**Nama : Nanda Hasyim Marfianshar**

**NIM : 09011281520096**

**Kelas : SK5C**

- **Web Browsing**

| Sources | Destination | INFO |
|---|---|---|
| IP address | IP address | |
| fe80::2562:1776:7b01:dbb1 | ff02::1:3 | Standar query 0x78cb A wpad |
| 192.168.137.1 | 224.0.0.252 | Standar query 0x78cb A wpad |
| 192.168.137.2 | 192.168.137.255 | Name query NB WPAD<00> |
| 192.168.137.3 | 192.168.137.256 | Name query NB WPAD<00> |
| 192.168.137.4 | 192.168.137.257 | Name query NB WPAD<00> |
| fe80::2562:1776:7b01:dbb1 | 192.168.137.258 | Standar query 0x78cb A wpad |

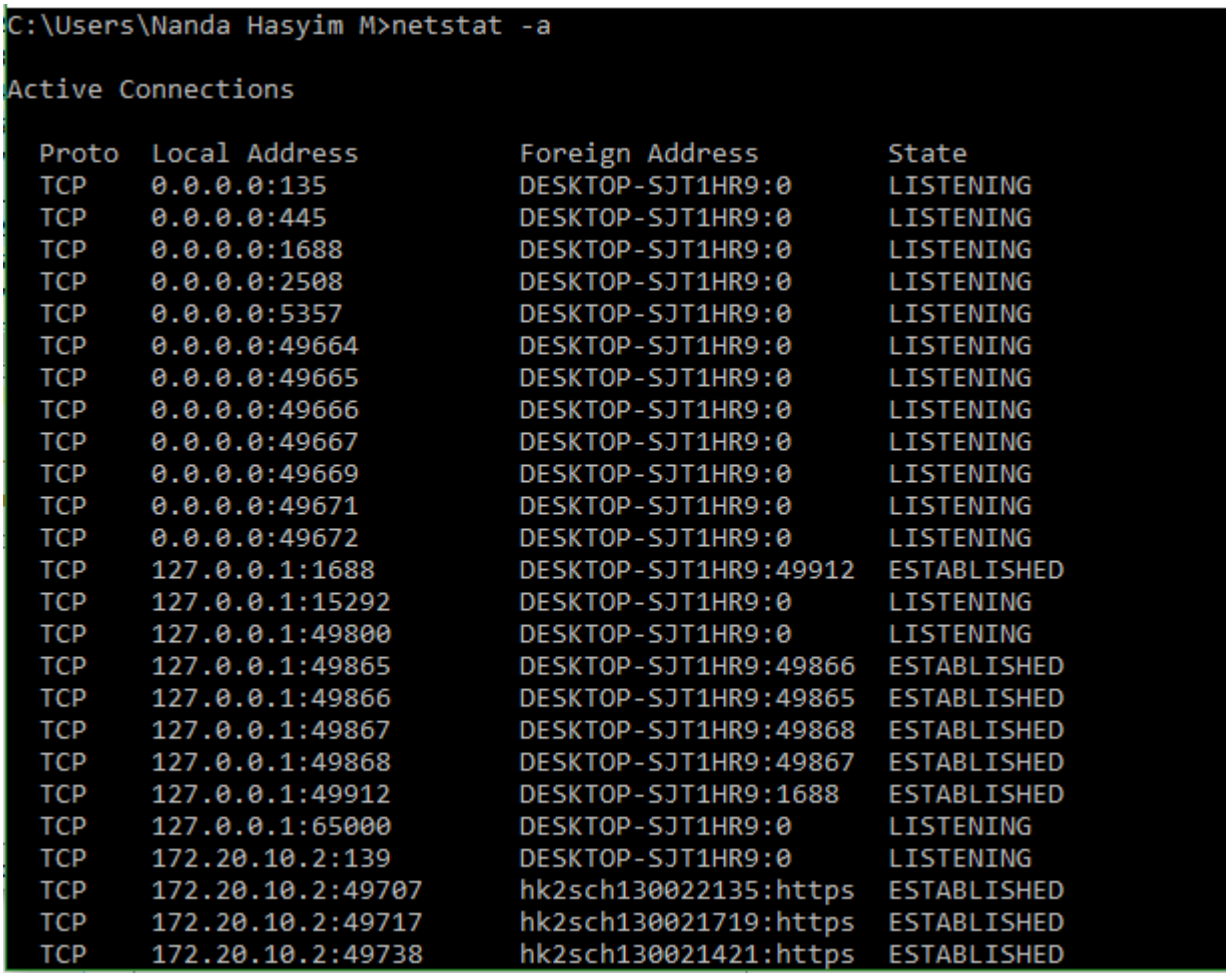
| | IP | MAC |
|---|---|---|
| Source | 192.168.137.1 | 0a : 00 : 27 : 00 : 00 : 13 |
| Destination | 203.190.242.211 | 33 : 33 : 00 : 01 : 00 : 03 |

