NFSU

National Forensic Sciences University

Knowledge | Wisdom | Fulfilment

An Institution of National Importance
(Ministry of Home Affairs, Government of India)

LABORATORY REPORT

ON

Information & Network Security

CTBTCSE SVII L3

Submitted To

Dr. Rashi Chaudhary

Department of Cyber Security & Digital Forensics

National Forensic Sciences University

Submitted By

DAYANANDA BINDHANI

(022200300004018)

National Forensic Sciences University

Delhi Campus, New Delhi – 110085, India

TABLE OF CONTENT

PRACTICAL – 1

- **AIM:**
  Analysing network connections using `netstat`. Using netstat to view information about incoming and outgoing network connections, routing table, etc. (include all the commands).

- **TOOLS/APPLICATIONS USED:**
  netstat

- **THEORY:**
  Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). Used without parameters, this command displays active TCP connections.

- **PROCEDURES:**
  - Launch your terminal or command-line interface.
  - Execute netstat to view active and listening connections (incoming & outgoing).
  - Inspect the displayed list: local addresses, foreign addresses, connection states.
  - Display the routing table to check how network paths are configured.
  - Examine protocol statistics to identify unusual behaviour (e.g., many TCP in unusual states).
  - Look at interface statistics to detect packet drops, errors or high-volume traffic.
  - Correlate connection states (e.g., ESTABLISHED, TIME_WAIT, SYN_SENT) with expected network activity.
  - Note any unexpected entries: unknown remote addresses, unexpected listening ports, many connections in anomalous states.
  - Save/capture the output for your report or further analysis.
  - Conclude by interpreting what the results suggest about network health, routing correctness or suspicious activity.

- **OUTPUT:**

COMMAND: *netstat -a*

```
PS C:\Windows\System32> netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            PROFESSOR:0            LISTENING
  TCP    0.0.0.0:445            PROFESSOR:0            LISTENING
  TCP    0.0.0.0:5040           PROFESSOR:0            LISTENING
  TCP    0.0.0.0:7680           PROFESSOR:0            LISTENING
  TCP    0.0.0.0:49664          PROFESSOR:0            LISTENING
  TCP    0.0.0.0:49665          PROFESSOR:0            LISTENING
  TCP    0.0.0.0:49666          PROFESSOR:0            LISTENING
  TCP    0.0.0.0:49667          PROFESSOR:0            LISTENING
  TCP    0.0.0.0:49668          PROFESSOR:0            LISTENING
  TCP    0.0.0.0:49674          PROFESSOR:0            LISTENING
  TCP    0.0.0.0:50131          PROFESSOR:0            LISTENING
  TCP    127.0.0.1:9080         PROFESSOR:0            LISTENING
  TCP    127.0.0.1:49350        PROFESSOR:0            LISTENING
  TCP    127.0.0.1:50242        PROFESSOR:0            LISTENING
  TCP    127.0.0.1:52356        PROFESSOR:0            LISTENING
  TCP    127.0.0.1:52357        PROFESSOR:52358        ESTABLISHED
  TCP    127.0.0.1:52358        PROFESSOR:52357        ESTABLISHED
  TCP    127.0.0.1:52362        PROFESSOR:52363        ESTABLISHED
  TCP    127.0.0.1:52363        PROFESSOR:52362        ESTABLISHED
  TCP    127.0.0.1:52940        PROFESSOR:49350        TIME_WAIT
  TCP    127.0.0.1:52941        PROFESSOR:49350        TIME_WAIT
  TCP    127.0.0.1:52942        PROFESSOR:49350        TIME_WAIT
```

COMMAND: *netstat -n*

```
PS C:\Windows\System32> netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49350        127.0.0.1:53328        CLOSE_WAIT
  TCP    127.0.0.1:52357        127.0.0.1:52358        ESTABLISHED
  TCP    127.0.0.1:52358        127.0.0.1:52357        ESTABLISHED
  TCP    127.0.0.1:52362        127.0.0.1:52363        ESTABLISHED
  TCP    127.0.0.1:52363        127.0.0.1:52362        ESTABLISHED
  TCP    127.0.0.1:53292        127.0.0.1:49350        TIME_WAIT
  TCP    127.0.0.1:53293        127.0.0.1:49350        TIME_WAIT
  TCP    127.0.0.1:53294        127.0.0.1:49350        TIME_WAIT
```

COMMAND: *netstat -b*

```
PS C:\Windows\System32> netstat -b

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49350        PROFESSOR:53233        CLOSE_WAIT
 [esrv_svc.exe]
  TCP    127.0.0.1:49350        PROFESSOR:53235        CLOSE_WAIT
 [esrv_svc.exe]
  TCP    127.0.0.1:49350        PROFESSOR:53236        CLOSE_WAIT
 [esrv_svc.exe]
  TCP    127.0.0.1:49350        PROFESSOR:53237        CLOSE_WAIT
 [esrv_svc.exe]
  TCP    127.0.0.1:49350        PROFESSOR:53238        CLOSE_WAIT
 [esrv_svc.exe]
  TCP    127.0.0.1:52357        PROFESSOR:52358        ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:52358        PROFESSOR:52357        ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:52362        PROFESSOR:52363        ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:52363        PROFESSOR:52362        ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:53197        PROFESSOR:49350        TIME_WAIT
  TCP    127.0.0.1:53204        PROFESSOR:49350        TIME_WAIT
  TCP    127.0.0.1:53205        PROFESSOR:49350        TIME_WAIT
  TCP    127.0.0.1:53206        PROFESSOR:49350        TIME_WAIT
  TCP    127.0.0.1:53207        PROFESSOR:49350        TIME_WAIT
  TCP    127.0.0.1:53208        PROFESSOR:49350        TIME_WAIT
  TCP    127.0.0.1:53209        PROFESSOR:49350        TIME_WAIT
  TCP    127.0.0.1:53210        PROFESSOR:49350        TIME_WAIT
```

COMMAND: *netstat -e*

```
PS C:\Windows\System32> netstat -e
Interface Statistics

                           Received            Sent

Bytes                    2323558772       216425440
Unicast packets             4622485         1839915
Non-unicast packets            1358            1694
Discards                          0               0
Errors                            0               0
Unknown protocols                 0
```

COMMAND: *netstat -o*

```
PS C:\Windows\System32> netstat -o

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    127.0.0.1:49350        PROFESSOR:53370        CLOSE_WAIT      11936
  TCP    127.0.0.1:52357        PROFESSOR:52358        ESTABLISHED     13604
  TCP    127.0.0.1:52358        PROFESSOR:52357        ESTABLISHED     13604
  TCP    127.0.0.1:52362        PROFESSOR:52363        ESTABLISHED     20936
  TCP    127.0.0.1:52363        PROFESSOR:52362        ESTABLISHED     20936
  TCP    127.0.0.1:53328        PROFESSOR:49350        TIME_WAIT       0
  TCP    127.0.0.1:53329        PROFESSOR:49350        TIME_WAIT       0
  TCP    127.0.0.1:53330        PROFESSOR:49350        TIME_WAIT       0
  TCP    127.0.0.1:53331        PROFESSOR:49350        TIME_WAIT       0
  TCP    127.0.0.1:53332        PROFESSOR:49350        TIME_WAIT       0
  TCP    127.0.0.1:53333        PROFESSOR:49350        TIME_WAIT       0
  TCP    127.0.0.1:53334        PROFESSOR:49350        TIME_WAIT       0
  TCP    127.0.0.1:53335        PROFESSOR:49350        TIME_WAIT       0
  TCP    127.0.0.1:53336        PROFESSOR:49350        TIME_WAIT       0
  TCP    127.0.0.1:53337        PROFESSOR:49350        TIME_WAIT       0
  TCP    127.0.0.1:53338        PROFESSOR:49350        TIME_WAIT       0
  TCP    127.0.0.1:53339        PROFESSOR:49350        TIME_WAIT       0
  TCP    127.0.0.1:53340        PROFESSOR:49350        TIME_WAIT       0
  TCP    127.0.0.1:53344        PROFESSOR:49350        TIME_WAIT       0
  TCP    127.0.0.1:53347        PROFESSOR:49350        TIME_WAIT       0
  TCP    127.0.0.1:53349        PROFESSOR:49350        TIME_WAIT       0
  TCP    127.0.0.1:53350        PROFESSOR:49350        TIME_WAIT       0
  TCP    127.0.0.1:53351        PROFESSOR:49350        TIME_WAIT       0
```

COMMAND: *netstat -p tcp*

```
PS C:\Windows\System32> netstat -p tcp

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49350        PROFESSOR:53450        CLOSE_WAIT
  TCP    127.0.0.1:52357        PROFESSOR:52358        ESTABLISHED
  TCP    127.0.0.1:52358        PROFESSOR:52357        ESTABLISHED
  TCP    127.0.0.1:52362        PROFESSOR:52363        ESTABLISHED
  TCP    127.0.0.1:52363        PROFESSOR:52362        ESTABLISHED
  TCP    127.0.0.1:53418        PROFESSOR:49350        TIME_WAIT
  TCP    127.0.0.1:53419        PROFESSOR:49350        TIME_WAIT
  TCP    127.0.0.1:53420        PROFESSOR:49350        TIME_WAIT
  TCP    127.0.0.1:53421        PROFESSOR:49350        TIME_WAIT
  TCP    127.0.0.1:53422        PROFESSOR:49350        TIME_WAIT
  TCP    127.0.0.1:53423        PROFESSOR:49350        TIME_WAIT
  TCP    127.0.0.1:53424        PROFESSOR:49350        TIME_WAIT
  TCP    127.0.0.1:53425        PROFESSOR:49350        TIME_WAIT
```

