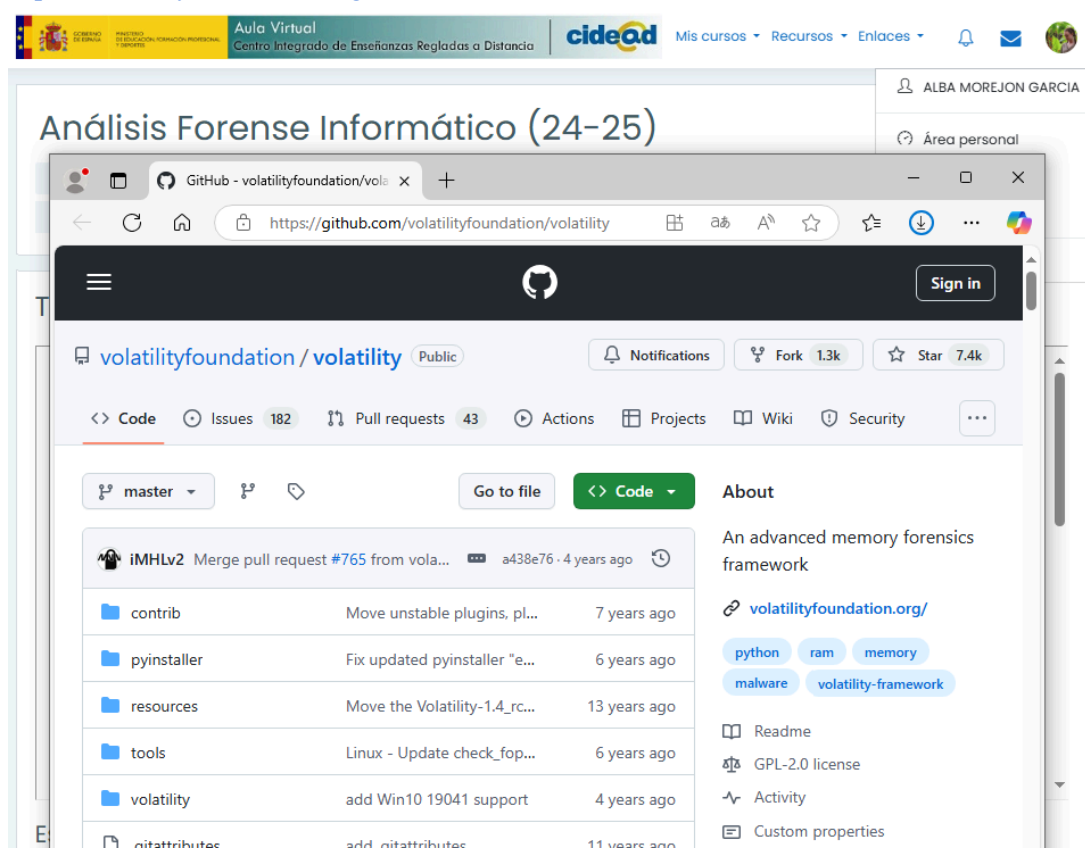
Floss: <https://github.com/mandiant/flare-floss>

DESCARGAS E INSTALACIONES

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/>

Aula Virtual
Centro Integrado de Enseñanzas Regladas a Distancia

cidead Mis cursos Recursos Enlaces

ALBA MOREJON GARCIA

Área personal

Análisis Forense Informático (24-25)

Python 2.7.18 is the last release of Python 2.

Files

Version	Operating System	Description	MD5 Sum	File Size	GPG
Gzipped source tarball	Source release		38c84292658ed4456157195f1c9bcbe1	16.7 MB	SIG
XZ compressed source tarball	Source release		fd6cc8ec0a78c44036f825e739f36e5a	12.3 MB	SIG
macOS 64-bit installer	macOS	for OS X 10.9 and later	ce98eeb7bdf806685adc265ec1444463	23.7 MB	SIG
Windows help file	Windows		b3b753dffe1c7930243c1c40ec3a72b1	6.0 MB	SIG
Windows debug information files	Windows		20b111ccfe8d06d2fe8c77679a86113d	24.0 MB	SIG
Windows debug information files for 64-bit binaries	Windows		bb0897ea20fda343e5179d413d4a4a7c	24.8 MB	SIG
Windows x86 MSI installer	Windows		db6ad9195b3086c6b4cefb9493d738d2	18.7 MB	SIG
Windows x86-64 MSI installer	Windows	for AMD64/EM64T/x64	a425c758d38f8e28b56f4724b499239a	19.6 MB	SIG

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

Aula Virtual
Centro Integrado de Enseñanzas Regladas a Distancia

cidead Mis cursos Recursos Enlaces

ALBA MOREJON GARCIA

Área personal

Perfil

Preferencias

Cerrar sesión

Análisis Forense Informático (24-25)

Página Principal Mis curso

Tarea para AFI01

Tarea online AFI01.

- 1.- Descripción de la tarea
- 2.- Información de interés.
- 3.- Evaluación de la tarea.

Python 2.7.18 (64-bit) Setup

Customize Python 2.7.18 (64-bit)

Select the way you want features to be installed. Click on the icons in the tree below to change the way features will be installed.

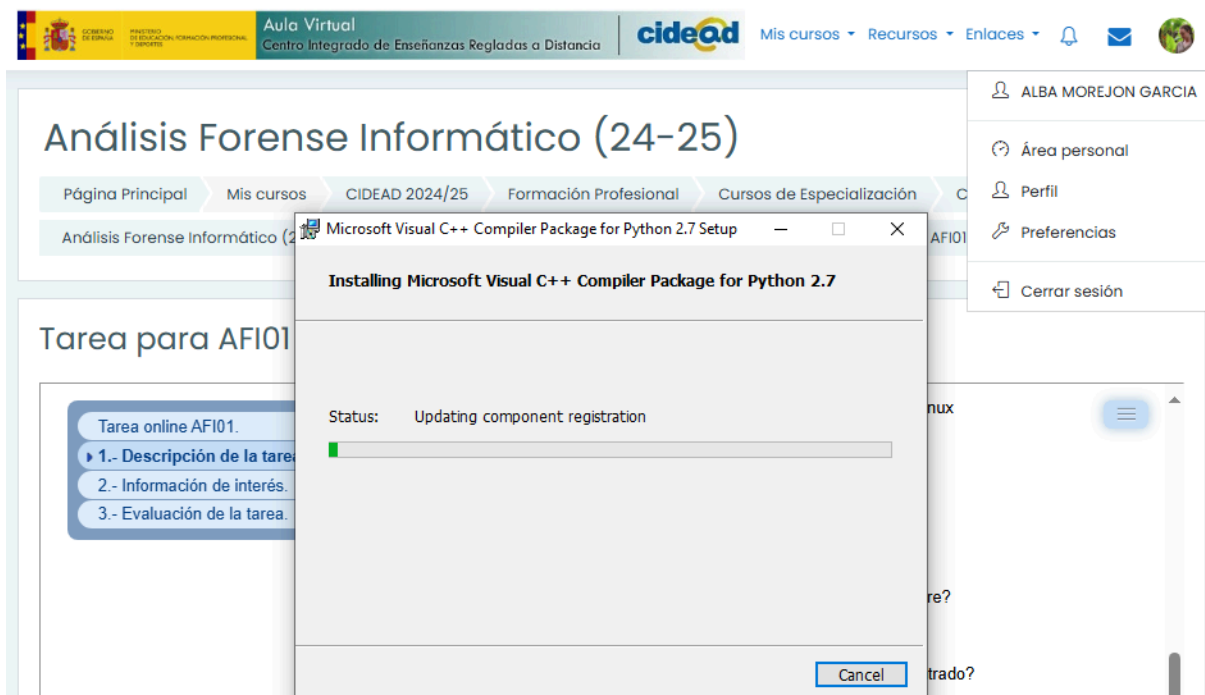
- Register Extensions
 - Tcl/Tk
 - Documentation
 - Utility Scripts
 - pip
 - Test suite
 - Add python.exe to Path**
 - Will be installed on local hard drive
 - Entire feature will be installed on local hard drive
 - Entire feature will be unavailable

Prepend C:\Python27 to PATH variable. This command prompt will be executed.

This feature requires 0KB on your hard drive.

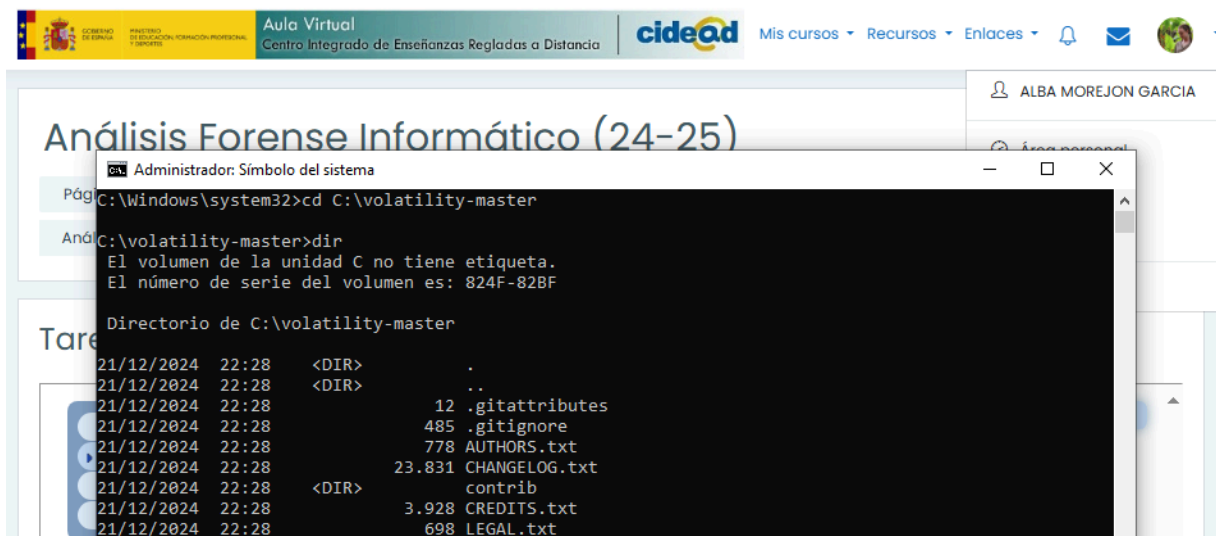
Disk Usage Advanced < Back Next > Cancel