- **Streaming Online**

| Sources | Destination | INFO |
|---|---|---|
| IP address | IP address | |
| 172.20.10.2 | 66.90.98.37 | Continuation Data |
| 50.7.182.181 | 172.20.10.2 | HTTP/1.1 200 OK (application/x-ns-proxy-autoconfig) |
| 172.20.10.2 | 50.7.182.181 | 53232 > 80 [ACK] seq=32 Ack=1 Win=64349 Len=0 |
| 172.20.10.2 | 172.20.10.15 | Name query NB WPAD<00> |
| 172.20.10.2 | 74.125.200.94 | Application data |
| 172.20.10.2 | 54.230.159.231 | Application data |

| | IP | MAC |
|---|---|---|
| Source | 172.20.10.2 | ac:b5:7d:bd:8c:77 |
| Destination | 52.77.135.185 | 3a:af:61:7c:cf:64 |

- Capture Netstat -a Web Browsing

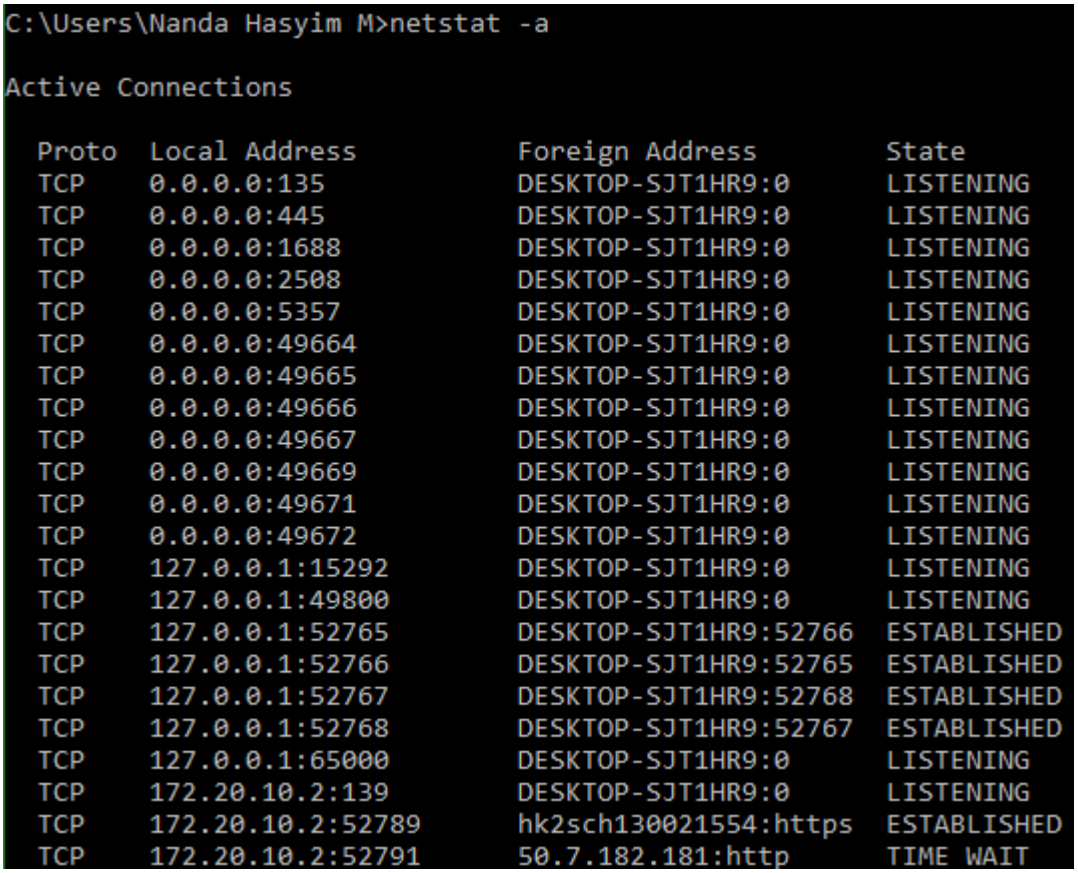


```
C:\Users\Nanda Hasyim M>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            DESKTOP-SJT1HR9:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-SJT1HR9:0      LISTENING
  TCP    0.0.0.0:1688           DESKTOP-SJT1HR9:0      LISTENING
  TCP    0.0.0.0:2508           DESKTOP-SJT1HR9:0      LISTENING
  TCP    0.0.0.0:5357           DESKTOP-SJT1HR9:0      LISTENING
  TCP    0.0.0.0:49664          DESKTOP-SJT1HR9:0      LISTENING
  TCP    0.0.0.0:49665          DESKTOP-SJT1HR9:0      LISTENING
  TCP    0.0.0.0:49666          DESKTOP-SJT1HR9:0      LISTENING
  TCP    0.0.0.0:49667          DESKTOP-SJT1HR9:0      LISTENING
  TCP    0.0.0.0:49669          DESKTOP-SJT1HR9:0      LISTENING
  TCP    0.0.0.0:49671          DESKTOP-SJT1HR9:0      LISTENING
  TCP    0.0.0.0:49672          DESKTOP-SJT1HR9:0      LISTENING
  TCP    127.0.0.1:1688         DESKTOP-SJT1HR9:49912  ESTABLISHED
  TCP    127.0.0.1:15292        DESKTOP-SJT1HR9:0      LISTENING
  TCP    127.0.0.1:49800        DESKTOP-SJT1HR9:0      LISTENING
  TCP    127.0.0.1:49865        DESKTOP-SJT1HR9:49866  ESTABLISHED
  TCP    127.0.0.1:49866        DESKTOP-SJT1HR9:49865  ESTABLISHED
  TCP    127.0.0.1:49867        DESKTOP-SJT1HR9:49868  ESTABLISHED
  TCP    127.0.0.1:49868        DESKTOP-SJT1HR9:49867  ESTABLISHED
  TCP    127.0.0.1:49912        DESKTOP-SJT1HR9:1688   ESTABLISHED
  TCP    127.0.0.1:65000        DESKTOP-SJT1HR9:0      LISTENING
  TCP    172.20.10.2:139        DESKTOP-SJT1HR9:0      LISTENING
  TCP    172.20.10.2:49707      hk2sch130022135:https  ESTABLISHED
  TCP    172.20.10.2:49717      hk2sch130021719:https  ESTABLISHED
  TCP    172.20.10.2:49738      hk2sch130021421:https  ESTABLISHED
```

