

Hasil capture menggunakan CMD (Command Prompt)

```

Command Prompt
C:\Users\ASUS>netstat -a

Active Connections

Proto Local Address           Foreign Address         State
TCP   0.0.0.0:135             DESKTOP-H0A3F7Q:0     LISTENING
TCP   0.0.0.0:445             DESKTOP-H0A3F7Q:0     LISTENING
TCP   0.0.0.0:5357            DESKTOP-H0A3F7Q:0     LISTENING
TCP   0.0.0.0:49664           DESKTOP-H0A3F7Q:0     LISTENING
TCP   0.0.0.0:49665           DESKTOP-H0A3F7Q:0     LISTENING
TCP   0.0.0.0:49666           DESKTOP-H0A3F7Q:0     LISTENING
TCP   0.0.0.0:49667           DESKTOP-H0A3F7Q:0     LISTENING
TCP   0.0.0.0:49681           DESKTOP-H0A3F7Q:0     LISTENING
TCP   0.0.0.0:49695           DESKTOP-H0A3F7Q:0     LISTENING
TCP   0.0.0.0:50983           DESKTOP-H0A3F7Q:0     LISTENING
TCP   127.0.0.1:1001          DESKTOP-H0A3F7Q:0     LISTENING
TCP   127.0.0.1:10400         DESKTOP-H0A3F7Q:0     LISTENING
TCP   127.0.0.1:30000         DESKTOP-H0A3F7Q:0     LISTENING
TCP   127.0.0.1:52128         DESKTOP-H0A3F7Q:0     LISTENING
TCP   127.0.0.1:52128         DESKTOP-H0A3F7Q:52667 ESTABLISHED
TCP   127.0.0.1:52130         DESKTOP-H0A3F7Q:52131 ESTABLISHED
TCP   127.0.0.1:52131         DESKTOP-H0A3F7Q:52130 ESTABLISHED
TCP   127.0.0.1:52132         DESKTOP-H0A3F7Q:52133 ESTABLISHED
TCP   127.0.0.1:52133         DESKTOP-H0A3F7Q:52132 ESTABLISHED
TCP   127.0.0.1:52663         DESKTOP-H0A3F7Q:52664 ESTABLISHED
TCP   127.0.0.1:52664         DESKTOP-H0A3F7Q:52663 ESTABLISHED
TCP   127.0.0.1:52665         DESKTOP-H0A3F7Q:52666 ESTABLISHED
TCP   127.0.0.1:52666         DESKTOP-H0A3F7Q:52665 ESTABLISHED
TCP   127.0.0.1:52667         DESKTOP-H0A3F7Q:52128 ESTABLISHED
TCP   192.168.43.229:139      DESKTOP-H0A3F7Q:0     LISTENING
TCP   192.168.43.229:52164    hk2sch130021032:https ESTABLISHED
TCP   192.168.43.229:52653    115.146.116.8:https   CLOSE_WAIT
TCP   192.168.43.229:52654    104.18.55.167:http    CLOSE_WAIT
TCP   192.168.43.229:52808    ec2-54-71-197-51:https TIME_WAIT
TCP   192.168.43.229:52809    117.18.237.29:http    TIME_WAIT
TCP   192.168.43.229:52816    ams15s32-in-f2:http   ESTABLISHED
TCP   192.168.43.229:52817    ams15s32-in-f2:http   ESTABLISHED
TCP   192.168.43.229:52818    ams15s32-in-f2:http   ESTABLISHED
TCP   192.168.43.229:52819    ams15s32-in-f2:http   ESTABLISHED
TCP   192.168.43.229:52820    ams15s32-in-f2:http   TIME_WAIT
TCP   192.168.43.229:52821    ams15s32-in-f2:https ESTABLISHED
TCP   192.168.43.229:52822    ams15s32-in-f2:http   TIME_WAIT
TCP   192.168.43.229:52823    ams15s32-in-f2:http   TIME_WAIT

```

Source :

IP	Info
192.168.43.229	Standard query 0x5736 PTR 100.4.146.202.in-addr.arpa
192.168.43.1	Standard query response 0x5736 No such name PTR 100.4.146.202.in-addr.arpa SOA ns1.kgcil.com
144.76.152.132	Encrypted Alert
172.217.17.66	80 → 52829 [ACK] Seq=1 Ack=2 Win=184 Len=0 SLE=1 SRE=2
202.61.113.71	80 → 52873 [ACK] Seq=1 Ack=2 Win=6643 Len=0

