

JARINGAN KOMPUTER
“CAPTURING DATA”



Nama : Ulviyana
NIM : 09011281520090
Dosen Pengampuh : Deris Stiawan, M.T., PH.D.

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2017

CAPTURING DATA

1. Browsing data melalui aplikasi wireshark.

IP source : 203.190.242.102

IP Destination : 10.94.14.109

MAC Source : (d4:ca:6d:44:6b;80)

MAC Destination : (1c:b7:2c:e7:5b;74)

Wireshark capture showing network traffic. The display filter is <CMI-/. The packet list shows:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	AsustekC_ba:5e:bd	Broadcast	ARP	60	Who has 10.94.14.183? Tell 10.94.14.232
2	0.133226	Routerbo_b3:c7:c5	Spanning-tree-(for-b...	STP	60	RST, Root = 32768/0/4c:5e:0c:b3:c7:c3 Cost = 0 Port = 0x8002
3	0.300268	AsustekC_ba:5e:c2	Broadcast	ARP	60	Who has 10.94.14.243? Tell 10.94.14.203
4	0.411734	Routerbo_44:6b:80	Spanning-tree-(for-b...	0x80bf	60	Ethernet II
5	0.489413	2001:0:9d38:90d7:280...	ff02::1	IPv6	82	IPv6 no next header
6	1.000144	AsustekC_ba:5e:bd	Broadcast	ARP	60	Who has 10.94.14.183? Tell 10.94.14.232
7	1.282956	fe80::20a1:bfd:36ac...	ff02::1:2	DHCPv6	153	Solicit XID: 0xdba28a CID: 000100011efd487b086266ba5e56
8	1.306708	2001:0:9d38:90d7:107...	ff02::1	IPv6	82	IPv6 no next header
9	1.596181	2001:0:9d38:90d7:14a...	ff02::1	IPv6	82	IPv6 no next header
10	1.698441	2001:0:9d38:90d7:c4...	ff02::1	IPv6	82	IPv6 no next header
11	1.699488	2001:0:9d38:90d7:c4...	ff02::1	IPv6	82	IPv6 no next header
12	1.801763	2001:0:9d38:90d7:20a...	ff02::1	IPv6	82	IPv6 no next header
13	2.125944	Routerbo_b3:c7:c5	Spanning-tree-(for-b...	STP	60	RST, Root = 32768/0/4c:5e:0c:b3:c7:c3 Cost = 0 Port = 0x8002
14	2.283117	fe80::20a1:bfd:36ac...	ff02::1:2	DHCPv6	153	Solicit XID: 0xdba28a CID: 000100011efd487b086266ba5e56
15	2.608636	2001:0:9d38:90d7:c4...	ff02::1	IPv6	82	IPv6 no next header
16	3.283153	fe80::20a1:bfd:36ac...	ff02::1:2	DHCPv6	153	Solicit XID: 0xdba28a CID: 000100011efd487b086266ba5e56
17	4.138168	Routerbo_b3:c7:c5	Spanning-tree-(for-b...	STP	60	RST, Root = 32768/0/4c:5e:0c:b3:c7:c3 Cost = 0 Port = 0x8002
18	4.579275	10.94.14.109	111.221.29.254	TCP	54	54440 -> 443 [FIN, ACK] Seq=1 Ack=1 Win=257 Len=0
19	4.595531	2001:0:9d38:90d7:c4...	ff02::1	IPv6	82	IPv6 no next header
20	4.597810	AsustekC_ba:5e:c2	Broadcast	ARP	60	Who has 10.94.14.243? Tell 10.94.14.203
21	4.624029	111.221.29.254	10.94.14.109	TCP	60	443 -> 54440 [FIN, ACK] Seq=2 Ack=2 Win=1026 Len=0
22	4.624100	10.94.14.109	111.221.29.254	TCP	54	54440 -> 443 [ACK] Seq=2 Ack=2 Win=257 Len=0
23	4.787197	10.94.14.109	13.107.21.200	TCP	54	54439 -> 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	5.010872	2001:0:9d38:90d7:102...	ff02::1	IPv6	82	IPv6 no next header
25	5.095701	2001:0:9d38:90d7:14a...	ff02::1	IPv6	82	IPv6 no next header
26	5.290300	fe80::20a1:bfd:36ac...	ff02::1:2	DHCPv6	153	Solicit XID: 0xdba28a CID: 000100011efd487b086266ba5e56
27	5.300841	AsustekC_ba:5e:c2	Broadcast	ARP	60	Who has 10.94.14.243? Tell 10.94.14.203

