SAT1: 008: Creating a Forensic Memory Capture

Overview

This tutorial will examine the process for capturing RAM in Windows with FTK Imager and Win64dd/MWMT DumpIt.

Time: 30 Minutes

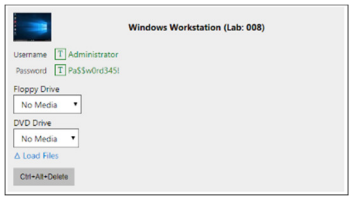
Learning Objectives

Upon completion of this lab, you should be able to:

1. Capture RAM with FTK Imager, and view resulting RAM data in FTK.
2. Capture RAM with DumpIt (Win64dd) and view the resulting file in FTK.

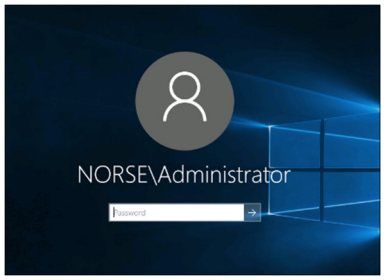
Log in to the Lab Machine

Select the **Windows 10** machine on the Machines Tab.



Select the Password on the **Windows 10** machine and

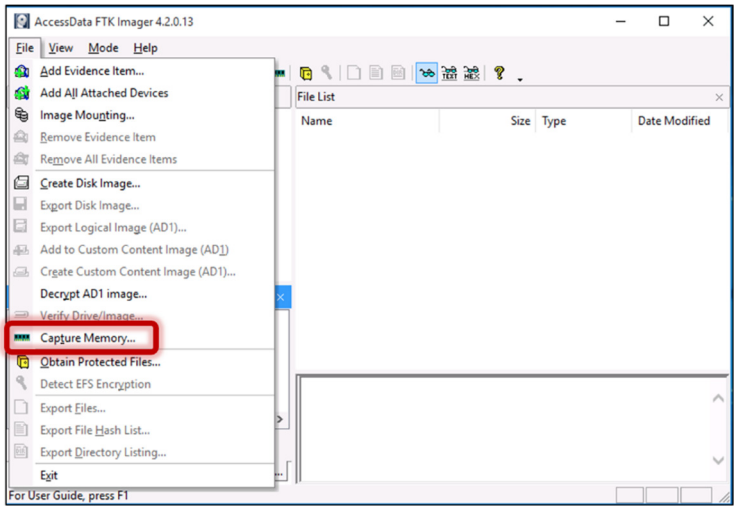
click on the Pa$$w0rd345! on the **Machines**, and press Enter to log in to the machine.



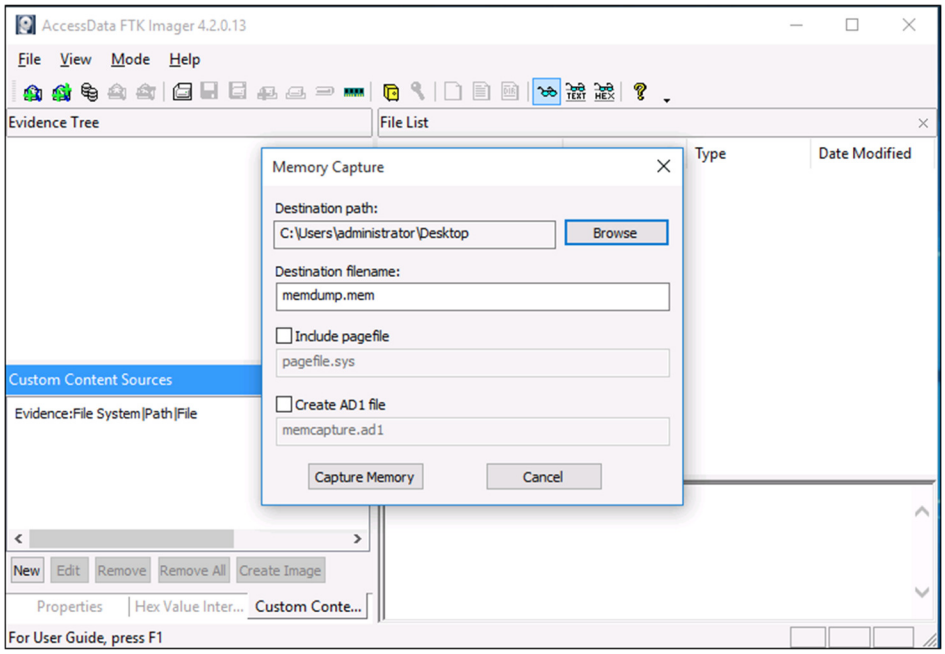

```
1.0 Capture RAM Image with FTK Imager
```