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

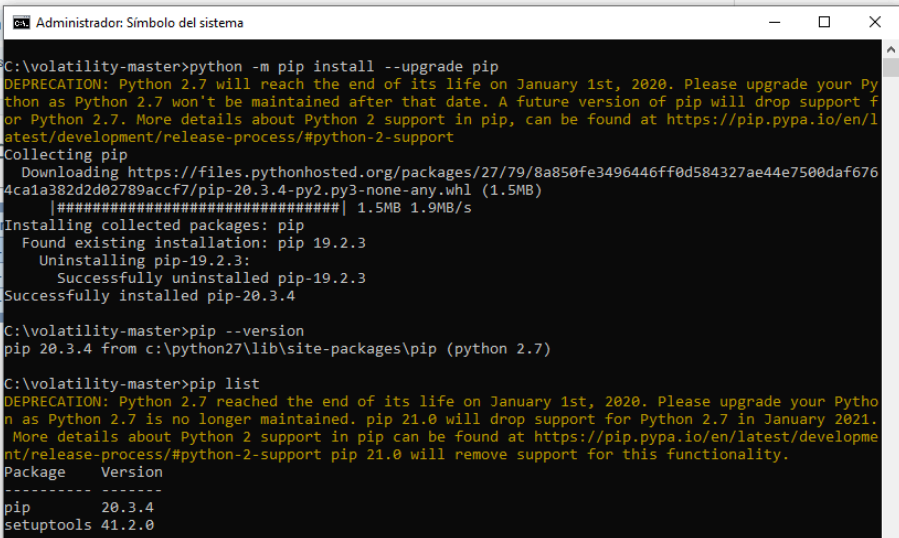


Revisamos la versión de python y la de pip:

- 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

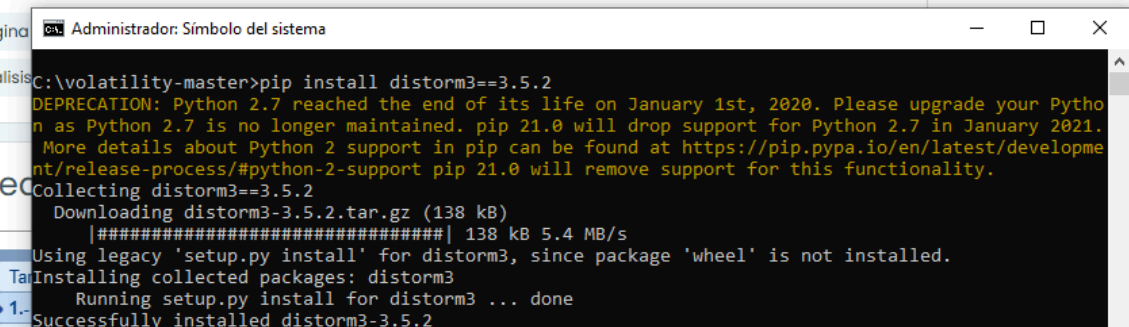


```
C:\volatility-master>python -m pip install --upgrade pip
DEPRECATION: Python 2.7 will reach the end of its life on January 1st, 2020. Please upgrade your Python to Python 3.x to avoid this message, which may affect the availability of some features and packages.
A future version of pip will drop support for Python 2.7. More details about Python 2 support in pip, can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support
Collecting pip
  Downloading https://files.pythonhosted.org/packages/27/79/8a850fe3496446ff0d584327ae44e7500daf6764ca1a382d2d02789accf7/pip-20.3.4-py2.py3-none-any.whl (1.5MB)
    |#####| 1.5MB 1.9MB/s
Installing collected packages: pip
  Found existing installation: pip 19.2.3
  Uninstalling pip-19.2.3:
    Successfully uninstalled pip-19.2.3
  Successfully installed pip-20.3.4

C:\volatility-master>pip --version
pip 20.3.4 from c:\python27\lib\site-packages\pip (python 2.7)

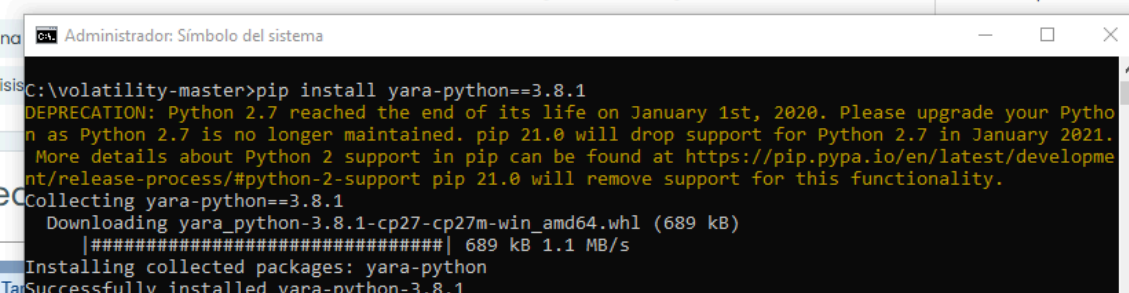
C:\volatility-master>pip list
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python to Python 3.x to avoid this message, which may affect the availability of some features and packages.
A future version of pip will drop support for Python 2.7 in January 2021. More details about Python 2 support in pip can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will remove support for this functionality.
Package Version
-----
pip      20.3.4
setuptools 41.2.0
```

A continuación instalamos las dependencias requeridas:
Distorm3 3.5.2



```
C:\volatility-master>pip install distorm3==3.5.2
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python to Python 3.x to avoid this message, which may affect the availability of some features and packages.
A future version of pip will drop support for Python 2.7 in January 2021. More details about Python 2 support in pip can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will remove support for this functionality.
Collecting distorm3==3.5.2
  Downloading distorm3-3.5.2.tar.gz (138 kB)
    |#####| 138 kB 5.4 MB/s
Using legacy 'setup.py install' for distorm3, since package 'wheel' is not installed.
Installing collected packages: distorm3
  Running setup.py install for distorm3 ... done
  Successfully installed distorm3-3.5.2
```

Yara-python 3.8.1



```
C:\volatility-master>pip install yara-python==3.8.1
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python to Python 3.x to avoid this message, which may affect the availability of some features and packages.
A future version of pip will drop support for Python 2.7 in January 2021. More details about Python 2 support in pip can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will remove support for this functionality.
Collecting yara-python==3.8.1
  Downloading yara_python-3.8.1-cp27-cp27m-win_amd64.whl (689 kB)
    |#####| 689 kB 1.1 MB/s
Installing collected packages: yara-python
  Successfully installed yara-python-3.8.1
```

Pycrypto 2.6.1

GOBIERNO DE ESPAÑA MINISTERIO DE EDUCACIÓN, FORMACIÓN PROFESIONAL Y EMPLEO

Aula Virtual Centro Integrado de Enseñanzas Regladas a Distancia

cidead Mis cursos Recursos Enlaces

ALBA MOREJON GARCIA

Análisis Forense Informático (24-25)

Área personal

Página

Administrador: Símbolo del sistema

```
C:\volatility-master>pip install pycrypto
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python to Python 3.x as Python 2.7 is no longer maintained. pip 21.0 will drop support for Python 2.7 in January 2021. More details about Python 2 support in pip can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will remove support for this functionality.
Collecting pycrypto
  Downloading pycrypto-2.6.1.tar.gz (446 kB)
    |#####| 446 kB 5.4 MB/s
Using legacy 'setup.py install' for pycrypto, since package 'wheel' is not installed.
Installing collected packages: pycrypto
  Running setup.py install for pycrypto ... done
Successfully installed pycrypto-2.6.1
```

Pillow 6.2.2

GOBIERNO DE ESPAÑA MINISTERIO DE EDUCACIÓN, FORMACIÓN PROFESIONAL Y EMPLEO

Aula Virtual Centro Integrado de Enseñanzas Regladas a Distancia

cidead MIS CURSOS Recursos Enlaces

ALBA MOREJON GARCIA

Análisis Forense Informático (24-25)

Área personal

Página

Administrador: Símbolo del sistema

```
C:\volatility-master>pip install pillow
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python to Python 3.x as Python 2.7 is no longer maintained. pip 21.0 will drop support for Python 2.7 in January 2021. More details about Python 2 support in pip can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will remove support for this functionality.
Collecting pillow
  Downloading Pillow-6.2.2-cp27-cp27m-win_amd64.whl (1.9 MB)
    |#####| 1.9 MB 4.9 MB/s
Installing collected packages: pillow
  Running setup.py install for pillow ... done
Successfully installed pillow-6.2.2
```

Openpyxl 2.6.4.

GOBIERNO DE ESPAÑA MINISTERIO DE EDUCACIÓN, FORMACIÓN PROFESIONAL Y EMPLEO

Aula Virtual Centro Integrado de Enseñanzas Regladas a Distancia

cidead Mis cursos Recursos Enlaces

ALBA MOREJON GARCIA

Análisis Forense Informático (24-25)

Área personal

Página

Administrador: Símbolo del sistema

```
C:\volatility-master>pip install openpyxl==2.6.4
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python to Python 3.x as Python 2.7 is no longer maintained. pip 21.0 will drop support for Python 2.7 in January 2021. More details about Python 2 support in pip can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will remove support for this functionality.
Collecting openpyxl==2.6.4
  Downloading openpyxl-2.6.4.tar.gz (173 kB)
    |#####| 173 kB 5.7 MB/s
Collecting jdcal
  Downloading jdcal-1.4.1-py2.py3-none-any.whl (9.5 kB)
Collecting et_xmlfile
  Downloading et_xmlfile-1.0.1.tar.gz (8.4 kB)
Using legacy 'setup.py install' for openpyxl, since package 'wheel' is not installed.
Using legacy 'setup.py install' for et-xmlfile, since package 'wheel' is not installed.
Installing collected packages: jdcal, et-xmlfile, openpyxl
  Running setup.py install for et-xmlfile ... done
  Running setup.py install for openpyxl ... done
Successfully installed et-xmlfile-1.0.1 jdcal-1.4.1 openpyxl-2.6.4
```


Ujson 1.35

ALBA MOREJON GARCIA

Área personal

Análisis Forense Informático (24-25)

```
Administrador: Símbolo del sistema
C:\volatility-master>pip install ujson==1.35
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python
n as Python 2.7 is no longer maintained. pip 21.0 will drop support for Python 2.7 in January 2021.
More details about Python 2 support in pip can be found at https://pip.pypa.io/en/latest/developme
nt/release-process/#python-2-support pip 21.0 will remove support for this functionality.
Collecting ujson==1.35
  Downloading ujson-1.35.tar.gz (192 kB)
    |#####| 192 kB 1.0 MB/s
Using legacy 'setup.py install' for ujson, since package 'wheel' is not installed.
Installing collected packages: ujson
  Running setup.py install for ujson ... done
Successfully installed ujson-1.35
```

Comprobamos los paquetes que hemos instalado

ALBA MOREJON GARCIA

Análisis Forense Informático (24-25)

