F20FO Lab 7

Live Forensics and IR

Chandrashekhar R (cr2007)

Contents

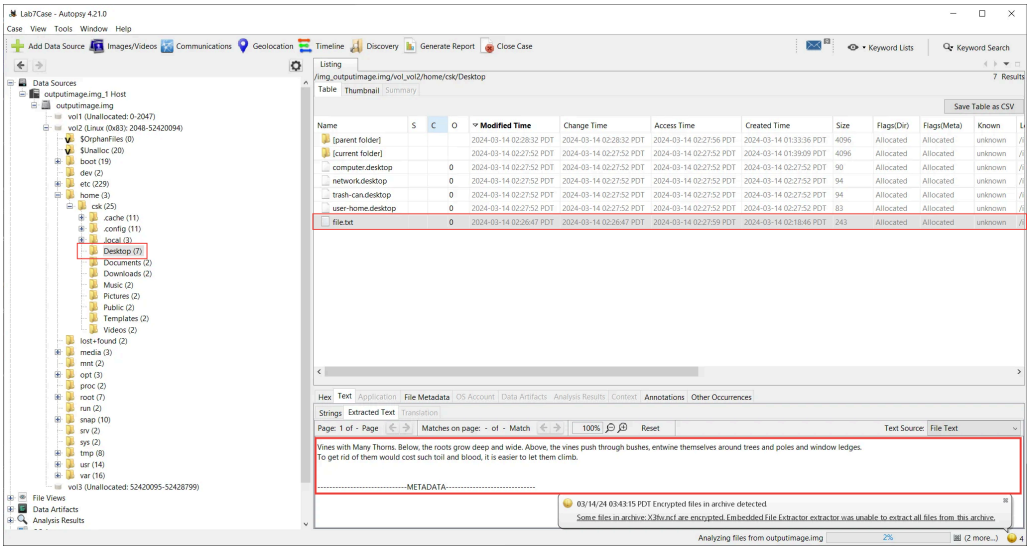
Lab 7.1: VM and Autopsy

How much RAM is allocated to your VM?

6 GB

Lab 7.1.1.: Viewing a VM

Using the Data Sources tree view can you find the data you put on the desktop? Upload a screenshot of your desktop in the quiz.



Lab 7.3: Live Forensics

Lab 7.3.1: Live Analysis

Note your USBMOUNT point

`/media/csk/FIRE-0.3.5b`

What does the Script command in Linux do?

The `script` command takes a copy of everything which is output to the terminal and place it in a log file.

Lab 7.3.6: Windows and Live Incident Response

Submit a paragraph detailing what you expect to find from the Windows system. After your live analysis, submit a list of what you recovered from the contents of RAM, the list of running processes and network connections. Did you find any content, which might be of interest to an investigation?

From the Windows system, we expect to find active processes and any suspicious files that may be present in the system. From the live analysis conducted, we recovered the following list of running processes. From the list of running processes and network connections, we were able to discover processes mostly containing from:

1. Microsoft Edge
2. OneDrive
3. CTFmod
4. Ruby

There are no active network connections available in the Windows system, and overall, from the RAM contents, there was no content available that might be of interest to an investigation. All the running processes are standard processes that exist in a Windows system, and there were no active network connections present in the system.
