Análise Forense Digital e a Inteligência de Ameaças Cibernéticas

MÓDULO 4 | Forense em sistemas Linux

NOME: Gonçalo João Santos Silva
N.º DE ESTUDANTE: 2000499
DATA DE ENTREGA: 13/10/2025

1- **Identificação do Perfil da Imagem de Memória (3 pontos):** determinar o perfil correto usando ferramentas adequadas.

Para iniciar esta análise, utilizei a minha máquina virtual com o sistema Kali Linux, que já tinha previamente configurado com o Volatility 2.6. No terminal, naveguei até à pasta onde se encontrava o ficheiro E-atividade.raw, localizado no ambiente de trabalho, e executei o comando do Volatility através do Python 2. Como o ambiente já estava preparado e o Volatility corretamente instalado, o processo foi rápido e direto.

python2 ~/volatility/vol.py -f ~/Desktop/E-atividade.raw imageinfo

- python2 - usa o interpretador Python (necessário para o Volatility).
- ~/volatility/vol.py - é o ficheiro principal do Volatility.
- -f ~/Desktop/E-atividade.raw - caminho da imagem de memória.
- imageinfo - o plugin que identifica o perfil correto da imagem.

Este comando permite-me identificar o perfil correto da imagem de memória. O Volatility faz isto analisando as estruturas internas (como o KDBG) e apresenta uma lista de perfis possíveis.

O resultado que obtive foi o seguinte:

Entre os perfis sugeridos, escolhi Win7SP1x64, por ser o primeiro da lista e o mais provável, já que corresponde a um sistema Windows 7 Service Pack 1 (64 bits), o que é consistente com o tipo de imagem utilizado.

2- Listagem de Processos Ativos (3 pontos): identificar todos os processos ativos na captura, destacando os suspeitos.

Para identificar os processos ativos na imagem de memória, utilizei o comando:

python2 ~/volatility/vol.py -f ~/Desktop/E-atividade.raw --profile=Win7SP1x64 pslist

- python2 - usa o interpretador Python (necessário para o Volatility).
- ~/volatility/vol.py - é o ficheiro principal do Volatility.
- -f ~/Desktop/E-atividade.raw - caminho da imagem de memória.
- --profile=Win7SP1x64- Indica o perfil que o Volatility deve usar para interpretar a estrutura da memória (KDBG, tabelas, offsets, etc.).
- Pslist - plugin que lista os processos presentes na lista de processos do kernel no momento da captura.

O resultado que obtive foi o seguinte:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ python2 ~/volatility/vol.py -f ~/Desktop/E-atividade.raw --profile=Win7SP1x64 pslist

Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xfffffa8000ca0040 System                    4      0     80      570 ------      0 2019-12-11 13:41:25 UTC+0000
0xfffffa800148f040 smss.exe                248      4      3       37 ------      0 2019-12-11 13:41:25 UTC+0000
0xfffffa800154f740 csrss.exe               320    312      9      457      0      0 2019-12-11 13:41:32 UTC+0000
0xfffffa8000ca81e0 csrss.exe               368    360      7      199      1      0 2019-12-11 13:41:33 UTC+0000
0xfffffa8001c45060 psxss.exe               376    248     18      786      0      0 2019-12-11 13:41:33 UTC+0000
0xfffffa8001c5f060 winlogon.exe            416    360      4      118      1      0 2019-12-11 13:41:34 UTC+0000
0xfffffa8001c5f630 wininit.exe             424    312      3       75      0      0 2019-12-11 13:41:34 UTC+0000
0xfffffa8001c98530 services.exe            484    424     13      219      0      0 2019-12-11 13:41:35 UTC+0000
0xfffffa8001ca0580 lsass.exe               492    424      9      764      0      0 2019-12-11 13:41:35 UTC+0000
0xfffffa8001ca4b30 lsm.exe                 500    424     11      185      0      0 2019-12-11 13:41:35 UTC+0000
0xfffffa8001cf4b30 svchost.exe             588    484     11      358      0      0 2019-12-11 13:41:39 UTC+0000
0xfffffa8001d327c0 VBoxService.ex          652    484     13      137      0      0 2019-12-11 13:41:40 UTC+0000
0xfffffa8001d49b30 svchost.exe             720    484      8      279      0      0 2019-12-11 13:41:41 UTC+0000
0xfffffa8001d8c420 svchost.exe             816    484     23      569      0      0 2019-12-11 13:41:42 UTC+0000
0xfffffa8001da5b30 svchost.exe             852    484     28      542      0      0 2019-12-11 13:41:43 UTC+0000
0xfffffa8001da96c0 svchost.exe             876    484     32      941      0      0 2019-12-11 13:41:43 UTC+0000
0xfffffa8001e1bb30 svchost.exe             472    484     19      476      0      0 2019-12-11 13:41:47 UTC+0000
0xfffffa8001e50b30 svchost.exe            1044    484     14      366      0      0 2019-12-11 13:41:48 UTC+0000
0xfffffa8001eba230 spoolsv.exe            1208    484     13      282      0      0 2019-12-11 13:41:51 UTC+0000
0xfffffa8001eda060 svchost.exe            1248    484     19      313      0      0 2019-12-11 13:41:52 UTC+0000
0xfffffa8001f58890 svchost.exe            1372    484     22      295      0      0 2019-12-11 13:41:54 UTC+0000
0xfffffa8001f91b30 TCPSVCS.EXE            1416    484      4       97      0      0 2019-12-11 13:41:55 UTC+0000
0xfffffa8000d3c400 sppsvc.exe             1508    484      4      141      0      0 2019-12-11 14:16:06 UTC+0000
0xfffffa8001c38580 svchost.exe             948    484     13      322      0      0 2019-12-11 14:16:07 UTC+0000
0xfffffa8002170630 wmpnetwk.exe           1856    484     16      451      0      0 2019-12-11 14:16:08 UTC+0000
0xfffffa8001d376f0 SearchIndexer.          480    484     14      701      0      0 2019-12-11 14:16:09 UTC+0000
0xfffffa8001eb47f0 taskhost.exe            296    484      8      151      1      0 2019-12-11 14:32:24 UTC+0000
0xfffffa8001dfa910 dwm.exe                1988    852      5       72      1      0 2019-12-11 14:32:25 UTC+0000
0xfffffa8002046960 explorer.exe            604   2016     33      927      1      0 2019-12-11 14:32:25 UTC+0000
0xfffffa80021c75d0 VBoxTray.exe           1844    604     11      140      1      0 2019-12-11 14:32:35 UTC+0000
0xfffffa80021da060 audiodg.exe            2064    816      6      131      0      0 2019-12-11 14:32:37 UTC+0000
0xfffffa80022199e0 svchost.exe            2368    484      9      365      0      0 2019-12-11 14:32:51 UTC+0000
0xfffffa8002222780 cmd.exe                1984    604      1       21      1      0 2019-12-11 14:34:54 UTC+0000
0xfffffa8002227140 conhost.exe            2692    368      2       50      1      0 2019-12-11 14:34:54 UTC+0000
0xfffffa80022bab30 mspaint.exe            2424    604      6      128      1      0 2019-12-11 14:35:14 UTC+0000
0xfffffa8000eac770 svchost.exe            2660    484      6      100      0      0 2019-12-11 14:35:14 UTC+0000
0xfffffa8001e68060 csrss.exe              2760   2680      7      172      2      0 2019-12-11 14:37:05 UTC+0000
0xfffffa8000ecbb30 winlogon.exe           2808   2680      4      119      2      0 2019-12-11 14:37:05 UTC+0000
0xfffffa8000f3aab0 taskhost.exe           2908    484      9      158      2      0 2019-12-11 14:37:13 UTC+0000
0xfffffa8000f4db30 dwm.exe                3004    852      5       72      2      0 2019-12-11 14:37:14 UTC+0000
0xfffffa8000f4c670 explorer.exe           2504   3000     34      825      2      0 2019-12-11 14:37:14 UTC+0000
0xfffffa8000f9a4e0 VBoxTray.exe           2304   2504     14      144      2      0 2019-12-11 14:37:14 UTC+0000
0xfffffa8000fff630 SearchProtocol         2524    480      7      226      2      0 2019-12-11 14:37:21 UTC+0000
0xfffffa8000ecea60 SearchFilterHo         1720    480      5       90      0      0 2019-12-11 14:37:21 UTC+0000
0xfffffa8001010b30 WinRAR.exe             1512   2504      6      207      2      0 2019-12-11 14:37:23 UTC+0000
0xfffffa8001020b30 SearchProtocol         2868    480      8      279      0      0 2019-12-11 14:37:23 UTC+0000
0xfffffa8001048060 DumpIt.exe              796    604      2       45      1      1 2019-12-11 14:37:54 UTC+0000
0xfffffa800104a780 conhost.exe            2260    368      2       50      1      0 2019-12-11 14:37:54 UTC+0000
```

Resultados obtidos:

O comando devolveu a lista completa de processos que estavam em execução na altura da captura. Entre os processos normais e esperados aparecem System, smss.exe, csrss.exe, wininit.exe, services.exe e lsass.exe. Também aparecem processos do ambiente de virtualização (VBoxService.exe, VBoxTray.exe) e aplicações típicas (explorer.exe, dwm.exe, SearchIndexer, audiodg.exe).

Destaco os processos que me chamaram a atenção e que vou investigar a seguir:

- **DumpIt.exe (PID 796)** — aplicação legítima usada para criar dumps de memória. Explica a existência do ficheiro de análise. Vou registar este PID porque pode indicar quem gerou o dump.
- **cmd.exe (PID 1984)** e respetivo conhost.exe — consola interactiva. É importante extrair o histórico de comandos para ver o que foi corrido.
- **WinRAR.exe (PID 1512)** — aplicação de compressão; pode ter sido usada para empacotar ou mover ficheiros.
- **mspaint.exe** — processo pouco relevante por si, mas interessante verificar se gerou ficheiros.
- **svchost.exe (vários PIDs)** — comportamento normal no Windows, mas vou analisar DLLs por PID caso haja indícios de anomalia.

O sistema parece um Windows 7 SP1 a correr numa VM. A presença do DumpIt.exe indica que alguém fez um dump da memória (ou a ferramenta foi usada para esse fim). Os PIDs referidos (796, 1984, 1512) são os que vou seguir nas próximas análises para confirmar se houve atividade maliciosa ou operações de exfiltração/compactação.

Para isso extrai o histórico de consola e do cmdscan através dos comandos que me guardou um txt no ambiente de trabalho.

cp ~/Desktop/consoles.txt ~/Desktop/Eatividade_results/consoles.txt

cp ~/Desktop/cmdscan.txt ~/Desktop/Eatividade_results/cmdscan.txt

