

Lakukan Capturing Data menggunakan Wireshark dan Netstat pada saat web browsing dan online streaming lalu analisis hasil tersebut.

Langkah pertama yang harus dilakukan saat capturing data adalah menginstal wireshark lalu buka browser dan pergi ke suatu web yang akan kita coba. Setelah itu jalan kan wireshark kurang lebih selama 2-3 menit. Lakukan hal yang sama dengan menggunakan command prompt. Begitu juga dengan saat online streaming , putar video lalu capturing data tersebut

Data yang di dapat dari hasil percobaan :

Browsing

Source	Destination	Info
IP Adress	IP Adress	
172.20.10.2	103.7.1.190	50648 → 80 [ACK] Seq=2425 Ack=362402 Win=64400 Len=0
172.20.10.2	94.31.29.55	50663 → 443 [RST] Seq=537 Win=0 Len=0
172.20.10.2	103.7.1.190	[TCP Dup ACK 4250#1] 50648 → 80 [ACK] Seq=2425 Ack=350114 Win=64400 Len=0
172.20.10.2	216.58.203.227	Client Hello
172.20.10.2	216.58.203.227	50670 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
172.20.10.2	54.231.114.169	50671 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1

IP Adress Source	172.20.10.2
IP Adress Destination	103.7.1.191
MAC Adress Source	ac:b5:7d:bd:8c:77
MAC Adress Destination	3a:af:61:7c:cf:64

Streaming

Source	Destination	Info
IP Adress	IP Adress	
172.20.10.2	54.230.156.179	[TCP Keep-Alive] 50929 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1
172.20.10.2	112.215.207.12	51112 → 443 [ACK] Seq=2 Ack=2 Win=1082 Len=0
172.20.10.2	172.20.10.15	Name query NB WPAD<00>
172.20.10.2	172.217.27.14	50944 → 80 [ACK] Seq=1 Ack=1 Win=258 Len=1
74.125.130.156	172.20.10.2	43 → 50993 [ACK] Seq=1 Ack=356 Win=811 Len=0
112.215.207.12	172.20.10.2	443 → 51111 [RST] Seq=2 Win=0 Len=0

IP Adress Source	172.20.10.2
IP Adress Destination	54.169.164.211
MAC Adress Source	ac:b5:7d:bd:8c:77
MAC Adress Destination	3a:af:61:7c:cf:64

Pada saat Browsing

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-SJT1HR9:50700	ESTABLISHED
TCP	127.0.0.1:15292	DESKTOP-SJT1HR9:0	LISTENING
TCP	127.0.0.1:49800	DESKTOP-SJT1HR9:0	LISTENING
TCP	127.0.0.1:50576	DESKTOP-SJT1HR9:50577	ESTABLISHED
TCP	127.0.0.1:50577	DESKTOP-SJT1HR9:50576	ESTABLISHED
TCP	127.0.0.1:50578	DESKTOP-SJT1HR9:50579	ESTABLISHED
TCP	127.0.0.1:50579	DESKTOP-SJT1HR9:50578	ESTABLISHED
TCP	127.0.0.1:50700	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	172.20.10.2:49787	d117158142:9100	ESTABLISHED
TCP	172.20.10.2:50317	50.7.182.181:http	ESTABLISHED
TCP	172.20.10.2:50581	112.215.161.34:http	ESTABLISHED
TCP	172.20.10.2:50582	ec2-35-161-157-65:https	ESTABLISHED
TCP	172.20.10.2:50584	117.18.237.29:http	ESTABLISHED
TCP	172.20.10.2:50585	117.18.237.29:http	TIME_WAIT
TCP	172.20.10.2:50589	sin11s01-in-f4:https	ESTABLISHED
TCP	172.20.10.2:50590	sb-in-f139:http	ESTABLISHED
TCP	172.20.10.2:50591	sb-in-f94:https	ESTABLISHED
TCP	172.20.10.2:50592	sin10s07-in-f97:https	ESTABLISHED
TCP	172.20.10.2:50593	sin11s03-in-f35:https	ESTABLISHED
TCP	172.20.10.2:50595	sb-in-f139:https	ESTABLISHED
TCP	172.20.10.2:50596	sa-in-f101:https	ESTABLISHED
TCP	172.20.10.2:50598	sc-in-f113:https	ESTABLISHED

