Lab 5 – Memory and Mobile Device Forensics

Shrutika Joshi

University of Maryland Baltimore County

Presented To – Gina Marie

Date – 9th July 2023

Week 4 Discussion – 2

Memory Forensics –

Memory forensics is the process of analyzing computers memory dump for investigating an incident or collecting evidence. Memory forensics focuses on the actual programs running on a device when memory dump was captured. The memory of a device is known as Random Access Memory (RAM). When a RAM dump is captured it contains data of any running processes at the time the capture was taken. This captured memory is useful in determining the root cause of system crash, identifying malware infections, or recovering lost or deleted data. Some of the most popular tools for memory forensics are Volatility, Varc, Rekall , FTK Imager. Memory forensics involves analysis of registry files and finding evidence of user activity.

The process of memory forensics involves:

Acquiring the memory dump – This involves creating copy of computer's memory

Analyze the memory dump – This involves analyzing memory dump using analysis tools. This process is time consuming and complex and required understanding of operating system

Report the findings – This involves documenting the result of analysis.

Citations –

1. Fox, N. (2021, July 26). Memory Forensics for Incident Response. Www.varonis.com. https://www.varonis.com/blog/memory-forensics
2. Messina, G. (2019, July 5). Computer Forensics: Memory Forensics. Infosec Resources. https://resources.infosecinstitute.com/topic/computer-forensics-memory-forensics/
3. 0xffccdd. (2022, December 15). Memory Forensics Tools. Medium. https://medium.com/@cloud_tips/memory-forensics-tools-123e32387adb

---

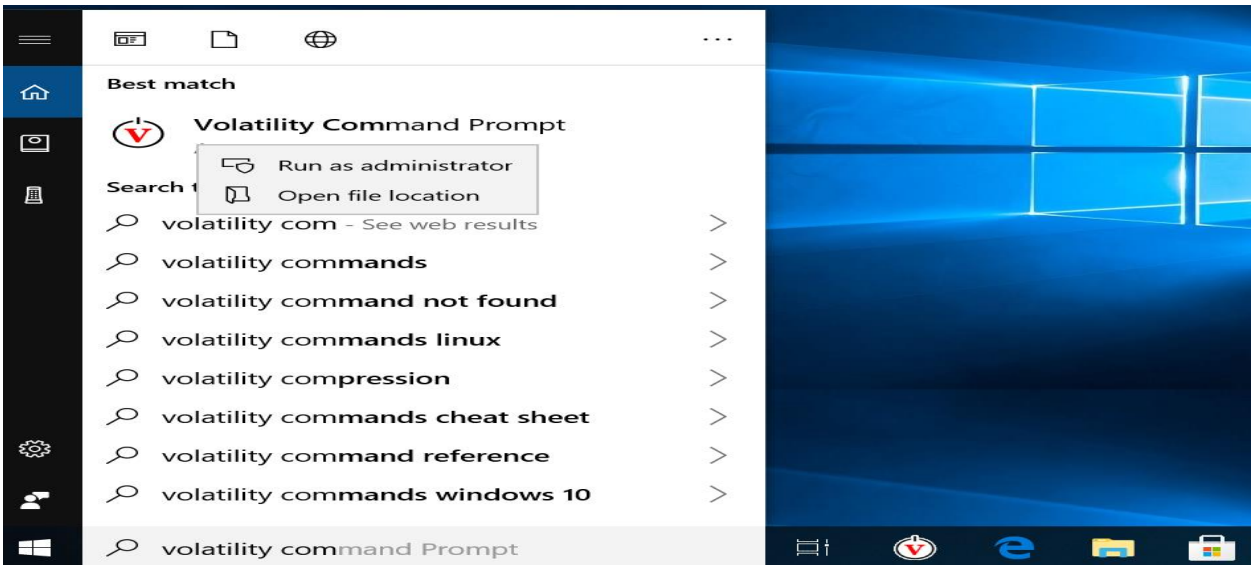
Introduction – Analyze suspicious executable and document to check whether it is malicious or not without running or opening the document using different tools. Also analyze basic dump of mobile device and network traffic captured from a mobile device using specific application.

Pre- Analysis - For this we are analyzing basic disk image of a suspicious machine. To analyze registry information we will be using Volatility tool. Also we will be using Plist and SQLiteSpy tools in mobile device forensics to analyze database and plist files. Further to analyze network traffic captured from mobile device we will be using wireshark.

Analysis –

1. **Memory Forensics with Volatility**

   - Copy the xp-laptop-2005-06-25.img file from the Evidence Drive, Memory Forensics folder into a working directory for the lab. Open Volatility by clicking the “V” icon at the bottom of the Windows task bar. Right click and select ‘Run as administrator’



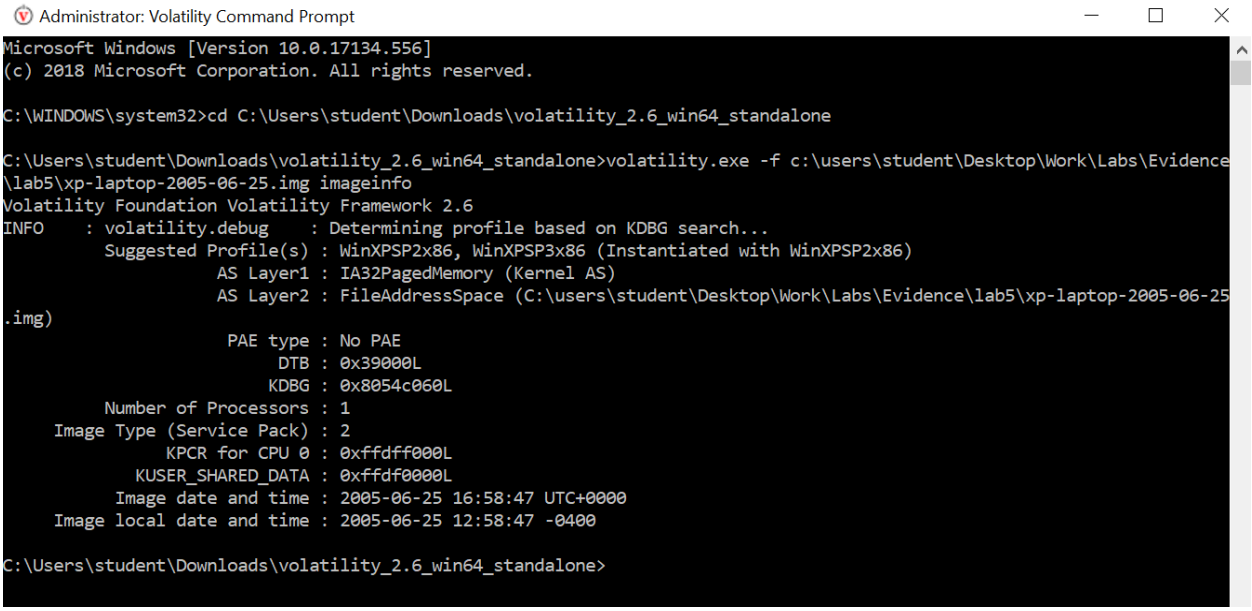
- **From within the Volatility Command Prompt, use the following EXAMPLE commands to analyze the XP laptop image.**

1. volatility.exe –h

```
Microsoft Windows [Version 10.0.17134.556]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd C:\Users\student\Downloads\volatility_2.6_win64_standalone

C:\Users\student\Downloads\volatility_2.6_win64_standalone>volatility.exe -h
Volatility Foundation Volatility Framework 2.6
Usage: Volatility - A memory forensics analysis platform.

Options:
  -h, --help            list all available options and their default values.
                        Default values may be set in the configuration file
                        (/etc/volatilityrc)
  --conf-file=.volatilityrc
                        User based configuration file
  -d, --debug           Debug volatility
  --plugins=PLUGINS     Additional plugin directories to use (semi-colon
                        separated)
  --info                Print information about all registered objects
  --cache-directory=C:\Users\student/.cache\volatility
                        Directory where cache files are stored
  --cache               Use caching
  --tz=TZ               Sets the (Olson) timezone for displaying timestamps
                        using pytz (if installed) or tzset
  -f FILENAME, --filename=FILENAME
                        Filename to use when opening an image
  --profile=WinXPSP2x86
                        Name of the profile to load (use --info to see a list
                        of supported profiles)
  -l LOCATION, --location=LOCATION
                        A URN location from which to load an address space
  -w, --write           Enable write support
  --dtb=DTB             DTB Address
  --shift=SHIFT         Mac KASLR shift address
```

2. volatility.exe -f c:\users\student\Desktop\Work\Labs\Evidence\lab5\xp-laptop-2005-06-25.img imageinfo

