

Faculty of Engineering Computing and the Environment

Undergraduate Modular Scheme

Kingston University London
ESOFT Metro Campus – Sri Lanka

Validated Provision

Examinations 2023/2024

Level 6

MODULE: CI6280 - Threat Hunting Analysis and Mitigation

DURATION: 3 hours

Instructions to Candidates

- Answer **ALL** questions.
- This question paper has **4** questions on **4** pages.
- This Practical Exam paper carries 20% of total module marks.
- Maximum marks allocated for each section of questions are shown.
- Do not refer resources from the internet or any other materials.

Mark Distribution

Assessable Item	Marks
<p>Question 01 (20 marks)</p> <ol style="list-style-type: none"> Write the steps that you have to follow when creating the disk image using the FTK imager. (10 marks) Write the steps that you have to follow when creating the memory image using the FTK imager. (10 marks) <p>Question 02 (30 marks)</p> <p>Download the memory image and save in the folder of Volatility. Analyze this memory image using the volatility tool and find answers to the following questions:</p> <ol style="list-style-type: none"> Which command is used to give all the information about the above memory image by Volatility and attach a screenshot after analyzing this command? (10 marks) Which command can be used to retrieve the list running processes from memory dump? (05 marks) Which command can be used to scan the existing networks from memory dump? (05 marks) Which command can be used to show the processes in the parent-child relationship format? (05 marks) Which command can be used to extract the list of open TCP connections from the memory file? (05 marks) <p>Question 03 (25 marks)</p> <p>Analyze the Packet Capture File. Examine the Wireshark window and find answers to the following questions:</p> <ol style="list-style-type: none"> This packet capture file contains two TCP handshakes. Find the first handshake and write down the packet numbers of those packets (the column labeled "No."). (05 marks) In this session, a client machine initiated a connection to a server and then downloaded a file. What is the client's IP address? (05 marks) How many HTTP GET request packets are there? (05 marks) Find the first HTTP GET request packet. What was the server's IP address? (The server is the Destination). (05 marks) Examine the first packet. Look at the center pane in Wireshark. How many bytes were sent on the wire to form this packet? (05 marks) 	100

Question 04

(25 marks)

The following screen shots showing the HTTP GET and HTTP REPLY answer these questions:

HTTP GET:

```
No.      Time      Source      Destination      Protocol Info
 133 4.098946 192.168.1.101 128.119.245.12  HTTP      GET /wireshark-labs/HTTP-wire

Frame 133 (488 bytes on wire, 488 bytes captured)
Ethernet II, Src: IntelCor dc:36:d0 (00:22:fa:dc:36:d0), Dst: Cisco-Li 45:1f:1b (00:22:6b:45:1f:1b)
Internet Protocol, Src: 192.168.1.101 (192.168.1.101), Dst: 128.119.245.12 (128.119.245.12)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
  Total Length: 474
  Identification: 0x036e (878)
  Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 128
  Protocol: TCP (0x06)
  Header checksum: 0xbe1e [correct]
  Source: 192.168.1.101 (192.168.1.101)
  Destination: 128.119.245.12 (128.119.245.12)
Transmission Control Protocol, Src Port: 55428 (55428), Dst Port: http (80), Seq: 1, Ack: 1, Len: 434
  Source port: 55428 (55428)
  Destination port: http (80)
  [Stream index: 27]
  Sequence number: 1 (relative sequence number)
  [Next sequence number: 435 (relative sequence number)]
  Acknowledgement number: 1 (relative ack number)
  Header length: 20 bytes
  Flags: 0x18 (PSH, ACK)
  Window size: 64240
  Checksum: 0xe737 [validation disabled]
  [SEQ/ACK analysis]
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.11) Gecko/20101012 Firefox/3.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: en-us,en;q=0.5\r\n
Accept-Encoding: gzip,deflate\r\n
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
Keep-Alive: 115\r\n
Connection: keep-alive\r\n
\r\n
```