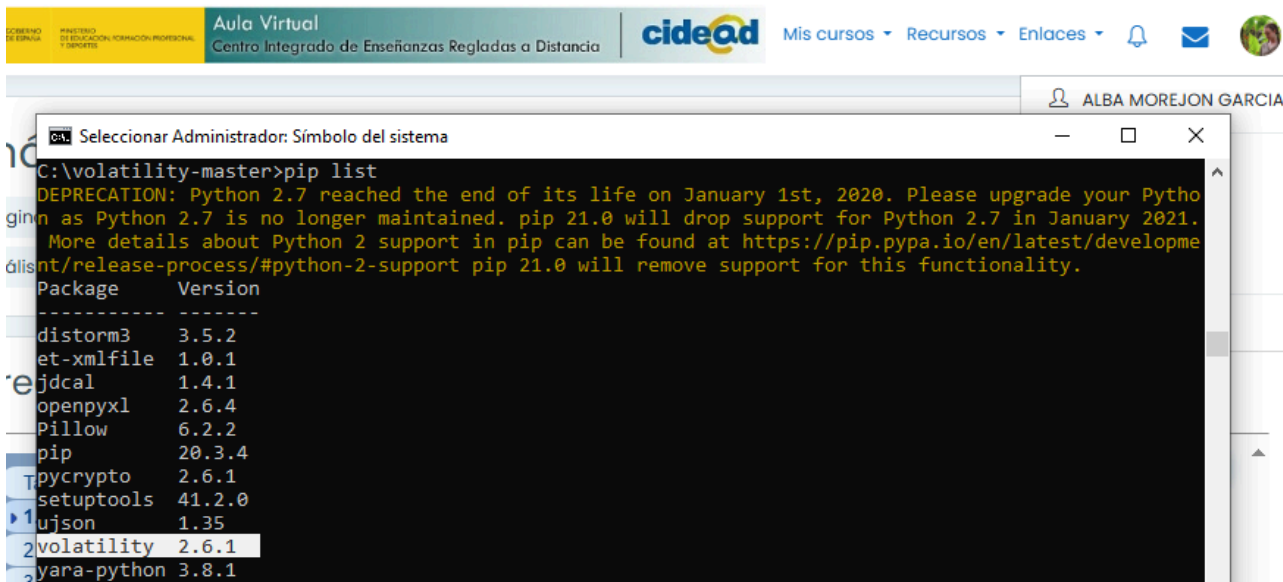
```
Administrador: Símbolo del sistema
C:\volatility-master>pip list
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python
n as Python 2.7 is no longer maintained. pip 21.0 will drop support for Python 2.7 in January 2021.
More details about Python 2 support in pip can be found at https://pip.pypa.io/en/latest/developme
nt/release-process/#python-2-support pip 21.0 will remove support for this functionality.
Package            Version
-----
distorm3           3.5.2
et-xmlfile         1.0.1
jdcal               1.4.1
openpyxl           2.6.4
Pillow             6.2.2
pip                20.3.4
pycrypto           2.6.1
setuptools         41.2.0
ujson              1.35
yara-python        3.8.1
```

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

ALBA MOREJON GARCIA

```
Administrador: Símbolo del sistema
C:\volatility-master>setup.py install
Running install
Running bdist_egg
Running egg_info
creating volatility.egg-info
writing volatility.egg-info\PKG-INFO
writing top-level names to volatility.egg-info\top_level.txt
writing dependency links to volatility.egg-info\dependency_links.txt
writing manifest file 'volatility.egg-info\SOURCES.txt'
reading manifest file 'volatility.egg-info\SOURCES.txt'
reading manifest template 'MANIFEST.in'
warning: no files found matching '*.*'

```



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)

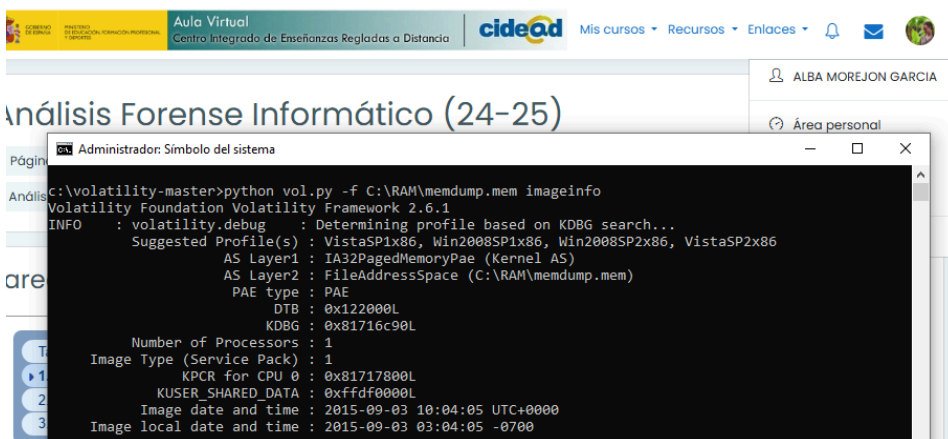
- VistaSP1x86
- Win2008SP1x86
- Win2008SP2x86
- VistaSP2x86

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
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	166	0	0	2015-08-23 20:29:18 UTC+0000
0x83945d90	lsass.exe	628	532	10	166	0	0	2015-08-23 20:29:19 UTC+0000
0x8394d020	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	1284	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
0x83acac90	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
0x83a6ec28	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
0x83cac020	taskeng.exe	1984	1024	5	135	0	0	2015-08-23 10:30:08 UTC+0000
0x83b20020	taskeng.exe	1444	1024	10	245	1	0	2015-08-23 10:30:34 UTC+0000
0x83e2f168	dmv.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	httdp.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	httdp.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”

Offset(P)	Name	PID	PPID	PDB	Time created	Time exited
0x0000000019c1100	cmd.exe	1972	816	0x3f4a7580	2015-09-02 09:28:30 UTC+0000	
0x000000002f57910	System	4	0	0x00122000	2015-08-23 20:27:20 UTC+0000	
0x0000000029e0730	wuauclt.exe	2516	1024	0x3f4a7440	2015-09-02 09:01:13 UTC+0000	
0x000000002e2f168	dmv.exe	1688	1176	0x3f4a73c0	2015-08-23 10:30:34 UTC+0000	
0x000000002e368e0	explorer.exe	816	676	0x3f4a7400	2015-08-23 10:30:34 UTC+0000	
0x000000002e4d7c0	httdp.exe	2796	2768	0x3f4a74c0	2015-08-23 10:32:21 UTC+0000	
0x000000002e652a0	VBoxTray.exe	1816	816	0x3f4a7420	2015-08-23 10:30:38 UTC+0000	
0x000000002e7b7f8	cmd.exe	612	816	0x3f4a7360	2015-08-23 10:30:44 UTC+0000	
0x000000002ef68300	FTK Imager.exe	2120	816	0x3f4a7560	2015-09-03 10:03:37 UTC+0000	
0x000000002ef84d90	svchost.exe	2424	608	0x3f4a7460	2015-08-23 10:31:51 UTC+0000	
0x000000002ef8e5d0	msdtc.exe	2620	608	0x3f4a7480	2015-08-23 10:32:10 UTC+0000	
0x000000002ef9ec70	mysqld.exe	2804	2768	0x3f4a74a0	2015-08-23 10:32:23 UTC+0000	
0x000000002efaa020	xampp-control.e	2768	816	0x3f4a74e0	2015-08-23 10:32:17 UTC+0000	
0x000000002efd5200	FileZillaServer	2856	2768	0x3f4a7500	2015-08-23 10:32:25 UTC+0000	
0x000000002efd77a8	httdp.exe	2880	2796	0x3f4a7520	2015-08-23 10:32:26 UTC+0000	
0x000000002f1ca020	taskeng.exe	1984	1024	0x3f4a7340	2015-08-23 10:30:08 UTC+0000	
0x000000002f206020	svchost.exe	984	608	0x3f4a71a0	2015-08-23 10:20:52 UTC+0000	
0x000000002f20eb88	svchost.exe	1024	608	0x3f4a71e0	2015-08-23 10:20:53 UTC+0000	
0x000000002f218020	svchost.exe	1012	608	0x3f4a71c0	2015-08-23 10:20:53 UTC+0000	
0x000000002f21e020	SLsvc.exe	1040	608	0x3f4a7200	2015-08-23 10:20:53 UTC+0000	
0x000000002f235630	svchost.exe	1108	608	0x3f4a7220	2015-08-23 10:20:54 UTC+0000	
0x000000002f2365d0	svchost.exe	1176	608	0x3f4a7240	2015-08-23 10:20:56 UTC+0000	
0x000000002f23e020	svchost.exe	1284	608	0x3f4a7260	2015-08-23 10:20:56 UTC+0000	
0x000000002f2ca900	spoolsv.exe	1476	608	0x3f4a72a0	2015-08-23 10:30:04 UTC+0000	
0x000000002f2daf90	svchost.exe	1512	608	0x3f4a72c0	2015-08-23 10:30:04 UTC+0000	
0x000000002f2dae40	svchost.exe	1556	608	0x3f4a72e0	2015-08-23 10:30:05 UTC+0000	
0x000000002f2a6c28	svchost.exe	1568	608	0x3f4a7300	2015-08-23 10:30:05 UTC+0000	
0x000000002f2f2d90	svchost.exe	1680	608	0x3f4a7320	2015-08-23 10:30:05 UTC+0000	
0x000000002f32b020	taskeng.exe	1444	1024	0x3f4a73a0	2015-08-23 10:30:34 UTC+0000	
0x000000002f4382d0	smss.exe	420	4	0x3f4a7020	2015-08-23 20:27:20 UTC+0000	
0x000000002f47ed90	winlogon.exe	560	516	0x3f4a7040	2015-08-23 20:27:28 UTC+0000	
0x000000002f4ed8c8	svchost.exe	1352	608	0x3f4a7280	2015-08-23 10:20:58 UTC+0000	
0x000000002f512208	csrss.exe	484	472	0x3f4a7060	2015-08-23 20:27:22 UTC+0000	
0x000000002f52c9f8	wininit.exe	532	472	0x3f4a70c0	2015-08-23 20:27:28 UTC+0000	
0x000000002f52d530	csrss.exe	524	516	0x3f4a70a0	2015-08-23 20:27:28 UTC+0000	
0x000000002f53bd90	services.exe	608	532	0x3f4a7080	2015-08-23 20:20:06 UTC+0000	
0x000000002f542020	lsass.exe	620	532	0x3f4a70e0	2015-08-23 20:20:18 UTC+0000	
0x000000002f545d90	lsass.exe	628	532	0x3f4a7100	2015-08-23 20:20:19 UTC+0000	
0x000000002f54d020	svchost.exe	792	608	0x3f4a7120	2015-08-23 20:20:45 UTC+0000	
0x000000002f5de900	VBoxService.exe	836	608	0x3f4a7140	2015-08-23 20:20:46 UTC+0000	
0x000000002f5f0020	svchost.exe	892	608	0x3f4a7160	2015-08-23 10:20:52 UTC+0000	
0x000000002fa4cb70	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 de 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)
- wuauc.lt.exe, es un proceso relacionado con las actualizaciones automáticas de windows
- cmd.exe, estaba ejecutando la consola de comandos
- TrustedInstaller, 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 análisis 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)
- wuauc.lt.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

