Student:	Email:
Jose Cruz	jose.cruz2@udc.edu

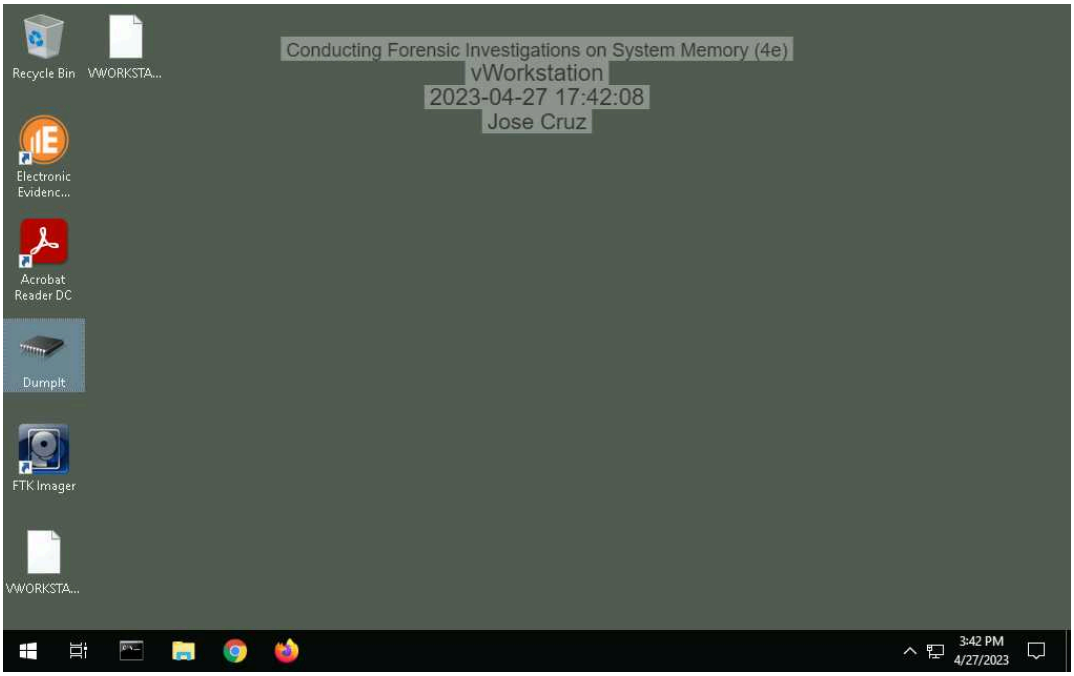
Time on Task:	Progress:
9 hours, 50 minutes	100%

