Lab Assignment

Cybersecurity Professional Program

Digital Forensics &
Incident Response

Data Acquisition

DFIR-04-L4
Built-in Memory Capture

Lab Objective

Become familiar with the built-in memory dumping in Windows 10.

Lab Mission

Configure Windows 10 to create a memory dump during a system crash.

Lab Duration

15–20 minutes

Requirements

- Basic knowledge of the Linux environment
- Knowledge of data acquisition

Resources

- Environment & Tools
    - VirtualBox
        - Windows 10
    - Extra Files
        - ***notmyfault64.exe***

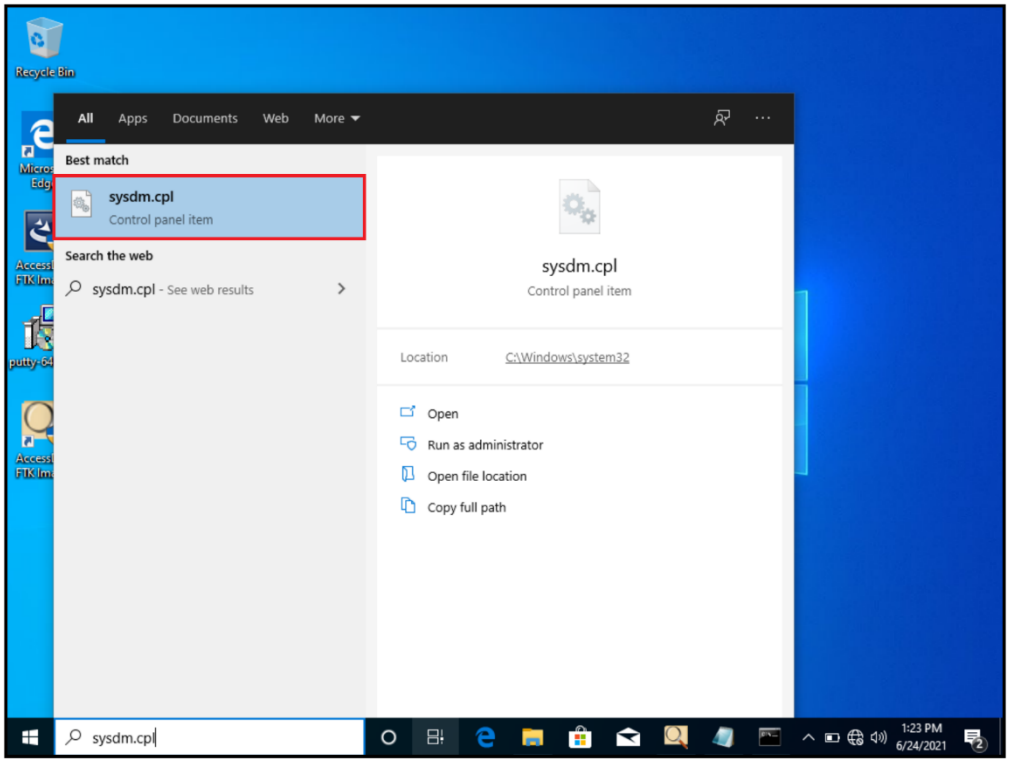
Textbook References

- Chapter 4: Data Acquisition
    - Section 6: Memory Dumping

Lab Task: Create a Memory Dump

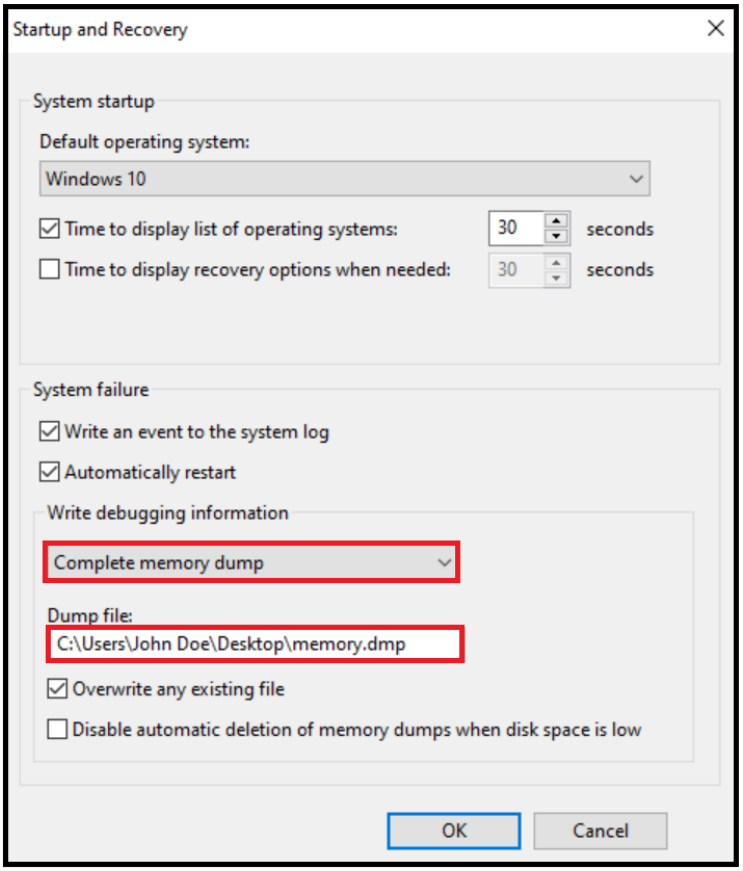
In this task, you will enter the Windows 10 settings and configure the system to generate a memory dump file in the event of a crash.