- Capture Netstat -a Streaming Online



```
C:\Users\Nanda Hasyim M>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            DESKTOP-SJT1HR9:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-SJT1HR9:0      LISTENING
  TCP    0.0.0.0:1688           DESKTOP-SJT1HR9:0      LISTENING
  TCP    0.0.0.0:2508           DESKTOP-SJT1HR9:0      LISTENING
  TCP    0.0.0.0:5357           DESKTOP-SJT1HR9:0      LISTENING
  TCP    0.0.0.0:49664          DESKTOP-SJT1HR9:0      LISTENING
  TCP    0.0.0.0:49665          DESKTOP-SJT1HR9:0      LISTENING
  TCP    0.0.0.0:49666          DESKTOP-SJT1HR9:0      LISTENING
  TCP    0.0.0.0:49667          DESKTOP-SJT1HR9:0      LISTENING
  TCP    0.0.0.0:49669          DESKTOP-SJT1HR9:0      LISTENING
  TCP    0.0.0.0:49671          DESKTOP-SJT1HR9:0      LISTENING
  TCP    0.0.0.0:49672          DESKTOP-SJT1HR9:0      LISTENING
  TCP    127.0.0.1:15292        DESKTOP-SJT1HR9:0      LISTENING
  TCP    127.0.0.1:49800        DESKTOP-SJT1HR9:0      LISTENING
  TCP    127.0.0.1:52765        DESKTOP-SJT1HR9:52766  ESTABLISHED
  TCP    127.0.0.1:52766        DESKTOP-SJT1HR9:52765  ESTABLISHED
  TCP    127.0.0.1:52767        DESKTOP-SJT1HR9:52768  ESTABLISHED
  TCP    127.0.0.1:52768        DESKTOP-SJT1HR9:52767  ESTABLISHED
  TCP    127.0.0.1:65000        DESKTOP-SJT1HR9:0      LISTENING
  TCP    172.20.10.2:139        DESKTOP-SJT1HR9:0      LISTENING
  TCP    172.20.10.2:52789      hk2sch130021554:https  ESTABLISHED
  TCP    172.20.10.2:52791      50.7.182.181:http      TIME_WAIT
```

