

JARINGAN KOMPUTER



Disusun Oleh :

Nama : Febrina Setianingsih

NIM : 09011181419021

Dosen Pembimbing :

Dr. Deris Stiawan, M.T., Ph.D.

**SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA**

Analisa Frame dari Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	10.100.224.145	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
2	0.19502500	10.100.227.14	10.100.239.255	NBNS	92	Name query NB WPAD=00-
3	0.19503400	Fe80::74F8:fc0e:b46ff02::1:3		LLMNR	84	Standard query 0x485f A wpad
4	0.19594900	10.100.227.14	224.0.0.252	LLMNR	64	Standard query 0x485f A wpad
5	0.19693100	Fe80::74F8:fc0e:b46ff02::1:3		LLMNR	84	Standard query 0x1cfa AAAA wpad
6	0.19693600	10.100.227.14	224.0.0.252	LLMNR	64	Standard query 0x1cfa AAAA wpad
7	0.60313200	Fe80::74F8:fc0e:b46ff02::1:3		LLMNR	84	Standard query 0x485f A wpad
8	0.60313900	Fe80::74F8:fc0e:b46ff02::1:3		LLMNR	84	Standard query 0x1cfa AAAA wpad
9	0.60314300	10.100.227.14	224.0.0.252	LLMNR	64	Standard query 0x485f A wpad
10	0.60314500	10.100.227.14	224.0.0.252	LLMNR	64	Standard query 0x1cfa AAAA wpad
11	0.75312700	10.100.225.197	52.1.10.2	TCP	54	49931→80 [FIN, ACK] Seq=1 Ack=1 Win=1020 Len=0
12	0.91515700	Liteonte_c0:ce:d2	Broadcast	ARP	60	who has 10.100.224.1? Tell 10.100.225.205
13	0.92214400	10.100.227.14	10.100.239.255	NBNS	92	Name query NB WPAD=00-
14	1.01290100	Fe80::7c7c:8061:b93ff02::1:3		LLMNR	84	Standard query 0x1a00 ANY asus
15	1.02012300	23.21.57.51	10.100.225.197	SSL	727	continuation data
16	1.11713700	10.100.225.197	23.21.57.51	TCP	54	49980→443 [ACK] Seq=1 Ack=674 Win=1021 Len=0
17	1.12113700	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x97df637
18	1.21820900	Fe80::7c7c:8061:b93ff02::1:3		LLMNR	84	Standard query 0x0327 ANY asus
19	1.22012005	10.100.225.205	224.0.0.252	LLMNR	64	Standard query 0x0327 ANY asus
20	1.41621000	10.100.225.197	52.1.10.2	TCP	54	49932→80 [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0
21	1.78225000	10.100.227.14	10.100.239.255	NBNS	92	Name query NB WPAD=00-
22	1.93828100	Liteonte_c0:ce:d2	Broadcast	ARP	60	who has 10.100.225.205? Tell 0.0.0.0
23	1.93828800	Fe80::7c7c:8061:b93ff02::1:3		ICMPv6	86	Neighbor Advertisement fe80::7c7c:8061:b93a:4ac5 (ovr) is at ac:b5:7d:c0:ce:d2
24	2.57986200	173.222.148.42	10.100.225.197	TLSv1	603	Application Data
25	2.97035300	Liteonte_c0:ce:d2	Broadcast	ARP	60	who has 10.100.225.205? Tell 0.0.0.0
26	2.97134800	10.100.224.167	224.0.0.251	MDNS	103	standard query 0x0000 PTR _233637De._sub._googlecast._tcp.local, "qm" question PTR _googlecast.tc
27	3.36843500	173.222.148.42	10.100.225.197	TLSv1	91	Encrypted Alert
28	3.38717700	10.100.225.197	23.21.57.51	TLSv1	848	Application Data, Application Data
29	3.54444800	23.21.57.51	10.100.225.197	TCP	1514	[TCP segment of a reassembled PDU]
30	3.98369000	Liteonte_c0:ce:d2	Broadcast	ARP	60	Gratuitous ARP for 10.100.225.205 (Request)
31	4.30152800	10.100.225.63	224.0.0.252	LLMNR	64	Standard query 0x6300 AAAA wpad
32	4.51064300	10.100.225.63	23.21.57.51	TLSv1	548	[TCP Retransmission] Application Data, Application Data
33	4.70565600	Samsung_Ef6199:61	Broadcast	ARP	60	who has 10.100.224.1? Tell 10.100.226.170
34	4.70566300	Fe80::f8b1:2ddd:17eff02::1:3		LLMNR	84	Standard query 0x6743 A wpad
35	4.70668600	10.100.225.63	224.0.0.252	LLMNR	64	Standard query 0x6743 A wpad
36	4.70669100	Fe80::f8b1:2ddd:17eff02::1:3		LLMNR	84	Standard query 0x6300 AAAA wpad
37	4.70750000	10.100.225.63	224.0.0.252	LLMNR	64	Standard query 0x6300 AAAA wpad
38	4.91418300	23.21.57.51	10.100.225.197	TCP	54	49965→443 [ACK] Seq=38 Ack=39 Win=1021 Len=0
39	4.98969300	207.244.65.147	10.100.225.197	TLSv1	91	Encrypted Alert
40	4.98970000	207.244.65.147	10.100.225.197	TCP	54	443→49965 [FIN, ACK] Seq=38 Ack=1 Win=10 Len=0
41	4.99003500	10.100.225.197	207.244.65.147	TCP	54	49963→443 [ACK] Seq=1 Ack=39 Win=1021 Len=0
42	5.00568000	Quantum_Lib:b9:ee	Broadcast	ARP	60	who has 10.100.224.1? Tell 10.100.225.229
43	5.06876200	207.244.65.147	10.100.225.197	TLSv1	91	Encrypted Alert
44	5.06877000	207.244.65.147	10.100.225.197	TCP	54	443→49965 [FIN, ACK] Seq=38 Ack=1 Win=10 Len=0
45	5.06916600	10.100.225.197	207.244.65.147	TCP	54	49965→443 [ACK] Seq=1 Ack=39 Win=1022 Len=0
46	5.11163800	10.100.225.63	10.100.239.255	NBNS	92	Name query NB WPAD=00-
47	5.31767500	10.100.225.205	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
48	5.82572700	10.100.225.63	10.100.239.255	NBNS	92	Name query NB WPAD=00-
49	6.03186800	10.100.225.205	10.100.239.255	NBNS	92	Name query NB WPAD=00-
50	6.03187800	Fe80::7c7c:8061:b93ff02::1:3		LLMNR	84	Standard query 0xc641 A wpad
51	6.34681500	Fe80::7c7c:8061:b93ff02::1:3		LLMNR	84	Standard query 0xc641 A wpad
52	6.34682300	10.100.225.205	224.0.0.252	LLMNR	64	Standard query 0xc641 A wpad
53	6.54575700	10.100.225.205	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
54	6.74208000	10.100.225.205	10.100.239.255	NBNS	92	Name query NB WPAD=00-
55	6.90364800	10.100.225.197	209.190.38.141	TLSv1	832	Application Data, Application Data
56	6.95008600	10.100.225.205	10.100.239.255	NBNS	92	Name query NB EREXOXIVKTYER<00-
57	6.95009200	10.100.225.205	10.100.239.255	NBNS	92	Name query NB FOBASFWNETP<00-
58	6.95081700	Fe80::7c7c:8061:b93ff02::1:3		LLMNR	92	Standard query 0x229c A fobasfwmetp
59	6.95405000	Fe80::7c7c:8061:b93ff02::1:3		LLMNR	94	Standard query 0x515d A erexoxivktyer
60	6.95405800	Fe80::7c7c:8061:b93ff02::1:3		LLMNR	93	Standard query 0x9f20 A azrxxvixxfasd

Gambar diatas merupakan hasil capture traffic packet data dengan menggunakan wireshark. Semua jenis paket informasi dalam berbagai format protokol dapat ditangkap dan dianalisa kinerja jaringannya. Wireshark akan menampilkan semua informasi tentang paket yang keluar dan masuk dalam interface yang telah dipilih. Pertama kita harus mengaktifkan wireshark setelah itu kita membuka browser kemudian mengetikkan alamat yang kita inginkan, misalnya www.cisco.com maka wireshark akan mengcapture packet secara lengkap. Pada panel ini berisi nomor paket, waktu saat paket di capture, sumber dan tujuan dari paket, protokol yang digunakan dan panjangnya, serta informasi dari hasil filter paket.

