



**security  
engineering  
capability**



# COMP6445 – Digital Forensics

Term 3 2019 - Week 3 part 2

1 October 2019

# Topics for this lecture

## Memory forensics

1. Windows memory forensics
2. Instructor-led exercise



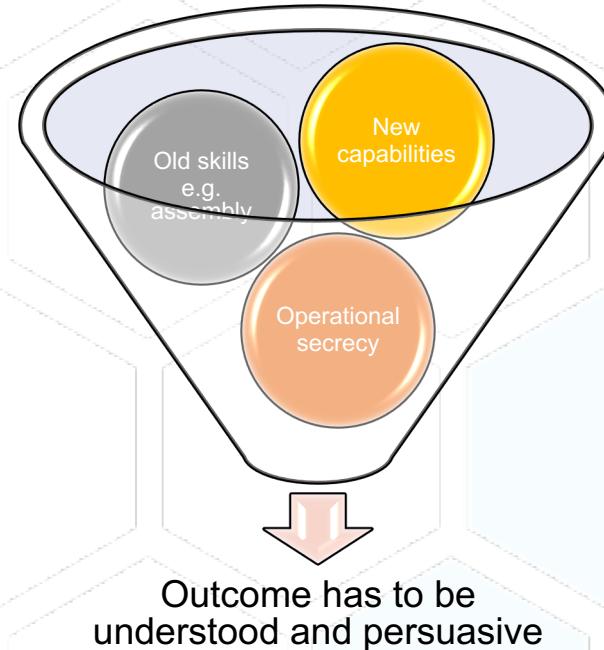
# My introduction to Memory Forensics...

- Was in 1993 when I was attached to NSW Police Joint Technical Support Group (what is now known as SEEB)
  - Decided in Burwood District Court in 1995
  - Defended by Chris Murphy and Clive Stern
  - More than 30 years has passed so no longer an official secret
- Convert arcade games such as pacman, frogger and space invaders into betting games such as blackjack and slot machines
  - A sequence of joystick movements combined with pressing buttons
  - The sequence was programmed by the operator at the beginning of the day
  - A kill switch sent it back to the arcade game and erased the sequence



# Memory Forensics

- Is typically practiced as part of incident response and usually relating to malware
  - An area that is being well researched and becoming better understood
  - Partly due to commercial application
- Is also used for extracting credentials
  - By intelligence and law enforcement ⇒ meaning it is not well publicised
  - Every Australian case I have been involved in, the evidence has been suppressed, usually under the guise of operational secrecy
- It is the discipline of digital forensics surrounded by most mystique and often referred to as a “black art”



Outcome has to be  
understood and persuasive

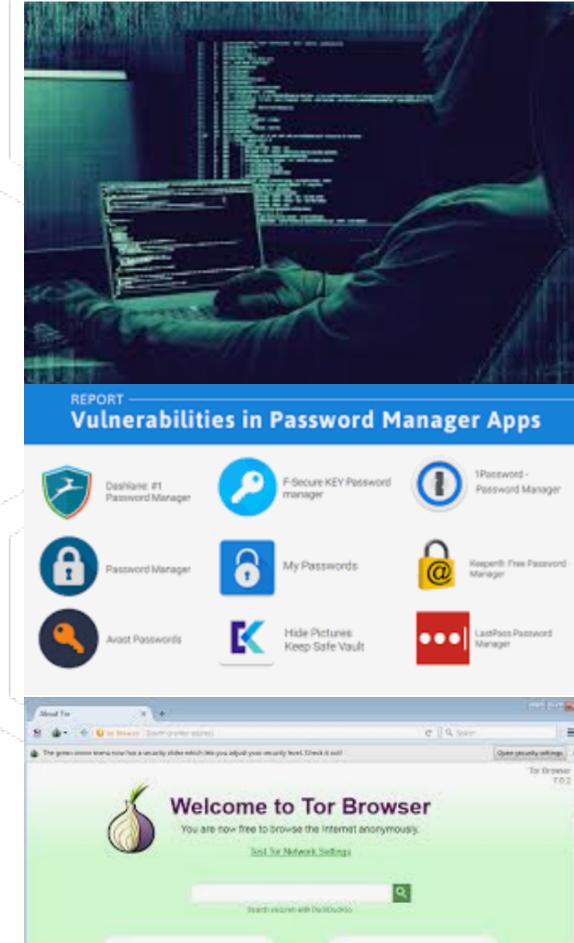
# Presenting memory forensic as evidence

- The biggest challenge is that it is often regarded as “black magic”. Technicians have been really bad at presenting and have too often avoided presenting under a veil of operational secrecy
  - Judges and barristers are both fascinated and sceptical regarding the “outcome” of memory forensics
  - Juries (and clients) expect you to be able to do this in 15 minute i.e. the CSI effect
- Be persuasive regarding your credibility and the credibility of your chosen process(es)
  - How many times have you done this before – be prepared to give specific case references
  - How have you avoided bias? Why only selected memory artefacts?
    - The other expert will try to pull some exculpatory artefacts – be proactive to explain why these are irrelevant or unreliable
  - Have you tried different processes and arrived at the same result?
  - Is there an academic research base?
- Some words used in Court to describe what I have done...

conjurer  
**ninja alchemist**  
shaman  
voodoo  
wizardry  
witchery **black art**  
**exorcism**

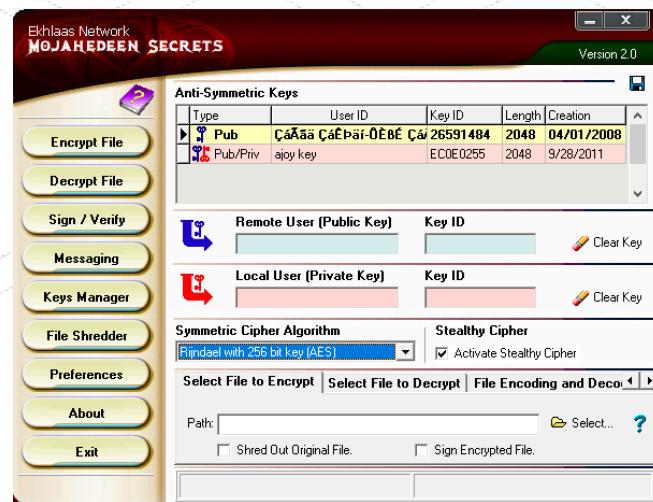
# Extract secrets from pagefile.sys and hibfil.sys

- Windows passwords
- Truecrypt and Veracrypt
- Password managers
  - KeePass
  - OnePassword
  - LastPass
- Grab TOR browsing i.e.  
Darkweb



# Asar al mujedeen

- Used extensively by jihadists across in 2010s
  - Still being used
  - Rumour that NSA inserted monitor into Asar al mujdeen
- GUI collection of tools based on shared libraries e.g. openpgp
- Asar.exe and keyfile on a USB key
- Extract the key from the virtual memory of a computer used by jihadist
  - pagfile.sys
  - hiberfile.sys



# Computer programs

- Programs written in languages like C, C++, etc are compiled into machine code
- Machine code can be executed directly by the CPU
- Machine code is difficult for a human to read
- Machine code cannot be reliably converted back to the source language
- Assembler is an intermediate form which is a direct translation of machine code

```
int _tmain(int argc, _TCHAR* argv[])
{
    int a, b;
    printf("a = ");
    scanf("%d", &a);
    printf("b = ");
    scanf("%d", &b);
    printf("a+b = %d", a+b);
    return 0;
}
```

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	55	9B	EC	83	EC	08	56	8B	35	A4	20	40	00	57	68	F4
00000010	20	40	00	FF	D6	8B	3D	9C	20	40	00	8D	45	F8	50	68
00000020	FC	20	40	00	FF	D7	68	00	21	40	00	FF	D6	8D	4D	FC
00000030	51	68	FC	20	40	00	FF	D7	8B	55	FC	03	55	F8	52	68
00000040	08	21	40	00	FF	D6	83	C4	20	5F	33	C0	5E	8B	E5	5D
00000050	C3	3B	0D	00	30	40	00	75	02	F3	C3	E9	98	02	00	00
00000060	68	32	15	40	00	E8	8B	04	00	00	A1	60	33	40	00	C7
00000070	04	24	2C	30	40	00	FF	35	5C	33	40	00	A3	2C	30	40

