

STEP5 LAB: RESOURCES AND PROCEDURES NOTES

Resources

1. A Windows system (this will be your evidence system) with Forensics Toolkit (FTK) Imager installed.

Virtual Machine Credentials

Username: **StudentFirst**

Password: **Cyb3rl@b**

Procedure Notes

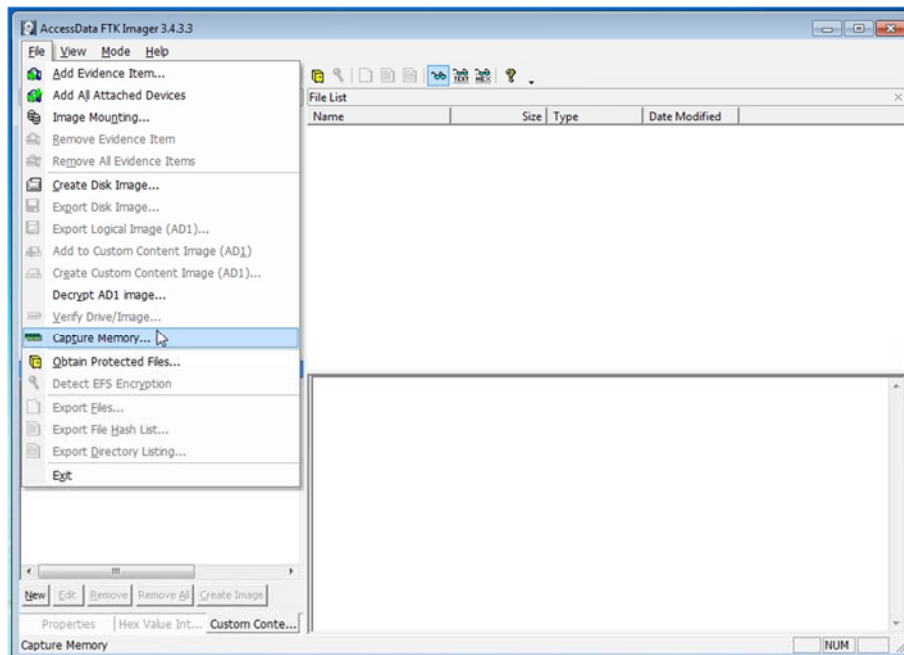
1. These procedures assume that your evidence computer is Windows 7 or later.
2. Placeholders are in [brackets].
3. Comments are in *(parentheses and italics)*.
4. Command line instructions are indicated as follows:
 - > command (*Windows normal user*)
 - admin> command (*Windows Administrator user*)