Report Generated: Friday, April 28, 2023 at 7:59 PM

Section 1: Hands-On Demonstration

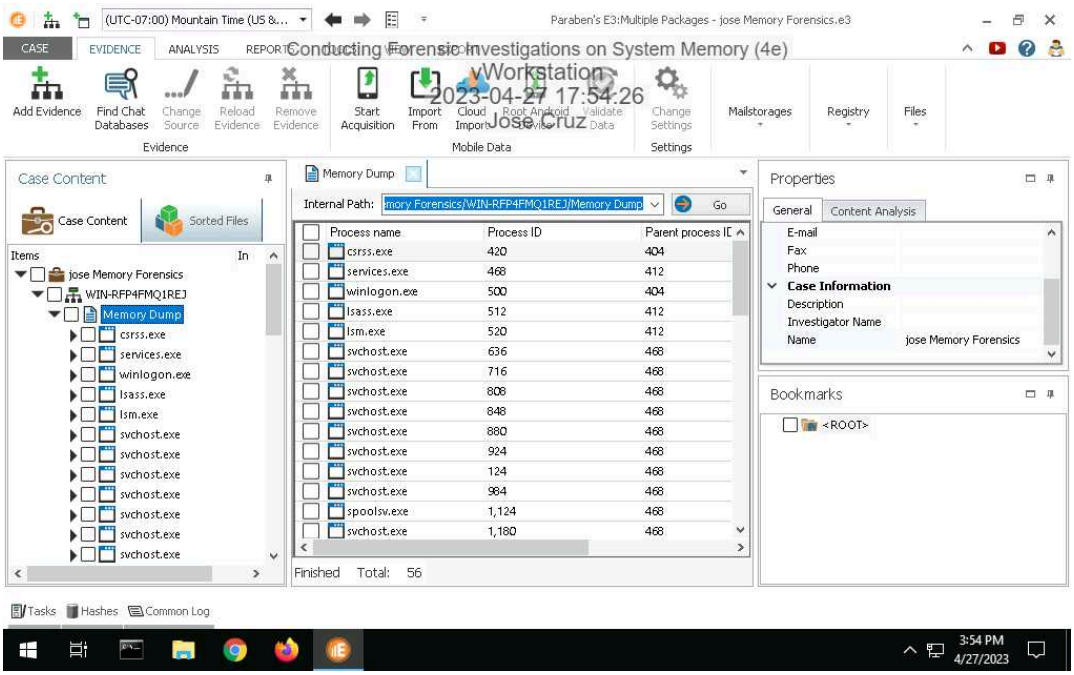
Part 1: Capture Memory using DumpIt

3. **Make a screen capture** showing the **DumpIt success notification**.



Part 2: Analyze Memory using E3

8. **Make a screen capture** showing the **list of processes in the memory dump**.



10. **Record** the start times for the oldest process and the newest process.

The status of the oldest process time is at 4:24:52 AM in 7/12/21.
For the status of the newest process is at 6:42:43 AM in 7/12/21.

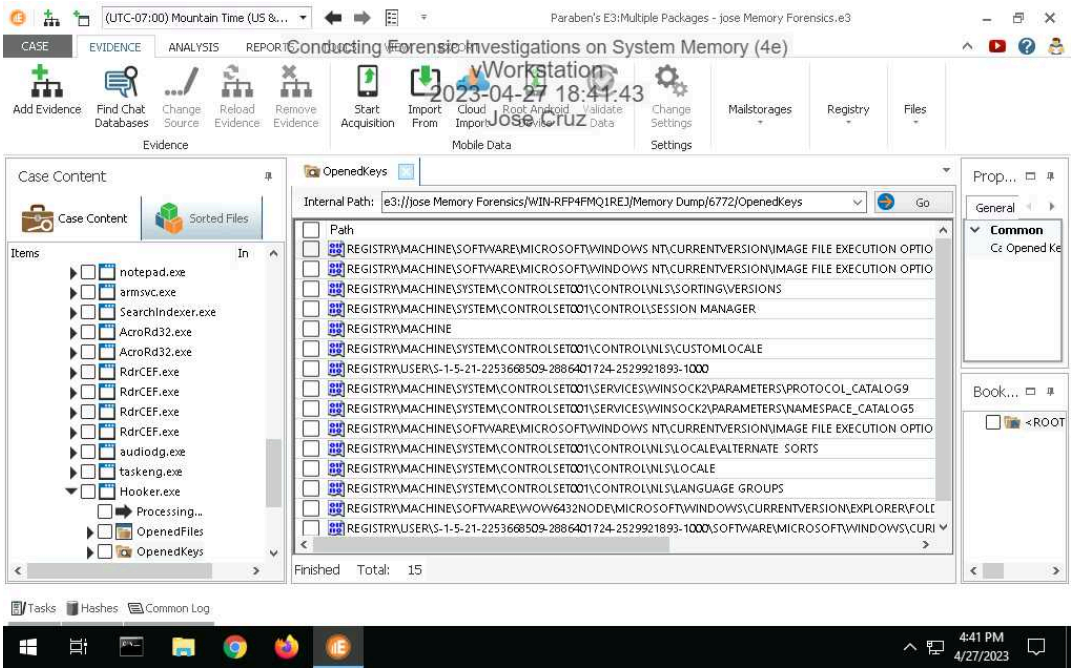
15. **Document** your findings for the conhost.exe process. What is it and what is it used for?

Conhost.exe or Console Host Window Process is a core part of Windows that houses any application that uses the command prompt.