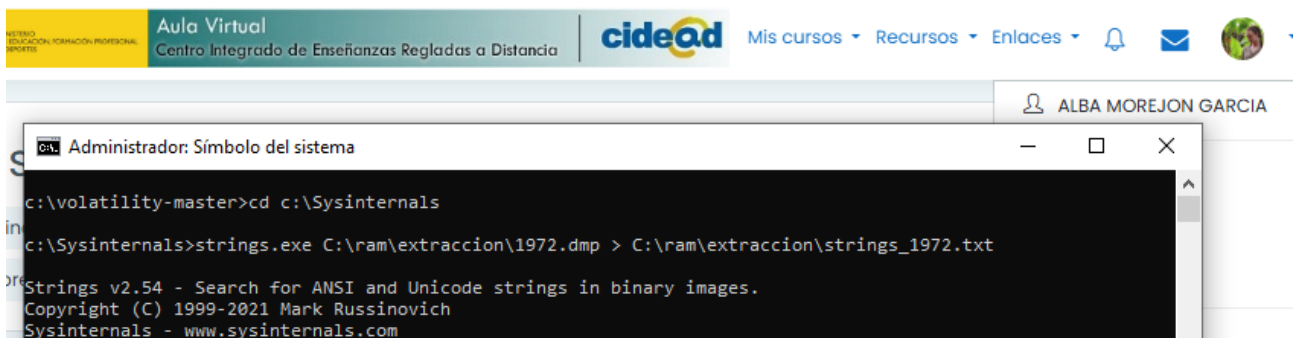
Descargamos Sysinternals Suite desde la página

<https://learn.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite> y extraemos los archivos en la carpeta c:\sysinternals ejecutamos el archivo string.exe

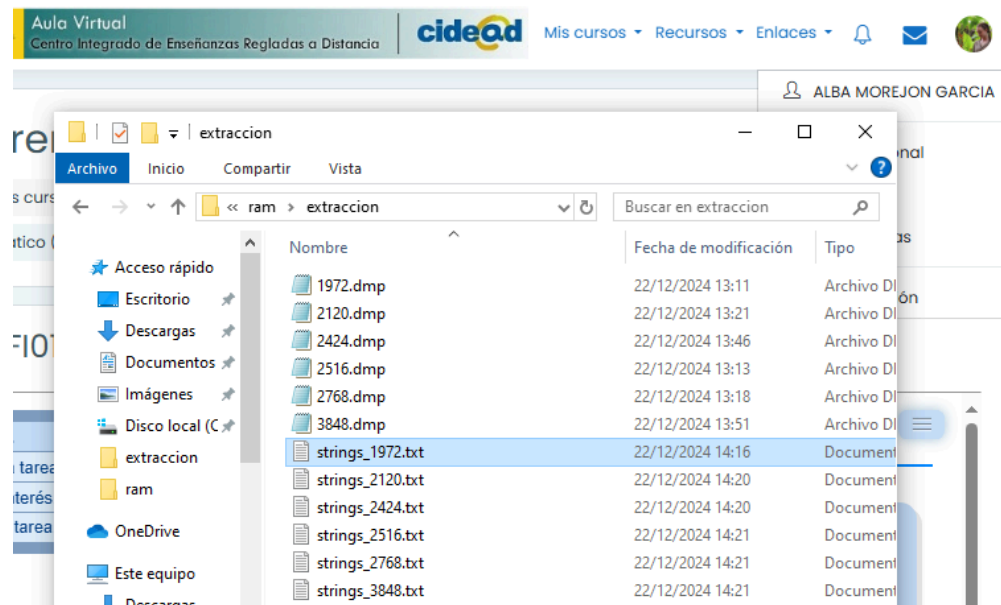
Situándonos en la carpeta recién creada y con el comando

“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:



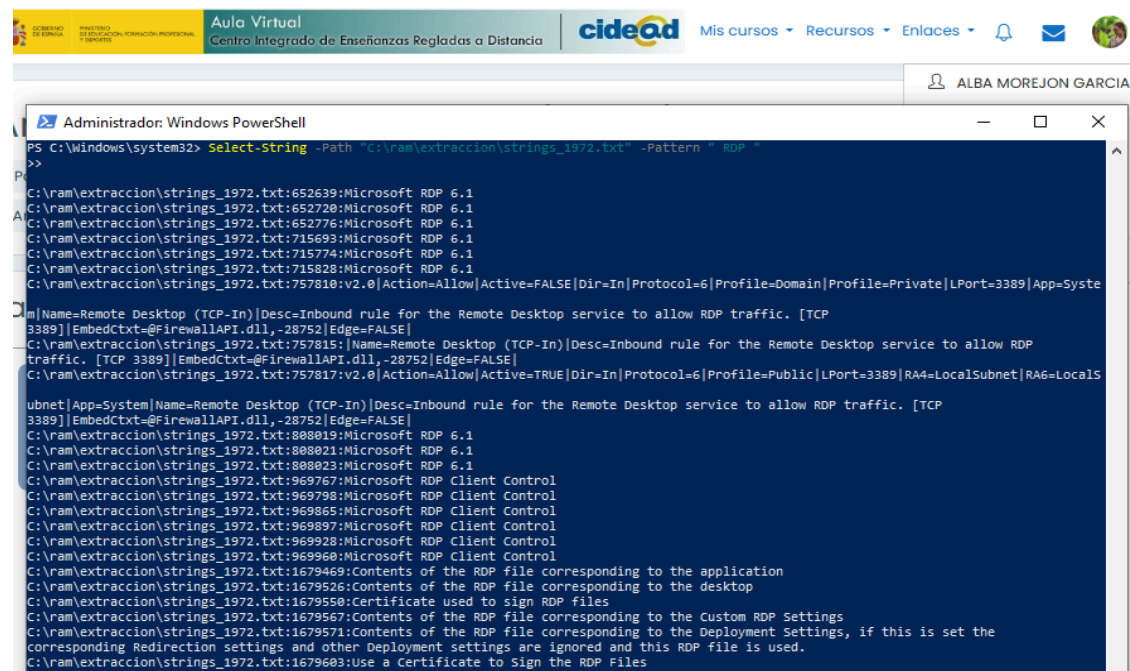
Analizamos uno por uno los archivos utilizando PowerShell y haciendo una búsqueda de palabras clave como: http, ftp, nc, password, admin, nc, RDP, PsTools, https://, .exe, .bat, net user, 192.168., taskkill...

"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...



Logo

SE

SECRETARÍA DE EDUCACIÓN

MINISTERIO DE EDUCACIÓN

COMUNICACIÓN PROFESIONAL Y TECNOLÓGICA

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:218939: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:22291:Enter password to decrypt:
C:\ram\extraccion\strings_2120.txt:223381:Certificate cannot be empty! Incorrect password or certificate
C:\ram\extraccion\strings_2120.txt:223383:Enter Password To Decrypt
C:\ram\extraccion\strings_2120.txt:223384:Enter Password To Decrypt: %s
C:\ram\extraccion\strings_2120.txt:223386:Enter Password To Encrypt
C:\ram\extraccion\strings_2120.txt:223387:Enter Password To Encrypt: %s
C:\ram\extraccion\strings_2120.txt:374954:The password was not allowed
C:\ram\extraccion\strings_2120.txt:928498: Windows BitLocker Drive Encryption Password Entry<br/>
Enter the recovery password for this drive.<br/>
C:\ram\extraccion\strings_2120.txt:928501: You must supply a BitLocker recovery password to start this system.<br/>
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:2107797: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.
```

Logo

SE

SECRETARÍA DE EDUCACIÓN

MINISTERIO DE EDUCACIÓN

COMUNICACIÓN PROFESIONAL Y TECNOLÓGICA

Aula Virtual

Centro Integrado de Enseñanzas Regladas a Distancia

cidead

Mis cursos ▾ Recursos ▾ Enlaces ▾

🔔

✉

🌐

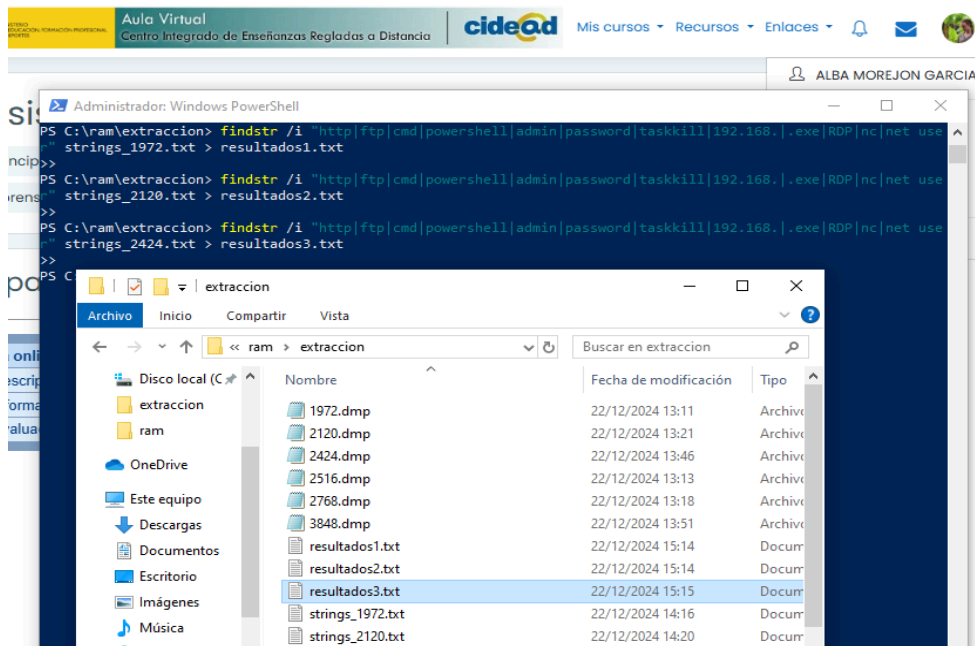
ALBA MOREJON GARCIA

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.exe
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.exe
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=NonSxS
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.manifestn1
```


Hemos creado también archivos con las palabras clave que contenían algunos de los procesos para poder analizarlo mejor:

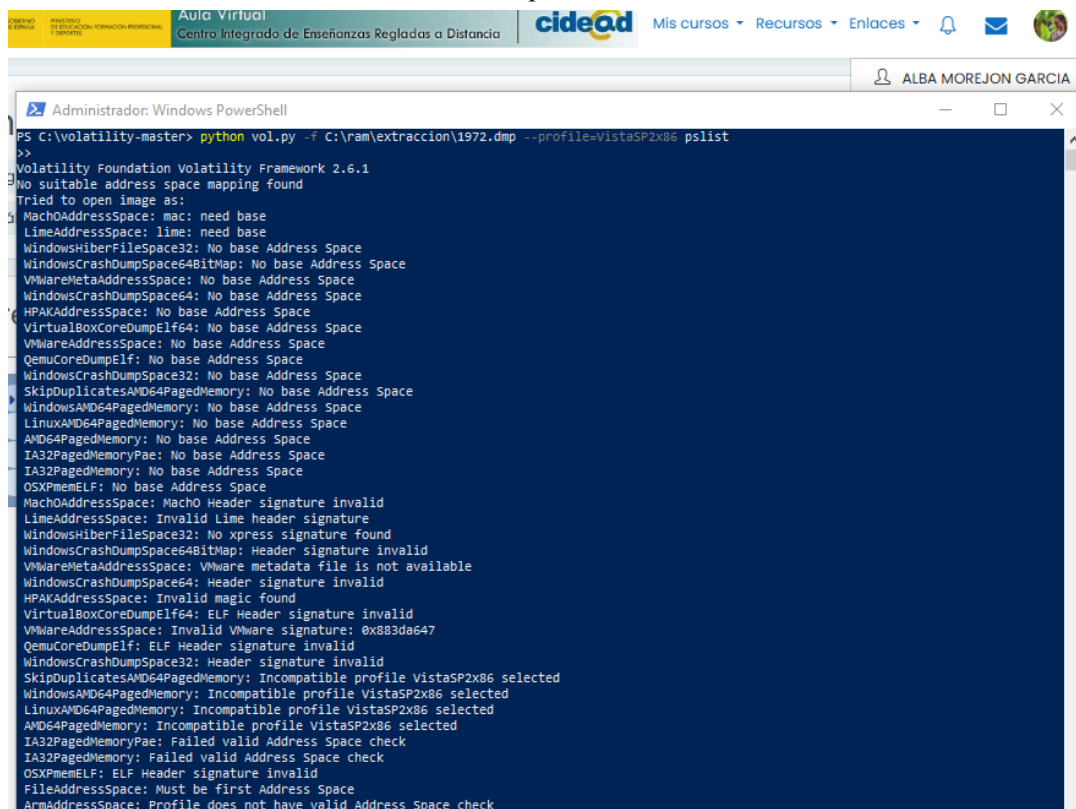
“findstr /i "http|ftp|cmd|powershell|admin|password|taskkill|192.168.|.exe|RDP|nc|net user" strings_1972.txt > resultados1.txt”



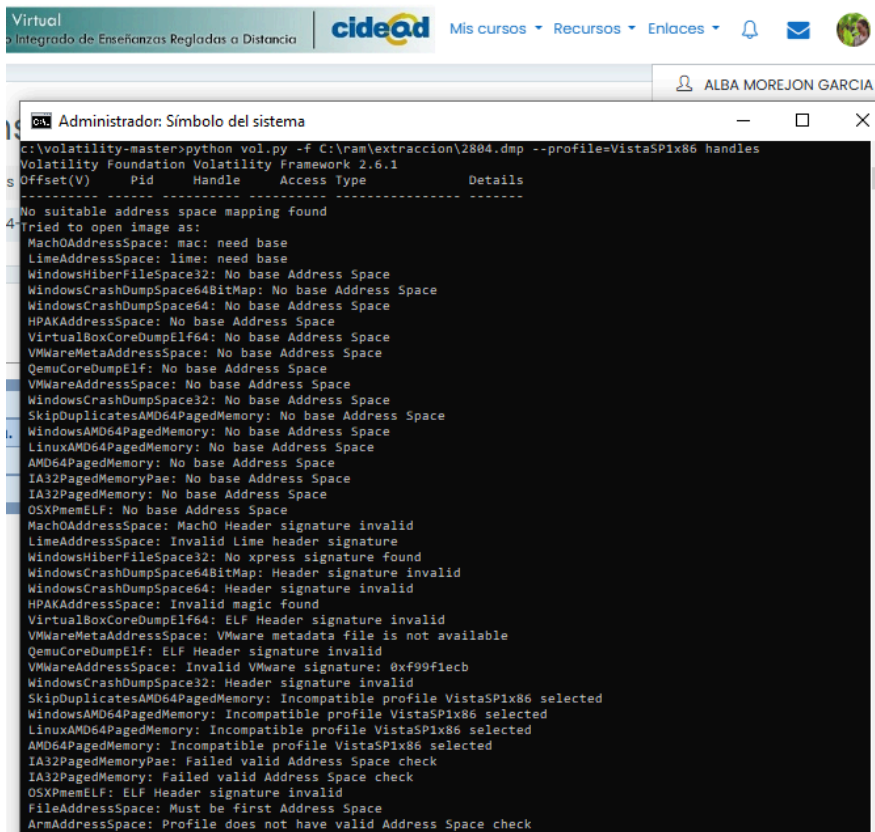
Vamos a pasar a ver más información sobre los procesos y sus propiedades:

“python vol.py -f C:\ram\extraccion\XXXX.dmp --profile=VistaSP2x86 pslist”

Nos sale este mismo resultado con todos los procesos



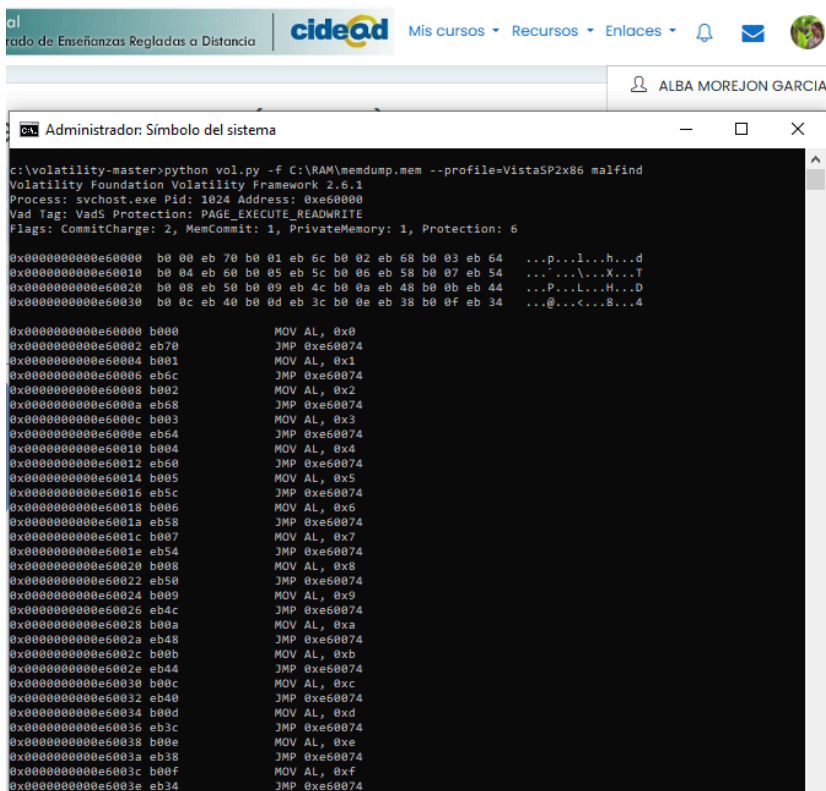
Nos aparece este mismo resultado con netscan, filescan, pslistcls, malfind y handles
Y probando los diferentes sistemas de la memoria VistaSP1x86, Win2008SP2x86 también pasa igual



```

C:\volatility-master>python vol.py -f C:\ram\extraccion\2804.dmp --profile=VistaSP1x86 handles
Volatility Foundation Volatility Framework 2.6.1
Offset(V)  Pid  Handle  Access Type  Details
-----
No suitable address space mapping found
4- tried to open image as:
MachOAddressSpace: mac: need base
LimeAddressSpace: lime: need base
WindowsHiberFileSpace32: No base Address Space
WindowsCrashDumpSpace64BitMap: No base Address Space
WindowsCrashDumpSpace64: No base Address Space
HPAKAddressSpace: No base Address Space
VirtualBoxCoreDumpElf64: No base Address Space
VMWareMetaAddressSpace: No base Address Space
QemuCoreDumpElf: No base Address Space
VMWareAddressSpace: No base Address Space
WindowsCrashDumpSpace32: No base Address Space
SkipDuplicatesAMD64PagedMemory: No base Address Space
WindowsAMD64PagedMemory: No base Address Space
LinuxAMD64PagedMemory: No base Address Space
AMD64PagedMemory: No base Address Space
IA32PagedMemoryPae: No base Address Space
IA32PagedMemory: No base Address Space
OSXPmemELF: No base Address Space
MachOAddressSpace: MachO Header signature invalid
LimeAddressSpace: Invalid Lime header signature
WindowsHiberFileSpace32: No xpress signature found
WindowsCrashDumpSpace64BitMap: Header signature invalid
WindowsCrashDumpSpace64: Header signature invalid
HPAKAddressSpace: Invalid magic found
VirtualBoxCoreDumpElf64: ELF Header signature invalid
VMWareMetaAddressSpace: VMware metadata file is not available
QemuCoreDumpElf: ELF Header signature invalid
VMWareAddressSpace: Invalid VMware signature: 0xf99f1ecb
WindowsCrashDumpSpace32: Header signature invalid
SkipDuplicatesAMD64PagedMemory: Incompatible profile VistaSP1x86 selected
WindowsAMD64PagedMemory: Incompatible profile VistaSP1x86 selected
LinuxAMD64PagedMemory: Incompatible profile VistaSP1x86 selected
AMD64PagedMemory: Incompatible profile VistaSP1x86 selected
IA32PagedMemoryPae: Failed valid Address Space check
IA32PagedMemory: Failed valid Address Space check
OSXPmemELF: ELF Header signature invalid
FileAddressSpace: Must be first Address Space
ArmAddressSpace: Profile does not have valid Address Space check
  