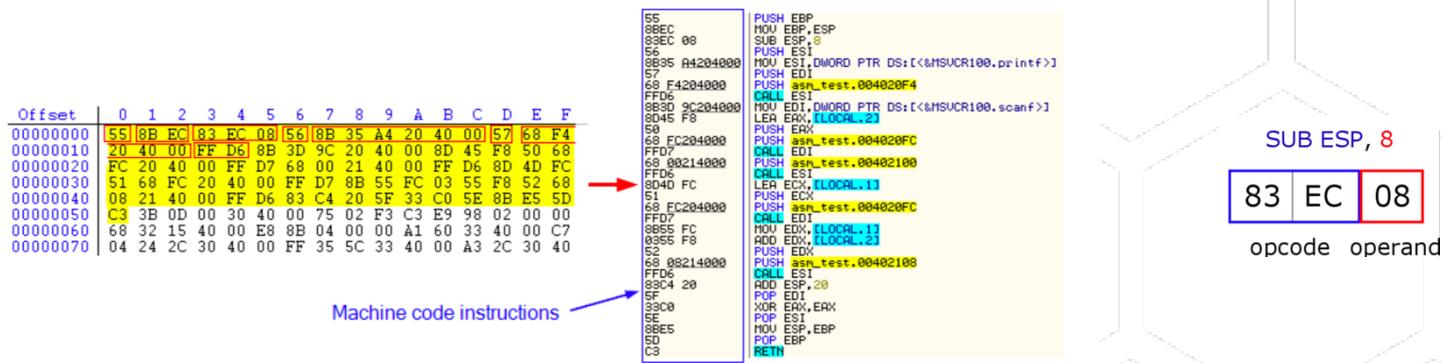
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	55	9B	BC	83	EC	08	56	8B	35	A4	20	40	00	57	68	F4
00000010	20	40	00	FF	D6	8B	3D	9C	20	40	00	8D	45	F8	50	68
00000020	FC	20	40	00	FF	D7	68	00	21	40	00	FF	D6	8D	4D	FC
00000030	51	68	FC	20	40	00	FF	D7	8B	55	FC	03	55	F8	52	68
00000040	08	21	40	00	FF	D6	83	C4	20	5F	33	C0	5E	8B	E5	5D
00000050	C3	3B	0D	00	30	40	00	75	02	F3	C3	E9	98	02	00	00
00000060	68	32	15	40	00	E8	8B	04	00	00	A1	60	33	40	00	C7
00000070	04	24	2C	30	40	00	FF	35	5C	33	40	00	A3	2C	30	40

Machine code instructions

Higher language  $\Rightarrow$  machine code

Higher language  $\Leftrightarrow$  machine code

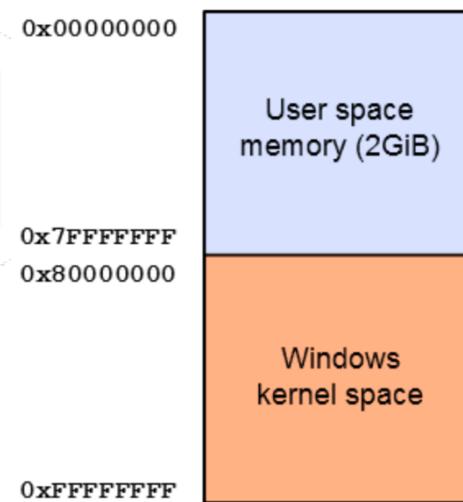
Machine code  $\Leftrightarrow$  assembler



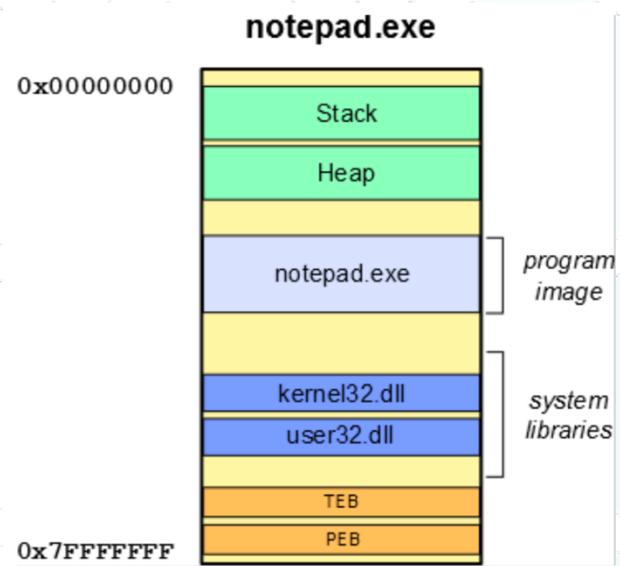
- Opcode = operation that should be performed
- Operand = argument to the operation
  - Immediate value – value encoded in the instruction itself e.g. sub esp, 8
  - Register – operand is one of the registers
  - Memory – operand is in the memory (specified by offset encoded in the instruction)
- 16 types of register
  - 8x general purpose registers (EAX, EBX, ECX, EDX, ESI, EDI, EBP, ESP)
  - 6x segment registers (CS, DS, SS, ES, FS, GS)
  - 1x flags register (EFLAGS)
  - 1x instruction pointer register (EIP)

# Memory

- The Microsoft Windows operating system (as well as most other contemporary operating systems) uses a flat memory model in which programs see memory as a contiguous and linear address space
- On Microsoft Windows, the system memory of 32-bit processes is addressed through 32-bit addresses starting from 0 up to 0xFFFFFFFF (4GB)
  - Not all address space is available to the user-mode processes.
  - User-mode processes can access freely only memory from 0 up to 0x7FFFFFFF (2GB).
  - The second half, that is addresses from 0x80000000 up to 0xFFFFFFFF, is reserved for the operating system

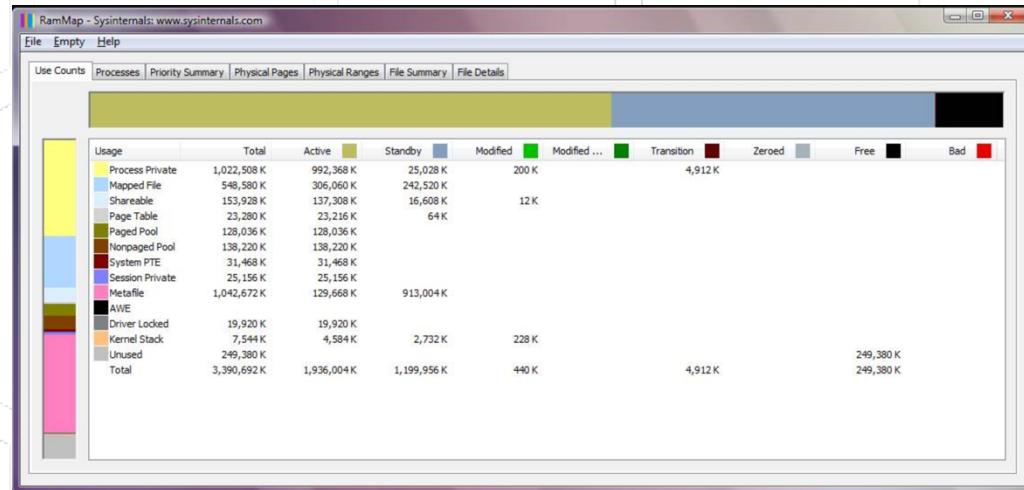


- When a new PE executable is started on a Windows system, a new process is created and the system loader maps the PE file into the process's address space as well as loads all DLL libraries needed by the program
- Process heap and stack are also created
- The Thread Environment Block (TEB) and the Process Environment Block (PEB) are system structures providing information about the current thread's context and the process itself
- Two important memory structures are stack and heap.
  - The **heap** is a memory region where dynamically allocated variables are put.
  - The **stack** is used for storing local variables and tracing function calls in the current thread
  - The stack is also used for passing function arguments and tracing function calls