ANALISA PROTOCOL HTTP (GET)

3833 129.972078 10.100.225.197 23.15.100.240 HTTP 474 GET /utag/cisco/cdc/prod/utag.2311.js?utv=ut4.42.201609061332 HTTP/1.1

Sebuah permintaan GET mengambil data dari web server dengan menentukan parameter di bagian URL dari permintaan.

1. MAC Address

Source MAC Address

= HonHaiPr_70:2a:e3 (e0:06:e6:70:2a:e3)

```
Frame 3833: 474 bytes on wire (3792 bits), 474 bytes captured (3792 bits) on interface 0
Interface id: 0 (\Device\NPF_{2CC53754-422C-42C1-8AED-AEE6C55794AE})
Encapsulation type: Ethernet (1)
Arrival Time: Sep 16, 2016 13:50:58.467674000 SE Asia Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1474008658.467674000 seconds
[Time delta from previous captured frame: 0.038554000 seconds]
[Time delta from previous displayed frame: 0.038554000 seconds]
[Time since reference or first frame: 129.972078000 seconds]
Frame Number: 3833
Frame Length: 474 bytes (3792 bits)
Capture Length: 474 bytes (3792 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http]
[Number of per-protocol-data: 1]
[Hypertext Transfer Protocol, key 0]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: HonHaiPr_70:2a:e3 (e0:06:e6:70:2a:e3), Dst: Compex_22:cf:fa (00:80:48:22:cf:fa)
  Destination: Compex_22:cf:fa (00:80:48:22:cf:fa)
    Address: Compex_22:cf:fa (00:80:48:22:cf:fa)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Source: HonHaiPr_70:2a:e3 (e0:06:e6:70:2a:e3)
    Address: HonHaiPr_70:2a:e3 (e0:06:e6:70:2a:e3)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
Type: IP (0x0800)
```

Destination MAC Address

= Compex_22:cf:fa (00:80:48:22:cf:fa)

```
Ethernet II, Src: HonHaiPr_70:2a:e3 (e0:06:e6:70:2a:e3), Dst: Compex_22:cf:fa (00:80:48:22:cf:fa)
  Destination: Compex_22:cf:fa (00:80:48:22:cf:fa)
    Address: Compex_22:cf:fa (00:80:48:22:cf:fa)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Source: HonHaiPr_70:2a:e3 (e0:06:e6:70:2a:e3)
    Address: HonHaiPr_70:2a:e3 (e0:06:e6:70:2a:e3)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
Type: IP (0x0800)
```

2. IP Address

Source IP Address

= 10:100:225:197

```
Internet Protocol Version 4, Src: 10.100.225.197 (10.100.225.197), Dst: 23.15.100.240 (23.15.100.240)
Version: 4
Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-capable Transport))
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    ....00 = Explicit Congestion Notification: Not-ECT (Not ECN-capable Transport) (0x00)
Total Length: 460
Identification: 0x1bae (7086)
  Flags: 0x02 (Don't Fragment)
    0... .... = Reserved bit: Not set
    .1.. .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
  Header checksum: 0x7555 [validation disabled]
    [Good: False]
    [Bad: False]
Source: 10.100.225.197 (10.100.225.197)
Destination: 23.15.100.240 (23.15.100.240)
[Source GeoIP: unknown]
[Destination GeoIP: unknown]
```

Destination IP Address

= 23.15.100.240

```
Internet Protocol Version 4, Src: 10.100.225.197 (10.100.225.197), Dst: 23.15.100.240 (23.15.100.240)
  Version: 4
  Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... 0000 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 460
  Identification: 0x1bae (7086)
  Flags: 0x02 (Don't Fragment)
    0... .... = Reserved bit: Not set
    .1.. .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 128
  Protocol: TCP (6)
  Header checksum: 0x7555 [validation disabled]
    [Good: False]
    [Bad: False]
  Source: 10.100.225.197 (10.100.225.197)
  Destination: 23.15.100.240 (23.15.100.240)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
```

3. Ukuran L2 dan L3

L2 (Layer 2)

Pada layer 2 terdapat alamat fisik. Alamat fisik adalah sistem pengalamatan pada jaringan komputer yang dikenal dengan nama Media Access Control Address (MAC address). MAC Address merupakan sistem pengalamatan yang menggunakan metode 48 bit. Alamat ini terletak pada Ethernet II. Ukuran pada layer ini adalah 14 byte. Dapat dilihat pada gambar

```
Ethernet II, Src: HonHaiPr_70:2a:e3 (e0:06:e6:70:2a:e3), Dst: Compex_22:cf:fa (00:80:48:22:cf:fa)
  Destination: Compex_22:cf:fa (00:80:48:22:cf:fa)
  Address: Compex_22:cf:fa (00:80:48:22:cf:fa)
    .... 00. .... = LG bit: Globally unique address (factory default)
    .... 0000 .... = IG bit: Individual address (unicast)
  Source: HonHaiPr_70:2a:e3 (e0:06:e6:70:2a:e3)
  Address: HonHaiPr_70:2a:e3 (e0:06:e6:70:2a:e3)
    .... 00. .... = LG bit: Globally unique address (factory default)
    .... 0000 .... = IG bit: Individual address (unicast)
  Type: IP (0x0800)
```

Pada gambar dapat dilihat bahwa pada Ethernet II terdiri dari :

- DA (Destination MAC Address) yang memiliki panjang 6 byte
- SA (Source MAC Address) yang memiliki panjang yang sama yaitu 6 byte, dan
- Type (Type Ethernet) sepanjang 2 byte.

Jadi, pada Ethernet II ini memiliki ukuran 14 byte.

L3 (Layer 3)

Pada Layer 3 atau Network layer terdapat alamat logika. Alamat logika menggunakan sebuah aturan atau metode yang dikenal dengan nama Internet Protocol address (IP address). Saat ini IP address terdiri atas dua versi yaitu IPv4 dan IPv6. Yang terdapat pada wireshark ini yaitu IPv4. Ukuran layer ini dapat dilihat pada total length-nya yaitu sebesar 460 byte.

```
Internet Protocol Version 4, Src: 10.100.225.197 (10.100.225.197), Dst: 23.15.100.240 (23.15.100.240)
  Version: 4
  Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 460
  Identification: 0x1bae (7086)
  Flags: 0x02 (Don't Fragment)
    0.. ... = Reserved bit: Not set
    .1. ... = Don't fragment: Set
    ..0. ... = More fragments: Not set
  Fragment offset: 0
  Time to live: 128
  Protocol: TCP (6)
  Header checksum: 0x7555 [validation disabled]
    [Good: False]
    [Bad: False]
  Source: 10.100.225.197 (10.100.225.197)
  Destination: 23.15.100.240 (23.15.100.240)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

4. Protocol

Protocol yang digunakan pada proses ini adalah protokol HTTP (Hyper Text Transfer Protocol).

```
Transmission Control Protocol, Src Port: 50095 (50095), Dst Port: 80 (80), Seq: 811, Ack: 48117, Len: 420
  Source Port: 50095 (50095)
  Destination Port: 80 (80)
  [Stream index: 138]
  [TCP segment Len: 420]
  Sequence number: 811 (relative sequence number)
  [Next sequence number: 1231 (relative sequence number)]
  Acknowledgment number: 48117 (relative ack number)
  Header Length: 20 bytes
  ... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    ... 0... .... = Congestion window Reduced (cwr): Not set
    ... .0.. .... = ECN-Echo: Not set
    ... ..0. .... = Urgent: Not set
    ... ...1 .... = Acknowledgment: set
    ... .... 1... = Push: Set
    ... .... .0. = Reset: Not set
    ... .... .0. = Syn: Not set
    ... .... .0. = Fin: Not set
  window size value: 1024
  [calculated window size: 262144]
  [window size scaling factor: 256]
  Checksum: 0xa4f5 [validation disabled]
    [Good Checksum: False]
    [Bad Checksum: False]
  Urgent pointer: 0
  [SEQ/ACK analysis]
    [iRTT: 0.019719000 seconds]
    [Bytes in Flight: 420]
```

