

Lab 5 – Memory and Mobile Device Forensics

Sai Sasaank Srivatsa Pallerla

University of Maryland, Baltimore County

Presented to: Gina Scaldaferri

Date: 10/22/2019

Introduction

Volatility is an open-source memory forensics framework for incident response and malware analysis. It is written in Python and supports memory dumps from all major 32- and 64-bit Windows versions and service packs including XP, 2003 Server, Vista, Server 2008, Server 2008 R2, and Seven. This tool introduces people to the techniques and complexities associated with extracting digital artifacts from volatile memory image.

Property List files, or more commonly known as plist files, are basically Mac application specific preference files. They contain information and settings for various applications and are usually in the easily identifiable format of `com.developer.Application.plist` and located within the `/Library/Preferences/` directories at the system and user level. Plist Editor is a tool that can help investigators to read and edit both XML and binary format plist files.

SQLitespy is a software library that provides a relational database management system. It is easy to use, in terms of setup, database administration, and required resource. SQLite has the following noticeable features: self-contained, serverless, zero-configuration, transactional.

Wireshark is one of the most famous tools that is used to monitor network traffic and protocols used. It lets us monitor the network at a microscopic level, both wired and wireless.

In this lab we will examine a basic disk image for any suspicious processes running. We will also examine the image to find more information in general, the way any forensic investigator would be using Volatility. Later in the lab we will examine iPhone data for any stored passwords/credentials, we will also examine the database to extract any useful and relevant information using Plist and SQLitespy. In the last part of the lab we will examine the network part of the data, i.e., using Wireshark.

Select Volatility										
0x01fa8650	svchost.exe	800	True	True	True	True	True	True	False	
0x02021a78	Rtvscon.exe	1304	True	True	True	True	True	True	True	
0x021d4da0	mqsvc.exe	1948	True	True	True	True	True	True	True	
0x02076558	ati2evxx.exe	432	True	True	True	True	True	True	True	
0x01ed84e8	dd.exe	4012	True	True	True	True	True	True	True	
0x020238e0	snmp.exe	1424	True	True	True	True	True	True	True	
0x021125d0	EM_EXEC.EXE	224	True	True	True	True	True	True	True	
0x02059da0	DefWatch.exe	864	True	True	True	True	True	True	True	
0x02199668	lsass.exe	592	True	True	True	True	True	True	True	
0x01f9a670	spoolsv.exe	1224	True	True	True	True	True	True	True	
0x01f6e7e8	svchost.exe	1024	True	True	True	True	True	True	True	
0x01faba78	svchost.exe	840	True	True	True	True	True	True	True	
0x0205eda0	wuaclt.exe	2424	True	True	True	True	True	True	True	
0x021ce4d8	Fast.exe	1700	True	True	True	True	True	True	True	
0x01f269e0	PluckUpdater.exe	3076	True	True	False	True	False	False	False	2005-06-25 16:51:30 UTC+0000
0x16c7f9d0	PluckUpdater.exe	1916	True	True	False	True	False	False	False	2005-06-25 16:53:49 UTC+0000
0x001f5a3b8	csrss.exe	504	True	True	True	True	False	True	True	
0x023c87c0	System	4	True	True	True	True	False	False	False	
0x01fd020	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	
0x1b4dd020	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	

