

Conducting Forensic Investigations on System Memory (4e)

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

Student:

Jordan Calvert

Email:

jordanryancalvert@gmail.com

Time on Task:

8 hours, 13 minutes

Progress:

100%

Report Generated: Wednesday, May 15, 2024 at 10:49 AM

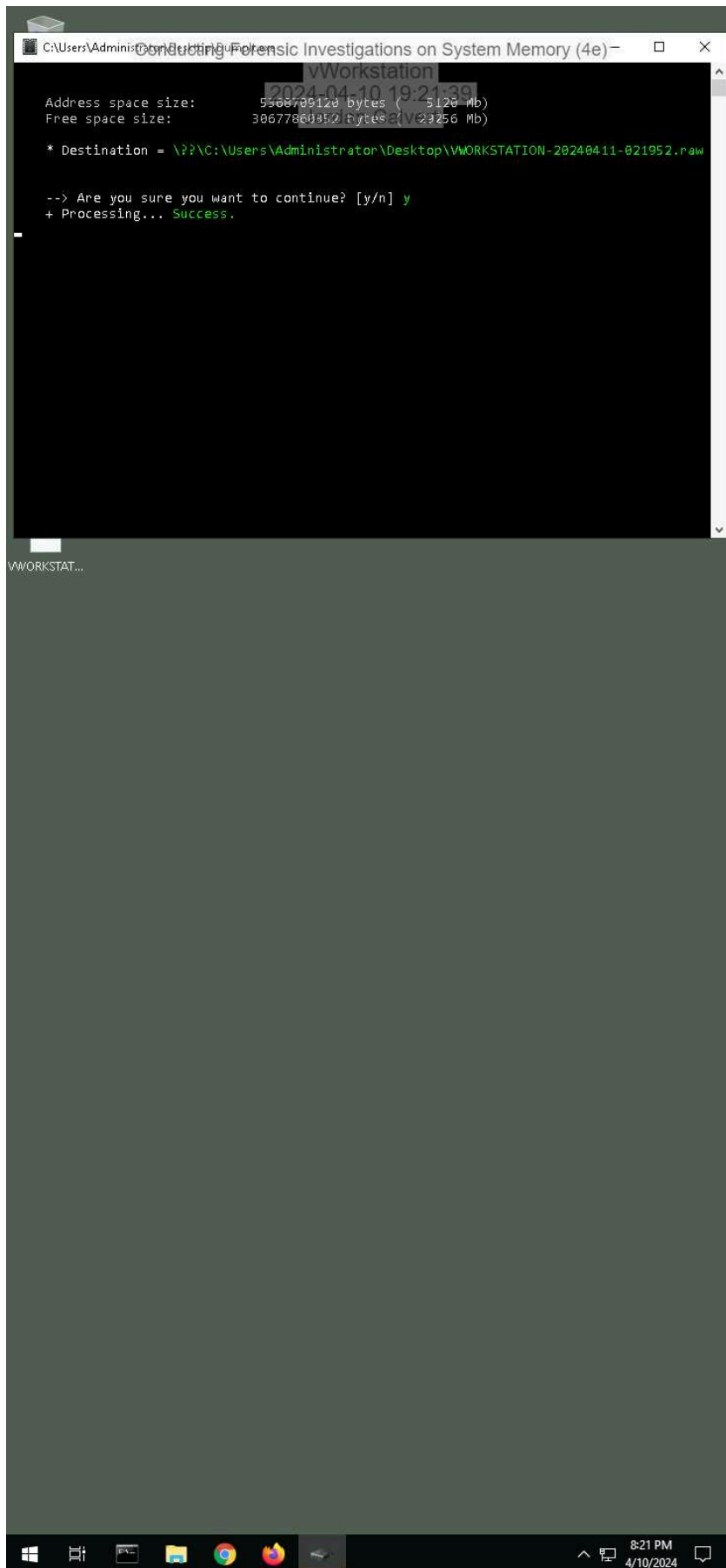
Section 1: Hands-On Demonstration

Part 1: Capture Memory using DumpIt

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