Destination :

IP	Info
192.168.43.1	Standard query 0x5736 PTR 100.4.146.202.in-addr.arpa
192.168.43.229	Standard query response 0x5736 No such name PTR 100.4.146.202.in-addr.arpa SOA ns1.kgcil.com
202.61.113.71	52873 → 80 [ACK] Seq=1 Ack=1 Win=65189 Len=1
144.76.152.132	52895 → 443 [ACK] Seq=1 Ack=33 Win=64026 Len=0
172.217.17.66	52829 → 80 [ACK] Seq=1 Ack=1 Win=258 Len=1

- Capture data dari www.vidio.com

Hasil capture dengan Wireshark

The screenshot shows the Wireshark interface with a network traffic capture. The main pane displays a list of 18 packets. The details pane for the selected packet (No. 1) shows the following information:

- Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
- Ethernet II, Src: aec1:ee:89:2d:d9 (aec1:ee:89:2d:d9), Dst: Azurewav_da:b0:b2 (6c:71:d9:da:b0:b2)
- Internet Protocol Version 4, Src: 103.243.221.75, Dst: 192.168.43.229
- Transmission Control Protocol, Src Port: 443, Dst Port: 53556, Seq: 1, Ack: 1, Len: 0

The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	103.243.221.75	192.168.43.229	TCP	54	443 → 53556 [ACK] Seq=1 Ack=1 Win=32200 Len=0
2	0.000002	103.243.221.75	192.168.43.229	TCP	54	443 → 53556 [ACK] Seq=1 Ack=0 Win=32200 Len=0
3	0.751741	192.168.43.229	104.16.94.65	SSL	55	Continuation Data
4	1.043363	104.16.94.65	192.168.43.229	TCP	66	443 → 53571 [ACK] Seq=1 Ack=2 Win=31 Len=0 SLE=1 SRE=2
5	4.173825	192.168.43.229	23.66.246.24	SSL	55	Continuation Data
6	4.907431	23.66.246.24	192.168.43.229	TCP	66	443 → 53519 [ACK] Seq=1 Ack=2 Win=900 Len=0 SLE=1 SRE=2
7	5.095772	192.168.43.229	52.84.225.72	SSL	55	Continuation Data
8	5.126964	192.168.43.229	52.84.225.248	SSL	55	Continuation Data
9	5.151591	52.84.225.72	192.168.43.229	TCP	66	443 → 53526 [ACK] Seq=1 Ack=2 Win=123 Len=0 SLE=1 SRE=2
10	5.197103	52.84.225.248	192.168.43.229	TCP	66	443 → 53537 [ACK] Seq=1 Ack=2 Win=123 Len=0 SLE=1 SRE=2
11	5.720746	192.168.43.229	13.228.194.45	SSL	55	Continuation Data
12	5.720746	192.168.43.229	13.228.194.45	SSL	55	Continuation Data
13	5.720782	192.168.43.229	13.228.194.45	SSL	55	Continuation Data
14	5.812040	13.228.194.45	192.168.43.229	TCP	66	443 → 53539 [ACK] Seq=1 Ack=2 Win=123 Len=0 SLE=1 SRE=2
15	5.812041	13.228.194.45	192.168.43.229	TCP	66	443 → 53540 [ACK] Seq=1 Ack=2 Win=120 Len=0 SLE=1 SRE=2
16	5.812042	13.228.194.45	192.168.43.229	TCP	66	443 → 53521 [ACK] Seq=1 Ack=2 Win=156 Len=0 SLE=1 SRE=2
17	6.095804	192.168.43.229	52.84.225.171	SSL	55	Continuation Data
18	6.165965	52.84.225.171	192.168.43.229	TCP	66	443 → 53549 [ACK] Seq=1 Ack=2 Win=125 Len=0 SLE=1 SRE=2

The hex dump at the bottom shows the raw data of the first packet:

```
0000 6c 71 d9 da b0 b2 ae c1 ee 89 2d d9 08 00 45 00 1q.....-...E.
0010 00 28 89 b4 40 00 2c 06 93 4f 67 f3 dd 4b c0 a8  .(...). .Og..K..
0020 2b e5 01 bb d1 34 af d7 4d 24 a7 4d 26 26 50 10  +...4.. M$.M&&P.
0030 7d c8 62 e0 00 00                                }.b...
```

