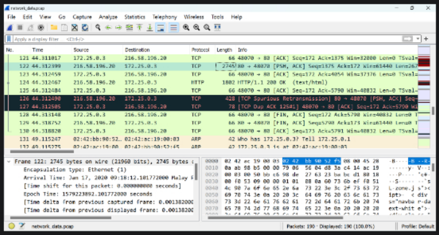
Challenge 9 Solves ×

[Forensic Tools]

100

Navigating an electronic evidence requires the right tools. Here are some essential forensic tools that CTF players normally use:

1. **Wireshark**: The undisputed king of network analysis. Wireshark is a tool to capture and analyse network traffic. CTF players use it to identify suspicious activity and hidden messages within network packets. Link: https://www.wireshark.org/download.html


network_data.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time       Source            Destination       Protocol Length Info
121 44.311817  172.25.0.3        216.58.196.20     TCP        66 48070 → 80 [ACK] Seq=172 Ack=1375 Win=32800 Len=0 TSval=
122 44.312399  216.58.196.20     172.25.0.3        TCP      2745 80 → 48070 [PSH, ACK] Seq=1375 Ack=172 Win=61440 Len=267
123 44.312459  172.25.0.3        216.58.196.20     TCP        66 48070 → 80 [ACK] Seq=172 Ack=4054 Win=37376 Len=0 TSval=
124 44.312467  216.58.196.20     172.25.0.3        HTTP     1802 HTTP/1.1 200 OK  (text/html)
125 44.312484  172.25.0.3        216.58.196.20     TCP        66 48070 → 80 [ACK] Seq=172 Ack=5790 Win=40832 Len=0 TSval=
126 44.312490  216.58.196.20     172.25.0.3        TCP       428 [TCP Spurious Retransmission] 80 → 48070 [PSH, ACK] Seq=
127 44.312505  172.25.0.3        216.58.196.20     TCP        78 [TCP Dup ACK 125#1] 48070 → 80 [ACK] Seq=172 Ack=5790 Wi
128 44.313148  172.25.0.3        216.58.196.20     TCP        66 48070 → 80 [FIN, ACK] Seq=172 Ack=5790 Win=40832 Len=0 T
129 44.318752  216.58.196.20     172.25.0.3        TCP        66 80 → 48070 [FIN, ACK] Seq=5790 Ack=173 Win=61440 Len=0 T
130 44.318820  172.25.0.3        216.58.196.20     TCP        66 48070 → 80 [ACK] Seq=173 Ack=5791 Win=40832 Len=0 TSval=
131 49.115247  02:42:bb:90:52…   02:42:ac:19:00:03 ARP        42 Who has 172.25.0.3? Tell 172.25.0.1
132 49.115275  02:42:ac:19:00…   02:42:bb:90:52:f5 ARP        42 172.25.0.3 is at 02:42:ac:19:00:03

Frame 122: 2745 bytes on wire (21960 bits), 2745 bytes c
   Encapsulation type: Ethernet (1)
   Arrival Time: Jan 17, 2020 09:18:12.101772000 Malay P
   [Time shift for this packet: 0.000000000 seconds]
   Epoch Time: 1579223892.101772000 seconds
   [Time delta from previous captured frame: 0.00138200
   [Time delta from previous displayed frame: 0.00138200

0000  02 42 ac 19 00 03 02 42  bb 90 52 f5 08 00 45 20   ·B·····B ··R···E
0010  0a ab 98 b5 00 00 79 06  56 04 d8 3a c4 14 ac 19   ······y· V··:····
0020  00 03 00 50 bb c6 98 de  27 63 23 be bc d1 80 18   ···P···· 'c#·····
0030  00 f0 53 09 00 00 01 01  08 0a 60 73 6b ef f0 51   ··S····· ··`sk··Q
0040  4c 90 7a 6f 6e 65 2e 6a  73 22 3e 3c 2f 73 63 72   L·zone.j s"></scr
0050  69 70 74 3e 0a 20 20 3c  64 69 76 20 63 6c 61 73   ipt>·  < div clas
0060  73 3d 22 6e 61 76 62 61  72 2d 64 61 72 6b 20 74   s="navba r-dark t
0070  65 78 74 2d 77 68 69 74  65 22 3e 0a 20 20 20 20   ext-whit e">·
```

Usage Instructions:

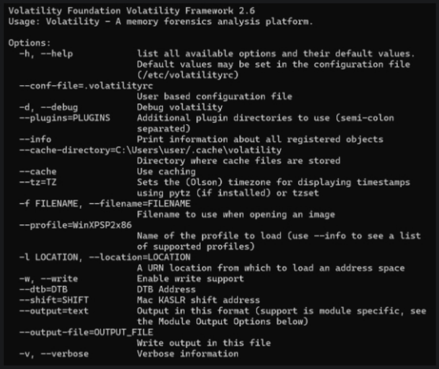
1. Under the "File" tab, click on "Open" and search for your network packet file to analyse. (Example: network_packet.pcap)
2. Filter the frames found in the packet as necessary by applying filters in the "Apply a display filter..." bar. (Example: ip.addr == 10.10.10.10)
3. Follow the network segments captured that are on the same connection as a selected packet. Example: TCP segments on a same TCP connection. -Right-click on a packet within the stream you want to follow. -Choose "Follow" -> "TCP Stream" (or the appropriate protocol stream option if not TCP).

YouTube Video Guide: https://www.youtube.com/watch?v=A4_DOr7Eiqo

2. **Volatility**
   Volatility is a memory forensics utility framework to extract digital artifacts from volatile memory (RAM) samples. It is an open-source command-line tool that CTF players use to analyse RAM dumps, which are snapshots of a computer's memory captured at a specific point in time.

Link:
Volatility 2.6:
https://github.com/volatilityfoundation/volatility
Volatility 3:
https://github.com/volatilityfoundation/volatility3

Differences: Volatility 2.6 has more plugins, Volatility 3 can find things faster.