COMMAND: *netstat -s*

```
PS C:\Windows\System32> netstat -s

IPv4 Statistics

  Packets Received                    = 746645
  Received Header Errors              = 0
  Received Address Errors             = 2
  Datagrams Forwarded                 = 0
  Unknown Protocols Received          = 0
  Received Packets Discarded          = 814
  Received Packets Delivered          = 746991
  Output Requests                     = 281266
  Routing Discards                    = 0
  Discarded Output Packets            = 34
  Output Packet No Route              = 0
  Reassembly Required                 = 0
  Reassembly Successful               = 0
  Reassembly Failures                 = 0
  Datagrams Successfully Fragmented   = 0
  Datagrams Failing Fragmentation     = 0
  Fragments Created                   = 0
```

```
IPv6 Statistics

  Packets Received                    = 0
  Received Header Errors              = 0
  Received Address Errors             = 0
  Datagrams Forwarded                 = 0
  Unknown Protocols Received          = 0
  Received Packets Discarded          = 0
  Received Packets Delivered          = 36
  Output Requests                     = 44
  Routing Discards                    = 0
  Discarded Output Packets            = 0
  Output Packet No Route              = 0
  Reassembly Required                 = 0
  Reassembly Successful               = 0
  Reassembly Failures                 = 0
  Datagrams Successfully Fragmented   = 0
  Datagrams Failing Fragmentation     = 0
  Fragments Created                   = 0
```

```
ICMPv4 Statistics

                              Received    Sent
  Messages                    392         307
  Errors                      0           0
  Destination Unreachable     391         306
  Time Exceeded               0           0
  Parameter Problems          0           0
  Source Quenches             0           0
  Redirects                   0           0
  Echo Replies                1           0
  Echos                       0           1
  Timestamps                  0           0
  Timestamp Replies           0           0
  Address Masks               0           0
  Address Mask Replies        0           0
  Router Solicitations        0           0
  Router Advertisements       0           0
```

```
TCP Statistics for IPv6

  Active Opens                            = 8
  Passive Opens                           = 0
  Failed Connection Attempts              = 385
  Reset Connections                       = 0
  Current Connections                     = 0
  Segments Received                       = 72
  Segments Sent                           = 44
  Segments Retransmitted                  = 28

UDP Statistics for IPv4

  Datagrams Received    = 16784
  No Ports              = 525
  Receive Errors        = 1
  Datagrams Sent        = 6078

UDP Statistics for IPv6

  Datagrams Received    = 2
  No Ports              = 0
  Receive Errors        = 0
  Datagrams Sent        = 2
```