Wireshark capture showing network traffic. The display filter is <CMI-/. The packet list shows:

No.	Time	Source	Destination	Protocol	Length	Info
189.	132.058729	74.125.24.138	10.94.14.109	TLSv1.2	1484	Application Data
189.	132.058731	74.125.24.138	10.94.14.109	TLSv1.2	1484	Application Data
189.	132.058738	74.125.24.138	10.94.14.109	TLSv1.2	1484	Application Data
189.	132.058740	74.125.24.138	10.94.14.109	TLSv1.2	737	Application Data
189.	132.058741	74.125.24.138	10.94.14.109	TLSv1.2	100	Application Data
189.	132.058918	10.94.14.109	74.125.24.138	TCP	54	54697 -> 443 [ACK] Seq=869 Ack=9853 Win=262144 Len=0
189.	132.061500	10.94.14.109	74.125.24.138	TLSv1.2	100	Application Data
189.	132.063566	203.190.242.132	10.94.14.109	TLSv1.2	92	Application Data
189.	132.063737	10.94.14.109	203.190.242.132	TCP	54	54727 -> 443 [ACK] Seq=842 Ack=222 Win=261920 Len=0
189.	132.064571	203.190.242.132	10.94.14.109	TCP	60	443 -> 54726 [ACK] Seq=1 Ack=410 Win=15872 Len=0
189.	132.065308	203.190.242.132	10.94.14.109	TLSv1.2	168	Server Hello, Change Cipher Spec, Encrypted Handshake Message
189.	132.065509	10.94.14.109	203.190.242.132	TCP	54	54726 -> 443 [ACK] Seq=410 Ack=115 Win=262024 Len=0
189.	132.066713	10.94.14.109	203.190.242.132	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
189.	132.068772	10.94.14.109	203.190.242.132	TLSv1.2	141	Application Data
189.	132.070282	203.190.242.132	10.94.14.109	TCP	60	443 -> 54727 [ACK] Seq=222 Ack=842 Win=16896 Len=0
189.	132.080827	203.190.242.132	10.94.14.109	TLSv1.2	123	Application Data
189.	132.080995	10.94.14.109	203.190.242.132	TCP	54	54726 -> 443 [ACK] Seq=548 Ack=184 Win=261960 Len=0
189.	132.087451	10.94.14.109	203.190.242.132	TLSv1.2	92	Application Data
189.	132.088584	203.190.242.132	10.94.14.109	TLSv1.2	92	Application Data
189.	132.088725	10.94.14.109	203.190.242.132	TCP	54	54726 -> 443 [ACK] Seq=586 Ack=222 Win=261920 Len=0
189.	132.115141	74.125.24.138	10.94.14.109	TCP	60	443 -> 54697 [ACK] Seq=9853 Ack=915 Win=45056 Len=0
189.	132.147555	203.190.242.132	10.94.14.109	TCP	60	443 -> 54726 [ACK] Seq=222 Ack=586 Win=15872 Len=0
189.	132.165532	203.190.242.132	10.94.14.109	TLSv1.2	427	Application Data
189.	132.165702	10.94.14.109	203.190.242.132	TCP	54	54727 -> 443 [ACK] Seq=842 Ack=595 Win=261544 Len=0
189.	132.177368	10.94.14.239	10.94.14.255	NBNS	92	Name query NB WPAD<00>
189.	132.287411	Routerbo_b3:c7:c5	Spanning-tree-(for-b...	STP	60	RST, Root = 32768/0/4c:5e:0c:b3:c7:c3 Cost = 0 Port = 0x8002
189.	132.352419	10.94.14.109	31.13.78.35	TLSv1.2	178	Application Data