```
**************************************************
ConsoleProcess: conhost.exe Pid: 2692
Console: 0×ff756200 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: %SystemRoot%\system32\cmd.exe
Title: C:\Windows\system32\cmd.exe - St4G3$1
AttachedProcess: cmd.exe Pid: 1984 Handle: 0×60
----
CommandHistory: 0×1fe9c0 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0×60
Cmd #0 at 0×1de3c0: St4G3$1
----
Screen 0×1e0f70 X:80 Y:300
Dump:
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\SmartNet>St4G3$1
ZmxhZ3t0aDFzXzFzX3RoM18xc3Rfc3Q0ZzMhIX0=
Press any key to continue . . .
**************************************************
ConsoleProcess: conhost.exe Pid: 2260
Console: 0×ff756200 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: C:\Users\SmartNet\Downloads\DumpIt\DumpIt.exe
Title: C:\Users\SmartNet\Downloads\DumpIt\DumpIt.exe
AttachedProcess: DumpIt.exe Pid: 796 Handle: 0×60
----
CommandHistory: 0×38ea90 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0×60
----
Screen 0×371050 X:80 Y:300
Dump:
  DumpIt - v1.3.2.20110401 - One click memory memory dumper
  Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
  Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>


    Address space size:        1073676288 bytes (   1023 Mb)
    Free space size:          24185389056 bytes (  23064 Mb)

    * Destination = \??\C:\Users\SmartNet\Downloads\DumpIt\SMARTNET-PC-20191211-
143755.raw

    --> Are you sure you want to continue? [y/n] y
    + Processing...

```

consoles.txt

```
**************************************************
CommandProcess: conhost.exe Pid: 2692
CommandHistory: 0×1fe9c0 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0×60
Cmd #0 @ 0×1de3c0: St4G3$1
Cmd #15 @ 0×1c0158: 00 1f
Cmd #16 @ 0×1fdb30: 00 1f
**************************************************
CommandProcess: conhost.exe Pid: 2260
CommandHistory: 0×38ea90 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0×60
Cmd #15 @ 0×350158: 8
Cmd #16 @ 0×38dc00: 8

```

cmdscan.txt

Nos resultados do consoles.txt e cmdscan.txt, encontrei um único comando executado no cmd.exe (PID 1984):

St4G3$1

Logo abaixo, a consola mostrava uma string codificada em Base64:

ZmxhZ3t0aDFzXzFzX3RoM18xc3Rfc3Q0ZzMhIX0=

Para verificar o que continha, fiz a decodificação com:

echo 'ZmxhZ3t0aDFzXzFzX3RoM18xc3Rfc3Q0ZzMhIX0=' | base64 -d

O resultado foi:

flag{th1s_1s_th3_1st_st4g3!!}

Isto confirma que o comando executado na consola devolvia a primeira flag do desafio, codificada em Base64.
Em paralelo, o DumpIt.exe (PID 796) estava a correr e criou o ficheiro:

C:\Users\SmartNet\Downloads\DumpIt\SMARTNET-PC-20191211-143755.raw

Tudo indica que o utilizador executou manualmente o comando St4G3$1, obteve a flag e logo a seguir criou o dump de memória.

Procura de Processos Ocultos (psscan e psxview)

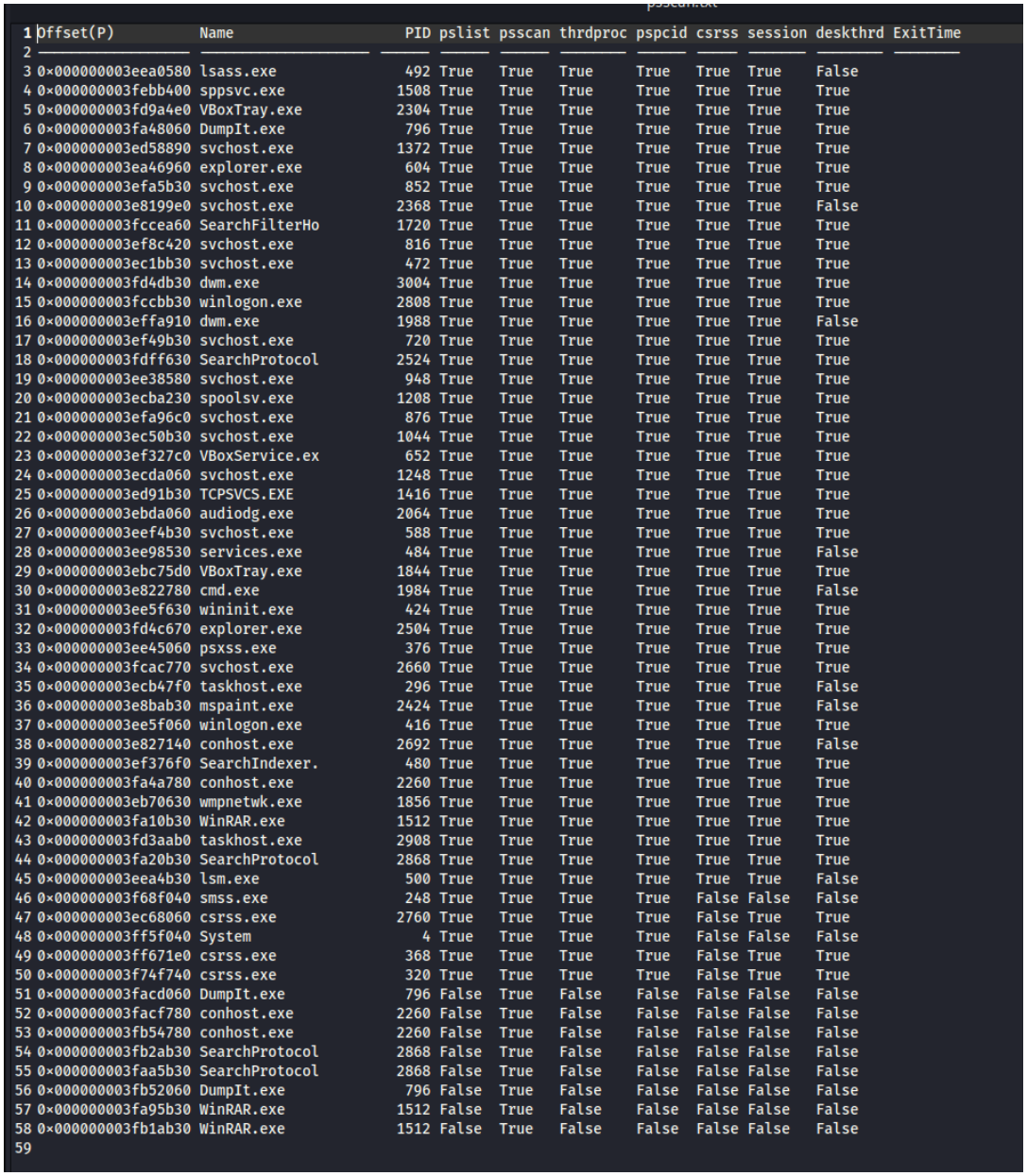
Depois de identificar os processos ativos, quis confirmar se não existiam processos ocultos ou anómalos.
Para isso usei os comandos:

```
python2 ~/volatility/vol.py -f ~/Desktop/E-atividade.raw --profile=Win7SP1x64 psscan > ~/Desktop/Eatividade_results/psscan.txt
```