```

Hypertext Transfer Protocol
  GET /utag/cisco/cdc/prod/utag.2311.js?utv=ut4.42.201609061332 HTTP/1.1\r\n
  [Expert Info (Chat/Sequence): GET /utag/cisco/cdc/prod/utag.2311.js?utv=ut4.42.201609061332 HTTP/1.1\r\n]
  [GET /utag/cisco/cdc/prod/utag.2311.js?utv=ut4.42.201609061332 HTTP/1.1\r\n]
  [Severity level: chat]
  [Group: Sequence]
  Request Method: GET
  Request URI: /utag/cisco/cdc/prod/utag.2311.js?utv=ut4.42.201609061332
  Request Version: HTTP/1.1
  Accept: application/javascript, */*;q=0.8\r\n
  Referer: http://www.cisco.com/c/m/en_us/training-events/events-webinars/webinars/techwise-tv/196-anyconnect-opens.html\r\n
  Accept-Language: id-ID\r\n
  User-Agent: Mozilla/5.0 (Compatible; MSIE 10.0; windows NT 6.2; Trident/6.0)\r\n
  Accept-Encoding: gzip, deflate\r\n
  Host: tags.tiqcdn.com\r\n
  Connection: keep-alive\r\n
  \r\n
  [Full request URI: http://tags.tiqcdn.com/utag/cisco/cdc/prod/utag.2311.js?utv=ut4.42.201609061332]
  [HTTP request 3/9]
  [Prev request in frame: 3817]
  [Response in frame: 3852]
  [Next request in frame: 3860]

```

Gambar dibawah ini merupakan bytes dari paket yang berisi data yang diterima atau dikirim dalam bentuk hexadesimal dan disamping kanan merupakan terjemahan dari data hexadesimal tersebut.

0000	00 80 48 22 cf fa e0 06 e6 70 2a e3 08 00 45 00	..H".... .p*...E.
0010	01 cc 1b ae 40 00 80 06 75 55 0a 64 e1 c5 17 0f	...@... uU.d...
0020	64 f0 c3 af 00 50 ab c0 f2 88 21 17 28 4f 50 18	d....P.. !!(.OP.
0030	04 00 a4 f5 00 00 47 45 54 20 2f 75 74 61 67 2fGE T /utag/
0040	63 69 73 63 6f 2f 63 64 63 2f 70 72 6f 64 2f 75	cisco/cd c/prod/u
0050	74 61 67 2e 32 33 31 31 2e 6a 73 3f 75 74 76 3d	tag.2311 .js?utv=
0060	75 74 34 2e 34 32 2e 32 30 31 36 30 39 30 36 31	ut4.42.2 01609061
0070	33 33 32 20 48 54 54 50 2f 31 2e 31 0d 0a 41 63	332 HTTP /1.1.AC
0080	63 65 70 74 3a 20 61 70 70 6c 69 63 61 74 69 6f	cept: ap plicatio
0090	6e 2f 6a 61 76 61 73 63 72 69 70 74 2c 20 2a 2f	n/javasc ript, /*
00a0	2a 3b 71 3d 30 2e 38 0d 0a 52 65 66 65 72 65 72	*;q=0.8. .Referer
00b0	3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 63 69 73	: http:// www.cis
00c0	63 6f 2e 63 6f 6d 2f 63 2f 6d 2f 65 6e 5f 75 73	co.com/c /m/en_us
00d0	2f 74 72 61 69 6e 69 6e 67 2d 65 76 65 6e 74 73	/trainin g-events
00e0	2f 65 76 65 6e 74 73 2d 77 65 62 69 6e 61 72 73	/events- webinars
00f0	2f 77 65 62 69 6e 61 72 73 2f 74 65 63 68 77 69	/webinar s/techwi
0100	73 65 2d 74 76 2f 31 39 36 2d 61 6e 79 63 6f 6e	se-tv/19 6-anycon
0110	6e 65 63 74 2d 6f 70 65 6e 64 6e 73 2e 68 74 6d	nect-ope ndns.htm
0120	6c 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61	l..Accep t-Langua
0130	67 65 3a 20 69 64 2d 49 44 0d 0a 55 73 65 72 2d	ge: id-I D..User-
0140	41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35	Agent: M ozilla/5
0150	2e 30 20 28 63 6f 6d 70 61 74 69 62 6c 65 3b 20	.0 (comp atible;
0160	4d 53 49 45 20 31 30 2e 30 3b 20 57 69 6e 64 6f	MSIE 10. 0; windo
0170	77 73 20 4e 54 20 36 2e 32 3b 20 54 72 69 64 65	ws NT 6. 2; Tride
0180	6e 74 2f 36 2e 30 29 0d 0a 41 63 63 65 70 74 2d	nt/6.0). .Accept-
0190	45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20	Encoding : gzip,
01a0	64 65 66 6c 61 74 65 0d 0a 48 6f 73 74 3a 20 74	deflate. .Host: t
01b0	61 67 73 2e 74 69 71 63 64 6e 2e 63 6f 6d 0d 0a	ags.tiqc dn.com..
01c0	43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70	Connecti on: Keep
01d0	2d 41 6c 69 76 65 0d 0a 0d 0a	-Alive.. ..

5. Ukuran paket data

Disini saya membandingkan 2 protokol. Ukuran paket data yang ada pada wireshark dengan protokol HTTP yaitu sebanyak 3988 paket. Dan ukuran paket yang menghubungkan antara Host pengirim dan Host penerima ialah sebanyak 3988 paket atau sebanyak 100,000% dari total paket yang ada.

Traffic	Captured	Displayed	Displayed %	Marked	Marked %
Packets	3988	3988	100.000%	0	0.000%
Between first and last packet	135,116 sec				
Avg. packets/sec	29,515				
Avg. packet size	521 bytes				
Bytes	2077182	2077182	100.000%	0	0.000%
Avg. bytes/sec	15373,284				
Avg. MBit/sec	0,123				

Sedangkan ukuran paket data yang ada pada wireshark dengan protokol TCP yaitu sebanyak 3988 paket. Tetapi ukuran paket yang menghubungkan antara Host pengirim dan Host penerima yaitu sebanyak 3126 paket atau sebanyak 78,385% dari total paket yang ada.

Display						
Display filter:	tcp					
Ignored packets:	0 (0,000%)					
Traffic	Captured	Displayed	Displayed %	Marked	Marked %	
Packets	3988	3126	78,385%	0	0,000%	
Between first and last packet	135,116 sec	134,363 sec				
Avg. packets/sec	29,515	23,265				
Avg. packet size	521 bytes	631 bytes				
Bytes	2077182	1973520	95,009%	0	0,000%	
Avg. bytes/sec	15373,284	14687,948				
Avg. MBit/sec	0,123	0,118				

Buttons: Help, OK, Cancel

PROTOCOL HTTP (POST)

```

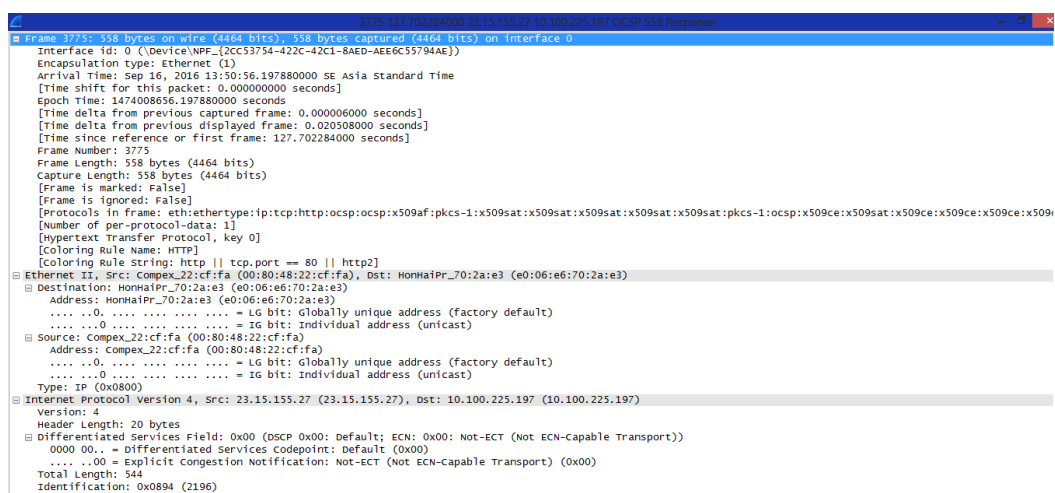
321 15.000595000.10.100.225.197.119.81.145.162 HTTP 256 POST /ui/ff/avast.com/urllinfo/v3/_/MD/008123425208F6A8000001575A2992C86364656161623132000001572B86CE51/1474007260 HTTP/1.1
  Frame 321: 266 bytes on wire (2128 bits), 266 bytes captured (2128 bits) on interface 0
  Interface id: 0 (Device\NPF_{2CC53754-422C-42C1-8AED-AEE6C55794AE})
  Encapsulation type: Ethernet (1)
  Arrival Time: Sep 16, 2016 13:49:03.496191000 SE Asia Standard Time
  [Time shift for this packet: 0.00000000 seconds]
  Epoch Time: 1474008843.496191000 seconds
  [Time delta from previous captured frame: 0.000600000 seconds]
  [Time delta from previous displayed frame: 2.842018000 seconds]
  [Time since reference or first frame: 15.000595000 seconds]
  Frame Number: 321
  Frame Length: 266 bytes (2128 bits)
  Capture Length: 266 bytes (2128 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in Frame: eth:ethertype:ip:tcp:http:data]
  [Number of per-protocol-data: 1]
  [Hypertext Transfer Protocol, key 0]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80 || http2]
  Ethernet II, Src: HonhaiPr_70:2a:e3 (e0:06:e6:70:2a:e3), Dst: Complex_22:cf:fa (00:80:48:22:cf:fa)
  Destination: Complex_22:cf:fa (00:80:48:22:cf:fa)
    Address: Complex_22:cf:fa (00:80:48:22:cf:fa)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Source: HonhaiPr_70:2a:e3 (e0:06:e6:70:2a:e3)
    Address: HonhaiPr_70:2a:e3 (e0:06:e6:70:2a:e3)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: IP (0x0800)
  Internet Protocol Version 4, Src: 10.100.225.197 (10.100.225.197), Dst: 119.81.145.162 (119.81.145.162)
  Version: 4
  Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    0000 00.. = Differentiated Services codepoint: Default (0x00)
    ....00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 252
  Identification: 0x7f39 (32569)
  Flags: 0x02 (Don't Fragment)
    0... .... = Reserved bit: Not set
    .1... .... = Don't fragment: Set
    ..0... .... = More fragments: Not set
  Fragment Offset: 0
  Time to live: 128
  Protocol: TCP (6)
  Header checksum: 0x85a5 [validation disabled]
    [good: False]
    [bad: False]
  Source: 10.100.225.197 (10.100.225.197)
  Destination: 119.81.145.162 (119.81.145.162)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
  Transmission Control Protocol, Src Port: 49970 (49970), Dst Port: 80 (80), Seq: 255, Ack: 1, Len: 212
  Source Port: 49970 (49970)
  Destination Port: 80 (80)
  [Stream Index: 21]
  [TCP Segment Len: 212]
  Sequence number: 255 (relative sequence number)
  [Next sequence number: 467 (relative sequence number)]
  Acknowledgment number: 1 (relative ack number)
  Header Length: 20 bytes