```

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)



```

c:\volatility-master>python vol.py -f C:\RAM\memdump.mem --profile=VistaSP2x86 malfind
Volatility Foundation Volatility Framework 2.6.1
Process: svchost.exe Pid: 1024 Address: 0xe60000
Vad Tag: Vad5 Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 2, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00000000e60000  b0 00 eb 70 b0 01 ab 6c b0 02 eb 68 b0 03 ab 64  ...p...l...h...d
0x00000000e60010  b0 04 eb 60 b0 05 ab 5c b0 06 eb 58 b0 07 ab 54  ... ..X...T
0x00000000e60020  b0 08 eb 50 b0 09 ab 4c b0 0a eb 48 b0 0b ab 44  ...P...L...H...D
0x00000000e60030  b0 0c eb 40 b0 0d ab 3c b0 0e eb 38 b0 0f ab 34  ...@...c...8...4

0x00000000e60000  b000      MOV AL, 0x0
0x00000000e60002  eb70      JMP 0xe60074
0x00000000e60004  b001      MOV AL, 0x1
0x00000000e60006  eb6c      JMP 0xe60074
0x00000000e60008  b002      MOV AL, 0x2
0x00000000e6000a  eb58      JMP 0xe60074
0x00000000e6000c  b003      MOV AL, 0x3
0x00000000e6000e  eb54      JMP 0xe60074
0x00000000e60010  b004      MOV AL, 0x4
0x00000000e60012  eb60      JMP 0xe60074
0x00000000e60014  b005      MOV AL, 0x5
0x00000000e60016  eb5c      JMP 0xe60074
0x00000000e60018  b006      MOV AL, 0x6
0x00000000e6001a  eb58      JMP 0xe60074
0x00000000e6001c  b007      MOV AL, 0x7
0x00000000e6001e  eb54      JMP 0xe60074
0x00000000e60020  b008      MOV AL, 0x8
0x00000000e60022  eb50      JMP 0xe60074
0x00000000e60024  b009      MOV AL, 0x9
0x00000000e60026  eb4c      JMP 0xe60074
0x00000000e60028  b00a      MOV AL, 0xa
0x00000000e6002a  eb48      JMP 0xe60074
0x00000000e6002c  b00b      MOV AL, 0xb
0x00000000e6002e  eb44      JMP 0xe60074
0x00000000e60030  b00c      MOV AL, 0xc
0x00000000e60032  eb40      JMP 0xe60074
0x00000000e60034  b00d      MOV AL, 0xd
0x00000000e60036  eb3c      JMP 0xe60074
0x00000000e60038  b00e      MOV AL, 0xe
0x00000000e6003a  eb38      JMP 0xe60074
0x00000000e6003c  b00f      MOV AL, 0xf
0x00000000e6003e  eb34      JMP 0xe60074
  
```


svchost.exe (PID 1108)

```
ual
grado de Enseñanzas Regladas a Distancia
cideon Mis cursos Recursos Enlaces ALBA MOREJON GARCIA

Administrador: Símbolo del sistema
Process: svchost.exe Pid: 1108 Address: 0x6c0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 2, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00000000006c0000 b0 00 eb 70 b0 01 eb 6c b0 02 eb 68 b0 03 eb 64 ...p...l...h...d
0x00000000006c0010 b0 04 eb 60 b0 05 eb 5c b0 06 eb 58 b0 07 eb 54 ...'...X...T
0x00000000006c0020 b0 08 eb 50 b0 09 eb 4c b0 0a eb 48 b0 0b eb 44 ...P...L...H...D
0x00000000006c0030 b0 0c eb 40 b0 0d eb 3c b0 0e eb 38 b0 0f eb 34 ...@...<...8...4

0x00000000006c0000 b000 MOV AL, 0x0
0x00000000006c0002 eb70 JMP 0x6c0074
0x00000000006c0004 b001 MOV AL, 0x1
0x00000000006c0006 eb6c JMP 0x6c0074
0x00000000006c0008 b002 MOV AL, 0x2
0x00000000006c000a eb68 JMP 0x6c0074
0x00000000006c000c b003 MOV AL, 0x3
0x00000000006c000e eb64 JMP 0x6c0074
0x00000000006c0010 b004 MOV AL, 0x4
0x00000000006c0012 eb60 JMP 0x6c0074
0x00000000006c0014 b005 MOV AL, 0x5
0x00000000006c0016 eb5c JMP 0x6c0074
0x00000000006c0018 b006 MOV AL, 0x6
0x00000000006c001a eb58 JMP 0x6c0074
0x00000000006c001c b007 MOV AL, 0x7
0x00000000006c001e eb54 JMP 0x6c0074
0x00000000006c0020 b008 MOV AL, 0x8
0x00000000006c0022 eb50 JMP 0x6c0074
0x00000000006c0024 b009 MOV AL, 0x9
0x00000000006c0026 eb4c JMP 0x6c0074
0x00000000006c0028 b00a MOV AL, 0xa
0x00000000006c002a eb48 JMP 0x6c0074
0x00000000006c002c b00b MOV AL, 0xb
0x00000000006c002e eb44 JMP 0x6c0074
0x00000000006c0030 b00c MOV AL, 0xc
0x00000000006c0032 eb40 JMP 0x6c0074
0x00000000006c0034 b00d MOV AL, 0xd
0x00000000006c0036 eb3c JMP 0x6c0074
0x00000000006c0038 b00e MOV AL, 0xe
0x00000000006c003a eb38 JMP 0x6c0074
0x00000000006c003c b00f MOV AL, 0xf
0x00000000006c003e eb34 JMP 0x6c0074
```

explorer.exe (PID 816)

```
ual
grado de Enseñanzas Regladas a Distancia
cideon Mis cursos Recursos Enlaces ALBA MOREJON GARCIA

Administrador: Símbolo del sistema
Process: explorer.exe Pid: 816 Address: 0x9d0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00000000009d0000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000000009d0010 00 00 9d 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000000009d0020 10 00 9d 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000000009d0030 20 00 9d 00 00 00 00 00 00 00 00 00 00 00 .....

0x00000000009d0000 0000 ADD [EAX], AL
0x00000000009d0002 0000 ADD [EAX], AL
0x00000000009d0004 0000 ADD [EAX], AL
0x00000000009d0006 0000 ADD [EAX], AL
0x00000000009d0008 0000 ADD [EAX], AL
0x00000000009d000a 0000 ADD [EAX], AL
0x00000000009d000c 0000 ADD [EAX], AL
0x00000000009d000e 0000 ADD [EAX], AL
0x00000000009d0010 0000 ADD [EAX], AL
0x00000000009d0012 9d POPF
0x00000000009d0013 0000 ADD [EAX], AL
0x00000000009d0015 0000 ADD [EAX], AL
0x00000000009d0017 0000 ADD [EAX], AL
0x00000000009d0019 0000 ADD [EAX], AL
0x00000000009d001b 0000 ADD [EAX], AL
0x00000000009d001d 0000 ADD [EAX], AL
0x00000000009d001f 0010 ADD [EAX], DL
0x00000000009d0021 009d00000000 ADD [EBP+0x0], BL
0x00000000009d0023 0000 ADD [EAX], AL
0x00000000009d0025 0000 ADD [EAX], AL
0x00000000009d0027 0000 ADD [EAX], AL
0x00000000009d0029 0000 ADD [EAX], AL
0x00000000009d002b 0000 ADD [EAX], AL
0x00000000009d002d 0000 ADD [EAX], AL
0x00000000009d002f 0020 ADD [EAX], AH
0x00000000009d0031 009d00000000 ADD [EBP+0x0], BL
0x00000000009d0033 0000 ADD [EAX], AL
0x00000000009d0035 0000 ADD [EAX], AL
0x00000000009d0037 0000 ADD [EAX], AL
0x00000000009d0039 0000 ADD [EAX], AL
0x00000000009d003b 0000 ADD [EAX], AL
0x00000000009d003d 0000 ADD [EAX], AL
0x00000000009d003f 00 DB 0x0
```

Grado de Enseñanzas Regladas a Distancia cidead Mis cursos Recursos Enlaces ALBA MOREJON GARCIA

Administrador: Símbolo del sistema

Process: explorer.exe Pid: 816 Address: 0x1f1000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 2, MemCommit: 1, PrivateMemory: 1, Protection: 6

```
0x00000000f10000 b0 00 eb 70 b0 01 eb 6c b0 02 eb 68 b0 03 eb 64 ...p...l...h...d
0x00000000f10010 b0 04 eb 60 b0 05 eb 5c b0 06 eb 58 b0 07 eb 54 ...'...\\...X...T
0x00000000f10020 b0 08 eb 50 b0 09 eb 4c b0 0a eb 48 b0 0b eb 44 ...P...L...H...D
0x00000000f10030 b0 0c eb 40 b0 0d eb 3c b0 0e eb 38 b0 0f eb 34 ...@...<...8...4

0x00000000f10000 b000 MOV AL, 0x0
0x00000000f10002 eb70 JMP 0x1f10074
0x00000000f10004 b001 MOV AL, 0x1
0x00000000f10006 eb6c JMP 0x1f10074
0x00000000f10008 b002 MOV AL, 0x2
0x00000000f1000a eb68 JMP 0x1f10074
0x00000000f1000c b003 MOV AL, 0x3
0x00000000f1000e eb64 JMP 0x1f10074
0x00000000f10010 b004 MOV AL, 0x4
0x00000000f10012 eb60 JMP 0x1f10074
0x00000000f10014 b005 MOV AL, 0x5
0x00000000f10016 eb5c JMP 0x1f10074
0x00000000f10018 b006 MOV AL, 0x6
0x00000000f1001a eb58 JMP 0x1f10074
0x00000000f1001c b007 MOV AL, 0x7
0x00000000f1001e eb54 JMP 0x1f10074
0x00000000f10020 b008 MOV AL, 0x8
0x00000000f10022 eb50 JMP 0x1f10074
0x00000000f10024 b009 MOV AL, 0x9
0x00000000f10026 eb4c JMP 0x1f10074
0x00000000f10028 b00a MOV AL, 0xa
0x00000000f1002a eb48 JMP 0x1f10074
0x00000000f1002c b00b MOV AL, 0xb
0x00000000f1002e eb44 JMP 0x1f10074
0x00000000f10030 b00c MOV AL, 0xc
0x00000000f10032 eb40 JMP 0x1f10074
0x00000000f10034 b00d MOV AL, 0xd
0x00000000f10036 eb3c JMP 0x1f10074
0x00000000f10038 b00e MOV AL, 0xe
0x00000000f1003a eb38 JMP 0x1f10074
0x00000000f1003c b00f MOV AL, 0xf
0x00000000f1003e eb34 JMP 0x1f10074
```

xampp-control.e (PID 2768)

Grado de Enseñanzas Regladas a Distancia cidead Mis cursos Recursos Enlaces ALBA MOREJON GARCIA