HTTP REPLY:

```
No.      Time      Source      Destination      Protocol Info
 135 4.126437 128.119.245.12 192.168.1.101  HTTP      HTTP/1.1 200 OK (text/html)

Frame 135 (488 bytes on wire, 488 bytes captured)
Ethernet II, Src: Cisco-Li 45:1f:1b (00:22:6b:45:1f:1b), Dst: IntelCor dc:36:d0 (00:22:fa:dc:36:d0)
Internet Protocol, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.101 (192.168.1.101)
Transmission Control Protocol, Src Port: http (80), Dst Port: 55428 (55428), Seq: 1, Ack: 435, Len: 43
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
  [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
  Request Version: HTTP/1.1
  Response Code: 200
  Date: Wed, 27 Oct 2010 11:26:58 GMT\r\n
  Server: Apache/2.0.52 (CentOS)\r\n
  Last-Modified: Wed, 27 Oct 2010 11:26:01 GMT\r\n
  ETag: "8734d-80-7d74e440"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 128\r\n
  [Content length: 128]
  Keep-Alive: timeout=10, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=ISO-8859-1\r\n
\r\n
Line-based text data: text/html
<html>\r\n
  Congratulations. You've downloaded the file \r\n
  http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\r\n
</html>\r\n
```

- | | |
|--|--|
| <ol style="list-style-type: none">1. What is the IP address of your computer and the gaia.cs.umass.edu server? (05 marks)2. What is the status code returned from the server to your browser? (05 marks)3. When was the HTML file that you were retrieving last modified on the server? (05 marks)4. How many bytes of content are being returned to your browser? (05 marks)5. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one. (05 marks) | |
|--|--|

END OF QUESTION PAPER

QUESTION NUMBER 01

01.