Part D: Random Access Memory (RAM) and Swap Acquisition from a Live System

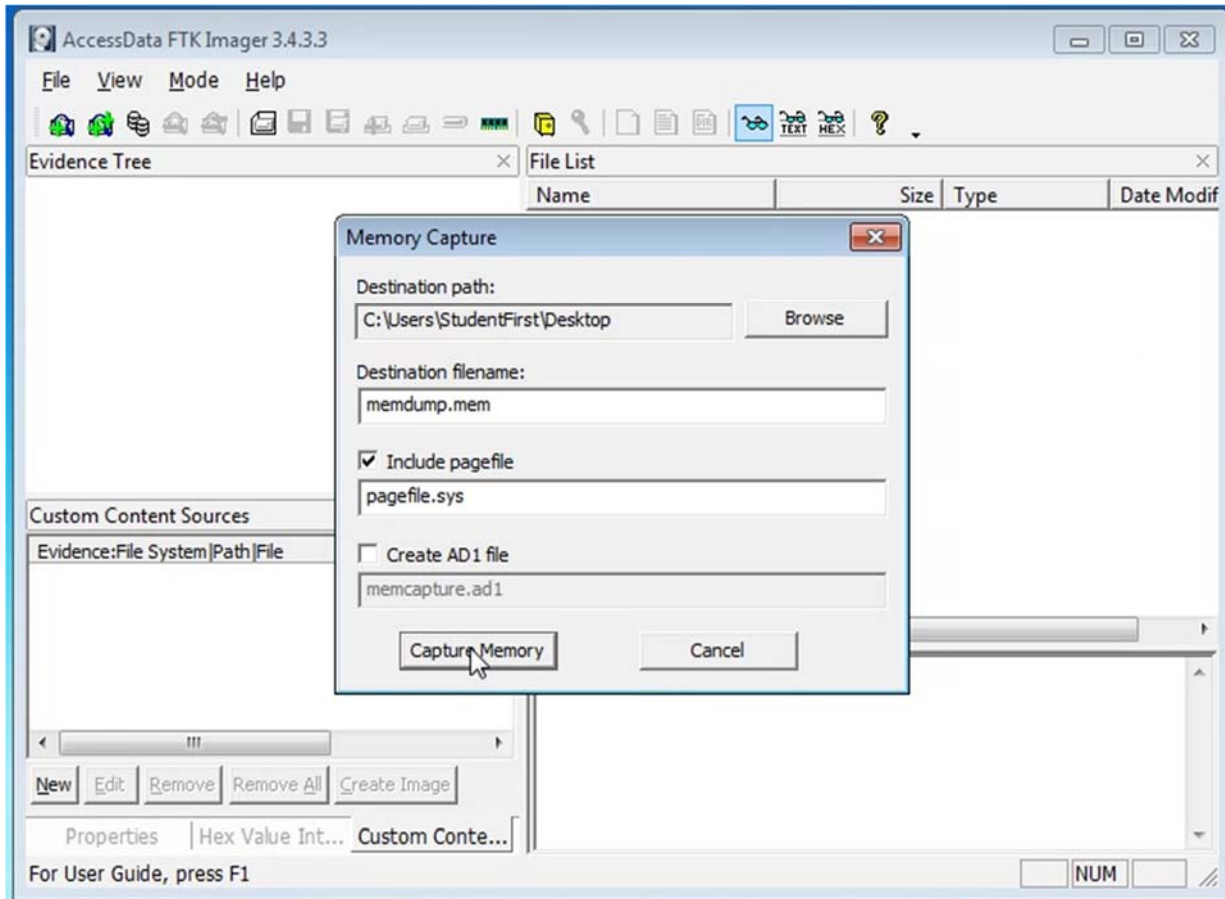
1. From the lab broker on your Workspace, allocate and connect to your Windows forensic VM, WINFOR01.