# RAMMap

- RAMMap is a tool from Microsoft sysinternals that allows you to view memory

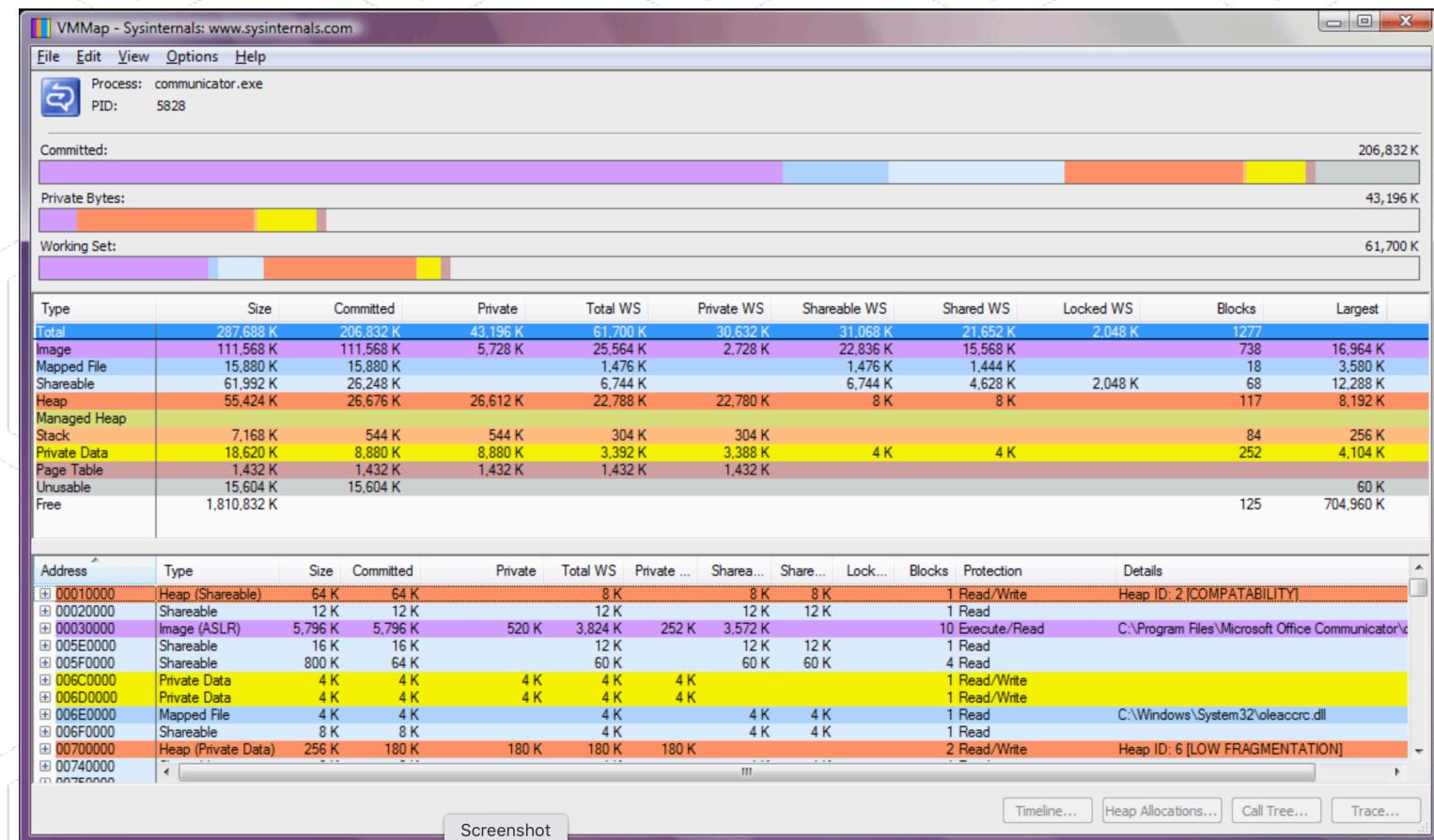


This screenshot shows the RAMMap interface with the 'Processes' tab selected. It lists various processes along with their session ID, PID, private memory usage, standby memory usage, modified memory usage, page table usage, and total memory usage.

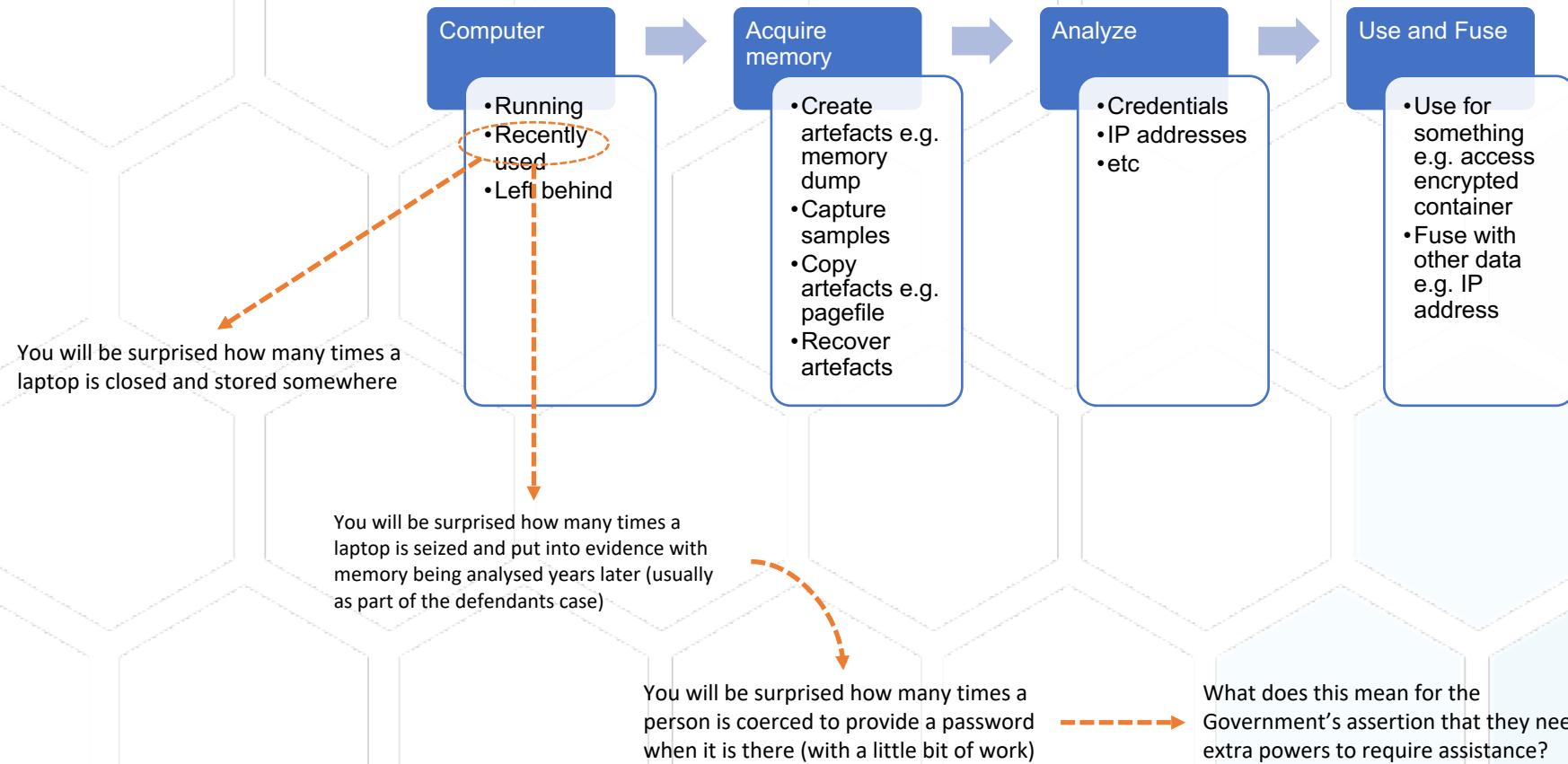
Process	Session	PID	Private	Standby	Modified	Page Table	Total
svchost.exe	0	1108	33,652 K	0 K	0 K	584 K	34,236 K
audiogd.exe	0	1224	13,104 K	0 K	0 K	196 K	13,300 K
winlogon.exe	1	1176	2,720 K	0 K	0 K	216 K	2,936 K
SLsvc.exe	0	1288	4,908 K	0 K	0 K	160 K	5,068 K
svchost.exe	0	1244	4,940 K	0 K	0 K	228 K	5,168 K
svchost.exe	0	1068	15,400 K	0 K	0 K	312 K	15,712 K
spoolsv.exe	0	1652	6,160 K	0 K	0 K	300 K	6,460 K
svchost.exe	0	1692	12,272 K	0 K	0 K	276 K	12,548 K
HPVirtualRooms.	1	4192	35,520 K	0 K	0 K	388 K	35,908 K
rundll32.exe	1	1948	4,300 K	0 K	0 K	228 K	4,528 K
VsTskMgr.exe	0	2404	532 K	584 K	0 K	248 K	1,364 K
WmiPrvSE.exe	0	3500	2,672 K	0 K	0 K	176 K	2,848 K
accoca.exe	0	952	3,072 K	0 K	0 K	176 K	3,248 K
AppleMobileDevI	0	1216	2,200 K	0 K	0 K	220 K	2,420 K
acevents.exe	0	1416	4,512 K	0 K	0 K	220 K	4,732 K
mDNSResponder.e	0	1452	1,872 K	0 K	0 K	180 K	2,052 K
FireSvc.exe	0	2044	1,356 K	11,204 K	0 K	284 K	12,844 K
PwIdMgmtProxy.ex	0	964	8,128 K	0 K	0 K	444 K	8,572 K
HIPSvc.exe	0	2160	5,164 K	0 K	0 K	180 K	5,344 K
LSSrvc.exe	0	2200	1,544 K	0 K	0 K	164 K	1,708 K
ivRegMgr.exe	0	2176	1,412 K	0 K	0 K	136 K	1,548 K
MsACore.exe	0	2252	4,470 K	252 K	0 K	284 K	4,956 K

# VMMap

- VMMap is another tool from Microsoft sysinternals that allows you to view memory