- The **imageinfo** command is used to identify the operating system, service pack, and hardware architecture (32 or 64 bit), but it also contains other useful information such as the DTB address and time the sample was collected. [1]



```
Administrator: Volatility Command Prompt
Microsoft Windows [Version 10.0.17134.556]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd C:\Users\student\Downloads\volatility_2.6_win64_standalone

C:\Users\student\Downloads\volatility_2.6_win64_standalone>volatility.exe -f c:\users\student\Desktop\Work\Labs\Evidence
\lab5\xp-laptop-2005-06-25.img imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\users\student\Desktop\Work\Labs\Evidence\lab5\xp-laptop-2005-06-25
.img)
                      PAE type : No PAE
                           DTB : 0x39000L
                          KDBG : 0x8054c060L
          Number of Processors : 1
     Image Type (Service Pack) : 2
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2005-06-25 16:58:47 UTC+0000
     Image local date and time : 2005-06-25 12:58:47 -0400

C:\Users\student\Downloads\volatility_2.6_win64_standalone>
```

3. volatility.exe -f c:\users\student\Desktop\Work\Labs\Evidence\lab5\xp-laptop-2005-06-25.img --profile WinXPSP2x86 psscan

- The **psscan** command is used to find processes that previously terminated (inactive) and processes that have been hidden or unlinked by a rootkit. The downside is that rootkits can still hide by overwriting the pool tag values (though not commonly seen in the wild). [1]

Administrator: Volatility Command Prompt

```
C:\Users\student\Downloads\volatility_2.6_win64_standalone>volatility.exe -f c:\users\student\Desktop\Work\Labs\Evidence\lab5\xp-lapto
p-2005-06-25.img --profile WinXPSP2x86 psscan
Volatility Foundation Volatility Framework 2.6
Offset(P)          Name                PID   PPID PDB        Time created                   Time exited
------------------ ---------------- ------ ------ ---------- ------------------------------ ------------------------------
0x0000000001343790 mqtgsvc.exe        2536    580 0x17406000 2005-06-25 16:48:05 UTC+0000
0x00000000014b13b0 iexplore.exe       2392   1812 0x16f8f000 2005-06-25 16:51:02 UTC+0000
0x0000000001ed76b0 PluckTray.exe      2740    944 0x175fc000 2005-06-25 16:51:10 UTC+0000
0x0000000001ed84e8 dd.exe             4012   2624 0x0eee8000 2005-06-25 16:58:46 UTC+0000
0x0000000001f269e0 PluckUpdater.ex    3076   1812 0x1a6c5000 2005-06-25 16:51:15 UTC+0000   2005-06-25 16:51:30 UTC+0000
0x0000000001f48da0 tcpsvcs.exe        1400    580 0x14e54000 2005-06-25 16:47:58 UTC+0000
0x0000000001f5a3b8 csrss.exe           504    448 0x0dac6000 2005-06-25 16:47:30 UTC+0000
0x0000000001f5f020 ssonsvr.exe        1632   1580 0x12b3f000 2005-06-25 16:47:46 UTC+0000
0x0000000001f67500 TaskSwitch.exe     1952   1812 0x139d2000 2005-06-25 16:47:48 UTC+0000
0x0000000001f68518 Crypserv.exe        688    580 0x14a49000 2005-06-25 16:47:55 UTC+0000
0x0000000001f6ca90 Fast.exe           1960   1812 0x13aaf000 2005-06-25 16:47:48 UTC+0000
0x0000000001f6db28 msdtc.exe          1076    580 0x14b6f000 2005-06-25 16:47:55 UTC+0000
0x0000000001f6e7e8 svchost.exe        1024    580 0x1043e000 2005-06-25 16:47:35 UTC+0000
0x0000000001f8dda0 svchost.exe         984    580 0x10220000 2005-06-25 16:47:35 UTC+0000
0x0000000001f8eb10 winlogon.exe        528    448 0x0dcf3000 2005-06-25 16:47:31 UTC+0000
0x0000000001f9a670 spoolsv.exe        1224    580 0x1147b000 2005-06-25 16:47:39 UTC+0000
0x0000000001fa5aa0 svchost.exe         740    580 0x0e575000 2005-06-25 16:47:32 UTC+0000
0x0000000001fa8240 Smc.exe             876    580 0x0eb72000 2005-06-25 16:47:33 UTC+0000
0x0000000001fa8650 svchost.exe         800    580 0x0e8ea000 2005-06-25 16:47:33 UTC+0000
0x0000000001faba78 svchost.exe         840    580 0x0ea71000 2005-06-25 16:47:33 UTC+0000
0x0000000001faf280 jusched.exe         188   1812 0x1413d000 2005-06-25 16:47:49 UTC+0000
0x0000000001fdf020 smss.exe            448      4 0x0c55a000 2005-06-25 16:47:28 UTC+0000
0x0000000002000980 wmiprvse.exe       4080    740 0x10b87000 2005-06-25 16:57:53 UTC+0000
0x0000000002021a78 Rtvscan.exe        1304    580 0x14cc6000 2005-06-25 16:47:58 UTC+0000
0x00000000020238e0 snmp.exe           1424    580 0x14f3a000 2005-06-25 16:47:58 UTC+0000
```


4. volatility.exe -f c:\users\student\Desktop\Work\Labs\Evidence\lab5\xp-laptop-2005-06-25.img --profile WinXPSP2x86 pslist

- The **pslist** command is used to list processes of a system. This command does not detect hidden or unlinked processes but psscan command can do that. If you see processes with 0 threads, 0 handles, and/or a non-empty exit time, the process may not actually still be active. Also, the two processes System and smss.exe will not have a Session ID, because System starts before sessions are established and smss.exe is the session manager itself.[1]

Administrator: Volatility Command Prompt

```
C:\Users\student\Downloads\volatility_2.6_win64_standalone>volatility.exe -f c:\users\student\Desktop\Work\Labs\Evidence\lab5\xp-laptop-2005-06-25.img --profile WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x823c87c0 System                    4      0     61     1140 ------      0

0x81fdf020 smss.exe                448      4      3       21 ------      0 2005-06-25 16:47:28 UTC+0000

0x81f5a3b8 csrss.exe               504    448     12      596      0      0 2005-06-25 16:47:30 UTC+0000

0x81f8eb10 winlogon.exe            528    448     21      508      0      0 2005-06-25 16:47:31 UTC+0000

0x820e0da0 services.exe            580    528     18      401      0      0 2005-06-25 16:47:31 UTC+0000

0x82199668 lsass.exe               592    528     21      374      0      0 2005-06-25 16:47:31 UTC+0000

0x81fa5aa0 svchost.exe             740    580     17      198      0      0 2005-06-25 16:47:32 UTC+0000

0x81fa8650 svchost.exe             800    580     10      302      0      0 2005-06-25 16:47:33 UTC+0000

0x81faba78 svchost.exe             840    580     83     1589      0      0 2005-06-25 16:47:33 UTC+0000

0x81fa8240 Smc.exe                 876    580     22      423      0      0 2005-06-25 16:47:33 UTC+0000

0x81f8dda0 svchost.exe             984    580      6       90      0      0 2005-06-25 16:47:35 UTC+0000
```


5. volatility.exe -f c:\users\student\Desktop\Work\Labs\Evidence\lab5\xp-laptop-2005-06-25.img --profile WinXPSP2x86 psxview

- The **psxview** command helps in detecting hidden processes by comparing what PsActiveProcessHead contains with what is reported by various other sources of process listings. A "False" in any column indicates that the respective process is missing. [1]

Administrator: Volatility Command Prompt

```
C:\Users\student\Downloads\volatility_2.6_win64_standalone>volatility.exe -f c:\users\student\Desktop\Work\Labs\Evidence\lab5\xp-laptop-2005-06-25.img --profile WinXPSP2x86 psxview
Volatility Foundation Volatility Framework 2.6
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
---------- -------------------- ------ ------ ------ -------- ------ ----- ------- -------- --------
0x01f67500 TaskSwitch.exe         1952 True   True   True     True   True  True    True
0x01faf280 jusched.exe             188 True   True   True     True   True  True    True
0x021ca3d0 wdfmgr.exe             1548 True   True   True     True   True  True    True
0x02081da0 svchost.exe            1484 True   True   True     True   True  True    True
0x020dd588 VPTray.exe             1980 True   True   True     True   True  True    True
0x17fdb020 alg.exe                2868 True   True   True     True   True  True    True
0x01f8eb10 winlogon.exe            528 True   True   True     True   True  True    True
0x02079c18 cmd.exe                2624 True   True   True     True   True  True    True
0x01f68518 Crypserv.exe            688 True   True   True     True   True  True    True
0x01fa5aa0 svchost.exe             740 True   True   True     True   True  True    True
0x020e0da0 services.exe            580 True   True   True     True   True  True    True
0x014b13b0 iexplore.exe           2392 True   True   True     True   True  True    True
0x01343790 mqtgsvc.exe            2536 True   True   True     True   True  True    True
0x01f48da0 tcpsvcs.exe            1400 True   True   True     True   True  True    True
0x01f6db28 msdtc.exe              1076 True   True   True     True   True  True    False
0x01ed76b0 PluckTray.exe          2740 True   True   True     True   True  True    True
0x02025608 atiptaxx.exe           2040 True   True   True     True   True  True    True
0x0202bda0 explorer.exe           1812 True   True   True     True   True  True    True
0x01f8dda0 svchost.exe             984 True   True   True     True   True  True    False
0x01f6ca90 Fast.exe               1960 True   True   True     True   True  True    True
0x01fa8240 Smc.exe                 876 True   True   True     True   True  True    True
0x01f5f020 ssonsvr.exe            1632 True   True   True     True   True  True    True
0x186fec10 firefox.exe            2160 True   True   True     True   True  True    True
0x02218020 PluckSvr.exe            944 True   True   True     True   True  True    True
```

6. volatility.exe -f c:\users\student\Desktop\Work\Labs\Evidence\lab5\xp-laptop-2005-06-25.img --profile WinXPSP2x86 connscan which were terminated.

