

Menganalisa ip dan MAC

menggunakan WIRESHARK dan CMD

TUGAS JARINGAN KOMPUTER SK5C(SISTEM
KOMPUTER_FASILKOM/2015_UNSRI) BY
HENNYPRATIWI_09011281520129

Menganalisa ip dan MAC menggunakan WIRESHARK dan CMD

Tugas Jaringan Komputer SK5C(Sistem Komputer_FASILKOM/2015_UNSRI) by HennyPratiwi_09011281520129

SOAL :

1. Instalah aplikasi wireshark
2. Capture data pada wireshark dan cmd saat online 3-5 menit
3. Dengan kasus :
 - a. Kompas.com(web browsing)
 - b. m.viva.co.id/tvone/live(live streaming)
4. Carilah (IP,MAC) source dan (IP,MAC) destination, buat dengan table di excel.
5. Format file pdf dan upload di edocs.ilkom.unsri.ac.id

JAWAB :

1. Buka aplikasi wireshark dan cmd kemudian browsing kasus selama 3-5 menit
2. Pada kolom filter di aplikasi wharshark ketik (ip.src == 192.168.43.91) maka akan muncul data ip source saja kemudian capture data seperti dibawah, klik pada list biru tua seperti digambar maka dibawahnya akan tampil MAC(Ethernet II) dan IP versi 4 :

The screenshot shows the Wireshark interface with a filter set to 'ip.src == 192.168.43.91'. The packet list pane displays various network protocols including SSL, TCP, DNS, and HTTP. Packet 34 is selected, and the packet details pane shows the following information:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.43.91	34.209.12.3	SSL	55	Continuation Data
2	1.000999000	192.168.43.91	34.209.12.3	TCP	55	[TCP Keep-Alive] 55835 > https [ACK] Seq=1 Ack=1 win=261 Len=1
6	4.269011000	192.168.43.91	192.168.43.1	DNS	70	Standard query 0x9d21 A kompas.com
7	4.284307000	192.168.43.91	192.168.43.1	DNS	74	Standard query 0x6b39 A www.kompas.com
8	4.427335000	192.168.43.91	192.168.43.1	DNS	70	Standard query 0x9d21 A kompas.com
9	4.443429000	192.168.43.91	192.168.43.1	DNS	74	Standard query 0x6b39 A www.kompas.com
11	4.742646000	192.168.43.91	202.146.4.100	TCP	66	55840 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
12	4.743898000	192.168.43.91	192.168.43.1	DNS	70	Standard query 0x5ce6 A kompas.com
14	4.746405000	192.168.43.91	192.168.43.1	DNS	70	Standard query 0xe9ae AAAA kompas.com
16	4.750393000	192.168.43.91	202.61.113.35	TCP	66	55841 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
17	4.751400000	192.168.43.91	192.168.43.1	DNS	74	Standard query 0xfe48 A www.kompas.com
19	4.755530000	192.168.43.91	192.168.43.1	DNS	74	Standard query 0x0b5d AAAA www.kompas.com
23	4.824905000	192.168.43.91	202.146.4.100	TCP	54	55840 > http [ACK] Seq=1 Ack=1 win=64860 Len=0
24	4.825890000	192.168.43.91	202.61.113.35	TCP	66	55842 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
26	4.843202000	192.168.43.91	202.61.113.35	TCP	54	55841 > http [ACK] Seq=1 Ack=1 win=65189 Len=0
27	4.843624000	192.168.43.91	202.61.113.35	TCP	1441	[TCP segment of a reassembled PDU]
28	4.843678000	192.168.43.91	202.61.113.35	HTTP	143	GET / HTTP/1.1
30	4.912013000	192.168.43.91	202.61.113.35	TCP	54	55842 > http [ACK] Seq=1 Ack=1 win=65189 Len=0
34	4.944173000	192.168.43.91	202.61.113.35	TCP	66	[TCP Dup ACK 28#1] 55841 > http [ACK] Seq=1477 Ack=1 win=65189 Len=0 SLE=1388 SRE=2775
35	4.951459000	192.168.43.91	111.221.29.136	TLSv1	107	Application Data
37	4.963127000	192.168.43.91	202.61.113.35	TCP	66	[TCP Dup ACK 28#2] 55841 > http [ACK] Seq=1477 Ack=1 win=65189 Len=0 SLE=1388 SRE=4162
39	5.025340000	192.168.43.91	202.61.113.35	TCP	54	55841 > http [ACK] Seq=1477 Ack=4162 win=65189 Len=0
43	5.077590000	192.168.43.91	202.61.113.35	TCP	54	55841 > http [ACK] Seq=1477 Ack=6936 win=65189 Len=0
44	5.126897000	192.168.43.91	111.221.29.136	TCP	54	55802 > https [ACK] Seq=54 Ack=139 win=260 Len=0
46	5.149290000	192.168.43.91	202.61.113.35	TCP	66	[TCP Dup ACK 43#1] 55841 > http [ACK] Seq=1477 Ack=6936 win=65189 Len=0 SLE=9710 SRE=11097
48	5.163094000	192.168.43.91	202.61.113.35	TCP	66	[TCP Dup ACK 43#2] 55841 > http [ACK] Seq=1477 Ack=6936 win=65189 Len=0 SLE=8323 SRE=11097