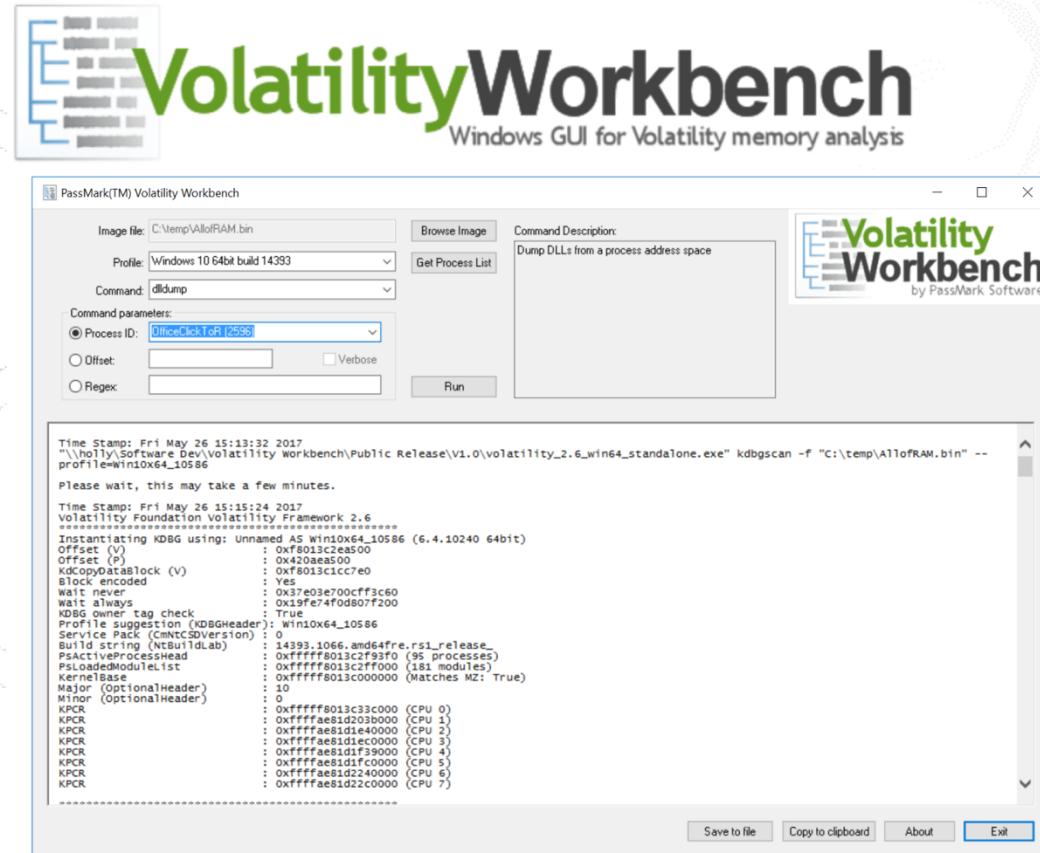


# Workflow



# Capturing memory using tools

- Windows
- Mandient Memoryze
- FTK Imager
- Encase winen.exe
- Magnet RAM Capture
- Belkasoft Live RAM Capture
- OSForensics
- Dumplt
- Memory DD
- WinPmem



<https://www.osforensics.com/tools/volatility-workbench.html>

# Copying memory files

## Windows

### PAGEFILE.SYS

- Virtual memory or “swap file”
- Locked whilst computer is being used

### HIBERFIL.SYS

- Supports hibernation
- In root directory i.e. c:\hiberfil.sys

## Mac (and Linux)

### SWAPFILE

- SWAPFILE and a number
- /private/var/vm
- Only starts when computer is low on memory

### SLEEPIMAGE

- Hibernation
- /var/vm

# BinText

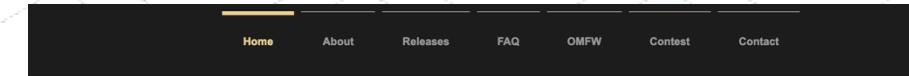
- Is a free tool provided by McAfee
- Used to extract strings from binary files
- IP address and domain names
- Passwords
- Anti-forensics

--	--

# Volatility

- Is the open source tool of choice for memory forensics

Let's do a small exercise using Volatility - you will do this in the tutorial/lab



## VOLATILITY FOUNDATION



### About

The Volatility Foundation is an independent 501(c) (3) nonprofit organization that maintains and promotes open source memory forensics with The Volatility Framework.



### Releases

The Volatility Framework is open source and written in Python. Releases are available in zip and tar archives, Python module installers, and standalone executables.



### OMFW

The Open Memory Forensics Workshop (OMFW) is a half-day event where participants learn about innovative, cutting-edge research from the industry's leading analysts.



### Contest

The Volatility Plugin Contest is your chance to win cash, swag, and the admiration of your peers while giving back to the community. Warning: competition may be fierce!



### FAQ

This is your one-stop shop for the most frequently asked questions regarding Volatility, open source memory forensics, and The Foundation.



### Documents

This page is a collection of books, blogs, white papers, code repositories, and other written sources of documentation authored by members of the community.



### Get Involved

There are many ways to get involved depending on your current skill set, interests, and availability. Visit this page to find out how you can become part of the community!



### Contact

Feel free to contact us via email or the web form. We're always glad to meet new people and entertain your ideas and questions.

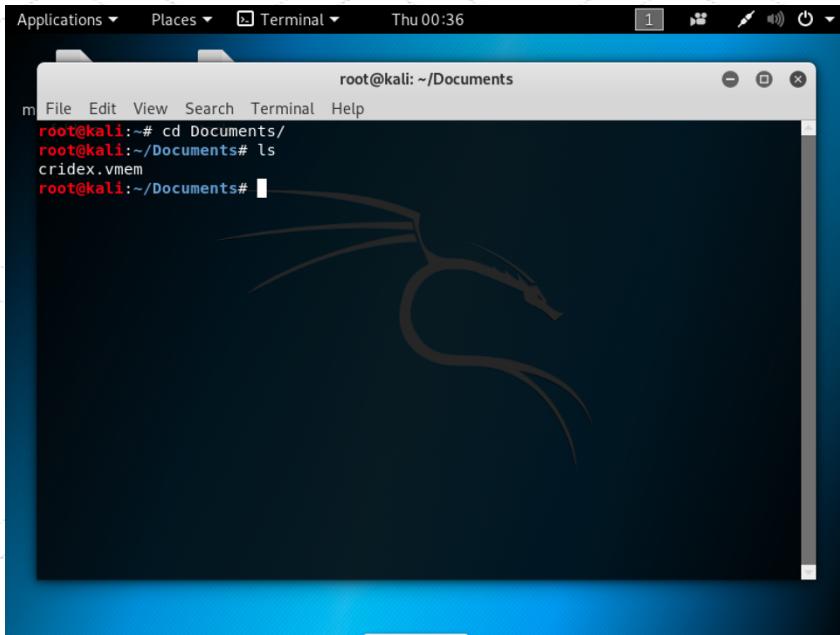
# Use Kali Linux

- Volatility is pre-installed in Kali Linux
- Screenshots are for Kali Linux
  - If you prefer, you can follow on using Windows

User = root

Password = toor





A screenshot of a Kali Linux terminal window titled "Terminal". The window shows the command line interface with the following session:

```
root@kali:~/Documents
m File Edit View Search Terminal Help
root@kali:~# cd Documents/
root@kali:~/Documents# ls
cridex.vmem
root@kali:~/Documents#
```

- Open a terminal
- Change directory to Documents
- Check that the cridex.mem file is there
  - Memory dump used for exercise

- View image information

```
$ volatility -f cridex.vmem imageinfo
```

- Write down the suggested profile – you will need it later

WinXPSP2x86

```
root@kali:~/Documents# volatility -f cridex.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with Win
XPSP2x86)
          AS Layer1 : IA32PagedMemoryPae (Kernel AS)
          AS Layer2 : FileAddressSpace (/root/Documents/cridex.vmem)
          PAE type : PAE
          DTB     : 0x2fe000L
          KDBG    : 0x80545ae0L
          Number of Processors : 1
          Image Type (Service Pack) : 3
          KPCR for CPU 0 : 0xffffdff000L
          KUSER_SHARED_DATA : 0xffffdf0000L
          Image date and time : 2012-07-22 02:45:08 UTC+0000
          Image local date and time : 2012-07-21 22:45:08 -0400
root@kali:~/Documents#
```

- View running processes

```
$ volatility -f cridex.vmem --profile=WinXPSP2x86 pslist
```

```
root@kali:~/Documents# volatility -f cridex.vmem --profile=WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V) Name PID PPID Thds Hnds Sess Wow64 Start Exit
0x823c89c8 System 4 0 53 240 ----- 0
0x822f1020 smss.exe 368 4 3 19 ----- 0 2012-07-22 02:42:31 UTC+0000
0x822a0598 csrss.exe 584 368 9 326 0 0 2012-07-22 02:42:32 UTC+0000
0x82298700 winlogon.exe 608 368 23 519 0 0 2012-07-22 02:42:32 UTC+0000
0x81e2ab28 services.exe 652 608 16 243 0 0 2012-07-22 02:42:32 UTC+0000
0x81e2a3b8 lsass.exe 664 608 24 330 0 0 2012-07-22 02:42:32 UTC+0000
0x82311360 svchost.exe 824 652 20 194 0 0 2012-07-22 02:42:33 UTC+0000
0x81e29ab8 svchost.exe 908 652 9 226 0 0 2012-07-22 02:42:33 UTC+0000
0x823001d0 svchost.exe 1004 652 64 1118 0 0 2012-07-22 02:42:33 UTC+0000
0x821dfda0 svchost.exe 1056 652 5 60 0 0 2012-07-22 02:42:33 UTC+0000
0x82295650 svchost.exe 1220 652 15 197 0 0 2012-07-22 02:42:35 UTC+0000
0x821dea70 explorer.exe 1484 1464 17 415 0 0 2012-07-22 02:42:36 UTC+0000
0x81eb17b8 spoolsv.exe 1512 652 14 113 0 0 2012-07-22 02:42:36 UTC+0000
0x81e7bda0 reader_sl.exe 1640 1484 5 39 0 0 2012-07-22 02:42:36 UTC+0000
0x820e8da0 alg.exe 788 652 7 104 0 0 2012-07-22 02:43:01 UTC+0000
0x821fcda0 wuauctl.exe 1136 1004 8 173 0 0 2012-07-22 02:43:46 UTC+0000
0x8205bda0 wuauctl.exe 1588 1004 5 132 0 0 2012-07-22 02:44:01 UTC+0000
root@kali:~/Documents#
```