COMMAND: *netstat -r*

```
===========================================================================
Interface List
 20...e4 a8 df c1 6a 14 ......Realtek PCIe GbE Family Controller
  9...b0 3c dc b3 cd 43 ......Microsoft Wi-Fi Direct Virtual Adapter #3
 22...b2 3c dc b3 cd 42 ......Microsoft Wi-Fi Direct Virtual Adapter #4
 16...52 97 60 ba da 43 ......Intel(R) Wi-Fi 6 AX201 160MHz
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1     192.168.1.11     50
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      192.168.1.0    255.255.255.0         On-link      192.168.1.11    306
     192.168.1.11  255.255.255.255         On-link      192.168.1.11    306
    192.168.1.255  255.255.255.255         On-link      192.168.1.11    306
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      192.168.1.11    306
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      192.168.1.11    306
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
  1    331 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

PRACTICAL – 2

- **AIM:**
  To monitor and analyse real-time TCP/IP connections on a Windows system using `CurrPorts`.

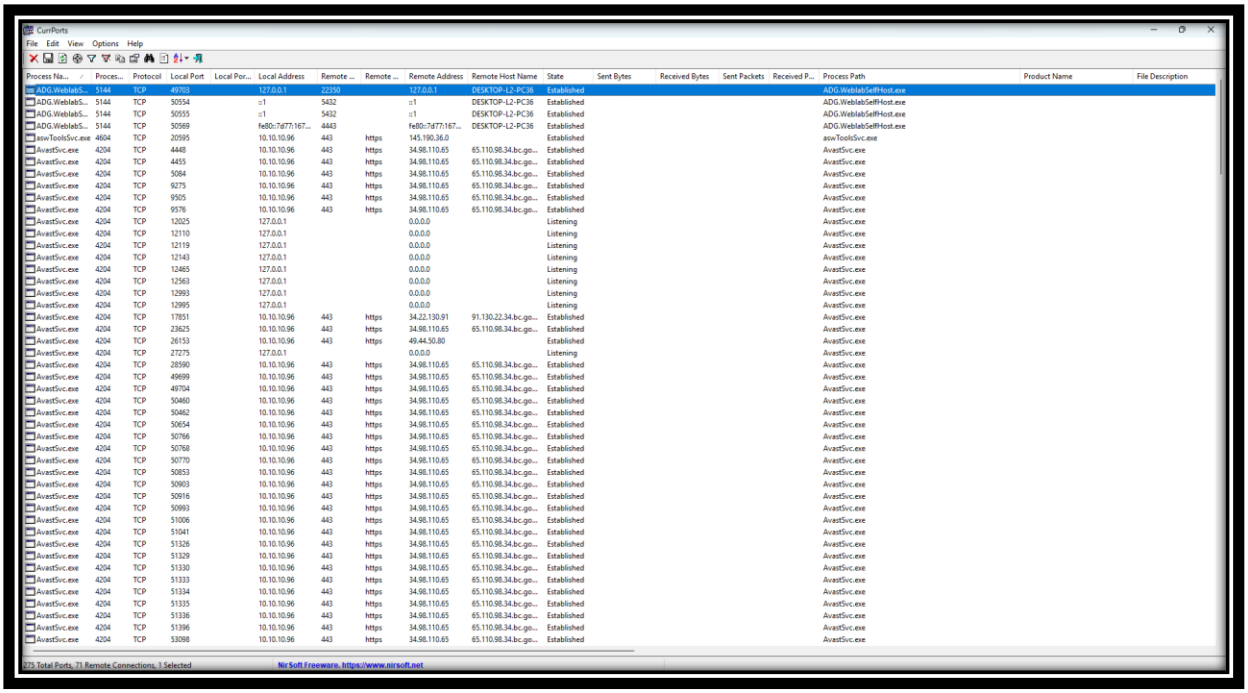
- **TOOLS/APPLICATIONS USED:**
  CurrPorts

- **THEORY:**
  CurrPorts is network monitoring software that displays the list of all currently opened TCP/IP and UDP ports on your local computer. For each port in the list, information about the process that opened the port is also displayed, including the process name, full path of the process, version information of the process (product name, file description, and so on), the time that the process was created, and the user that created it.

- **PROCEDURES:**

  - Download CurrPorts and run it (it's portable — no installation needed).
  - Open the program so you can see the list of currently open TCP & UDP ports, with info like process name, local/remote address and port, state, etc.
  - Use the "Options" or View menu to enable display of listening ports, established connections, and any states you care about (e.g., TIME_WAIT, CLOSE_WAIT).
  - Optionally adjust refresh interval or enable automatic refresh so you can watch changes in real-time.
  - Use filters (include/exclude) to focus on specific processes, ports, or remote IP ranges you want to monitor.
  - Review the list for unusual or unexpected entries: e.g., unknown process names, remote addresses you didn't expect, many connections in odd states. Marked items may be flagged (e.g., pink) if the application is unidentified.
  - If needed, select one or more connections to close them (or the process that opened them) — useful for terminating unwanted/unknown connections.
  - Save or export the current list (to text, HTML, XML) for reporting or further investigation.

- **OUTPUTS:**


CurrPorts
File Edit View Options Help
Process Na... Proces... Protocol Local Port Local Por... Local Address Remote ... Remote ... Remote Address Remote Host Name State Sent Bytes Received Bytes Sent Packets Received P... Process Path Product Name File Description
ADG.WeblabS... 5144 TCP 49703 127.0.0.1 22350 127.0.0.1 DESKTOP-L2-PC36 Established ADG.WeblabSelfHost.exe
ADG.WeblabS... 5144 TCP 50554 ::1 5432 ::1 DESKTOP-L2-PC36 Established ADG.WeblabSelfHost.exe
ADG.WeblabS... 5144 TCP 50555 ::1 5432 ::1 DESKTOP-L2-PC36 Established ADG.WeblabSelfHost.exe
ADG.WeblabS... 5144 TCP 50569 fe80::7d77:167... 4443 fe80::7d77:167... DESKTOP-L2-PC36 Established ADG.WeblabSelfHost.exe
aswToolsSvc.exe 4604 TCP 20595 10.10.10.96 443 https 145.190.36.0 Established aswToolsSvc.exe
AvastSvc.exe 4204 TCP 4448 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 4455 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 5084 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 9275 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 9505 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 9576 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 12025 127.0.0.1 0.0.0.0 Listening AvastSvc.exe
AvastSvc.exe 4204 TCP 12110 127.0.0.1 0.0.0.0 Listening AvastSvc.exe
AvastSvc.exe 4204 TCP 12119 127.0.0.1 0.0.0.0 Listening AvastSvc.exe
AvastSvc.exe 4204 TCP 12143 127.0.0.1 0.0.0.0 Listening AvastSvc.exe
AvastSvc.exe 4204 TCP 12465 127.0.0.1 0.0.0.0 Listening AvastSvc.exe
AvastSvc.exe 4204 TCP 12563 127.0.0.1 0.0.0.0 Listening AvastSvc.exe
AvastSvc.exe 4204 TCP 12993 127.0.0.1 0.0.0.0 Listening AvastSvc.exe
AvastSvc.exe 4204 TCP 12995 127.0.0.1 0.0.0.0 Listening AvastSvc.exe
AvastSvc.exe 4204 TCP 17851 10.10.10.96 443 https 34.22.130.91 91.130.22.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 23625 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 26153 10.10.10.96 443 https 49.44.50.80 Established AvastSvc.exe
AvastSvc.exe 4204 TCP 27275 127.0.0.1 0.0.0.0 Listening AvastSvc.exe