Step 01. Opening FTK File Imager

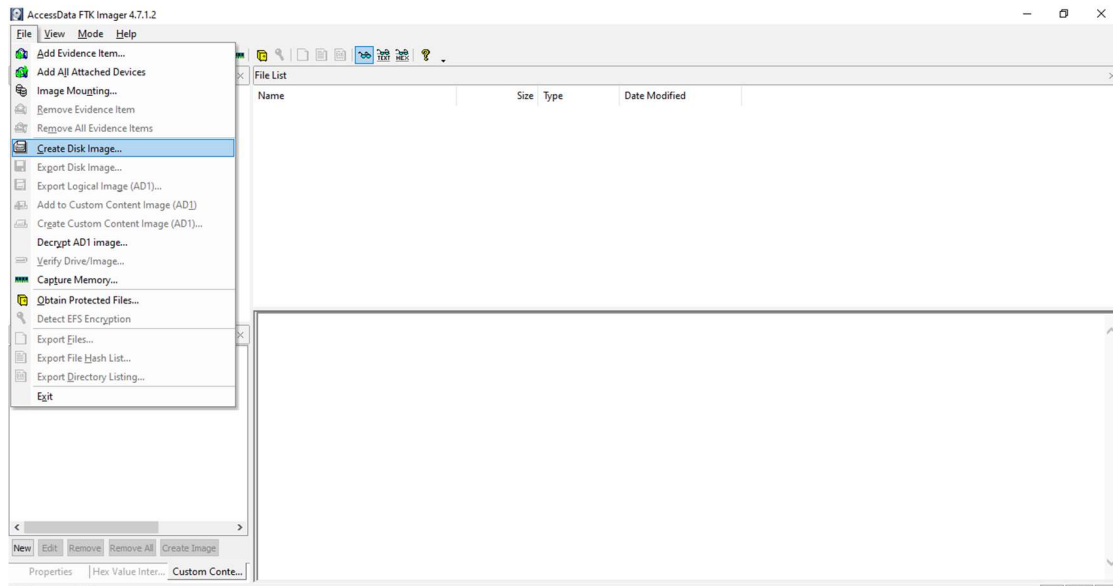


Figure 1:FTK Imager interface

Step 02 Selecting Create Disk Image From File

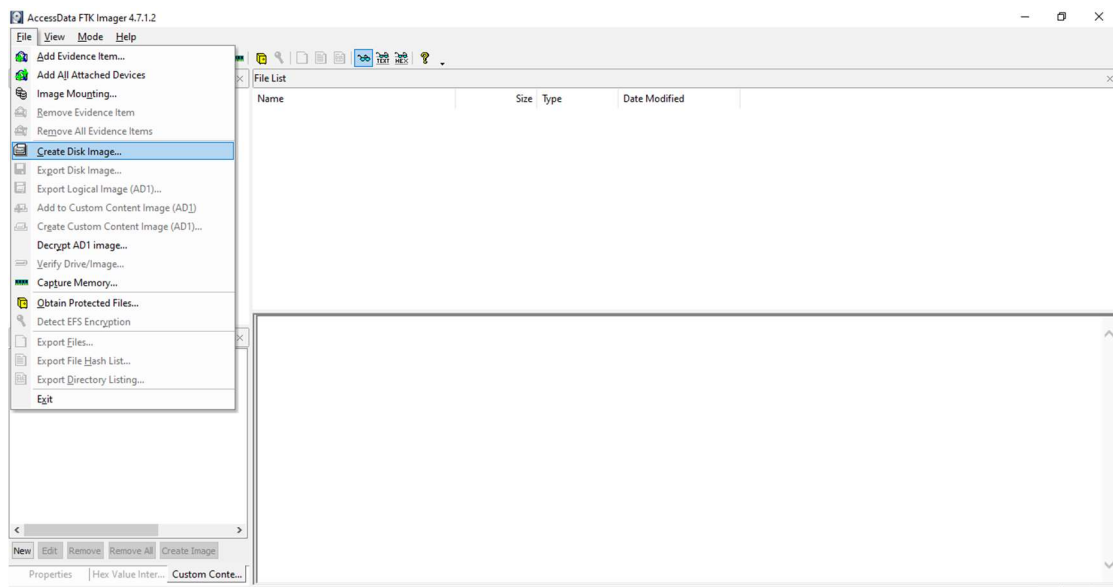


Figure 2:Selecting Disk Image

Step 03 Selecting Source Evidence Type

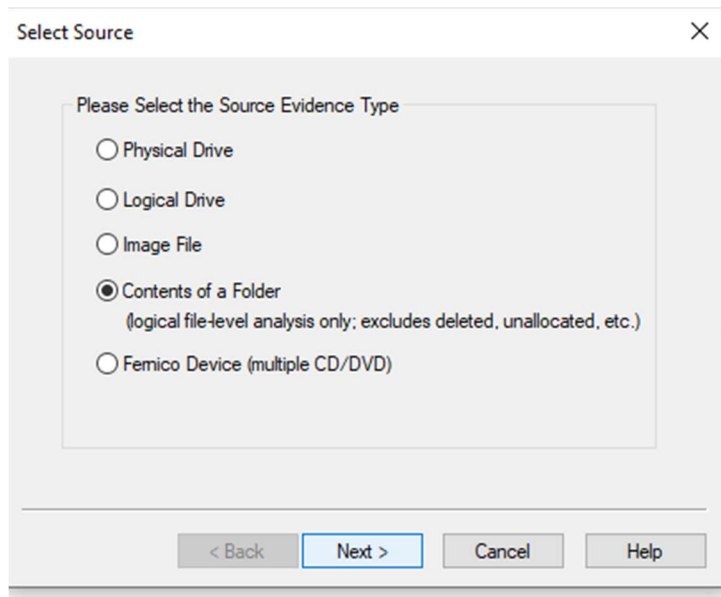


Figure 3: Selecting Source Evidence

Step 04: Selecting Available Drives

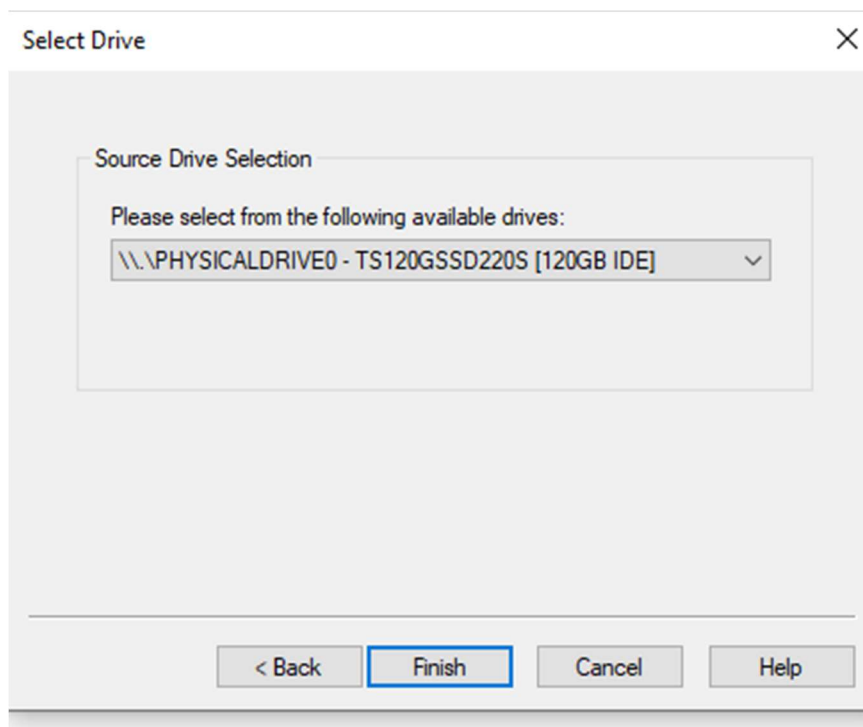
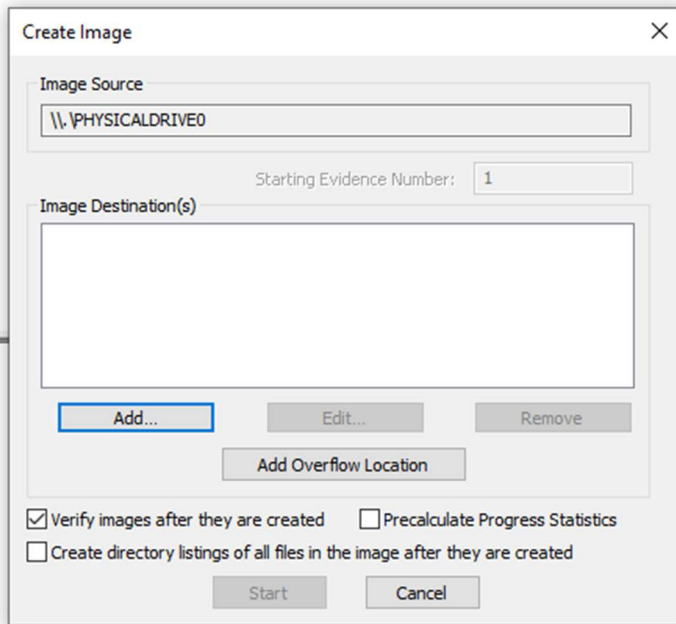


Figure 4: Selecting Available Drives

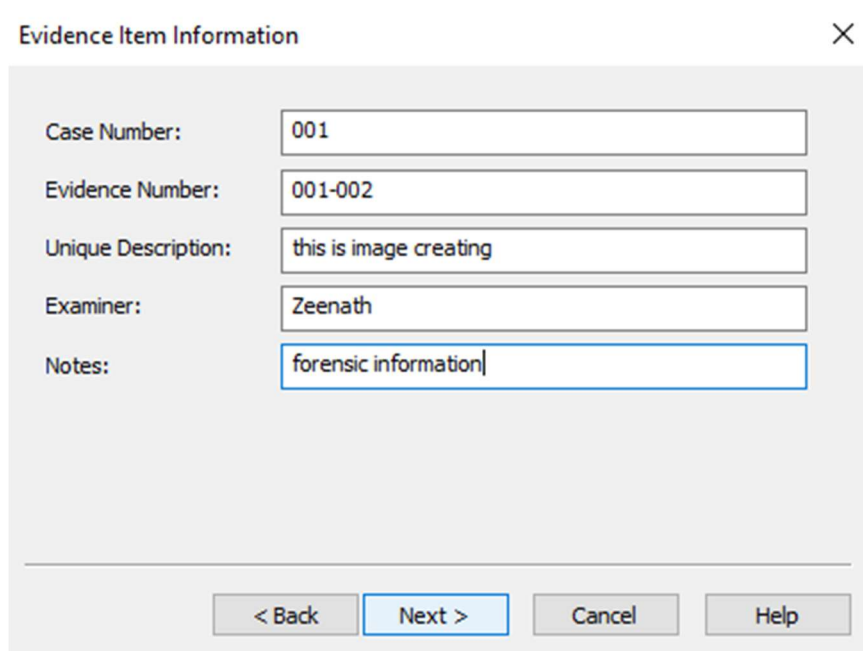
Step 05: Entering Image Source And Image Destination



The 'Create Image' dialog box is shown. It has a title bar with a close button (X). The 'Image Source' field contains '\\.\PHYSICALDRIVE0'. Below it, the 'Starting Evidence Number' is set to 1. The 'Image Destination(s)' section is empty, with buttons for 'Add...', 'Edit...', 'Remove', and 'Add Overflow Location'. At the bottom, there are checkboxes for 'Verify images after they are created' (checked), 'Precalculate Progress Statistics' (unchecked), and 'Create directory listings of all files in the image after they are created' (unchecked). 'Start' and 'Cancel' buttons are at the bottom right.