- View parent processes

```
$ volatility -f cridex.vmem --profile=WinXPSP2x86 pstree
```

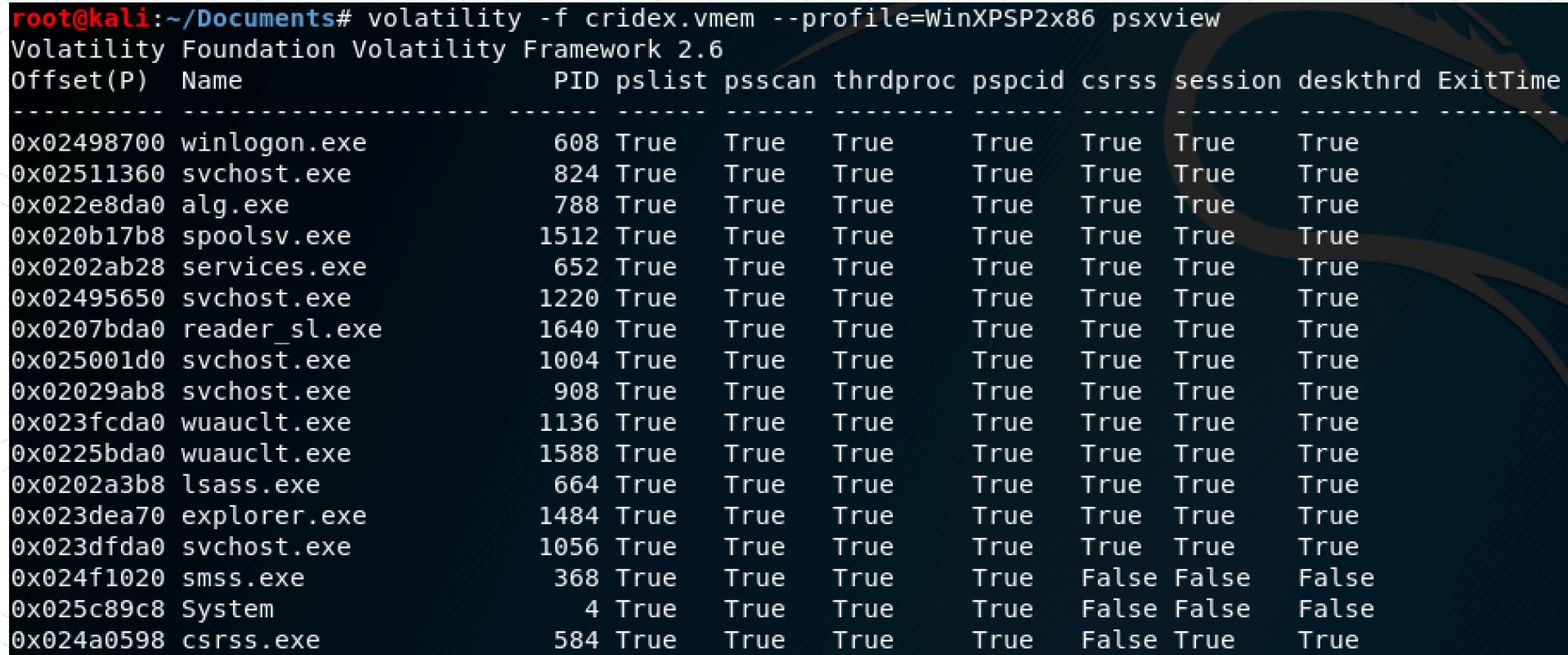
- Notice reader\_sl.exe spawned by explorer

```
root@kali:~/Documents# volatility -f cridex.vmem --profile=WinXPSP2x86 pstree
Volatility Foundation Volatility Framework 2.6
Name          Pid  PPid  Thds  Hnds Time
-----+-----+-----+-----+-----+-----+
0x823c89c8:System          4      0    53   240 1970-01-01 00:00:00 UTC+0000
. 0x822f1020:smss.exe      368     4     3    19 2012-07-22 02:42:31 UTC+0000
.. 0x82298700:winlogon.exe 608    368    23   519 2012-07-22 02:42:32 UTC+0000
... 0x81e2ab28:services.exe 652    608    16   243 2012-07-22 02:42:32 UTC+0000
.... 0x821dfda0:svchost.exe 1056   652     5    60 2012-07-22 02:42:33 UTC+0000
..... 0x81eb17b8:spoolsv.exe 1512   652    14   113 2012-07-22 02:42:36 UTC+0000
..... 0x81e29ab8:svchost.exe 908    652     9   226 2012-07-22 02:42:33 UTC+0000
..... 0x823001d0:svchost.exe 1004   652    64  1118 2012-07-22 02:42:33 UTC+0000
..... 0x8205bda0:wuauclt.exe 1588   1004    5   132 2012-07-22 02:44:01 UTC+0000
..... 0x821fcda0:wuauclt.exe 1136   1004    8   173 2012-07-22 02:43:46 UTC+0000
..... 0x82311360:svchost.exe 824    652    20   194 2012-07-22 02:42:33 UTC+0000
..... 0x820e8da0:alg.exe     788    652     7   104 2012-07-22 02:43:01 UTC+0000
..... 0x82295650:svchost.exe 1220   652    15   197 2012-07-22 02:42:35 UTC+0000
... 0x81e2a3b8:lsass.exe     664    608    24   330 2012-07-22 02:42:32 UTC+0000
.. 0x822a0598:csrss.exe     584    368     9   326 2012-07-22 02:42:32 UTC+0000
0x821dea70:explorer.exe    1484   1464    17   415 2012-07-22 02:42:36 UTC+0000
. 0x81e7bda0:reader_sl.exe 1640   1484     5    39 2012-07-22 02:42:36 UTC+0000
root@kali:~/Documents#
```

- Are any processes trying to hide?

```
$ volatility -f cridex.vmem --profile=WinXPSP2x86 psxview
```

- If so, FALSE will appear in the first two columns



Offset(P)	Name	PID	pslist	psscan	thrdproc	pspcid	csrss	session	deskthrd	ExitTime
0x02498700	winlogon.exe	608	True	True	True	True	True	True	True	
0x02511360	svchost.exe	824	True	True	True	True	True	True	True	
0x022e8da0	alg.exe	788	True	True	True	True	True	True	True	
0x020b17b8	spoolsv.exe	1512	True	True	True	True	True	True	True	
0x0202ab28	services.exe	652	True	True	True	True	True	True	True	
0x02495650	svchost.exe	1220	True	True	True	True	True	True	True	
0x0207bda0	reader_sl.exe	1640	True	True	True	True	True	True	True	
0x025001d0	svchost.exe	1004	True	True	True	True	True	True	True	
0x02029ab8	svchost.exe	908	True	True	True	True	True	True	True	
0x023fcda0	wuauctl.exe	1136	True	True	True	True	True	True	True	
0x0225bda0	wuauctl.exe	1588	True	True	True	True	True	True	True	
0x0202a3b8	lsass.exe	664	True	True	True	True	True	True	True	
0x023dea70	explorer.exe	1484	True	True	True	True	True	True	True	
0x023dfda0	svchost.exe	1056	True	True	True	True	True	True	True	
0x024f1020	smss.exe	368	True	True	True	True	False	False	False	
0x025c89c8	System	4	True	True	True	True	False	False	False	
0x024a0598	csrss.exe	584	True	True	True	True	False	True	True	

- Look at connections and sockets

```
$ volatility -f cridex.vmem --profile=WinXPSP2x86 connscan
```

```
$ volatility -f cridex.vmem --profile=WinXPSP2x86 sockets
```

- Normally use netscan but not available for WinXPSP2x86

```
root@kali:~/Documents# volatility -f cridex.vmem --profile=WinXPSP2x86 connscan
Volatility Foundation Volatility Framework 2.6
Offset(P) Local Address           Remote Address          Pid
-----
0x02087620 172.16.112.128:1038    41.168.5.140:8080    1484
0x023a8008 172.16.112.128:1037    125.19.103.198:8080   1484
root@kali:~/Documents# volatility -f cridex.vmem --profile=WinXPSP2x86 sockets
Volatility Foundation Volatility Framework 2.6
Offset(V)  PID  Port Proto Protocol      Address      Create Time
-----
0x81ddb780  664  500   17 UDP          0.0.0.0      2012-07-22 02:42:53 UTC+0000
0x82240d08  1484  1038   6 TCP          0.0.0.0      2012-07-22 02:44:45 UTC+0000
0x81dd7618  1220  1900   17 UDP          172.16.112.128 2012-07-22 02:43:01 UTC+0000
0x82125610  788   1028   6 TCP          127.0.0.1     2012-07-22 02:43:01 UTC+0000
0x8219cc08  4     445    6 TCP          0.0.0.0      2012-07-22 02:42:31 UTC+0000
0x81ec23b0  908   135    6 TCP          0.0.0.0      2012-07-22 02:42:33 UTC+0000
0x82276878  4     139    6 TCP          172.16.112.128 2012-07-22 02:42:38 UTC+0000
0x82277460  4     137    17 UDP         172.16.112.128 2012-07-22 02:42:38 UTC+0000
0x81e76620  1004  123    17 UDP         127.0.0.1     2012-07-22 02:43:01 UTC+0000
0x82172808  664   0     255 Reserved    0.0.0.0      2012-07-22 02:42:53 UTC+0000
0x81e3f460  4     138    17 UDP         172.16.112.128 2012-07-22 02:42:38 UTC+0000
0x821f0630  1004  123    17 UDP         172.16.112.128 2012-07-22 02:43:01 UTC+0000
0x822cd2b0  1220  1900   17 UDP         127.0.0.1     2012-07-22 02:43:01 UTC+0000
0x82172c50  664   4500   17 UDP         0.0.0.0      2012-07-22 02:42:53 UTC+0000
0x821f0d00  4     445    17 UDP         0.0.0.0      2012-07-22 02:42:31 UTC+0000
```