AvastSvc.exe 4204 TCP 28590 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 49699 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 49704 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 50460 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 50462 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 50654 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 50766 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 50768 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 50770 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 50853 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 50903 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 50916 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 50993 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 51006 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 51041 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 51326 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 51329 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 51330 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 51333 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 51334 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 51335 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 51336 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 51396 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
AvastSvc.exe 4204 TCP 53098 10.10.10.96 443 https 34.98.110.65 65.110.98.34.bc.go... Established AvastSvc.exe
275 Total Ports, 71 Remote Connections, 1 Selected
Nir Soft Freeware. https://www.nirsoft.net

PRACTICAL – 3

- **AIM:**
  To monitor and analyse real-time TCP/IP connections on a Windows system using `TCPView`.

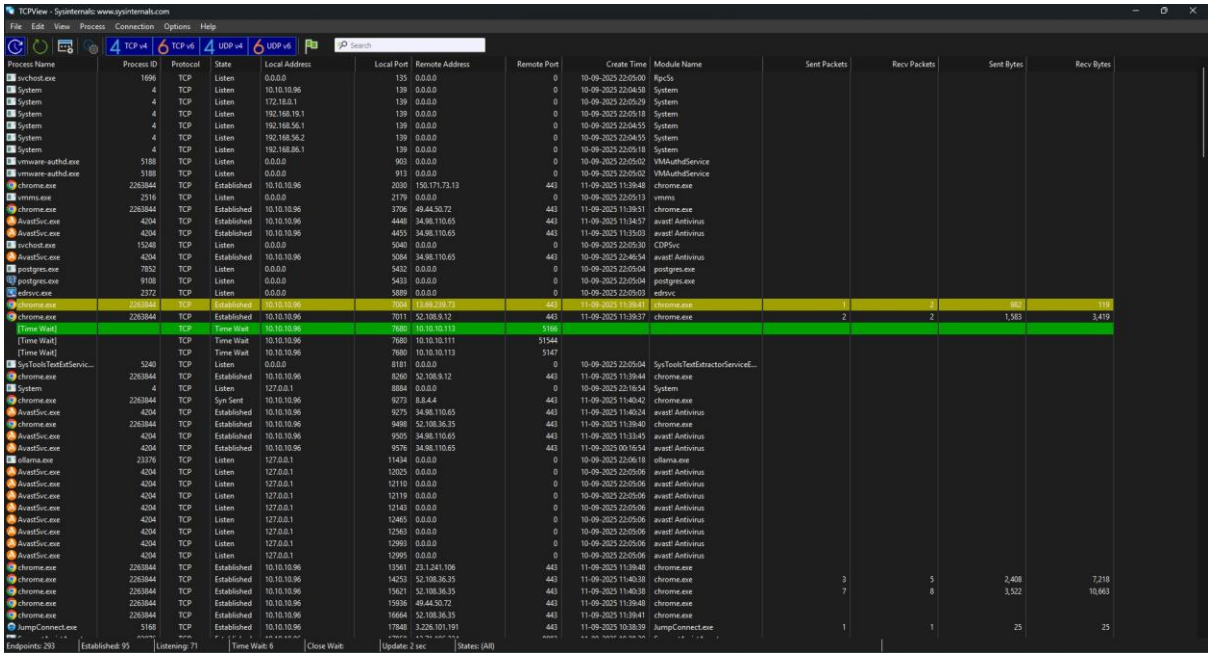
- **TOOLS/APPLICATIONS USED:**
  TCPView

- **THEORY:**
  TCPView is a lightweight and straightforward utility that is part of the venerable Sysinternals Suite, now owned by Microsoft. It is a program that will show detailed listings of all TCP and UDP endpoints on the system, including the local and remote addresses and state of TCP connections. TCPView also reports the name of the process that owns the endpoint. It provides a more informative and conveniently presented subset of the Netstat program that ships with the OS. It's download includes Tcpvcon, a command-line version with the same functionality.

- **PROCEDURES:**

  - Download and launch TCPView.
  - Let it list all active TCP and UDP endpoints (local & remote addresses + owning process).
  - Observe the table: process name, PID, protocol, local/remote address/port, connection state.
  - Watch live updates: new connections shown in green, terminated in red, changed states highlighted.
  - Use filters/search to focus on specific ports, processes or remote addresses of interest.
  - Identify any unexpected or suspicious entries — e.g., unknown process making outbound connections, connections in odd states.
  - If needed, close a connection or terminate its owning process via right-click/context menu.
  - Save/export the view for reporting (to text/HTML) for later analysis.
  - After monitoring, interpret what you observed: normal vs unusual behavior, what the connections imply, and if any action is required.

- **OUTPUT:**


TCPView - Sysinternals: www.sysinternals.com
File Edit View Process Connection Options Help
TCP v4 TCP v6 UDP v4 UDP v6
Process Name Process ID Protocol State Local Address Local Port Remote Address Remote Port Create Time Module Name Sent Packets Recv Packets Sent Bytes Recv Bytes
svchost.exe 1696 TCP Listen 0.0.0.0 135 0.0.0.0 0 10-09-2025 22:05:00 RpcSs
System 4 TCP Listen 10.10.10.96 139 0.0.0.0 0 10-09-2025 22:04:58 System
System 4 TCP Listen 172.18.0.1 139 0.0.0.0 0 10-09-2025 22:05:29 System
System 4 TCP Listen 192.168.19.1 139 0.0.0.0 0 10-09-2025 22:05:18 System
System 4 TCP Listen 192.168.56.1 139 0.0.0.0 0 10-09-2025 22:04:55 System
System 4 TCP Listen 192.168.56.2 139 0.0.0.0 0 10-09-2025 22:04:55 System
System 4 TCP Listen 192.168.86.1 139 0.0.0.0 0 10-09-2025 22:05:18 System
vmware-authd.exe 5188 TCP Listen 0.0.0.0 903 0.0.0.0 0 10-09-2025 22:05:02 VMAuthdService
vmware-authd.exe 5188 TCP Listen 0.0.0.0 913 0.0.0.0 0 10-09-2025 22:05:02 VMAuthdService
chrome.exe 2263844 TCP Established 10.10.10.96 2030 150.171.73.13 443 11-09-2025 11:39:48 chrome.exe
vmms.exe 2516 TCP Listen 0.0.0.0 2179 0.0.0.0 0 10-09-2025 22:05:13 vmms
chrome.exe 2263844 TCP Established 10.10.10.96 3706 49.44.50.72 443 11-09-2025 11:39:51 chrome.exe
AvastSvc.exe 4204 TCP Established 10.10.10.96 4448 34.98.110.65 443 11-09-2025 11:34:57 avast! Antivirus
AvastSvc.exe 4204 TCP Established 10.10.10.96 4455 34.98.110.65 443 11-09-2025 11:35:03 avast! Antivirus
svchost.exe 15248 TCP Listen 0.0.0.0 5040 0.0.0.0 0 10-09-2025 22:05:30 CDPSvc
AvastSvc.exe 4204 TCP Established 10.10.10.96 5084 34.98.110.65 443 10-09-2025 22:46:54 avast! Antivirus
postgres.exe 7852 TCP Listen 0.0.0.0 5432 0.0.0.0 0 10-09-2025 22:05:04 postgres.exe
postgres.exe 9108 TCP Listen 0.0.0.0 5433 0.0.0.0 0 10-09-2025 22:05:04 postgres.exe
edrsvc.exe 2372 TCP Listen 0.0.0.0 5889 0.0.0.0 0 10-09-2025 22:05:03 edrsvc
chrome.exe 2263844 TCP Established 10.10.10.96 7004 13.69.239.73 443 11-09-2025 11:39:41 chrome.exe 1 2 982 118
chrome.exe 2263844 TCP Established 10.10.10.96 7011 52.108.9.12 443 11-09-2025 11:39:37 chrome.exe 2 2 1,583 3,419