Apply a display filter ... <Ctrl-/>

Time	Source	Destination	Protocol	Length	Info
4640	52.214835	172.20.10.2	TCP	54	50643 → 80 [ACK] Seq=1212 Ack=524198 Win=63376 Len=0
4638	52.211987	172.20.10.2	TCP	54	50670 → 443 [ACK] Seq=194 Ack=2801 Win=66048 Len=0
4635	52.211462	172.20.10.2	TCP	66	50671 → 80 [SVN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4633	52.203172	172.20.10.2	TCP	54	50642 → 80 [ACK] Seq=2071 Ack=335277 Win=64400 Len=0
4632	52.203137	172.20.10.2	TCP	54	[TCP Dup ACK 4631#1] 50642 → 80 [ACK] Seq=2071 Ack=333229 Win=64400 Len=0
4631	52.203106	172.20.10.2	TCP	54	50642 → 80 [ACK] Seq=2071 Ack=333229 Win=64400 Len=0
4630	52.203046	172.20.10.2	TCP	54	50642 → 80 [ACK] Seq=2071 Ack=331181 Win=63376 Len=0
4624	52.202196	172.20.10.2	TCP	54	50646 → 80 [ACK] Seq=2554 Ack=349069 Win=64400 Len=0
4623	52.202145	172.20.10.2	TCP	54	50642 → 80 [ACK] Seq=2071 Ack=330157 Win=64400 Len=0
4622	52.202021	172.20.10.2	TCP	54	50642 → 80 [ACK] Seq=2071 Ack=326061 Win=64400 Len=0
4612	52.200952	172.20.10.2	TCP	54	50646 → 80 [ACK] Seq=2554 Ack=344973 Win=64400 Len=0
4611	52.200899	172.20.10.2	TCP	54	50642 → 80 [ACK] Seq=2071 Ack=324013 Win=64400 Len=0
4610	52.200731	172.20.10.2	TCP	54	50646 → 80 [ACK] Seq=2554 Ack=339853 Win=64400 Len=0
4601	52.197910	172.20.10.2	TCP	54	[TCP Dup ACK 4600#1] 50646 → 80 [ACK] Seq=2554 Ack=337805 Win=64400 Len=0
4600	52.197838	172.20.10.2	TCP	54	50646 → 80 [ACK] Seq=2554 Ack=337805 Win=64400 Len=0
4599	52.197615	172.20.10.2	TCP	54	[TCP Dup ACK 4595#1] 50646 → 80 [ACK] Seq=2554 Ack=335757 Win=64400 Len=0
4595	52.196870	172.20.10.2	TCP	54	50646 → 80 [ACK] Seq=2554 Ack=335757 Win=64400 Len=0
4592	52.195756	172.20.10.2	TCP	54	50642 → 80 [ACK] Seq=2071 Ack=322989 Win=63376 Len=0

> Frame 4635: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

> Ethernet II, Src: Liteonte_bd:8c:77 (ac:b5:7d:bd:8c:77), Dst: 3a:af:61:7c:cf:64 (3a:af:61:7c:cf:64)

> Destination: 3a:af:61:7c:cf:64 (3a:af:61:7c:cf:64)

> Source: Liteonte_bd:8c:77 (ac:b5:7d:bd:8c:77)

Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 172.20.10.2, Dst: 54.231.114.169

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 52

Identification: 0x1e79 (7801)

> Flags: 0x02 (Don't Fragment)

Fragment offset: 0

Pada Saat Streaming

No.	Time	Source	Destination	Protocol	Length	Info
126	4.709523	172.20.10.2	172.20.10.15	NBNS	92	Name query NB WPAD<00>
127	4.710158	fe80::d091:f3f1:e35...	ff02::1:3	LLMNR	84	Standard query 0xe66c A wpad
128	4.710426	172.20.10.2	224.0.0.252	LLMNR	64	Standard query 0xe66c A wpad
129	5.128741	fe80::d091:f3f1:e35...	ff02::1:3	LLMNR	84	Standard query 0xe66c A wpad
130	5.128912	172.20.10.2	224.0.0.252	LLMNR	64	Standard query 0xe66c A wpad
131	5.145723	50.7.182.171	172.20.10.2	TCP	66	50451 → 51058 [ACK] Seq=1 Ack=2 Win=127 Len=0 SLE=1 SRE=2
132	5.146020	50.7.182.171	172.20.10.2	TCP	66	50451 → 51058 [ACK] Seq=1 Ack=2 Win=127 Len=0 SLE=1 SRE=2
133	5.473504	172.20.10.2	172.20.10.15	NBNS	92	Name query NB WPAD<00>
134	5.721477	172.20.10.2	50.7.182.181	HTTP	441	GET /wpad.dat?0a5afe9bbe643ce4538307a3d64b4ef125322783 HTTP/1.1
135	5.884792	203.117.158.142	172.20.10.2	TCP	55	9100 → 49787 [ACK] Seq=1 Ack=1 Win=255 Len=1
136	5.884849	172.20.10.2	203.117.158.142	TCP	66	49787 → 9100 [ACK] Seq=1 Ack=2 Win=253 Len=0 SLE=1 SRE=2
137	5.921841	112.215.207.12	172.20.10.2	TCP	54	443 → 51111 [FIN, ACK] Seq=1 Ack=1 Win=191 Len=0
138	5.921931	172.20.10.2	112.215.207.12	TCP	54	51111 → 443 [ACK] Seq=1 Ack=2 Win=4618 Len=0
139	5.922095	172.20.10.2	112.215.207.12	TLSv1.2	85	Encrypted Alert
140	5.922174	172.20.10.2	112.215.207.12	TCP	54	51111 → 443 [FIN, ACK] Seq=32 Ack=2 Win=4618 Len=0
141	5.971727	112.215.207.12	172.20.10.2	TCP	54	443 → 51111 [RST] Seq=2 Win=0 Len=0
142	5.971871	112.215.207.12	172.20.10.2	TCP	54	443 → 51111 [RST] Seq=2 Win=0 Len=0
143	6.186278	50.7.182.181	172.20.10.2	HTTP	233	HTTP/1.1 200 OK (application/x-ns-proxy-autoconfig)
144	6.238002	172.20.10.2	50.7.182.181	TCP	54	50317 → 80 [ACK] Seq=388 Ack=180 Win=255 Len=0
145	6.238083	172.20.10.2	172.20.10.15	NBNS	92	Name query NB WPAD<00>
146	8.169909	172.20.10.2	66.90.98.37	TCP	55	[TCP segment of a reassembled PDU]
147	8.216414	172.20.10.2	54.230.156.179	SSL	55	Continuation Data
148	8.264949	172.20.10.2	104.118.145.230	SSL	55	Continuation Data
149	8.311307	54.230.156.179	172.20.10.2	TCP	66	443 → 50929 [ACK] Seq=1 Ack=2 Win=150 Len=0 SLE=1 SRE=2
150	8.339067	104.118.145.230	172.20.10.2	TCP	66	443 → 50911 [ACK] Seq=1 Ack=2 Win=1131 Len=0 SLE=1 SRE=2
151	8.461333	172.20.10.2	66.90.98.37	TCP	55	[TCP segment of a reassembled PDU]