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

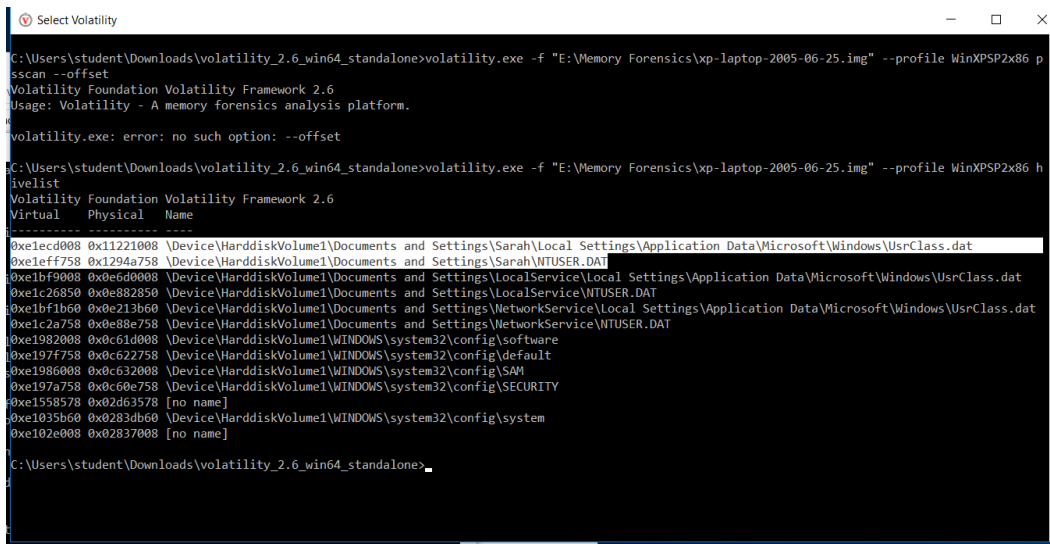
The primary username is Sarah.

Command used: `volatility.exe -f E:\Memory Forensics\xp-laptop-2005-06-25.img --profile WinXPSP2x86 psxview`

`-f`: this used to specify the filename to use when opening the image

`--profile`: this is used to specify the profile to load, in this case the profile is WinXPSP2x86 which define WindowsXP Service Pack 2 32bit OS.

`hivelist`: prints the list of registry hives.



```
Select Volatility
C:\Users\student\Downloads\volatility_2.6_win64_standalone>volatility.exe -f "E:\Memory Forensics\xp-laptop-2005-06-25.img" --profile WinXPSP2x86 p
sscan --offset
Volatility Foundation Volatility Framework 2.6
Usage: Volatility - A memory forensics analysis platform.

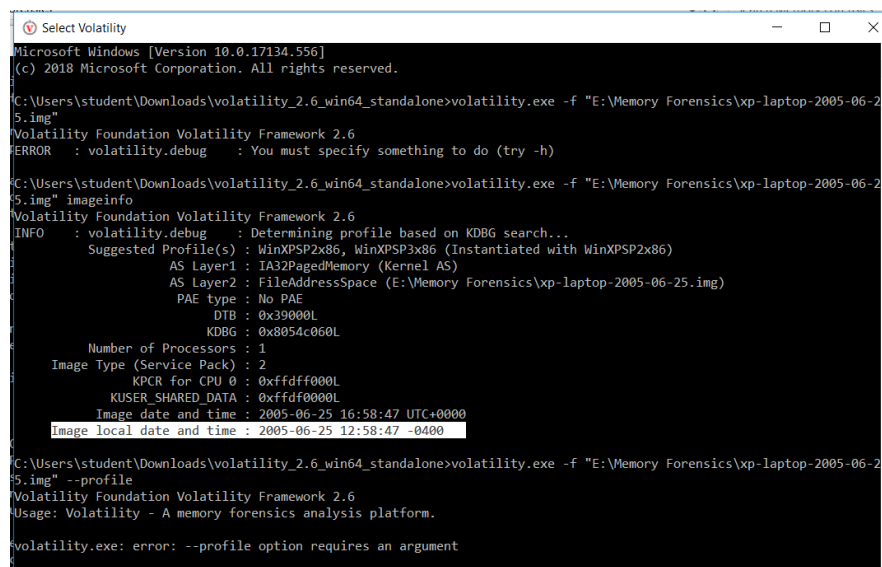
volatility.exe: error: no such option: --offset

C:\Users\student\Downloads\volatility_2.6_win64_standalone>volatility.exe -f "E:\Memory Forensics\xp-laptop-2005-06-25.img" --profile WinXPSP2x86 h
ivelist
Volatility Foundation Volatility Framework 2.6
Virtual Physical Name
-----
0xe12cd008 0x11221908 \Device\HarddiskVolume1\Documents and Settings\Sarah\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe10ff758 0x1294a758 \Device\HarddiskVolume1\Documents and Settings\Sarah\NTUSER.DAT
0xe1bf9908 0x0e6d0808 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\Microsoft\Windows\UsrClass.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 local time zone is EDT we can figure this out from the -0400 after local time.



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

C:\Users\student\Downloads\volatility_2.6_win64_standalone>volatility.exe -f "E:\Memory Forensics\xp-laptop-2005-06-25.img"
Volatility Foundation Volatility Framework 2.6
ERROR : volatility.debug : You must specify something to do (try -h)

C:\Users\student\Downloads\volatility_2.6_win64_standalone>volatility.exe -f "E:\Memory Forensics\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 (E:\Memory Forensics\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 : 0xfffff000L
KUSER_SHARED_DATA : 0xfffff000L
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>volatility.exe -f "E:\Memory Forensics\xp-laptop-2005-06-25.img" --profile
Volatility Foundation Volatility Framework 2.6
Usage: Volatility - A memory forensics analysis platform.

volatility.exe: error: --profile option requires an argument
```