SOURCE	
IP	INFO
203.190.242.107	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10.94.14.109	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
103.49.221.211	Application Data
10.94.14.109	443 → 54489 [ACK] Seq=3866 Ack=473 Win=29440 Len=0
10.94.14.109	Application Data

DESTINATION	
IP	INFO
10.94.14.158	Standard query Ox7ea3 A isatap
103.49.221.122	Application Data
10.94.14.109	54489 → 443 [ACK] Seq=6556 Ack=7612 Win=261760 Len=0
31.13.78.35	Application Data
10.94.14.109	54700 → 443 [ACK] Seq=1875 Ack=476862 Win=262144 Len=0

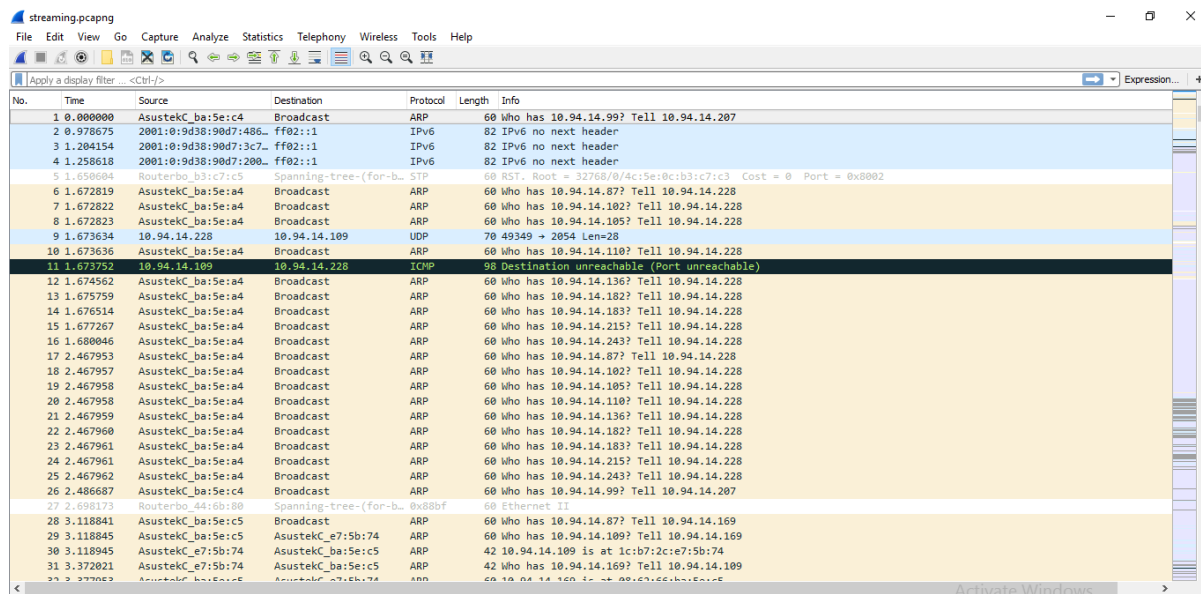
2. Streaming video melalui aplikasi wireshark.