Figure 5: Entering Image Source And Image Destination

Step 06 Entering Evidence Item Information



The 'Evidence Item Information' dialog box is shown. It has a title bar with a close button (X). The fields are: 'Case Number:' with value '001', 'Evidence Number:' with value '001-002', 'Unique Description:' with value 'this is image creating', 'Examiner:' with value 'Zeenath', and 'Notes:' with value 'forensic information'. At the bottom, there are buttons for '< Back', 'Next >', 'Cancel', and 'Help'.

Figure 6: Entering Evidence Item Information

Step 07 Selecting Image Destination

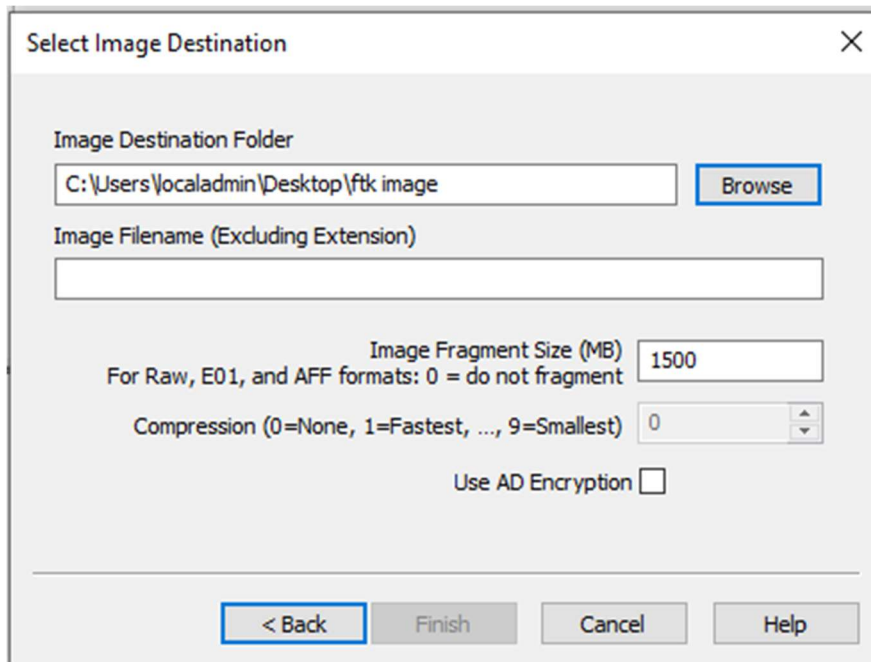


Figure 7: Selecting Image Destination

Step 08 By Clicking Start Creating Image

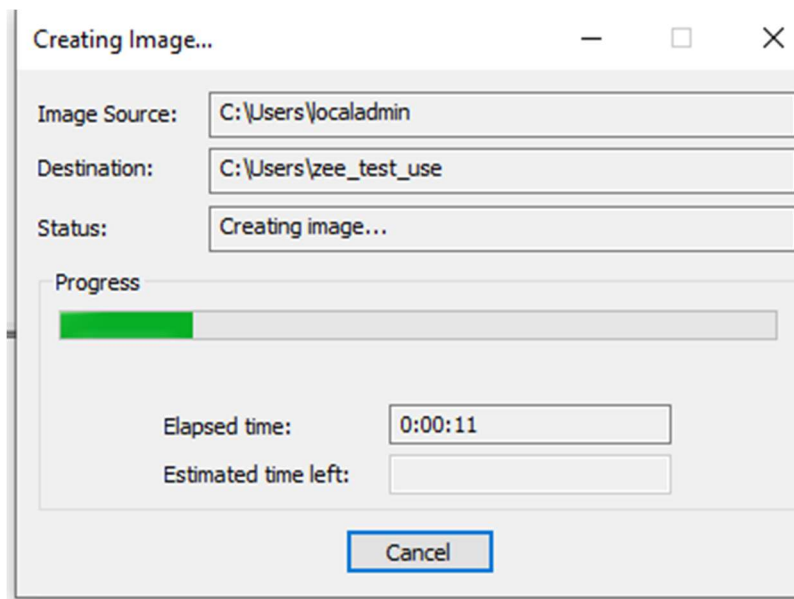


Figure 8: By Clicking Start Creating Image

02.