Hasil capture menggunakan CMD (Commad Prompt)

```

Command Prompt
C:\Users\ASUS>netstat -a

Active Connections

Proto Local Address           Foreign Address         State
TCP   0.0.0.0:135             DESKTOP-H0A3F7Q:0     LISTENING
TCP   0.0.0.0:445             DESKTOP-H0A3F7Q:0     LISTENING
TCP   0.0.0.0:5357            DESKTOP-H0A3F7Q:0     LISTENING
TCP   0.0.0.0:49664           DESKTOP-H0A3F7Q:0     LISTENING
TCP   0.0.0.0:49665           DESKTOP-H0A3F7Q:0     LISTENING
TCP   0.0.0.0:49666           DESKTOP-H0A3F7Q:0     LISTENING
TCP   0.0.0.0:49667           DESKTOP-H0A3F7Q:0     LISTENING
TCP   0.0.0.0:49681           DESKTOP-H0A3F7Q:0     LISTENING
TCP   0.0.0.0:49695           DESKTOP-H0A3F7Q:0     LISTENING
TCP   0.0.0.0:50983           DESKTOP-H0A3F7Q:0     LISTENING
TCP   127.0.0.1:1001          DESKTOP-H0A3F7Q:0     LISTENING
TCP   127.0.0.1:10400         DESKTOP-H0A3F7Q:0     LISTENING
TCP   127.0.0.1:30000         DESKTOP-H0A3F7Q:0     LISTENING
TCP   127.0.0.1:52128         DESKTOP-H0A3F7Q:0     LISTENING
TCP   127.0.0.1:52128         DESKTOP-H0A3F7Q:52667 ESTABLISHED
TCP   127.0.0.1:52130         DESKTOP-H0A3F7Q:52131 ESTABLISHED
TCP   127.0.0.1:52131         DESKTOP-H0A3F7Q:52130 ESTABLISHED
TCP   127.0.0.1:52132         DESKTOP-H0A3F7Q:52133 ESTABLISHED
TCP   127.0.0.1:52133         DESKTOP-H0A3F7Q:52132 ESTABLISHED
TCP   127.0.0.1:52663         DESKTOP-H0A3F7Q:52664 ESTABLISHED
TCP   127.0.0.1:52664         DESKTOP-H0A3F7Q:52663 ESTABLISHED
TCP   127.0.0.1:52665         DESKTOP-H0A3F7Q:52666 ESTABLISHED
TCP   127.0.0.1:52666         DESKTOP-H0A3F7Q:52665 ESTABLISHED
TCP   127.0.0.1:52667         DESKTOP-H0A3F7Q:52128 ESTABLISHED
TCP   192.168.43.229:139      DESKTOP-H0A3F7Q:0     LISTENING
TCP   192.168.43.229:52164    hk2sch130021032:https ESTABLISHED
TCP   192.168.43.229:52653    115.146.116.8:https   CLOSE_WAIT
TCP   192.168.43.229:52654    104.18.55.167:http    CLOSE_WAIT
TCP   192.168.43.229:53517    ams15s33-in-f14:https ESTABLISHED
TCP   192.168.43.229:53518    ams16s22-in-f232:https TIME_WAIT
TCP   192.168.43.229:53521    ec2-13-228-194-45:https TIME_WAIT
TCP   192.168.43.229:53524    21:https               ESTABLISHED
TCP   192.168.43.229:53526    server-52-84-225-72:https TIME_WAIT
TCP   192.168.43.229:53537    server-52-84-225-248:https TIME_WAIT

TCP   192.168.43.229:53538    arn02s05-in-f2:https  TIME_WAIT
TCP   192.168.43.229:53539    ec2-13-228-194-45:https TIME_WAIT
TCP   192.168.43.229:53540    ec2-13-228-194-45:https TIME_WAIT
  
```

Source :