1.1 Launch AccessData FTK Imager from the Windows desktop.

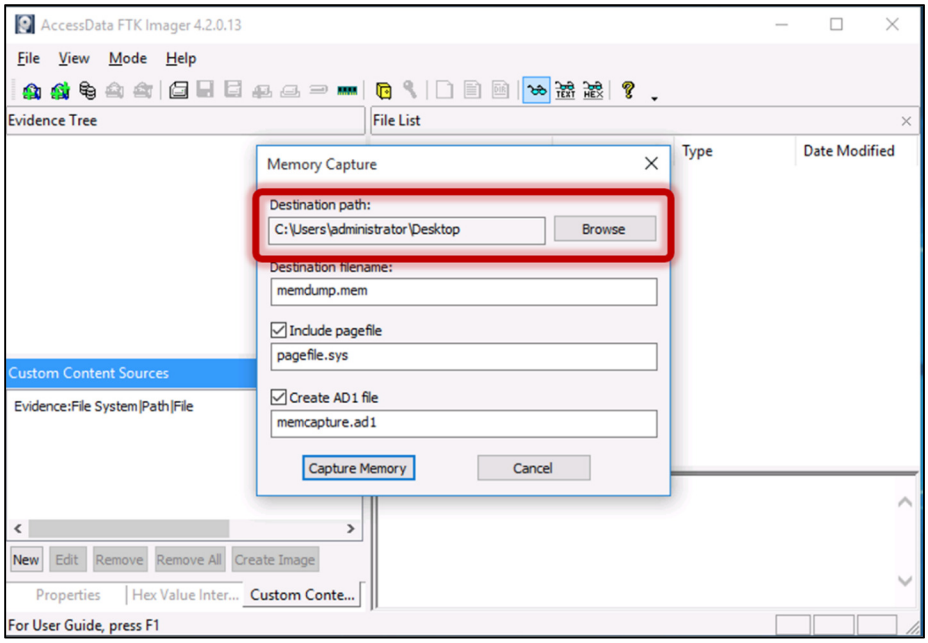
1.2 Click on **File** and click on **Capture Memory**.