  Cache-Control: no-cache\r\n
  Connection: Keep-Alive\r\n
  Pragma: no-cache\r\n
  User-Agent: avast! WVC IE plugin\r\n
  Content-Length: 212\r\n
  [Content Length: 212]
  Host: ui.ff.avast.com\r\n
  \r\n
  [Full request URI: http://ui.ff.avast.com/urllinfo/v3/_/MD/008123425208F6A8000001575A2992C86364656161623132000001572B86CE51/1474007260]
  [HTTP request 1/1]
  [Response in frame: 325]
  Data (212 bytes)
  Data: 0d3301e5721a5ab2f71043ad8629da5de84158898826e741...
  [Length: 212]
  
```

Protokol HTTP merupakan sebuah protokol yang meminta/menjawab antara klien dan server. Klien HTTP memulai permintaan dengan membuat hubungan ke port tertentu di sebuah server webhosting tertentu (port 80) melalui entity body dalam HTTP Request dengan permintaan post.

PROTOCOL OSCP (RESPONSE)

Protokol OSCP (online certificate status protocol). Pada protokol ini



```
3775 127.702284000 23.15.155.27 10.100.225.197 OSCP'S58 Response
Frame 3775: 558 bytes on wire (4464 bits), 558 bytes captured (4464 bits) on interface 0
  Interface Id: 0 (Device WPF_{2cc53754-422c-42c1-8aed-ae66c55794ae})
  Encapsulation type: Ethernet (1)
  Arrival Time: Sep 16, 2016 13:50:56.197880000 SE Asia Standard Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1474008656.197880000 seconds
  [Time delta from previous captured frame: 0.000006000 seconds]
  [Time delta from previous displayed frame: 0.020508000 seconds]
  [Time since reference or first frame: 127.702284000 seconds]
  Frame Number: 3775
  Frame Length: 558 bytes (4464 bits)
  Capture Length: 558 bytes (4464 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp:http:ocsp:ocsp:x509af:pkcs-1:x509sat:x509sat:x509sat:x509sat:x509sat:pkcs-1:ocsp:x509ce:x509sat:x509ce:x509ce:x509ce:x509ce]
  [Number of per-protocol-data: 1]
  [Hypertext Transfer Protocol, key 0]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80 || http2]
  Ethernet II, Src: Complex_22:cf:fa (00:80:48:22:cf:fa), Dst: HonHaiPr_70:2a:e3 (e0:06:e6:70:2a:e3)
    Address: HonHaiPr_70:2a:e3 (e0:06:e6:70:2a:e3)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
    Source: complex_22:cf:fa (00:80:48:22:cf:fa)
      Address: complex_22:cf:fa (00:80:48:22:cf:fa)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Type: TP (0x0800)
  Internet Protocol Version 4, Src: 23.15.155.27 (23.15.155.27), Dst: 10.100.225.197 (10.100.225.197)
    Version: 4
    Header Length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
      0000 00. = Differentiated Services Codepoint: Default (0x00)
      ....00. = Explicit congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
    Total Length: 544
    Identification: 0x0894 (2196)
```

ANALISA PROTOCOL TCP

Pada wireshark ini banyak sekali paket data yang terbentuk dengan protocol yang berbeda-beda. Pada protocol TCP ini kita dapat melihat beberapa protocol jenis TCP dengan info yang berbeda-beda dan saya akan menunjukkan MAC address dan IP address saya. Dari berbagai protocol yang dapat kita lihat, ada tahap pengkoneksian sebuah komputer yang mengirim data (Host pengirim) ke destination (Host Penerima).

1. Pada awalnya Host pengirim (yaitu komputer saya) mengirim paket SYN ke Host penerima, hal ini dapat dilihat pada gambar dibawah ini (yang telah diberi tanda garis biru).

181	10.9846520	10.100.225.197	54.165.221.175	TLSv1	560 Application Data, Application Data
183	11.2254490	10.100.225.197	74.125.200.94	TCP	54 49958-443 [FIN, ACK] Seq=1 Ack=1 win=1024 Len=0
184	11.2261110	10.100.225.197	74.125.200.94	TCP	54 49957-443 [FIN, ACK] Seq=1 Ack=1 win=1020 Len=0
185	11.2273620	10.100.225.197	74.125.200.94	TCP	66 50002-443 [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
186	11.2275800	10.100.225.197	74.125.200.94	TCP	66 50003-443 [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
191	11.5545230	74.125.200.94	10.100.225.197	TCP	66 443-50003 [SYN, ACK] Seq=0 Ack=1 win=42780 Len=0 MSS=1380 SACK_PERM=1 WS=128
192	11.5545300	74.125.200.94	10.100.225.197	TCP	66 50003-443 [SYN, ACK] Seq=0 Ack=1 win=42780 Len=0 MSS=1380 SACK_PERM=1 WS=128
193	11.5550110	10.100.225.197	74.125.200.94	TCP	54 50002-443 [ACK] Seq=1 Ack=1 win=262144 Len=0
194	11.5552500	10.100.225.197	74.125.200.94	TCP	54 50002-443 [ACK] Seq=1 Ack=1 win=262144 Len=0
195	11.5568110	10.100.225.197	74.125.200.94	TLSv1	366 Client Hello
196	11.5578550	10.100.225.197	74.125.200.94	TLSv1	366 Client Hello
197	11.5705180	10.100.225.197	74.125.200.94	TCP	54 [TCP Retransmission] 49957-443 [FIN, ACK] Seq=1 Ack=1 win=1020 Len=0
198	11.5845030	74.125.200.94	10.100.225.197	TLSv1	173 Server Hello, Change Cipher Spec, Encrypted Handshake Message
199	11.5934280	74.125.200.94	10.100.225.197	TCP	66 443-49957 [ACK] Seq=2 Ack=2 win=368 Len=0 SLE=1 SRE=2
200	11.6090140	10.100.225.197	74.125.200.94	TLSv1	113 Change Cipher Spec, Encrypted Handshake Message
201	11.6165300	10.100.225.197	74.125.200.94	TCP	54 [TCP Retransmission] 49958-443 [FIN, ACK] Seq=1 Ack=1 win=1024 Len=0
202	11.6340570	74.125.200.94	10.100.225.197	TCP	66 443-49958 [ACK] Seq=2 Ack=2 win=360 Len=0 SLE=1 SRE=2
203	11.6655300	74.125.200.94	10.100.225.197	TCP	54 443-50003 [ACK] Seq=120 Ack=372 win=43904 Len=0

2. Setelah Host penerima menerima paket tersebut kemudian Host penerima mengirim paket SYN serta meng-ACK paket SYN tersebut, hal ini dapat dilihat pada gambar dibawah ini (yang telah diberi tanda garis biru).

181	10.9846520	10.100.225.197	54.165.221.175	TLSv1	560 Application data, Application Data
183	11.2254490	10.100.225.197	74.125.200.94	TCP	54 49958-443 [FIN, ACK] Seq=1 Ack=1 win=1024 Len=0
184	11.2261110	10.100.225.197	74.125.200.94	TCP	54 49957-443 [FIN, ACK] Seq=1 Ack=1 win=1020 Len=0
185	11.2273620	10.100.225.197	74.125.200.94	TCP	66 50002-443 [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
186	11.2275800	10.100.225.197	74.125.200.94	TCP	66 50003-443 [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
191	11.5545230	74.125.200.94	10.100.225.197	TCP	66 443-50003 [SYN, ACK] Seq=0 Ack=1 win=42780 Len=0 MSS=1380 SACK_PERM=1 WS=128
192	11.5545300	74.125.200.94	10.100.225.197	TCP	66 443-50002 [SYN, ACK] Seq=0 Ack=1 win=42780 Len=0 MSS=1380 SACK_PERM=1 WS=128
193	11.5550110	10.100.225.197	74.125.200.94	TCP	54 50003-443 [ACK] Seq=1 Ack=1 win=262144 Len=0
194	11.5552500	10.100.225.197	74.125.200.94	TCP	54 50002-443 [ACK] Seq=1 Ack=1 win=262144 Len=0
195	11.5568110	10.100.225.197	74.125.200.94	TLSv1	366 Client Hello
196	11.5578550	10.100.225.197	74.125.200.94	TLSv1	366 Client Hello
197	11.5705180	10.100.225.197	74.125.200.94	TCP	54 [TCP Retransmission] 49957-443 [FIN, ACK] Seq=1 Ack=1 win=1020 Len=0
198	11.5845030	74.125.200.94	10.100.225.197	TLSv1	173 Server Hello, Change Cipher Spec, Encrypted Handshake Message
199	11.5934280	74.125.200.94	10.100.225.197	TCP	66 443-49957 [ACK] Seq=2 Ack=2 win=368 Len=0 SLE=1 SRE=2
200	11.6090140	10.100.225.197	74.125.200.94	TLSv1	113 Change Cipher Spec, Encrypted Handshake Message
201	11.6165300	10.100.225.197	74.125.200.94	TCP	54 [TCP Retransmission] 49958-443 [FIN, ACK] Seq=1 Ack=1 win=1024 Len=0
202	11.6340570	74.125.200.94	10.100.225.197	TCP	66 443-49958 [ACK] Seq=2 Ack=2 win=360 Len=0 SLE=1 SRE=2
203	11.6655300	74.125.200.94	10.100.225.197	TCP	54 443-50003 [ACK] Seq=120 Ack=372 win=43904 Len=0