[Time Wait] TCP Time Wait 10.10.10.96 7680 10.10.10.113 5166
[Time Wait] TCP Time Wait 10.10.10.96 7680 10.10.10.111 51544
[Time Wait] TCP Time Wait 10.10.10.96 7680 10.10.10.113 5147
SysToolsTextEstServic... 5240 TCP Listen 0.0.0.0 8181 0.0.0.0 0 10-09-2025 22:05:04 SysToolsTextExtractorServiceE...
chrome.exe 2263844 TCP Established 10.10.10.96 8260 52.108.9.12 443 11-09-2025 11:39:44 chrome.exe
System 4 TCP Listen 127.0.0.1 8884 0.0.0.0 0 10-09-2025 22:16:54 System
chrome.exe 2263844 TCP Syn Sent 10.10.10.96 9273 8.8.4.4 443 11-09-2025 11:40:42 chrome.exe
AvastSvc.exe 4204 TCP Established 10.10.10.96 9275 34.98.110.65 443 11-09-2025 11:40:24 avast! Antivirus
chrome.exe 2263844 TCP Established 10.10.10.96 9498 52.108.36.35 443 11-09-2025 11:39:40 chrome.exe
AvastSvc.exe 4204 TCP Established 10.10.10.96 9505 34.98.110.65 443 11-09-2025 11:33:45 avast! Antivirus
AvastSvc.exe 4204 TCP Established 10.10.10.96 9576 34.98.110.65 443 11-09-2025 00:16:54 avast! Antivirus
ollama.exe 23376 TCP Listen 127.0.0.1 11434 0.0.0.0 0 10-09-2025 22:06:18 ollama.exe
AvastSvc.exe 4204 TCP Listen 127.0.0.1 12025 0.0.0.0 0 10-09-2025 22:05:06 avast! Antivirus
AvastSvc.exe 4204 TCP Listen 127.0.0.1 12110 0.0.0.0 0 10-09-2025 22:05:06 avast! Antivirus
AvastSvc.exe 4204 TCP Listen 127.0.0.1 12119 0.0.0.0 0 10-09-2025 22:05:06 avast! Antivirus
AvastSvc.exe 4204 TCP Listen 127.0.0.1 12143 0.0.0.0 0 10-09-2025 22:05:06 avast! Antivirus
AvastSvc.exe 4204 TCP Listen 127.0.0.1 12465 0.0.0.0 0 10-09-2025 22:05:06 avast! Antivirus
AvastSvc.exe 4204 TCP Listen 127.0.0.1 12563 0.0.0.0 0 10-09-2025 22:05:06 avast! Antivirus
AvastSvc.exe 4204 TCP Listen 127.0.0.1 12993 0.0.0.0 0 10-09-2025 22:05:06 avast! Antivirus
AvastSvc.exe 4204 TCP Listen 127.0.0.1 12995 0.0.0.0 0 10-09-2025 22:05:06 avast! Antivirus
chrome.exe 2263844 TCP Established 10.10.10.96 13561 23.1.241.106 443 11-09-2025 11:39:48 chrome.exe
chrome.exe 2263844 TCP Established 10.10.10.96 14253 52.108.36.35 443 11-09-2025 11:40:38 chrome.exe 3 5 2,408 7,218
chrome.exe 2263844 TCP Established 10.10.10.96 15621 52.108.36.35 443 11-09-2025 11:40:38 chrome.exe 7 8 3,522 10,663
chrome.exe 2263844 TCP Established 10.10.10.96 15936 49.44.50.72 443 11-09-2025 11:39:48 chrome.exe
chrome.exe 2263844 TCP Established 10.10.10.96 16664 52.108.36.35 443 11-09-2025 11:39:41 chrome.exe
JumpConnect.exe 5168 TCP Established 10.10.10.96 17848 3.226.101.191 443 11-09-2025 10:38:39 JumpConnect.exe 1 1 25 25
Endpoints: 293 Established: 95 Listening: 71 Time Wait: 6 Close Wait: Update: 2 sec States: (All)

PRACTICAL – 4

- **AIM:**
  To create a disk image (.DD format) via `FTK imager`, do its analysis using `Autopsy` and generate the report.

- **TOOLS/APPLICATIONS USED:**
  - FTK Imager
  - Autopsy

- **THEORY:**
  FTK Imager is a forensic-imaging and preview tool developed by AccessData (now under Exterro) that lets investigators create bit-for-bit copies (images) of storage media (hard drives, external drives, USBs) and capture volatile memory in some cases.

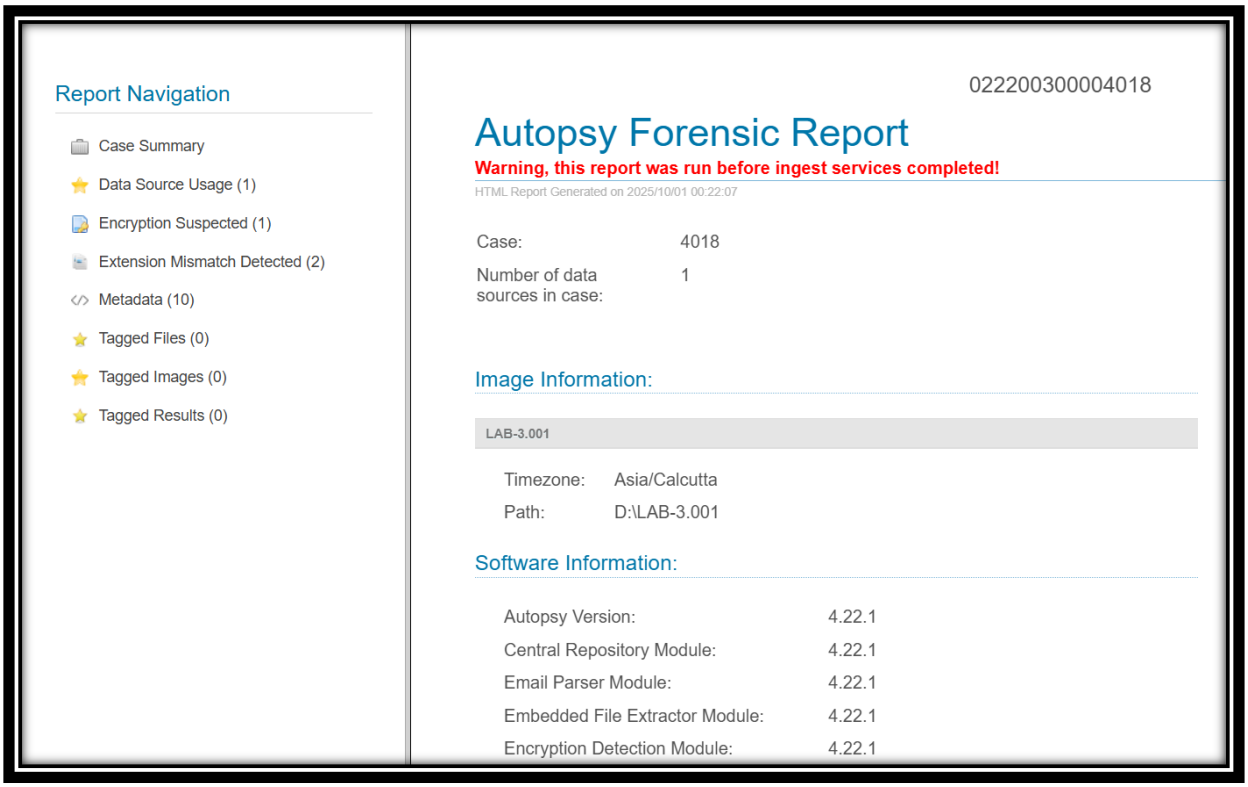
  Autopsy is an open-source, graphical digital forensics platform built on top of The Sleuth Kit (TSK) that provides investigators a UI to analyse disk images, file systems, recover deleted files, perform timeline analysis, keyword search, web artefact extraction, etc.

- **PROCEDURES:**

  - Prepare your forensic workstation and ensure you have write-blocking enabled on the source drive (so you don't alter the original evidence).
  - Launch FTK Imager.
  - In FTK Imager: select **File** → **Create Disk Image**.
  - Choose the source evidence type (e.g., Physical Drive) and select the correct drive you want to image.
  - Choose the image destination: select destination folder, filename, and importantly select the "Raw (dd)" / ".DD" / "Raw image" format in the image type drop-down.
  - Enter case information or metadata (case number, examiner name, description) if required (helps documentation).
  - Optional but recommended: check the "Verify images after they are created" or similar verification/hash option. This generates hash values (MD5/SHA1) of the image to confirm integrity.
  - Click Start (or finish as prompted) and wait for the imaging process to complete. The tool will produce the raw image - .DD (or .001/.002 segments if fragmented) and the log/hash report.
  - Once completed, confirm the hash values match, and note the image filename, size, destination path, hash values and tool version for your documentation.

- Launch Autopsy.
- Create a new case: provide case name, base directory, etc.
- Add your data source: choose “Disk Image or VM File” and browse to your .DD image file you created earlier.
- Configure the ingest modules: select which modules (e.g., file type identification, keyword search, recent activity, hash lookup) to run.
- Run the ingest/analysis process: Autopsy will process the image, parse file systems, recover deleted files, carve unallocated space, build timelines, etc.