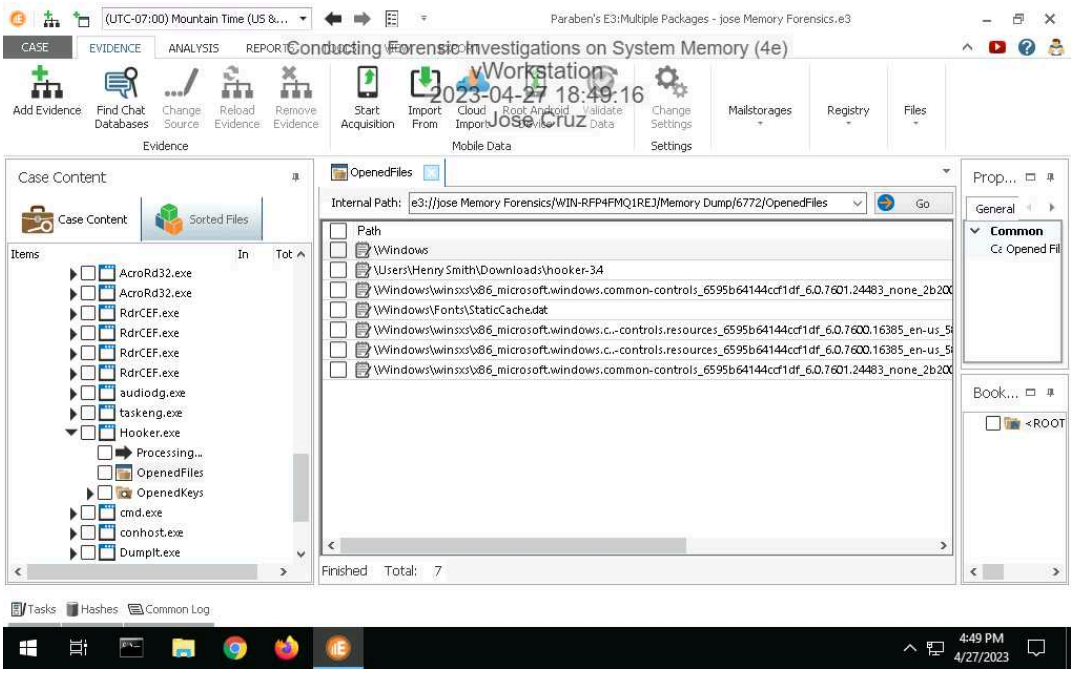
17. **Document** your findings for the hooker.exe process. What is it and what is it used for?

The hooker.exe file is able to record keyboard inputs. Hooker.exe is not a Windows system file. Hooker.exe is able to connect to the internet, record keyboard.

21. **Make a screen capture** showing the **registry keys opened by the Hooker.exe process**.



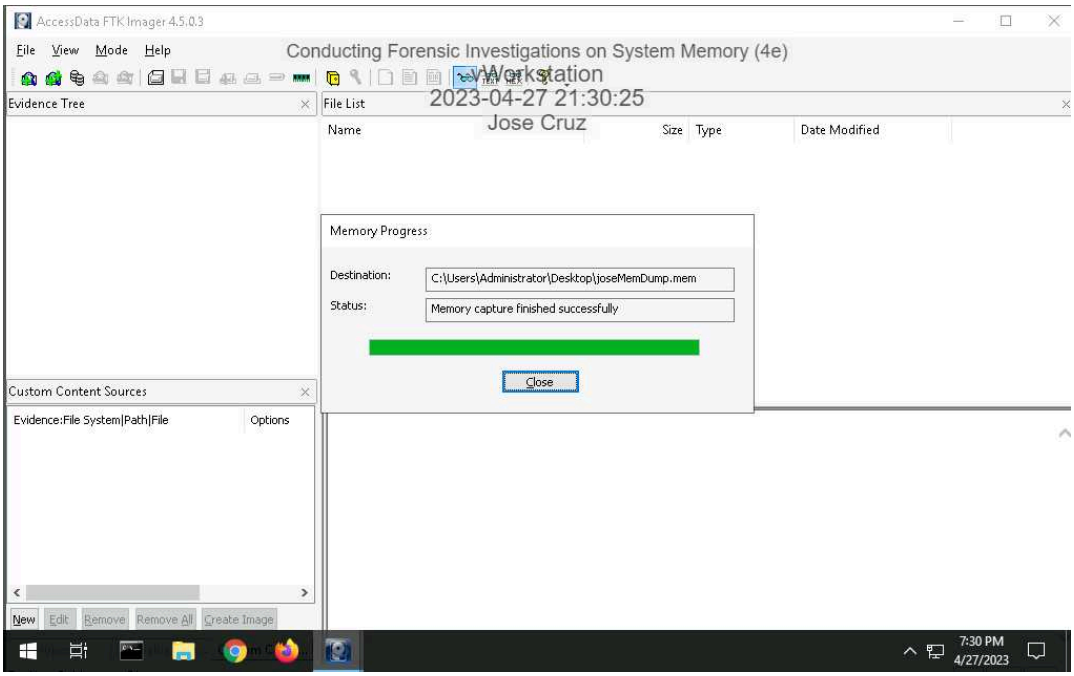
23. **Make a screen capture** showing the **files opened by the hooker.exe process**.



Section 2: Applied Learning

Part 1: Capture Memory using FTK Imager

6. **Make a screen capture** showing the ***Memory capture finished successfully*** **confirmation.**



Part 2: Analyze Memory using Volatility

7. **Document** your findings for the rvlkl.exe process. What is it and what is it used for?