4. What browser(s) were running?

The two browsers in that we get from using psscan, a pool scanner for all process objects, are Explorer and Firefox

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	Crypsserv.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	msdtd.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
0x0000000001fd0f20	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	Rtvsan.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
0x0000000002025608	atiptaxx.exe	2040	1812	0x13d79000	2005-06-25	16:47:49	UTC+0000
0x000000000202bda0	explorer.exe	1812	1764	0x131eb000	2005-06-25	16:47:47	UTC+0000
0x0000000002059da0	DeFWatch.exe	864	580	0x14aa7000	2005-06-25	16:47:55	UTC+0000
0x0000000004096da0	svchost.exe	1484	580	0x1515f000	2005-06-25	16:47:59	UTC+0000
0x000000000ee763b0	iexplore.exe	2392	1812	0x16f8f000	2005-06-25	16:51:02	UTC+0000
0x000000000f55d670	spoolsv.exe	1224	580	0x1147b000	2005-06-25	16:47:39	UTC+0000
0x000000000fe5f8e0	snmp.exe	1424	580	0x14f3a000	2005-06-25	16:47:58	UTC+0000
0x00000000012cd3020	smss.exe	448	4	0x0c55a000	2005-06-25	16:47:28	UTC+0000
0x00000000012d67a90	Fast.exe	1960	1812	0x13aaf000	2005-06-25	16:47:48	UTC+0000
0x000000000131f0da0	svchost.exe	984	580	0x10220000	2005-06-25	16:47:35	UTC+0000
0x00000000013a36a78	svchost.exe	840	580	0x0ea71000	2005-06-25	16:47:33	UTC+0000
0x00000000013a597e8	svchost.exe	1024	580	0x1043e000	2005-06-25	16:47:35	UTC+0000
0x00000000013f924e8	dd.exe	4012	2624	0x0eee8000	2005-06-25	16:58:46	UTC+0000
0x00000000016c7f9d0	PluckUpdater.exe	1916	944	0x1ba0e000	2005-06-25	16:51:40	UTC+0000
0x000000000171033b0	iexplore.exe	2392	1812	0x16f8f000	2005-06-25	16:51:02	UTC+0000
0x00000000017fdb020	alg.exe	2868	580	0x18679000	2005-06-25	16:48:11	UTC+0000
0x000000000186fec10	firefox.exe	2160	1812	0x1d484000	2005-06-25	16:49:22	UTC+0000
0x00000000018899da0	svchost.exe	984	580	0x10220000	2005-06-25	16:47:35	UTC+0000
0x0000000001a192a90	Fast.exe	1960	1812	0x13aaf000	2005-06-25	16:47:48	UTC+0000

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

Command used: volatility.exe -f E:\Memory Forensics\xp-laptop-2005-06-25.img --profile WinXPSP2x86 cmdscan

Cmdscan: used to display the command that were typed in command prompt

```
Select Volatility
C:\Users\student\Downloads\volatility 2.6_win64_standalone>volatility.exe -f "E:\Memory Forensics\xp-laptop-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
C:\Users\student\Downloads\volatility 2.6_win64_standalone>
```

6. What processes potentially were running malware?

Command used: volatility.exe -f E:\Memory Forensics\xp-laptop-2005-06-25.img --profile WinXPSP2x86 malfind