- This command is used to find artifacts from previous connections, in addition to active ones. This command is for x86 and x64 Windows XP and Windows 2003 Server only. Also it may detect false positive sometimes. [1]

Administrator: Volatility Command Prompt

```
C:\Users\student\Downloads\volatility_2.6_win64_standalone>volatility.exe -f c:\users\student\Desktop\Work\Labs\Evidence\lab5\xp-lapto
p-2005-06-25.img --profile WinXPSP2x86 connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x01370e70 192.168.2.7:1115          207.126.123.29:80         1916
0x01ed1a50 3.0.48.2:17985            66.179.81.245:20084       4287933200
0x01f0e358 192.168.2.7:1164          66.179.81.247:80          944
0x01f11e70 192.168.2.7:1082          205.161.7.134:80          2392
0x01f35cd0 192.168.2.7:1086          199.239.137.200:80        1916
0x01f88e70 192.168.2.7:1162          170.224.8.51:80           1916
0x020869b0 127.0.0.1:1055            127.0.0.1:1056            2160
0x021ca8b8 192.168.2.7:1116          66.161.12.81:80           1916
0x021d2e70 192.168.2.7:1161          66.135.211.87:443         1916
0x02201800 192.168.2.7:1091          209.73.26.183:80          1916
0x02207ab0 192.168.2.7:1151          66.150.96.111:80          1916
0x0220c008 192.168.2.7:1077          64.62.243.144:80          2392
0x0220d6b8 192.168.2.7:1066          199.239.137.200:80        2392
0x02210c48 192.168.2.7:1157          66.151.149.10:80          1916
0x02889800 192.168.2.7:1091          209.73.26.183:80          1916
0x108d2e70 192.168.2.7:1115          207.126.123.29:80         1916
0x187a8008 192.168.2.7:1155          66.35.250.150:80          1916
0x18fffaf0 127.0.0.1:1056            127.0.0.1:1055            2160
0x1d5bde70 192.168.2.7:1115          207.126.123.29:80         1916
0x1f4eb008 192.168.2.7:1155          66.35.250.150:80          1916
```

7. volatility.exe -f c:\users\student\Desktop\Work\Labs\Evidence\lab5\xp-laptop-2005-06-25.img --profile WinXPSP2x86 hivelist

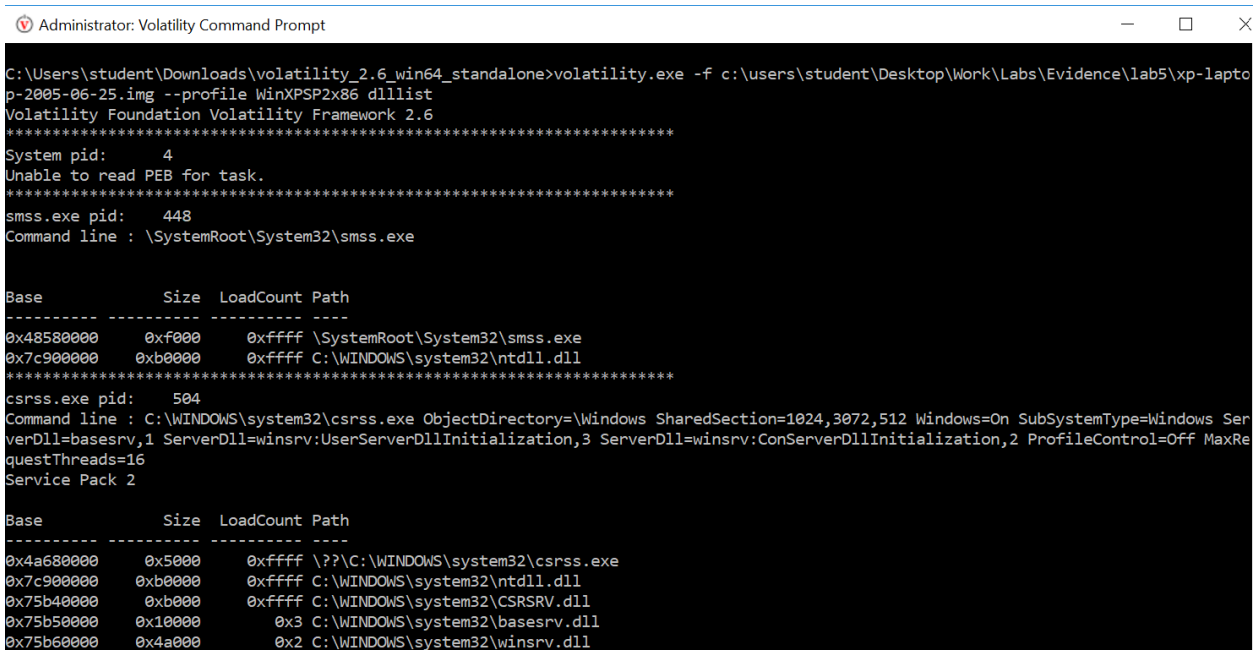
- This command is used to locate the virtual addresses of registry hives in memory, and the full paths to the corresponding hive on disk. [1]

Administrator: Volatility Command Prompt

```
C:\Users\student\Downloads\volatility_2.6_win64_standalone>volatility.exe -f c:\users\student\Desktop\Work\Labs\Evidence\lab5\xp-lapto
p-2005-06-25.img --profile WinXPSP2x86 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual    Physical   Name
---------- ---------- ----
0xe1ecd008 0x11221008 \Device\HarddiskVolume1\Documents and Settings\Sarah\Local Settings\Application Data\Microsoft\Windows\UsrClass.
dat
0xe1eff758 0x1294a758 \Device\HarddiskVolume1\Documents and Settings\Sarah\NTUSER.DAT
0xe1bf9008 0x0e6d0008 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\Microsoft\Windows\Us
rClass.dat
0xe1c26850 0x0e882850 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
0xe1bf1b60 0x0e213b60 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Application Data\Microsoft\Windows\
UsrClass.dat
0xe1c2a758 0x0e88e758 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
0xe1982008 0x0c61d008 \Device\HarddiskVolume1\WINDOWS\system32\config\software
0xe197f758 0x0c622758 \Device\HarddiskVolume1\WINDOWS\system32\config\default
0xe1986008 0x0c632008 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0xe197a758 0x0c60e758 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
0xe1558578 0x02d63578 [no name]
0xe1035b60 0x0283db60 \Device\HarddiskVolume1\WINDOWS\system32\config\system
0xe102e008 0x02837008 [no name]

C:\Users\student\Downloads\volatility_2.6_win64_standalone>
```

8. volatility.exe -f c:\users\student\Desktop\Work\Labs\Evidence\lab5\xp-laptop-2005-06-25.img --profile WinXPSP2x86 dlllist

- This command is used to display process's loaded DLL's. The load count column tells you if a DLL was statically loaded or dynamically loaded. This allows the analyst to determine if a suspect process has accessed these files when it was executed [1]



```
Administrator: Volatility Command Prompt

C:\Users\student\Downloads\volatility_2.6_win64_standalone>volatility.exe -f c:\users\student\Desktop\Work\Labs\Evidence\lab5\xp-laptop-2005-06-25.img --profile WinXPSP2x86 dlllist
Volatility Foundation Volatility Framework 2.6
**************************************************************************
System pid:      4
Unable to read PEB for task.
**************************************************************************
smss.exe pid:    448
Command line : \SystemRoot\System32\smss.exe


Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x48580000     0xf000     0xffff \SystemRoot\System32\smss.exe
0x7c900000    0xb0000     0xffff C:\WINDOWS\system32\ntdll.dll
**************************************************************************
csrss.exe pid:    504
Command line : C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,512 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off MaxRequestThreads=16
Service Pack 2

Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x4a680000     0x5000     0xffff \??\C:\WINDOWS\system32\csrss.exe
0x7c900000    0xb0000     0xffff C:\WINDOWS\system32\ntdll.dll
0x75b40000     0xb000     0xffff C:\WINDOWS\system32\CSRSRV.dll
0x75b50000    0x10000        0x3 C:\WINDOWS\system32\basesrv.dll
0x75b60000    0x4a000        0x2 C:\WINDOWS\system32\winsrv.dll
```

