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**

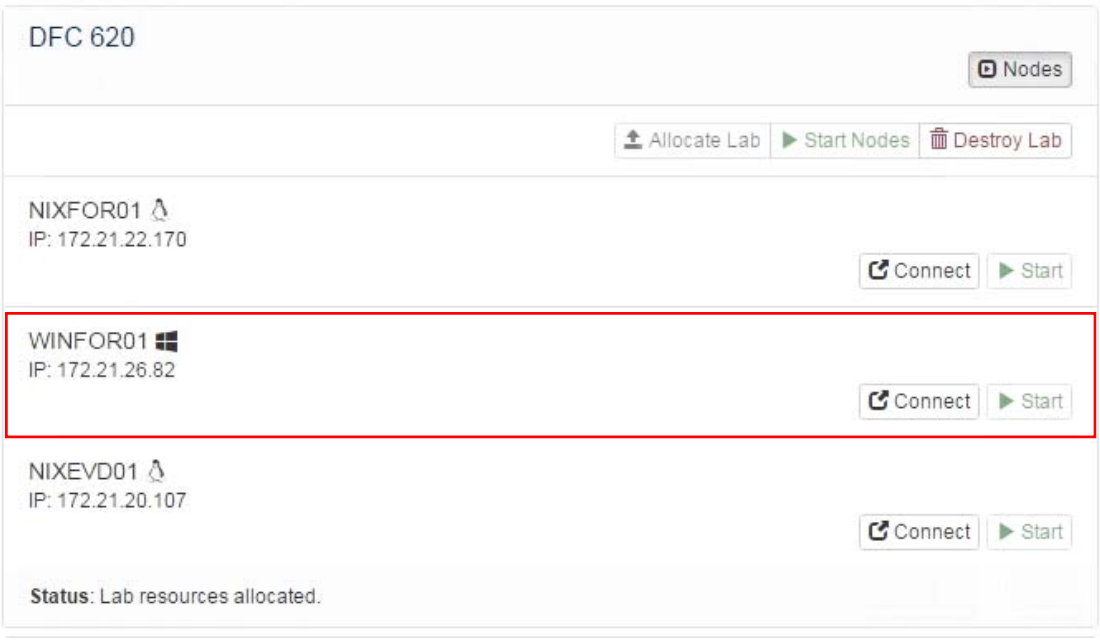
Password: **Cyb3rl@b**

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)*

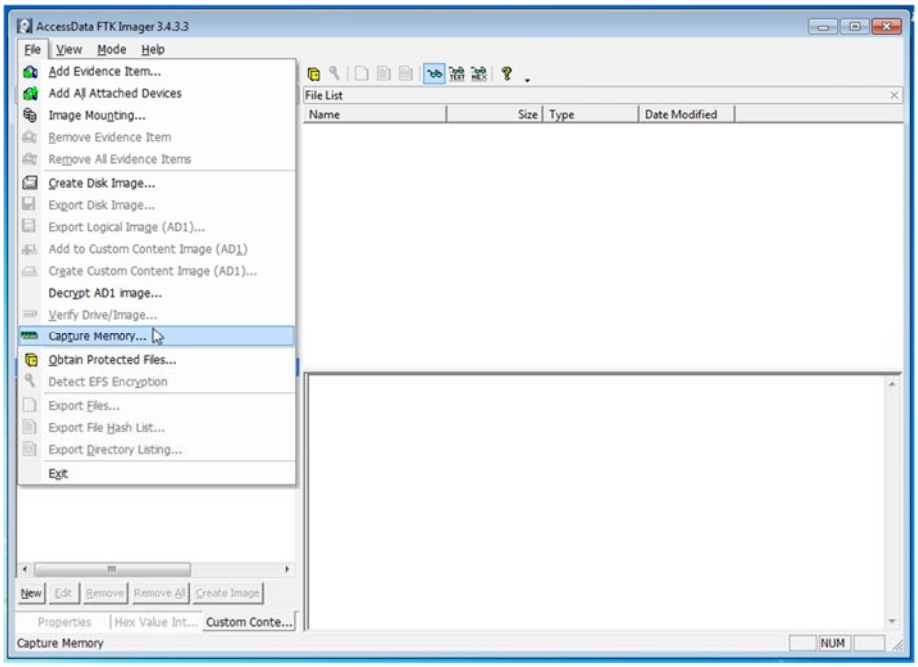
Part D: Random Access Memory (RAM) and Swap Acquisition from a Live System