```
python2 ~/volatility/vol.py -f ~/Desktop/E-atividade.raw --profile=Win7SP1x64 psxview > ~/Desktop/Eatividade_results/psxview.txt
```

Offset(P)	Name	PID	PPID	PDB	Time created	Time exited
0x000000003e8199e0	svchost.exe	2368	484	0x000000002f8cf000	2019-12-11 14:32:51 UTC+0000	
0x000000003e822780	cmd.exe	1984	604	0x000000002457b000	2019-12-11 14:34:54 UTC+0000	
0x000000003e827140	conhost.exe	2692	368	0x0000000023e17000	2019-12-11 14:34:54 UTC+0000	
0x000000003e8bab30	mspaint.exe	2424	604	0x000000003a581000	2019-12-11 14:35:14 UTC+0000	
0x000000003ea46960	explorer.exe	604	2016	0x0000000035a79000	2019-12-11 14:32:25 UTC+0000	
0x000000003eb70630	wmpnetwk.exe	1856	484	0x000000000e83e000	2019-12-11 14:16:08 UTC+0000	
0x000000003ebc75d0	VBoxTray.exe	1844	604	0x0000000034c66000	2019-12-11 14:32:35 UTC+0000	
0x000000003ebda060	audiodg.exe	2064	816	0x000000003218c000	2019-12-11 14:32:37 UTC+0000	
0x000000003ec1bb30	svchost.exe	472	484	0x000000001aa76000	2019-12-11 13:41:47 UTC+0000	
0x000000003ec50b30	svchost.exe	1044	484	0x000000001a6be000	2019-12-11 13:41:48 UTC+0000	
0x000000003ec68060	csrss.exe	2760	2680	0x000000001b94e000	2019-12-11 14:37:05 UTC+0000	
0x000000003ecb47f0	taskhost.exe	296	484	0x0000000036347000	2019-12-11 14:32:24 UTC+0000	
0x000000003ecba230	spoolsv.exe	1208	484	0x00000000177ce000	2019-12-11 13:41:51 UTC+0000	
0x000000003ecda060	svchost.exe	1248	484	0x000000001729c000	2019-12-11 13:41:52 UTC+0000	
0x000000003ed58890	svchost.exe	1372	484	0x0000000013f1b000	2019-12-11 13:41:54 UTC+0000	
0x000000003ed91b30	TCPSVCS.EXE	1416	484	0x00000000098c0000	2019-12-11 13:41:55 UTC+0000	
0x000000003ee38580	svchost.exe	948	484	0x000000000eab3000	2019-12-11 14:16:07 UTC+0000	
0x000000003ee45060	psxss.exe	376	248	0x000000001f70a000	2019-12-11 13:41:33 UTC+0000	
0x000000003ee5f060	winlogon.exe	416	360	0x000000001f20c000	2019-12-11 13:41:34 UTC+0000	
0x000000003ee5f630	wininit.exe	424	312	0x000000001f079000	2019-12-11 13:41:34 UTC+0000	
0x000000003ee98530	services.exe	484	424	0x000000001e531000	2019-12-11 13:41:35 UTC+0000	
0x000000003eea0580	lsass.exe	492	424	0x000000001e3d2000	2019-12-11 13:41:35 UTC+0000	
0x000000003eea4b30	lsm.exe	500	424	0x000000001e55a000	2019-12-11 13:41:35 UTC+0000	
0x000000003eef4b30	svchost.exe	588	484	0x000000001d4f4000	2019-12-11 13:41:39 UTC+0000	
0x000000003ef327c0	VBoxService.ex	652	484	0x000000001d0dc000	2019-12-11 13:41:40 UTC+0000	
0x000000003ef376f0	SearchIndexer.	480	484	0x000000000dc08000	2019-12-11 14:16:09 UTC+0000	
0x000000003ef49b30	svchost.exe	720	484	0x000000001cdac000	2019-12-11 13:41:41 UTC+0000	
0x000000003ef8c420	svchost.exe	816	484	0x000000001c795000	2019-12-11 13:41:42 UTC+0000	
0x000000003efa5b30	svchost.exe	852	484	0x000000001bfde000	2019-12-11 13:41:43 UTC+0000	
0x000000003efa96c0	svchost.exe	876	484	0x000000001c0e4000	2019-12-11 13:41:43 UTC+0000	
0x000000003effa910	dwm.exe	1988	852	0x000000000360d7000	2019-12-11 14:32:25 UTC+0000	
0x000000003f68f040	smss.exe	248	4	0x0000000261ec000	2019-12-11 13:41:25 UTC+0000	
0x000000003f74f740	csrss.exe	320	312	0x000000001fcb3000	2019-12-11 13:41:32 UTC+0000	
0x000000003fa10b30	WinRAR.exe	1512	2504	0x0000000019835000	2019-12-11 14:37:23 UTC+0000	
0x000000003fa20b30	SearchProtocol	2868	480	0x0000000017b1b000	2019-12-11 14:37:23 UTC+0000	
0x000000003fa48060	DumpIt.exe	796	604	0x0000000143d6000	2019-12-11 14:37:54 UTC+0000	
0x000000003fa4a780	conhost.exe	2260	368	0x0000000012d9b000	2019-12-11 14:37:54 UTC+0000	
0x000000003fa95b30	WinRAR.exe	1512	2504	0x0000000019835000	2019-12-11 14:37:23 UTC+0000	
0x000000003faa5b30	SearchProtocol	2868	480	0x0000000017b1b000	2019-12-11 14:37:23 UTC+0000	
0x000000003facd060	DumpIt.exe	796	604	0x0000000143d6000	2019-12-11 14:37:54 UTC+0000	
0x000000003facf780	conhost.exe	2260	368	0x0000000012d9b000	2019-12-11 14:37:54 UTC+0000	
0x000000003fb1ab30	WinRAR.exe	1512	2504	0x0000000019835000	2019-12-11 14:37:23 UTC+0000	
0x000000003fb2ab30	SearchProtocol	2868	480	0x0000000017b1b000	2019-12-11 14:37:23 UTC+0000	
0x000000003fb52060	DumpIt.exe	796	604	0x0000000143d6000	2019-12-11 14:37:54 UTC+0000	
0x000000003fb54780	conhost.exe	2260	368	0x0000000012d9b000	2019-12-11 14:37:54 UTC+0000	
0x000000003fcac770	svchost.exe	2660	484	0x0000000001d2e000	2019-12-11 14:35:14 UTC+0000	
0x000000003fccbb30	winlogon.exe	2808	2680	0x0000000261d3000	2019-12-11 14:37:05 UTC+0000	
0x000000003fccea60	SearchFilterHo	1720	480	0x0000000019b05000	2019-12-11 14:37:21 UTC+0000	
0x000000003fd3aab0	taskhost.exe	2908	484	0x000000000b291000	2019-12-11 14:37:13 UTC+0000	
0x000000003fd4c670	explorer.exe	2504	3000	0x0000000008771000	2019-12-11 14:37:14 UTC+0000	
0x000000003fd4db30	dwm.exe	3004	852	0x0000000016de7000	2019-12-11 14:37:14 UTC+0000	
0x000000003fd9a4e0	VBoxTray.exe	2304	2504	0x0000000007a54000	2019-12-11 14:37:14 UTC+0000	
0x000000003fdff630	SearchProtocol	2524	480	0x0000000037d69000	2019-12-11 14:37:21 UTC+0000	
0x000000003febb400	sppsvc.exe	1508	484	0x000000000f4ee000	2019-12-11 14:16:06 UTC+0000	
0x000000003ff5f040	System	4	0	0x0000000000187000	2019-12-11 13:41:25 UTC+0000	
0x000000003ff671e0	csrss.exe	368	360	0x000000003bd46000	2019-12-11 13:41:33 UTC+0000	

psscan.txt



Offset(P)	Name	PID	pslist	psscan	thrdproc	pspcid	csrss	session	deskthrd	ExitTime
0x000000003eea0580	lsass.exe	492	True	True	True	True	True	True	False	
0x000000003febb400	sppsvc.exe	1508	True	True	True	True	True	True	True	
0x000000003fd9a4e0	VBoxTray.exe	2304	True	True	True	True	True	True	True	
0x000000003fa48060	DumpIt.exe	796	True	True	True	True	True	True	True	
0x000000003ed58890	svchost.exe	1372	True	True	True	True	True	True	True	
0x000000003ea46960	explorer.exe	604	True	True	True	True	True	True	True	
0x000000003efa5b30	svchost.exe	852	True	True	True	True	True	True	True	