9. volatility.exe -f c:\users\student\Desktop\Work\Labs\Evidence\lab5\xp-laptop-2005-06-25.img --profile WinXPSP2x86 apihooks

- This command used to find API hooks in user or kernel mode. This finds IAT, EAT, Inline style hooks, and several special types of hooks. [1]

Select Administrator: Volatility Command Prompt - volatility.exe -f c:\users\student\Desktop\Work\Labs\Evidence\lab5\xp-laptop-2005-06-25.img --profile ...

```
C:\Users\student\Downloads\volatility_2.6_win64_standalone>volatility.exe -f c:\users\student\Desktop\Work\Labs\Evidence\lab5\xp-lapto
p-2005-06-25.img --profile WinXPSP2x86 apihooks
Volatility Foundation Volatility Framework 2.6
**********************************************************************
Hook mode: Usermode
Hook type: Import Address Table (IAT)
Process: 840 (svchost.exe)
Victim module: tapisrv.dll (0x733e0000 - 0x7341f000)
Function: activeds.dll!<unknown>
Hook address: 0x76e1ef91
Hooking module: adsldpc.dll

Disassembly(0):
0x76e1ef91 8bff             MOV EDI, EDI
0x76e1ef93 55               PUSH EBP
0x76e1ef94 8bec             MOV EBP, ESP
0x76e1ef96 ff7508           PUSH DWORD [EBP+0x8]
0x76e1ef99 ff150812e176     CALL DWORD [0x76e11208]
0x76e1ef9f f7d8             NEG EAX
0x76e1efa1 1bc0             SBB EAX, EAX
0x76e1efa3 40               INC EAX
0x76e1efa4 5d               POP EBP
0x76e1efa5 c20400           RET 0x4
0x76e1efa8 90               NOP

**********************************************************************
Hook mode: Usermode
Hook type: Import Address Table (IAT)
Process: 840 (svchost.exe)
```

10. volatility.exe -f c:\users\student\Desktop\Work\Labs\Evidence\lab5\xp-laptop-2005-06-25.img --profile WinXPSP2x86 malfind

- The malfind command helps find hidden or injected code/DLLs in user mode memory, based on characteristics such as VAD tag and page permissions. [1]

Select Volatility Command Prompt

```
C:\Users\student\Downloads\volatility_2.6_win64_standalone>volatility.exe -f c:\users\student\Desktop\Work\Labs\Evidence\lab5\xp-lapt
op-2005-06-25.img --profile WinXPSP2x86 malfind
Volatility Foundation Volatility Framework 2.6
Process: csrss.exe Pid: 504 Address: 0x7f6f0000
Vad Tag: Vad  Protection: PAGE_EXECUTE_READWRITE
Flags: Protection: 6

0x7f6f0000  c8 00 00 00 2c 01 00 00 ff ee ff ee 08 70 00 00   ....,........p..
0x7f6f0010  08 00 00 00 00 fe 00 00 00 00 10 00 00 20 00 00   .................
0x7f6f0020  00 02 00 00 00 20 00 00 8d 01 00 00 ff ef fd 7f   .................
0x7f6f0030  03 00 08 06 00 00 00 00 00 00 00 00 00 00 00 00   .................

0x7f6f0000 c8000000         ENTER 0x0, 0x0
0x7f6f0004 2c01             SUB AL, 0x1
0x7f6f0006 0000             ADD [EAX], AL
0x7f6f0008 ff               DB 0xff
0x7f6f0009 ee               OUT DX, AL
0x7f6f000a ff               DB 0xff
0x7f6f000b ee               OUT DX, AL
0x7f6f000c 087000           OR [EAX+0x0], DH
0x7f6f000f 0008             ADD [EAX], CL
0x7f6f0011 0000             ADD [EAX], AL
0x7f6f0013 0000             ADD [EAX], AL
0x7f6f0015 fe00             INC BYTE [EAX]
0x7f6f0017 0000             ADD [EAX], AL
0x7f6f0019 0010             ADD [EAX], DL
0x7f6f001b 0000             ADD [EAX], AL
0x7f6f001d 2000             AND [EAX], AL
0x7f6f001f 0000             ADD [EAX], AL
0x7f6f0021 0200             ADD AL, [EAX]
```

1. Were there any processes running on this computer that were hidden?

- Using psxview command we can see hidden process. In the pslist column wherever there is False values those are all hidden processes. For example, svchost.exe, iexplorer.exe spoolsv.exe, dd.exe, Fast.exe except System and smss.exe processes cannot be tracked by csrss as they have already started before it; nor do they have a corresponding logon session, or desktop threads.

```
0x0205eda0 wuauclt.exe          2424 True   True   True    True   True  True   True
0x021ce4d8 Fast.exe             1700 True   True   True    True   True  True   True
0x01f269e0 PluckUpdater.ex      3076 True   True   False   True   False False  False   2005-06-25 16:51:30 UTC+0000
0x16c7f9d0 PluckUpdater.ex      1916 True   True   False   True   False False  False   2005-06-25 16:53:49 UTC+0000
0x01f5a3b8 csrss.exe             504 True   True   True    True   False True   True
0x023c87c0 System                  4 True   True   True    True   False False  False
0x01fdf020 smss.exe              448 True   True   True    True   False False  False
0x021fb3b8 PluckTray.exe        3256 True   True   False   True   False False  False   2005-06-25 16:54:28 UTC+0000
0x022148f0 PluckTray.exe        3100 True   True   False   True   False False  False   2005-06-25 16:57:59 UTC+0000
0x02000980 wmiprvse.exe         4080 True   True   True    False  False True   True
0x12cd3020 smss.exe              448 False  True   False   False  False False  False
0x0fe5f8e0 snmp.exe             1424 False  True   False   False  False False  False
0x131f0da0 svchost.exe           984 False  True   False   False  False False  False
0x18899da0 svchost.exe           984 False  True   False   False  False False  False
0x1b4db020 smss.exe              448 False  True   False   False  False False  False
0x12d67a90 Fast.exe             1960 False  True   False   False  False False  False
0x0ee763b0 iexplore.exe         2392 False  True   False   False  False False  False
0x13a36a78 svchost.exe           840 False  True   False   False  False False  False
0x1a192a90 Fast.exe             1960 False  True   False   False  False False  False
0x0f55d670 spoolsv.exe          1224 False  True   False   False  False False  False
0x1e5b2670 spoolsv.exe          1224 False  True   False   False  False False  False
0x04096da0 svchost.exe          1484 False  True   False   False  False False  False
0x171033b0 iexplore.exe         2392 False  True   False   False  False False  False
0x13f924e8 dd.exe               4012 False  True   False   False  False False  False
0x13a597e8 svchost.exe          1024 False  True   False   False  False False  False
```

2. What is the username of the primary user on this computer?

- By using hivelist command, I am able to view primary user name as ‘Sarah’ in the registry hive path

Administrator: Volatility Command Prompt

```
C:\Users\student\Downloads\volatility_2.6_win64_standalone>volatility.exe -f c:\users\student\Desktop\Work\Labs\Evidence\lab5\xp-lapto
p-2005-06-25.img --profile WinXPSP2x86 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual    Physical   Name
---------- ---------- ----
0xe1ecd008 0x11221008 \Device\HarddiskVolume1\Documents and Settings\Sarah\Local Settings\Application Data\Microsoft\Windows\UsrClass.
dat
0xe1eff758 0x1294a758 \Device\HarddiskVolume1\Documents and Settings\Sarah\NTUSER.DAT
0xe1bf9008 0x0e6d0008 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\Microsoft\Windows\Us
rClass.dat
0xe1c26850 0x0e882850 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
0xe1bf1b60 0x0e213b60 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Application Data\Microsoft\Windows\
UsrClass.dat
0xe1c2a758 0x0e88e758 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
0xe1982008 0x0c61d008 \Device\HarddiskVolume1\WINDOWS\system32\config\software
0xe197f758 0x0c622758 \Device\HarddiskVolume1\WINDOWS\system32\config\default
0xe1986008 0x0c632008 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0xe197a758 0x0c60e758 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
0xe1558578 0x02d63578 [no name]
0xe1035b60 0x0283db60 \Device\HarddiskVolume1\WINDOWS\system32\config\system
0xe102e008 0x02837008 [no name]

C:\Users\student\Downloads\volatility_2.6_win64_standalone>
```

3. What is the system time?

➢ The imageinfo command helps in finding the system time details. Image Date and time is 2005-06-25 16:58:47 UTC+0000s

Administrator: Volatility Command Prompt

```
Microsoft Windows [Version 10.0.17134.556]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd C:\Users\student\Downloads\volatility_2.6_win64_standalone

C:\Users\student\Downloads\volatility_2.6_win64_standalone>volatility.exe -f c:\users\student\Desktop\Work\Labs\Evidence
\lab5\xp-laptop-2005-06-25.img imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\users\student\Desktop\Work\Labs\Evidence\lab5\xp-laptop-2005-06-25
.img)
                      PAE type : No PAE
                           DTB : 0x39000L
                          KDBG : 0x8054c060L
          Number of Processors : 1
     Image Type (Service Pack) : 2
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2005-06-25 16:58:47 UTC+0000
     Image local date and time : 2005-06-25 12:58:47 -0400

C:\Users\student\Downloads\volatility_2.6_win64_standalone>
```

4. What browser(s) were running?

➢ psxview command which is showing two browser processes running, it is clear that two browsers were running firefox, and internet explorer

5. What command was typed/running in a command prompt?

- We can check last commands run on computer using **cmdscan, consoles and cmdline plugins.**

  Cmdscan – Extracts command history by scanning for _COMMAND_HISTORY

  Consoles – Extracts command history by scanning for _CONSOLE_INFORMATION

  Cmdline – Display process command-line arguments [2]

  Using cmdscan and consoles plugin I am able to see few commands like

  cd – to change directory, dd – allow copying raw data from one source to another,

  dir –listing files and directories within current directory.

