Lab Report

Name: Inor Wang
Title: Memory Analysis w/ Volatility 3
Case: 25-T108
Date: 11/06/2025

Table of Contents

Document Revision History

Name	Revision Date	Version	Description
Inor Wang	11/06/2025	0.1	Draft

Executive Summary

On 6 Nov 2025, the examiner analyzed Windows memory from CITADEL-DC01 and DESKTOP-SDN1RPT with Volatility 3, then triaged dumped regions using file, ClamAV, FLOSS, and capa. The focus was to capture image context (system time / NT version), identify short-lived processes, confirm spoolsv.exe injection, enumerate DLLs/handles/mutants, map sockets, and tie memory artifacts to a single C2. The lab shows: a brief coreupdater.exe stager on both hosts that could not be dumped; spoolsv.exe on both hosts with malfind-positive VADs containing MZ and dumping to PE32+ DLLs; AV hits (Meterpreter/Razy); FLOSS pulling 203.78.103.109; capa calling out embedded PE/zlib on DC01's shellcode; netscan showing ESTABLISHED connections to 203.78.103.109:443; and ICANN geolocating that IP to Thailand.

Key findings

DC01 (citadeldc01.mem)

- **System time / NT:** 2020-09-19 04:39:59 UTC; NtMajor 6 / NtMinor 3.
- **coreupdater.exe (PID 3644, PPID 2244):** pslist; created 03:56:37 UTC → exited 03:56:52 UTC (~15s); no DLLs, no handles; dump failed → short-lived/deleted; no other processes with exit times.
- **spoolsv.exe (PID 3724, PPID 452):** present; created 03:29:40 UTC; no exit time; legitimate Windows print spooler. DLLs/handles/mutants: 83 DLLs (all under Windows), 410 handles, 14 Mutants (none with data).
- **Network:** netscan shows two ESTABLISHED connections for coreupdater.exe to 203.78.103.109:443.
- **malfind:** spoolsv.exe = 4 suspicious VADs, 3 with MZ; coreupdater.exe = none.
- **file (spoolsv dumps):** pid.3724.vad.0x4afbf20000-0x4afbf51fff.dmp = data; …0x4afc1f0000-0x4afc25afff.dmp = PE32+ DLL (x86-64, 6 sections); …0x4afc070000-0x4afc0a8fff.dmp = PE32+ DLL (x86-64, 6 sections); …0x4afc260000-0x4afc283fff.dmp = PE32+ DLL (x86-64, 6 sections).
- **ClamAV (by dump):** 0x4afbf20000…51fff = Win.Exploit.Meterpreter-9752338-0; 0x4afc1f0000…25afff = Win.Malware.Meterpreter-9872014-0; 0x4afc070000…0a8fff =

Win.Exploit.Meterpreter-9752338-0; 0x4afc260000…283fff = Win.Malware.Razy-9865903-0.

- **FLOSS**: 203.78.103.109 in 0x4afbf20000…51fff.
- **capa (on 0x4afbf20000…51fff, -f sc64)**: contains embedded PE; linked against zlib.
- **ICANN:** 203.78.103.109 → Thailand.

DESKTOP (DESKTOP-SDN1RPT.mem)

- **System time / NT**: 2020-09-19 05:10:39 UTC; NtMajor 10 / NtMinor 0.
- **spoolsv.exe (PID 2188, PPID 616)**: present; created 01:24:09 UTC; no exit time.
- **coreupdater.exe (PID 8324, PPID 4008):** created 03:40:49 UTC → exited 03:43:10 UTC; dump failed.
- **Network**: netscan lists two ESTABLISHED connections to 203.78.103.109:443 (no process name in output).
- **malfind**: spoolsv.exe = 1 suspicious VAD with MZ; coreupdater.exe = none.
- **file (spoolsv dump pid.2188.vad.0x1840000-0x1863fff.dmp):** PE32+ DLL (x86-64, 5 sections).
- **ClamAV:** Win.Malware.Razy-9865903-0 on 0x1840000…63fff.
- **capa (on 0x1840000…63fff, -f sc64):** no capabilities reported.
- **Same malware (Q30):** The examiner assesses DC01 PID 3724 and DESKTOP PID 2188 as the same malware (matching injection + PE DLL dumps + Razy).

From this lab's artifacts alone: short-lived coreupdater.exe stagers, in-memory DLL injection into spoolsv.exe on both hosts, and traffic to 203.78.103.109:443 (ICANN: Thailand). Together, these show coordinated activity across DC01 and DESKTOP, with DC01 carrying a loader/stager (embedded-PE, zlib) and the desktop holding a PE DLL stage; thus spoolsv.exe (PID 3724) and spoolsv.exe (PID 2188) represent the same malware family within the captured window.

Synopsis

The examiner conducted memory-first forensics on Windows images from CITADEL-DC01 and DESKTOP-SDN1RPT using Volatility 3 to determine access paths, account usage, and signs of data staging during a suspected RDP-driven intrusion. Analysis showed a brute-force of Administrator (domain C137) from 194.61.24.102 culminating in a successful RDP login to DC01 at approximately 03:21 UTC (2020-09-19), followed by lateral RDP to the desktop minutes later. Both systems exhibited code injection into spoolsv.exe (DC01 PID 3724, DESKTOP PID 2188) with MZ-bearing VADs; off-host triage of dumped regions produced ClamAV detections (Meterpreter/Razy), FLOSS recovery of C2 203.78.103.109, and capa results consistent with a zlib-packed loader embedding a PE on DC01. Short-lived coreupdater.exe processes (DC01 PID 3644, DESKTOP PID 8324) appeared and could not be fully recovered, aligning with ephemeral/deleted stagers; netscan correlated ESTABLISHED traffic to 203.78.103.109:443 during the activity window.

Client Questions:

dc01 Image

1. What is the date timestamp (system time) of which this image was captured?
2. What is the NtMajorVersion and NtMinorVersion?
3. In your previous assignment, you discovered several applications that were ran during the suspicious RDP session. Are any of them present in the process list (pslist, psscan, etc), if so, what is the PID, PPID, name, and time it started (created) and exited execution? (Hint: review question 31)
4. Are there any DLLs mapped to this process? Are any of them outside of Windows?
5. Are there any handles for this process? If so, how many File handles are there?
6. Attempt to dump the process from memory based on its PID. Was in successful?
7. What do you think happened to this process?
8. Are there any other processes that have an exit time?
9. In your previous assignment, you discovered evidence of an application that crashed. Is this application present in the process list? If so, what is the PID, PPID, name, and time it started (created) and exited execution? (Hint: review question 39)
10. Do some research on this process name. What is it? Is it legitimate?
11. Are there any DLLs mapped to this process? Are any of them outside of Windows?

12. Are there any handles for this process? If so, how many File handles are there?
13. Are there any mutants for this process? How many actually have data?
14. Review network connections from the system (netscan and netstat). Did any of the above processes have an "ESTABLISHED" connection? If so, what is the process name and what remote IP address and port was it connected to?
15. Run malfind. Are there any processes that have suspicious memory sections from previous questions? If so, how many sections were found and do any of them contain code (i.e. MZ header)? Dump all sections using the "–pid PID and –dump" arguments.
16. Run the file command on all dumped malfind files. What is the output of each file?
17. Run clamscan on all the dumped malfind files. What are the detections for each file?
18. Run FLOSS on all files, there is an IP address in one of the files lsat the end of the output. What file contains the IP address?
19. Run capa on this file. What are the capabilities of this file? (Hint: this is shellcode, not an executable)
20. What country is the IP address from?

desktop Image

21. What is the date timestamp (system time) of which this image was captured?
22. What is the NtMajorVersion and NtMinorVersion?
23. Are the suspicious processes from the last image in this one? If so, what is the PID, PPID, name, and time it started (created) and exited execution?
24. Are you able to recover (dump) both?
25. Review the network connections. Do you see connections to the IP address from the last image? If so, what is the process name and what remote IP address and port was it connected to?
26. Run malfind. Are there any processes that have suspicious memory sections from previous questions? If so, how many sections were found and do any of them contain code (i.e. MZ header)? Dump all sections using the "–pid PID and –dump" arguments.
27. Run the file command on all dumped malfind files. What is the output of each file?
28. Focus on the PE files, remove the others. Run clamscan, what are the detections for each file?
29. Does capa report any capabilities for either file?
30. Do you believe this is the same malware as seen on the DC?

Scope of Work:

- Acquisition of memory captures, DC01-memory.zip and DESKTOP-SDN1RPT-memory.zip.
- Analyzation of memory captures using Volatility 3
- Verification of evidentiary integrity using MD5, SHA1, and SHA256 cryptographic hashes.
- All tools were run against mounted, read-only images to preserve evidentiary integrity.

Evidence Analyzed

This section provides details of the digital evidence collected

Evidence ID	**E001**
Name	DC01-memory.zip
Type	Zip archive data, at least v2.0 to extract, compression method=store
Size	561,424,278 bytes (561.42 MB)
MD5	64A4E2CB47138084A5C2878066B2D7B1
SHA1	E8DD11314A2501DC0AD98901A321350D9CD111C2
SHA256	86658D85D8254E8D30DCCC4F50D9C2A8B550A101D2E78A6D932316849E37AD80
SSDeep	12582912:H8xocBIyVnRyMhq6vKFU9HW9JIkwtZ0zC:HG7BImRvP2U9aPc
Entropy	7.994373345582934

Evidence ID	**E002**
Name	DESKTOP-SDN1RPT-memory.zip
Type	Zip archive data, at least v2.0 to extract, compression method=deflate
Size	802,767,348 bytes (802.76 MB)
MD5	CF31E2635C77811AAA1BB04A92A721E2
SHA1	74B2C80AC8E9D249855E7318AD9DB37CA40799DF
SHA256	FCE1BDD584CD52D7830F7F9A209E960CA151CE174EBDEF3FAD03205AB7E33D01
SSDeep	12582912:nEX7AJzR6rYFYnTj7P1Bpq49Rf2rNcHpeIOTFRL98/MB0RMDLL/9OOBT4XwzgLjz:EXUo7TnPbpl+6HpEb9WI/A6hULj/E9Rg
Entropy	7.998123849644843

Tools Used

Workstation

Hostname	Operating System	Build	Physical / Virtual	Built
IS-4523-001-GREYMHATTER	Fedora	2025	Virtual	10/31/2025

Software

Name	Version	Release	Purpose
Volatility 3 (Volatility Foundation)	2.26.2	Sep 2025	Perform Windows memory forensics on citadeldc01.mem and DESKTOP-SDN1RPT.mem to enumerate processes, detect code injection/persistence, correlate network sockets, and extract suspicious VADs/process images for off-host triage, enabling the examiner to reconstruct the 2020-09-19 intrusion window.