< Frame 1: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits) on interface 0

> Ethernet II, Src: Liteontel_bd:8c:77 (ac:b5:7d:bd:8c:77), Dst: 3a:af:61:7c:cf:64 (3a:af:61:7c:cf:64)

> Internet Protocol Version 4, Src: 172.20.10.2, Dst: 130.211.37.21

> Transmission Control Protocol, Src Port: 50878, Dst Port: 443, Seq: 1, Ack: 1, Len: 79

> Secure Sockets Layer

```

0000  3a af 61 7c cf 64 ac b5 7d bd 8c 77 08 00 45 00  :a|.d...}.w..E.
0010  00 77 0a 4b 40 00 80 06 92 37 ac 14 0a 02 82 d3  .w.k@...7.....
0020  25 15 c6 be 01 bb 51 55 26 3b b2 e9 d6 68 50 18  %. ....QU & ;...hp.
0030  01 01 dd e8 00 00 17 03 03 00 4a 00 00 00 00 00  .....J.....
    
```

```

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-SJT1HR9:50840 ESTABLISHED
TCP 127.0.0.1:15292 DESKTOP-SJT1HR9:0 LISTENING
TCP 127.0.0.1:49800 DESKTOP-SJT1HR9:0 LISTENING
TCP 127.0.0.1:50840 DESKTOP-SJT1HR9:1688 ESTABLISHED
TCP 127.0.0.1:50841 DESKTOP-SJT1HR9:50842 ESTABLISHED
TCP 127.0.0.1:50842 DESKTOP-SJT1HR9:50841 ESTABLISHED
TCP 127.0.0.1:50843 DESKTOP-SJT1HR9:50844 ESTABLISHED
TCP 127.0.0.1:50844 DESKTOP-SJT1HR9:50843 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 172.20.10.2:49787 d117158142:9100 ESTABLISHED
TCP 172.20.10.2:50317 50.7.182.181:http ESTABLISHED
TCP 172.20.10.2:50825 104.41.207.73:https ESTABLISHED
TCP 172.20.10.2:50826 50.7.182.181:http TIME_WAIT
TCP 172.20.10.2:50827 50.7.182.181:http TIME_WAIT
TCP 172.20.10.2:50828 50.7.182.181:http TIME_WAIT
TCP 172.20.10.2:50829 50.7.182.181:http TIME_WAIT
TCP 172.20.10.2:50830 sa-in-f94:https TIME_WAIT
TCP 172.20.10.2:50831 sin11s02-in-f10:https TIME_WAIT
TCP 172.20.10.2:50835 sin11s03-in-f35:https TIME_WAIT
TCP 172.20.10.2:50838 sa-in-f84:https TIME_WAIT
TCP 172.20.10.2:50839 sin11s03-in-f4:https TIME_WAIT
TCP 172.20.10.2:50846 112.215.161.34:http ESTABLISHED
TCP 172.20.10.2:50847 ec2-52-40-210-31:https ESTABLISHED
TCP 172.20.10.2:50849 117.18.237.29:http ESTABLISHED
TCP 172.20.10.2:50850 117.18.237.29:http TIME_WAIT
TCP 172.20.10.2:50851 sc-in-f190:https ESTABLISHED
TCP 172.20.10.2:50852 sin11s02-in-f14:http ESTABLISHED
TCP 172.20.10.2:50853 sb-in-f113:https ESTABLISHED

```

Dari screenshot diatas kita ketahui bahwa data di wireshark lebih complete dan lebih rumit. Sedangkan pada netstat hanya menampilkan tujuan atau rute yang dilalui oleh data tersebut. dan kita tidak tau apa proses yang terjadi dan hubungan seperti apa , tapi dalam wireshark semua data bisa di dapatkan dengan sangat jelas dan rinci.