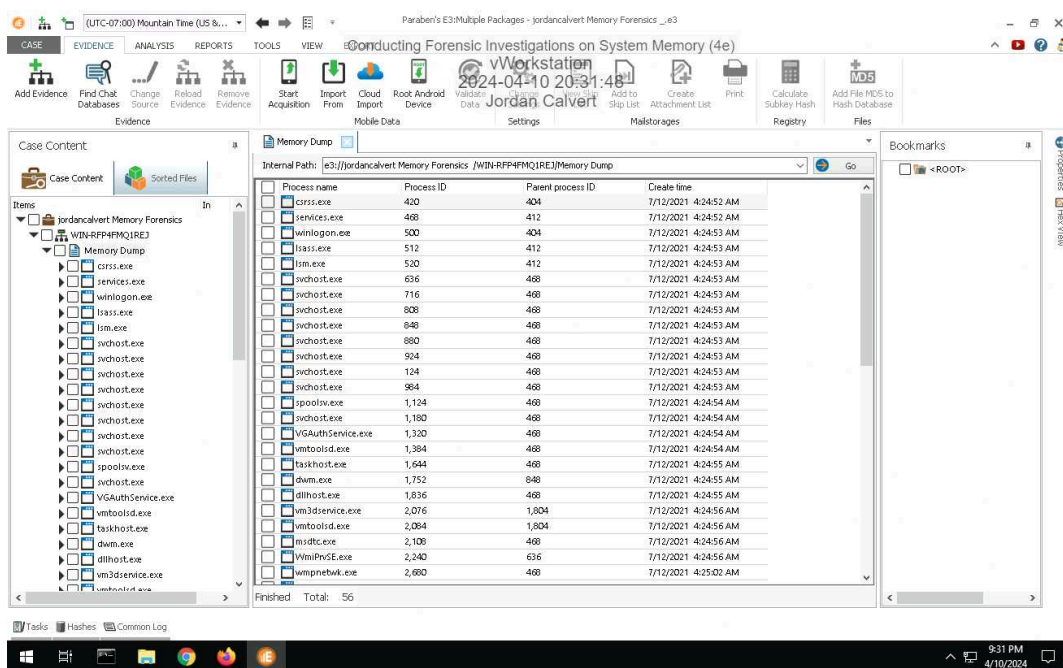
Conducting Forensic Investigations on System Memory (4e)

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



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.

oldest is process 4 newest is process 6,000

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

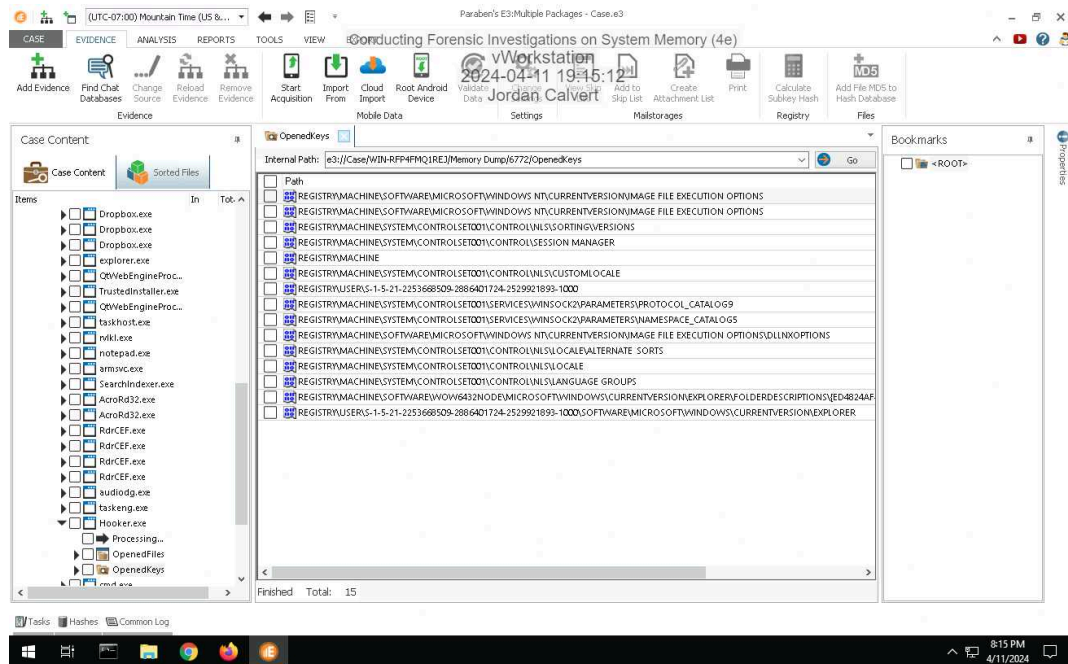
conhost.exe is the command line host process in Windows, responsible for creating console windows to run command line applications.