1.3 The resulting window will ask you to select a destination path for the memory dump.

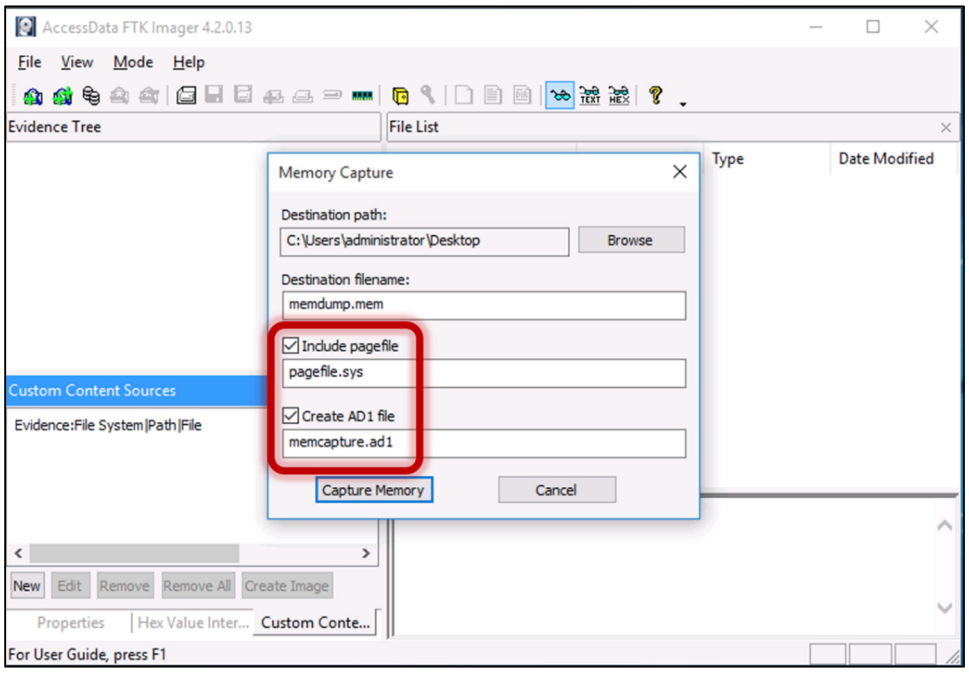


1.4 For the **Destination path:**, click on **Browse**, select **Desktop**, and click on **OK**. You can also name the file in the **Destination filename:** section.

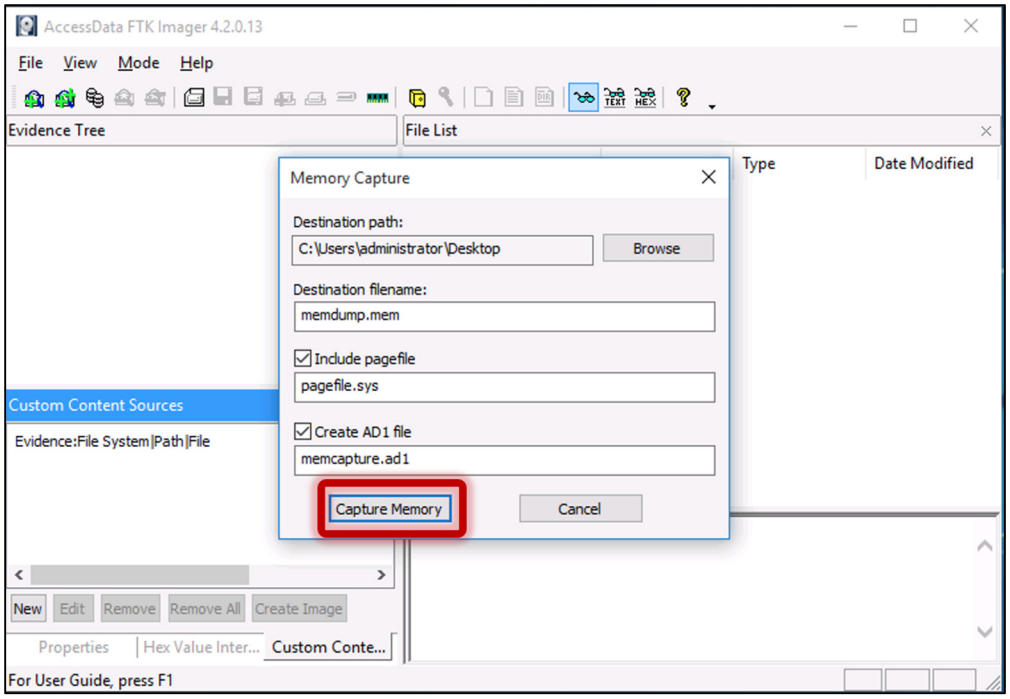


NOTE: The default filename is memdump.mem

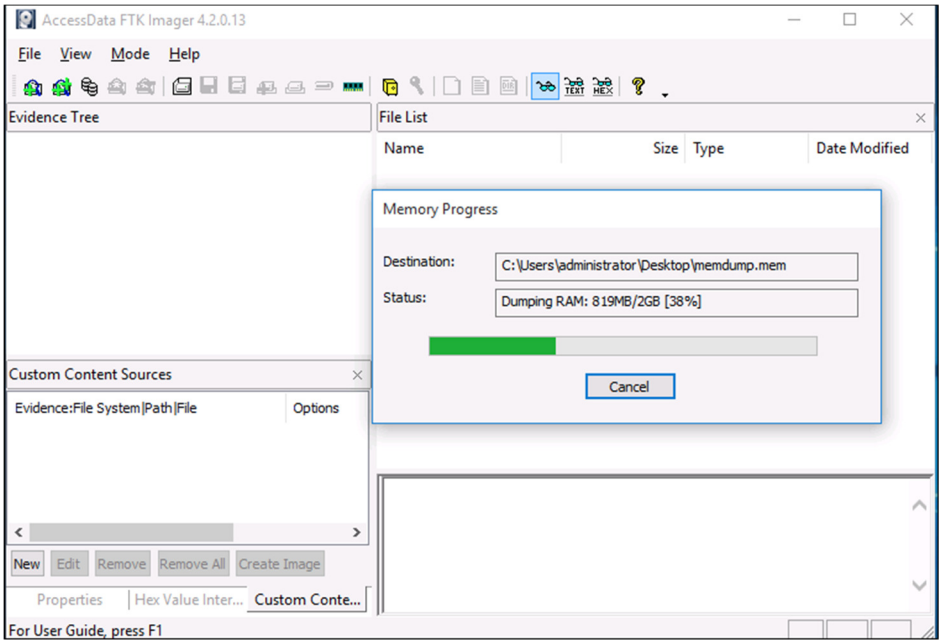
1.5 You can also elect to include the pagefile and create an AD1 file.