Malfind: used to check for hidden processes and injected code, it doesn't give which process/ dll the code was injected to but the process that runs the injected code.

```
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 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 .....

0x7f6f0000 c8000000 ENTER 0x0, 0x0
0x7f6f0004 2c01 SUB AL, 0x1
0x7f6f0006 0000 ADD [EAX], AL
Process: explorer.exe Pid: 1812 Address: 0x046e0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x046e0000 00 00 00 00 59 e9 c6 29 e5 ff e8 f5 ff ff ff 00 ....Y..).....
0x046e0010 00 00 00 00 00 00 00 e8 e8 ff ff ff 0a 00 6e 04 .....n.
0x046e0020 00 00 00 00 e8 db ff ff ff 17 00 6e 04 00 00 00 .....n....
0x046e0030 00 e8 ce ff ff ff 24 00 6e 04 00 00 00 e8 c1 .....$.n.....

0x046e0000 0000 ADD [EAX], AL
0x046e0002 0000 ADD [EAX], AL
0x046e0004 59 POP ECX
Process: svchost.exe Pid: 840 Address: 0x1eca0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 4, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x1eca0000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x1eca0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x1eca0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x1eca0030 00 00 00 00 25 00 25 00 01 00 00 00 00 00 00 .....%.%.....

0x1eca0000 0000 ADD [EAX], AL
0x1eca0002 0000 ADD [EAX], AL
0x1eca0004 0000 ADD [EAX], AL
0x1eca0006 0000 ADD [EAX], AL
```

2. Mobile Device Filesystem Forensics

To use SQLiteSpy one must have knowledge about SQL, which is a language used to query the database. For this lab we used very simple commands like ‘select * from message’

Select – this is used to specify the mode of operation

* from - is used to say ‘display everything’ (in a table)

message – this is the name of the table that we are trying to access

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

SQLiteSpy - E:\Mobile Device Forensics\iphone-data\private\var\mobile\Library\SMS\sms.db