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

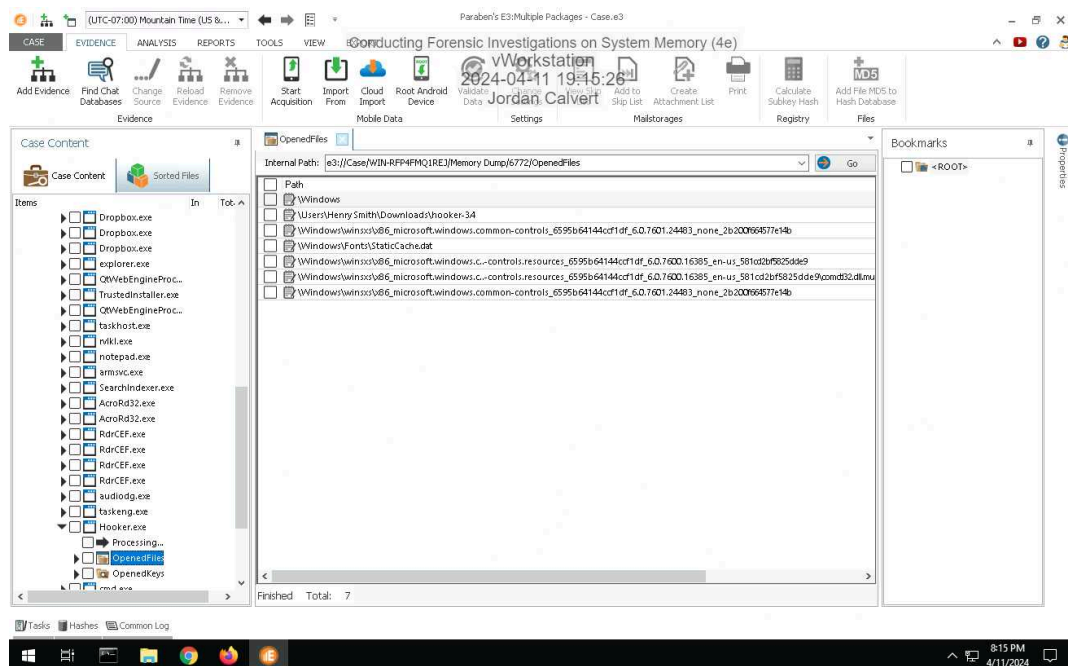
Hooker is a password and data stealing trojan. Being run it installs itself as KERN32.EXE into \Windows\System\directory and modifies RunOnce key in the Registry to be run during next Windows session.

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

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



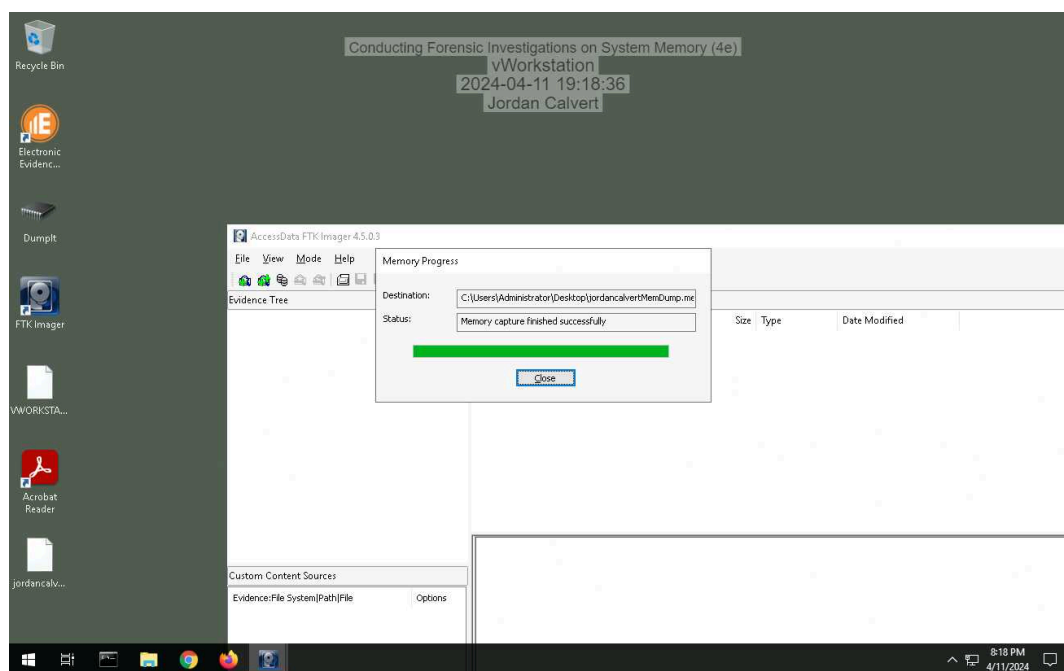
23. **Make a screen capture** showing the files opened by the hooker.exe process.