- Browse the results: review artefacts such as user files, system logs, browser history, email, USB device history, deleted files, timeline of events.
- Perform searches/filters as needed: keyword search, filter by file type, time ranges, hash matches, etc.
- Tag relevant items/artefacts: mark items of interest (evidence), add notes or bookmarks for reporting.
- Generate the report: use Autopsy’s report generation feature (export in HTML/PDF format) summarizing case metadata, evidence sources, findings, tagged artefacts, summary of results.

- **OUTPUT:**



Report Navigation

- Case Summary
- Data Source Usage (1)
- Encryption Suspected (1)
- Extension Mismatch Detected (2)
- Metadata (10)
- Tagged Files (0)
- Tagged Images (0)
- Tagged Results (0)

Extension Mismatch Detector Module:	4.22.1
File Type Identification Module:	4.22.1
Hash Lookup Module:	4.22.1
Interesting Files Identifier Module:	4.22.1
Keyword Search Module:	4.22.1
Picture Analyzer Module:	4.22.1
Recent Activity Module:	4.22.1

Ingest History:

Job 1:

Data Source:	LAB-3.001
Status:	STARTED
Enabled Modules:	Recent Activity Hash Lookup File Type Identification Extension Mismatch Detector Embedded File Extractor Picture Analyzer Keyword Search Email Parser Encryption Detection Interesting Files Identifier Central Repository

Report Navigation

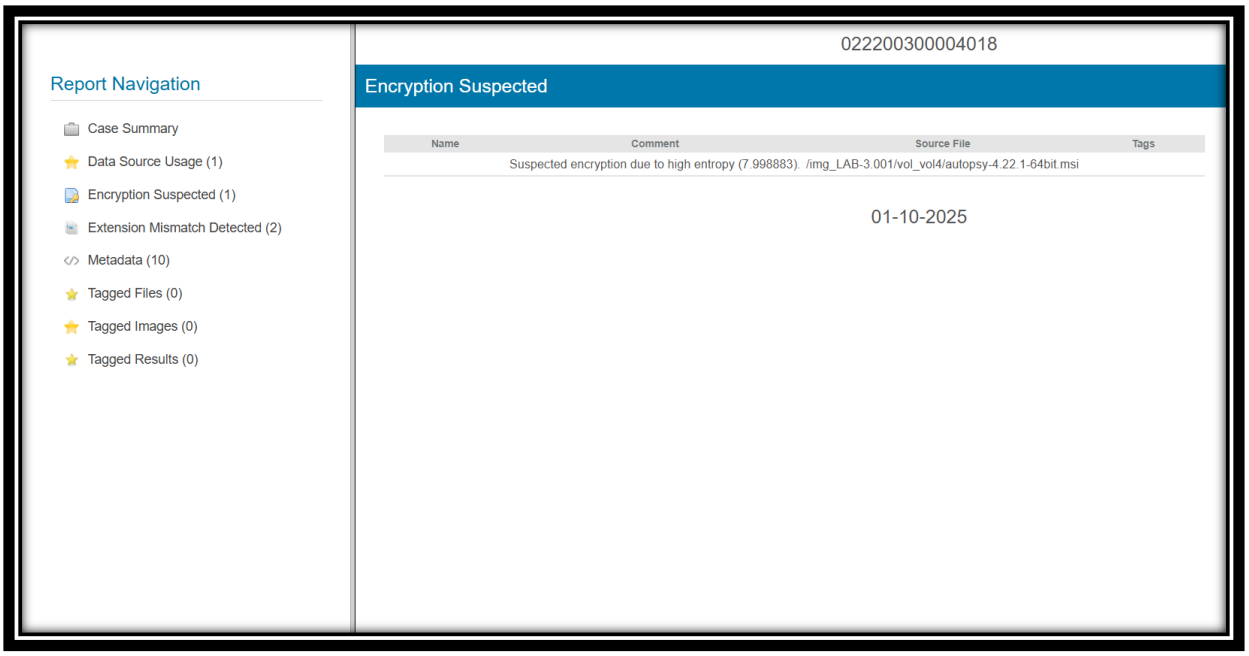
- Case Summary
- Data Source Usage (1)
- Encryption Suspected (1)
- Extension Mismatch Detected (2)
- Metadata (10)
- Tagged Files (0)
- Tagged Images (0)
- Tagged Results (0)

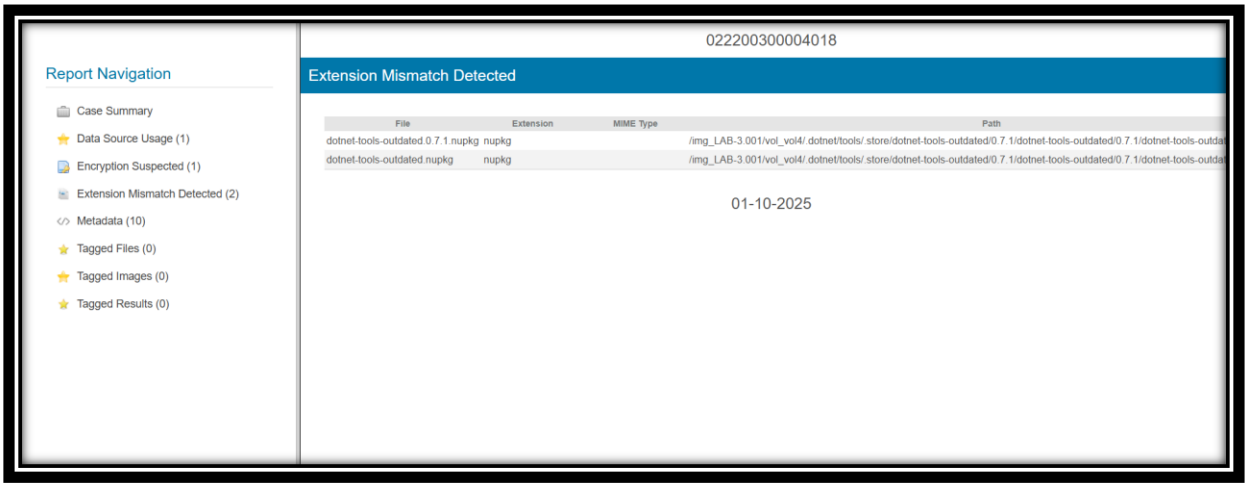
022200300004018

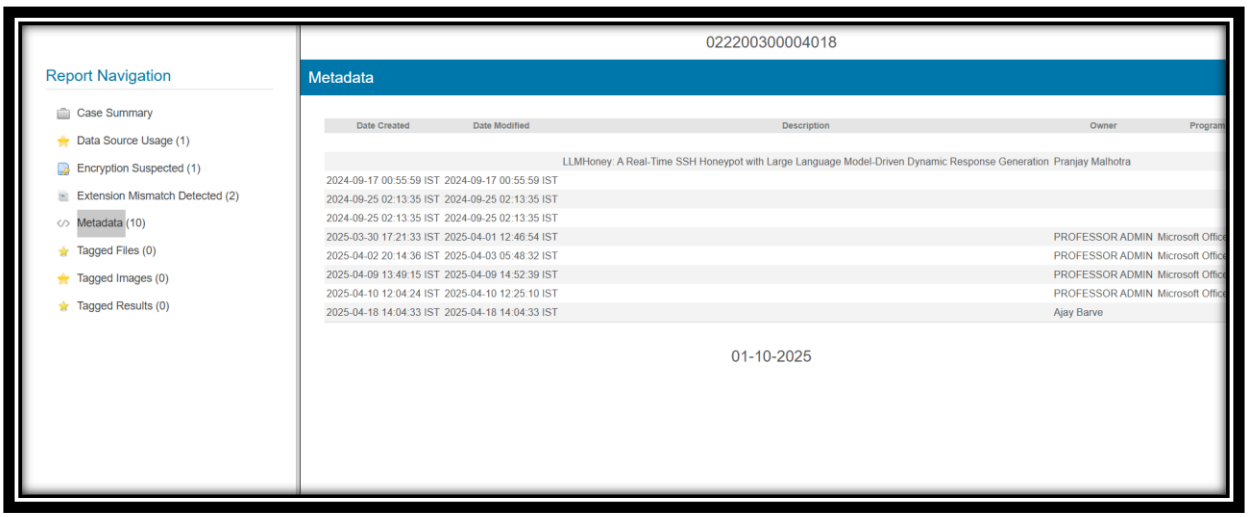
Data Source Usage

Description	Source File	Tags
Flash Drive	/img_LAB-3.001	

01-10-2025


Report Navigation
Case Summary
Data Source Usage (1)
Encryption Suspected (1)
Extension Mismatch Detected (2)
Metadata (10)
Tagged Files (0)
Tagged Images (0)
Tagged Results (0)
022200300004018
Encryption Suspected
Name
Comment
Source File
Tags
Suspected encryption due to high entropy (7.998883). /img_LAB-3.001/vol_vol4/autopsy-4.22.1-64bit.msi
01-10-2025


Report Navigation
Case Summary
Data Source Usage (1)
Encryption Suspected (1)
Extension Mismatch Detected (2)
Metadata (10)
Tagged Files (0)
Tagged Images (0)
Tagged Results (0)
022200300004018
Extension Mismatch Detected
File
Extension
MIME Type
Path
dotnet-tools-outdated.0.7.1.nupkg nupkg
/img_LAB-3.001/vol_vol4/.dotnet/tools/.store/dotnet-tools-outdated/0.7.1/dotnet-tools-outdated/0.7.1/dotnet-tools-outda
dotnet-tools-outdated.nupkg nupkg
/img_LAB-3.001/vol_vol4/.dotnet/tools/.store/dotnet-tools-outdated/0.7.1/dotnet-tools-outdated/0.7.1/dotnet-tools-outda
01-10-2025


Report Navigation
Case Summary
Data Source Usage (1)
Encryption Suspected (1)
Extension Mismatch Detected (2)
Metadata (10)
Tagged Files (0)
Tagged Images (0)
Tagged Results (0)
022200300004018
Metadata
Date Created
Date Modified
Description
Owner
Program
LLMHoney: A Real-Time SSH Honeypot with Large Language Model-Driven Dynamic Response Generation Pranjay Malhotra
2024-09-17 00:55:59 IST 2024-09-17 00:55:59 IST
2024-09-25 02:13:35 IST 2024-09-25 02:13:35 IST
2024-09-25 02:13:35 IST 2024-09-25 02:13:35 IST
2025-03-30 17:21:33 IST 2025-04-01 12:46:54 IST
PROFESSOR ADMIN Microsoft Offic
2025-04-02 20:14:36 IST 2025-04-03 05:48:32 IST
PROFESSOR ADMIN Microsoft Offic
2025-04-09 13:49:15 IST 2025-04-09 14:52:39 IST
PROFESSOR ADMIN Microsoft Offic
2025-04-10 12:04:24 IST 2025-04-10 12:25:10 IST
PROFESSOR ADMIN Microsoft Offic
2025-04-18 14:04:33 IST 2025-04-18 14:04:33 IST
Ajay Barve
01-10-2025

PRACTICAL – 5

- **AIM:**
  Using Wireshark analyse and filter the TCP (SYN, ACK, Packet transmissions) details.

- **TOOLS/APPLICATIONS USED:**
  - Wireshark

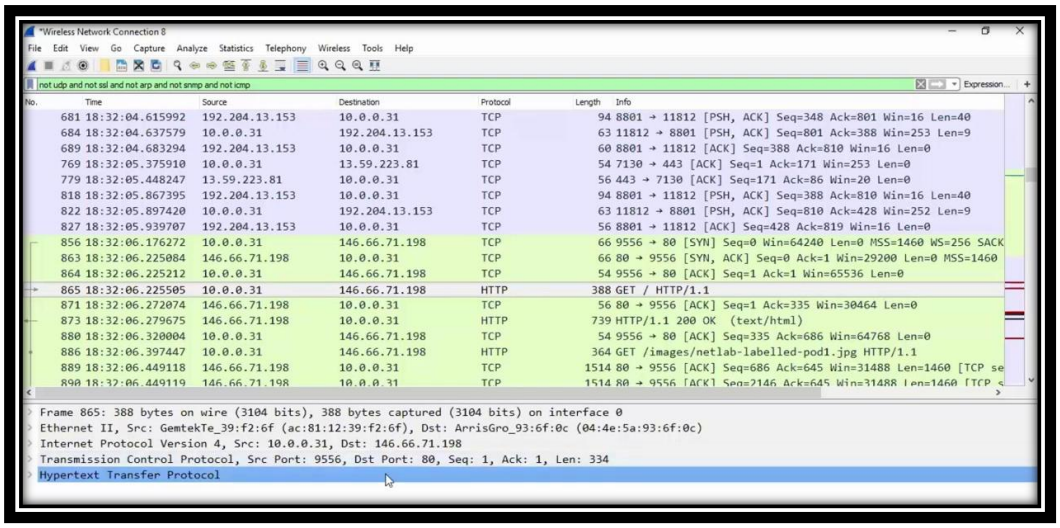
- **THEORY:**
  Wireshark is a powerful, open-source network protocol analyzer that allows users to capture and interactively browse the traffic running on a computer network, providing deep inspection of hundreds of protocols.

  Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible.

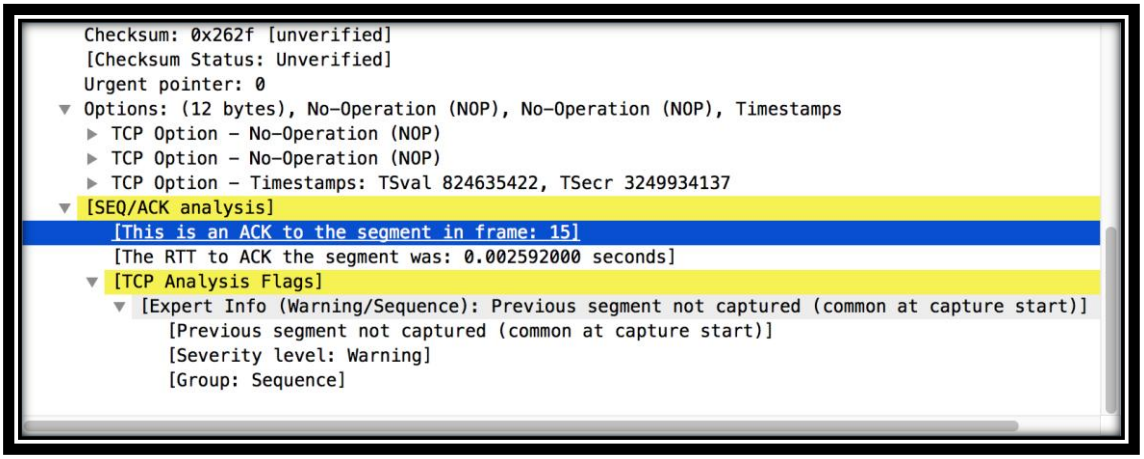
- **PROCEDURES:**
  - Open Wireshark and select the network interface through which traffic will be captured.
  - Start the packet capture on that interface.
  - Initiate a TCP connection (for example by opening a website or connecting to a service).
  - After the connection is established, stop the capture.
  - Apply a filter to display only TCP-related packets.
  - Locate and inspect the first three TCP packets of the conversation (SYN from client, SYN+ACK from server, ACK from client) to verify the handshake.
  - Examine subsequent packets in the TCP stream for sequence numbers, acknowledgment numbers, payload length and any anomalies (e.g., retransmissions).
  - Use the “Follow TCP Stream” feature (or equivalent) to view the entire conversation context.
  - Save the capture file and export relevant packet details, screenshots or summaries for your report.
  - In your report: note the interface used, start/stop times, key handshake packet details, any unusual findings in the TCP transmissions and your interpretation of what that indicates about the connection.

