Lab Assignment 0 – Optional VM Setup

Background

In this optional assignment, students will setup their forensic virtual machine and install forensic applications required for the course. You may use a host Windows system for course materials, but the VM is recommended.

Objectives

- Setup a forensic workstation for the semester (Windows host, a local VM, and in a cloud environment)
- Download core forensic tools to begin the semester and complete initial assignments

Exercise Preparation

Download and install the **optional** Windows 10 IA Lab VM that will be used throughout the course. This VM will allow you to perform the majority of forensic labs and assignments required for this course. All evidence files can be accessed and folder structures created for easy organization. Please do not share this image with anyone else. Some of these tools can be installed on Linux/macOS.

Link: https://www.dropbox.com/sh/4izs5y6idjz95rf/AAD3rLdU02xQxjttmEP7JtAwa?dl=0

Note: This VM setup is optional and **requires a valid Windows 10 license key**; some Microsoft features will be disabled until activation. Using a license without activation is also illegal. These tools and evidence files may also be downloaded and installed on a Windows host computer as well, the VM is not required, but will allow you to have a forensic workstation that can be used when the semester is over.

VM Settings:

- 4GB RAM (should be increased to 8GB)
- 2 Processor/1Core each
- 60GB HDD space for evidence (should be expanded to 100GB)
- Username: **Student**
- Password: **./ForensicsIA5210!**

Install the initial open source forensic software used for the course. These have been downloaded to the VM and saved in the C:\GCFIWork\Software folder, but visit the URLs listed for the latest software for your personal system. You may want to create desktop shortcuts for all applications.

Install Autopsy (4.8) for Windows

1. URL: https://www.sleuthkit.org/autopsy/download.php
2. 64-bit downloaded to the VM based on architecture
3. Install with default settings

Install FTK Imager

1. Download FTK Imager Lite 3.1.1 https://marketing.accessdata.com/ftkimagerlite3.1.1
2. The unzipped directory in the VM is fully operational. The .EXE is a portable application.
3. If downloading, use a personal email address and decide to "Opt In" before requesting the link.
4. You should right-click the FTK Imager .EXE and send to desktop for ease of use.
5. The full application can also be installed, with more features, but is not portable https://accessdata.com/product-download/ftk-imager-version-4-3-1-1

Install WinHex

1. http://x-ways.com/winhex/
2. Click "Download" and download the user manual for additional features.
3. Extract the file contents (completed in VM)
4. Right-click the winhex.exe and send to desktop.

Bookmark Autopsy Documentation

1. Using Autopsy for Windows (Optional)
2. https://sleuthkit.org/autopsy/docs/user-docs/4.3/ (latest documentation)
3. Learn more about the Autopsy interface. Read documents and search YouTube for Autopsy for Windows and review version 4 content. This is the primary open source forensic tool used in the course.

Exercise – Questions

None.

Exercise—Key Takeaways

- Determine if a host system, local VM, or OS cloud installation provides the most flexibility for course assignments during the semester.
- Creating a virtual machine will allow you to have an open source forensics workstation after the course ends.
- Install initial forensic tools to begin CY5210 Lab assignments and case studies.