Analysis Findings

Overview of Examination Procedures

The examiner received Windows memory captures from CITADEL-DC01 and DESKTOP-SDN1RPT and analyzed them in a read-only workflow using Volatility 3 (v3.11). The examiner first established image context with info.Info (system time and NT version), then enumerated processes via windows.pslist and windows.psscan, flagging short-lived coreupdater.exe instances (DC01 PID 3644; DESKTOP PID 8324) and service spoolsv.exe processes (DC01 PID 3724; DESKTOP PID 2188) for deeper review. For each target process, the examiner profiled modules with windows.dlllist, enumerated objects with windows.handles (including Mutant handles), attempted process extractions with windows.dumpfiles, and correlated network state using windows.netscan to identify ESTABLISHED traffic—specifically connections to 203.78.103.109:443. Indicators of code injection were isolated with windows.malfind; all suspicious VADs (including those containing MZ headers) were dumped and triaged off-host using file (type verification), ClamAV (clamscan) for malware families (Meterpreter / Razy detections), FLOSS to recover strings and command-and-control (203.78.103.109), and capa to characterize behaviors (e.g., embedded PE and zlib linkage within DC01's injected shellcode, with no capabilities reported for the DESKTOP PE DLL dump).Additional targeted analysis was performed using:

- **Volatility 3 (Volatility Foundation)** — Used to analyze the memory files of the domain controller and desktop.

Throughout the process, all findings were documented and evidence files were correctly hashed.

Evidence Reviewed

1. **DC01-memory.zip (E001): Windows system memory (domain controller)**
2. **DESKTOP-SDN1RPT-memory.zip (E002): Windows desktop workstation memory**

Key Findings

dc01 Image

1. What is the date timestamp (system time) of which this image was captured?

- **Analysis Performed:**
  - The examiner used Volatility 3 via the command line shown in Figure 1, to extract the image info of the dc01 image which contains the date timestamp (system time) of which this image was captured.
  - Command: *vol -f citadeldc01.mem info.Info*
- **Answer:**
  The system time of the dc01 memory image is **2020-09-19 04:39:59 UTC**, as shown in Figure 1.

- **Supporting Evidence:**

```
~/Desktop/Evidence ❯ vol -f citadeldc01.mem info.Info                    04:01:30+0000
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
Variable        Value

Kernel Base     0xf800cb804000
DTB     0x1a7000
Symbols jar:file:/home/hatter/.local/lib/python3.13/site-packages/volatility3/symbols/windows.zip!windo
ws/ntkrnlmp.pdb/6066913DFBAD4EF6B754E136C12BECA3-1.json.xz
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdVersionBlock  0xf800cba9bd80
Major/Minor     15.9600
MachineType     34404
KeNumberProcessors      2
SystemTime      2020-09-19 04:39:59+00:00
NtSystemRoot    C:\Windows
NtProductType   NtProductLanManNt
NtMajorVersion  6
NtMinorVersion  3
PE MajorOperatingSystemVersion  6
PE MinorOperatingSystemVersion  3
PE Machine      34404
PE TimeDateStamp        Sat Feb 22 08:08:18 2014
```

Figure 1. Volatility 3 info.Info for citadeldc01.mem

2. What is the NtMajorVersion and NtMinorVersion?

- **Analysis Performed:**
  - The examiner used Volatility 3 via the command line shown in Figure 2, to extract the image info of the dc01 image which contains the NtMajorVersion and NtMinorVersion.
  - Command: *vol -f citadeldc01.mem info.Info*
- **Answer:**
  The NtMajorVersion of the memory image is **6** and the NtMinorVersion of the memory image is **3**, as shown in Figure 2.

- **Supporting Evidence:**

```
~/Desktop/Evidence ❯ vol -f citadeldc01.mem info.Info              04:01:30+0000
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
Variable        Value

Kernel Base     0xf800cb804000
DTB     0x1a7000
Symbols jar:file:/home/hatter/.local/lib/python3.13/site-packages/volatility3/symbols/windows.zip!windo
ws/ntkrnlmp.pdb/6066913DFBAD4EF6B754E136C12BECA3-1.json.xz
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdVersionBlock  0xf800cba9bd80
Major/Minor     15.9600
MachineType     34404
KeNumberProcessors      2
SystemTime      2020-09-19 04:39:59+00:00
NtSystemRoot    C:\Windows
NtProductType   NtProductLanManNt
NtMajorVersion  6
NtMinorVersion  3
PE MajorOperatingSystemVersion  6
PE MinorOperatingSystemVersion  3
PE Machine      34404
PE TimeDateStamp        Sat Feb 22 08:08:18 2014
```

Figure 2. Volatility 3 info.Info for citadeldc01.mem

3. In your previous assignment, you discovered several applications that were ran during theD suspicious RDP session. Are any of them present in the process list (pslist, psscan, etc), if so, what is the PID, PPID, name, and time it started (created) and exited execution? (Hint: review question 31)

- **Analysis Performed:**
  - The examiner used Volatility 3 via the command line shown in Figure 3, to extract the processes (pslist) of the dc01 image.
  - Command: *vol -f citadeldc01.mem windows.pslist*
- **Answer:**
  The **coreupdater.exe** application is present in the process list (pslist) and the PID is **3644**, PPID is **2244**, name is **coreupdater.exe**, created date timestamp is **2020-09-19 03:56:37 UTC**, and the exited date timestamp is **2020-09-19 03:56:52 UTC**, as shown in Figure 3.

- **Supporting Evidence:**

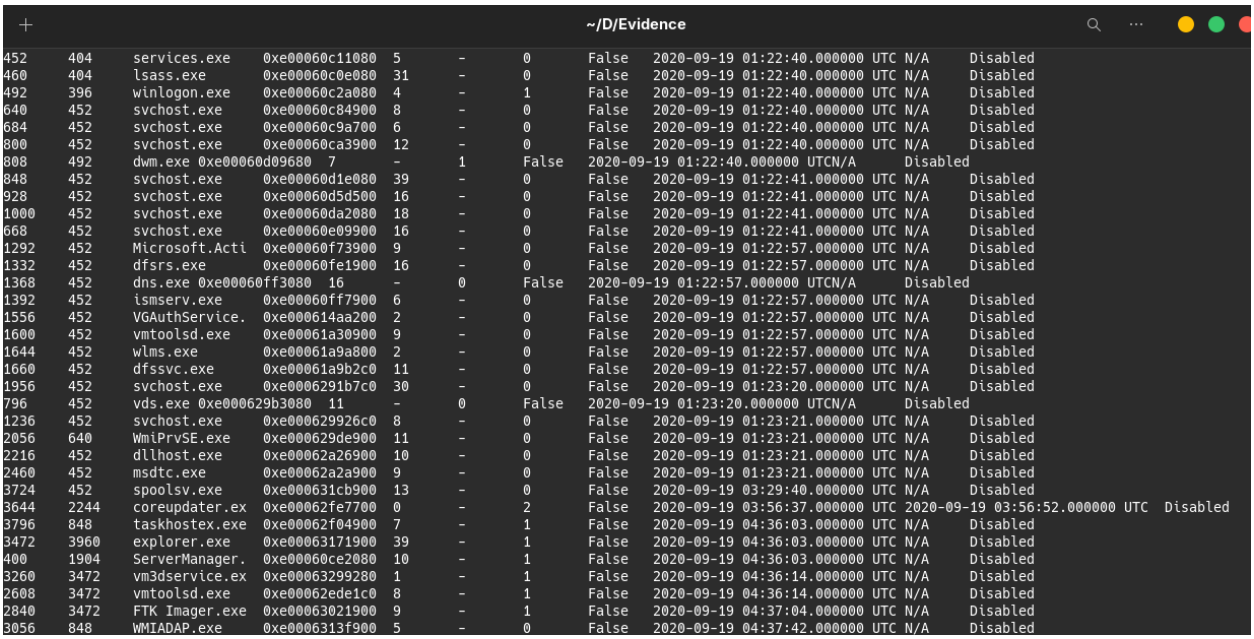

Figure 3. Volatility 3 windows.pslist for citadeldc01.mem

4. Are there any DLLs mapped to this process? Are any of them outside of Windows?

- **Analysis Performed:**
  - The examiner used Volatility 3 via the command line shown in Figure 4, to extract the DLLs mapped to the coreupdater.exe (PID: 3644) process of the dc01 image.
  - Command: *vol -f citadeldc01.mem windows.dlllist --pid 3644*
- **Answer:**
  There are **no** DLLs mapped to the coreupdater.exe (PID: 3644) process within the citadeldc01.mem image, as shown in Figure 4.

- **Supporting Evidence:**

```
~/Desktop/Evidence ❯ vol -f citadeldc01.mem windows.dlllist --pid 3644
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
PID     Process Base    Size    Name    Path    LoadTime        File output
```

Figure 4. Volatility 3 windows.dlllist (specifically for PID: 3644) of citadeldc01.mem

5. Are there any handles for this process? If so, how many File handles are there?

- **Analysis Performed:**
  - The examiner used Volatility 3 via the command line shown in Figure 5, to extract the information of whether there are any handles for the coreupdater.exe (PID: 3644) process of the dc01 image.
  - Command: *vol -f citadeldc01.mem windows.handles --pid 3644*
- **Answer:**
  There are **no** handles for the coreupdater.exe (PID: 3644) process as shown in Figure 5.