Administrador: Símbolo del sistema

Process: xampp-control.e Pid: 2768 Address: 0x280000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

```
0x00000000280000 00 00 00 00 59 e9 0a 7b 1d 00 e8 f5 ff ff ff 00 ....V..{.....
0x00000000280010 00 00 00 00 00 00 e8 e8 ff ff ff 0a 00 28 00 .....(.....
0x00000000280020 00 00 00 00 e8 db ff ff ff 17 00 28 00 00 00 .....(.....
0x00000000280030 00 e8 ce ff ff ff 24 00 28 00 00 00 00 e8 c1 .....$.{.....

0x00000000280000 0000 ADD [EAX], AL
0x00000000280002 0000 ADD [EAX], AL
0x00000000280004 59 POP ECX
0x00000000280005 e90a7b1d00 JMP 0x457b14
0x0000000028000a e8f5ffffff CALL 0x280004
0x0000000028000f 0000 ADD [EAX], AL
0x00000000280011 0000 ADD [EAX], AL
0x00000000280013 0000 ADD [EAX], AL
0x00000000280015 0000 ADD [EAX], AL
0x00000000280017 e8e8ffffff CALL 0x280004
0x0000000028001c 0a00 OR AL, [EAX]
0x0000000028001e 2800 SUB [EAX], AL
0x00000000280020 0000 ADD [EAX], AL
0x00000000280022 0000 ADD [EAX], AL
0x00000000280024 e8dbffffff CALL 0x280004
0x00000000280029 17 POP SS
0x0000000028002a 0028 ADD [EAX], CH
0x0000000028002c 0000 ADD [EAX], AL
0x0000000028002e 0000 ADD [EAX], AL
0x00000000280030 00e8 ADD AL, CH
0x00000000280032 ce INTO
0x00000000280033 ff DB 0xff
0x00000000280034 ff DB 0xff
0x00000000280035 ff2400 JMP DWORD [EAX+EAX]
0x00000000280038 2800 SUB [EAX], AL
0x0000000028003a 0000 ADD [EAX], AL
0x0000000028003c 0000 ADD [EAX], AL
0x0000000028003e e8 DB 0xe8
0x0000000028003f c1 DB 0xc1
```

FTK Imager.exe (PID 2120)

```

ALBA MOREJON GARCIA

Administrador: Símbolo del sistema

Process: FTK Imager.exe Pid: 2120 Address: 0x4f40000
Vad Tag: Vad5 Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 2, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x000000004f40000 b0 00 eb 70 b0 01 ab 6c b0 02 ab 68 b0 03 eb 64 ...p...l...h...d
0x000000004f40010 b0 04 eb 60 b0 05 ab 5c b0 06 ab 58 b0 07 eb 54 ...P...X...T
0x000000004f40020 b0 08 eb 50 b0 09 ab 4c b0 0a ab 48 b0 0b eb 44 ...P...L...H...D
0x000000004f40030 b0 0c eb 40 b0 0d ab 3c b0 0e ab 38 b0 0f eb 34 ...@...c...8...4

0x000000004f40000 b000 MOV AL, 0x0
0x000000004f40002 eb70 JMP 0x4f40074
0x000000004f40004 b001 MOV AL, 0x1
0x000000004f40006 eb6c JMP 0x4f40074
0x000000004f40008 b002 MOV AL, 0x2
0x000000004f4000a eb68 JMP 0x4f40074
0x000000004f4000c b003 MOV AL, 0x3
0x000000004f4000e eb64 JMP 0x4f40074
0x000000004f40010 b004 MOV AL, 0x4
0x000000004f40012 eb60 JMP 0x4f40074
0x000000004f40014 b005 MOV AL, 0x5
0x000000004f40016 eb5c JMP 0x4f40074
0x000000004f40018 b006 MOV AL, 0x6
0x000000004f4001a eb58 JMP 0x4f40074
0x000000004f4001c b007 MOV AL, 0x7
0x000000004f4001e eb54 JMP 0x4f40074
0x000000004f40020 b008 MOV AL, 0x8
0x000000004f40022 eb50 JMP 0x4f40074
0x000000004f40024 b009 MOV AL, 0x9
0x000000004f40026 eb4c JMP 0x4f40074
0x000000004f40028 b00a MOV AL, 0xa
0x000000004f4002a eb48 JMP 0x4f40074
0x000000004f4002c b00b MOV AL, 0xb
0x000000004f4002e eb44 JMP 0x4f40074
0x000000004f40030 b00c MOV AL, 0xc
0x000000004f40032 eb40 JMP 0x4f40074
0x000000004f40034 b00d MOV AL, 0xd
0x000000004f40036 eb3c JMP 0x4f40074
0x000000004f40038 b00e MOV AL, 0xe
0x000000004f4003a eb38 JMP 0x4f40074
0x000000004f4003c b00f MOV AL, 0xf
0x000000004f4003e eb34 JMP 0x4f40074

```

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”

```

Aula Virtual
Centro Integrado de Enseñanzas Regladas a Distancia

cideon Mis cursos Recursos Enlaces

ALBA MOREJON GARCIA

Selección Administrador: Símbolo del sistema

c:\volatility-master>python vol.py -f C:\ram\memdump.mem --profile=VistaSP2x86 netscan
Volatility Foundation Volatility Framework 2.6.1

Offset(P) Proto Local Address Foreign Address State Pid Owner Created
0x1972938 UDPv4 0.0.0.0:123 *:* 1108 svchost.exe 2015-09-03 06:08:35 UTC+0000
0x1972938 UDPv6 :::123 *:* 1108 svchost.exe 2015-09-03 06:08:35 UTC+0000
0x1974a80 UDPv4 0.0.0.0:3702 *:* 1108 svchost.exe 2015-09-03 10:03:20 UTC+0000
0x196d320 TCPv4 192.168.56.101:139 0.0.0.0 LISTENING 4 System
0x3ee4540 UDPv4 0.0.0.0:123 *:* 1108 svchost.exe 2015-09-03 06:08:35 UTC+0000
0x3ee5548 UDPv4 0.0.0.0:5355 *:* 1204 svchost.exe 2015-09-03 06:08:37 UTC+0000
0x3ee5548 UDPv6 :::5355 *:* 1204 svchost.exe 2015-09-03 06:08:37 UTC+0000
0x3ee8040 UDPv4 0.0.0.0 *:* 1176 svchost.exe 2015-08-23 10:30:48 UTC+0000
0x3ee99a0 UDPv4 0.0.0.0:62184 *:* 1108 svchost.exe 2015-09-03 10:03:20 UTC+0000
0x3ef3380 UDPv4 0.0.0.0:3702 *:* 1108 svchost.exe 2015-09-03 10:03:20 UTC+0000
0x3ef3380 UDPv6 :::3702 *:* 1108 svchost.exe 2015-09-03 10:03:20 UTC+0000
0x3ef5260 UDPv4 0.0.0.0:62185 *:* 1108 svchost.exe 2015-09-03 10:03:20 UTC+0000
0x3ef5260 UDPv6 :::62185 *:* 1108 svchost.exe 2015-09-03 10:03:20 UTC+0000
0x3ef7100 UDPv4 192.168.56.101:138 *:* 4 System 2015-09-03 06:08:35 UTC+0000
0x3f1e1438 UDPv4 192.168.56.101:137 *:* 4 System 2015-09-03 06:08:35 UTC+0000
0x3f1e6308 UDPv4 0.0.0.0 *:* 836 VBoxService.exe 2015-09-03 10:04:08 UTC+0000
0x3efccbe8 TCPv4 0.0.0.0:80 0.0.0.0 LISTENING 2796 httpd.exe
0x3efccbe8 TCPv6 :::80 *:* LISTENING 2796 httpd.exe
0x3efcd008 TCPv4 0.0.0.0:443 0.0.0.0 LISTENING 2796 httpd.exe
0x3efcd008 TCPv6 0.0.0.0:443 0.0.0.0 LISTENING 2796 httpd.exe
0x3efcd008 TCPv6 :::443 *:* LISTENING 2796 httpd.exe
0x3efcd008 TCPv4 0.0.0.0:80 0.0.0.0 LISTENING 2796 httpd.exe
0x3f1f6320 TCPv4 0.0.0.0:49157 0.0.0.0 LISTENING 608 services.exe
0x3f1f9320 TCPv4 0.0.0.0:49157 0.0.0.0 LISTENING 608 services.exe
0x3f1f9320 TCPv6 :::49157 *:* LISTENING 608 services.exe
0x3f81c18 TCPv6 fe80::3816:d72e:759b:70b9:3306::f02::1:3:51128 CLOSED 2804 mysqld.exe
0x3f250678 UDPv4 0.0.0.0:500 *:* 1024 svchost.exe 2015-08-23 10:30:05 UTC+0000
0x3f26c508 UDPv4 0.0.0.0:4500 *:* 1024 svchost.exe 2015-08-23 10:30:05 UTC+0000
0x3f26d960 UDPv4 0.0.0.0:5355 *:* 1204 svchost.exe 2015-09-03 06:08:37 UTC+0000
0x3f28e2a0 UDPv4 0.0.0.0:500 *:* 1024 svchost.exe 2015-08-23 10:30:05 UTC+0000
0x3f28e2a0 UDPv6 :::500 *:* 1024 svchost.exe 2015-08-23 10:30:05 UTC+0000
0x3f2e3108 UDPv4 0.0.0.0 *:* 1024 svchost.exe 2015-08-23 10:30:05 UTC+0000
0x3f2e3108 UDPv6 :::0 *:* 1024 svchost.exe 2015-08-23 10:30:05 UTC+0000
0x3f2ead98 UDPv4 0.0.0.0 *:* 1024 svchost.exe 2015-08-23 10:30:05 UTC+0000
0x3f2f4908 UDPv4 0.0.0.0:55813 *:* 1204 svchost.exe 2015-09-03 10:03:55 UTC+0000
0x3f2fc9f0 UDPv4 0.0.0.0 *:* 1108 svchost.exe 2015-08-23 10:30:05 UTC+0000
0x3f2fc9f0 UDPv6 :::0 *:* 1556 svchost.exe 2015-08-23 10:30:05 UTC+0000
0x3f2fe070 UDPv4 0.0.0.0 *:* 1556 svchost.exe 2015-08-23 10:30:05 UTC+0000
0x3f2ff280 UDPv4 0.0.0.0 *:* 1108 svchost.exe 2015-08-23 10:30:05 UTC+0000
0x3f300e40 UDPv4 0.0.0.0 *:* 1108 svchost.exe 2015-08-23 10:30:05 UTC+0000
0x3f300e40 UDPv6 :::0 *:* 1108 svchost.exe 2015-08-23 10:30:05 UTC+0000
0x3f3258d8 UDPv4 127.0.0.1:57557 *:* 1204 svchost.exe 2015-08-23 10:30:07 UTC+0000
0x3f552990 UDPv4 0.0.0.0:3702 *:* 1108 svchost.exe 2015-09-03 10:03:20 UTC+0000
0x3f552990 UDPv6 :::3702 *:* 1108 svchost.exe 2015-09-03 10:03:20 UTC+0000
0x3f593330 UDPv4 0.0.0.0:3702 *:* 1108 svchost.exe 2015-09-03 10:03:20 UTC+0000
0x3f9a1948 UDPv4 0.0.0.0 *:* 1204 svchost.exe 2015-09-03 06:08:37 UTC+0000
0x3f9a1948 UDPv6 :::0 *:* 1204 svchost.exe 2015-09-03 06:08:37 UTC+0000
0x3f204188 TCPv4 0.0.0.0:49153 0.0.0.0 LISTENING 984 svchost.exe
0x3f204188 TCPv6 :::49153 *:* LISTENING 984 svchost.exe
0x3f260b78 TCPv4 0.0.0.0:49154 0.0.0.0 LISTENING 620 lsass.exe
0x3f260b78 TCPv6 :::49154 *:* LISTENING 620 lsass.exe
0x3f260f08 TCPv4 0.0.0.0:49154 0.0.0.0 LISTENING 620 lsass.exe
0x3f260f08 TCPv6 0.0.0.0:49154 0.0.0.0 LISTENING 1556 svchost.exe
0x3f303cc8 TCPv4 0.0.0.0:49156 0.0.0.0 LISTENING 1556 svchost.exe
0x3f303cc8 TCPv6 :::49156 *:* LISTENING 1556 svchost.exe
0x3f321c60 TCPv4 0.0.0.0:445 0.0.0.0 LISTENING 4 System