0x000000003e8199e0	svchost.exe	2368	True	True	True	True	True	True	False	
0x000000003fccea60	SearchFilterHo	1720	True	True	True	True	True	True	True	
0x000000003ef8c420	svchost.exe	816	True	True	True	True	True	True	True	
0x000000003ec1bb30	svchost.exe	472	True	True	True	True	True	True	True	
0x000000003fd4db30	dwm.exe	3004	True	True	True	True	True	True	True	
0x000000003fccbb30	winlogon.exe	2808	True	True	True	True	True	True	True	
0x000000003effa910	dwm.exe	1988	True	True	True	True	True	True	False	
0x000000003ef49b30	svchost.exe	720	True	True	True	True	True	True	True	
0x000000003fdff630	SearchProtocol	2524	True	True	True	True	True	True	True	
0x000000003ee38580	svchost.exe	948	True	True	True	True	True	True	True	
0x000000003ecba230	spoolsv.exe	1208	True	True	True	True	True	True	True	
0x000000003efa96c0	svchost.exe	876	True	True	True	True	True	True	True	
0x000000003ec50b30	svchost.exe	1044	True	True	True	True	True	True	True	
0x000000003ef327c0	VBoxService.ex	652	True	True	True	True	True	True	True	
0x000000003ecda060	svchost.exe	1248	True	True	True	True	True	True	True	
0x000000003ed91b30	TCPSVCS.EXE	1416	True	True	True	True	True	True	True	
0x000000003ebda060	audiodg.exe	2064	True	True	True	True	True	True	True	
0x000000003eef4b30	svchost.exe	588	True	True	True	True	True	True	True	
0x000000003ee98530	services.exe	484	True	True	True	True	True	True	False	
0x000000003ebc75d0	VBoxTray.exe	1844	True	True	True	True	True	True	True	
0x000000003e822780	cmd.exe	1984	True	True	True	True	True	True	False	
0x000000003ee5f630	wininit.exe	424	True	True	True	True	True	True	True	
0x000000003fd4c670	explorer.exe	2504	True	True	True	True	True	True	True	
0x000000003ee45060	psxss.exe	376	True	True	True	True	True	True	True	
0x000000003fcac770	svchost.exe	2660	True	True	True	True	True	True	True	
0x000000003ecb47f0	taskhost.exe	296	True	True	True	True	True	True	False	
0x000000003e8bab30	mspaint.exe	2424	True	True	True	True	True	True	False	
0x000000003ee5f060	winlogon.exe	416	True	True	True	True	True	True	True	
0x000000003e827140	conhost.exe	2692	True	True	True	True	True	True	False	
0x000000003ef376f0	SearchIndexer.	480	True	True	True	True	True	True	True	
0x000000003fa4a780	conhost.exe	2260	True	True	True	True	True	True	True	
0x000000003eb70630	wmpnetwk.exe	1856	True	True	True	True	True	True	True	
0x000000003fa10b30	WinRAR.exe	1512	True	True	True	True	True	True	True	
0x000000003fd3aab0	taskhost.exe	2908	True	True	True	True	True	True	True	
0x000000003fa20b30	SearchProtocol	2868	True	True	True	True	True	True	True	
0x000000003eea4b30	lsm.exe	500	True	True	True	True	True	True	False	
0x000000003f68f040	smss.exe	248	True	True	True	True	False	False	False	
0x000000003ec68060	csrss.exe	2760	True	True	True	True	False	True	True	
0x000000003ff5f040	System	4	True	True	True	True	False	False	False	
0x000000003ff671e0	csrss.exe	368	True	True	True	True	False	True	True	
0x000000003f74f740	csrss.exe	320	True	True	True	True	False	True	True	
0x000000003facd060	DumpIt.exe	796	False	True	False	False	False	False	False	
0x000000003facf780	conhost.exe	2260	False	True	False	False	False	False	False	
0x000000003fb54780	conhost.exe	2260	False	True	False	False	False	False	False	
0x000000003fb2ab30	SearchProtocol	2868	False	True	False	False	False	False	False	
0x000000003faa5b30	SearchProtocol	2868	False	True	False	False	False	False	False	
0x000000003fb52060	DumpIt.exe	796	False	True	False	False	False	False	False	
0x000000003fa95b30	WinRAR.exe	1512	False	True	False	False	False	False	False	
0x000000003fb1ab30	WinRAR.exe	1512	False	True	False	False	False	False	False	

psxview.txt

O **psscan** serve para procurar diretamente na memória estruturas de processos (EPROCESS), incluindo processos que já terminaram, e o **psxview** compara diferentes métodos de deteção para identificar possíveis ocultações.

A análise mostrou vários processos adicionais no psscan, nomeadamente:

- **DumpIt.exe (PID 796)**
- **WinRAR.exe (PID 1512)**
- **conhost.exe (PID 2260)**
- **SearchProtocolHost (PID 2868)**

Estes não aparecem em pslist, o que indica que **foram terminados pouco antes da captura**, deixando apenas as estruturas residuais em memória.
No psxview, estes mesmos PIDs aparecem com pslist=False e psscan=True, confirmando que não estavam ativos, mas também que **não há sinais de ocultação** (os campos ExitTime e thrdproc mostram comportamento normal).

Verificando os horários de criação:

- **WinRAR.exe** foi iniciado às **14:37:23**
- **DumpIt.exe** às **14:37:54**

Ou seja, o utilizador primeiro compactou algo (WinRAR) e logo depois executou o DumpIt para gerar o ficheiro de memória.
A sequência é lógica e consistente com uma atividade legítima.

Interpretação Final da Análise

Com base na comparação entre pslist, psscan e psxview, concluo que **não existem processos ocultos** nem sinais de malware.
As múltiplas instâncias de WinRAR e DumpIt que aparecem no psscan correspondem a resíduos normais de processos terminados.
O cmd.exe estava ativo e foi usado apenas para executar o comando que revelou a flag.
Todos os restantes processos pertencem ao sistema ou ao ambiente virtual (VirtualBox).

Em resumo:

- Nenhum processo oculto foi encontrado.
- A sequência de execução (WinRAR -> DumpIt -> cmd -> flag) faz sentido e está coerente.
- O sistema estava limpo no momento da captura, sem sinais de comportamento malicioso.

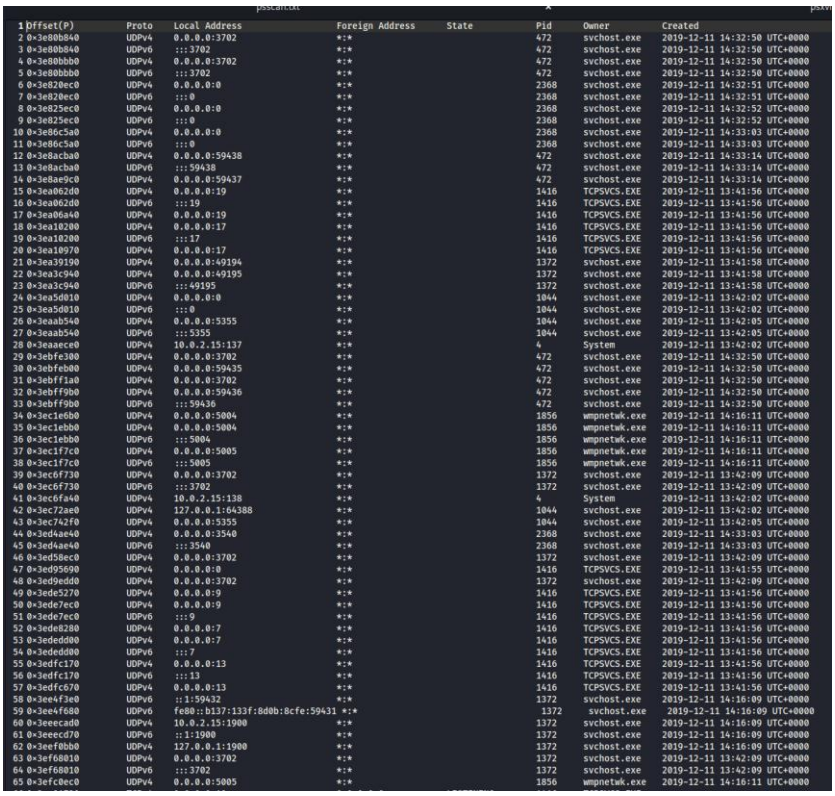
3- Análise de Ligações de Rede (3 pontos): verificar conexões ativas e processos que estavam a comunicar pela rede.

Para esta parte da análise quis perceber se, no momento da captura, o sistema tinha **ligações de rede ativas ou processos a comunicar externamente**. Usei o plugin netscan do Volatility, que permite identificar todas as conexões TCP e UDP encontradas na memória, juntamente com os PIDs e nomes dos processos responsáveis.

