

# Conducting Forensic Investigations on System Memory (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 10

Student:

Jose Cruz

Email:

jose.cruz2@udc.edu

Time on Task:

9 hours, 50 minutes

Progress:

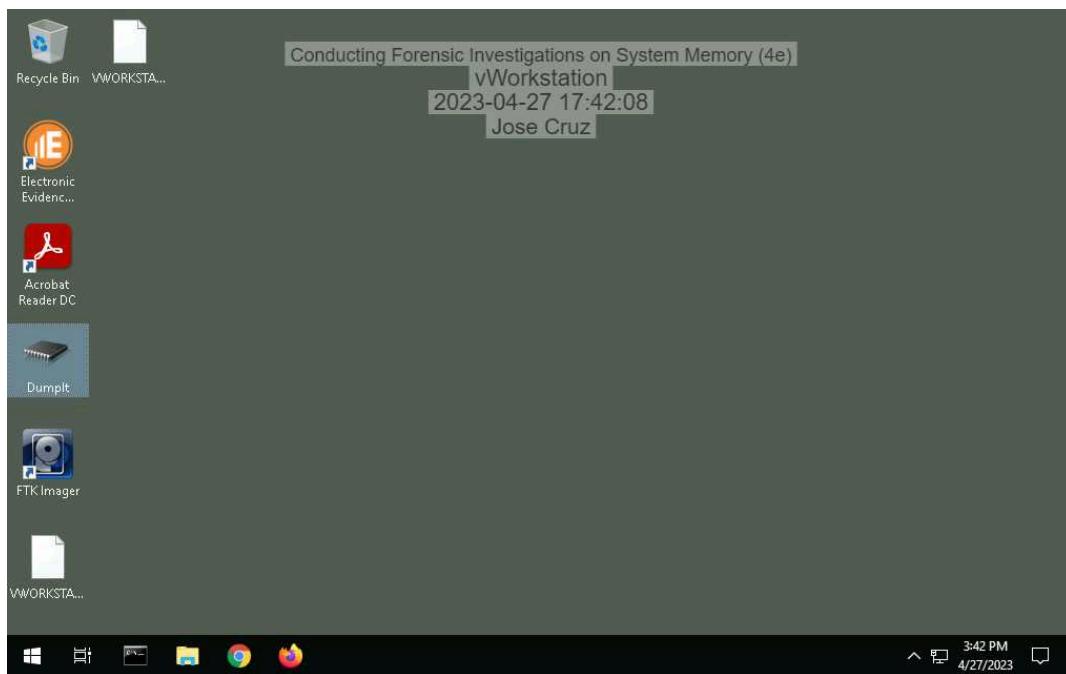
100%

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

## Section 1: Hands-On Demonstration

### Part 1: Capture Memory using DumplIt

3. Make a screen capture showing the DumplIt success notification.



### Part 2: Analyze Memory using E3

# Conducting Forensic Investigations on System Memory (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 10

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

The screenshot shows the Paraben's E3:Memory Forensics software interface. The main window displays a list of processes from a memory dump. The left sidebar shows the case structure, including a 'Memory Dump' folder containing various system processes like csrss.exe, services.exe, winlogon.exe, lsass.exe, lsrm.exe, svchost.exe, and others. The right panel shows detailed properties for a selected process, with tabs for General and Content Analysis. The General tab includes fields for E-mail, Fax, Phone, and Case Information (Description, Investigator Name, Name). The Content Analysis tab is currently empty. The bottom status bar shows the date and time as 4/27/2023 at 3:54 PM.

Process name	Process ID	Parent process ID
csrss.exe	420	404
services.exe	468	412
winlogon.exe	500	404
lsass.exe	512	412
lsrm.exe	520	412
svchost.exe	636	468
svchost.exe	716	468
svchost.exe	808	468
svchost.exe	848	468
svchost.exe	880	468
svchost.exe	924	468
svchost.exe	124	468
svchost.exe	984	468
spoolsv.exe	1,124	468
svchost.exe	1,180	468