- **Supporting Evidence:**

```
~/Desktop/Evidence ❯ vol -f citadeldc01.mem windows.handles --pid 3644
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
PID     Process Offset  HandleValue     Type    GrantedAccess   Name
```

Figure 5. Volatility 3 windows.handle (specifically for PID: 3644) of citadeldc01.mem

6. Attempt to dump the process from memory based on its PID. Was in successful?

- **Analysis Performed:**
  - The examiner used Volatility 3 via the command line shown in Figure 6, to dump the process from memory, based on its PID.
  - Command: *vol -f citadeldc01.mem windows.dumpfiles --pid 3644*
- **Answer:**
  No, the attempt to dump the process (coreupdater.ex) from memory, based on its PID (3644), was **unsuccessful**, as shown in Figure 6.

- **Supporting Evidence:**

```
~/Desktop/Evidence ❯ vol -f citadeldc01.mem windows.dumpfiles --pid 3644
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result


took 3s
```

Figure 6. Volatility 3 windows.dumpfiles of the coreupdater.ex (PID: 3644) process in citadeldc01.mem

7. What do you think happened to this process?

- **Analysis Performed:**
  - The examiner examined and analyzed the conclusions drawn from answering Questions 3-6, as shown in Figure 7. Additionally, the examiner utilized OSINT.
- **Answer:**
  Based off the information collected in Questions 3-6, **the examiner believes that the process was deleted from the system.** As shown in Figure 3 and 7, this process has an exit date timestamp of 2020-09-19 03:56:52 UTC, which is when it was terminated. As shown in Figure 4 and 7, this process has no DLLs associated with it. As shown in Figure 5 and 7, this process has no handles associated with it. As shown in Figure 6 and 7, the examiner attempted to dump the process via memory however, it did not work. **All these things are similar to what would happen when you conduct memory forensics on a process that has been deleted.**

- **Supporting Evidence:**

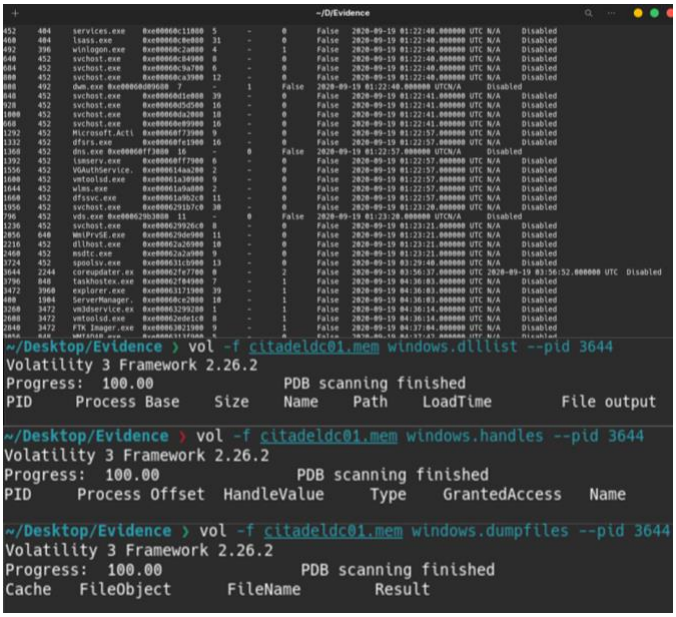

Figure 7. A compilation of all the screenshots from Questions 3-6

8. Are there any other processes that have an exit time?

- **Analysis Performed:**
  - The examiner used Volatility 3 via the command line shown in Figure 8, to examine all of the processes that were on the dc01 machine.
  - Command: *vol -f citadeldc01.mem windows.pslist*
- **Answer:**
  There are **no** other processes that have an exit time, as shown in Figure 8.

- **Supporting Evidence:**

```
~/Desktop/Evidence ❯ vol -f citadeldc01.mem windows.pslist
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0xe0005f273040  98      -       N/A     False   2020-09-19 01:22:38.000000 UTC  N/A     Disabled
204     4       smss.exe        0xe00060354900  2       -       N/A     False   2020-09-19 01:22:38.000000 UTC  N/A     Disabled
324     316     csrss.exe       0xe000602c2080  8       -       0       False   2020-09-19 01:22:39.000000 UTC  N/A     Disabled
404     316     wininit.exe     0xe000602cc900  1       -       0       False   2020-09-19 01:22:40.000000 UTC  N/A     Disabled
412     396     csrss.exe       0xe000602c1900  10      -       1       False   2020-09-19 01:22:40.000000 UTC  N/A     Disabled
452     404     services.exe    0xe00060c11080  5       -       0       False   2020-09-19 01:22:40.000000 UTC  N/A     Disabled
460     404     lsass.exe       0xe00060c0e080  31      -       0       False   2020-09-19 01:22:40.000000 UTC  N/A     Disabled
492     396     winlogon.exe    0xe00060c2a080  4       -       1       False   2020-09-19 01:22:40.000000 UTC  N/A     Disabled
640     452     svchost.exe     0xe00060c84900  8       -       0       False   2020-09-19 01:22:40.000000 UTC  N/A     Disabled
684     452     svchost.exe     0xe00060c9a700  6       -       0       False   2020-09-19 01:22:40.000000 UTC  N/A     Disabled
800     452     svchost.exe     0xe00060ca3900  12      -       0       False   2020-09-19 01:22:40.000000 UTC  N/A     Disabled
808     492     dwm.exe 0xe00060d09680  7       -       1       False   2020-09-19 01:22:40.000000 UTC  N/A     Disabled
848     452     svchost.exe     0xe00060d1e080  39      -       0       False   2020-09-19 01:22:41.000000 UTC  N/A     Disabled
928     452     svchost.exe     0xe00060d5d500  16      -       0       False   2020-09-19 01:22:41.000000 UTC  N/A     Disabled
1000    452     svchost.exe     0xe00060da2080  18      -       0       False   2020-09-19 01:22:41.000000 UTC  N/A     Disabled
668     452     svchost.exe     0xe00060e09900  16      -       0       False   2020-09-19 01:22:41.000000 UTC  N/A     Disabled
1292    452     Microsoft.Acti  0xe00060f73900  9       -       0       False   2020-09-19 01:22:57.000000 UTC  N/A     Disabled
1332    452     dfsrs.exe       0xe00060fe1900  16      -       0       False   2020-09-19 01:22:57.000000 UTC  N/A     Disabled
1368    452     dns.exe 0xe00060ff3080  16      -       0       False   2020-09-19 01:22:57.000000 UTC  N/A     Disabled
1392    452     ismserv.exe     0xe00060ff7900  6       -       0       False   2020-09-19 01:22:57.000000 UTC  N/A     Disabled
1556    452     VGAuthService.  0xe000614aa200  2       -       0       False   2020-09-19 01:22:57.000000 UTC  N/A     Disabled
1600    452     vmtoolsd.exe    0xe00061a30900  9       -       0       False   2020-09-19 01:22:57.000000 UTC  N/A     Disabled
1644    452     wlms.exe        0xe00061a9a800  2       -       0       False   2020-09-19 01:22:57.000000 UTC  N/A     Disabled
1660    452     dfssvc.exe      0xe00061a9b2c0  11      -       0       False   2020-09-19 01:22:57.000000 UTC  N/A     Disabled
1956    452     svchost.exe     0xe0006291b7c0  30      -       0       False   2020-09-19 01:23:20.000000 UTC  N/A     Disabled
796     452     vds.exe 0xe000629b3080  11      -       0       False   2020-09-19 01:23:20.000000 UTC  N/A     Disabled
1236    452     svchost.exe     0xe000629926c0  8       -       0       False   2020-09-19 01:23:21.000000 UTC  N/A     Disabled
2056    640     WmiPrvSE.exe    0xe000629de900  11      -       0       False   2020-09-19 01:23:21.000000 UTC  N/A     Disabled
2216    452     dllhost.exe     0xe00062a26900  10      -       0       False   2020-09-19 01:23:21.000000 UTC  N/A     Disabled
2460    452     msdtc.exe       0xe00062a2a900  9       -       0       False   2020-09-19 01:23:21.000000 UTC  N/A     Disabled
3724    452     spoolsv.exe     0xe000631cb900  13      -       0       False   2020-09-19 03:29:40.000000 UTC  N/A     Disabled
3644    2244    coreupdater.ex  0xe00062fe7700  0       -       2       False   2020-09-19 03:56:37.000000 UTC  2020-09-19 03:56:52.000000 UTC  Disabled
3796    848     taskhostex.exe  0xe00062f04900  7       -       1       False   2020-09-19 04:36:03.000000 UTC  N/A     Disabled
3472    3960    explorer.exe    0xe00063171900  39      -       1       False   2020-09-19 04:36:03.000000 UTC  N/A     Disabled
400     1904    ServerManager.  0xe00060ce2080  10      -       1       False   2020-09-19 04:36:03.000000 UTC  N/A     Disabled
3260    3472    vm3dservice.ex  0xe00063299280  1       -       1       False   2020-09-19 04:36:14.000000 UTC  N/A     Disabled
2608    3472    vmtoolsd.exe    0xe00062ede1c0  8       -       1       False   2020-09-19 04:36:14.000000 UTC  N/A     Disabled
2840    3472    FTK Imager.exe  0xe00063021900  9       -       1       False   2020-09-19 04:37:04.000000 UTC  N/A     Disabled
3056    848     WMIADAP.exe     0xe0006313f900  5       -       0       False   2020-09-19 04:37:42.000000 UTC  N/A     Disabled
2764    640     WmiPrvSE.exe    0xe00062c0a900  6       -       0       False   2020-09-19 04:37:42.000000 UTC  N/A     Disabled
```

Figure 8. The entire Volatility 3 windows.pslist output for citadeldc01.mem

9. In your previous assignment, you discovered evidence of an application that crashed. Is this application present in the process list? If so, what is the PID, PPID, name, and time it started (created) and exited execution? (Hint: review question 39)

- **Analysis Performed:**
  - The examiner used Volatility 3 via the command line shown in Figure 9, to extract the processes (pslist) of the dc01 image.
  - Command: *vol -f citadeldc01.mem windows.pslist*
- **Answer:**
  The **spoolsv.exe** application (discovered in the previous assignment that the application crashed) is present in the process list (pslist) and the PID is **3724**, PPID is **452**, name is **spoolsv.exe**, created date timestamp is **2020-09-19 03:29:40 UTC**, and exited date timestamp is **N/A**, as shown in Figure 9.

