Texas Tech University

A Course on Digital forensics

Memory Forensics

Module 1 – System Overview

Akbar S. Namin, Spring 2018

QUIZ-1

It includes chapter1, and includes 5 multiple choice questions, 1 true-false question, and 1 open-ended question that requires practice.

Q1-6: 0.5 points

Q7: 2 points

1. What component assists the CPU in address translation?

The Memory Management Unit (MMU)
The Address Translation Unit (ATU)
The Central Memory Hub (CMH)
The Memory Management Controller (MMC)
The correct answer is: A

2. The unit which acts as an intermediate agent between memory and backing store to reduce process time is _____.
   - **A.** TLB's
   - **B.** Registers
   - **C.** Page tables
   - **D.** Cache

The correct answer is: D
Explanation: The cache's help in data transfers by storing most recently used memory pages.

3. When dealing with raw, padded memory dumps, a physical address is an offset into the memory dump file. True or False?

The correct answer is: True

4. Which statement(s) are false?
   - **A.** IA32 architecture is also known as x86.
   - **B.** Physical Address Extension (PAE) allows up to 64GB of physical memory.
   - **C.** 64-bit CPUs only actually use 52 bits of the available address space.
   - **D.** A typical page size is 4KB, but it can be larger if the page size entry (PSE) flag is set.

E. All of the above.

The correct answer is: C (they use 48 bits)

5. Which CPU register is used to store the directory table base (page directory base)?
   A. CR0
   B. EAX
   C. CR3
   D. DR3

The correct answer is: C

6. Which statement(s) are true?
   A. Paging allows processes to "see" more RAM than is physically present.
   B. The page fault handler code must never be paged.
   C. Paging complicates memory forensics because not all data is memory resident at the time of acquisition.
   D. Paging writes potentially valuable volatile evidence to non-volatile storage such as a disk.
   E. All of the above.

The correct answer is: E

7. The winlogon.exe process (PID 628) in sample001.bin has a virtual address 0x77a80000 and DTB value 0x682e000. What is the corresponding physical offset? What do you see at the physical offset within the file?

The correct answer is: 72159232 (an MZ header)

```
$ python vol.py -f AMF_MemorySamples/windows/sample001.bin volshell
Volatility Foundation Volatility Framework 2.4 (Beta)
Current context: System @ 0x823c8830, pid=4, ppid=0 DTB=0x39000
Python 2.7.6 (v2.7.6:3a1db0d2747e, Nov 10 2013, 00:42:54)
Type "copyright", "credits" or "license" for more information.

IPython 2.0.0 -- An enhanced Interactive Python.
?         -> Introduction and overview of IPython's features.
%quickref -> Quick reference.
help      -> Python's own help system.
object?   -> Details about 'object', use 'object??' for extra details.

In [1]: cc(pid = 628)
Current context: winlogon.exe @ 0x82189da0, pid=628, ppid=356 DTB=0x682e000

In [2]: proc().get_process_address_space().vtop(0x77a80000)
```

Out[2]: 72159232

In [3]: quit()
$ xxd -s 72159232 AMF_MemorySamples/windows/sample001.bin | less

```
44d1000: 4d5a 9000 0300 0000 0400 0000 ffff 0000  MZ..............
44d1010: b800 0000 0000 0000 4000 0000 0000 0000  ........@.......
44d1020: 0000 0000 0000 0000 0000 0000 0000 0000  ................
44d1030: 0000 0000 0000 0000 0000 0000 f000 0000  ................
44d1040: 0e1f ba0e 00b4 09cd 21b8 014c cd21 5468  ........!..L.!Th
44d1050: 6973 2070 726f 6772 616d 2063 616e 6e6f  is program canno
44d1060: 7420 6265 2072 756e 2069 6e20 444f 5320  t be run in DOS
44d1070: 6d6f 6465 2e0d 0d0a 2400 0000 0000 0000  mode....$.......
44d1080: 1ac1 36e1 5ea0 58b2 5ea0 58b2 5ea0 58b2  ..6.^.X.^.X.^.X.
```