## 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.

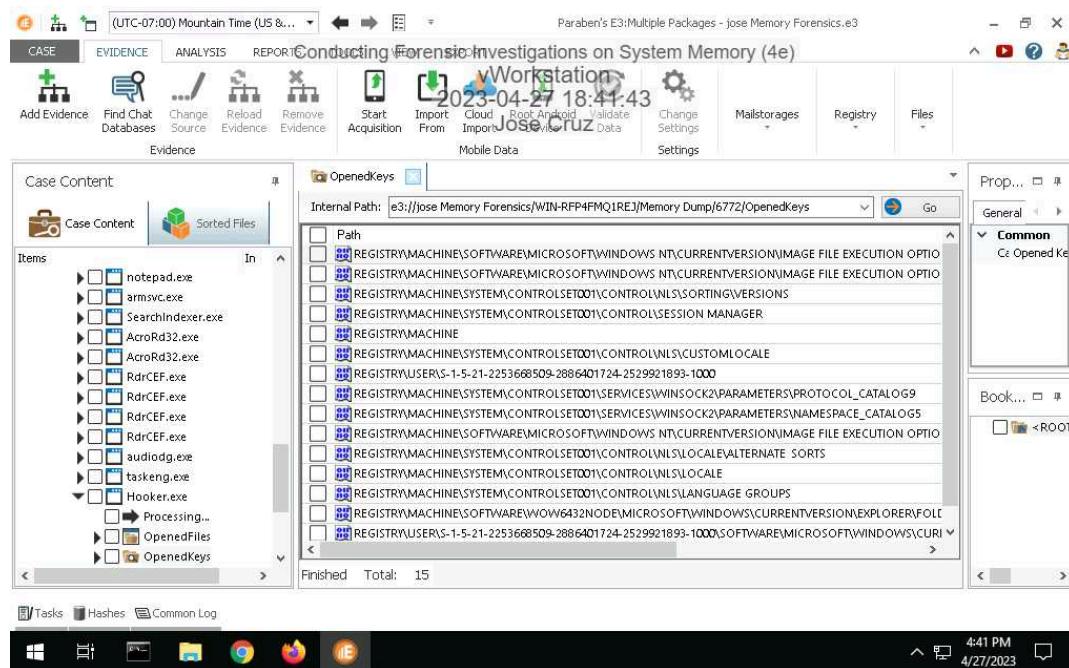
## 17. Document your findings for the hooker.exe process. What is it and what is it used for?

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.

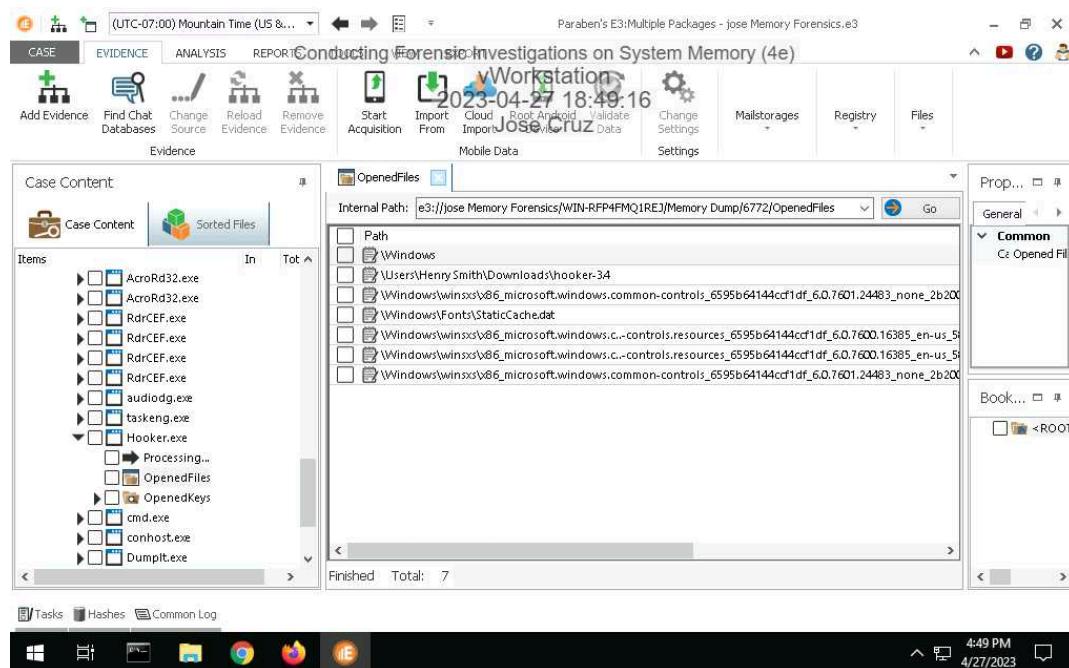
# Conducting Forensic Investigations on System Memory (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 10