Step 01: Selecting Capture Memory From Files

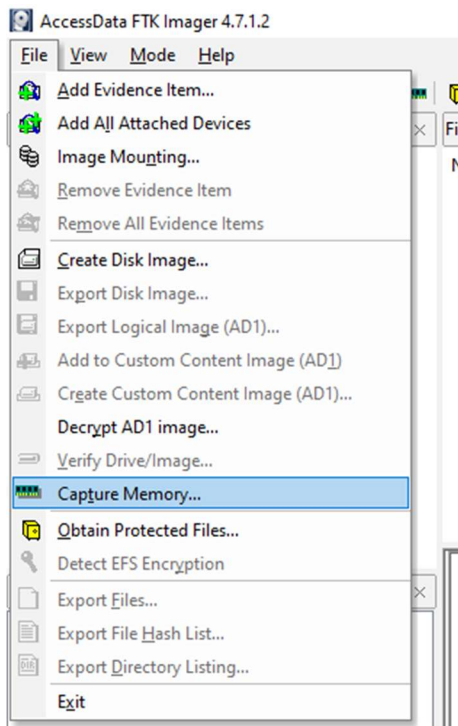


Figure 9: Selecting Capture Memory From Files

Step 02: Entering Destination Path

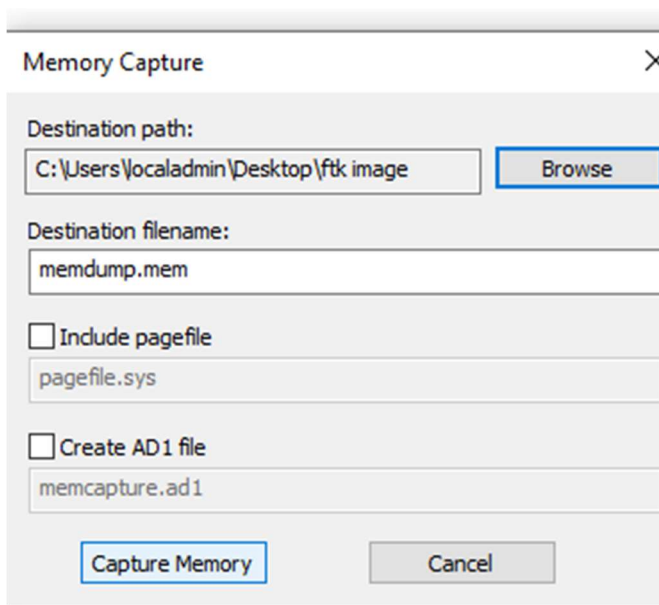