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 rvkl.exe process. What is it and what is it used for?

rvkl.exe is an executable exe file that belongs to the Revealer Keylogger process which comes along with the Revealer Keylogger Software developed by Logixoft software developer. Revealer Keylogger is a program that allows you to monitor the keystrokes types on your computer. such as passwords, chat messages, emails, and web searches.

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

There are no processes that are flagged as hidden.

Conducting Forensic Investigations on System Memory (4e)

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

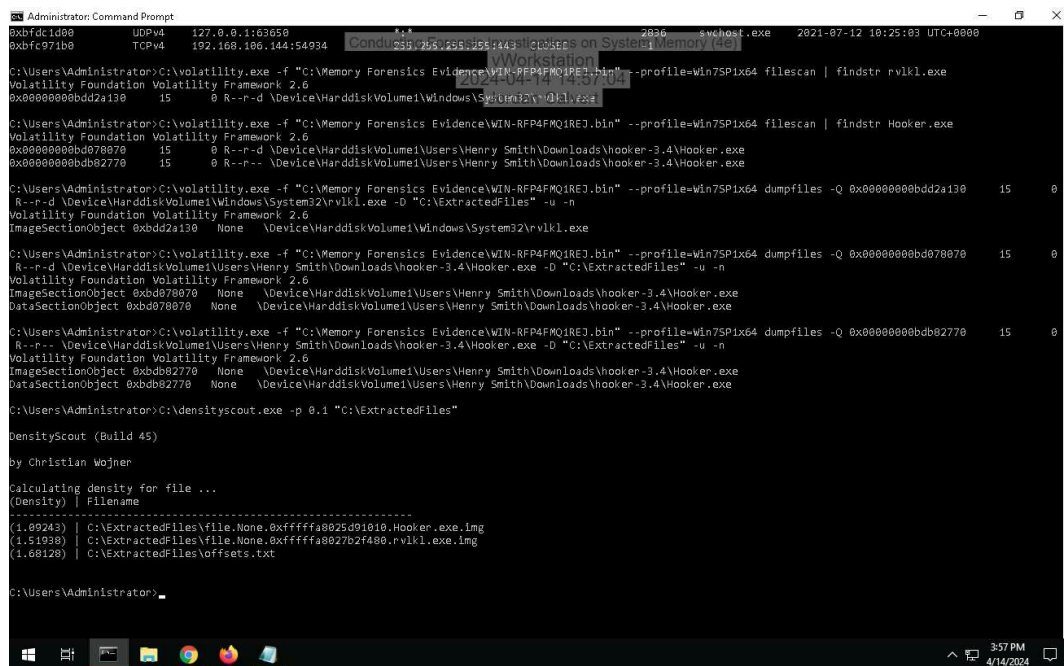
12. **Document** whether the netscan module displays network usage associated with the Hooker.exe or rvkl.exe processes.

There are no indications of network usage associated with the Hooker.exe or rvkl.exe processes.

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

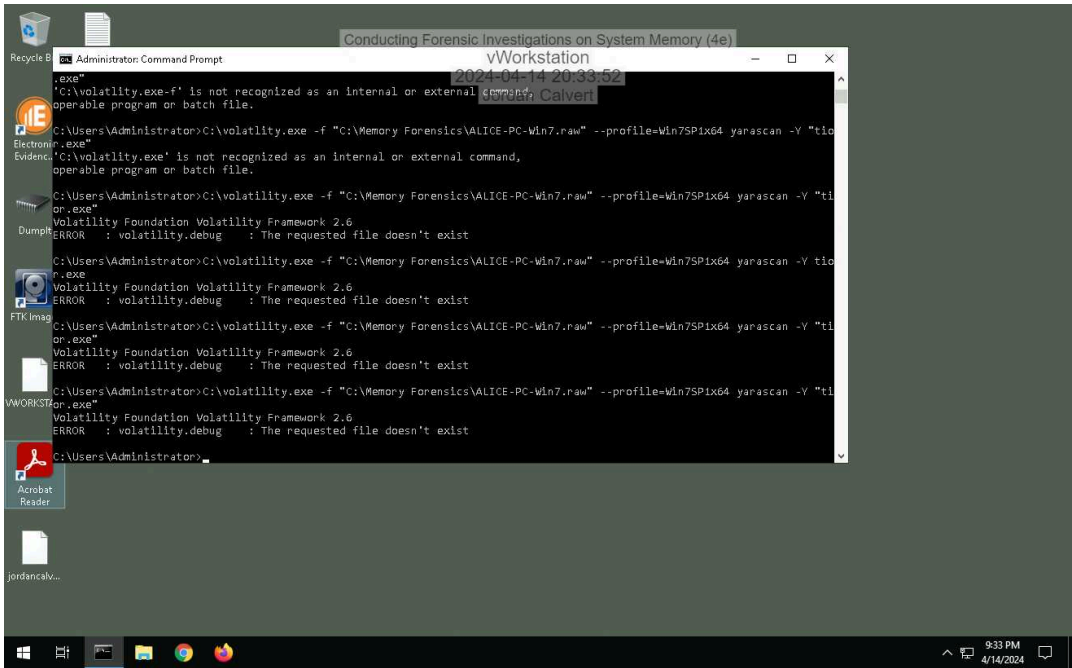
-falls within the 49152-65535 port range-often used for specific, custom configurations-requires network monitoring to determine usage-unassigned status warrants cautious monitoring for unusual activities