- **Supporting Evidence:**

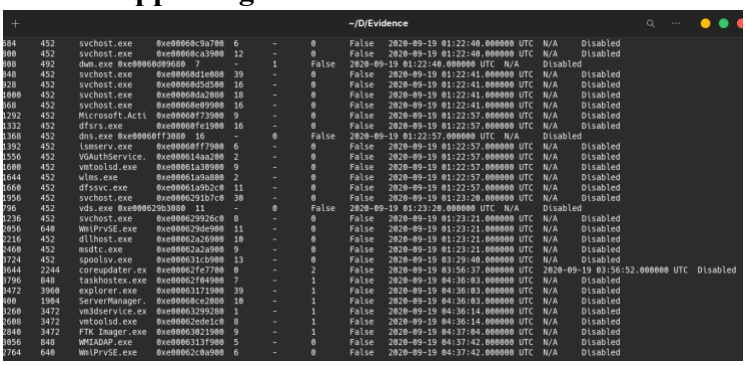

Figure 9. Volatility 3 windows.pslist for citadeldc01.mem

10. Do some research on this process name. What is it? Is it legitimate?

- **Analysis Performed:**
  - The examiner used OSINT (Google.com) to search the process name, spoolsv.exe.
  - Website: *https://www.computerhope.com/issues/ch000914.htm*
- **Answer:**
  The spoolsv.exe process is a Windows file that is responsible for how Windows handles print and fax jobs on Windows computers and it is not spyware, a trojan, or a virus, as shown in Figure 10.

- **Supporting Evidence:**

Figure 10. Info about spoolsv.exe from https://www.computerhope.com/issues/ch000914.htm

11. Are there any DLLs mapped to this process? Are any of them outside of Windows?

- **Analysis Performed:**
  - The examiner used Volatility 3 via the command line shown in Figure 11, to extract the DLLs mapped to the spoolsv.exe (PID: 3724) process of the dc01 image.
  - Command: *vol -f citadeldc01.mem windows.dlllist --pid 3724*
- **Answer:**
  There are **83** DLLs mapped to the spoolsv.exe (PID: 3724) process within the citadeldc01.mem image, as shown in Figure 4. **None** of them are outside of Windows.

- **Supporting Evidence:**

~/D/Evidence

```
3724    spoolsv.exe     0x7fffda3e0000  0xa000  kernel.appcore.dll      C:\Windows\SYSTEM32\kernel.appcore.dll  2020-09-19 03:29:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffdc130000  0xa000  CRYPTBASE.dll   C:\Windows\System32\CRYPTBASE.dll       2020-09-19 03:29:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffdc0d0000  0x60000 bcryptPrimitives.dll    C:\Windows\System32\bcryptPrimitives.dll        2020-09-19 03:29:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffdc0a0000  0x2b000 sspicli.dll     C:\Windows\System32\sspicli.dll 2020-09-19 03:29:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffdba60000  0x58000 mswsock.dll     C:\Windows\System32\mswsock.dll 2020-09-19 03:29:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffd6fa0000  0x6b000 clusapi.dll     C:\Windows\System32\clusapi.dll 2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffdbbd0000  0x18000 cryptdll.dll    C:\Windows\System32\cryptdll.dll        2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffdd7c0000  0xa5000 advapi32.dll    C:\Windows\SYSTEM32\advapi32.dll        2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffdb110000  0x29000 IPHLPAPI.DLL    C:\Windows\System32\IPHLPAPI.DLL        2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffdad10000  0xa000  WINNSI.DLL      C:\Windows\System32\WINNSI.DLL  2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffd78f0000  0x9000  rasadhlp.dll    C:\Windows\System32\rasadhlp.dll        2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffd7ca0000  0x67000 fwpuclnt.dll    C:\Windows\System32\fwpuclnt.dll        2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffc0200000  0xfd000 localspl.dll    C:\Windows\System32\localspl.dll        2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffdbe00000  0x25000 srvcli.dll      C:\Windows\System32\srvcli.dll  2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffdc6b0000  0x4a000 cfgmgr32.dll    C:\Windows\SYSTEM32\cfgmgr32.dll        2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffdbac0000  0x1e000 CRYPTSP.dll     C:\Windows\System32\CRYPTSP.dll 2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffcc4a0000  0x12000 SPOOLSS.DLL     C:\Windows\System32\SPOOLSS.DLL 2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffdc7c0000  0x1d4000        SETUPAPI.dll    C:\Windows\system32\SETUPAPI.dll        2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffcc9a0000  0x7b000 winspool.drv    C:\Windows\system32\winspool.drv        2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffcc2f0000  0x12000 PrintIsolationProxy.dll C:\Windows\System32\PrintIsolationProxy.dll     2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffca300000  0x36000 tcpmon.dll      C:\Windows\System32\tcpmon.dll  2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffcd270000  0xc000  snmpapi.dll     C:\Windows\System32\snmpapi.dll 2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffcc160000  0x13000 wsnmp32.dll     C:\Windows\System32\wsnmp32.dll 2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffc9930000  0x49000 usbmon.dll      C:\Windows\System32\usbmon.dll  2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffdc700000  0xb7000 OLEAUT32.dll    C:\Windows\system32\OLEAUT32.dll        2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffda5b0000  0x26000 DEVOBJ.dll      C:\Windows\system32\DEVOBJ.dll  2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffdc4a0000  0x4c000 WINTRUST.dll    C:\Windows\system32\WINTRUST.dll        2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffdc2c0000  0x1d7000        CRYPT32.dll     C:\Windows\system32\CRYPT32.dll 2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffdc2a0000  0x12000 MSASN1.dll      C:\Windows\system32\MSASN1.dll  2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffc5ab0000  0x4c000 WSDMon.dll      C:\Windows\System32\WSDMon.dll  2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffc0160000  0x9b000 wsdapi.dll      C:\Windows\System32\wsdapi.dll  2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffbfd90000  0x15f000        webservices.dll C:\Windows\System32\webservices.dll     2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffda640000  0xb6000 FirewallAPI.dll C:\Windows\System32\FirewallAPI.dll     2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffdd8e0000  0xa4000 clbcatq.dll     C:\Windows\SYSTEM32\clbcatq.dll 2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffcb9f0000  0x28000 FunDisc.dll     C:\Windows\System32\FunDisc.dll 2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffd82b0000  0x38000 XmlLite.dll     C:\Windows\System32\XmlLite.dll 2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffcafe0000  0x11000 fdPnp.dll       C:\Windows\System32\fdPnp.dll   2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffd8830000  0x1b000 ATL.DLL C:\Windows\System32\ATL.DLL     2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffcc230000  0xb9000 drvstore.dll    C:\Windows\system32\drvstore.dll        2020-09-19 03:31:40.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffcd1d0000  0xe000  winprint.dll    C:\Windows\system32\spool\PRTPROCS\x64\winprint.dll     2020-09-19 03:31:41.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffdb810000  0x1f000 USERENV.dll     C:\Windows\System32\USERENV.dll 2020-09-19 03:31:41.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffdc1f0000  0x14000 profapi.dll     C:\Windows\System32\profapi.dll 2020-09-19 03:31:41.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffda910000  0x23000 gpapi.dll       C:\Windows\SYSTEM32\gpapi.dll   2020-09-19 03:31:41.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffdada0000  0xa000  VERSION.dll     C:\Windows\System32\VERSION.dll 2020-09-19 03:31:41.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffdaa90000  0x9000  DSROLE.dll      C:\Windows\System32\DSROLE.dll  2020-09-19 03:31:41.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffbd820000  0xc9000 win32spl.dll    C:\Windows\System32\win32spl.dll        2020-09-19 03:31:41.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffcc140000  0x14000 DEVRTL.dll      C:\Windows\system32\DEVRTL.dll  2020-09-19 03:31:41.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffdbdb0000  0x1d000 SPINF.dll       C:\Windows\System32\SPINF.dll   2020-09-19 03:31:41.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffdb5b0000  0x57000 WINSTA.dll      C:\Windows\System32\WINSTA.dll  2020-09-19 03:31:41.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffdb720000  0x35000 rsaenh.dll      C:\Windows\System32\rsaenh.dll  2020-09-19 03:31:41.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffdbdd0000  0x26000 bcrypt.dll      C:\Windows\System32\bcrypt.dll  2020-09-19 03:31:41.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffd6f40000  0x10000 cscapi.dll      C:\Windows\System32\cscapi.dll  2020-09-19 03:31:41.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffdaa30000  0xc000  netutils.dll    C:\Windows\System32\netutils.dll        2020-09-19 03:31:41.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffd80d0000  0x11000 WTSAPI32.dll    C:\Windows\System32\WTSAPI32.dll        2020-09-19 03:56:04.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffd25b0000  0x230000        WININET.dll     C:\Windows\System32\WININET.dll 2020-09-19 03:56:52.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffd27e0000  0x2a9000        iertutil.dll    C:\Windows\System32\iertutil.dll        2020-09-19 03:56:52.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffd0a70000  0xc5000 WINHTTP.dll     C:\Windows\System32\WINHTTP.dll 2020-09-19 03:56:52.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffdc9a0000  0x178000        ole32.dll       C:\Windows\system32\ole32.dll   2020-09-19 03:56:52.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffcec10000  0x1b000 MPR.dll C:\Windows\System32\MPR.dll     2020-09-19 03:56:52.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffd8850000  0x15000 NETAPI32.dll    C:\Windows\System32\NETAPI32.dll        2020-09-19 03:56:52.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffd9ec0000  0x16000 wkscli.dll      C:\Windows\System32\wkscli.dll  2020-09-19 03:56:52.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffdd8d0000  0x7000  PSAPI.DLL       C:\Windows\system32\PSAPI.DLL   2020-09-19 03:56:52.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffcfb60000  0x1f000 WINMM.dll       C:\Windows\System32\WINMM.dll   2020-09-19 03:56:52.000000 UTC  Disabled
3724    spoolsv.exe     0x7fffcfa30000  0x2a000 WINMMBASE.dll   C:\Windows\System32\WINMMBASE.dll       2020-09-19 03:56:52.000000 UTC  Disabled
```

Figure 11. Volatility 3 windows.dlllist (specifically for spoolsv.exe (PID: 3724) of citadeldc01.mem

12. Are there any handles for this process? If so, how many File handles are there?

- **Analysis Performed:**
  - The examiner used Volatility 3 via the command line shown in Figure 12, to extract the handles for the spoolsv.exe (PID: 3724) process of the dc01 image.
  - Command 1: *vol -f citadeldc01.mem windows.handles --pid 3724*
  - Command 2: *vol -f citadeldc01.mem windows.handles --pid 3724 | grep -i "spoolsv.exe" | wc -l*
- **Answer:**
  Yes, there are **410** handles for the spoolsv.exe (PID: 3724) process of citadeldc01.mem, as shown in Figure 12.