- **OUTPUT:**

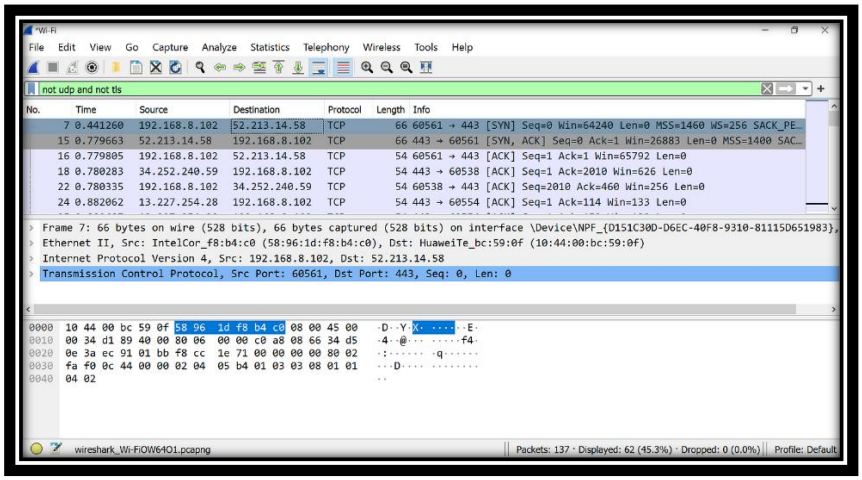
TCP -> SYN



TCP -> SYN/ACK



TCP -> ACK



PRACTICAL – 6

- **AIM:**
  Using Wireshark analyse and filter the HTTP `get` method.

- **TOOLS/APPLICATIONS USED:**
  - Wireshark

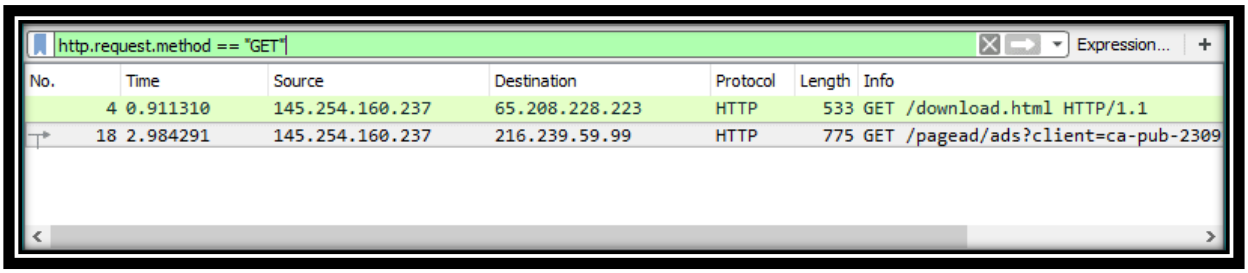
- **THEORY:**
  Wireshark is a powerful, open-source network protocol analyzer that allows users to capture and interactively browse the traffic running on a computer network, providing deep inspection of hundreds of protocols.

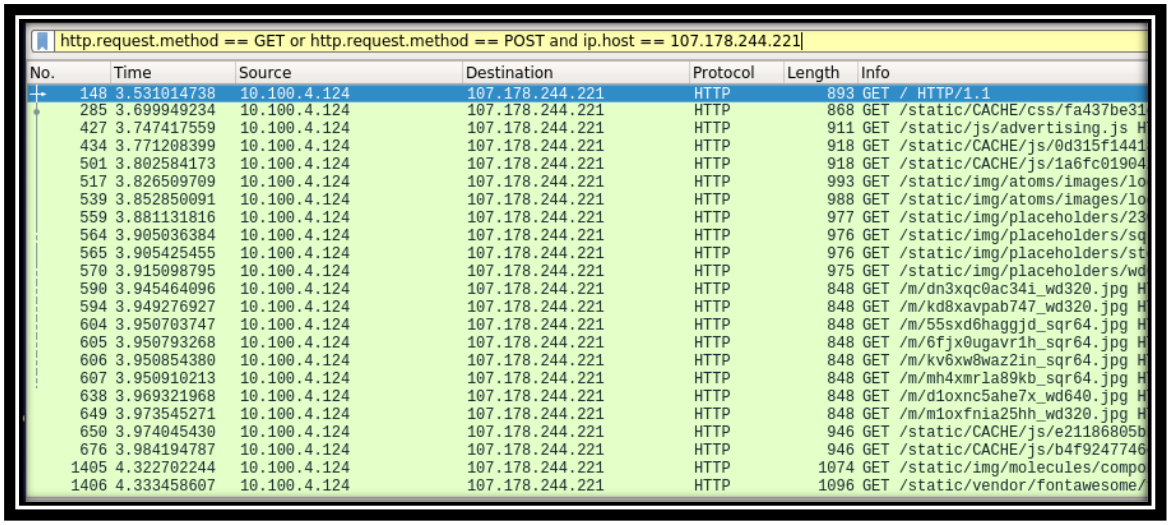
  Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible.

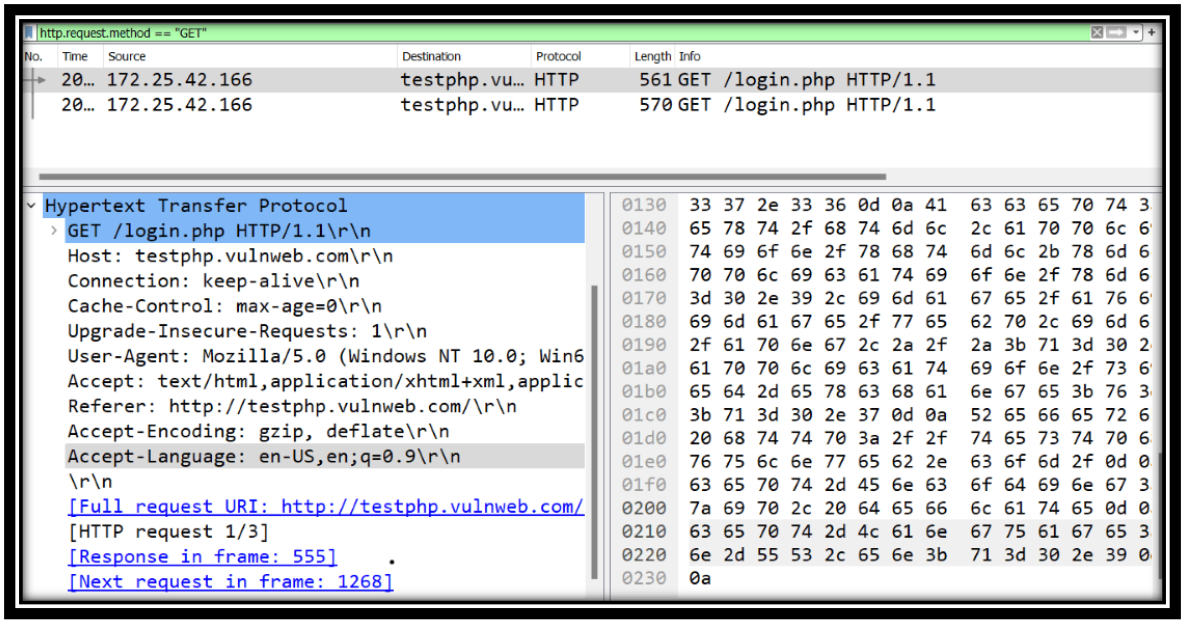
- **PROCEDURES:**
  - Launch Wireshark and select the network interface to capture.
  - Start the packet capture and then trigger a simple HTTP GET (for example, open a webpage).
  - Stop the capture once the request and response are captured.
  - Apply a filter to only show HTTP traffic (so you focus on GET requests).
  - In the packet list, locate the GET request packet from the client to the server.
  - Expand its details: check the HTTP method, requested URL, headers, and payload length.
  - Locate the corresponding HTTP response packet from server to client: check status code, headers, data size.
  - Optionally follow the TCP stream to view the full request-response conversation.

- **OUTPUT:**

HTTP METHOD `GET`







PRACTICAL – 7

- **AIM:**
  Using Wireshark analyse and filter the HTTP `post` method.

- **TOOLS/APPLICATIONS USED:**
  - Wireshark

- **THEORY:**
  Wireshark is a powerful, open-source network protocol analyzer that allows users to capture and interactively browse the traffic running on a computer network, providing deep inspection of hundreds of protocols.

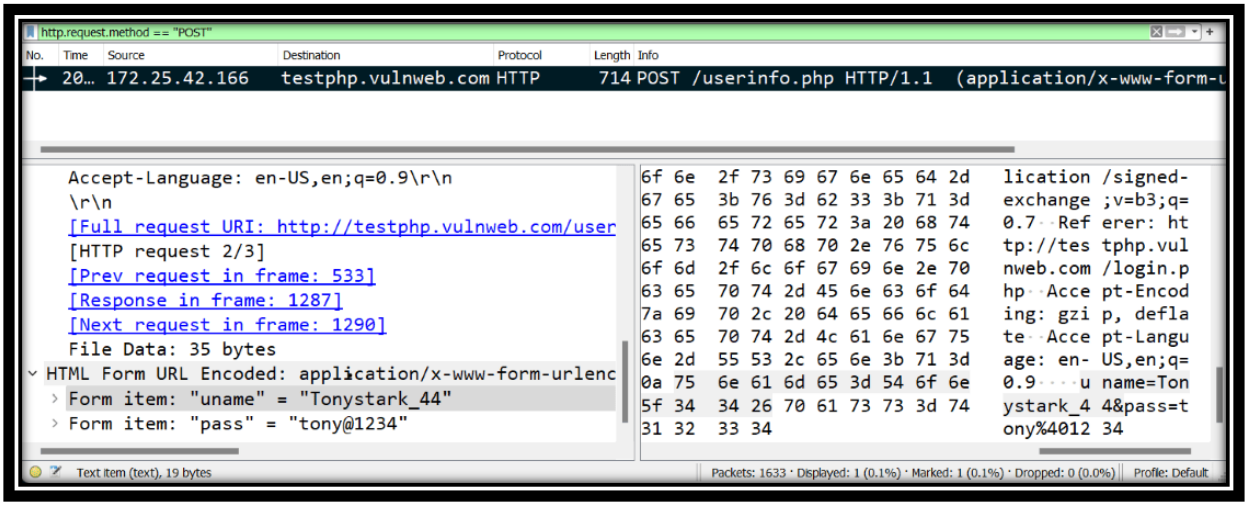
  Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible.

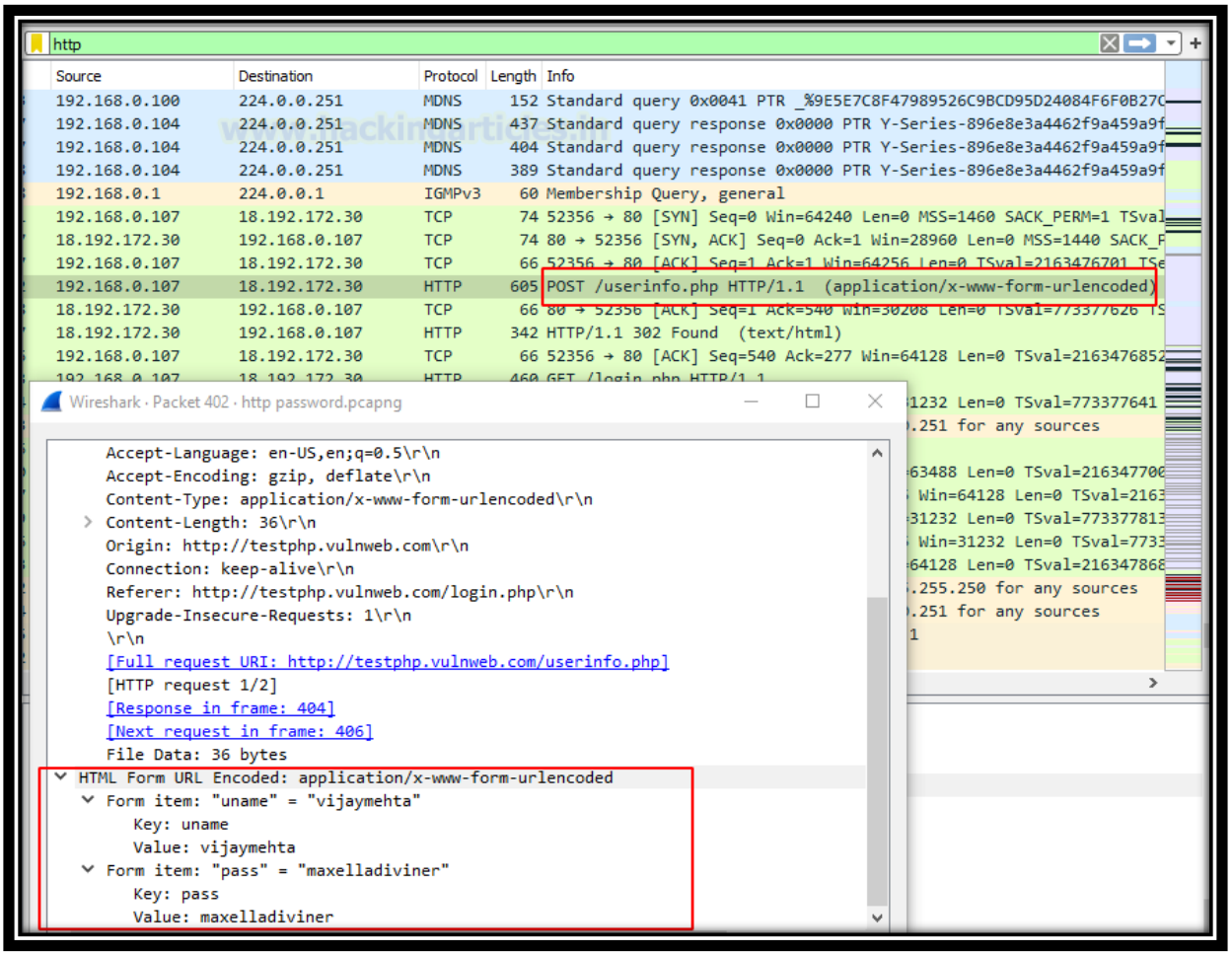
- **PROCEDURES:**

  - Launch Wireshark and select the network interface to capture.
  - Start capturing packets.
  - Trigger a HTTP POST transaction (for example submit a form or an API request).
  - Stop the capture once the request and server response are present.
  - Apply a filter to show only HTTP traffic (so you isolate POST requests).
  - In the packet list, locate the POST request from client to server. Expand details: check HTTP method, URL, headers, payload length.
  - Locate the corresponding HTTP response from server to client: check status code, headers, data size.

- **OUTPUT:**

HTTP METHOD `POST`





PRACTICAL – 8

- **AIM:**
  Using `Nmap` to discover, scan, IP, ports, services, OS, versions etc.

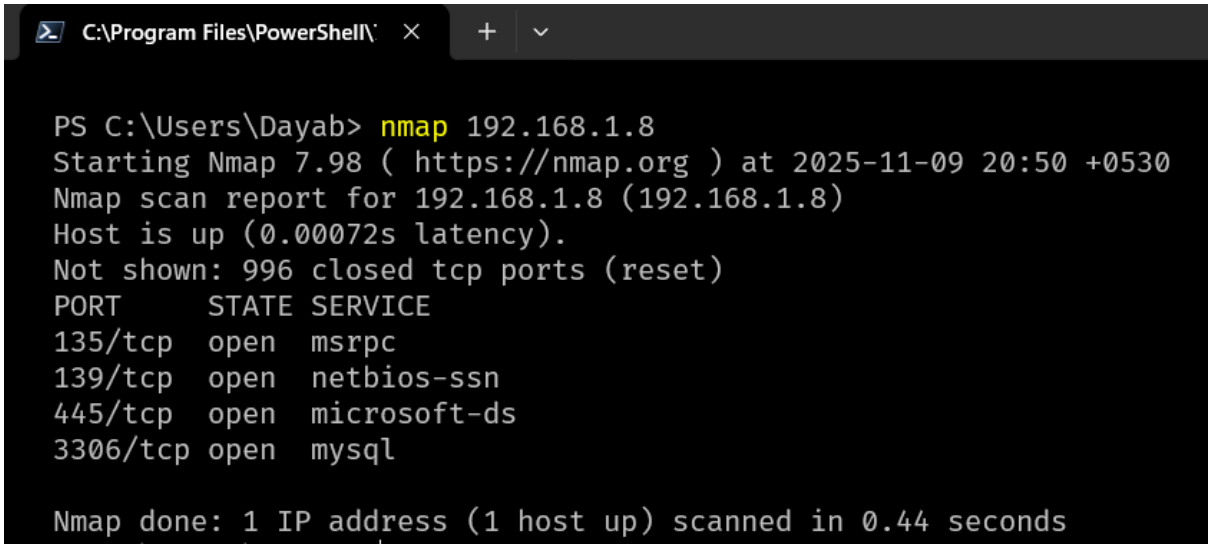
- **TOOLS/APPLICATIONS USED:**
  - Nmap

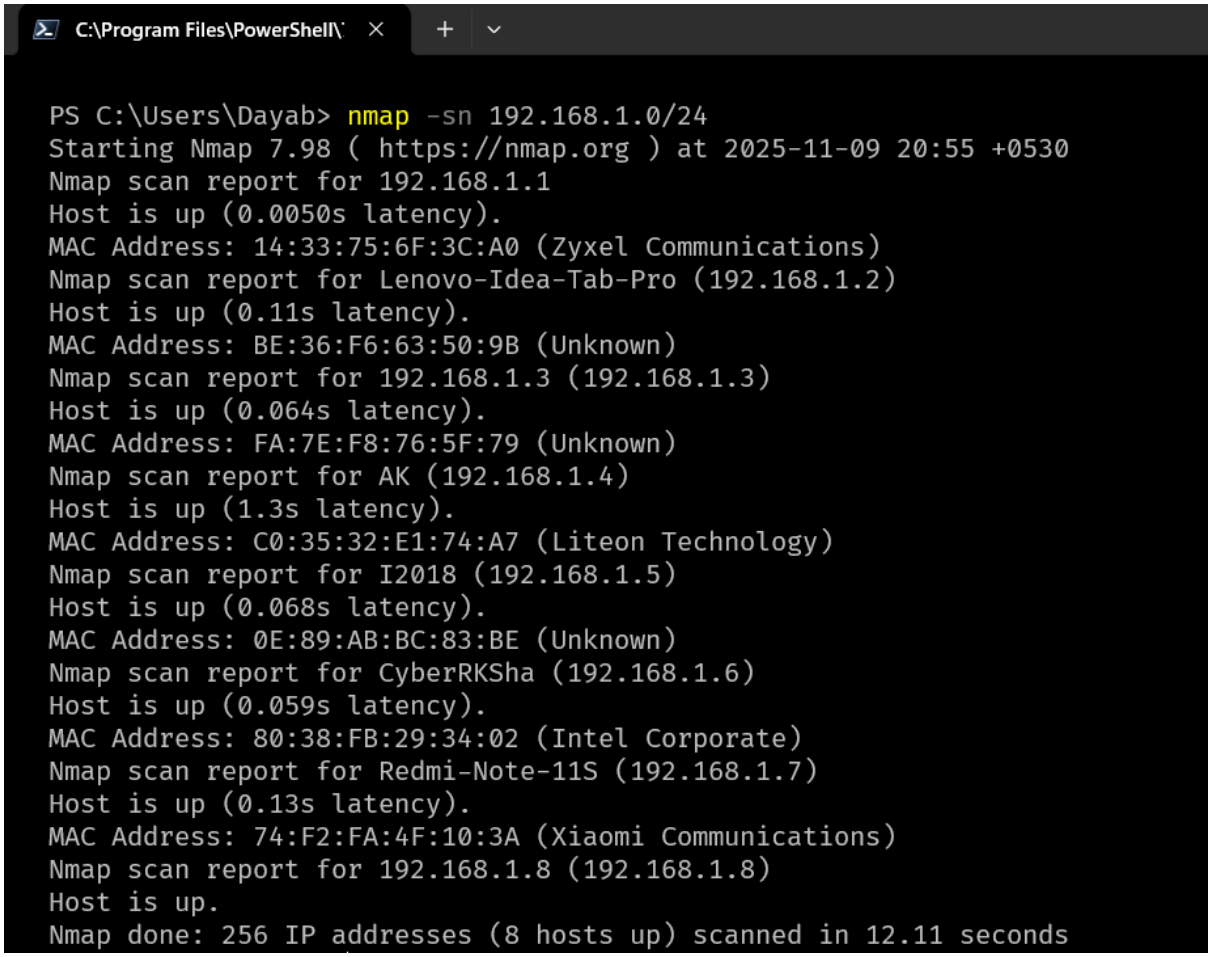
- **THEORY:**
  Nmap ("Network Mapper") is an open-source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

- **PROCEDURES:**

  - Determine the target host (IP address or hostname) you'll scan.
  - Launch Nmap on your scanning machine with appropriate privileges.
  - Perform a basic host/port discovery to see which IPs are up and which ports respond.
  - Once you identify live host(s), perform a port scan to find open/closed/filtered TCP/UDP ports.
  - Enable service/version detection to identify services running on open ports and their versions.
  - Enable OS / device detection to attempt to identify the operating system and device type.
  - Review the scan results: IP address, open ports, service names & versions, OS details, device type.

- **OUTPUT:**


C:\Program Files\PowerShell\
PS C:\Users\Dayab> nmap 192.168.1.8
Starting Nmap 7.98 (https://nmap.org) at 2025-11-09 20:50 +0530
Nmap scan report for 192.168.1.8 (192.168.1.8)
Host is up (0.00072s latency).
Not shown: 996 closed tcp ports (reset)
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3306/tcp open mysql
Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds


C:\Program Files\PowerShell\
PS C:\Users\Dayab> nmap -sn 192.168.1.0/24
Starting Nmap 7.98 (https://nmap.org) at 2025-11-09 20:55 +0530
Nmap scan report for 192.168.1.1
Host is up (0.0050s latency).
MAC Address: 14:33:75:6F:3C:A0 (Zyxel Communications)
Nmap scan report for Lenovo-Idea-Tab-Pro (192.168.1.2)
Host is up (0.11s latency).
MAC Address: BE:36:F6:63:50:9B (Unknown)
Nmap scan report for 192.168.1.3 (192.168.1.3)
Host is up (0.064s latency).
MAC Address: FA:7E:F8:76:5F:79 (Unknown)
Nmap scan report for AK (192.168.1.4)
Host is up (1.3s latency).
MAC Address: C0:35:32:E1:74:A7 (Liteon Technology)
Nmap scan report for I2018 (192.168.1.5)
Host is up (0.068s latency).
MAC Address: 0E:89:AB:BC:83:BE (Unknown)
Nmap scan report for CyberRKSha (192.168.1.6)
Host is up (0.059s latency).
MAC Address: 80:38:FB:29:34:02 (Intel Corporate)
Nmap scan report for Redmi-Note-11S (192.168.1.7)
Host is up (0.13s latency).
MAC Address: 74:F2:FA:4F:10:3A (Xiaomi Communications)
Nmap scan report for 192.168.1.8 (192.168.1.8)
Host is up.
Nmap done: 256 IP addresses (8 hosts up) scanned in 12.11 seconds