  However, cmdline provided some more details regarding the process commands. [5]

Administrator: Volatility Command Prompt

```
C:\Users\student\Downloads\volatility_2.6_win64_standalone>volatility.exe -f c:\users\student\Desktop\Work\Labs\Evidence\lab5\xp-lapto
p-2005-06-25.img --profile WinXPSP2x86 cmdscan
Volatility Foundation Volatility Framework 2.6
**************************************************
CommandProcess: csrss.exe Pid: 504
CommandHistory: 0x4e4d88 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 7 LastAdded: 6 LastDisplayed: 6
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x4c8
Cmd #0 @ 0x4e2d28: d:
Cmd #1 @ 0x4e1f78: cd  dd
Cmd #2 @ 0x4e2cc8: dir
Cmd #3 @ 0x4e2e00: cd UnicodeRelease
Cmd #4 @ 0x4e2cb8: dir
Cmd #5 @ 0x4e1f90: dd
Cmd #6 @ 0x4e1ff8: dd if=\\.\PhysicalMemory of=c:\xp-laptop-2005-06-25.img conv=noerror
Cmd #7 @ 0x4e2df0: c
Cmd #8 @ 0x4e2e00: cd UnicodeRelease
Cmd #10 @ 0x4e2e40: N?N??
dd.exe
Cmd #11 @ 0x4e2e50: d.exe
Cmd #13 @ 0x4e2ee8: md.exe
**************************************************
CommandProcess: csrss.exe Pid: 504
CommandHistory: 0x11253b0 Application: dd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x2a4
Cmd #0 @ 0x4e2df0: c
```

Administrator: Volatility Command Prompt - smss.exe pid: 448

```
C:\Users\student\Downloads\volatility_2.6_win64_standalone>volatility.exe -f c:\users\student\Desktop\Work\Labs\Evidence\lab5\xp-lapto
p-2005-06-25.img --profile WinXPSP2x86 cmdline
Volatility Foundation Volatility Framework 2.6
**********************************************************************
System pid:      4
**********************************************************************
smss.exe pid:    448
Command line : \SystemRoot\System32\smss.exe
**********************************************************************
csrss.exe pid:    504
Command line : C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,512 Windows=On SubSystemType=Windows Ser
verDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off MaxRe
questThreads=16
**********************************************************************
winlogon.exe pid:    528
Command line : winlogon.exe
**********************************************************************
services.exe pid:    580
Command line : C:\WINDOWS\system32\services.exe
**********************************************************************
lsass.exe pid:    592
Command line : C:\WINDOWS\system32\lsass.exe
**********************************************************************
svchost.exe pid:    740
Command line : C:\WINDOWS\system32\svchost -k DcomLaunch
**********************************************************************
svchost.exe pid:    800
Command line : C:\WINDOWS\system32\svchost -k rpcss
**********************************************************************
svchost.exe pid:    840
Command line : C:\WINDOWS\System32\svchost.exe -k netsvcs
**********************************************************************
```

Administrator: Volatility Command Prompt

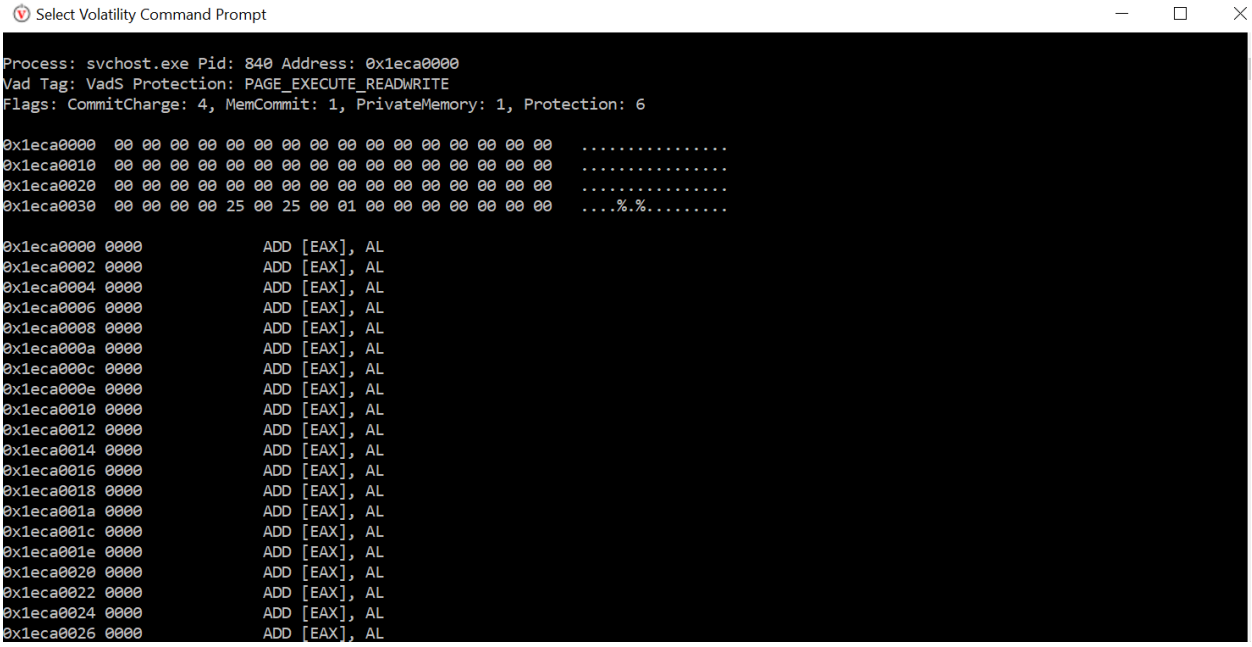
```
C:\Users\student\Downloads\volatility_2.6_win64_standalone>volatility.exe -f c:\users\student\Desktop\Work\Labs\Evidence\lab5\xp-lapto
p-2005-06-25.img --profile WinXPSP2x86 consoles
Volatility Foundation Volatility Framework 2.6
**************************************************
ConsoleProcess: csrss.exe Pid: 504
Console: 0x4e23b0 CommandHistorySize: 50
HistoryBufferCount: 2 HistoryBufferMax: 4
OriginalTitle: %SystemRoot%\system32\cmd.exe
Title: C:\WINDOWS\system32\cmd.exe - dd if=\\.\PhysicalMemory of=c:\xp-laptop-2005-06-25.img conv=noerror
AttachedProcess: dd.exe Pid: 4012 Handle: 0x2a4
AttachedProcess: cmd.exe Pid: 2624 Handle: 0x4c8
----
CommandHistory: 0x11253b0 Application: dd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x2a4
Cmd #0 at 0x4e2df0: c
----
CommandHistory: 0x4e4d88 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 7 LastAdded: 6 LastDisplayed: 6
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x4c8
Cmd #0 at 0x4e2d28: d:
Cmd #1 at 0x4e1f78: cd  dd
Cmd #2 at 0x4e2cc8: dir
Cmd #3 at 0x4e2e00: cd UnicodeRelease
Cmd #4 at 0x4e2cb8: dir
Cmd #5 at 0x4e1f90: dd
Cmd #6 at 0x4e1ff8: dd if=\\.\PhysicalMemory of=c:\xp-laptop-2005-06-25.img conv=noerror
----
Screen 0x4e2ab0 X:80 Y:300
Dump:
```

```
Administrator: Volatility Command Prompt
Smc.exe pid:    876
Command line : "C:\Program Files\Sygate\SPF\smc.exe"
**********************************************************************
svchost.exe pid:    984
Command line : C:\WINDOWS\System32\svchost.exe -k NetworkService
**********************************************************************
svchost.exe pid:   1024
Command line : C:\WINDOWS\System32\svchost.exe -k LocalService
**********************************************************************
spoolsv.exe pid:   1224
Command line : C:\WINDOWS\system32\spoolsv.exe
**********************************************************************
ssonsvr.exe pid:   1632
Command line : "C:\Program Files\Citrix\ICA Client\ssonsvr.exe"
**********************************************************************
explorer.exe pid:   1812
Command line : C:\WINDOWS\Explorer.EXE
**********************************************************************
Directcd.exe pid:   1936
Command line : "C:\Program Files\Roxio\Easy CD Creator 5\DirectCD\DirectCD.exe"
**********************************************************************
TaskSwitch.exe pid:   1952
Command line : "C:\WINDOWS\System32\taskswitch.exe"
**********************************************************************
Fast.exe pid:   1960
Command line : "C:\WINDOWS\System32\fast.exe"
**********************************************************************
VPTray.exe pid:   1980
Command line : "C:\PROGRA~1\SYMANT~1\SYMANT~1\vptray.exe"
**********************************************************************
atiptaxx.exe pid:   2040
Command line : "C:\WINDOWS\system32\Atiptaxx.exe"
**********************************************************************
```

