Texas Tech University

A Course on Digital forensics

Memory Forensics

Module 4 – Memory Acquisition

Akbar S. Namin, Spring 2018

QUIZ-3

Please complete the Quiz3 located under the Module4. Quiz3 covers the chapter4 topics and includes 2 multiple choice, 1 true-false, and 1 open-ended questions. No late submission will be allowed.

Q1-4: 1.25 points

1. If a suspect computer is not powered on, you can attempt to recover memory in which of the following ways?
   A) page files on disk
   B) hibernation files
   C) old crash dumps
   D) introspection

The correct answer is: A, B, C

2. Why is memory acquisition not a trivial task? What are some of the "gotchas" you need to watch out for?

The correct answer is: cache coherency, device memory, anti-forensics, etc.

3. Which API is not commonly used by acquisition tools?
   A) MmCreateMemoryDump
   B) MmMapMemoryDumpMdl
   C) MmProbeAndLockPages
   D) ZwMapViewOfMemory
   E) MmMapIoSpace

The correct answer is: A

4. It is important to run live response tools to gather evidence before acquiring physical memory, so that your memory capture contains the extra data generated by the live IR tools. True or False?

The correct answer is: False (you should run live IR tools *after* acquiring physical memory, so you don't taint the evidence)