```
PS C:\Users\Dayab> nmap -sS -p 1-1024 -T4 microsoft.com
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-09 20:58 +0530
Nmap scan report for microsoft.com (13.107.246.68)
Host is up (0.051s latency).
Other addresses for microsoft.com (not scanned): 13.107.213.68 2603:1030:b:3::152
10:3:3::5b
Not shown: 1022 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 6.47 seconds
```

```
PS C:\Users\Dayab> nmap -O --osscan-guess 192.168.1.8
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-09 21:12 +0530
Nmap scan report for 192.168.1.8 (192.168.1.8)
Host is up (0.00042s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
Aggressive OS guesses: Microsoft Windows 10 1607 - 11 23H2 (99%), Microsoft Windows 10 1511 (97%),
rosoft Windows 10 1703 (96%), Microsoft Windows 10 1703 or Windows 11 21H2 (96%), Microsoft Windows
R1 (94%), Microsoft Windows 11 21H2 (94%), Microsoft Windows 10 1809 - 21H2 (93%)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.98%E=4%D=11/9%OT=135%CT=1%CU=37129%PV=Y%DS=0%DC=L%G=Y%TM=6910B6
OS:55%P=i686-pc-windows-windows)SEQ(SP=100%GCD=1%ISR=10B%TI=I%CI=I%II=I%SS=
OS:S%TS=A)SEQ(SP=101%GCD=1%ISR=106%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=106%GCD=
OS:1%ISR=108%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=107%GCD=1%ISR=106%TI=I%CI=I%II
OS:=I%SS=S%TS=A)SEQ(SP=FE%GCD=1%ISR=10E%TI=I%CI=I%II=I%SS=S%TS=A)OPS(O1=MFF
OS:D7NW8ST11%O2=MFFD7NW8ST11%O3=MFFD7NW8NNT11%O4=MFFD7NW8ST11%O5=MFFD7NW8ST
OS:11%O6=MFFD7ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(
OS:R=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%
OS:W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)
OS:T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A
OS:=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%D
OS:F=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=8
OS:0%CD=Z)

Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.38 seconds
```

```
PS C:\Users\Dayab> nmap -sU -p 53,67,161 google.com
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-09 21:12 +0530
Nmap scan report for google.com (172.217.24.78)
Host is up (0.0090s latency).
Other addresses for google.com (not scanned): 2404:6800:4002:80a::200e
rDNS record for 172.217.24.78: hkg07s33-in-f14.1e100.net

PORT    STATE         SERVICE
53/udp  open|filtered domain
67/udp  open|filtered dhcps
161/udp open|filtered snmp

Nmap done: 1 IP address (1 host up) scanned in 1.61 seconds
```