Usei o comando:

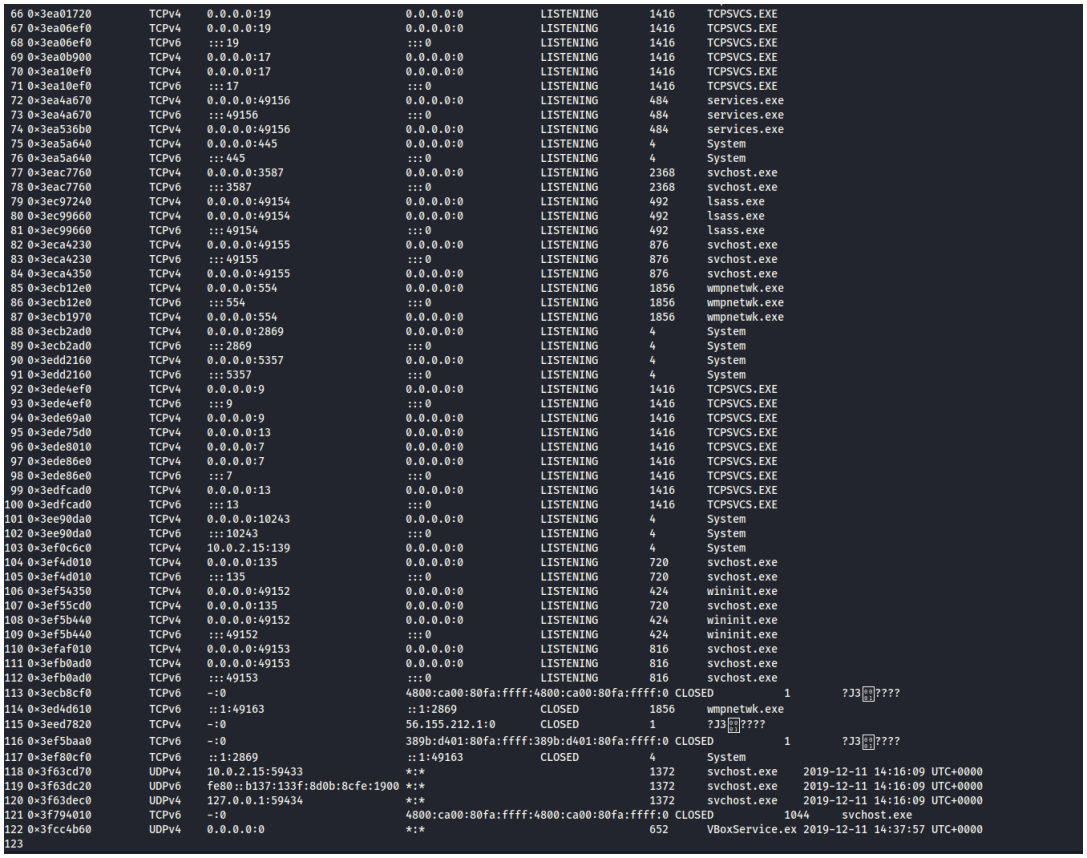
python2 ~/volatility/vol.py -f ~/Desktop/E-atividade.raw --profile=Win7SP1x64 netscan > ~/Desktop/Eatividade_results/netscan.txt

- python2 - executa o Volatility com o interpretador Python 2.
- ~/volatility/vol.py - localização do ficheiro principal do Volatility.
- -f ~/Desktop/E-atividade.raw - caminho da imagem de memória.
- --profile=Win7SP1x64 - perfil do sistema
- netscan - plugin usado para detetar sockets de rede, tanto TCP como UDP.
- > ~/Desktop/Eatividade_results/netscan.txt - grava o resultado num ficheiro .txt.



Offset(P)	Proto	Local Address	Foreign Address	State	Pid	Owner	Created
0x3e80b840	UDPv4	0.0.0.0:3702	*:*		472	svchost.exe	2019-12-11 14:32:50 UTC+0000
0x3e80b840	UDPv6	:::3702	*:*		472	svchost.exe	2019-12-11 14:32:50 UTC+0000
0x3e80bbb0	UDPv4	0.0.0.0:3702	*:*		472	svchost.exe	2019-12-11 14:32:50 UTC+0000
0x3e80bbb0	UDPv6	:::3702	*:*		472	svchost.exe	2019-12-11 14:32:50 UTC+0000
0x3e820ec0	UDPv4	0.0.0.0:0	*:*		2368	svchost.exe	2019-12-11 14:32:51 UTC+0000
0x3e820ec0	UDPv6	:::0	*:*		2368	svchost.exe	2019-12-11 14:32:51 UTC+0000
0x3e825ec0	UDPv4	0.0.0.0:0	*:*		2368	svchost.exe	2019-12-11 14:32:52 UTC+0000
0x3e825ec0	UDPv6	:::0	*:*		2368	svchost.exe	2019-12-11 14:32:52 UTC+0000
0x3e86c5a0	UDPv4	0.0.0.0:0	*:*		2368	svchost.exe	2019-12-11 14:33:03 UTC+0000
0x3e86c5a0	UDPv6	:::0	*:*		2368	svchost.exe	2019-12-11 14:33:03 UTC+0000
0x3e8acba0	UDPv4	0.0.0.0:59438	*:*		472	svchost.exe	2019-12-11 14:33:14 UTC+0000
0x3e8acba0	UDPv6	:::59438	*:*		472	svchost.exe	2019-12-11 14:33:14 UTC+0000
0x3e8ae9c0	UDPv4	0.0.0.0:59437	*:*		472	svchost.exe	2019-12-11 14:33:14 UTC+0000
0x3ea062d0	UDPv4	0.0.0.0:19	*:*		1416	TCPSVCS.EXE	2019-12-11 13:41:56 UTC+0000
0x3ea062d0	UDPv6	:::19	*:*		1416	TCPSVCS.EXE	2019-12-11 13:41:56 UTC+0000
0x3ea06a40	UDPv4	0.0.0.0:19	*:*		1416	TCPSVCS.EXE	2019-12-11 13:41:56 UTC+0000
0x3ea10200	UDPv4	0.0.0.0:17	*:*		1416	TCPSVCS.EXE	2019-12-11 13:41:56 UTC+0000
0x3ea10200	UDPv6	:::17	*:*		1416	TCPSVCS.EXE	2019-12-11 13:41:56 UTC+0000
0x3ea10970	UDPv4	0.0.0.0:17	*:*		1416	TCPSVCS.EXE	2019-12-11 13:41:56 UTC+0000
0x3ea39190	UDPv4	0.0.0.0:49194	*:*		1372	svchost.exe	2019-12-11 13:41:58 UTC+0000
0x3ea3c940	UDPv4	0.0.0.0:49195	*:*		1372	svchost.exe	2019-12-11 13:41:58 UTC+0000
0x3ea3c940	UDPv6	:::49195	*:*		1372	svchost.exe	2019-12-11 13:41:58 UTC+0000
0x3ea5d010	UDPv4	0.0.0.0:0	*:*		1044	svchost.exe	2019-12-11 13:42:02 UTC+0000
0x3ea5d010	UDPv6	:::0	*:*		1044	svchost.exe	2019-12-11 13:42:02 UTC+0000
0x3eaab540	UDPv4	0.0.0.0:5355	*:*		1044	svchost.exe	2019-12-11 13:42:05 UTC+0000
0x3eaab540	UDPv6	:::5355	*:*		1044	svchost.exe	2019-12-11 13:42:05 UTC+0000
0x3eaaece0	UDPv4	10.0.2.15:137	*:*		4	System	2019-12-11 13:42:02 UTC+0000
0x3ebfe300	UDPv4	0.0.0.0:3702	*:*		472	svchost.exe	2019-12-11 14:32:50 UTC+0000
0x3ebfeb00	UDPv4	0.0.0.0:59435	*:*		472	svchost.exe	2019-12-11 14:32:50 UTC+0000
0x3ebff1a0	UDPv4	0.0.0.0:3702	*:*		472	svchost.exe	2019-12-11 14:32:50 UTC+0000
0x3ebff9b0	UDPv4	0.0.0.0:59436	*:*		472	svchost.exe	2019-12-11 14:32:50 UTC+0000
0x3ebff9b0	UDPv6	:::59436	*:*		472	svchost.exe	2019-12-11 14:32:50 UTC+0000
0x3ec1e6b0	UDPv4	0.0.0.0:5004	*:*		1856	wmpnetwk.exe	2019-12-11 14:16:11 UTC+0000
0x3ec1ebb0	UDPv4	0.0.0.0:5004	*:*		1856	wmpnetwk.exe	2019-12-11 14:16:11 UTC+0000
0x3ec1ebb0	UDPv6	:::5004	*:*		1856	wmpnetwk.exe	2019-12-11 14:16:11 UTC+0000
0x3ec1f7c0	UDPv4	0.0.0.0:5005	*:*		1856	wmpnetwk.exe	2019-12-11 14:16:11 UTC+0000
0x3ec1f7c0	UDPv6	:::5005	*:*		1856	wmpnetwk.exe	2019-12-11 14:16:11 UTC+0000
0x3ec6f730	UDPv4	0.0.0.0:3702	*:*		1372	svchost.exe	2019-12-11 13:42:09 UTC+0000
0x3ec6f730	UDPv6	:::3702	*:*		1372	svchost.exe	2019-12-11 13:42:09 UTC+0000
0x3ec6fa40	UDPv4	10.0.2.15:138	*:*		4	System	2019-12-11 13:42:02 UTC+0000
0x3ec72ae0	UDPv4	127.0.0.1:64388	*:*		1044	svchost.exe	2019-12-11 13:42:02 UTC+0000
0x3ec742f0	UDPv4	0.0.0.0:5355	*:*		1044	svchost.exe	2019-12-11 13:42:05 UTC+0000
0x3ed4ae40	UDPv4	0.0.0.0:3540	*:*		2368	svchost.exe	2019-12-11 14:33:03 UTC+0000
0x3ed4ae40	UDPv6	:::3540	*:*		2368	svchost.exe	2019-12-11 14:33:03 UTC+0000
0x3ed58ec0	UDPv4	0.0.0.0:3702	*:*		1372	svchost.exe	2019-12-11 13:42:09 UTC+0000
0x3ed95690	UDPv4	0.0.0.0:0	*:*		1416	TCPSVCS.EXE	2019-12-11 13:41:55 UTC+0000
0x3ed9edd0	UDPv4	0.0.0.0:3702	*:*		1372	svchost.exe	2019-12-11 13:42:09 UTC+0000
0x3ede5270	UDPv4	0.0.0.0:9	*:*		1416	TCPSVCS.EXE	2019-12-11 13:41:56 UTC+0000
0x3ede7ec0	UDPv4	0.0.0.0:9	*:*		1416	TCPSVCS.EXE	2019-12-11 13:41:56 UTC+0000
0x3ede7ec0	UDPv6	:::9	*:*		1416	TCPSVCS.EXE	2019-12-11 13:41:56 UTC+0000
0x3ede8280	UDPv4	0.0.0.0:7	*:*		1416	TCPSVCS.EXE	2019-12-11 13:41:56 UTC+0000
0x3eded00	UDPv4	0.0.0.0:7	*:*		1416	TCPSVCS.EXE	2019-12-11 13:41:56 UTC+0000
0x3eded00	UDPv6	:::7	*:*		1416	TCPSVCS.EXE	2019-12-11 13:41:56 UTC+0000
0x3edfc170	UDPv4	0.0.0.0:13	*:*		1416	TCPSVCS.EXE	2019-12-11 13:41:56 UTC+0000
0x3edfc170	UDPv6	:::13	*:*		1416	TCPSVCS.EXE	2019-12-11 13:41:56 UTC+0000
0x3edfc670	UDPv4	0.0.0.0:13	*:*		1416	TCPSVCS.EXE	2019-12-11 13:41:56 UTC+0000
0x3ee4f3e0	UDPv6	::1:59432	*:*		1372	svchost.exe	2019-12-11 14:16:09 UTC+0000
0x3ee4f680	UDPv6	fe80::b137:133f:8d0b:8cfe:59431	*:*		1372	svchost.exe	2019-12-11 14:16:09 UTC+0000
0x3eeecad0	UDPv4	10.0.2.15:1900	*:*		1372	svchost.exe	2019-12-11 14:16:09 UTC+0000
0x3eeecd70	UDPv6	::1:1900	*:*		1372	svchost.exe	2019-12-11 14:16:09 UTC+0000
0x3eef0bb0	UDPv4	127.0.0.1:1900	*:*		1372	svchost.exe	2019-12-11 14:16:09 UTC+0000
0x3ef68010	UDPv4	0.0.0.0:3702	*:*		1372	svchost.exe	2019-12-11 13:42:09 UTC+0000
0x3ef68010	UDPv6	:::3702	*:*		1372	svchost.exe	2019-12-11 13:42:09 UTC+0000
0x3efc0ec0	UDPv4	0.0.0.0:5005	*:*		1856	wmpnetwk.exe	2019-12-11 14:16:11 UTC+0000

netscan.txt parte 1