- Wireshark Web Browsing

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | fe80::2562:1776:7b01:dbb1 | ff02::1:3 | LLMNR | 84 | Standard query 0x78cb A wpad |
| 2 | 0.000109 | 192.168.137.1 | 224.0.0.252 | LLMNR | 64 | Standard query 0x78cb A wpad |
| 3 | 0.340225 | 192.168.137.1 | 192.168.137.255 | NBNS | 92 | Name query NB WPAD<00> |
| 4 | 1.090845 | 192.168.137.1 | 192.168.137.255 | NBNS | 92 | Name query NB WPAD<00> |
| 5 | 9.538533 | 192.168.137.1 | 192.168.137.255 | NBNS | 92 | Name query NB WPAD<00> |
| 6 | 9.539041 | fe80::2562:1776:7b01:dbb1 | ff02::1:3 | LLMNR | 84 | Standard query 0x0708 A wpad |
| 7 | 9.539189 | 192.168.137.1 | 224.0.0.252 | LLMNR | 64 | Standard query 0x0708 A wpad |
| 8 | 9.949348 | fe80::2562:1776:7b01:dbb1 | ff02::1:3 | LLMNR | 84 | Standard query 0x0708 A wpad |
| 9 | 9.949457 | 192.168.137.1 | 224.0.0.252 | LLMNR | 64 | Standard query 0x0708 A wpad |
| 10 | 10.290579 | 192.168.137.1 | 192.168.137.255 | NBNS | 92 | Name query NB WPAD<00> |
| 11 | 11.040777 | 192.168.137.1 | 192.168.137.255 | NBNS | 92 | Name query NB WPAD<00> |
| 12 | 19.524495 | 192.168.137.1 | 192.168.137.255 | NBNS | 92 | Name query NB WPAD<00> |
| 13 | 19.524832 | fe80::2562:1776:7b01:dbb1 | ff02::1:3 | LLMNR | 84 | Standard query 0xebe3 A wpad |
| 14 | 19.524974 | 192.168.137.1 | 224.0.0.252 | LLMNR | 64 | Standard query 0xebe3 A wpad |
| 15 | 19.935519 | fe80::2562:1776:7b01:dbb1 | ff02::1:3 | LLMNR | 84 | Standard query 0xebe3 A wpad |
| 16 | 19.935580 | 192.168.137.1 | 224.0.0.252 | LLMNR | 64 | Standard query 0xebe3 A wpad |
| 17 | 20.275352 | 192.168.137.1 | 192.168.137.255 | NBNS | 92 | Name query NB WPAD<00> |
| 18 | 21.026230 | 192.168.137.1 | 192.168.137.255 | NBNS | 92 | Name query NB WPAD<00> |
| 19 | 29.592081 | 192.168.137.1 | 192.168.137.255 | NBNS | 92 | Name query NB WPAD<00> |
| 20 | 29.592302 | fe80::2562:1776:7b01:dbb1 | ff02::1:3 | LLMNR | 84 | Standard query 0x5e11 A wpad |
| 21 | 29.592397 | 192.168.137.1 | 224.0.0.252 | LLMNR | 64 | Standard query 0x5e11 A wpad |
| 22 | 30.002507 | fe80::2562:1776:7b01:dbb1 | ff02::1:3 | LLMNR | 84 | Standard query 0x5e11 A wpad |
| 23 | 30.002580 | 192.168.137.1 | 224.0.0.252 | LLMNR | 64 | Standard query 0x5e11 A wpad |
| 24 | 30.342270 | 192.168.137.1 | 192.168.137.255 | NBNS | 92 | Name query NB WPAD<00> |
| 25 | 31.095310 | 192.168.137.1 | 192.168.137.255 | NBNS | 92 | Name query NB WPAD<00> |
| 26 | 39.513968 | 192.168.137.1 | 192.168.137.255 | NBNS | 92 | Name query NB WPAD<00> |

