Texas Tech University

A Course on Digital forensics

Memory Forensics

Module 4 – Memory Acquisition

Akbar S. Namin, Spring 2018

ASSIGNMENT-4

Please get screenshot all of the steps you will do, paste them to word document, and answer the questions. Please upload your file "YourSurname_Assignment4" under the assignment link.

1. Perform the following steps:
   - **A)** Dump memory from one of your machines to local USB/Firewire/ESATA
   - **B)** Dump memory across the network (you can use a NAT or Host-only VM configuration). Make sure to use compression and encryption.
   - **C)** If possible, analyze memory using remote interrogation. Capture traffic while you run Volatility plugins. How much data is transferred with a basic process listing?

2. Perform the following steps:
   - **A)** Analyze the registry of a target system to determine how many page files are in use.
   - **B)** Extract the page files from the running system (with TSK Windows binaries).
   - **C)** Can Volatility analyze page files directly? Why or why not?
   - **D)** Can you use Volatility's imagecopy plugin to convert a page file into a raw memory dump? Why or why not?
   - **E)** Use page_brute to scan across your extracted page files. Does it find any hits?
   - **F)** If necessary, extend page_brute's default Yara rules and scan your page files again.

The correct answer is: Volatility cannot analyze page files directly at this time. You cannot use imagecopy to convert a page file into a raw memory dump (page file is just the "holes").