- **Supporting Evidence:**

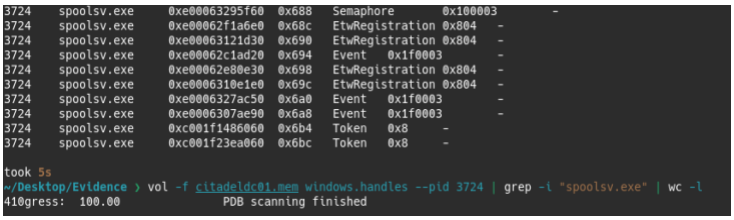

Figure 12. Volatility window.handles and the count (specifically for spoolsv.exe, PID: 3724) for citadeldc01.mem

13. Are there any mutants for this process? How many actually have data?

- **Analysis Performed:**
  - The examiner used Volatility 3 via the command line shown in Figure 13, to extract the mutant handles for the spoolsv.exe (PID: 3724) process of the dc01 image.
  - Command 1: *vol -f citadeldc01.mem windows.handles --pid 3724 | grep -i "Mutant" | wc -l*
  - Command 2: *vol -f citadeldc01.mem windows.handles --pid 3724 | grep -i "Mutant"*
- **Answer:**
  There are **14 mutant handles** for the spoolsv.exe (PID: 3724) process, as shown in Figure 13. None of them have any data as shown in Figure 13.

- **Supporting Evidence:**

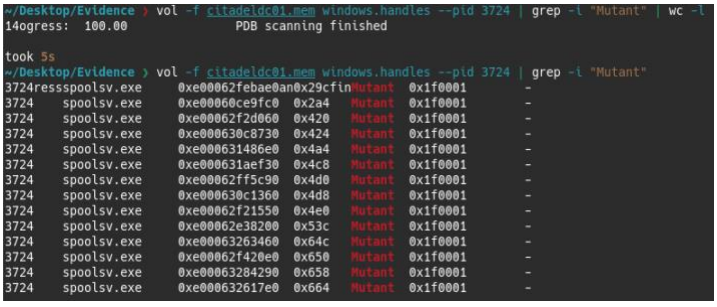

Figure 13. Volatility 3 windows.handles (specifically for spoolsv.exe, PID: 3724) looking for Mutant handles for citadeldc01.mem

14. Review network connections from the system (netscan and netstat). Did any of the above processes have an "ESTABLISHED" connection? If so, what is the process name and what remote IP address and port was it connected to?

- **Analysis Performed:**
  - The examiner used Volatility 3 via the command line shown in Figure 14, to see if there is an "ESTABLISHED" connection for the spoolsv.exe and coreupdater.exe processes shown before.
  - Command 1: *vol -f citadeldc01.mem windows.netscan | grep -i "ESTABLISHED" | grep -i "coreupdater.ex"*
  - Command 2: *vol -f citadeldc01.mem windows.netscan | grep -i "ESTABLISHED" | grep -i "spoolsv.exe"*
- **Answer:**
  The coreupdater.ex process has two "ESTABLISHED" connections, as shown in Figure 14. The remote IP address and port that it was connected to for both connections is **203.78.103.109 on port 443**, as shown in Figure 14.

- **Supporting Evidence:**

```
~/Desktop/Evidence ❯ vol -f citadeldc01.mem windows.netscan | grep -i "ESTABLISHED" | grep -i "coreupdater.ex"
0x20fc7590 100.0TCPv4   10.42.85.10 scan62613fin203.78.103.109  443     ESTABLISHED     3644    coreupdater.ex  N/A
0x60182590      TCPv4   10.42.85.10     62613   203.78.103.109  443     ESTABLISHED     3644    coreupdater.ex  N/A

took 47s
~/Desktop/Evidence ❯ vol -f citadeldc01.mem windows.netscan | grep -i "ESTABLISHED" | grep -i "spoolsv.exe"

took 47s
```

Figure 14. Volatility 3 windows.netscan looking specifically for coreupdate.ex and spoolsv.exe and if they have an established connection for citadeldc01.mem

15. Run malfind. Are there any processes that have suspicious memory sections from previous questions? If so, how many sections were found and do any of them contain code (i.e. MZ header)? Dump all sections using the "–pid PID and –dump" arguments.

- **Analysis Performed:**
  - The examiner used Volatility 3 via the command line shown in Figures 15 and 16, to find any processes that have suspicious memory sections.
  - Command 1: *vol -f citadeldc01.mem windows.malfind --pid 3644 --dump*
  - Command 2: *vol -f citadeldc01.mem windows.malfind --pid 3724 --dump*
- **Answer:**
  coreupdater.exe does **not** have any suspicious memory sections as shown in Figure 15. spoolsv.exe does have **four sections** of suspicious memory sections and three of the sections contains code (MZ header), as shown in Figure 16.

- **Supporting Evidence:**

Figure 15. Volatility 3 windows.malfind (specifically for PID: 3644) for citadeldc01.mem

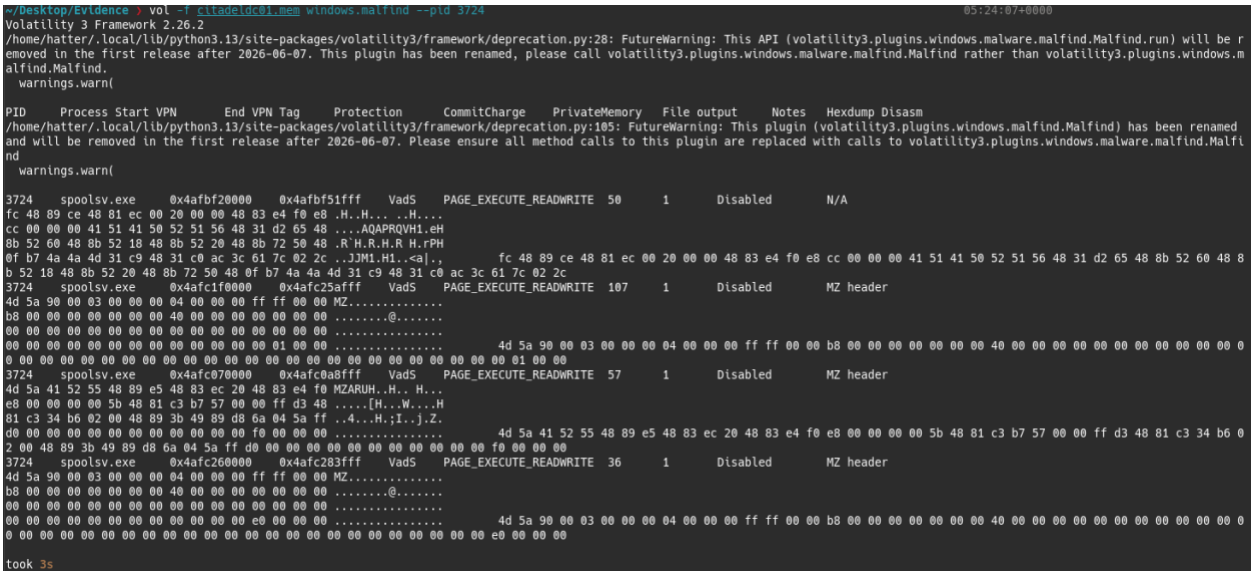

Figure 16. Volatility 3 windows.malfind (specifically for PID: 3724) for citadeldc01.mem

16. Run the file command on all dumped malfind files. What is the output of each file?

- **Analysis Performed:**
  - The examiner used the file command via the command line shown in Figure 17, to examine the output of each file.
  - Command 1: *file pid.3724.vad.0x4afbf20000-0x4afbf51fff.dmp*
  - Command 2: *file pid.3724.vad.0x4afc1f0000-0x4afc25afff.dmp*
  - Command 3: *file pid.3724.vad.0x4afc070000-0x4afc0a8fff.dmp*
  - Command 4: *file pid.3724.vad.0x4afc260000-0x4afc283fff.dmp*
- **Answer:**
  The output for the "pid.3724.vad.0x4afbf20000-0x4afbf51fff.dmp" file is **data**, as shown in Figure 17. The output for the "pid.3724.vad.0x4afc1f0000-0x4afc25afff.dmp" file is **PE32+ executable for MS Windows 5.02 (DLL), x86-64, 6 sections**, as shown in Figure 17. The output for the "0x4afc070000-0x4afc0a8fff.dmp" file is **PE32+ executable for MS Windows 5.02 (DLL), x86-64, 6 sections**, as shown in Figure 17. The output for the "0x4afc260000-0x4afc283fff.dmp" file is **PE32+ executable for MS Windows 5.02 (DLL), x86-64, 6 sections**, as shown in Figure 17.