- Look at PID 1484 i.e. explorer
  - two connections, port 1038 and port 1037
- One is still open i.e. port 1038
- There is no socket entry for 1037 so that is suspicious

```
root@kali:~/Documents# volatility -f cridex.vmem --profile=WinXPSP2x86 connscan
Volatility Foundation Volatility Framework 2.6
Offset(P) Local Address           Remote Address          Pid
-----
0x02087620 172.16.112.128:1038    41.168.5.140:8080    1484
0x023a8008 172.16.112.128:1037    125.19.103.198:8080  1484
root@kali:~/Documents# volatility -f cridex.vmem --profile=WinXPSP2x86 sockets
Volatility Foundation Volatility Framework 2.6
Offset(V)   PID   Port Proto Protocol      Address      Create Time
-----
0x81ddb780   664    500   17 UDP          0.0.0.0      2012-07-22 02:42:53 UTC+0000
0x82240d08   1484   1038   6 TCP          0.0.0.0      2012-07-22 02:44:45 UTC+0000
0x81dd7618   1220   1900   17 UDP          172.16.112.128 2012-07-22 02:43:01 UTC+0000
0x82125610   788    1028   6 TCP          127.0.0.1     2012-07-22 02:43:01 UTC+0000
0x8219cc08     4    445    6 TCP          0.0.0.0      2012-07-22 02:42:31 UTC+0000
0x81ec23b0   908    135    6 TCP          0.0.0.0      2012-07-22 02:42:33 UTC+0000
0x82276878     4    139    6 TCP          172.16.112.128 2012-07-22 02:42:38 UTC+0000
0x82277460     4    137    17 UDP         172.16.112.128 2012-07-22 02:42:38 UTC+0000
0x81e76620   1004   123    17 UDP         127.0.0.1     2012-07-22 02:43:01 UTC+0000
0x82172808   664    0     255 Reserved    0.0.0.0      2012-07-22 02:42:53 UTC+0000
0x81e3f460     4    138    17 UDP         172.16.112.128 2012-07-22 02:42:38 UTC+0000
0x821f0630   1004   123    17 UDP         172.16.112.128 2012-07-22 02:43:01 UTC+0000
0x822cd2b0   1220   1900   17 UDP         127.0.0.1     2012-07-22 02:43:01 UTC+0000
0x82172c50   664    4500   17 UDP         0.0.0.0      2012-07-22 02:42:53 UTC+0000
0x821f0d00     4    445    17 UDP         0.0.0.0      2012-07-22 02:42:31 UTC+0000
```

- Look at last commands run using cmdscan, consoles and cmdline

- cmdscan and consoles don't produce relevant results in this example

```
$ volatility -f cridex.vmem --profile=WinXPSP2x86 cmdline
```

```
Command line : C:\WINDOWS\system32\lsass.exe
*****
svchost.exe pid: 824
Command line : C:\WINDOWS\system32\svchost -k DcomLaunch
*****
svchost.exe pid: 908
Command line : C:\WINDOWS\system32\svchost -k rpcss
*****
svchost.exe pid: 1004
Command line : C:\WINDOWS\System32\svchost.exe -k netsvcs
*****
svchost.exe pid: 1056
Command line : C:\WINDOWS\system32\svchost.exe -k NetworkService
*****
svchost.exe pid: 1220
Command line : C:\WINDOWS\system32\svchost.exe -k LocalService
*****
explorer.exe pid: 1484
Command line : C:\WINDOWS\Explorer.EXE
*****
spoolsv.exe pid: 1512
Command line : C:\WINDOWS\system32\spoolsv.exe
*****
reader_sl.exe pid: 1640
Command line : "C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe"
*****
alg.exe pid: 788
Command line : C:\WINDOWS\System32\alg.exe
*****
wuauctl.exe pid: 1136
Command line : "C:\WINDOWS\system32\wuauctl.exe" /RunStoreAsComServer Local\[3ec]SUSDSb81eb56fa3105543beb3109274ef8ec1
*****
wuauctl.exe pid: 1588
Command line : "C:\WINDOWS\system32\wuauctl.exe"
```

- Look at last commands run using cmdscan, consoles and cmdline

- cmdscan and consoles don't produce relevant results in this example

```
$ volatility -f cridex.vmem --profile=WinXPSP2x86 cmdline
```

```
Command line : C:\WINDOWS\system32\lsass.exe
*****
svchost.exe pid: 824
Command line : C:\WINDOWS\system32\svchost -k DcomLaunch
*****
svchost.exe pid: 908
Command line : C:\WINDOWS\system32\svchost -k rpcss
*****
svchost.exe pid: 1004
Command line : C:\WINDOWS\System32\svchost.exe -k netsvcs
*****
svchost.exe pid: 1056
Command line : C:\WINDOWS\system32\svchost.exe -k NetworkService
*****
svchost.exe pid: 1220
Command line : C:\WINDOWS\system32\svchost.exe -k LocalService
*****
explorer.exe pid: 1484
Command line : C:\WINDOWS\Explorer.EXE
*****
spoolsv.exe pid: 1512
Command line : C:\WINDOWS\system32\spoolsv.exe
*****
reader_sl.exe pid: 1640
Command line : "C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe"
*****
alg.exe pid: 788
Command line : C:\WINDOWS\System32\alg.exe
*****
wuauctl.exe pid: 1136
Command line : "C:\WINDOWS\system32\wuauctl.exe" /RunStoreAsComServer Local\[3ec]SUSDSb81eb56fa3105543beb3109274ef8ec1
*****
wuauctl.exe pid: 1588
Command line : "C:\WINDOWS\system32\wuauctl.exe"
```

- Look at last commands run using cmdscan, consoles and cmdline

```
$ volatility -f cridex.vmem --profile=WinXPSP2x86 procdump -p 1640 --dump-dir .
```

```
$ volatility -f cridex.vmem --profile=WinXPSP2x86 memdump -p 1640 --dump-dir .
```

```
root@kali:~/Documents# volatility -f cridex.vmem --profile=WinXPSP2x86 procdump -p1640 --dump-dir .
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase Name Result
-----
0x81e7bda0 0x00400000 reader_sl.exe OK: executable.1640.exe
root@kali:~/Documents# volatility -f cridex.vmem --profile=WinXPSP2x86 memdump -p1640 --dump-dir .
Volatility Foundation Volatility Framework 2.6
*****
Writing reader_sl.exe [ 1640] to 1640.dmp
```

- Result is a file 1640.dmp
  - Extract strings and save as text

```
$ strings 1640.dmp > 1640.txt
```