3. Setelah Host pengirim menerima paket ini, maka Host Pengirim akan meng-ACK paket tersebut ke Host penerima (dapat dilihat pada gambar a). Setelah itu maka koneksi pun terbuka, dapat dilihat pada gambar b

181	10.9846520	10.100.225.197	54.165.221.175	TLSv1	560 Application Data, Application Data
183	11.2254490	10.100.225.197	74.125.200.94	TCP	54 49958-443 [FIN, ACK] Seq=1 Ack=1 win=1024 Len=0
184	11.2261110	10.100.225.197	74.125.200.94	TCP	54 49957-443 [FIN, ACK] Seq=1 Ack=1 win=1020 Len=0
185	11.2273620	10.100.225.197	74.125.200.94	TCP	66 50002-443 [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
186	11.2275800	10.100.225.197	74.125.200.94	TCP	66 50003-443 [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
191	11.5545230	74.125.200.94	10.100.225.197	TCP	66 443-50003 [SYN, ACK] Seq=0 Ack=1 win=42780 Len=0 MSS=1380 SACK_PERM=1 WS=128
192	11.5545300	74.125.200.94	10.100.225.197	TCP	66 443-50002 [SYN, ACK] Seq=0 Ack=1 win=42780 Len=0 MSS=1380 SACK_PERM=1 WS=128
193	11.5550110	10.100.225.197	74.125.200.94	TCP	54 50003-443 [ACK] Seq=1 Ack=1 win=262144 Len=0
194	11.5552500	10.100.225.197	74.125.200.94	TCP	54 50002-443 [ACK] Seq=1 Ack=1 win=262144 Len=0
195	11.5568110	10.100.225.197	74.125.200.94	TLSv1	366 Client Hello
196	11.5578550	10.100.225.197	74.125.200.94	TLSv1	366 Client Hello
197	11.5705180	10.100.225.197	74.125.200.94	TCP	54 [TCP Retransmission] 49957-443 [FIN, ACK] Seq=1 Ack=1 win=1020 Len=0
198	11.5845030	74.125.200.94	10.100.225.197	TLSv1	173 Server Hello, Change Cipher Spec, Encrypted Handshake Message
199	11.5934280	74.125.200.94	10.100.225.197	TCP	66 443-49957 [ACK] Seq=2 Ack=2 win=368 Len=0 SLE=1 SRE=2
200	11.6090140	10.100.225.197	74.125.200.94	TLSv1	113 Change Cipher Spec, Encrypted Handshake Message
201	11.6165300	10.100.225.197	74.125.200.94	TCP	54 [TCP Retransmission] 49958-443 [FIN, ACK] Seq=1 Ack=1 win=1024 Len=0
202	11.6340570	74.125.200.94	10.100.225.197	TCP	66 443-49958 [ACK] Seq=2 Ack=2 win=360 Len=0 SLE=1 SRE=2
203	11.6655300	74.125.200.94	10.100.225.197	TCP	54 443-50003 [ACK] Seq=120 Ack=372 win=43904 Len=0

Gambar a. Pada saat Host Pengirim mengirimkan ACK ke Host penerima

181	10.9846520	10.100.225.197	54.165.221.175	TLSv1	560 Application Data, Application Data
183	11.2254490	10.100.225.197	74.125.200.94	TCP	54 49958-443 [FIN, ACK] Seq=1 Ack=1 win=1024 Len=0
184	11.2261110	10.100.225.197	74.125.200.94	TCP	54 49957-443 [FIN, ACK] Seq=1 Ack=1 win=1020 Len=0
185	11.2273620	10.100.225.197	74.125.200.94	TCP	66 50002-443 [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
186	11.2275800	10.100.225.197	74.125.200.94	TCP	66 50003-443 [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
191	11.5545230	74.125.200.94	10.100.225.197	TCP	66 443-50003 [SYN, ACK] Seq=0 Ack=1 win=42780 Len=0 MSS=1380 SACK_PERM=1 WS=128
192	11.5545300	74.125.200.94	10.100.225.197	TCP	66 443-50002 [SYN, ACK] Seq=0 Ack=1 win=42780 Len=0 MSS=1380 SACK_PERM=1 WS=128
193	11.5550110	10.100.225.197	74.125.200.94	TCP	54 50003-443 [ACK] Seq=1 Ack=1 win=262144 Len=0
194	11.5552500	10.100.225.197	74.125.200.94	TCP	54 50002-443 [ACK] Seq=1 Ack=1 win=262144 Len=0
195	11.5568110	10.100.225.197	74.125.200.94	TLSv1	366 Client Hello
196	11.5578550	10.100.225.197	74.125.200.94	TLSv1	366 Client Hello
197	11.5705180	10.100.225.197	74.125.200.94	TCP	54 [TCP Retransmission] 49957-443 [FIN, ACK] Seq=1 Ack=1 win=1020 Len=0
198	11.5845030	74.125.200.94	10.100.225.197	TLSv1	173 Server Hello, Change Cipher Spec, Encrypted Handshake Message
199	11.5934280	74.125.200.94	10.100.225.197	TCP	66 443-49957 [ACK] Seq=2 Ack=2 win=368 Len=0 SLE=1 SRE=2
200	11.6090140	10.100.225.197	74.125.200.94	TLSv1	113 Change Cipher Spec, Encrypted Handshake Message

Gambar b. Pada saat koneksi terbuka dengan client dan server saling menyapa

- Setiap kali sebuah paket tiba di Host Penerima, maka Host penerima akan mengeceknya dan mengirim ACK yang menandakan paket telah diterima. Proses ini berlangsung berulang-ulang sampai semua paket dikirim dan tiba dengan baik.

No.	Time	Source	Destination	Protocol	Length	Info
345	16.2486870	10.100.225.197	54.165.221.175	TLSv1	592	Application Data, Application Data
346	16.2521340	23.15.96.170	10.100.225.197	TCP	54	80-49842 [FIN, ACK] Seq=1 Ack=2 win=1628 Len=0
347	16.2521390	23.15.96.170	10.100.225.197	TCP	54	80-49824 [FIN, ACK] Seq=1 Ack=2 win=2047 Len=0
348	16.2521420	23.15.96.170	10.100.225.197	TCP	66	80-50007 [SYN, ACK] Seq=0 Ack=1 win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=32
349	16.2524210	10.100.225.197	23.15.96.170	TCP	54	49842-80 [ACK] Seq=2 Ack=2 win=1024 Len=0
350	16.2527320	10.100.225.197	23.15.96.170	TCP	54	49824-80 [ACK] Seq=2 Ack=2 win=1018 Len=0
351	16.2530660	10.100.225.197	23.15.96.170	TCP	54	50007-80 [ACK] Seq=1 Ack=1 win=262144 Len=0
352	16.2563030	10.100.225.197	23.15.96.170	HTTP	1265	GET / HTTP/1.1
353	16.2946640	23.15.96.170	10.100.225.197	TCP	54	80-50007 [ACK] Seq=1 Ack=1212 win=31648 Len=0
354	16.3040810	23.15.96.170	10.100.225.197	TCP	1514	[TCP segment of a reassembled PDU]
355	16.3343010	23.15.96.170	10.100.225.197	TCP	1514	[TCP segment of a reassembled PDU]
356	16.3343080	23.15.96.170	10.100.225.197	TCP	1514	[TCP segment of a reassembled PDU]
357	16.3343120	23.15.96.170	10.100.225.197	TCP	1514	[TCP segment of a reassembled PDU]
358	16.3343150	23.15.96.170	10.100.225.197	TCP	1514	[TCP segment of a reassembled PDU]
359	16.3343240	23.15.96.170	10.100.225.197	TCP	1514	[TCP segment of a reassembled PDU]
360	16.3343290	23.15.96.170	10.100.225.197	TCP	1514	[TCP segment of a reassembled PDU]
361	16.3343310	23.15.96.170	10.100.225.197	TCP	1514	[TCP segment of a reassembled PDU]
362	16.3343340	23.15.96.170	10.100.225.197	TCP	1514	[TCP segment of a reassembled PDU]
363	16.3343370	23.15.96.170	10.100.225.197	TCP	1514	[TCP segment of a reassembled PDU]
364	16.3343400	23.15.96.170	10.100.225.197	HTTP	121	HTTP/1.1 200 OK (text/html)
365	16.3351390	10.100.225.197	23.15.96.170	TCP	54	50007-80 [ACK] Seq=1212 Ack=14668 win=262144 Len=0
367	16.5521360	54.165.221.175	10.100.225.197	TCP	54	443-50005 [ACK] Seq=439 Ack=1412 win=21504 Len=0
368	16.5523410	10.100.225.197	54.165.221.175	TLSv1	960	Application Data, Application Data
369	16.8191810	54.165.221.175	10.100.225.197	TCP	54	443-50005 [ACK] Seq=439 Ack=2318 win=23296 Len=0
370	16.8220880	54.165.221.175	10.100.225.197	TLSv1	587	Application Data
371	16.8711660	10.100.225.197	54.165.221.175	TCP	54	50005-443 [ACK] Seq=2318 Ack=972 win=261120 Len=0

Gambar c. Pada saat Host pengirim mengirim data ke Host penerima

No.	Time	Source	Destination	Protocol	Length	Info
345	16.2486870	10.100.225.197	54.165.221.175	TLSv1	592	Application Data, Application Data
346	16.2521340	23.15.96.170	10.100.225.197	TCP	54	80-49842 [FIN, ACK] Seq=1 Ack=2 win=1628 Len=0
347	16.2521390	23.15.96.170	10.100.225.197	TCP	54	80-49824 [FIN, ACK] Seq=1 Ack=2 win=2047 Len=0
348	16.2521420	23.15.96.170	10.100.225.197	TCP	66	80-50007 [SYN, ACK] Seq=0 Ack=1 win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=32
349	16.2524210	10.100.225.197	23.15.96.170	TCP	54	49842-80 [ACK] Seq=2 Ack=2 win=1024 Len=0
350	16.2527320	10.100.225.197	23.15.96.170	TCP	54	49824-80 [ACK] Seq=2 Ack=2 win=1018 Len=0
351	16.2530660	10.100.225.197	23.15.96.170	TCP	54	50007-80 [ACK] Seq=1 Ack=1 win=262144 Len=0
352	16.2563030	10.100.225.197	23.15.96.170	HTTP	1265	GET / HTTP/1.1