- **Supporting Evidence:**

```
~/Desktop/Evidence ❯ file pid.3724.vad.0x4afbf20000-0x4afbf51fff.dmp
pid.3724.vad.0x4afbf20000-0x4afbf51fff.dmp: data


~/Desktop/Evidence ❯ file pid.3724.vad.0x4afc1f0000-0x4afc25afff.dmp
pid.3724.vad.0x4afc1f0000-0x4afc25afff.dmp: PE32+ executable for MS Windows 5.02 (DLL), x86-64, 6 sections


~/Desktop/Evidence ❯ file pid.3724.vad.0x4afc070000-0x4afc0a8fff.dmp
pid.3724.vad.0x4afc070000-0x4afc0a8fff.dmp: PE32+ executable for MS Windows 5.02 (DLL), x86-64, 5 sections


~/Desktop/Evidence ❯ file pid.3724.vad.0x4afc260000-0x4afc283fff.dmp
pid.3724.vad.0x4afc260000-0x4afc283fff.dmp: PE32+ executable for MS Windows 5.02 (DLL), x86-64, 5 sections
```

Figure 17. file command of the four sections of dumped malfind

17. Run clamscan on all the dumped malfind files. What are the detections for each file?

- **Analysis Performed:**
  - The examiner used the clamscan command via the command line shown in Figures 18-21, to examine the ClamAV detections of each file.
  - Command 1: *clamscan pid.3724.vad.0x4afbf20000-0x4afbf51fff.dmp*
  - Command 2: *clamscan pid.3724.vad.0x4afc1f0000-0x4afc25afff.dmp*
  - Command 3: *clamscan pid.3724.vad.0x4afc070000-0x4afc0a8fff.dmp*
  - Command 4: *clamscan pid.3724.vad.0x4afc260000-0x4afc283fff.dmp*
- **Answer:**
  Using clamscan within ClamAV, it detected that pid.3724.vad.0x4afbf20000-0x4afbf51fff.dmp found "**Win.Exploit.Meterpreter-9752338-0**", as shown in Figure 18. Clamscan detected that pid.3724.vad.0x4afc1f0000-0x4afc25afff.dmp found "**Win.Malware.Meterpreter-9872014-0**", as shown in Figure 19. Clamscan detected that pid.3724.vad.0x4afc070000-0x4afc0a8fff.dmp found "**Win.Exploit.Meterpreter-9752338-0**", as shown in Figure 20. Clamscan detected that pid.3724.vad.0x4afc260000-0x4afc283fff.dmp found "**Win.Malware.Razy-9865903-0"**, as shown in Figure 21.

- **Supporting Evidence:**

```
~/Desktop/Evidence ❯ clamscan pid.3724.vad.0x4afbf20000-0x4afbf51fff.dmp
Loading:    19s, ETA:   0s [=========================>]    8.71M/8.71M sigs
Compiling:   3s, ETA:   0s [=========================>]       41/41 tasks

/home/hatter/Desktop/Evidence/pid.3724.vad.0x4afbf20000-0x4afbf51fff.dmp: Win.Exploit.Meterpreter-9752338-0 FOUND

----------- SCAN SUMMARY -----------
Known viruses: 8708684
Engine version: 1.4.3
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.20 MB
Data read: 0.20 MB (ratio 1.02:1)
Time: 24.333 sec (0 m 24 s)
Start Date: 2025:11:06 05:41:11
End Date:   2025:11:06 05:41:36
```

Figure 18. clamscan output for pid.3724.vad.0x4afbf20000-0x4afbf51fff.dmp

```
~/Desktop/Evidence ❯ clamscan pid.3724.vad.0x4afc1f0000-0x4afc25afff.dmp
Loading:    18s, ETA:   0s [=========================>]    8.71M/8.71M sigs
Compiling:   3s, ETA:   0s [=========================>]       41/41 tasks

/home/hatter/Desktop/Evidence/pid.3724.vad.0x4afc1f0000-0x4afc25afff.dmp: Win.Malware.Meterpreter-9872014-0 FOUND

----------- SCAN SUMMARY -----------
Known viruses: 8708684
Engine version: 1.4.3
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.44 MB
Data read: 0.42 MB (ratio 1.05:1)
Time: 22.719 sec (0 m 22 s)
Start Date: 2025:11:06 05:43:24
End Date:   2025:11:06 05:43:47
```

Figure 19. clamscan output for pid.3724.vad.0x4afc1f0000-0x4afc25afff.dmp

```
~/Desktop/Evidence ❯ clamscan pid.3724.vad.0x4afc070000-0x4afc0a8fff.dmp
Loading:    18s, ETA:   0s [=========================>]    8.71M/8.71M sigs
Compiling:   2s, ETA:   0s [=========================>]       41/41 tasks

/home/hatter/Desktop/Evidence/pid.3724.vad.0x4afc070000-0x4afc0a8fff.dmp: Win.Exploit.Meterpreter-9752338-0 FOUND

----------- SCAN SUMMARY -----------
Known viruses: 8708684
Engine version: 1.4.3
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.23 MB
Data read: 0.22 MB (ratio 1.02:1)
Time: 22.080 sec (0 m 22 s)
Start Date: 2025:11:06 05:45:13
End Date:   2025:11:06 05:45:35
```

Figure 20. clamscan output for pid.3724.vad.0x4afc070000-0x4afc0a8fff.dmp

```
~/Desktop/Evidence ❯ clamscan pid.3724.vad.0x4afc260000-0x4afc283fff.dmp
Loading:    18s, ETA:   0s [=========================>]    8.71M/8.71M sigs
Compiling:   3s, ETA:   0s [=========================>]       41/41 tasks

/home/hatter/Desktop/Evidence/pid.3724.vad.0x4afc260000-0x4afc283fff.dmp: Win.Malware.Razy-9865903-0 FOUND

----------- SCAN SUMMARY -----------
Known viruses: 8708684
Engine version: 1.4.3
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.14 MB
Data read: 0.14 MB (ratio 1.03:1)
Time: 22.988 sec (0 m 22 s)
Start Date: 2025:11:06 05:46:03
End Date:   2025:11:06 05:46:26
```

Figure 21. clamscan output for pid.3724.vad.0x4afc260000-0x4afc283fff.dmp

18. Run FLOSS on all files, there is an IP address in one of the files lsat the end of the output. What file contains the IP address?

- **Analysis Performed:**
  - The examiner used the FLOSS command via the command line shown in Figure 22, to find the IP address at the end of the output.
  - Command: *floss pid.3724.vad.0x4afbf20000-0x4afbf51fff.dmp*
- **Answer:**
  The file that contains the IP address is **pid.3724.vad.0x4afbf20000-0x4afbf51fff.dmp**, as shown in Figure 22. The IP address is **203.78.103.109**.

- **Supporting Evidence:**

```
sr-sp-latn
sv-fi
sv-se
sw-ke
syr-sy
ta-in
te-in
th-th
tn-za
tr-tr
tt-ru
uk-ua
ur-pk
uz-uz-cyrl
uz-uz-latn
vi-vn
xh-za
zh-chs
zh-cht
zh-cn
zh-hk
zh-mo
zh-sg
zh-tw
zu-za
CONOUT$
tcp://203.78.103.109:443
```

Figure 22. FLOSS output showing the IP address for pid.3724.vad.0x4afbf20000-0x4afbf51fff.dmp

19. Run capa on this file. What are the capabilities of this file? (Hint: this is shellcode, not an executable)

- **Analysis Performed:**
  - The examiner used the capa command via the command line shown in Figure 23, to find the capabilities of the file.
  - Command: *capa -f sc64 pid.3724.vad.0x4afbf20000-0x4afbf51fff.dmp*
- **Answer:**
  The capabilities of the capa.pid.3624.vad.0x4afbf20000-0x4afbf51fff.dmp file are: "**contain an embedded PE file (namespace: executable/subfile/pe)**" and "**linked against ZLIB (namespace: linking/static/zlib)**", as shown in Figure 23.

- **Supporting Evidence:**

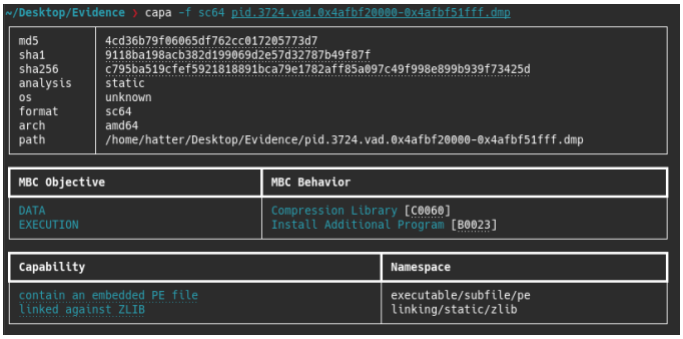

Figure 23. capa output for pid.3724.vad.0x4afbf20000-0x4afbf51fff.dmp

20. What country is the IP address from?

- **Analysis Performed:**
  - The examiner used the IP address (203.78.103.109) that was found from question 18, as shown in Figure 22.
  - The examiner used OSINT (ICANN Lookup) to find what country the IP address is from, as shown in Figure 24.
  - Website: *https://lookup.icann.org/en/lookup*
- **Answer:**
  The IP address, 203.78.103.109, is from **Thailand**, as shown in Figure 24.

- **Supporting Evidence:**

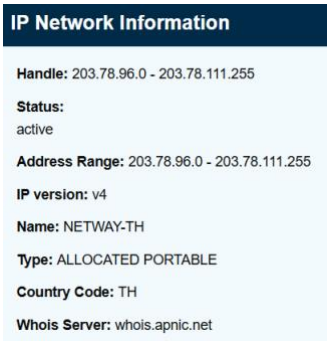

Figure 24. ICANN Lookup for the IP address (203.78.103.109)

desktop Image

21. What is the date timestamp (system time) of which this image was captured?

- **Analysis Performed:**
  - The examiner used Volatility 3 via the command line shown in Figure 25, to extract the image info of the desktop image which contains the date timestamp (system time) of which this image was captured.
  - Command: *vol -f DESKTOP-SDN1RPT.mem info.Info*
- **Answer:**
  The system time of the desktop memory image is **2020-09-19 05:10:39 UTC**, as shown in Figure 25.