1 Enter the virtual machine's system properties by opening the search for **sysdm.cpl**.



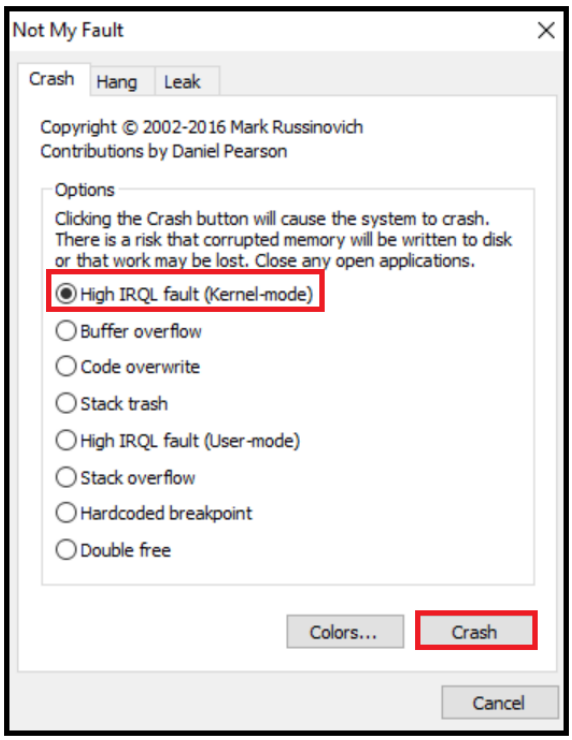
2 In the **Advanced** tab, use the **Startup and Recovery** settings to configure memory dump creation upon a system crash.

3 In the **Startup and Recovery** window, select ***Complete memory dump*** and change the file path to: **C:\Users\[username]\Desktop\memory.dmp.** Then click **OK** to prompt a restart.



4 Drag and drop the ***notmyfault64.exe*** file to the Windows machine's desktop and run the .exe file.

5 Once **Not My Fault** is open, select ***High IRQL fault (Kernel-mode)*** and click **Crash**. The system will crash and restart.



6 Log back in and you should have the ***memory.dmp*** file on your desktop.