IP	Info
103.243.221.75	443 → 53556 [ACK] Seq=1 Ack=1 Win=32200 Len=0
192.168.43.229	[TCP segment of a reassembled PDU]
104.16.94.65	443 → 53571 [ACK] Seq=1 Ack=2 Win=31 Len=0 SLE=1 SRE=2
23.66.246.24	443 → 53519 [ACK] Seq=1 Ack=2 Win=980 Len=0 SLE=1 SRE=2
52.84.225.72	443 → 53526 [ACK] Seq=1 Ack=2 Win=123 Len=0 SLE=1 SRE=2
52.84.225.248	443 → 53537 [ACK] Seq=1 Ack=2 Win=123 Len=0 SLE=1 SRE=2
13.228.194.45	443 → 53539 [ACK] Seq=1 Ack=2 Win=123 Len=0 SLE=1 SRE=2
52.84.225.171	443 → 53549 [ACK] Seq=1 Ack=2 Win=125 Len=0 SLE=1 SRE=2
38.72.130.155	443 → 53560 [RST, ACK] Seq=1 Ack=1 Win=25617 Len=0

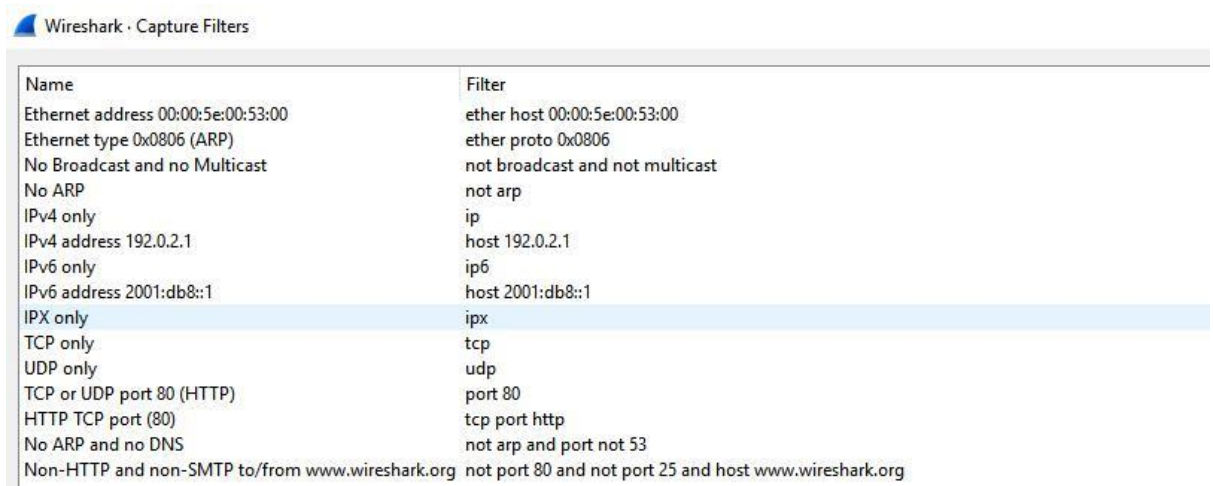
Destination :

IP	Info
192.168.43.229	443 → 53556 [ACK] Seq=1 Ack=1 Win=32200 Len=0
104.16.94.65	[TCP segment of a reassembled PDU]
23.66.246.24	[TCP segment of a reassembled PDU]
52.84.225.72	[TCP segment of a reassembled PDU]
52.84.225.248	Continuation Data
13.228.194.45	[TCP segment of a reassembled PDU]
52.84.225.171	[TCP segment of a reassembled PDU]
23.41.75.27	53562 → 80 [ACK] Seq=1 Ack=1 Win=257 Len=1

- Perbedaan Capture Data menggunakan Wireshark dan Cmd;

Analisis paket data dengan menggunakan Wireshark lebih lengkap dan terinci dibandingkan dengan menggunakan Cmd, selain itu juga Cmd hanya dapat membaca protocol TCP sedangkan pada Wireshark dapat membaca berbagai jenis protocol sehingga banyak data yang muncul, termasuk berbagai jenis data error yang terjadi saat pembacaan data.

- Capture Filters



Name	Filter
Ethernet address 00:00:5e:00:53:00	ether host 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	ether proto 0x0806
No Broadcast and no Multicast	not broadcast and not multicast
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	host 192.0.2.1
IPv6 only	ip6
IPv6 address 2001:db8::1	host 2001:db8::1
IPX only	ipx
TCP only	tcp
UDP only	udp
TCP or UDP port 80 (HTTP)	port 80
HTTP TCP port (80)	tcp port http
No ARP and no DNS	not arp and port not 53
Non-HTTP and non-SMTP to/from www.wireshark.org	not port 80 and not port 25 and host www.wireshark.org