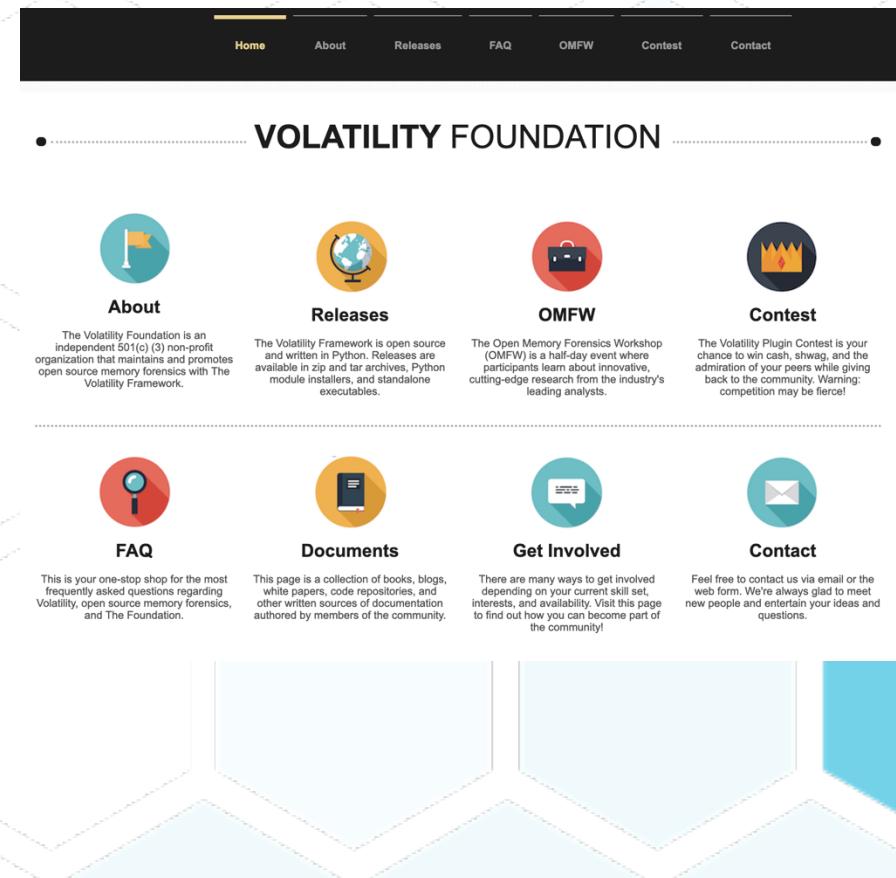
\*treasurypathways.com\*  
\*CorporateAccounts.com\*  
\*weblink.websterbank.co m\*  
\*secure7.onlineaccess1.co m\*  
\*tr.tranzact.org\*  
\*onlineaccess1.com\*  
\*secureport.texascapitalba nk.com\*  
\*Authentication/zbf/k/\*  
\*ebc\_ebc1961\*  
\*tdbank.com\*  
\*online.ocvb.com\*  
\*ebanking-services.com\*  
\*schwab.com\*  
\*billmeler.com\*  
\*chase.com\*  
\*bankofamerica.com\*  
\*pnc.com\*  
\*suntrust.com\*  
\*wellsfargo.com\*  
\*ibanking-services.com\*  
\*bankonline.umpquabank.co m\*  
\*servlet/teller\*  
\*nsbank.com\*  
\*securitycalbanktrust.c om\*  
\*security\*  
\*/Common/SignOn/Starta sp\*  
\*telepc.net\*  
\*enterprise2.openbank.co m\*  
\*BusinessAppsHome\*  
\*global1.onlinebank.com\*  
\*webexpress\*  
\*/sbuser/\*  
\*webcash\*  
\*firstbanks.com\*  
\*bxs.com\*  
\*businesslogin\*  
\*hbcash.exe\*  
\*otm.suntrust.com\*  
\*/inets/\*  
\*corpCH\*  
\*/IBWS/\*  
\*/bs.\*  
\*livewire/\*  
\*/olbb/\*  
\*fnfgbusnessonline.enter prisebanker.com\*  
\*lakelcitybank.webcashmg mt.com\*  
\*/inets/\*  
\*bobs.sovereignbank.com\*  
\*CLKCCM\*  
\*directive4biz.com\*  
\*e-moneyer.com\*  
\*cashman\*  
\*securentrycorp.amegyban k.com\*  
\*netteller\*  
\*onlineserv/CM\*  
\*nubi\*  
\*ib5.secure-banking\*  
\*ib5.secure-banking\*  
\*bilk\*  
\*svbconnect.com\*  
\*goldleaf\*  
\*webcm/\*  
\*www.amegybank.com/\*  
\*/wires/\*  
\*bankbyweb\*  
\*internet-ebanking.com\*  
\*treasury.pnbank.com\*  
\*sso.uboc\*  
\*cashplus\*  
\*towernet.capitalonebank .com\*  
\*nationalcity.com/consln t\*  
\*authmaster.nationalcity.c om\*  
\*om/tmgmt\*  
\*businessonline.tdbank.co m\*  
\*treasurydirect.tdbank.co m\*  
\*express.53.com/express/l ogon.action\*  
\*access.usbank.com\*  
\*treasury.wamu.com\*  
\*associated.bank.com\*  
\*cashproonline.bankofame rica.com\*  
\*cib.bankofthewest.com\*  
\*cmol.bbt.com/auth\*  
\*bmoharrisprivatebanking online.com\*  
\*bnycash.bankofny.com\*  
\*cib.bankofthewest.com\*  
\*cmol.bbt.com/auth\*  
\*bmoharrisprivatebanking online.com\*  
\*bnycash.bankofny.com\*  
\*singlepoint.usbank.com\*  
\*sso.unionbank.com\*  
\*commercial.wachovia.co m\*  
\*wcmfd/wcmpw\*  
\*phpc/servlet\*  
\*webinfoius.mandtbank.co m\*  
\*wellsoffice.wellsfargo.co m\*  
\*bmomutualfunds.com\*  
\*/netbnx/\*  
\*businessbanking.cibc.com \*  
\*nashvillecitizensbank.com \*  
\*access.rbsm.com/logon\*  
\*bolb-west.associatedbank.com\*  
\*com/K1/\*  
\*pub/htm\*  
\*businessaccess citibank.ci tgroup.com\*  
\*achieveaccess.citizensban k.com\*  
\*cib.bankofthewest.com\*  
\*cmol.bbt.com/auth\*  
\*bmoharrisprivatebanking asbank.com\*  
\*bnycash.bankofny.com\*  
\*cashanalyzer.com\*  
\*fixmanager.bnymellon.co m\*  
\*ebanking-services.com\*  
\*/ebc\_ebc1961/\*  
\*cashman\*  
\*express.53.com/express/\*  
\*cbs.firstcitizens.com\*  
\*banking.firsttennessee.biz \*  
\*efirstbank.com\*  
\*treas-mgt.frostbank.com\*  
\*businessonline.huntingto n.com\*  
\*lbbpowerlink.com\*  
\*access.jpmorgan.com\*  
\*bilk.com\*  
\*businessportal.mibank.co m\*  
\*webbankingforbusiness. mandtbank.com\*  
\*mbahexpress.com\*  
\*premierview.membersuni ted.org\*  
\*cashmanager.mizuhoe- treasurer.com\*  
\*enterbank.com\*  
\*ntrs.com\*  
\*northerntrust.com\*  
\*Common/SignOn/\*  
\*/CLKCCM/\*  
\*bankofamerica.com\*  
\*onlinresv/CM\*  
\*treasury.pnbank.com\*  
\*rbs.com/wps/portal/cb/a pplications\*  
\*sandsysbank.com\*  
\*ssl.selectpayment.com/m p\*  
\*svbconnect.com\*  
\*onlinebanking.banksterlin g.com\*  
\*businessonline.tdbank.co m\*  
\*treasurydirect.tdbank.co m\*  
\*passport.texascapitalbank .com\*  
\*nashvillecitizensbank.com \*  
\*singlepoint.usbank.com\*  
\*sso.unionbank.com\*  
\*commercial.wachovia.co m\*  
\*wcmfd/wcmpw\*  
\*phpc/servlet\*  
\*webinfoius.mandtbank.co m\*  
\*wellsoffice.wellsfargo.co m\*  
\*bmomutualfunds.com\*  
\*/netbnx/\*  
\*businessbanking.cibc.com \*  
\*nashvillecitizensbank.com \*  
\*/Authentication/zbf/k/\*  
\*singlepoint.usbank.com\*  
\*sso.unionbank.com\*  
\*commercial.wachovia.co m\*  
\*wcmfd/wcmpw\*  
\*phpc/servlet\*  
\*webinfoius.mandtbank.co m\*  
\*wellsoffice.wellsfargo.co m\*  
\*bmomutualfunds.com\*  
\*/netbnx/\*  
\*businessbanking.cibc.com \*  
\*cibc.online.cibc.com\*  
\*royalbank.com/cgi-bin/rbaccess\*  
\*access.rbsm.com/logon\*  
\*/cmserver/\*  
\*com/K1/\*  
\*pub/html\*  
\*businessaccess citibank.ci tgroup.com\*  
\*achieveaccess.citizensban k.com\*  
\*cbs.firstcitizens.com\*  
\*banking.firsttennessee.biz \*  
\*efirstbank.com\*  
\*treas-mgt.frostbank.com\*  
\*businessonline.huntingto n.com\*  
\*lbbpowerlink.com\*  
\*access.jpmorgan.com\*  
\*bilk.com\*  
\*businessportal.mibank.co m\*  
\*webbankingforbusiness. mandtbank.com\*  
\*mbahexpress.com\*  
\*premierview.membersuni ted.org\*  
\*cashmanager.mizuhoe- treasurer.com\*  
\*enterbank.com\*  
\*ntrs.com\*  
\*treas-mgt.frostbank.com\*  
\*businessonline.huntingto n.com\*  
\*lbbpowerlink.com\*  
\*access.jpmorgan.com\*  
\*bilk.com\*  
\*businessportal.mibank.co m\*  
\*webbankingforbusiness. mandtbank.com\*  
\*mbahexpress.com\*  
\*premierview.membersuni ted.org\*  
\*cashmanager.mizuhoe- treasurer.com\*  
\*enterbank.com\*  
\*ntrs.com\*  
\*cbscse1.\*  
\*e-moneyer\*  
\*createWire\*  
\*createCorpWire\*  
\*business.netbankerplus.c om\*  
\*secure.fundsexpress.com\*  
\*firstranks.com/olb\*  
\*/CASHplus/\*  
\*sbuser/\*  
\*cashman\*  
\*onineaccess1.com\*  
\*Pres\_WA\_Wires\*  
\*onlinencr.com\*  
\*bankonline.umpquabank.co m\*  
\*globalin.leumiusa.com\*  
\*my.statestreet.com\*  
\*secure.com/TekPortfolio\*  
\*inetbanker\*  
\*secure.ally.com\*  
\*unitedbankwi.com\*  
\*hproxy.exe\*  
\*/inets/\*  
\*otm.suntrust.com\*  
\*cmserver\*  
\*svbconnect\*  
\*secure.fsbperkasie.com\*  
\*scottvalleybank.com\*  
\*hillsbank.com\*  
\*vpn1.\*  
\*/olb/\*  
\*cu.com\*  
\*cu.org\*  
\*paylinks.cunet.org\*  
\*1stunitedbankfl\*  
\*paylinks.cunet.org\*  
\*adworks.com\*  
\*bankonline.sboff.com\*  
\*bankofbermuda.com\*  
\*tdcommercialbanking\*  