IP source : 10.94.14.109

IP Destination : 23.0.177.143

MAC Source : (1c:b7:2c:e7:5b:74)

MAC Destination : (d4:ca:6d:44:6b:80)



No.	Time	Source	Destination	Protocol	Length	Info
9397	100.848349	23.0.177.143	10.94.14.109	TLSv1.2	1506	Application Data
9398	100.848354	23.0.177.143	10.94.14.109	TLSv1.2	268	Application Data
9399	100.848355	23.0.177.143	10.94.14.109	TLSv1.2	1506	Application Data
9400	100.848356	23.0.177.143	10.94.14.109	TLSv1.2	1514	Application Data
9401	100.848358	23.0.177.143	10.94.14.109	TLSv1.2	1498	Application Data
9402	100.848359	23.0.177.143	10.94.14.109	TLSv1.2	1514	Application Data
9403	100.848532	10.94.14.109	23.0.177.143	TCP	54	54774 → 443 [ACK] Seq=2792 Ack=3816250 Win=262144 Len=0
9404	100.850082	23.0.177.143	10.94.14.109	TLSv1.2	1514	Application Data [TCP segment of a reassembled PDU]
9405	100.850219	10.94.14.109	23.0.177.143	TCP	54	54774 → 443 [ACK] Seq=2792 Ack=3817710 Win=262144 Len=0
9406	100.950743	23.0.177.143	10.94.14.109	TLSv1.2	1514	Application Data [TCP segment of a reassembled PDU]
9407	100.950748	23.0.177.143	10.94.14.109	TLSv1.2	1514	Application Data [TCP segment of a reassembled PDU]
9408	100.950749	23.0.177.143	10.94.14.109	TLSv1.2	1514	Application Data [TCP segment of a reassembled PDU]
9409	100.950751	23.0.177.143	10.94.14.109	TLSv1.2	1514	Application Data [TCP segment of a reassembled PDU]
9410	100.950752	23.0.177.143	10.94.14.109	TLSv1.2	1514	Application Data [TCP segment of a reassembled PDU]
9411	100.950916	10.94.14.109	23.0.177.143	TCP	54	54774 → 443 [ACK] Seq=2792 Ack=3825018 Win=262144 Len=0
9412	100.952243	23.0.177.143	10.94.14.109	TLSv1.2	1514	Application Data [TCP segment of a reassembled PDU]
9413	100.952247	23.0.177.143	10.94.14.109	TLSv1.2	1514	Application Data [TCP segment of a reassembled PDU]
9414	100.952248	23.0.177.143	10.94.14.109	TLSv1.2	1514	Application Data [TCP segment of a reassembled PDU]
9415	100.952374	10.94.14.109	23.0.177.143	TCP	54	54774 → 443 [ACK] Seq=2792 Ack=3829398 Win=262144 Len=0
9416	101.039778	fe80::e995:5e6c:8585...	ff02::1:2	DHCPv6	153	Solicit XID: 0x334ae0 CID: 000100011efdc084086266ba5ea4
9417	101.052054	23.0.177.143	10.94.14.109	TLSv1.2	1514	Application Data [TCP segment of a reassembled PDU]
9418	101.052060	23.0.177.143	10.94.14.109	TLSv1.2	1514	Application Data [TCP segment of a reassembled PDU]
9419	101.052062	23.0.177.143	10.94.14.109	TLSv1.2	1514	Application Data [TCP segment of a reassembled PDU]
9420	101.052065	23.0.177.143	10.94.14.109	TLSv1.2	1514	Application Data [TCP segment of a reassembled PDU]
9421	101.052300	10.94.14.109	23.0.177.143	TCP	54	54774 → 443 [ACK] Seq=2792 Ack=3835238 Win=262144 Len=0
9422	101.053903	23.0.177.143	10.94.14.109	TLSv1.2	1514	[TCP Previous segment not captured], Ignored Unknown Record
9423	101.053906	23.0.177.143	10.94.14.109	TLSv1.2	1514	Ignored Unknown Record
9424	101.053912	23.0.177.143	10.94.14.109	TLSv1.2	1514	Ignored Unknown Record
9425	101.054032	10.94.14.109	23.0.177.143	TCP	66	[TCP Dup ACK 9421#1] 54774 → 443 [ACK] Seq=2792 Ack=3835238 Win=262144 Len=0 SLE=3838150 SRE=3839610
9426	101.054112	10.94.14.109	23.0.177.143	TCP	66	[TCP Dup ACK 9421#2] 54774 → 443 [ACK] Seq=2792 Ack=3835238 Win=262144 Len=0 SLE=3838150 SRE=3841070
9427	101.054167	10.94.14.109	23.0.177.143	TCP	66	[TCP Dup ACK 9421#3] 54774 → 443 [ACK] Seq=2792 Ack=3835238 Win=262144 Len=0 SLE=3838150 SRE=3842530