File Edit View Execute Options Help

Name: main Type: E:\Mobil

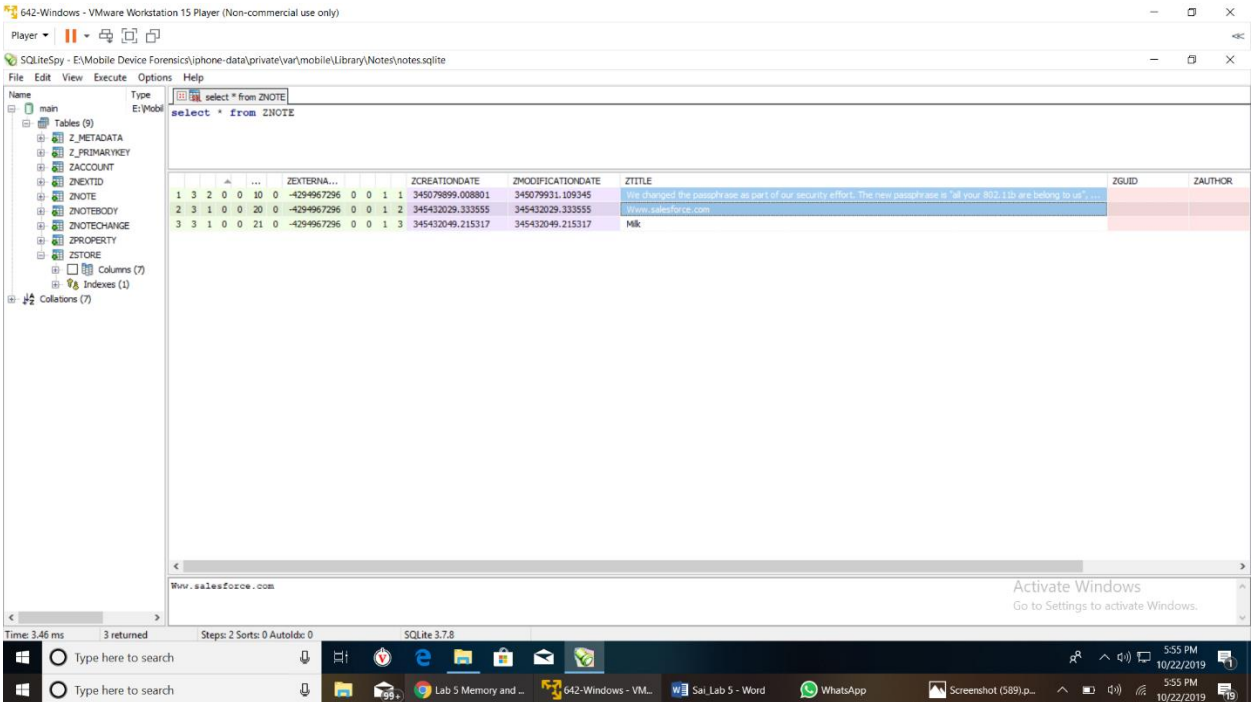
Select * from message

ROWID	address	date	text	flags	replace	g...	association_id	height	UPflags
1	1111559064	1322585754	5: Your account status has changed.	2	0	1	0	0	0
2	+11113272604	1322591479	AT&T Free Msg: Welcome to GoPhone! To learn more about GoPhone data & text messaging features, check your balan...	2	0	2	0	0	0
3	7106	1322662338	Joshua, thanks for buying your phone from Lori at our AT&T store. We'll text you shortly for some feedback. (SURVEY ...	2	0	3	0	0	0
4	7106	1322662436	Q1 of 2: How satisfied were you with the service provided by Lori our retail Rep - on a scale from 10 (completely) to 1 (...	2	0	3	0	0	0
5	(904) 403-8024	1323220736	Hey Kevin it's Don Sawyer on was on the corporate web app and it seems to be broken. Do you know anything about th...	3	0	4	0	0	4
6	+19044038024	1323220776	Call me please	2	0	4	0	0	4
8	+19044038024	1323220994	Will do in about 5 minutes	3	0	4	0	0	4
9	+19044038024	1323221408	The server is the one at 10.42.6.27 correct?	2	0	4	0	0	4
10	+19044038024	1323221446	Yes	3	0	4	0	0	4
11	+19044038024	1323221501	The user name is jwright and the password is 5u9H1	2	0	4	0	0	4
12	+19044038024	1323221784	?	3	0	4	0	0	0
13	+19044038024	1323221804	Perfect	2	0	4	0	0	0
14	+19044038024	1323221813	Don	2	0	4	0	0	0
15	+19044038024	1323221855	Thanks Kevin	3	0	4	0	0	0
16	(401) 524-2911	1323220825	Hey Josh its Don Sawyer I was just on the corporate wifi and it wasn't working. Do you know why?	3	0	5	0	0	4
17	+14015242911	1323222074	We changed the passphrase as part of our security effort. The new passphrase is "all your 802.11b are belong to us", ...	2	0	5	0	0	4
	+14015242911	1323222489	Oh ok. What's why I wasn't connecting. Thanks. I'm going to make a note of that for future reference.	3	0	5	0	0	0