Frame 34: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: 80:a5:89:55:4a:45 (80:a5:89:55:4a:45), Dst: 18:89:5b:7f:e6:75 (18:89:5b:7f:e6:75)
Internet Protocol Version 4, Src: 192.168.43.91 (192.168.43.91), Dst: 202.61.113.35 (202.61.113.35)
Transmission Control Protocol, Src Port: 55841 (55841), Dst Port: http (80), Seq: 1477, Ack: 1, Len: 0

Wireshark kompas.com

No.	Time	Source	Destination	Protocol	Length	Info
122	7.208199000	192.168.43.91	192.168.43.1	DNS	73	Standard query 0x1379 AAAA traffic.em.io
125	7.233044000	192.168.43.91	128.199.79.195	TCP	54	58248 > http [ACK] Seq=1461 Ack=6971 win=16728 Len=0
128	7.235167000	192.168.43.91	192.168.43.1	DNS	89	Standard query 0x0cbc A d31qbv1cthcecs.cloudfront.net
129	7.235167000	192.168.43.91	192.168.43.1	DNS	82	Standard query 0x8a18 A viva.api.sociaplus.com
131	7.235773000	192.168.43.91	128.199.79.195	TCP	66	[TCP Dup ACK 125#1] 58248 > http [ACK] Seq=1461 Ack=6971 win=16728 Len=0 SLE=8365 SRE=8968
134	7.238897000	192.168.43.91	192.168.43.1	DNS	89	Standard query 0xa887 AAAA d31qbv1cthcecs.cloudfront.net
135	7.238967000	192.168.43.91	192.168.43.1	DNS	82	Standard query 0xebe1 AAAA viva.api.sociaplus.com
137	7.248444000	192.168.43.91	128.199.79.195	TCP	54	58248 > http [ACK] Seq=1461 Ack=8968 win=16728 Len=0
139	7.272129000	192.168.43.91	192.168.43.1	DNS	88	Standard query 0x6340 A d5nxst8fruw4z.cloudfront.net
141	7.296376000	192.168.43.91	192.168.43.1	DNS	89	Standard query 0xd820 A cloudfront-labs.amazonaws.com
143	7.336498000	192.168.43.91	128.199.79.195	TCP	66	58455 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
144	7.337377000	192.168.43.91	128.199.79.195	TCP	66	58456 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
145	7.337924000	192.168.43.91	128.199.79.195	TCP	66	58457 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
147	7.338463000	192.168.43.91	192.168.43.1	DNS	80	Standard query 0x9ea9 A engine.wideworld.com
148	7.341943000	192.168.43.91	192.168.43.1	DNS	88	Standard query 0x933f A d5nxst8fruw4z.cloudfront.net
150	7.344896000	192.168.43.91	192.168.43.1	DNS	88	Standard query 0x6f21 AAAA d5nxst8fruw4z.cloudfront.net
151	7.355108000	192.168.43.91	128.199.79.195	TCP	66	58458 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
152	7.356808000	192.168.43.91	128.199.79.195	TCP	66	58459 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
153	7.357285000	192.168.43.91	128.199.79.195	TCP	66	58460 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
155	7.438973000	192.168.43.91	192.168.43.1	DNS	89	Standard query 0x949f A cloudfront-labs.amazonaws.com
158	7.441858000	192.168.43.91	192.168.43.1	DNS	80	Standard query 0x3508 A engine.wideworld.com
160	7.442586000	192.168.43.91	192.168.43.1	DNS	89	Standard query 0x4f40 AAAA cloudfront-labs.amazonaws.com
162	7.444924000	192.168.43.91	192.168.43.1	DNS	80	Standard query 0x0e18 AAAA engine.wideworld.com
164	7.456244000	192.168.43.91	128.199.79.195	TCP	54	58287 > http [ACK] Seq=2 Ack=2 Win=16450 Len=0
165	7.456369000	192.168.43.91	128.199.79.195	TCP	54	58287 > http [FIN, ACK] Seq=2 Ack=2 Win=16450 Len=0
167	7.487585000	192.168.43.91	128.199.79.195	TCP	54	58455 > http [ACK] Seq=1 Ack=1 Win=66917 Len=0