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



```
Administrator: Command Prompt
0xbfdcd00 UDPv4 127.0.0.1:63650 2021-07-12 18:25:03 UTC+0000
0xbfc97100 TCPv4 192.168.186.144:54934
C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\WIN-RFP4FMQ1REJ.bin" --profile=Win7SP1x64 filescan | findstr rvkl.exe
Volatility Foundation Volatility Framework 2.6
0x00000000bdd2a130 15 0 R--r-d \Device\HarddiskVolume1\Windows\System32\rvkl.exe
C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\WIN-RFP4FMQ1REJ.bin" --profile=Win7SP1x64 filescan | findstr Hooker.exe
Volatility Foundation Volatility Framework 2.6
0x00000000bd070070 15 0 R--r-d \Device\HarddiskVolume1\Users\Henry Smith\Downloads\hooker-3.4\Hooker.exe
0x00000000bd072770 15 0 R--r-d \Device\HarddiskVolume1\Users\Henry Smith\Downloads\hooker-3.4\Hooker.exe
C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\WIN-RFP4FMQ1REJ.bin" --profile=Win7SP1x64 dumpfiles -Q 0x00000000bdd2a130 15 0
R--r-d \Device\HarddiskVolume1\Windows\System32\rvkl.exe -D "C:\ExtractedFiles" -u -n
Volatility Foundation Volatility Framework 2.6
ImageSectionObject 0xbdd2a130 None \Device\HarddiskVolume1\Windows\System32\rvkl.exe
C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\WIN-RFP4FMQ1REJ.bin" --profile=Win7SP1x64 dumpfiles -Q 0x00000000bd070070 15 0
R--r-d \Device\HarddiskVolume1\Users\Henry Smith\Downloads\hooker-3.4\Hooker.exe -D "C:\ExtractedFiles" -u -n
Volatility Foundation Volatility Framework 2.6
ImageSectionObject 0xbd070070 None \Device\HarddiskVolume1\Users\Henry Smith\Downloads\hooker-3.4\Hooker.exe
DataSectionObject 0xbd070070 None \Device\HarddiskVolume1\Users\Henry Smith\Downloads\hooker-3.4\Hooker.exe
C:\Users\Administrator>C:\volatility.exe -f "C:\Memory Forensics Evidence\WIN-RFP4FMQ1REJ.bin" --profile=Win7SP1x64 dumpfiles -Q 0x00000000bd072770 15 0
R--r-d \Device\HarddiskVolume1\Users\Henry Smith\Downloads\hooker-3.4\Hooker.exe -D "C:\ExtractedFiles" -u -n
Volatility Foundation Volatility Framework 2.6
ImageSectionObject 0xbdb02770 None \Device\HarddiskVolume1\Users\Henry Smith\Downloads\hooker-3.4\Hooker.exe
DataSectionObject 0xbdb02770 None \Device\HarddiskVolume1\Users\Henry Smith\Downloads\hooker-3.4\Hooker.exe
C:\Users\Administrator>C:\densityscout.exe -p 0.1 "C:\ExtractedFiles"
DensityScout (Build 45)
by Christian Wojner
Calculating density for file ...
(Density) | Filename
-----|-----
(1.00243) | C:\ExtractedFiles\file.None.0xfffffa8025d91010.Hooker.exe.img
(1.51093) | C:\ExtractedFiles\file.None.0xfffffa8027b2f480.rvkl.exe.img
(1.60128) | C:\ExtractedFiles\offsets.txt
C:\Users\Administrator>
```


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.