Figure 10: : Entering Destination Path

Step 03: Memory Progress

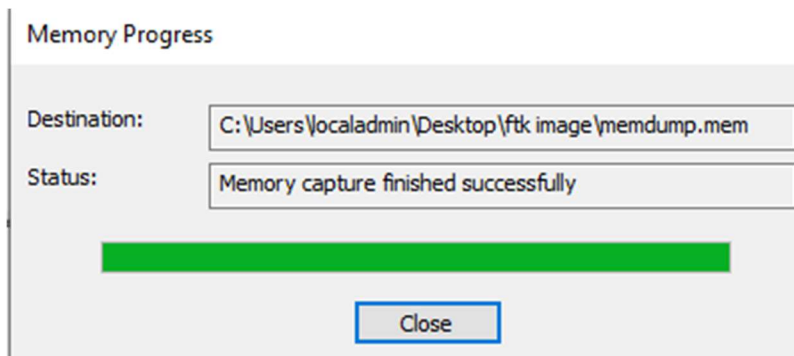


Figure 11:Memory Capturing

Step 04: Captured File

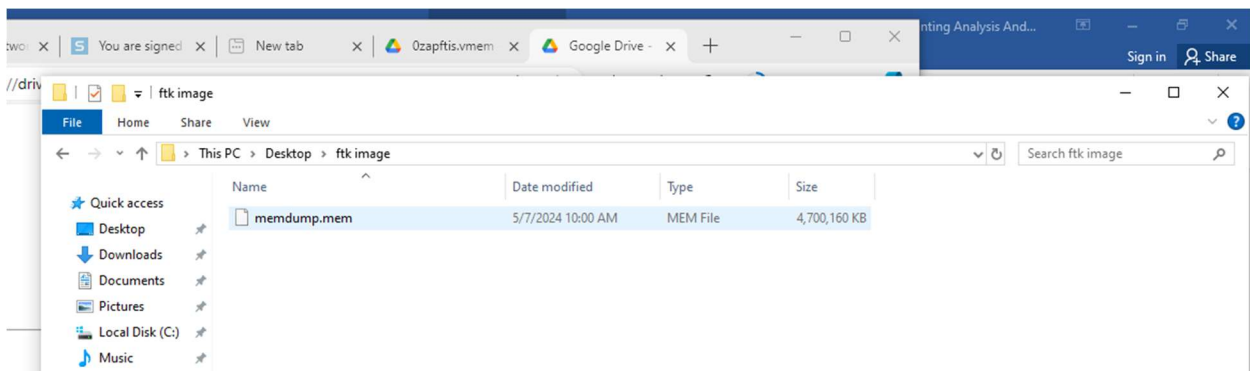
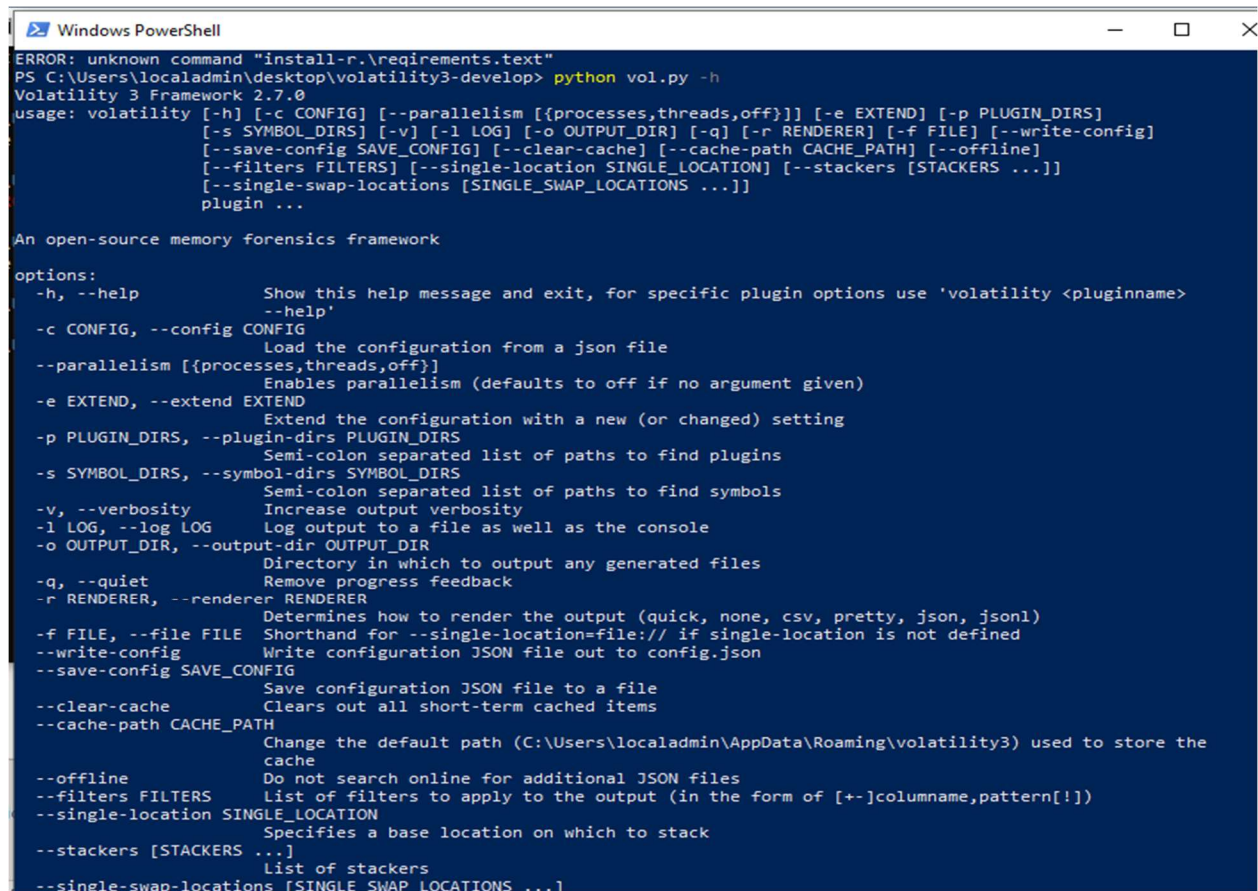