6. What processes potentially were running malware?

➢ Malfind command displays processes which were potentially running malware based on characteristics such as VAD tag and Page Permissions.

```
Select Volatility Command Prompt
C:\Users\student\Downloads\volatility_2.6_win64_standalone>volatility.exe -f c:\users\student\Desktop\Work\Labs\Evidence\lab5\xp-lapt
op-2005-06-25.img --profile WinXPSP2x86 malfind
Volatility Foundation Volatility Framework 2.6
Process: csrss.exe Pid: 504 Address: 0x7f6f0000
Vad Tag: Vad  Protection: PAGE_EXECUTE_READWRITE
Flags: Protection: 6

0x7f6f0000  c8 00 00 00 2c 01 00 00 ff ee ff ee 08 70 00 00   ....,........p..
0x7f6f0010  08 00 00 00 00 fe 00 00 00 00 10 00 00 20 00 00   ................
0x7f6f0020  00 02 00 00 00 20 00 00 8d 01 00 00 ff ef fd 7f   ................
0x7f6f0030  03 00 08 06 00 00 00 00 00 00 00 00 00 00 00 00   ................

0x7f6f0000 c8000000         ENTER 0x0, 0x0
0x7f6f0004 2c01             SUB AL, 0x1
0x7f6f0006 0000             ADD [EAX], AL
0x7f6f0008 ff               DB 0xff
0x7f6f0009 ee               OUT DX, AL
0x7f6f000a ff               DB 0xff
0x7f6f000b ee               OUT DX, AL
0x7f6f000c 087000           OR [EAX+0x0], DH
0x7f6f000f 0008             ADD [EAX], CL
0x7f6f0011 0000             ADD [EAX], AL
0x7f6f0013 0000             ADD [EAX], AL
0x7f6f0015 fe00             INC BYTE [EAX]
0x7f6f0017 0000             ADD [EAX], AL
0x7f6f0019 0010             ADD [EAX], DL
0x7f6f001b 0000             ADD [EAX], AL
0x7f6f001d 2000             AND [EAX], AL
0x7f6f001f 0000             ADD [EAX], AL
0x7f6f0021 0200             ADD AL, [EAX]
```

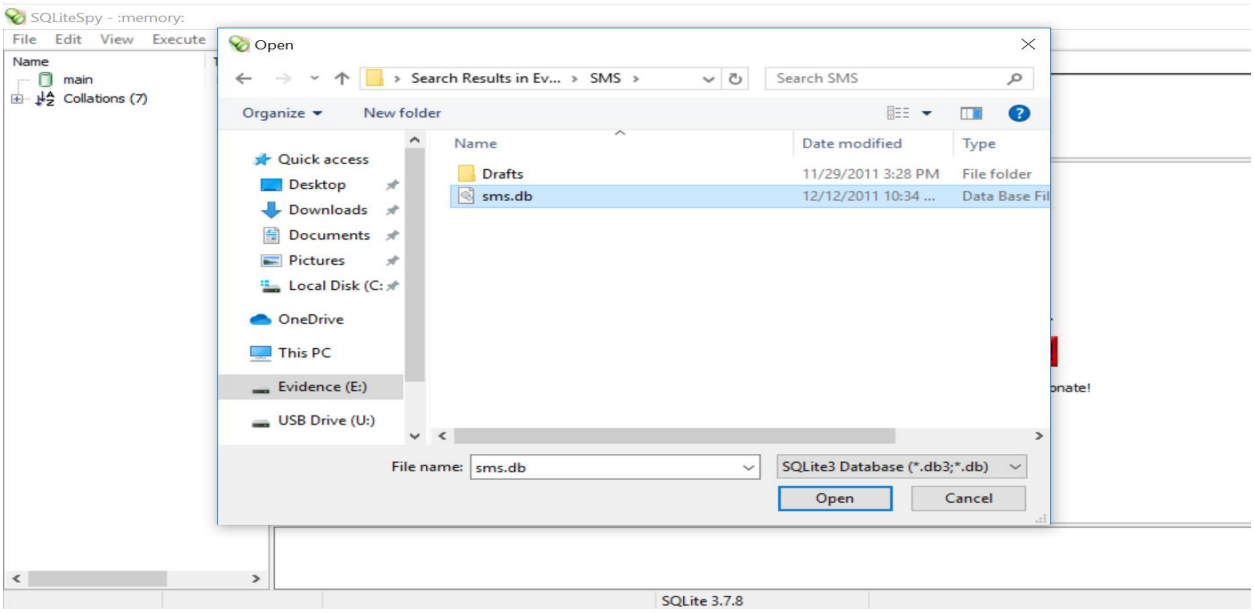


2. Mobile Device Filesystem Forensics

- Mobile device forensics deals with recovering and analyzing digital evidence from mobile devices such as smartphones and tablets.
- Open Windows Explorer, navigate to the Evidence Drive →Mobile Device Forensics →iphone-data folder. Navigate through the directories to find the database and plist files needed for the questions below. **Note -** Use Plist Editor and SQLiteSpy application to open the plists and .db files respectively

1. Access the SMS database and look for login credentials and wireless network credentials that were texted on the device

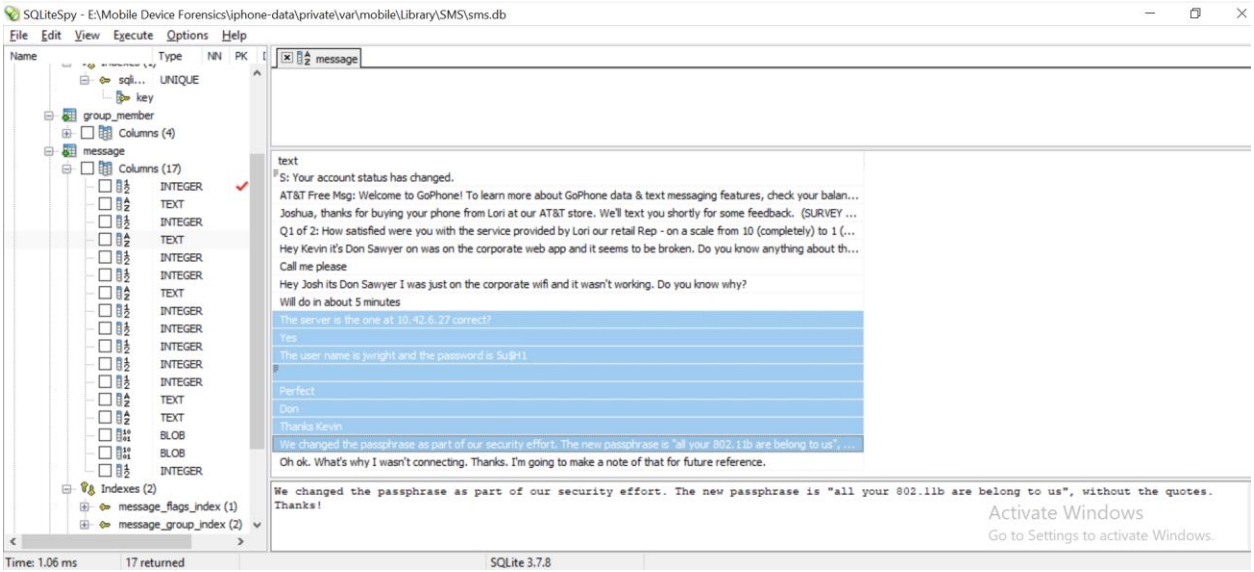
   ➢ Open the SQLiteSpy application and click on File → Open Database. Navigate to the SMS database, click on file and select Open option.



- After checking each and every file, I am able to find server IP address and username and password details.