```
66 0×3ea01720        TCPv4    0.0.0.0:19                    0.0.0.0:0              LISTENING       1416    TCPSVCS.EXE
67 0×3ea06ef0        TCPv4    0.0.0.0:19                    0.0.0.0:0              LISTENING       1416    TCPSVCS.EXE
68 0×3ea06ef0        TCPv6    :::19                         :::0                   LISTENING       1416    TCPSVCS.EXE
69 0×3ea0b900        TCPv4    0.0.0.0:17                    0.0.0.0:0              LISTENING       1416    TCPSVCS.EXE
70 0×3ea10ef0        TCPv4    0.0.0.0:17                    0.0.0.0:0              LISTENING       1416    TCPSVCS.EXE
71 0×3ea10ef0        TCPv6    :::17                         :::0                   LISTENING       1416    TCPSVCS.EXE
72 0×3ea4a670        TCPv4    0.0.0.0:49156                 0.0.0.0:0              LISTENING       484     services.exe
73 0×3ea4a670        TCPv6    :::49156                      :::0                   LISTENING       484     services.exe
74 0×3ea536b0        TCPv4    0.0.0.0:49156                 0.0.0.0:0              LISTENING       484     services.exe
75 0×3ea5a640        TCPv4    0.0.0.0:445                   0.0.0.0:0              LISTENING       4       System
76 0×3ea5a640        TCPv6    :::445                        :::0                   LISTENING       4       System
77 0×3eac7760        TCPv4    0.0.0.0:3587                  0.0.0.0:0              LISTENING       2368    svchost.exe
78 0×3eac7760        TCPv6    :::3587                       :::0                   LISTENING       2368    svchost.exe
79 0×3ec97240        TCPv4    0.0.0.0:49154                 0.0.0.0:0              LISTENING       492     lsass.exe
80 0×3ec99660        TCPv4    0.0.0.0:49154                 0.0.0.0:0              LISTENING       492     lsass.exe
81 0×3ec99660        TCPv6    :::49154                      :::0                   LISTENING       492     lsass.exe
82 0×3eca4230        TCPv4    0.0.0.0:49155                 0.0.0.0:0              LISTENING       876     svchost.exe
83 0×3eca4230        TCPv6    :::49155                      :::0                   LISTENING       876     svchost.exe
84 0×3eca4350        TCPv4    0.0.0.0:49155                 0.0.0.0:0              LISTENING       876     svchost.exe
85 0×3ecb12e0        TCPv4    0.0.0.0:554                   0.0.0.0:0              LISTENING       1856    wmpnetwk.exe
86 0×3ecb12e0        TCPv6    :::554                        :::0                   LISTENING       1856    wmpnetwk.exe
87 0×3ecb1970        TCPv4    0.0.0.0:554                   0.0.0.0:0              LISTENING       1856    wmpnetwk.exe
88 0×3ecb2ad0        TCPv4    0.0.0.0:2869                  0.0.0.0:0              LISTENING       4       System
89 0×3ecb2ad0        TCPv6    :::2869                       :::0                   LISTENING       4       System
90 0×3edd2160        TCPv4    0.0.0.0:5357                  0.0.0.0:0              LISTENING       4       System
91 0×3edd2160        TCPv6    :::5357                       :::0                   LISTENING       4       System
92 0×3ede4ef0        TCPv4    0.0.0.0:9                     0.0.0.0:0              LISTENING       1416    TCPSVCS.EXE
93 0×3ede4ef0        TCPv6    :::9                          :::0                   LISTENING       1416    TCPSVCS.EXE
94 0×3ede69a0        TCPv4    0.0.0.0:9                     0.0.0.0:0              LISTENING       1416    TCPSVCS.EXE
95 0×3ede75d0        TCPv4    0.0.0.0:13                    0.0.0.0:0              LISTENING       1416    TCPSVCS.EXE
96 0×3ede8010        TCPv4    0.0.0.0:7                     0.0.0.0:0              LISTENING       1416    TCPSVCS.EXE
97 0×3ede86e0        TCPv4    0.0.0.0:7                     0.0.0.0:0              LISTENING       1416    TCPSVCS.EXE
98 0×3ede86e0        TCPv6    :::7                          :::0                   LISTENING       1416    TCPSVCS.EXE
99 0×3edfcad0        TCPv4    0.0.0.0:13                    0.0.0.0:0              LISTENING       1416    TCPSVCS.EXE
100 0×3edfcad0       TCPv6    :::13                         :::0                   LISTENING       1416    TCPSVCS.EXE
101 0×3ee90da0       TCPv4    0.0.0.0:10243                 0.0.0.0:0              LISTENING       4       System
102 0×3ee90da0       TCPv6    :::10243                      :::0                   LISTENING       4       System
103 0×3ef0c6c0       TCPv4    10.0.2.15:139                 0.0.0.0:0              LISTENING       4       System
104 0×3ef4d010       TCPv4    0.0.0.0:135                   0.0.0.0:0              LISTENING       720     svchost.exe
105 0×3ef4d010       TCPv6    :::135                        :::0                   LISTENING       720     svchost.exe
106 0×3ef54350       TCPv4    0.0.0.0:49152                 0.0.0.0:0              LISTENING       424     wininit.exe
107 0×3ef55cd0       TCPv4    0.0.0.0:135                   0.0.0.0:0              LISTENING       720     svchost.exe
108 0×3ef5b440       TCPv4    0.0.0.0:49152                 0.0.0.0:0              LISTENING       424     wininit.exe
109 0×3ef5b440       TCPv6    :::49152                      :::0                   LISTENING       424     wininit.exe
110 0×3efaf010       TCPv4    0.0.0.0:49153                 0.0.0.0:0              LISTENING       816     svchost.exe
111 0×3efb0ad0       TCPv4    0.0.0.0:49153                 0.0.0.0:0              LISTENING       816     svchost.exe
112 0×3efb0ad0       TCPv6    :::49153                      :::0                   LISTENING       816     svchost.exe
113 0×3ecb8cf0       TCPv6    -:0                           4800:ca00:80fa:ffff:4800:ca00:80fa:ffff:0 CLOSED          1       ?J3??????
114 0×3ed4d610       TCPv6    ::1:49163                     ::1:2869               CLOSED          1856    wmpnetwk.exe
115 0×3eed7820       TCPv4    -:0                           56.155.212.1:0         CLOSED          1       ?J3??????
116 0×3ef5baa0       TCPv6    -:0                           389b:d401:80fa:ffff:389b:d401:80fa:ffff:0 CLOSED          1       ?J3??????
117 0×3ef80cf0       TCPv6    ::1:2869                      ::1:49163              CLOSED          4       System
118 0×3f63cd70       UDPv4    10.0.2.15:59433               *:*                                    1372    svchost.exe     2019-12-11 14:16:09 UTC+0000
119 0×3f63dc20       UDPv6    fe80::b137:133f:8d0b:8cfe:1900 *:*                                   1372    svchost.exe     2019-12-11 14:16:09 UTC+0000
120 0×3f63dec0       UDPv4    127.0.0.1:59434               *:*                                    1372    svchost.exe     2019-12-11 14:16:09 UTC+0000
121 0×3f794010       TCPv6    -:0                           4800:ca00:80fa:ffff:4800:ca00:80fa:ffff:0 CLOSED          1044    svchost.exe
122 0×3fcc4b60       UDPv4    0.0.0.0:0                     *:*                                    652     VBoxService.ex 2019-12-11 14:37:57 UTC+0000
123
```

netscan.txt parte 2

Resultados obtidos

O comando devolveu uma lista extensa de portas **em escuta (LISTENING)** e sockets UDP, a maioria associada a serviços de sistema e componentes normais do Windows.
Não foi identificada **nenhuma conexão externa ativa** no momento da captura.

Os principais processos observados foram:

- **svchost.exe (vários PIDs)** — responsável por vários serviços do Windows, como DNS Client, DHCP, SSDP Discovery e WS-Discovery. A maioria das portas (3702, 49194, 49195, etc.) estão associadas a esses serviços.
- **System (PID 4)** — gere portas do kernel e comunicações locais (ex.: 445, 2869, 5357).
- **TCPSVCS.EXE (PID 1416)** — processo legítimo relacionado com serviços TCP (Daytime, Echo, Discard, etc.), típico de ambientes de teste.
- **wmpnetwk.exe (PID 1856)** — relacionado com partilhas do Windows Media Player (portas 5004 e 5005).
- **VBoxService.exe e VBoxTray.exe** — ligados ao ambiente virtual (VirtualBox), esperados neste tipo de sistema.

Interpretação dos resultados

O netscan mostra apenas **ligações locais e portas em escuta**, não havendo nenhuma sessão TCP estabelecida ou conexão para IPs externos.
Todos os endereços pertencem a **interfaces internas (127.0.0.1 e 10.0.2.x)**, o que confirma que não houve tráfego de saída nem comunicação remota durante a execução dos processos anteriores.

O sistema estava a correr em ambiente de máquina virtual e encontrava-se isolado da rede no momento da recolha.
Não foram detetados programas estranhos ou processos suspeitos com sockets ativos.

Conclusão

Concluo que **não existiam conexões de rede ativas** nem qualquer evidência de comunicação maliciosa.
Os processos que aparecem estão todos associados ao funcionamento normal do Windows e da virtualização.
Isto reforça a ideia de que a criação do dump foi uma operação **local e legítima**, sem qualquer transferência ou exfiltração de dados pela rede.

4- **Revisão dos Logs de Consola (2 pontos):** identificar comandos ou entradas que possam indicar atividade maliciosa.

Para esta análise utilizei os *plugins* cmdscan e consoles do Volatility, executados com os seguintes comandos:

```
python2 ~/volatility/vol.py -f ~/Desktop/E-atividade.raw --profile=Win7SP1x64
                                cmdscan > cmdscan.txt
```

```
python2 ~/volatility/vol.py -f ~/Desktop/E-atividade.raw --profile=Win7SP1x64
                                consoles > consoles.txt
```

Os resultados mostraram duas consolas ativas no momento da captura:

- **cmd.exe (PID 1984)** – associada ao processo conhost.exe (PID 2692);
- **DumpIt.exe (PID 796)** – associada ao processo conhost.exe (PID 2260).

```
1 **************************************************
2 ConsoleProcess: conhost.exe Pid: 2692
3 Console: 0xff756200 CommandHistorySize: 50
4 HistoryBufferCount: 1 HistoryBufferMax: 4
5 OriginalTitle: %SystemRoot%\system32\cmd.exe
6 Title: C:\Windows\system32\cmd.exe - St4G3$1
7 AttachedProcess: cmd.exe Pid: 1984 Handle: 0x60
8 ----
9 CommandHistory: 0x1fe9c0 Application: cmd.exe Flags: Allocated, Reset
10 CommandCount: 1 LastAdded: 0 LastDisplayed: 0
11 FirstCommand: 0 CommandCountMax: 50
12 ProcessHandle: 0x60
13 Cmd #0 at 0x1de3c0: St4G3$1
14 ----
15 Screen 0x1e0f70 X:80 Y:300
16 Dump:
17 Microsoft Windows [Version 6.1.7601]
18 Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
19
20 C:\Users\SmartNet>St4G3$1
21 ZmxhZ3t0aDFzXzFzX3RoM18xc3Rfc3Q0ZzMhIX0=
22 Press any key to continue . . .
23 **************************************************
24 ConsoleProcess: conhost.exe Pid: 2260
25 Console: 0xff756200 CommandHistorySize: 50
26 HistoryBufferCount: 1 HistoryBufferMax: 4
27 OriginalTitle: C:\Users\SmartNet\Downloads\DumpIt\DumpIt.exe
28 Title: C:\Users\SmartNet\Downloads\DumpIt\DumpIt.exe
29 AttachedProcess: DumpIt.exe Pid: 796 Handle: 0x60
30 ----
31 CommandHistory: 0x38ea90 Application: DumpIt.exe Flags: Allocated
32 CommandCount: 0 LastAdded: -1 LastDisplayed: -1
33 FirstCommand: 0 CommandCountMax: 50
34 ProcessHandle: 0x60
35 ----
36 Screen 0x371050 X:80 Y:300
37 Dump:
38   DumpIt - v1.3.2.20110401 - One click memory memory dumper
39   Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
40   Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>
41
42
43    Address space size:        1073676288 bytes (   1023 Mb)
44    Free space size:           24185389056 bytes (  23064 Mb)
45
46    * Destination = \??\C:\Users\SmartNet\Downloads\DumpIt\SMARTNET-PC-20191211-
47 143755.raw
48
49    --> Are you sure you want to continue? [y/n] y
50    + Processing...
51
```

consoles.txt

```
1 **************************************************
2 CommandProcess: conhost.exe Pid: 2692
3 CommandHistory: 0x1fe9c0 Application: cmd.exe Flags: Allocated, Reset
4 CommandCount: 1 LastAdded: 0 LastDisplayed: 0
5 FirstCommand: 0 CommandCountMax: 50
6 ProcessHandle: 0x60
7 Cmd #0 @ 0x1de3c0: St4G3$1
8 Cmd #15 @ 0x1c0158:
9 Cmd #16 @ 0x1fdb30:
10 **************************************************
11 CommandProcess: conhost.exe Pid: 2260
12 CommandHistory: 0x38ea90 Application: DumpIt.exe Flags: Allocated
13 CommandCount: 0 LastAdded: -1 LastDisplayed: -1
14 FirstCommand: 0 CommandCountMax: 50
15 ProcessHandle: 0x60
16 Cmd #15 @ 0x350158: 8
17 Cmd #16 @ 0x38dc00: 8
18
```

cmdscan.txt

Resultados

Na consola do **cmd.exe**, o histórico apresenta apenas um comando introduzido manualmente:

St4G3$1

Logo abaixo, em **consoles.txt**, surge o mesmo comando com a saída no ecrã, que contém uma *string* em Base64:

ZmxhZ3t0aDFzXzFzX3RoM18xc3Rfc3Q0ZzMhIX0=

Ao decodificar essa *string* com o comando:

echo 'ZmxhZ3t0aDFzXzFzX3RoM18xc3Rfc3Q0ZzMhIX0=' | base64 -d

o resultado devolve a flag:

flag{th1s_1s_th3_1st_st4g3!!}

Isto confirma que o utilizador executou manualmente o comando **St4G3$1** e que este imprimiu a *flag* codificada em Base64.

No mesmo *dump*, observa-se o processo **DumpIt.exe** a ser executado logo de seguida, com a consola a pedir confirmação para criar o ficheiro de memória:

Are you sure you want to continue? [y/n] y

Processing...

O caminho indicado é:

C:\Users\SmartNet\Downloads\DumpIt\SMARTNET-PC-20191211-143755.raw

O que demonstra que a captura de memória foi feita imediatamente após a execução do comando, revelando atividade humana direta.

Nenhum comando suspeito foi encontrado (sem uso de PowerShell, scripts de rede, downloads, ou compressões de dados).

- O único comando existente serviu para **mostrar a flag do desafio**, seguido da criação legítima do *dump* com **DumpIt**.
- Não há sinais de automatização, persistência, exfiltração nem tentativa de ocultação.

Conclusão

Os logs de consola demonstram que o utilizador executou apenas o comando St4G3$1, que revelou uma *string* Base64 correspondente à flag do exercício, e logo de seguida utilizou o **DumpIt.exe** para gerar a imagem de memória. Toda a atividade registada é **legítima e controlada**, sem qualquer evidência de comportamento malicioso.

5- **Recuperação de Ficheiros Importantes (4 pontos):** localizar e recuperar ficheiros relevantes, documentando os caminhos e alterações.

Para esta fase foquei-me em localizar ficheiros relevantes no disco (Downloads e Documents dos utilizadores) e em recuperar quaisquer ficheiros que pudessem conter flags ou informação útil. Segui uma sequência lógica: identificar entradas com filescan, extrair ficheiros encontrados na memória para a pasta recovered, confirmar o tipo dos ficheiros com file, e finalmente desempacotar/abrir os ficheiros protegidos por password.

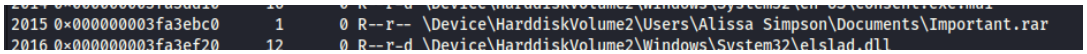
Comandos e passos que executei

Gerei a lista de ficheiros presentes na imagem de memória para procurar nomes relevantes (Important, WinRAR, .rar, Downloads, Documents):

python2 ~/volatility/vol.py -f ~/Desktop/E-atividade.raw --profile=Win7SP1x64 filescan > ~/Desktop/Eatividade_results/filescan.txt

Depois pesquisei no filescan.txt por termos como Important, SW1, WinRAR, Downloads, Documents para localizar ficheiros potencialmente relevantes.

Do filescan encontrei Important.rar que despertou a minha curiosidade:



\Device\HarddiskVolume2\Users\Alissa Simpson\Documents\Important.rar

ou, conforme o output, a mesma entrada aparecia listada com o offset associado. Foi esta referência que me permitiu procurar o ficheiro na memória e tentar extrair uma cópia.

Extraí os blocos correspondentes e gravei-os para a pasta recovered. O Volatility deixou-me um ficheiro com nome automático, do tipo file.None.0xfffffa8001034450.dat. Para confirmar o formato do ficheiro, usei:

file ~/Desktop/Eatividade_results/recovered/file.None.0xfffffa8001034450.dat

O comando file devolveu:

RAR archive data, v5

Ou seja, o ficheiro era de facto um RAR (versão 5). Renomeei-o para facilitar o trabalho:

mv ~/Desktop/Eatividade_results/recovered/file.None.0xfffffa8001034450.dat \

~/Desktop/Eatividade_results/recovered/Important.rar

Antes de tentar extrair, verifiquei o conteúdo/comentário do RAR:

unrar l -p- ~/Desktop/Eatividade_results/recovered/Important.rar

O unrar listou o ficheiro flag3.png dentro do archive e mostrou um comentário que é importante para a password:

Archive comment:

Password is NTLM hash(in uppercase) of Alissa's account passwd.

Isto indicava que a password do RAR não era uma palavra normal, mas sim o hash NTLM da password da conta da utilizadora Alissa, em maiúsculas.

Para obter esse NTLM hash, usei a técnica de extrair os hives e os hashes SAM (Volatility):

python2 ~/volatility/vol.py -f ~/Desktop/E-atividade.raw --profile=Win7SP1x64 hivelist | tee ~/Desktop/Eatividade_results/hivelist.txt

Localizei os offsets dos hives SYSTEM e SAM no hivelist.txt. Depois executei:

defini os offsets correctos no meu caso

SYS=0xfffff8a000024010

SAM=0xfffff8a0014e9010

**python2 ~/volatility/vol.py -f ~/Desktop/E-atividade.raw --profile=Win7SP1x64 **

hashdump -y "$SYS" -s "$SAM" | tee ~/Desktop/Eatividade_results/hashdump.txt

O hashdump devolveu os NTLM hashes dos utilizadores, entre eles a entrada de **Alissa Simpson**.

Extraí exactamente o hash da Alissa e converti para maiúsculas (conforme o comentário do RAR):

awk -F: '/Alissa Simpson/{print toupper($4)}' ~/Desktop/Eatividade_results/hashdump.txt \

| tee ~/Desktop/Eatividade_results/ALISSA_NTLM.txt

No meu caso ficou:

F4FF64C8BAAC57D22F22EDC681055BA6

Com a password agora conhecida (o hash em uppercase), abri o RAR e extraí o ficheiro:

unrar l -p"$F4FF64C8BAAC57D22F22EDC681055BA6" \

~/Desktop/Eatividade_results/recovered/Important.rar

E para extrair:

mkdir -p ~/Desktop/Eatividade_results/recovered/unpacked

unrar x -o+ -p"$F4FF64C8BAAC57D22F22EDC681055BA6" \

~/Desktop/Eatividade_results/recovered/Important.rar \

~/Desktop/Eatividade_results/recovered/unpacked/

Resultados obtidos

- O ficheiro Important.rar continha o ficheiro flag3.png.
- Confirmei o tipo do ficheiro extraído com file e abri a imagem para verificar o conteúdo (flag).

Conclusão

Concluo que foi possível localizar e recuperar um ficheiro relevante (Important.rar) na imagem de memória. O ficheiro é um RAR v5 que continha flag3.png. A password do RAR estava documentada no comentário do archive e correspondia ao NTLM hash da conta de utilizador **Alissa Simpson** - hash que recuperei dos hives (SAM + SYSTEM) usando o plugin hashdump do Volatility. Com esse hash em uppercase consegui extrair o conteúdo e recuperar a flag.

6- **Análise de Atividades de Compressão (2 pontos):** verificar tentativas de compressão de ficheiros sensíveis.

Para verificar se ocorreram atividades de compressão de ficheiros sensíveis, analisei os resultados dos comandos filescan e strings, procurando referências à utilização do WinRAR e à criação de ficheiros com a extensão .rar**.**

Passos realizados:

Consulta ao ficheiro filescan.txt
Comecei por analisar o ficheiro filescan.txt, que contém todas as entradas de ficheiros detetadas na memória.

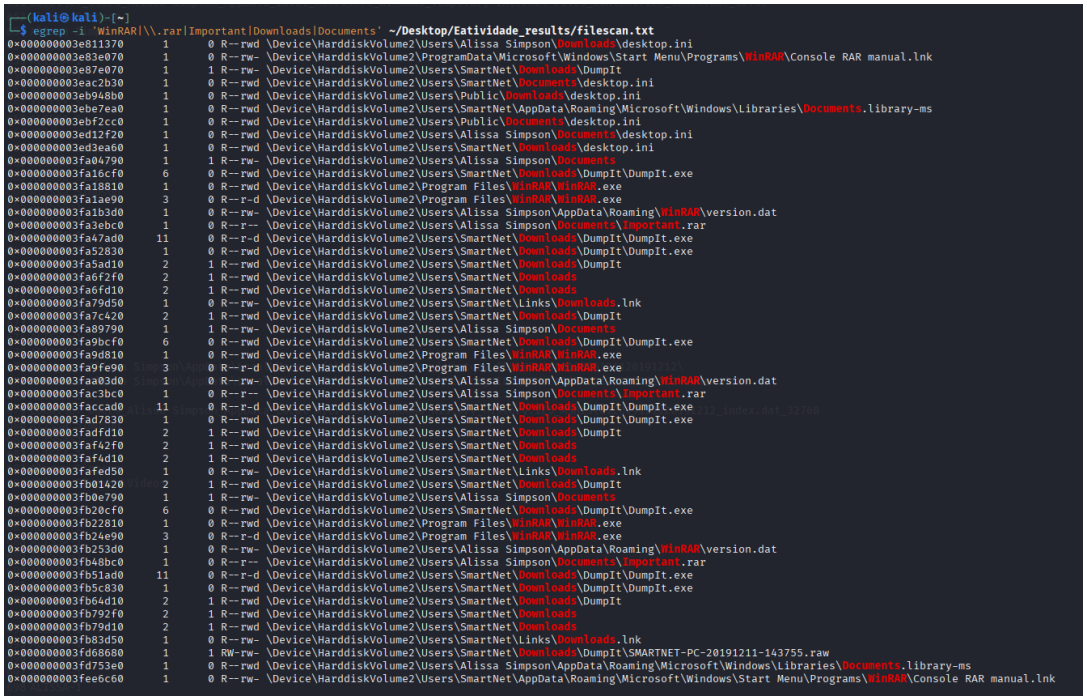
Extração de strings da memória
Extraí todas as *strings* da imagem de memória para um ficheiro separado, de modo a identificar nomes, caminhos e possíveis artefactos associados ao utilizador:

python2 ~/volatility/vol.py -f ~/Desktop/E-atividade.raw --profile=Win7SP1x64 strings > ~/Desktop/Eatividade_results/alissa_Strings.txt

Pesquisa de referências relevantes
Procurei termos associados a compressão e ficheiros .rar nos dois ficheiros (filescan.txt e alissa_Strings.txt) com o egrep:

egrep -i 'WinRAR|\.rar|Important|Downloads|Documents' ~/Desktop/Eatividade_results/filescan.txt
egrep -i 'Important|Important.rar' ~/Desktop/Eatividade_results/alissa_Strings.txt

Resultados obtidos:



Encontrei diversas entradas relacionadas com o WinRAR e com o ficheiro Important.rar, situadas em:

C:\Users\Alissa Simpson\Documents\Important.rar

As mesmas referências também surgiram no ficheiro alissa_Strings.txt, onde foi identificada uma versão codificada do nome do ficheiro em **Base64**:

SW1wb3J0YW50.rar

Após decodificação, confirmei o nome original:

echo SW1wb3J0YW50 | base64 -d
-> Important

Conclusão:

As evidências encontradas no filescan e nas strings demonstram que a utilizadora **Alissa Simpson** executou o WinRAR para comprimir ficheiros sensíveis, nomeadamente o Important.rar.
A presença repetida de referências ao WinRAR.exe, associadas aos diretórios Documents e Downloads, confirma a atividade de compressão imediatamente antes da criação do dump de memória analisado.

7 **Identificação e Análise de Artefatos de Aplicações (3 pontos):** examinar artefatos de softwares executados, recuperando dados úteis.

Para identificar artefatos de aplicações executadas durante a sessão analisada, concentrei-me nos resultados do filescan e do strings, procurando evidências de programas utilizados, respetivos caminhos e dados residuais na memória.

Passos realizados:

Gerei strings da imagem de memória e guardei para análise:

1) ASCII