353	16.2946640	23.15.96.170	10.100.225.197	TCP	54	80-50007 [ACK] Seq=1 Ack=1212 win=31648 Len=0
354	16.3040810	23.15.96.170	10.100.225.197	TCP	1514	[TCP segment of a reassembled PDU]
355	16.3343010	23.15.96.170	10.100.225.197	TCP	1514	[TCP segment of a reassembled PDU]
356	16.3343080	23.15.96.170	10.100.225.197	TCP	1514	[TCP segment of a reassembled PDU]
357	16.3343120	23.15.96.170	10.100.225.197	TCP	1514	[TCP segment of a reassembled PDU]
358	16.3343150	23.15.96.170	10.100.225.197	TCP	1514	[TCP segment of a reassembled PDU]
359	16.3343240	23.15.96.170	10.100.225.197	TCP	1514	[TCP segment of a reassembled PDU]
360	16.3343290	23.15.96.170	10.100.225.197	TCP	1514	[TCP segment of a reassembled PDU]
361	16.3343310	23.15.96.170	10.100.225.197	TCP	1514	[TCP segment of a reassembled PDU]
362	16.3343340	23.15.96.170	10.100.225.197	TCP	1514	[TCP segment of a reassembled PDU]
363	16.3343370	23.15.96.170	10.100.225.197	TCP	1514	[TCP segment of a reassembled PDU]
364	16.3343400	23.15.96.170	10.100.225.197	HTTP	121	HTTP/1.1 200 OK (text/html)
365	16.3351390	10.100.225.197	23.15.96.170	TCP	54	50007-80 [ACK] Seq=1212 Ack=14668 win=262144 Len=0
367	16.5521360	54.165.221.175	10.100.225.197	TCP	54	443-50005 [ACK] Seq=439 Ack=1412 win=21504 Len=0
368	16.5523410	10.100.225.197	54.165.221.175	TLSv1	960	Application Data, Application Data
369	16.8191810	54.165.221.175	10.100.225.197	TCP	54	443-50005 [ACK] Seq=439 Ack=2318 win=23296 Len=0
370	16.8220880	54.165.221.175	10.100.225.197	TLSv1	587	Application Data
371	16.8711660	10.100.225.197	54.165.221.175	TCP	54	50005-443 [ACK] Seq=2318 Ack=972 win=261120 Len=0

Gambar d. Pada saat Host penerima memberikan pesan dari Host pengirim jika paket telah diterima dengan baik

- Pada percobaan ini saya menemukan bahwa paket dapat hilang atau rusak ditengah jalan, maka Host penerima akan memberitahukan Host pengirim dengan meminta kembali Host pengirim untuk mengirimkan data tersebut. Dapat dilihat pada gambar

No.	Time	Source	Destination	Protocol	Length	Info
2821	105.390557	10.100.225.197	23.15.96.170	HTTP	509	GET /C/M/en_US/Training-Events/Events-Webinars/webinars/tecnwise-tv/196-anyconnect-opensn...
2822	105.416664	10.100.225.197	72.163.10.10	TCP	54	[TCP Retransmission] 50048-80 [FIN, ACK] Seq=3541 Ack=371 Win=65335 Len=0
2823	105.593577	103.20.94.1	10.100.225.197	TLSv1	95	Server Key Exchange
2824	105.670557	10.100.225.197	103.20.94.1	TCP	54	50067-443 [ACK] Seq=166 Ack=2962 Win=261888 Len=0
2825	105.753596	72.163.10.10	10.100.225.197	TCP	54	80-50049 [FIN, ACK] Seq=370 Ack=3919 Win=14600 Len=0
2826	105.753895	10.100.225.197	72.163.10.10	TCP	54	50049-80 [ACK] Seq=3919 Ack=371 Win=65535 Len=0
2827	105.770606	10.100.225.197	23.15.96.170	TCP	1514	[TCP Retransmission] 50018-80 [ACK] Seq=10100 Ack=186855 Win=261632 Len=1460
2828	105.829583	23.15.96.170	10.100.225.197	TCP	54	80-50018 [ACK] Seq=186855 Ack=11560 Win=53920 Len=0
2829	105.829583	10.100.225.197	23.15.96.170	TCP	33	[TCP Retransmission] 50018-80 [FIN, ACK] Seq=11560 Ack=186855 Win=261632 Len=341 [reassembly error]
2830	105.863571	23.15.96.170	10.100.225.197	TCP	54	80-50018 [ACK] Seq=186855 Ack=11901 Win=56864 Len=0
2831	105.900567	23.15.96.170	10.100.225.197	TCP	66	[TCP dup ACK 2830#1] 80-50018 [ACK] Seq=186855 Ack=11901 Win=56864 Len=0 SLE=11960 SRE=11901
2832	105.970338	10.100.225.197	103.20.94.1	TLSv1	188	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2833	105.972041	10.100.225.197	103.20.94.1	TLSv1	896	Application Data: Application Data
2834	106.078603	103.20.94.1	10.100.225.197	TLSv1	635	[TCP Previous segment not captured] Application Data
2835	106.078823	10.100.225.197	103.20.94.1	TCP	66	[TCP dup ACK 2824#1] 50067-443 [ACK] Seq=1142 Ack=2962 Win=261888 Len=0 SLE=3021 SRE=3602
2836	106.095273	103.20.94.1	10.100.225.197	TLSv1	155	Application Data

[Frame 2829: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface 0
 [Ethernet II, Src: NonHwIPr_70:2a:e3 (e0:06:e6:70:2a:e3), Dst: Complex_22:cf:fa (00:80:48:22:cf:fa)
 [Internet Protocol Version 4, Src: 10.100.225.197 (10.100.225.197), Dst: 23.15.96.170 (23.15.96.170)
 [Transmission Control Protocol, Src Port: 50018 (50018), Dst Port: 80 (80), Seq: 11560, Ack: 186855, Len: 341
 [Reassembly error, protocol TCP: New fragment overlaps old data (retransmission?)
 [Expert Info (Error/Malformed): New fragment overlaps old data (retransmission?)
 [Severity level: Error]
 [Group: Malformed]

Gambar e. Pada saat Host penerima menandakan data dari Host pengirim tidak diterima dengan baik dan meminta pengiriman data kembali.

Analisa Frame dari Command Prompt

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Aspire One 725>netstat -a

Active Connections

Proto Local Address           Foreign Address         State
TCP   0.0.0.0:135             AspireOne:0           LISTENING
TCP   0.0.0.0:445             AspireOne:0           LISTENING
TCP   0.0.0.0:2343            AspireOne:0           LISTENING
TCP   0.0.0.0:3500            AspireOne:0           LISTENING
TCP   0.0.0.0:3502            AspireOne:0           LISTENING
TCP   0.0.0.0:8000            AspireOne:0           LISTENING
TCP   0.0.0.0:8888            AspireOne:0           LISTENING
TCP   0.0.0.0:49152           AspireOne:0           LISTENING
TCP   0.0.0.0:49153           AspireOne:0           LISTENING
TCP   0.0.0.0:49154           AspireOne:0           LISTENING
TCP   0.0.0.0:49155           AspireOne:0           LISTENING
TCP   0.0.0.0:49202           AspireOne:0           LISTENING
TCP   0.0.0.0:59110           AspireOne:0           LISTENING
TCP   0.0.0.0:59111           AspireOne:0           LISTENING
TCP   0.0.0.0:60426           AspireOne:0           LISTENING
TCP   10.100.225.197:139      AspireOne:0           LISTENING
TCP   10.100.225.197:49562    se14:http              ESTABLISHED
TCP   10.100.225.197:49916   66-117.25.199:http     ESTABLISHED
TCP   10.100.225.197:50220   edge-staw-mini-shv-01-sin6:https CLOSE_WAIT
TCP   10.100.225.197:50228   se-in-f139:http        TIME_WAIT
TCP   10.100.225.197:50229   se-in-f139:http        TIME_WAIT
TCP   10.100.225.197:50235   kul06s17-in-f227:http  TIME_WAIT
TCP   10.100.225.197:50237   kul06s14-in-f196:http  TIME_WAIT
TCP   10.100.225.197:50239   hotspot-idl:http       TIME_WAIT
TCP   10.100.225.197:50241   hotspot-idl:http       TIME_WAIT
TCP   10.100.225.197:50242   hotspot-idl:http       TIME_WAIT
TCP   10.100.225.197:50245   a173-222-148-16:http   TIME_WAIT
TCP   10.100.225.197:50246   hotspot-idl:http       CLOSE_WAIT
TCP   10.100.225.197:50247   43:http                ESTABLISHED
TCP   10.100.225.197:50248   hotspot-idl:http       LAST_ACK
TCP   10.100.225.197:50252   a173-222-148-41:http   FIN_WAIT_1
TCP   10.100.225.197:50253   ec2-107-22-241-244:http LAST_ACK
TCP   10.100.225.197:50254   ec2-107-22-241-244:http LAST_ACK
TCP   10.100.225.197:50257   80:http                FIN_WAIT_1
TCP   10.100.225.197:50258   80:http                FIN_WAIT_1
TCP   10.100.225.197:50264   sa-in-f132:https       ESTABLISHED
TCP   10.100.225.197:50265   sa-in-f132:https       ESTABLISHED
TCP   10.100.225.197:50266   sa-in-f132:https       ESTABLISHED
TCP   10.100.225.197:50267   sa-in-f132:https       ESTABLISHED
TCP   10.100.225.197:50268   server-52-85-77-173:https ESTABLISHED
TCP   10.100.225.197:50269   server-52-85-77-173:https CLOSE_WAIT
  