  Server IP Address – 10.42.6.27

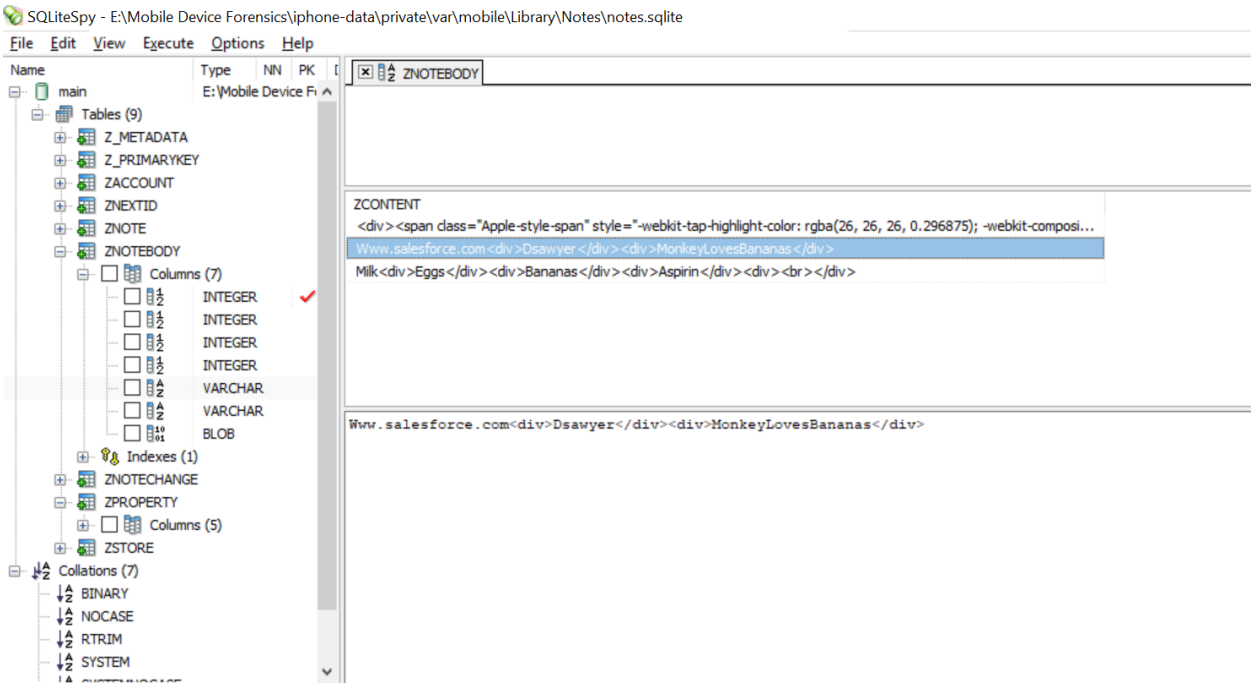
  Username – jwright, Password – 5u$H1



2. Access the notes database to look for information related to salesforce.com credentials.

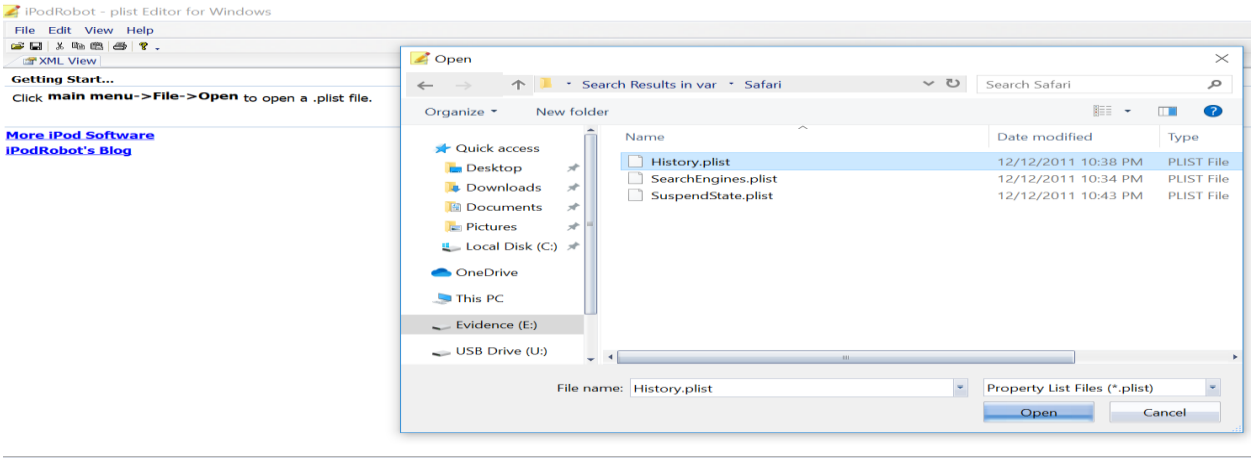
- After searching through all directories and files, password details found in the 'ZNOTEBODDY' folder under VARCHAR and details as below for www.Salesforce.com:

  UserName – Dsawyer, Password – MonkeyLoveBananas



3. Access the Safari History plist file and review it for a visit to a website that has a password document

   - For this we will be using Plist Editor – plist or Property List files are the most commonly used data formats in IOS devices. These files stores configuration information, preferences, and settings. [6]
   - Open the plist Editor and click on File → Open and find the Safari folder in Mobile Device Forensics folder. Open the History.plist file. Now can find keywords using ctrl +F
   - The website is http://www.willhackforsushi.com which has a 'password.txt' document → on path http://www.willhackforsushi.com/password.txt



4. Access the Safari History snapshot to view the image of the last screen seen in the browser.

   - In this case, the "lastVisitedDate" value for the entry corresponding to the Google website is "344923122.9". Since this value is the highest among all the "lastVisitedDate" values in the array, it indicates that this entry represents the last visited site.

History.plist - plist Editor for Windows

File Edit View Help

XML View

```
18          </dict>
19          <dict>
20            <key></key>
21            <string>http://www.willhackforsushi.com/</string>
22            <key>D</key>
23            <array>
24              <integer>1</integer>
25            </array>
26            <key>lastVisitedDate</key>
27            <string>345432894.3</string>
28            <key>title</key>
29            <string>Will Hack For SUSHI</string>
30            <key>visitCount</key>
31            <integer>1</integer>
32          </dict>
33          <dict>
34            <key></key>
35            <string>http://www.google.com/</string>
36            <key>D</key>
37            <array>
38              <integer>1</integer>
39              <integer>0</integer>
40              <integer>0</integer>
41              <integer>0</integer>
42              <integer>1</integer>
43            </array>
44            <key>lastVisitedDate</key>
45            <string>344923122.9</string>
46            <key>title</key>
47            <string>Google</string>
48            <key>visitCount</key>
49            <integer>2</integer>
50          </dict>
51        </array>
52        <key>WebHistoryFileVersion</key>
53        <integer>1</integer>
54      </dict>
55      </plist>
```

3. Mobile Device Network Forensics

- Open Windows Explorer, navigate to the Evidence Drive →Mobile Device Forensics, and open ios-network-traffic.pcap in Wireshark.
- In the Wireshark filter bar, type tcp.stream eq 241. Right click on the packet and select "Follow TCP Stream"

ios-network-traffic.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 241

No.	Time	Source	Destination	Protocol	Length	Info
13329	366.345131	172.16.0.192	174.143.49.201	TCP	78	55677 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16 TSval=780844007 TSecr=0 SACK_PERM=1
13330	366.345367	172.16.0.192	174.143.49.201	TCP	78	[TCP Out-Of-Order] 55677 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16 TSval=780844007 TS…
13331	366.405895	174.143.49.201	172.16.0.192	TCP	62	80 → 55677 [SYN, ACK] Seq=0 Ack=1 Win=8760 Len=0 MSS=1380 WS=1
13332	366.406092	174.143.49.201	172.16.0.192	TCP	62	[TCP Out-Of-Order] 80 → 55677 [SYN, ACK] Seq=0 Ack=1 Win=8760 Len=0 MSS=1380 WS=1
13333	366.441686	172.16.0.192	174.143.49.201	TCP	60	55677 → 80 [ACK] Seq=1 Ack=1 Win=131088 Len=0
13334	366.441864	172.16.0.192	174.143.49.201	TCP	54	[TCP Dup ACK 13333#1] 55677 → 80 [ACK] Seq=1 Ack=1 Win=131088 Len=0
13335	366.467136	172.16.0.192	174.143.49.201	TCP	346	[TCP segment of a reassembled PDU]
13336	366.467362	172.16.0.192	174.143.49.201	TCP	346	[TCP Retransmission] 55677 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131088 Len=292
13337	366.473444	172.16.0.192	174.143.49.201	HTTP	243	POST /middleware/MWServlet HTTP/1.1 (application/x-www-form-urlencoded)
13338	366.473658	172.16.0.192	174.143.49.201	TCP	243	[TCP Retransmission] 55677 → 80 [PSH, ACK] Seq=293 Ack=1 Win=131088 Len=189
13358	366.544372	174.143.49.201	172.16.0.192	TCP	60	80 → 55677 [ACK] Seq=1 Ack=293 Win=54 Len=0
13359	366.544526	174.143.49.201	172.16.0.192	TCP	60	80 → 55677 [ACK] Seq=1 Ack=482 Win=63 Len=0
13360	366.544595	174.143.49.201	172.16.0.192	TCP	54	80 → 55677 [ACK] Seq=1 Ack=293 Win=54 Len=0
13361	366.544656	174.143.49.201	172.16.0.192	TCP	54	80 → 55677 [ACK] Seq=1 Ack=482 Win=63 Len=0