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



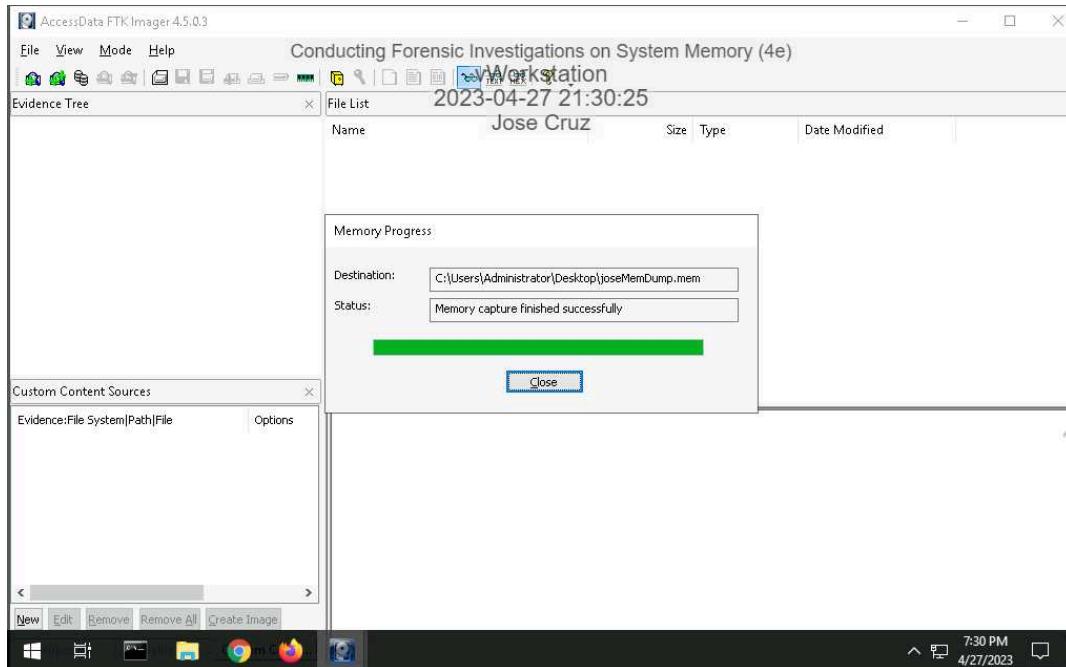
## 23. Make a screen capture showing the files opened by the hooker.exe process.



## 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.

# Conducting Forensic Investigations on System Memory (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 10

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.**

The screenshot shows a Windows Command Prompt window with the title 'Administrator: Command Prompt'. The window contains the following text:

```
C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\WIN-RFP4FMQ1REJ.bin" --profile=Win7SP1x64 dumpfiles -Q <> -D "C:\ExtractedFiles" -u -n  
> was unexpected at this time.  
2023-04-27 23:08:37  
C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\WIN-RFP4FMQ1REJ.bin" --profile=Win7SP1x64 dumpfiles -Q <> -D "C:\ExtractedFiles" -u -n  
> was unexpected at this time.  
C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\WIN-RFP4FMQ1REJ.bin" --profile=Win7SP1x64 dumpfiles -Q <0x00000000bdd2a130> -D "C:\ExtractedFiles" -u -n  
The system cannot find the file specified.  
  
C:\Users\Administrator>C:\densityscout.exe -p 0.1 "C:\ExtractedFiles"  
  
DensityScout (Build 45)  
by Christian Wojner  
Calculating density for file ...  
  
C:\Users\Administrator>  
C:\Users\Administrator>
```

The taskbar at the bottom of the screen shows several icons, including File Explorer, Google Chrome, and Mozilla Firefox. The system tray in the bottom right corner displays the date and time as '9:08 PM 4/27/2023'.