SOURCE	
IP	INFO
23.0.177.143	54774 → 443 [ACK] Seq=2792 Ack=3817710 Win=262144 Len=0
10.94.14.109	Application Data [TCP segment of a reassembled PDU]
10.94.14.109	Encrypted Heartbeat, Ignored Unknown Record
130.211.37.21	Application Data
10.94.14.109	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message

DESTINATION	
IP	INFO
130.211.37.21	Application Data
74.125.24.113	443 → 54760 [ACK] Seq=913 Ack=2015 Win=48384 Len=0
10.94.14.109	Client Hello
106.10.198.33	Server Hello
54.230.156.60	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message

1. Browsing data melalui CMD.

ca. Command Prompt

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\ASUS X453SA>netstat -a

Active Connections

Proto Local Address           Foreign Address         State
TCP   0.0.0.0:135             DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:445             DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:2508            DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:5357            DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:49664           DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:49665           DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:49666           DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:49667           DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:49668           DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:49669           DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:53228           DESKTOP-6Q502CS:0     LISTENING
TCP   10.94.14.109:139        DESKTOP-6Q502CS:0     LISTENING
TCP   10.94.14.109:54475      203.190.242.59:https  TIME_WAIT
TCP   10.94.14.109:54532      74.125.24.113:https   ESTABLISHED
TCP   10.94.14.109:54562      203.190.242.187:https TIME_WAIT
TCP   10.94.14.109:54563      203.190.242.187:https TIME_WAIT
TCP   10.94.14.109:54564      203.190.242.172:https TIME_WAIT
TCP   10.94.14.109:54565      203.190.242.172:https TIME_WAIT
TCP   10.94.14.109:54566      203.190.242.172:https TIME_WAIT
TCP   10.94.14.109:54567      203.190.242.172:https TIME_WAIT
TCP   10.94.14.109:54568      203.190.242.172:https TIME_WAIT
TCP   10.94.14.109:54569      203.190.242.172:https TIME_WAIT
```

ca. Command Prompt