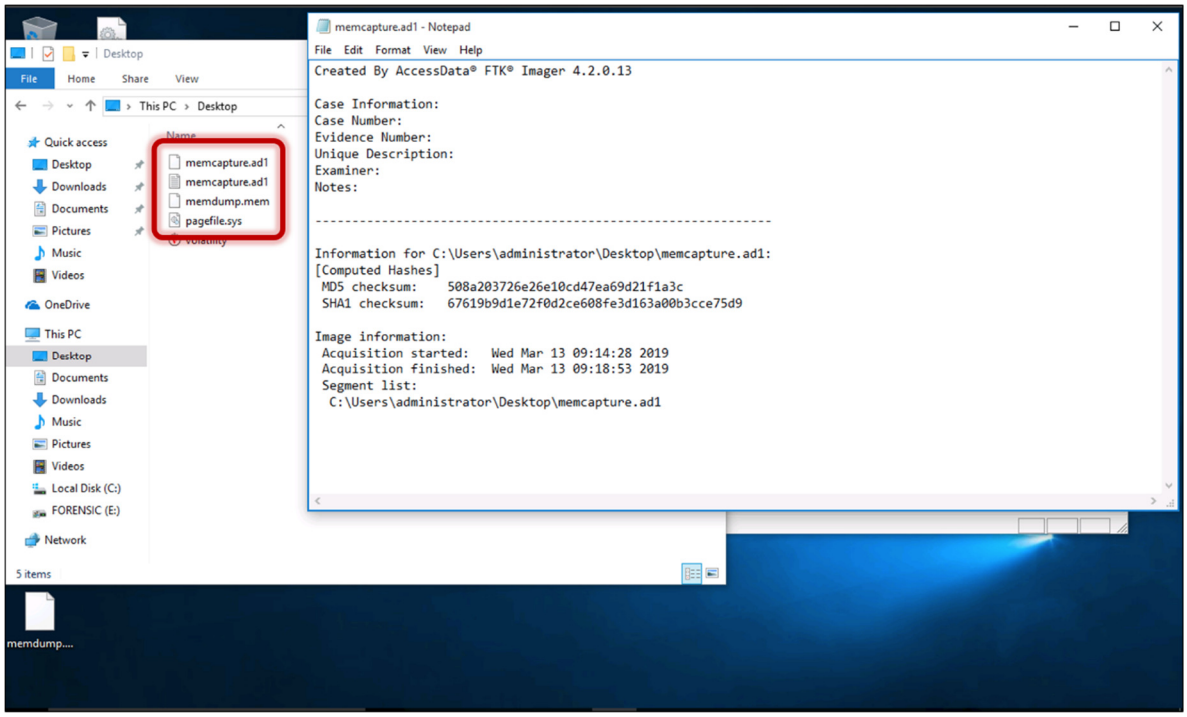
1.6 Click **Capture Memory** to begin the memory capture.



The Capture will run, it will take between 5-10 minutes to run the capture.



Once the capture is complete, you will be able to see it on the Windows desktop, along with `ad1` file, `pagefile.sys`, and a notepad document that will give you more information about the capture, including the MD5 and SHA1 hash values.



1.7 Close FTK Imager.

Great job, you have completed LAB008!

Thank You, you may now close this module.