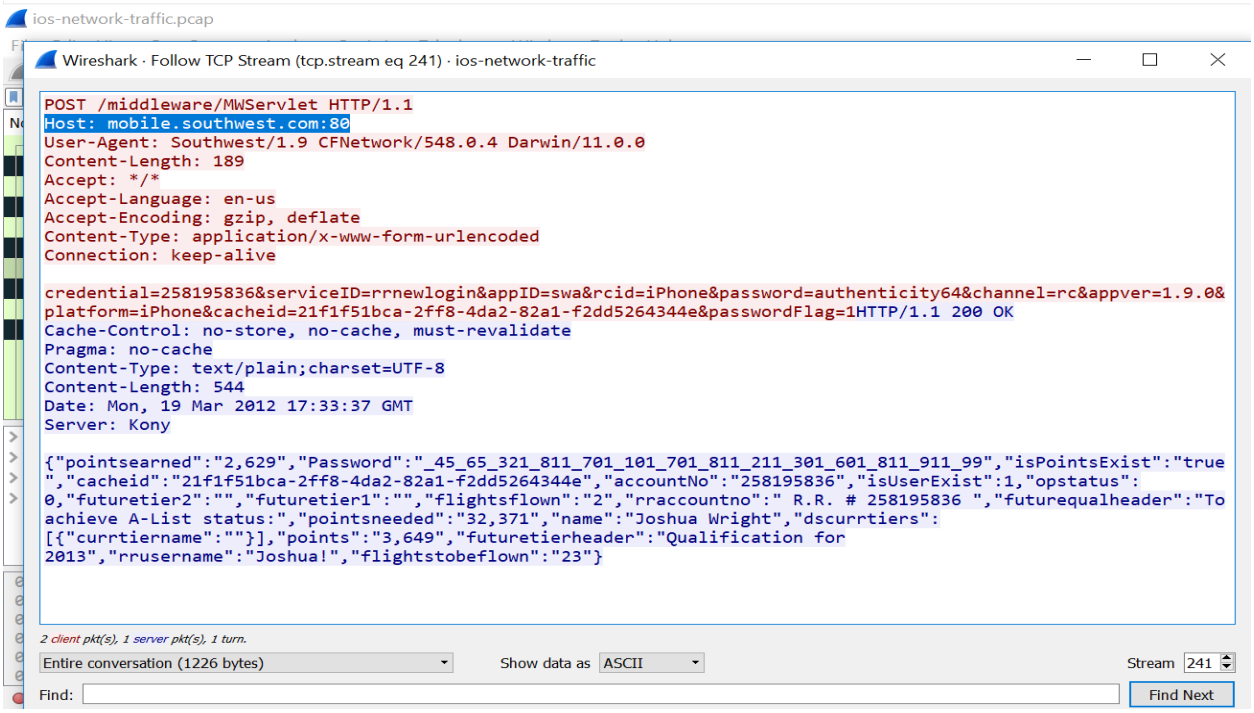
```
> Frame 13329: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
> Ethernet II, Src: Apple_fa:de:d9 (88:c6:63:fa:de:d9), Dst: Dell_ad:2a:c7 (00:18:8b:ad:2a:c7)
> Internet Protocol Version 4, Src: 172.16.0.192, Dst: 174.143.49.201
> Transmission Control Protocol, Src Port: 55677 (55677), Dst Port: 80 (80), Seq: 0, Len: 0

0000  00 18 8b ad 2a c7 88 c6  63 fa de d9 08 00 45 00   ....*... c.....E.
0010  00 40 b7 1c 40 00 40 06  f6 72 ac 10 00 c0 ae 8f   .@..@.@. .r......
0020  31 c9 d9 7d 00 50 ea f4  2e 1c 00 00 00 00 b0 02   1..}.P.. ........
0030  ff ff cc 84 00 00 02 04  05 b4 01 03 03 04 01 01   ........ ........
0040  08 0a 2e 8a bb e7 00 00  00 00 04 02 00 00         ........ ......
```

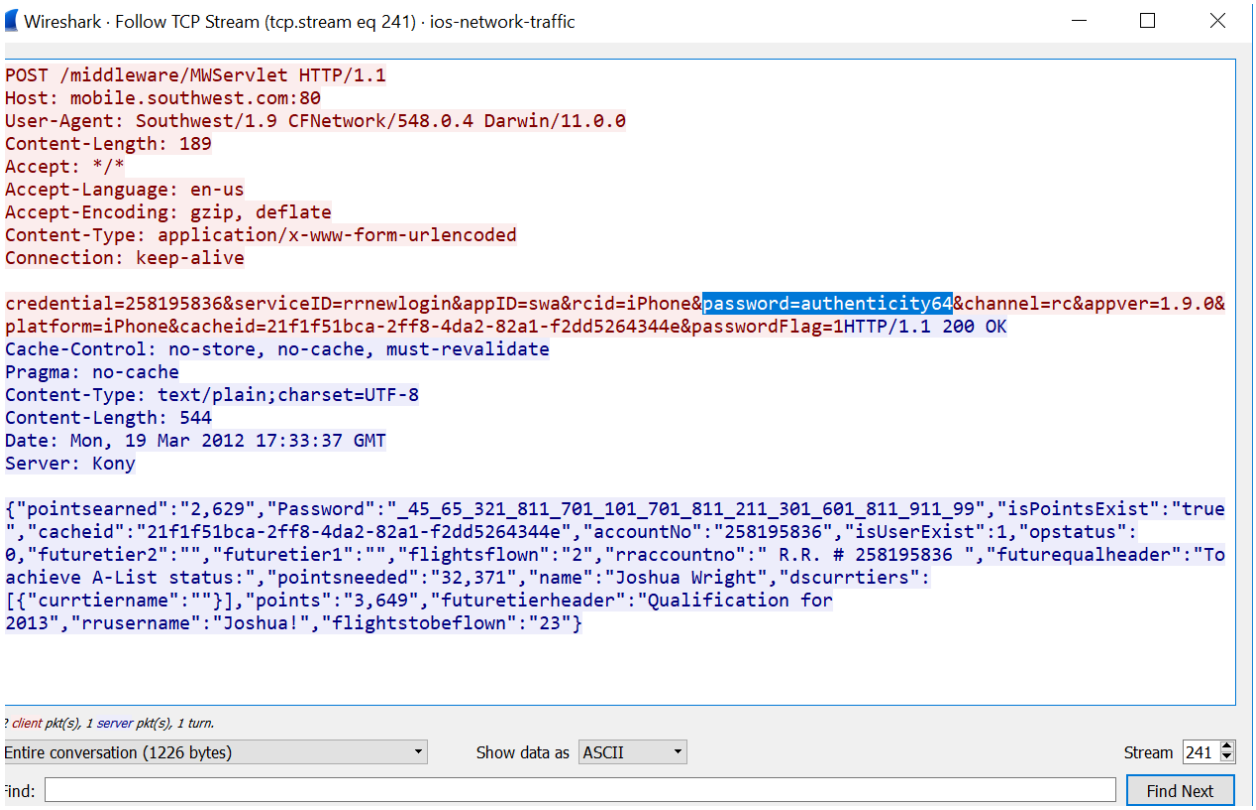
Activate Windows
Go to Settings to activate Windows.

1. What is the password used, and with what app on this iPhone?

- After following the TCP stream, I could see password and app details.

  Password is ‘authenticity64’ and app used by user is ‘mobile.southwest.com’ on port 80





Citations –

1. Volatility Foundation. (2020, May 08). Command Reference - Volatility. Retrieved from https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#imageinfo
2. LIFARS. (2020). Windows Memory Forensics Technical Guide - Part 2 [PDF]. Retrieved from https://lifars.com/wp-content/uploads/2020/06/Windows-Memory-Forensics-Technical-Guide-Part-2.pdf
3. Hacktivities (2021, Dec 29). Forensics: Memory Analysis with Volatility. Retrieved from https://infosecwriteups.com/forensics-memory-analysis-with-volatility-6f2b9e859765
4. Volatility Foundation. (n.d.). Volatility Cheat Sheet - Version 2.4 [PDF]. Retrieved from https://downloads.volatilityfoundation.org/releases/2.4/CheatSheet_v2.4.pdf
5. Shaikh H. (2019, Jan 13). First Steps to Volatile Memory Analysis. Retrieved from https://medium.com/@zemelusa/first-steps-to-volatile-memory-analysis-dcbd4d2d56a1

6. Author(s) or Organization. (2021, Sep 07). iOS Forensics. Retrieved from https://resources.infosecinstitute.com/topic/ios-forensics/