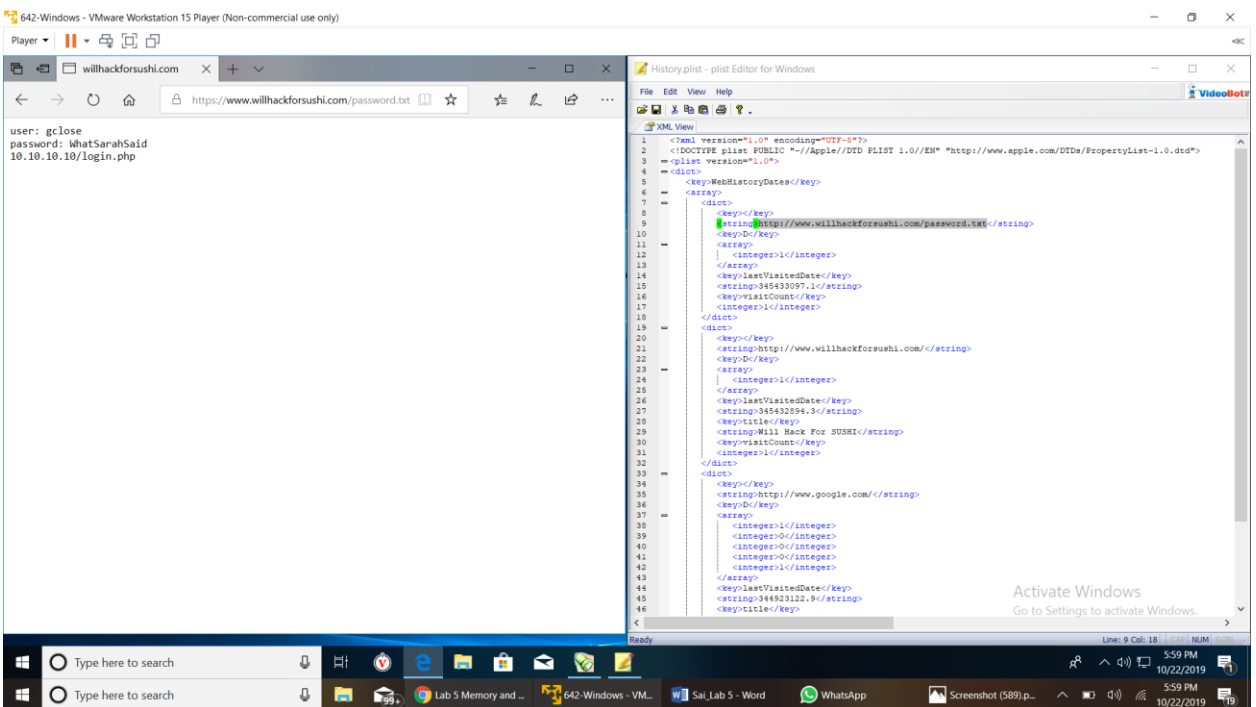
Time: 10.03 ms 17 returned Steps: 16 Sorts: 0 Autoidx: 0 SQLite 3.7.8

Activate Windows
Go to Settings to activate Windows.

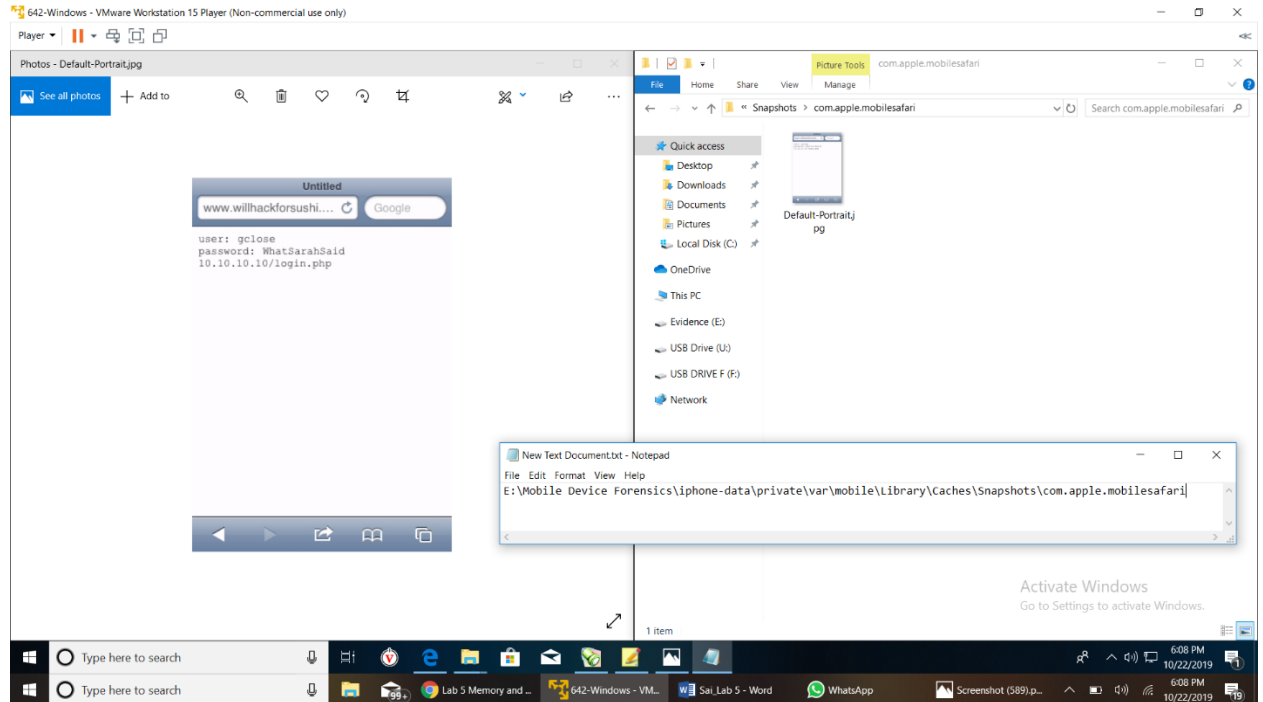
2. Access the notes database to look for information related to salesforce.com credentials.