```
Volatility Foundation Volatility Framework 2.6
Usage: Volatility - A memory forensics analysis platform.

Options:
  -h, --help            list all available options and their default values.
                        Default values may be set in the configuration file
                        (/etc/volatilityrc)
  --conf-file=.volatilityrc
                        User based configuration file
  -d, --debug           Debug volatility
  --plugins=PLUGINS     Additional plugin directories to use (semi-colon
                        separated)
  --info                Print information about all registered objects
  --cache-directory=C:\Users\user/.cache\volatility
                        Directory where cache files are stored
  --cache               Use caching
  --tz=TZ               Sets the (Olson) timezone for displaying timestamps
                        using pytz (if installed) or tzset
  -f FILENAME, --filename=FILENAME
                        Filename to use when opening an image
  --profile=WinXPSP2x86
                        Name of the profile to load (use --info to see a list
                        of supported profiles)
  -l LOCATION, --location=LOCATION
                        A URN location from which to load an address space
  -w, --write           Enable write support
  --dtb=DTB             DTB Address
  --shift=SHIFT         Mac KASLR shift address
  --output=text         Output in this format (support is module specific, see
                        the Module Output Options below)
  --output-file=OUTPUT_FILE
                        Write output in this file
  -v, --verbose         Verbose information
```

Usage Instructions: python vol.py [Command] -f [Image Name] [Profile]

[Command]: Predefined volatility plugins used to extract different type of data
[Image Name]: Name of the memory file to analyse
[Profile]: Parameter to tell volatility about the operating system that the memory image obtained from

CTF

[Welcome to CTFPrep] ✓
50

[CTF Formats] ✓
100

[CTF Challenge] ✓
100

Binary Exploitation/Pwn

[Pwn? Binary Exploitation?] ✓
100

[Stack-Based Buffer Overflow ✓
100

[Challenge Summary: Scammi ✓
100

Smashing the Stack ✓
200

Cryptography

[Cryptography?] ✓
100

[Base64] ✓
100

128/2? ✓
200

[Challenge Summary: A Meal I ✓
100

A Meal Fit for the Emperor ✓
200

CTFd

[CTFd?] ✓
100

CTF Strategies, Tips and

[CTF Strategies?] ✓
100

Reverse Engineering

[Reverse Engineering?] ✓
100

OSINT

[OSINT?] ✓
100

Steganography

[Steganography?] ✓

100

Web Exploitation

[Web Exploitation?] ✓

100

Forensics

[Forensics?] ✓

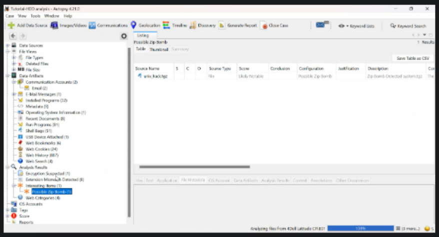
100

system that the memory image obtained from.

Example: python vol.py pslist -f /path/to/memory.img --profile=Win7SP1x64 (Extracts the list of processes from a Windows XP SP2 x86 memory dump)

YouTube Video Guide: https://youtu.be/Uk3DEgY5Ue8

3. **Autopsy**
   Autopsy is a free digital forensics platform with a graphical interface to utilise The Sleuthkit Tools. It is often used by CTF players to **analyse** the contents of **disk images or memory dumps and recover deleted files**. Link: https://www.autopsy.com/download/



Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Description
unix_hack.tgz				File	Likely Notable		Possible Zip Bomb		Zip Bomb Detected system.tgz

Usage Instructions: https://sleuthkit.org/autopsy/docs/user-

Powered by CTFd