- Wireshark Streaming Online

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | 172.20.10.2 | 66.90.98.37 | SSL | 55 | Continuation Data |
| 2 | 0.122135 | 50.7.182.181 | 172.20.10.2 | HTTP | 233 | HTTP/1.1 200 OK  (application/x-ns-proxy-autoconfig) |
| 3 | 0.171915 | 172.20.10.2 | 50.7.182.181 | TCP | 54 | 53232 → 80 [ACK] Seq=1 Ack=180 Win=253 Len=0 |
| 4 | 0.194442 | 172.20.10.2 | 172.20.10.15 | NBNS | 92 | Name query NB WPAD<00> |
| 5 | 0.357675 | 172.20.10.2 | 74.125.200.94 | TLSv1.2 | 100 | Application Data |
| 6 | 0.358243 | 172.20.10.2 | 54.230.159.231 | TLSv1.2 | 100 | Application Data |
| 7 | 0.358391 | 172.20.10.2 | 34.209.12.3 | TLSv1.2 | 85 | Encrypted Alert |
| 8 | 0.358450 | 172.20.10.2 | 34.209.12.3 | TCP | 54 | 53237 → 443 [FIN, ACK] Seq=32 Ack=1 Win=64349 Len=0 |
| 9 | 0.415623 | 66.90.98.37 | 172.20.10.2 | TCP | 66 | 443 → 52939 [ACK] Seq=1 Ack=2 Win=287 Len=0 SLE=1 SRE=2 |
| 10 | 0.419777 | 52.74.120.185 | 172.20.10.2 | TLSv1.2 | 85 | Encrypted Alert |
| 11 | 0.454909 | 172.20.10.2 | 52.74.120.185 | TCP | 54 | 53074 → 443 [ACK] Seq=1 Ack=32 Win=256 Len=0 |
| 12 | 0.458924 | 172.20.10.2 | 172.20.10.1 | DNS | 87 | Standard query 0xe5fc PTR 139.200.125.74.in-addr.arpa |
| 13 | 0.498471 | 54.230.159.231 | 172.20.10.2 | TCP | 54 | 443 → 52952 [ACK] Seq=1 Ack=47 Win=127 Len=0 |
| 14 | 0.501970 | 74.125.200.94 | 172.20.10.2 | TCP | 54 | 443 → 52831 [ACK] Seq=1 Ack=47 Win=184 Len=0 |
| 15 | 0.526575 | 172.20.10.2 | 54.230.159.231 | TLSv1.2 | 85 | Encrypted Alert |
| 16 | 0.526665 | 172.20.10.2 | 54.230.159.231 | TCP | 54 | 52952 → 443 [FIN, ACK] Seq=78 Ack=1 Win=253 Len=0 |
| 17 | 0.526885 | 172.20.10.2 | 74.125.200.94 | TLSv1.2 | 85 | Encrypted Alert |
| 18 | 0.526929 | 172.20.10.2 | 74.125.200.94 | TCP | 54 | 52831 → 443 [FIN, ACK] Seq=78 Ack=1 Win=255 Len=0 |
| 19 | 0.527254 | 172.20.10.2 | 52.74.120.185 | TCP | 54 | 53074 → 443 [FIN, ACK] Seq=1 Ack=32 Win=256 Len=0 |
| 20 | 0.581406 | 74.125.200.94 | 172.20.10.2 | TCP | 54 | 443 → 52831 [ACK] Seq=1 Ack=78 Win=184 Len=0 |
| 21 | 0.581645 | 74.125.200.94 | 172.20.10.2 | TCP | 54 | 443 → 52831 [FIN, ACK] Seq=1 Ack=78 Win=184 Len=0 |
| 22 | 0.581645 | 54.230.159.231 | 172.20.10.2 | TCP | 66 | [TCP Dup ACK 13#1] 443 → 52952 [ACK] Seq=1 Ack=47 Win=127 Len=0 SLE=78 SRE=79 |
| 23 | 0.581684 | 172.20.10.2 | 74.125.200.94 | TCP | 54 | 52831 → 443 [ACK] Seq=79 Ack=2 Win=255 Len=0 |
| 24 | 0.582180 | 54.230.159.231 | 172.20.10.2 | TCP | 54 | 443 → 52952 [ACK] Seq=1 Ack=79 Win=127 Len=0 |
| 25 | 0.582180 | 54.230.159.231 | 172.20.10.2 | TCP | 54 | 443 → 52952 [FIN, ACK] Seq=1 Ack=79 Win=127 Len=0 |
| 26 | 0.582210 | 172.20.10.2 | 54.230.159.231 | TCP | 54 | 52952 → 443 [ACK] Seq=79 Ack=2 Win=253 Len=0 |

Pada capture yang tertera diatas, wireshark memiliki tampilan paket dengan informasi protocol yang sangat rinci. Setiap baris dalam daftar paket sesuai dengan satu paket dalam file yang diambil. Dan pada dasarnya perbandingan antara cmd dan wireshark terlihat bahwa tidak ada tools yang sempurna. Masing-masing memiliki kelebihan dan kekurangan masing-masing.