```
TCP   0.0.0.0:49667           DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:49668           DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:49669           DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:53228           DESKTOP-6Q502CS:0     LISTENING
TCP   10.94.14.109:139        DESKTOP-6Q502CS:0     LISTENING
TCP   10.94.14.109:54475      203.190.242.59:https  TIME_WAIT
TCP   10.94.14.109:54532      74.125.24.113:https   ESTABLISHED
TCP   10.94.14.109:54562      203.190.242.187:https TIME_WAIT
TCP   10.94.14.109:54563      203.190.242.187:https TIME_WAIT
TCP   10.94.14.109:54564      203.190.242.172:https TIME_WAIT
TCP   10.94.14.109:54565      203.190.242.172:https TIME_WAIT
TCP   10.94.14.109:54566      203.190.242.172:https TIME_WAIT
TCP   10.94.14.109:54567      203.190.242.172:https TIME_WAIT
TCP   10.94.14.109:54568      203.190.242.172:https TIME_WAIT
TCP   10.94.14.109:54569      203.190.242.172:https TIME_WAIT
TCP   10.94.14.109:54570      203.190.242.102:https TIME_WAIT
TCP   10.94.14.109:54571      203.190.242.102:https TIME_WAIT
TCP   10.94.14.109:54572      103.49.221.122:https  TIME_WAIT
TCP   10.94.14.109:54573      103.49.221.122:https  TIME_WAIT
TCP   10.94.14.109:54574      203.190.242.102:https TIME_WAIT
TCP   10.94.14.109:54575      103.49.221.115:https  TIME_WAIT
TCP   10.94.14.109:54576      103.49.221.115:https  TIME_WAIT
TCP   10.94.14.109:54577      203.190.242.102:https TIME_WAIT
TCP   10.94.14.109:54578      203.190.242.102:https TIME_WAIT
TCP   10.94.14.109:54579      203.190.242.102:https TIME_WAIT
TCP   10.94.14.109:54580      103.49.221.249:https  TIME_WAIT
TCP   10.94.14.109:54581      103.49.221.249:https  TIME_WAIT
^C
C:\Users\ASUS X453SA>
```

2. Stearming video melalui CMD.

CA Command Prompt

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\ASUS X453SA>netstat -a

Active Connections

Proto Local Address           Foreign Address         State
TCP   0.0.0.0:135             DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:445             DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:2508            DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:5357            DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:49664           DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:49665           DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:49666           DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:49667           DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:49668           DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:49669           DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:53228           DESKTOP-6Q502CS:0     LISTENING
TCP   10.94.14.109:139        DESKTOP-6Q502CS:0     LISTENING
TCP   10.94.14.109:54867      kul09s01-in-f3:https  TIME_WAIT
TCP   10.94.14.109:55022      a-0001:https          ESTABLISHED
TCP   10.94.14.109:55024      kul09s01-in-f3:http   ESTABLISHED
TCP   10.94.14.109:55025      kul09s01-in-f3:http   ESTABLISHED
TCP   10.94.14.109:55026      kul09s01-in-f3:https  ESTABLISHED
TCP   10.94.14.109:55027      74.125.24.156:https   ESTABLISHED
TCP   10.94.14.109:55028      74.125.24.156:https   ESTABLISHED
TCP   10.94.14.109:55029      74.125.24.94:https    ESTABLISHED
TCP   10.94.14.109:55030      74.125.24.94:https    ESTABLISHED
TCP   10.94.14.109:55031      74.125.24.132:https   ESTABLISHED
```

CA Command Prompt

```
Proto Local Address           Foreign Address         State
TCP   0.0.0.0:135             DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:445             DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:2508            DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:5357            DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:49664           DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:49665           DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:49666           DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:49667           DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:49668           DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:49669           DESKTOP-6Q502CS:0     LISTENING
TCP   0.0.0.0:53228           DESKTOP-6Q502CS:0     LISTENING
TCP   10.94.14.109:139        DESKTOP-6Q502CS:0     LISTENING
TCP   10.94.14.109:54867      kul09s01-in-f3:https  TIME_WAIT
TCP   10.94.14.109:55022      a-0001:https          ESTABLISHED
TCP   10.94.14.109:55024      kul09s01-in-f3:http   ESTABLISHED
TCP   10.94.14.109:55025      kul09s01-in-f3:http   ESTABLISHED
TCP   10.94.14.109:55026      kul09s01-in-f3:https  ESTABLISHED
TCP   10.94.14.109:55027      74.125.24.156:https   ESTABLISHED
TCP   10.94.14.109:55028      74.125.24.156:https   ESTABLISHED
TCP   10.94.14.109:55029      74.125.24.94:https    ESTABLISHED
TCP   10.94.14.109:55030      74.125.24.94:https    ESTABLISHED
TCP   10.94.14.109:55031      74.125.24.132:https   ESTABLISHED
TCP   10.94.14.109:55032      74.125.24.132:https   ESTABLISHED
TCP   10.94.14.109:55033      74.125.24.94:https    ESTABLISHED
TCP   10.94.14.109:55034      74.125.24.94:https    ESTABLISHED

^C
C:\Users\ASUS X453SA>
```