```

0x3f31c60	TCPv4	0.0.0.0:445	0.0.0.0:0	LISTENING	4	System
0x3f31c60	TCPv6	:::445	:::0	LISTENING	4	System
0x3f495a30	TCPv6	:::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
0x3f5e6088	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
0x3f5f5e30	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
0x3f5fdd08	TCPv4	0.0.0.0:49152	0.0.0.0:0	LISTENING	532	wininit.exe
0x3f5fdd08	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
0x3ff04008	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

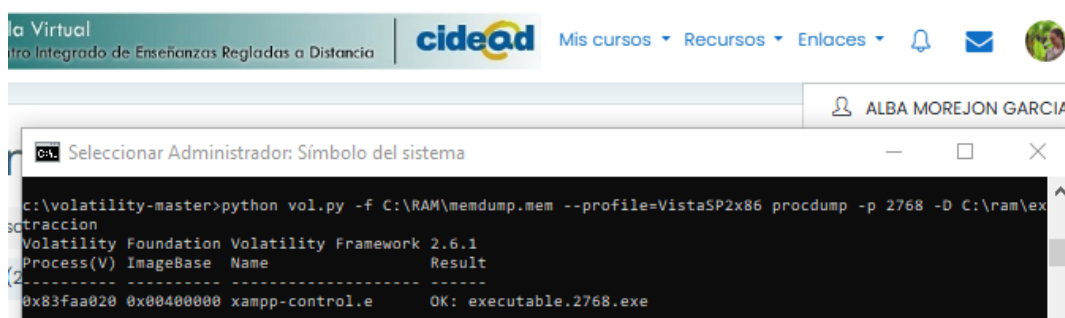
- Conexión establecida a través del puerto 5357 (servicio web for devices)

192.168.56.101:51157 a 192.168.56.1:5357

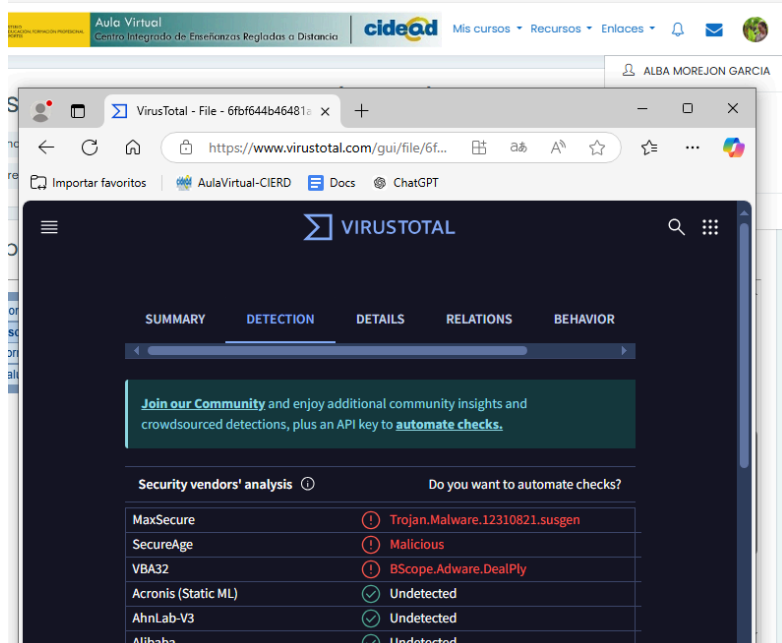
- El proceso svchost.exe se esta ejecutando de manera repetida en los puertos UDP 3702, 5355, 500, 4500 y TCP entre 49152 y 49157
- EL proceso VBoxService tiene una creación tardía en comparación con otros procesos

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”

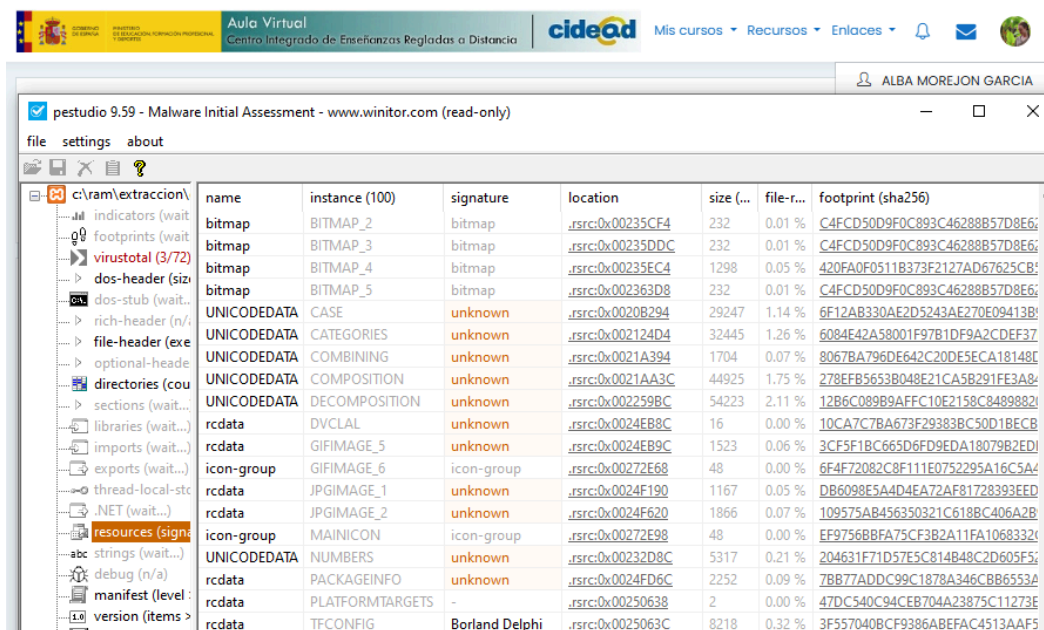


Se crea el archivo “executable.2768.exe”



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.

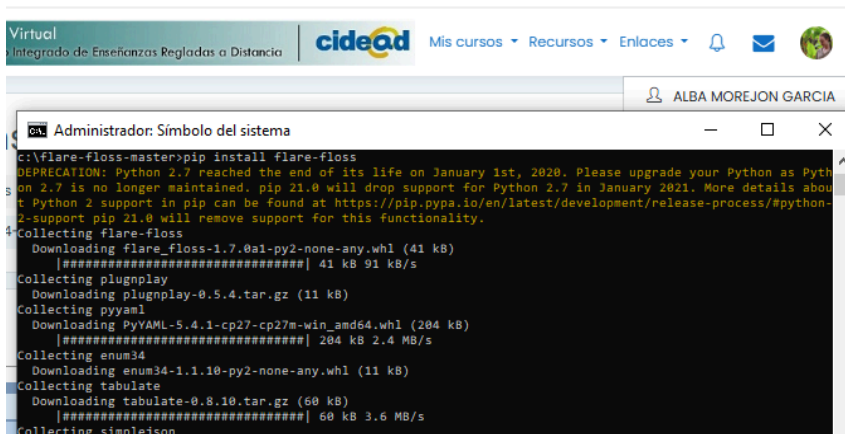


Algunos resultados que hemos obtenido con los datos de esta aplicación:

Los datos de recursos 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.dll, 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 están intentando inyectar código en otros procesos.

Las cadenas relacionadas con xampp_control podrían indicar que el malware se disfraza como software legítimo (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)

Virtual Integrado de Enseñanzas Regladas a Distancia | cidead Mis cursos Recursos Enlaces ALBA MOREJON GARCIA

```
ca. Administrador: Símbolo del sistema
c:\volatility-master>floss --version
Traceback (most recent call last):
  File "c:\python27\lib\runpy.py", line 174, in _run_module_as_main
    "__main__", fname, loader, pkg_name)
  File "c:\python27\lib\runpy.py", line 72, in _run_code
    exec code in run_globals
  File "C:\Python27\Scripts\floss.exe\__main__.py", line 4, in <module>
  File "c:\python27\lib\site-packages\floss\main.py", line 17, in <module>
    import viv_utils
  File "c:\python27\lib\site-packages\viv_utils\__init__.py", line 10, in <module>
    import funcy
  File "c:\python27\lib\site-packages\funcy\__init__.py", line 3, in <module>
    from .calc import *
  File "c:\python27\lib\site-packages\funcy\calc.py", line 19
    def memoize(_func=None, *, key_func=None):
                                ^
SyntaxError: invalid syntax
```

Virtual Integrado de Enseñanzas Regladas a Distancia | cidead Mis cursos Recursos Enlaces ALBA MOREJON GARCIA

```
ca. Administrador: Símbolo del sistema
c:\volatility-master>pip list
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python as Pyt
hon 2.7 is no longer maintained. pip 21.0 will drop support for Python 2.7 in January 2021. More details ab
out Python 2 support in pip can be found at https://pip.pypa.io/en/latest/development/release-process/#pyth
on-2-support pip 21.0 will remove support for this functionality.
Package            Version
-----
cxxfilt            0.2.1
distorm3           3.5.2
enum34             1.1.10
et-xmlfile         1.0.1
flare-floss        1.7.0a1
funcy              2.0
future             1.0.0
intervaltree       3.1.0
jdcal              1.4.1
msgpack            1.0.0
openpyxl           2.6.4
pefile             2019.4.18
Pillow             6.2.2
pip               20.3.4
pluginplay         0.5.4
pyasn1             0.4.5
pyasn1-modules     0.2.4
pycparser          2.20
pycrypto           2.6.1
PyYAML             5.4.1
setuptools         41.2.0
simplejson          3.19.3
sortedcontainers   2.4.0
tabulate           0.8.10
tjson              1.35
viv-utils          0.3.17
vivisect           0.1.0
volatility          2.6.1
yara-python        3.8.1
```


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 análisis 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 (OpenThreadToken, 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.