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

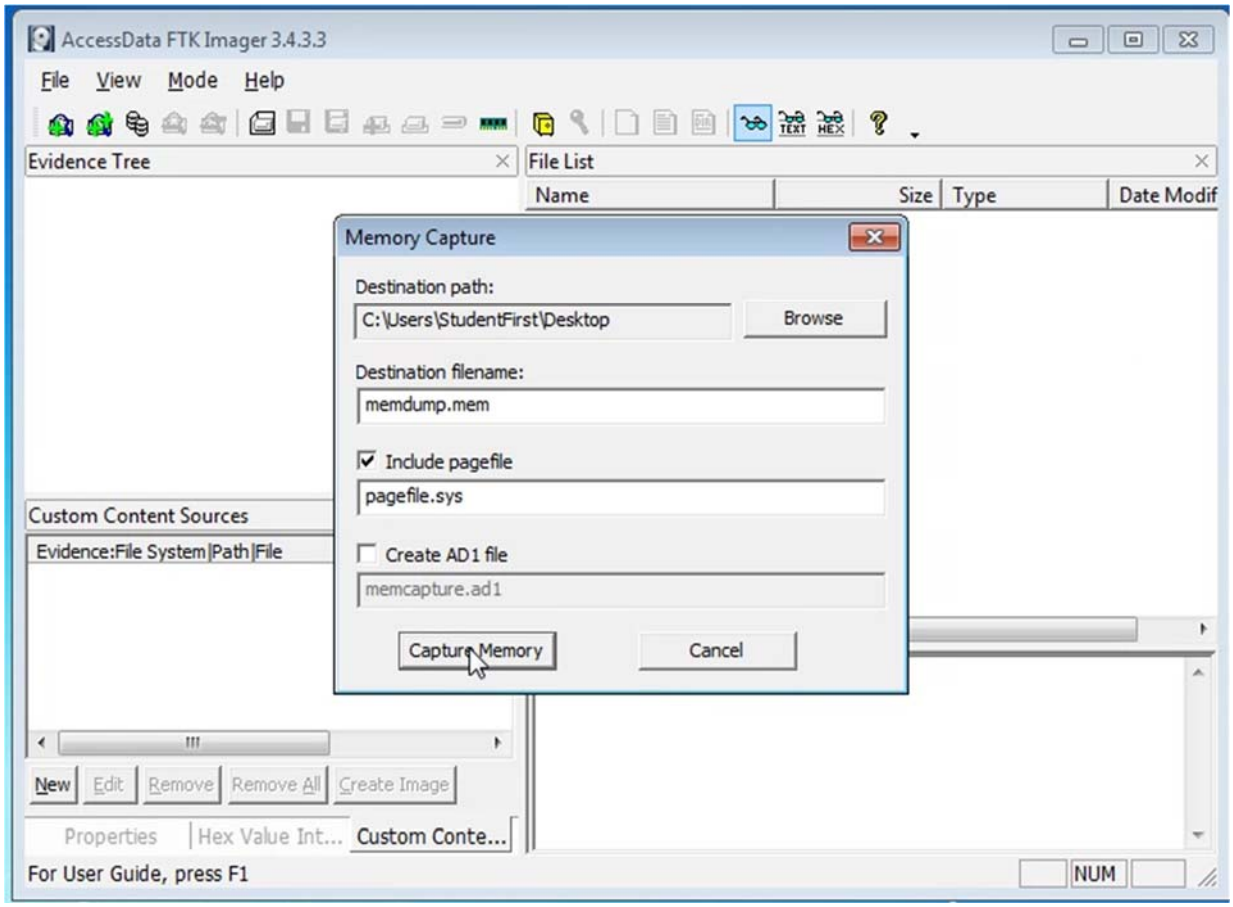


2. Run FTK Imager from your Windows forensic VM, WONFOR01.

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.