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



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



3. Mobile Device Network Forensics

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

Application/ Website: southwest.com (on iPhone)

Password: authenticity64

642-Windows - VMware Workstation 15 Player (Non-commercial use only)

Player

ios-network-traffic.pcap

Wireshark: Follow TCP Stream (tcp.stream eq 241) - ios-network-traffic

POST /middleware/WMServlet HTTP/1.1
Host: mobile.southwest.com:80
User-Agent: Southwest/1.9 CFNetwork/548.0.4 Darwin/11.0.0
Content-Length: 189
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Connection: keep-alive
credential=258195836&serviceID=rnewlogin&appID=swa&rcid=iPhone&password=authenticity64&channel=rc&appver=1.9.0&platform=iPhone&cached=21f1f51bca-2ff8-4da2-82a1-f2dd526434de&password=lag-IHTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Type: text/plain; charset=UTF-8
Content-Length: 544
Date: Mon, 19 Mar 2012 17:33:37 GMT
Server: Kony

Full request URI: http://mobile.southwest.com:80/middleware/WMServlet
[HTTP request 1/1]
[Response in frame: 13378]
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "credential" = "258195836"
Form item: "serviceID" = "rnewlogin"
Form item: "appID" = "swa"
Form item: "rcid" = "iPhone"
Form item: "password" = "authenticity64"

0160 6f 6e 65 26 70 61 73 73 72 6f 72 64 3d 61 75 26 one&password=au
0170 88 65 60 74 69 63 69 74 79 36 34 2d 63 68 61 6e tenticity64&chan
0180 6e 65 6c 3d 72 63 26 61 70 70 76 65 72 3d 31 2e nelerc& pper=1.
0190 39 2e 30 26 70 6c 61 74 66 6f 72 6d 3d 69 50 68 9.0&plat form=iPh

Frame (243 bytes) Reassembled TCP (481 bytes)

No.: 2237 Time: 36.629941 Sources: 172.16.0.192 Destination: 174.143.49.201 Protocol: ... Length: 243 Info: POST /middleware/WMServlet HTTP/1.1 (application/x-www-form-urlencoded)

ios-network-traffic

Packets: 15824 · Dig

Type here to search

Type here to search

Lab 5 Memory and ...

642-Windows - VM...

Sai Lab 5 - Word

WhatsApp

Screenshot (589)p...

6:17 PM 10/22/2019

6:17 PM 10/22/2019

Conclusion

In this lab we could use tools like SQLlitespy, Plist Editor, Wireshark and Volatility which are all used to traverse through an image that was created, for volatility, and iPhone's image for the other tools. This lab gives us an introduction to using forensic tools and an idea of how mobile forensics is conducted.

References

- [1] <https://resources.infosecinstitute.com/finding-and-enumerating-processes-within-memory-part-1/#gref>
- [2] <https://anupriti.blogspot.com/2015/10/extracting-usernamepasswords-from-ram.html>
- [3] <https://medium.com/@zemelusa/first-steps-to-volatile-memory-analysis-dcbd4d2d56a1>
- [4] <https://www.timeanddate.com/time/map/>