2. Run FTK Imager from your Windows forensic VM, WONFOR01.
3. Choose File, Capture Memory.



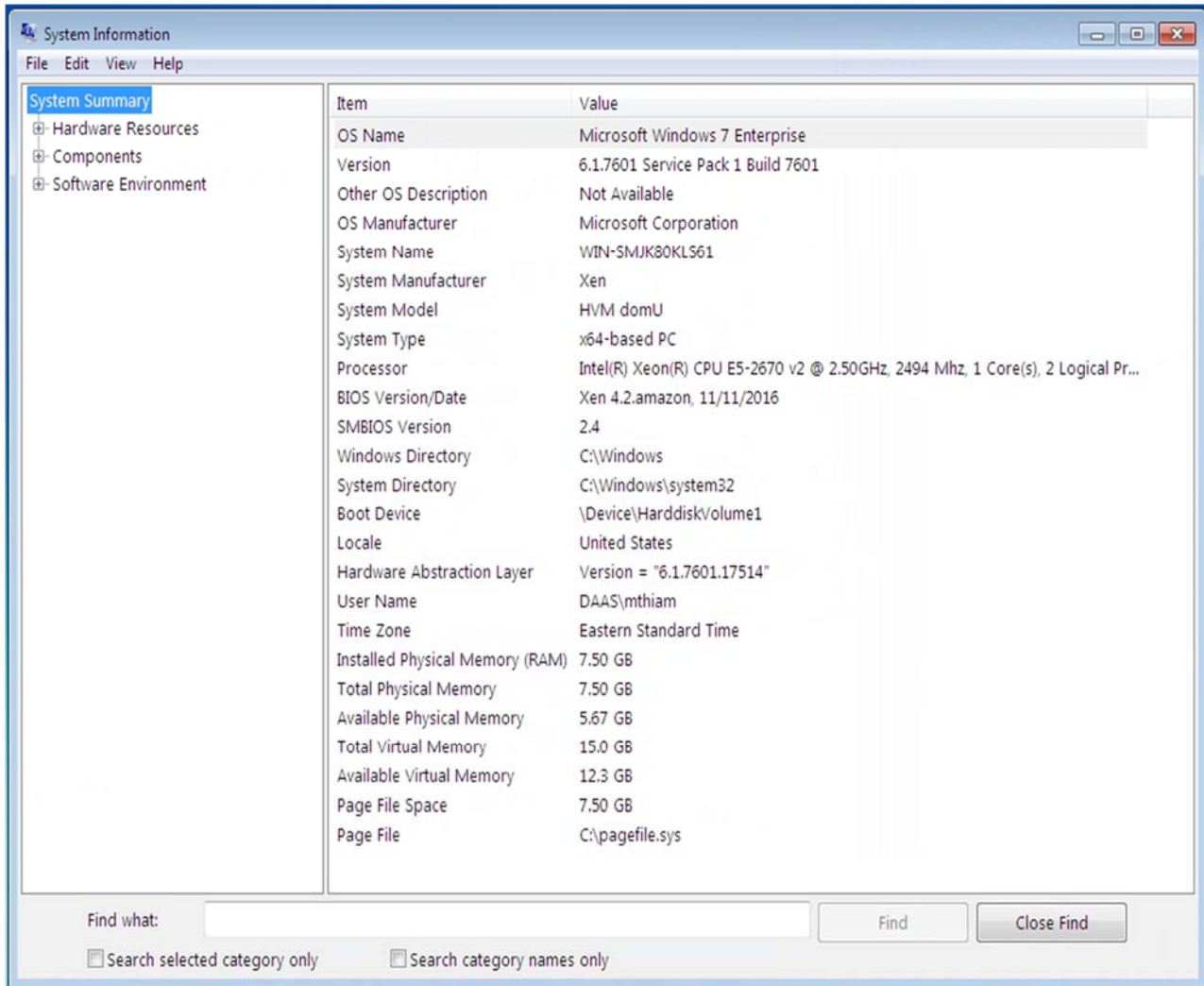
4. Set the destination path to your desktop, select “Include pagefile”, and click “Capture Memory” to start the process.



5. When the capture finishes, check and record the hash values of the memory and swap file images.

Note: The capture process could take about an hour. If you get disconnected from the Workspace during the capture, the process should still continue in your Windows forensic VM.

6. Record the hardware and software specifications of the evidence system for your report and notes. This information is at Windows: System Information: System Summary.



The screenshot shows the Windows System Information window, specifically the System Summary tab. The window title is "System Information" and it has a menu bar with "File", "Edit", "View", and "Help". On the left, there is a tree view with "System Summary" selected, and other options like "Hardware Resources", "Components", and "Software Environment". The main area displays a list of system items and their values.

Item	Value
OS Name	Microsoft Windows 7 Enterprise
Version	6.1.7601 Service Pack 1 Build 7601
Other OS Description	Not Available
OS Manufacturer	Microsoft Corporation
System Name	WIN-SMJK80KLS61
System Manufacturer	Xen
System Model	HVM domU
System Type	x64-based PC
Processor	Intel(R) Xeon(R) CPU E5-2670 v2 @ 2.50GHz, 2494 Mhz, 1 Core(s), 2 Logical Pr...
BIOS Version/Date	Xen 4.2.amazon, 11/11/2016
SMBIOS Version	2.4
Windows Directory	C:\Windows
System Directory	C:\Windows\system32
Boot Device	\Device\HarddiskVolume1
Locale	United States
Hardware Abstraction Layer	Version = "6.1.7601.17514"
User Name	DAAS\mthiam
Time Zone	Eastern Standard Time
Installed Physical Memory (RAM)	7.50 GB
Total Physical Memory	7.50 GB
Available Physical Memory	5.67 GB
Total Virtual Memory	15.0 GB
Available Virtual Memory	12.3 GB
Page File Space	7.50 GB
Page File	C:\pagefile.sys

At the bottom of the window, there is a search section with a "Find what:" text box, a "Find" button, and a "Close Find" button. Below the search box are two checkboxes: "Search selected category only" and "Search category names only".