\*bxs.com\*  
\*solutions.corporate.com\*  
\*cbusinessonline.com\*  
\*checkgateway\*  
\*constitutioncor.org\*  
\*corporate.epfc.com\*  
\*epd.uscentral.org\*  
\*login\_business.asp\*  
\*global.ebanking.com\*  
\*itinternet.net\*  
\*mcb-home.com/online\*  
\*metronbankdirect.com\*  
\*midatlanticcorp.org\*  
\*nmcn-icm.com\*  
\*online.1stnb.com\*  
\*westfield.accounts-in-view.com\*  
\*secure-eccu.org\*  
\*secure.1stfedbank.com\*  
\*securebanking.ctbks.com \*  
\*secure.dalhartfederal.co m\*  
\*businesslogins.asp\*  
\*CorporateAccounts\*  
\*securentry\*  
\*/ach/\*  
\*/wire/\*  
\*corpCH\*  
\*treasurypathways.com\*  
\*mycorporate.org\*  
\*ecash.\*  
\*secure.fnbnhutch.com\*  
\*hsbc.com.mx\*  
\*/IBWS/\*  
\*CorporateAccounts\*  
\*securentry\*  
\*/ach/\*  
\*/wire/\*  
\*corpCH\*  
\*treasurypathways.com\*  
\*mycorporate.org\*  
\*ecash.\*  
\*secure.fnbnhutch.com\*  
\*westernpb.comcash.com\*  
\*springbankconnect.com/v iews/login/\*  
\*statebanktx.cgi-bin/prosperity.asp\*  
\*treasurylinweb.com\*  
\*web.accessor.com\*  
\*wtdirect.com\*  
\*business.macu.com\*  
\*cencorpco.com\*  
\*webinfocus.mandtbank.c om\*  
\*commercialservices.mand tbank.com\*  
\*commercialservices\*  
\*sbuser/\*  
\*fixmanager.bankofny.com \*  
\*commercebusinessdirect .com\*  
\*corporatebankingweb\*  
\*comerica.com/businessco nnect/\*  
\*firstranks.com/olb\*  
\*ebill.highmark.com\*  
\*businessonline.huntingto n.com\*  
\*businessmanager.com\*  
\*gib.bankofthewest.com\*  
\*secure.2.umb.com\*  
\*sso.uboc.com\*  
\*libertymutualbusinessdire ct.com\*  
\*portfolioonline.metavant e.com\*  
\*scottvalleybank.com\*  
\*hillsbank.com\*  
\*authmaster.nationalcity.c om\*  
\*ibusinessnet.com\*  
\*lbbpowerlink.com\*  
\*nbarizona.com/login\_busi ness.jsp\*  
\*online.dollarbank.com\*  
\*nsbank.com/biz\*  
\*nsbank.com/biz\*  
\*banking.calbanktrust.com \*  
\*BB/LOGON/\*  
\*trustmark.openbank.com\*  
\*businessclassonline.com\*  
\*constitutioncor.org\*  
\*corporate.epfc.com\*  
\*epd.uscentral.org\*  
\*login\_business.asp\*  
\*global.ebanking.com\*  
\*itinternet.net\*  
\*mcb-home.com/online\*  
\*metronbankdirect.com\*  
\*midatlanticcorp.org\*  
\*nmcn-icm.com\*  
\*online.1stnb.com\*  
\*westfield.accounts-in-view.com\*  
\*secure-eccu.org\*  
\*secure.1stfedbank.com\*  
\*securebanking.ctbks.com \*  
\*secure.dalhartfederal.co m\*  
\*businesslogins.asp\*  
\*CorporateAccounts\*  
\*securentry\*  
\*/ach/\*  
\*/wire/\*  
\*corpCH\*  
\*treasurypathways.com\*  
\*mycorporate.org\*  
\*ecash.\*  
\*secure.fnbnhutch.com\*  
\*westernpb.comcash.com\*  
\*springbankconnect.com/v iews/login/\*  
\*statebanktx.cgi-bin/prosperity.asp\*  
\*treasurylinweb.com\*  
\*web.accessor.com\*  
\*commercialservices.mand tbank.com\*  
\*commercialservices\*  
\*moneymanagersps.com\*  
\*usgateaway2.rbs.com\*  
\*top.capitalonelbank.com\*  
\*otm.unsuntrust.com\*  
\*suntrust.com\*  
\*onlinebanker.usbank.com\*  
\*onlinebanker\*  
\*bbo.1stsource.com\*  
\*lasallebank.com/business \_solutions.html\*  
\*business\_solutions\*  
\*ab.portalvalut.com\*  
\*trustweb.com\*  
\*secure.bancinternetgroup .com\*  
\*onlinebank.wesbanco.co m\*  
\*online.wilberbank.com\*  
\*northbaybarcorp.com\*  
\*internetbanker.cc\*  
\*auth.umb.com\*  
\*merchantsbk.inetbanker.co m\*  
\*bizcurrency.com\*  
\*metronbankdirect.com/cor p\_login.page.asp\*  
\*metronbankdirect.com\*  
\*lakelandbank.com\*  
\*chase.com\*  
\*etrade.com\*  
\*paypal.com\*  
\*schwab.com\*  
\*ameritrade.com\*  
\*santander.co.uk\*  
\*ffinonline.com\*  
\*exness.com\*  
\*suncorpbank.com.au\*  
\*hsbc.co.uk\*  
\*ablv.com\*  
\*access.bankplc.com\*  
\*alphanet.com.cy\*  
\*baltikums.com\*  
\*baltikums.eu\*  
\*banesco.com.pa\*  
\*bankaustria.at\*  
\*banknet.lv\*  
\*bankofcyprus.com\*  
\*bobibanking.com\*  
\*butterfieldonline.ky\*  
\*cimbangque.net\*  
\*cs.directnet.com\*  
\*directnet.com\*  
\*sunshinestatefederal.wbl nk.com\*  
\*cashplus\*  
\*cfgbusinessaccess.com\*  
\*RBS\_Corporal\*  
\*treasury.amsouth.com\*  
\*fbncconnect.com\*  
\*lionbank.com\*  
\*ecash.fsbm.com\*  
\*bscincky.com\*  
\*pacificeenterprisebank.co m\*  
\*westernpb.comcash.com\*  
\*springbankconnect.com/v iews/login/\*  
\*statebanktx.cgi-bin/prosperity.asp\*  
\*treasurylinweb.com\*  
\*web.accessor.com\*  
\*commercialservices.mand tbank.com\*  
\*i-linija.lt\*  
\*loyalbank.com\*  
\*marfinbank.com.cy\*  
\*multineb.eu\*  
\*nordea.com\*  
\*secure.ltblbank.com\*  
\*secure.ltvlbank.com\*  
\*swedbank.lv\*  
\*norvik.lv\*  
\*online.alphabank.com.cy\*  
\*online.citadelte.lv\*  
\*online.lbk.lv\*  
\*online.ibl.com.lb\*  
\*online- offshore.lloydsts.com\*  
\*online.usb.com.cy\*  
\*parax.lv\*  
\*handelsbanken.lv\*  
\*pastabanka.lv\*  
\*piraeusbank.com\*  
\*iv.uncreditbanking.net\*  
\*privatbank.lv\*  
\*rbcscouts.com\*  
\*rbdigital.com\*  
\*rbsibanking.com\*  
\*rbsm.com\*  
\*bwboard.lv\*  
\*rcbcom\*  
\*rietumu.lv\*  
\*s2b.\*  
\*s2b.standardchartered.co m\*  
\*sampopank\*  
\*sampopank.ree\*  
\*seb.ree\*  
\*seb.lt\*  
\*seb.lv\*  
\*secure.currency.lloydsts b-offshore.com\*  
\*snoras.com\*  
\*tbb.ee\*  
\*trast.net\*  
\*trastnet.tkb.com.cy\*  
\*ub.lt\*  
\*valartis.at\*  
\*valartis.li\*  
\*vpbank.com\*  
\*ubs.com\*  
\*acbtz.com\*  
\*azanibank.co.tz\*  
\*bankm.co.tz\*  
\*dtbafrika.com\*  
\*habibbank\*  
\*BusinessappsHome\*  
\*nab.com.au\*  
\*us.hsbc.com\*  
\*online.citibank.com/\*  
\*BalanceHome\*  
\*PassmarkChallenge\*  
\*ktt.key.com\*  
\*cm.neteller.com\*  
\*/Web\_Bank\*  
\*jqueryaddonsv2.js\*  
http://188.0.138.8080/zb/\_v\_01\_a/in/cp.php  
\*account.authorize.net



# Other useful plug-ins

- Convert raw memory dump to dmp format
  - Raw2dump
- Extract memory cached files
  - dumpfiles
- Dump password hashes from memory
  - dummp hashes
  - hashdump
- Truecrypt
  - Truecryptmaster
  - Truecryptpassphrase
  - Truecryptsummary

See <https://www.volatilityfoundation.org/>



# Short break – 5 mins

And then Week 3 part 3:

- Explain weekly tutorial/lab