## Section 3: Challenge and Analysis

### Part 1: Identify Malicious Connections

**Document** the three processes that connected to 205.134.253.10:4444.

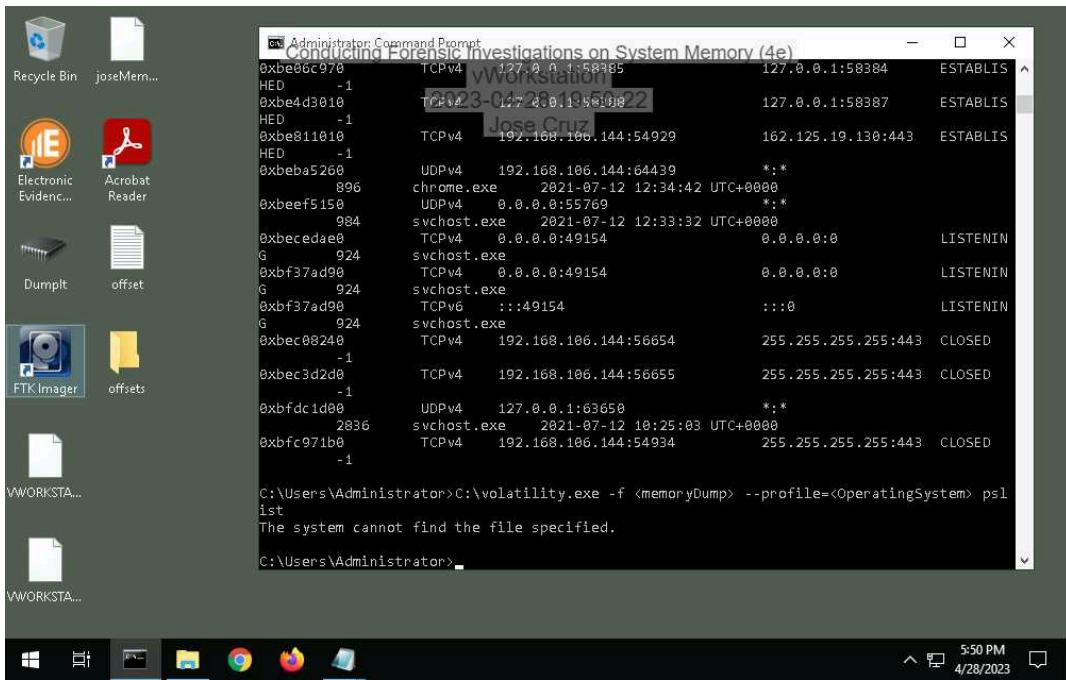
127.0.0.1:58385, 127.0.0.1:58388, 192.168.106.144:54929

**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.



```
Administrator: Command Prompt
0xb0e6c970 TCPv4 127.0.0.1:58385 127.0.0.1:58384 ESTABLISHED
0xb4d3010 TCPv4 127.0.0.1:58388 127.0.0.1:58387 ESTABLISHED
0xb811010 TCPv4 192.168.106.144:54929 162.125.19.130:443 ESTABLISHED
0xb811010 TCPv4 192.168.106.144:64439 *:*
0xbeef5150 UDPv4 0.0.0.0:55769 *:*
0x896 svchost.exe 2021-07-12 12:34:42 UTC+0000
0x984 svchost.exe 2021-07-12 12:33:32 UTC+0000
0x8eceda8 TCPv4 0.0.0.0:49154 0.0.0.0:8 LISTENING
0x924 svchost.exe
0x8bf37ad90 TCPv4 0.0.0.0:49154 0.0.0.0:8 LISTENING
0x924 svchost.exe
0x8bf37ad90 TCPv6 :::49154 :::0 LISTENING
0x924 svchost.exe
0x8bf37ad90 TCPv4 192.168.106.144:56654 255.255.255.255:443 CLOSED
0x8bf37ad90 TCPv4 192.168.106.144:56655 255.255.255.255:443 CLOSED
0x8bf37ad90 UDPv4 127.0.0.1:63650 *:*
0x8bf37ad90 svchost.exe 2021-07-12 10:25:03 UTC+0000
0x2836 svchost.exe 192.168.106.144:54934 255.255.255.255:443 CLOSED
0x8bf37ad90 TCPv4 192.168.106.144:54934 255.255.255.255:443 CLOSED
0x8bf37ad90 -1

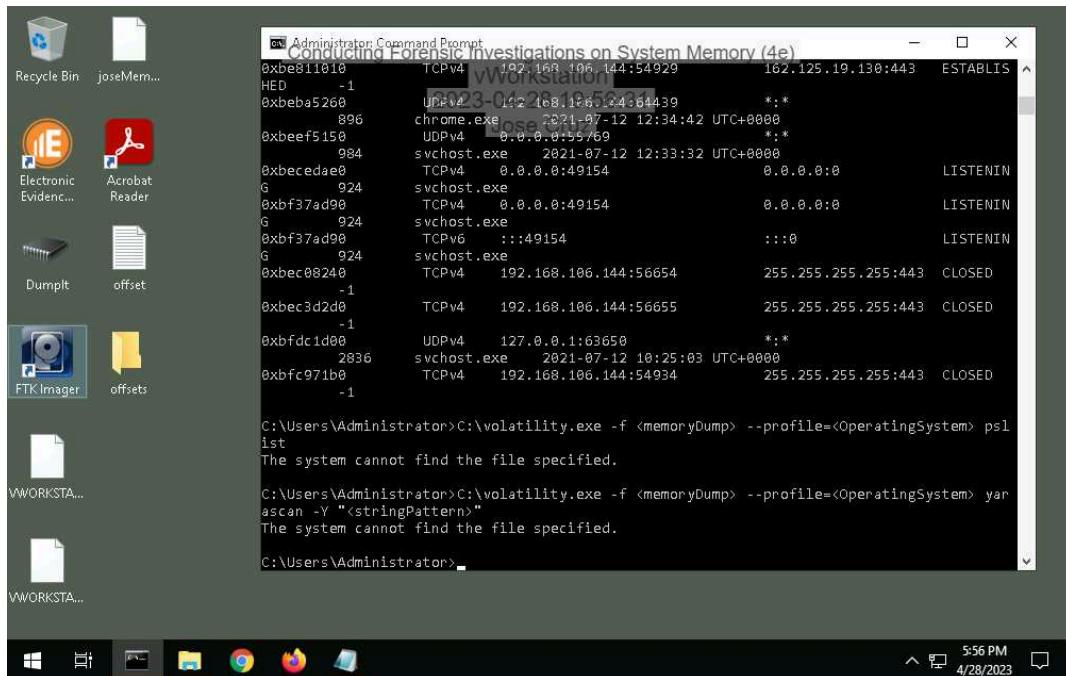
C:\Users\Administrator>C:\volatility.exe -f <memoryDump> --profile=<OperatingSystem> pslist
The system cannot find the file specified.

C:\Users\Administrator>
```