My finding where that "rvlkl.exe" is a keylogger.

9. **Document** whether any processes are flagged as hidden.

There was not any false statement under pslist in the command line.

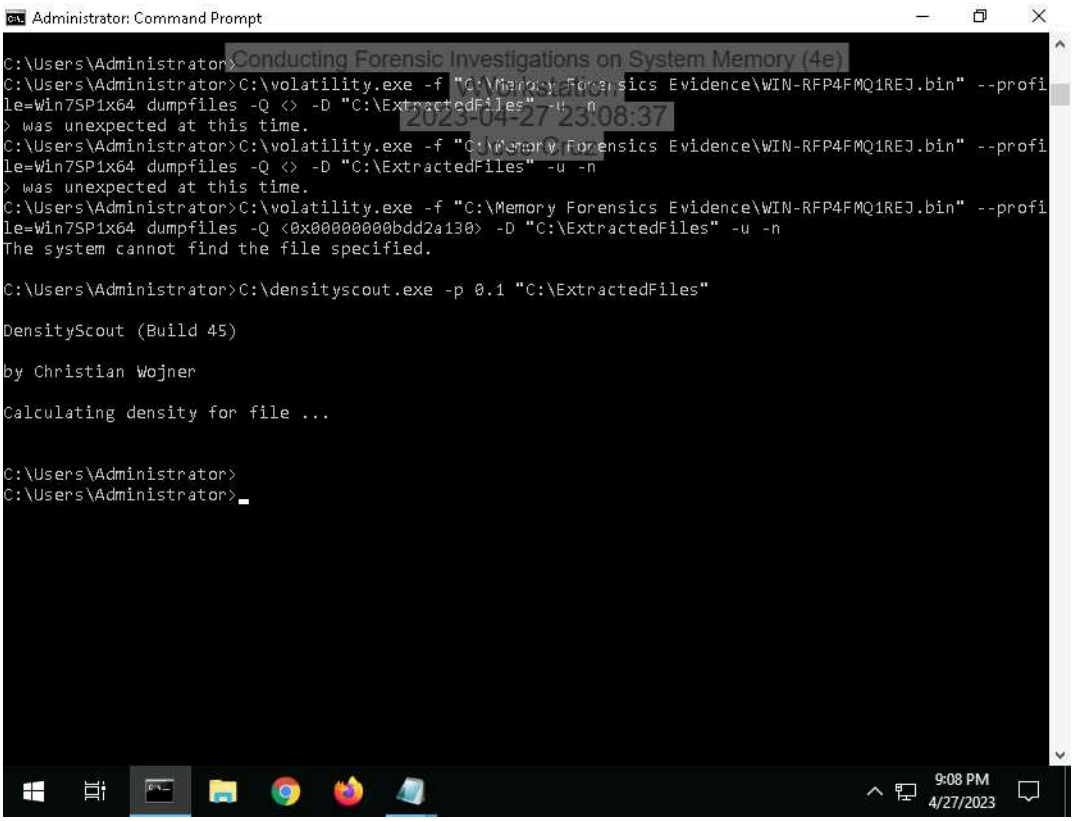
12. **Document** whether the netscan module displays network usage associated with the Hooker.exe or rvlkl.exe processes.

Couldn't find any netscan network usage associated with Hooker.exe or rvlkl.exe processes.

15. **Document** any information you were able to gather about port 56610.

Port 56610 is tcp/udp, TCP enables two hosts to establish a connection and exchange streams of data.

26. **Make a screen capture** showing the **DensityScout results**.



Section 3: Challenge and Analysis

Part 1: Identify Malicious Connections

Document the three processes that connected to 205.134.253.10:4444.