Figure 12:Captured file

QUESTION NUMBER 02

01. python vol.py -h



```
Windows PowerShell
ERROR: unknown command "install-r.\requirements.text"
PS C:\Users\localadmin\desktop\volatility3-develop> python vol.py -h
Volatility 3 Framework 2.7.0
usage: volatility [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS]
                  [-s SYMBOL_DIRS] [-v] [-l LOG] [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE] [--write-config]
                  [--save-config SAVE_CONFIG] [--clear-cache] [--cache-path CACHE_PATH] [--offline]
                  [--filters FILTERS] [--single-location SINGLE_LOCATION] [--stackers [STACKERS ...]]
                  [--single-swap-locations [SINGLE_SWAP_LOCATIONS ...]]
                  plugin ...

An open-source memory forensics framework

options:
  -h, --help            Show this help message and exit, for specific plugin options use 'volatility <pluginname>
                        --help'
  -c CONFIG, --config CONFIG
                        Load the configuration from a json file
  --parallelism [{processes,threads,off}]
                        Enables parallelism (defaults to off if no argument given)
  -e EXTEND, --extend EXTEND
                        Extend the configuration with a new (or changed) setting
  -p PLUGIN_DIRS, --plugin-dirs PLUGIN_DIRS
                        Semi-colon separated list of paths to find plugins
  -s SYMBOL_DIRS, --symbol-dirs SYMBOL_DIRS
                        Semi-colon separated list of paths to find symbols
  -v, --verbosity        Increase output verbosity
  -l LOG, --log LOG      Log output to a file as well as the console
  -o OUTPUT_DIR, --output-dir OUTPUT_DIR
                        Directory in which to output any generated files
  -q, --quiet            Remove progress feedback
  -r RENDERER, --renderer RENDERER
                        Determines how to render the output (quick, none, csv, pretty, json, jsonl)
                        Shorthand for --single-location=file:// if single-location is not defined
  --write-config          Write configuration JSON file out to config.json
  --save-config SAVE_CONFIG
                        Save configuration JSON file to a file
                        Clears out all short-term cached items
  --clear-cache          Clears out all short-term cached items
  --cache-path CACHE_PATH
                        Change the default path (C:\Users\localadmin\AppData\Roaming\volatility3) used to store the
                        cache
  --offline              Do not search online for additional JSON files
  --filters FILTERS      List of filters to apply to the output (in the form of [+<columnname,pattern[!<columnname>]]
  --single-location SINGLE_LOCATION
                        Specifies a base location on which to stack
  --stackers [STACKERS ...]
                        List of stackers
  --single-swap-locations [SINGLE_SWAP_LOCATIONS ...]
```

Figure 13: Screenshot of above command

02. python vol.py -f C:\Users\localadmin\Desktop\volatility3-develop.vmem psscan

03. python vol.py -f C:\Users\localadmin\Desktop\volatility3-develop.vmem netscan

04. python vol.py -f C:\Users\localadmin\Desktop\volatility3-develop.vmem pstree

05. python vol.py -f C:\Users\localadmin\Desktop\volatility3-develop.vmem connections

QUESTION NUMBER 03

- 01. No.9
- 02. 147.144.1.212
- 03. 3 HTTP Packets
- 04. 74.125.19.113
- 05. 66 packets

QUESTION NUMBER 04

- 01. Source: 192.168.1.101
Destination: 128.119.245.12
- 02. Status code:200
- 03. Wed, 27 Oct 2010
- 04. 488 Packets were returned
- 05. Payload time