[Frame 131: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
 Ethernet II, Src: 80:a5:89:55:4a:45 (80:a5:89:55:4a:45), Dst: 18:89:5b:7f:e6:75 (18:89:5b:7f:e6:75)
 Internet Protocol Version 4, Src: 192.168.43.91 (192.168.43.91), Dst: 128.199.79.195 (128.199.79.195)
 Transmission Control Protocol, Src Port: 58248 (58248), Dst Port: http (80), Seq: 1461, Ack: 6971, Len: 0

Wireshark m.viva.co.id/tvone/live

3. Pada cmd di komputer ketik “netstat -a” (tampa tanda petik),

```

TCP        127.0.0.1:5354          bandicam:49668      ESTABLISHED
TCP        127.0.0.1:5354          bandicam:49669      ESTABLISHED
TCP        127.0.0.1:9990          DESKTOP-1VABD9S:0  LISTENING
TCP        127.0.0.1:23409        DESKTOP-1VABD9S:0  LISTENING
TCP        127.0.0.1:27015        DESKTOP-1VABD9S:0  LISTENING
TCP        127.0.0.1:27015        bandicam:55720      ESTABLISHED
TCP        127.0.0.1:49668        bandicam:5354       ESTABLISHED
TCP        127.0.0.1:49669        bandicam:5354       ESTABLISHED
TCP        127.0.0.1:55720        bandicam:27015      ESTABLISHED
TCP        127.0.0.1:55761        bandicam:55762      ESTABLISHED
TCP        127.0.0.1:55762        bandicam:55761      ESTABLISHED
TCP        127.0.0.1:55768        bandicam:55769      ESTABLISHED
TCP        127.0.0.1:55769        bandicam:55768      ESTABLISHED
TCP        192.168.43.91:139      DESKTOP-1VABD9S:0  LISTENING
TCP        192.168.43.91:55728    hk2sch130021236:https ESTABLISHED
TCP        192.168.43.91:55745    hk2sch130021456:https ESTABLISHED
TCP        192.168.43.91:55758    hk2sch130021035:https ESTABLISHED
TCP        192.168.43.91:55802    hk2sch130021623:https ESTABLISHED
TCP        192.168.43.91:55834    202.70.49.139:http  ESTABLISHED
TCP        192.168.43.91:55835    ec2-34-209-12-3:https TIME_WAIT
TCP        192.168.43.91:55837    server-54-192-151-127:https TIME_WAIT
TCP        192.168.43.91:55838    server-54-192-151-127:https TIME_WAIT
TCP        192.168.43.91:55839    server-54-192-151-127:https TIME_WAIT
TCP        192.168.43.91:55840    202.146.4.100:http  TIME_WAIT
TCP        192.168.43.91:55841    202.61.113.35:http  ESTABLISHED
TCP        192.168.43.91:55842    202.61.113.35:http  TIME_WAIT
TCP        192.168.43.91:55843    sa-in-f95:https     ESTABLISHED
TCP        192.168.43.91:55844    xx-fbcdn-shv-01-sit4:https ESTABLISHED
  