- **Supporting Evidence:**

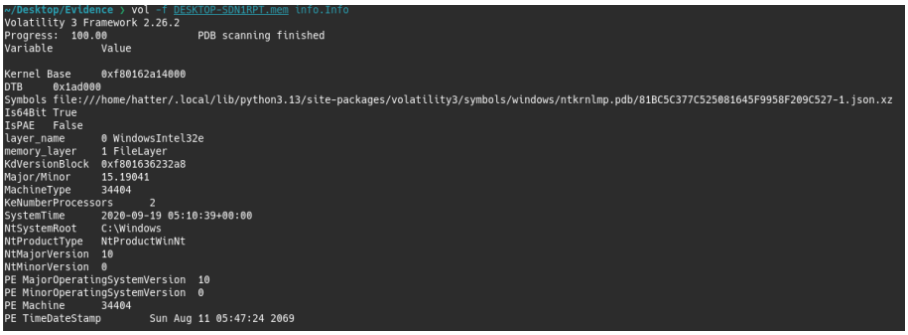

Figure 25. Volatility 3 info.Info for DESKTOP-SDN1RPT.mem

22. What is the NtMajorVersion and NtMinorVersion?

- **Analysis Performed:**
  - The examiner used Volatility 3 via the command line shown in Figure 26, to extract the image info of the desktop image which contains the NtMajorVersion and NtMinorVersion.
  - Command: *vol -f DESKTOP-SDN1RPT.mem info.Info*
- **Answer:**
  The NtMajorVersion of the memory image is **10** and the NtMinorVersion of the memory image is **0**, as shown in Figure 26.

- **Supporting Evidence:**

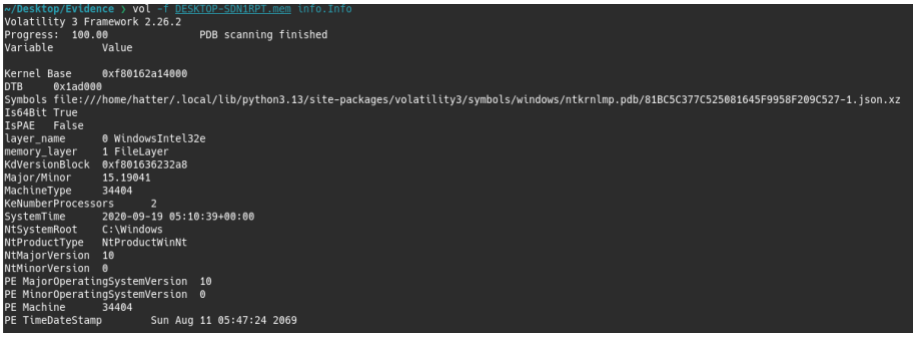

Figure 26. Volatility 3 info.info for DESKTOP-SDN1RPT.mem

23. Are the suspicious processes from the last image in this one? If so, what is the PID, PPID, name, and time it started (created) and exited execution?

- **Analysis Performed:**
  - The examiner used Volatility 3 via the command line shown in Figure 27, to find the suspicious process from the dc01 image in the desktop image.
  - Command 1: *vol -f DESKTOP-SDN1RPT.mem windows.pslist | grep -i "spoolsv.exe"*
  - *Command 2: vol -f DESKTOP-SDN1RPT.mem windows.pslist | grep -i coreupdater.ex"*
- **Answer:**
  Yes, the suspicious processes from the last image are in this one. For the spoolsv.exe process, the PID is **2188**, PPID is **616**, created date timestamp is **2020-09-19 01:24:09 UTC**, and the exited date timestamp is **N/A**, as shown in Figure 27. For the coreupdater.ex process, the PID is **8324**, PPID is **4008**, created date timestamp is **2020-09-19 03:40:49 UTC**, and exited date timestamp is **2020-09-19 03:43:10 UTC**, as shown in Figure 27.

- **Supporting Evidence:**

```
~/Desktop/Evidence ❯ vol -f DESKTOP-SDN1RPT.mem windows.pslist | grep -i "spoolsv.exe"
2188ress616100.0spoolsv.exe     0xbe8e75c2c200in10hed   -       0       False   2020-09-19 01:24:09.000000 UTC  N/A     Disabled

took 6s
~/Desktop/Evidence ❯ vol -f DESKTOP-SDN1RPT.mem windows.pslist | grep -i "coreupdater.ex"
8324ress400800.0coreupdater.ex  0xbe8e7a447080in0shed   -       3       False   2020-09-19 03:40:49.000000 UTC  2020-09-19 03:43:10.000000 UTC  Disabled
```

Figure 27. Volatility 3 windows.pslist for the desktop memory image to look for the two suspicious processes (spoolsv.exe and coreupdater.ex)

24. Are you able to recover (dump) both?

- **Analysis Performed:**
  - The examiner used Volatility 3 via the command shown in Figure 28 and 29, to dump the process from memory, based on its PID.
  - Command 1: *vol -f DESKTOP-SDN1RPT.mem -o 2188-DUMP windows.dumpfiles --pid 2188*
  - Command 2: *vol -f DESKTOP-SDN1RPT.mem -o 8324-DUMP windows.dumpfiles --pid 8324*
- **Answer:**
  The examiner was able to recover (dump) the spoolsv.exe process (PID: 2188) however, was not able to recover (dump) the coreupdater.ex process (PID: 8324), as shown in Figures 28 and 29. The examiner not being able to recover (dump) the coreupdater.ex process (PID: 8324) as shown in Figure 29 further corroborates the hypothesis that it was deleted from the system as noted in Question 7.

- **Supporting Evidence:**

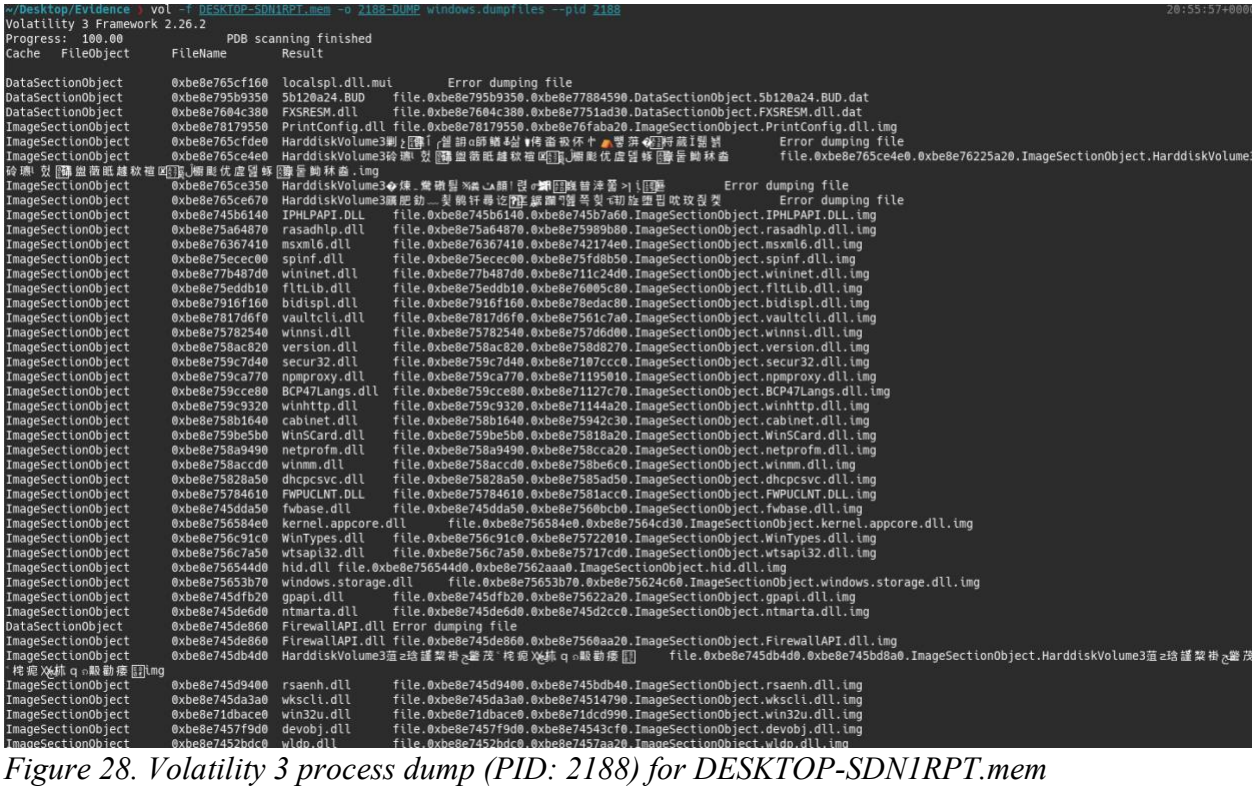

Figure 28. Volatility 3 process dump (PID: 2188) for DESKTOP-SDN1RPT.mem

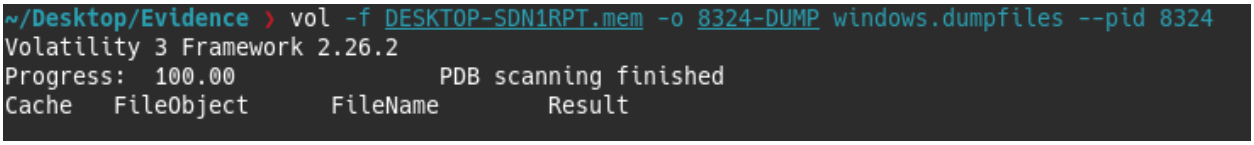

Figure 29. Volatility 3 process dump (PID: 8324) for DESKTOP-SDN1RPT.mem

25. Review the network connections. Do you see connections to the IP address from the last image? If so, what is the process name and what remote IP address and port was it connected to?

- **Analysis Performed:**
  - The examiner used Volatility 3 via the command line shown in Figure 30, to see if there is an "ESTABLISHED" connection for the IP address found in citadeldc01.mem.
  - Command: *vol -f DESKTOP-SDN1RPT.mem windows.netscan | grep -i "203.78.103.109"*
- **Answer:**
  There are **two established connections** to 203.78.103.109, as shown in Figure 30. There is **no process name** associated with the two established connections to 203.78.103.109. Additionally, the remote IP address is **203.78.103.109** on port **443**.