# Conducting Forensic Investigations on System Memory (4e)

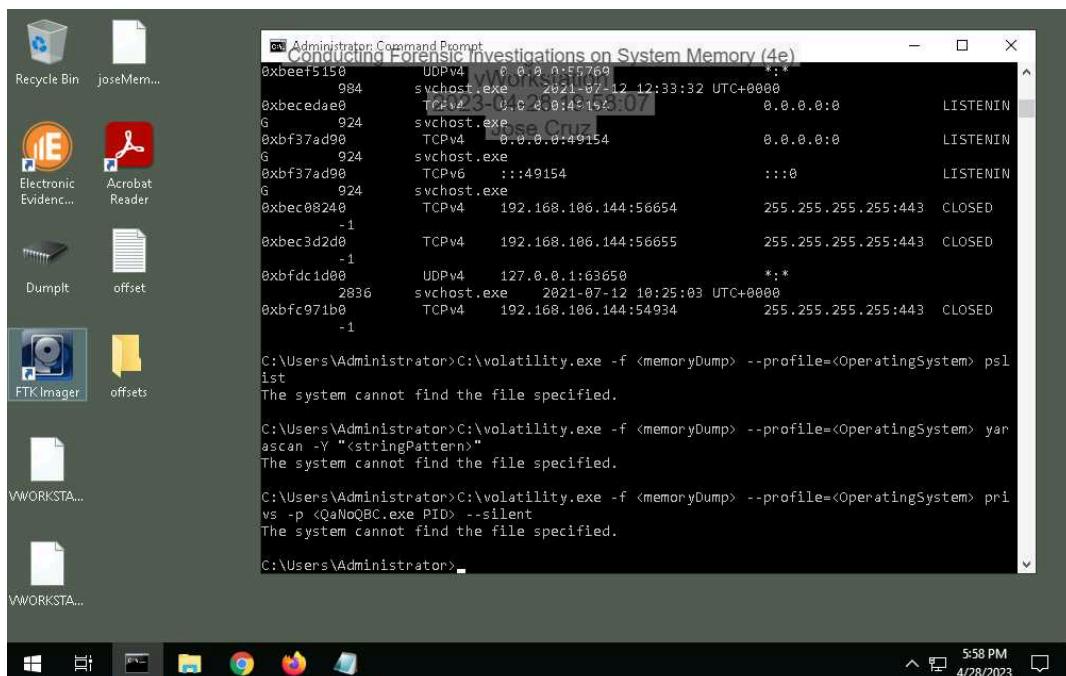
Digital Forensics, Investigation, and Response, Fourth Edition - Lab 10

**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.**



# **Conducting Forensic Investigations on System Memory (4e)**

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 10

---