```
strings -a -td ~/Desktop/E-atividade.raw >
~/Desktop/Eatividade_results/strings_ascii.txt
```

2) Unicode

```
strings -a -td -el ~/Desktop/E-atividade.raw >
~/Desktop/Eatividade_results/strings_unicode.txt
```

3) Juntar para um único ficheiro de trabalho

```
cat ~/Desktop/Eatividade_results/strings_ascii.txt \
~/Desktop/Eatividade_results/strings_unicode.txt \
| awk '{$1=""; sub(/^ /,""); print}' \
> ~/Desktop/Eatividade_results/alissa_strings.txt
```

4) Gerei strings da imagem de memória e guardei para análise:

```
egrep -i 'Program
Files|WinRAR|DumpIt|SmartNet|Alissa|\.rar|Important' \
~/Desktop/Eatividade_results/alissa_strings.txt
```

Procurei artefatos de aplicações e ficheiros relevantes:

```
egrep -i 'Program Files|WinRAR|DumpIt|SmartNet|Alissa|\.rar' \
~/Desktop/Eatividade_results/alissa_strings.txt
```

Corroborei com o inventário de ficheiros em memória (já produzido em filescan.txt) procurando executáveis/artefatos das mesmas apps:

**egrep -i 'WinRAR|DumpIt|Program Files|AppData\\Roaming\\WinRAR|\.rar' **

~/Desktop/Eatividade_results/filescan.txt

Achados principais

WinRAR
Evidências indicam uso ativo do WinRAR pelo perfil **Alissa Simpson**:

- **Atalho:** C:\Users\Alissa Simpson\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\WinRAR\WinRAR.lnk.
- **Executável carregado em memória:** \Program Files\WinRAR\WinRAR.exe (múltiplas entradas no *filescan*).
- **Ficheiro de configuração/versão:** C:\Users\Alissa Simpson\AppData\Roaming\WinRAR\version.dat.

Ficheiros manipulados (e registos "Visited" recuperados nas strings):

- C:\Users\Alissa Simpson\Documents\Important.rar — múltiplos acessos no *filescan*.
- C:\Users\Alissa Simpson\Downloads\SW1wb3J0YW50.rar — nome ofuscado (Base64) da cópia de *Important.rar* em Downloads.
- Entradas "Visited":
- file:///C:/Users/Alissa%20Simpson/Documents/Important.rar
- file:///C:/Users/Alissa%20Simpson/Downloads/SW1wb3J0YW50.rar

Comentário interno do RAR (recuperado da memória):

"Password is NTLM hash (in uppercase) of Alissa's account passwd."

stAg3_5.txt e mspaint.exe

Foi identificado o artefato C:\Users\Alissa Simpson\stAg3_5.txt em múltiplas strings e no inventário de ficheiros (filescan.txt), acompanhado de um atalho stAg3_5.lnk.
As referências indicam que o ficheiro existiu e foi provavelmente utilizado pela Alissa.

Foram realizadas várias tentativas de extração, incluindo dumpfiles por offset, *carving* manual (dd), e análise do processo mspaint.exe (PID 2424), onde surgiram também diversas referências a .png, .bmp e ao mesmo stAg3_5.lnk.
A partir deste processo foi possível reconstruir uma pequena imagem bitmap (00199144.bmp), com dimensões 126x126 px, porém sem conteúdo legível nem flag visível (analisada com strings, binwalk e OCR).

A ausência de dados legíveis indica que o ficheiro ou imagem foram encerrados ou descarregados da memória antes da aquisição, ou que os blocos se encontravam fragmentados.
Mesmo assim, estas evidências provam que o ficheiro stAg3_5.txt existiu e foi acedido, e que o Paint foi usado para abrir ou visualizar artefatos gráficos associados às etapas intermédias da análise.

DumpIt (aquisição de memória)
Artefatos mostram execução do DumpIt a partir do utilizador **SmartNet** e presença do ficheiro gerado:

- \Users\SmartNet\Downloads\DumpIt\DumpIt.exe
- \Users\SmartNet\Downloads\DumpIt\SMARTNET-PC-20191211-143755.raw

Conclusão:

Os artefatos recolhidos confirmam a execução de **WinRAR**, **DumpIt**, e a criação/acesso de ficheiros auxiliares como stAg3_5.txt, possivelmente visualizados no **mspaint.exe**.
As strings e o filescan provam o uso ativo do WinRAR para manipular um ficheiro sensível (Important.*rar*), incluindo uma cópia ofuscada em Base64. O comentário interno do RAR com a regra da palavra-passe foi recuperado da memória e foi essencial para o acesso ao conteúdo.

O DumpIt foi executado a partir do perfil **SmartNet**, explicando a existência da imagem de memória analisada, onde também surgiram vestígios do Paint e de ficheiros intermédios.