```

```

TCP 10.100.225.197:50366 a-0001:http ESTABLISHED
TCP 10.100.225.197:50367 13.107.5.80:http ESTABLISHED
TCP 10.100.225.197:50368 13.107.5.80:http ESTABLISHED
TCP 10.100.225.197:50369 a23-15-96-170:http ESTABLISHED
TCP 10.100.225.197:50370 xx-fhcdn-shv-01-sin6:http ESTABLISHED
TCP 10.100.225.197:50371 xx-fhcdn-shv-01-sin6:http ESTABLISHED
TCP 10.100.225.197:50372 62:http ESTABLISHED
TCP 10.100.225.197:50373 62:http ESTABLISHED
TCP 10.100.225.197:50374 a23-15-96-170:http ESTABLISHED
TCP 10.100.225.197:50375 a23-15-96-170:http ESTABLISHED
TCP 10.100.225.197:50376 a23-15-96-170:http SYN_SENT
TCP 10.100.225.197:50377 a23-15-96-170:http SYN_SENT
TCP 10.100.225.197:50380 a23-15-96-170:http SYN_SENT
TCP 10.100.225.197:50381 218.93.250.18:http SYN_SENT
TCP 10.100.225.197:50382 218.93.250.18:http SYN_SENT
TCP 10.100.225.197:50383 ec2-54-152-109-246:https SYN_SENT
TCP 10.100.225.197:50384 ec2-54-152-109-246:https SYN_SENT
TCP 10.100.225.197:50385 ec2-107-22-241-244:http SYN_SENT
TCP 10.100.225.197:50386 a23-15-96-170:http SYN_SENT
TCP 10.100.225.197:50387 a23-15-96-170:http SYN_SENT
TCP 10.100.225.197:50388 a173-222-148-41:http SYN_SENT
TCP 10.100.225.197:50389 80:http SYN_SENT
TCP 10.100.225.197:50390 80:http SYN_SENT
TCP 10.100.225.197:50391 218.93.250.18:http SYN_SENT
TCP 10.100.225.197:50392 218.93.250.18:http SYN_SENT
TCP 10.100.225.197:60426 10.100.224.129:37141 FIN_WAIT_2
TCP 127.0.0.1:1001 AspireOne:0 LISTENING
TCP 127.0.0.1:5037 AspireOne:0 LISTENING
TCP 127.0.0.1:5354 AspireOne:0 LISTENING
TCP 127.0.0.1:6543 AspireOne:0 LISTENING
TCP 127.0.0.1:6543 AspireOne:49242 ESTABLISHED
TCP 127.0.0.1:6543 AspireOne:50202 ESTABLISHED
TCP 127.0.0.1:6544 AspireOne:0 LISTENING
TCP 127.0.0.1:7037 AspireOne:0 LISTENING
TCP 127.0.0.1:27275 AspireOne:0 LISTENING
TCP [::]:1135 AspireOne:0 LISTENING
TCP [::]:1445 AspireOne:0 LISTENING
TCP [::]:149152 AspireOne:0 LISTENING
TCP [::]:149153 AspireOne:0 LISTENING
TCP [::]:149154 AspireOne:0 LISTENING
TCP [::]:149155 AspireOne:0 LISTENING
TCP [::]:149202 AspireOne:0 LISTENING
TCP [::]:11:27275 AspireOne:0 LISTENING
UDP 0.0.0.0:500 **:*
UDP 0.0.0.0:2343 **:*
UDP 0.0.0.0:4500 **:*
UDP 0.0.0.0:5000 **:*
UDP 0.0.0.0:5001 **:*
UDP 0.0.0.0:5002 **:*
UDP 0.0.0.0:5353 **:*
UDP 0.0.0.0:5353 **:*
UDP 0.0.0.0:5353 **:*
UDP 0.0.0.0:5353 **:*
UDP 0.0.0.0:5355 **:*
UDP 0.0.0.0:6000 **:*
UDP 0.0.0.0:6001 **:*
UDP 0.0.0.0:6002 **:*
UDP 0.0.0.0:9986 **:*
UDP 0.0.0.0:59696 **:*
UDP [fe80::5499:4959:9f0a:fech:131]:546 **:*
UDP [fe80::5499:4959:9f0a:fech:131]:1900 **:*
UDP [fe80::803e:ce20:ce47:4132::171]:546 **:*
UDP [fe80::803e:ce20:ce47:4132::171]:1900 **:*
C:\Users\Aspire One 725>

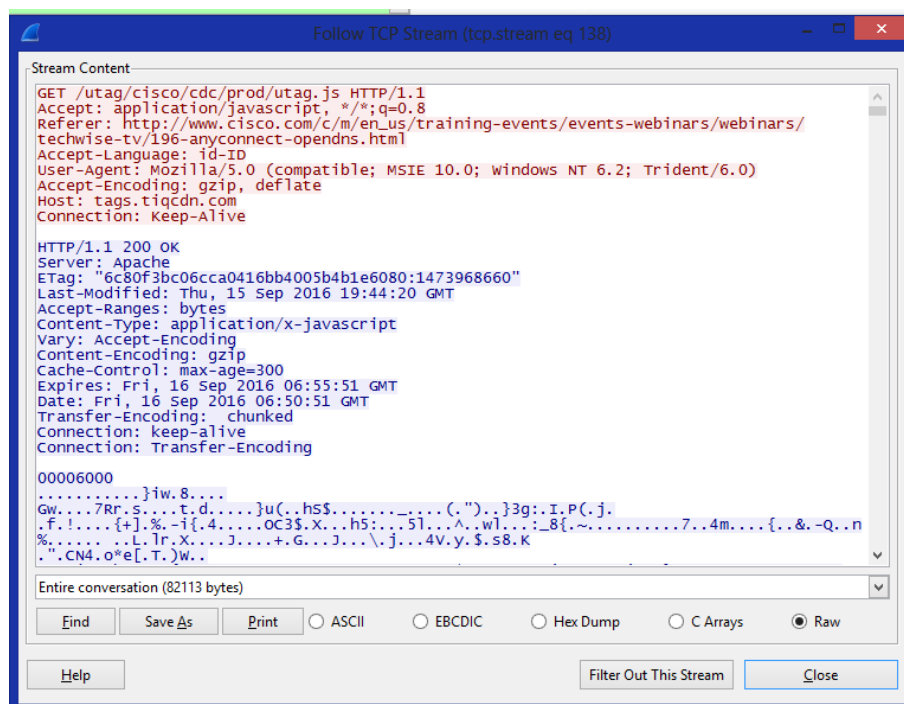
```