- **Supporting Evidence:**

```
~/Desktop/Evidence ❯ vol -f DESKTOP-SDN1RPT.mem windows.netscan | grep -i "203.78.103.109"
0xbe8e79337b20.0TCPv4   10.42.85.115scan50875fin203.78.103.109  443     ESTABLISHED     -       -       N/A
0xbe8e79f80010  TCPv4   10.42.85.115    50972   203.78.103.109  443     ESTABLISHED     -       -       N/A

took 26m10s
```

Figure 30. Volatility 3 windows netscan looking specifically for "203.78.103.109" within DESKTOP-SDN1RPT.mem

26. Run malfind. Are there any processes that have suspicious memory sections from previous questions? If so, how many sections were found and do any of them contain code (i.e. MZ header)? Dump all sections using the "–pid PID and –dump" arguments.

- **Analysis Performed:**
  - The examiner used Volatility 3 via the command line shown in Figure 31, to find any processes that have suspicious memory sections.
  - Command 1: *vol -f DESKTOP-SDN1RPT.mem windows.malfind --pid 2188 --dump*
  - Command 2: *vol -f DESKTOP-SDN1RPT.mem windows.malfind --pid 8324 --dump*
- **Answer:**
  coreupdater.exe does **not** have any suspicious memory sections as shown in Figure 31. spoolsv.exe does have **one section** of suspicious memory and the section contains code (MZ header), as shown in Figure 31.

- **Supporting Evidence:**

Figure 31. Running malfind on PIDs: 2188 and 8324, within DESKTOP-SDN1RPT.mem

27. Run the file command on all dumped malfind files. What is the output of each file?

- **Analysis Performed:**
  - The examiner used the file command via the command line shown in Figure 32, to examine the output of the dumped malfind file.
  - Command: *file pid.2188.vad.0x1840000-0x1863fff.dmp*
- **Answer:**
  The output for the "pid.2188.vad.0x1840000-0x1863fff.dmp" file is **PE32+ executable for MS Windows 5.02 (DLL), x86-64, 5 sections,** as shown in Figure 32.

- **Supporting Evidence:**

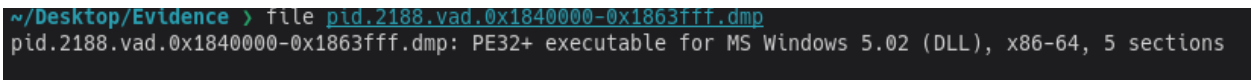

Figure 32. Running the file command on the dumped malfind file.

28. Focus on the PE files, remove the others. Run clamscan, what are the detections for each file?

- **Analysis Performed:**
  - The examiner used the clamscan command via the command line shown in Figure 33, to examine the ClamAV detections of the dumped malfind file.
  - Command: *clamscan pid.2188.vad.0x1840000-0x1863fff.dmp*
- **Answer:**
  Using clamscan within ClamAV, it detected that pid.2188.vad.0x1840000-0x1863fff.dmp, the dumped malfind file, found "**Win.Malware.Razy-9865903-0**", as shown in Figure 33.

- **Supporting Evidence:**

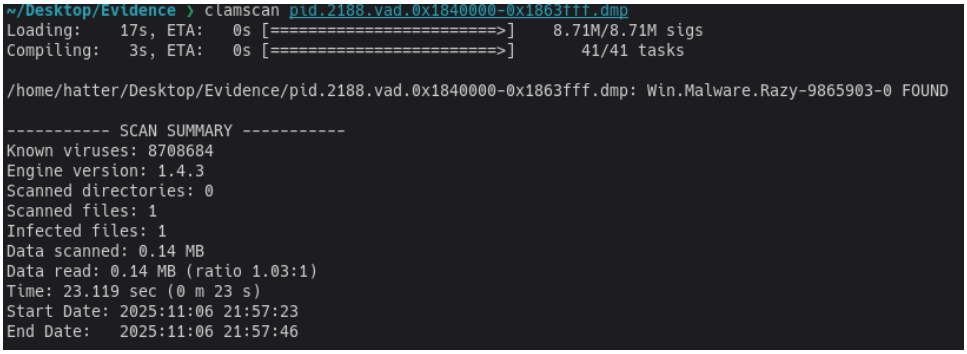

Figure 33. clamscan output for pid.2188.vad.0x1840000-0x1863fff.dmp

29. Does capa report any capabilities for either file?

- **Analysis Performed:**
  - The examiner used the capa command via the command line shown in Figure 34, to find the capabilities of the file.
  - Command: *capa -f sc64 pid.2188.vad.0x1840000-0x1863fff.dmp*
- **Answer:**
  There are **no capabilities** for the pid.2188.vad.0x1840000-0x1863fff.dmp file, as shown in Figure 34.

- **Supporting Evidence:**

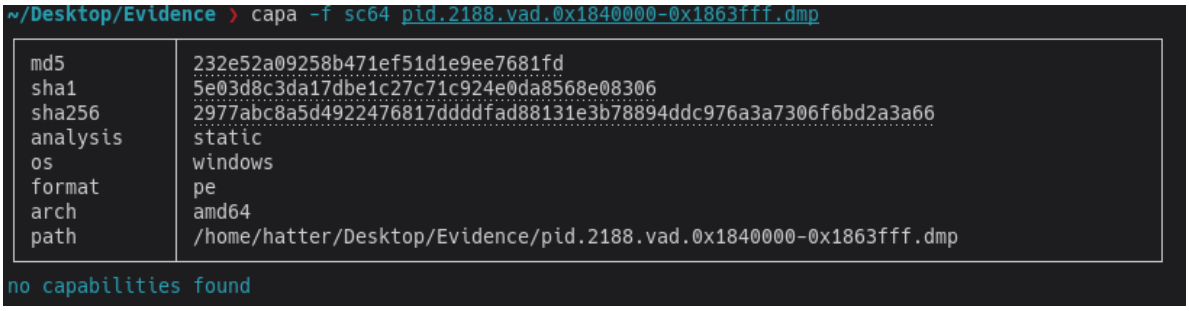

Figure 34. capa output for pid.2188.vad.0x1840000-0x1863fff.dmp

30. Do you believe this is the same malware as seen on the DC?

- **Analysis Performed:**
  - The examiner examined and analyzed the conclusions drawn from answering the questions associated with the processes, PID: 2188 and 3724, to determine if they are the same malware, as shown in Figure 35.
- **Answer:**
  Yes, the examiner believes that the DC01\spoolsv.exe (PID: 3724) and DESKTOP\spoolsv.exe (PID: 2188) are the same malware. The reason why is that both spoolsv.exe are injected with malfind-positive VADs containing code (MZ), both are PE files, and ClamAV flagged both to contain Win.Malware.Razy-9865903-0, all shown in Figure 35.

- **Supporting Evidence:**

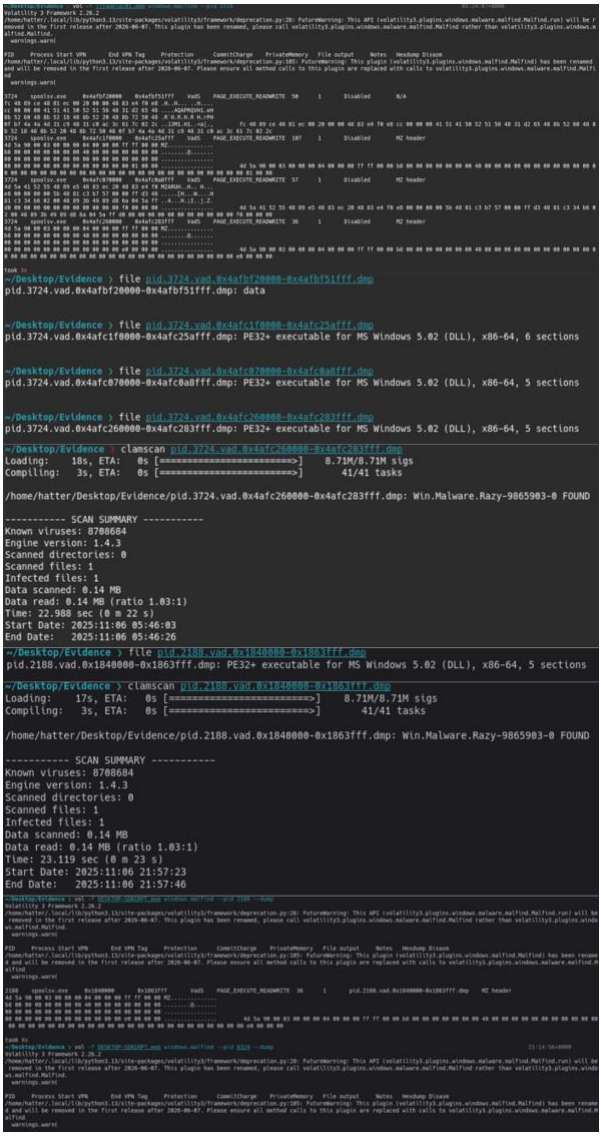

Figure 35. A compilation of the outputs for PID 3724 within dc01 and PID 2188 within desktop

Conclusion

The examiner, Inor Wang, enjoyed this lab. There is no critique from me. Thank you.

References

Carvey, H. A. (2014). Windows forensic analysis toolkit: Advanced analysis techniques for Windows 8 (Fourth edition). Syngress.

Computer Hope. (n.d.). *What is spoolsv.exe?* Retrieved November 6, 2025, from https://www.computerhope.com/issues/ch000914.htm

Internet Corporation for Assigned Names and Numbers. (n.d.). *ICANN Lookup: Registration data lookup tool.* Retrieved November 6, 2025, from https://lookup.icann.org/en/lookup

Johansen, G., & Safari, an O. M. C. (2020). Digital Forensics and Incident Response—Second Edition.

Ligh, M. H., Case, A., Levy, J., & Walters, A. (2014). The art of memory forensics: Detecting malware and threats in Windows, Linux, and Mac memory. Wiley.

Malware forensics field guide for Windows systems digital forensics field guides. (2012). Syngress.

Oettinger, W., & Safari, an O. M. C. (2020). Learn Computer Forensics.

Reddy, N. (2019). Practical cyber forensics: An incident-based approach to forensic investigations. APress. https://doi.org/10.1007/978-1-4842-4460-9.