```

CMD kompas.com

```

TCP 127.0.0.1:58232 bandicam:58233 ESTABLISHED
TCP 127.0.0.1:58233 bandicam:58232 ESTABLISHED
TCP 127.0.0.1:58237 bandicam:58238 ESTABLISHED
TCP 127.0.0.1:58238 bandicam:58237 ESTABLISHED
TCP 192.168.43.91:139 DESKTOP-1VABD9S:0 LISTENING
TCP 192.168.43.91:58208 hk2sch130022129:https ESTABLISHED
TCP 192.168.43.91:58210 hk2sch130021535:https ESTABLISHED
TCP 192.168.43.91:58211 hk2sch130021336:https ESTABLISHED
TCP 192.168.43.91:58212 hk2sch130021327:https ESTABLISHED
TCP 192.168.43.91:58234 23.99.125.126:https FIN_WAIT_1
TCP 192.168.43.91:58235 111.221.29.254:https TIME_WAIT
TCP 192.168.43.91:58240 202.70.49.153:http TIME_WAIT
TCP 192.168.43.91:58248 128.199.79.195:http ESTABLISHED
TCP 192.168.43.91:58249 sin10s07-in-f8:https ESTABLISHED
TCP 192.168.43.91:58253 sa-in-f95:https ESTABLISHED
TCP 192.168.43.91:58255 ams15s29-in-f110:https ESTABLISHED
TCP 192.168.43.91:58261 sc-in-f157:https ESTABLISHED
TCP 192.168.43.91:58266 sin10s07-in-f8:https TIME_WAIT
TCP 192.168.43.91:58267 sc-in-f157:http TIME_WAIT
TCP 192.168.43.91:58270 sb-in-f139:http ESTABLISHED
TCP 192.168.43.91:58272 sb-in-f139:http ESTABLISHED
TCP 192.168.43.91:58274 ec2-35-167-220-41:https TIME_WAIT
TCP 192.168.43.91:58275 sb-in-f139:http ESTABLISHED
TCP 192.168.43.91:58276 sb-in-f139:http ESTABLISHED
TCP 192.168.43.91:58277 sb-in-f139:http ESTABLISHED
TCP 192.168.43.91:58282 ec2-54-255-203-16:http TIME_WAIT
TCP 192.168.43.91:58290 117.18.237.29:http TIME_WAIT
TCP 192.168.43.91:58291 128.199.79.195:http TIME_WAIT
TCP 192.168.43.91:58292 128.199.79.195:http TIME_WAIT
TCP 192.168.43.91:58293 117.18.237.29:http TIME_WAIT

```

CMD m.viva.co.id/tvone/live

4. Untuk melihat MAC source di CMD kita bisa menggunakan “ipconfig /all”(tampa petik)

```

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . :
Description . . . . . : Qualcomm Atheros AR956x Wireless Network Adapter
Physical Address. . . . . : 80-A5-89-55-4A-45
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::464:b6b:aa38:7ced%7(Preferred)
IPv4 Address. . . . . : 192.168.43.91(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, August 29, 2017 7:12:11 AM
Lease Expires . . . . . : Tuesday, August 29, 2017 9:00:12 AM
Default Gateway . . . . . : 192.168.43.1
DHCP Server . . . . . : 192.168.43.1
DHCPv6 IAID . . . . . : 92317065
DHCPv6 Client DUID. . . . . : 00-01-00-01-1E-CD-24-E1-2C-56-DC-7F-4A-01
DNS Servers . . . . . : 192.168.43.1
NetBIOS over Tcpi. . . . . : Enabled

```

CMD kompas.com dan m.viva.co.id/tvone/live

5. Dari data diatas dapat kita analisa dalam bentuk table dibawah ini :

a. Kompas.com(web browsing) :

IP	192.168.43.91
MAC	80:a5:89:55:4a:45

Source

IP	202.61.113.35
MAC	18:89:5b:7f:e6:75

Destination

b. m.viva.co.id/tvone/live(live streaming)

IP	192.168.43.91
MAC	80:a5:89:55:4a:45

Source

IP	128.199.79.195
MAC	18:89:5b:7f:e6:75

Destination