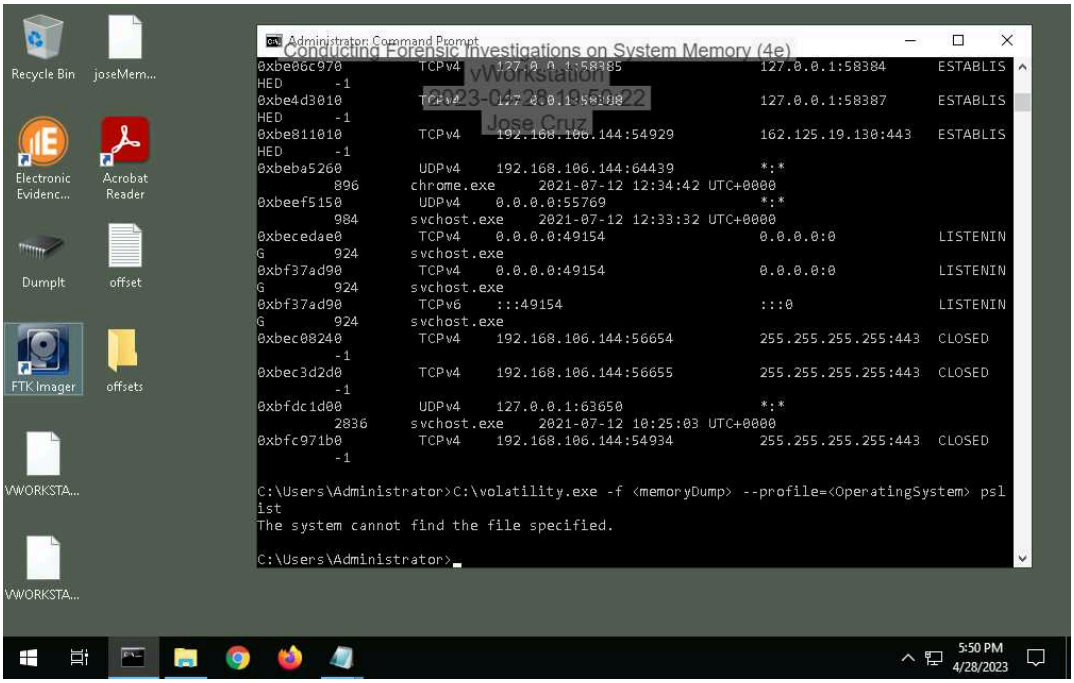
127.0.0.1:58385, 127.0.0.1:58388, 192.168.106.144:54929

Document the name and purpose of the software you discovered.

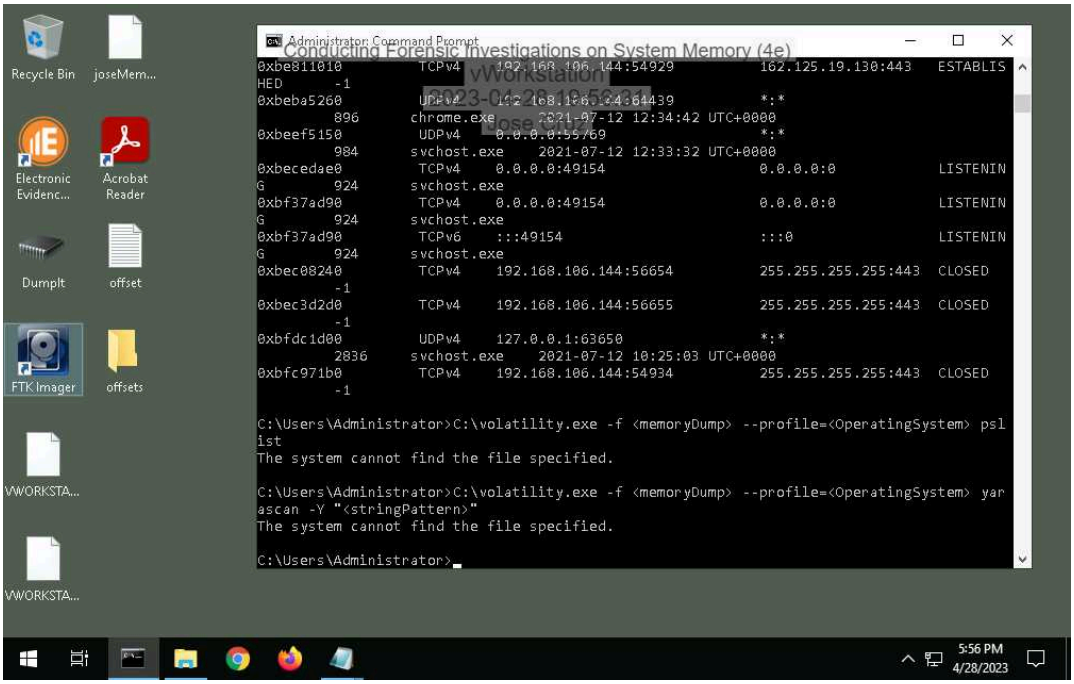
The name of the port is Transfer Control Protocol; It uses this port to eavesdrop on traffic and communications, for these communications, and to receive data from the compromised computer.

Part 2: Identify Malicious Processes

Make a screen capture showing the **fixtureComputer.exe process, and all those below it, in the pslist output.**



Make a screen capture showing the **output of the yarascan**.



Part 3: Identify Privilege Escalation

Make a screen capture showing the **output of your privilege comparison**.