Ketika kita menulis perintah “netstat -a” pada command prompt maka akan muncul tampilan seperti pada gambar diatas. Ada 2 protokol yang muncul pada command prompt ini, yaitu TCP (Transfer Control Protocol) dan UDP (User Data Protocol). Protokol merupakan bahasa yang dimengerti oleh sender to destination. UDP merupakan protokol lapisan transpor TCP/IP yang mendukung komunikasi unreliable tanpa koneksi antara host. Netstat digunakan untuk monitoring traffic jaringan, melacak sumber paket yang didapat, menampilkan statistik protokol dan TCP/IP koneksi jaringan dan informasi yang terkait dengan koneksi port, antara lain alamat IP yang terhubung, status koneksi dan aplikasi yang digunakan.

Komputer berkomunikasi dengan menggunakan protokol TCP dan Local Address (IP address) yang aktif melakukan koneksi dengan Foreign Address. Untuk port-nya dapat dilihat disebelah host komputer. State (status koneksi) yang sering terjadi

seperti LISTENING (siap untuk melakukan koneksi), ESTABLISHED (koneksi terjadi dan siap mengirimkan data), TIME_WAIT (sedang menunggu koneksi), SYS_SENT (mengirimkan paket SYS), FIN_WAIT_1 (bersiap untuk meninggalkan server), TIME_WAIT (siap keluar dari server), CLOSE_WAIT (server mencatat history), FIN_WAIT_2 (server telah mengijinkan client untuk meninggalkan server), dan LAST_ACK (server mengantar client keluar dari server)

No.	Time	Source	Destination	Protocol	Length	Info
300	16.4701020	10.100.225.205	10.100.239.255	NBNS	92	Name query NB WPAD<OO>
373	16.9881900	fe80::b12c:e7d:6583ff02::1:3		LLMNR	95	Standard query 0x2f3f ANY HPTouchSmart600
374	16.9891050	10.100.224.193	224.0.0.252	LLMNR	75	Standard query 0x2f3f ANY HPTouchSmart600
375	16.9909870	10.100.224.193	239.255.255.250	UDP	1034	Source port: 54489 Destination port: 3702
376	16.9930750	fe80::b12c:e7d:6583ff02::c		UDP	1054	Source port: 54490 Destination port: 3702
377	16.9930810	fe80::b12c:e7d:6583ff02::1:3		LLMNR	95	Standard query 0x2f3f ANY HPTouchSmart600
378	16.9930840	10.100.224.193	224.0.0.252	LLMNR	75	Standard query 0x2f3f ANY HPTouchSmart600
380	17.1921430	fe80::b12c:e7d:6583ff02::c		UDP	1054	Source port: 54490 Destination port: 3702
381	17.1936850	10.100.224.193	239.255.255.250	UDP	1034	Source port: 54489 Destination port: 3702
382	17.1936900	10.100.224.193	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
391	17.4984540	10.100.227.14	10.100.239.255	NBNS	92	Name query NB WPAD<OO>
392	17.4999510	fe80::74f8:fc0e:b46ff02::1:3		LLMNR	84	Standard query 0xd4ad A wpad
393	17.4999580	10.100.227.14	224.0.0.252	LLMNR	64	Standard query 0xd4ad A wpad
394	17.5013280	fe80::74f8:fc0e:b46ff02::1:3		LLMNR	84	Standard query 0x3ecd AAAA wpad
395	17.5013340	10.100.227.14	224.0.0.252	LLMNR	64	Standard query 0x3ecd AAAA wpad



Port sumber dan port tujuan pada wireshark dapat dilihat pada protokol UDP. Ini merupakan hasil protokol UDP yang telah di capture dari wireshark. Bagian yang berwarna merah merupakan request sent (permintaan dikirim). Dan bagian berwarna biru merupakan response received (respon diterima).

ANALISA

Disini kita dapat melihat perbandingan antara wireshark dan netstat dimana pada wireshark secara terus menerus melakukan pengambilan nilai atau data untuk diamati pada saat proses berlangsung. Sedangkan pada netstat, pengambilan data lebih sedikit dan hanya dilakukan pada saat tertentu secara periodik. Dapat kita lihat juga pada netstat, ada protokol TCP dimana ada reply dari destination sedangkan pada protokol UDP tidak ada reply dari destination tetapi pada protokol ini hemat bandwidth.

KESIMPULAN

- Sebuah komputer yang ingin mengirim data harus mengirim SYN terlebih dahulu kemudian SYN tersebut di ACK dan komputer pengirim meng-ACK maka komunikasi akan terbuka.
- MAC sebuah komputer tidak dapat berubah-ubah sedangkan IP dapat berubah.
- Komunikasi yang dijalankan pada proses ini adalah komunikasi Half-duplex, yaitu komunikasi secara bergantian dimana satu komputer dengan komputer lainnya akan bergantian mengirim data dan menerima balasan, tidak dapat secara langsung.
- Sebuah komputer yang mengirim data, maka komputer penerima akan memberikan balasan dengan cara meng-ACK ke komputer pengirim, tetapi jika data tersebut hilang atau rusak, maka komputer penerima akan meng-ACK komputer pengirim untuk meminta data dikirim ulang (Retransmission Data).