

JARINGAN KOMPUTER



NAMA : KARYN VUSVYTA

NIM : 09011181419007

KELAS : SK5A

DOSEN PENGAJAR : Dr. DERIS DTIAWAN, M.T.

FAKULTAS ILMU KOMPUTER
JURUSAN SISTEM KOMPUTER
UNIVERSITAS SRIWIJAYA

2016

TASK 5

MENGANALISIS IP/PORT PADA SOFTWARE APLIKASI WIRESHARK DAN COMMAND PROMPT.

Sebelum melihat hasil capture dan menganalisa paket capture yang saya dapat, terlebih dahulu saya akan memberikan langkah-langkah yang saya lakukan saat melakukan capture interface pada software aplikasi wireshark. Awalnya saya membuka terlebih dahulu aplikasi software wireshark setelah selesai ter-install, kemudian saya membuka web browser melalui mozilla. Web browser yang saya pakai adalah www.cnnindonesia.com. Kemudian saya kembali membuka wireshark dan memilih interface yang akan saya capture, lalu saya klik start kemudian web browser tersebut meload page dari situs www.cnnindonesia.com dan banyak muncul paket-paket data yang didapat saat melakukan capture paket. Disini saya men-stop capture paket data nya sampai jumlah paket data nya lebih dari 5000 paket data. Berikut capture paket data terakhir yang saya dapat saat saya stop capture paket data.

```
5034 364.716268 10.100.225.197 10.100.239.255 NBNS 92 Name query NB RMHOYGFYKL<00>
```

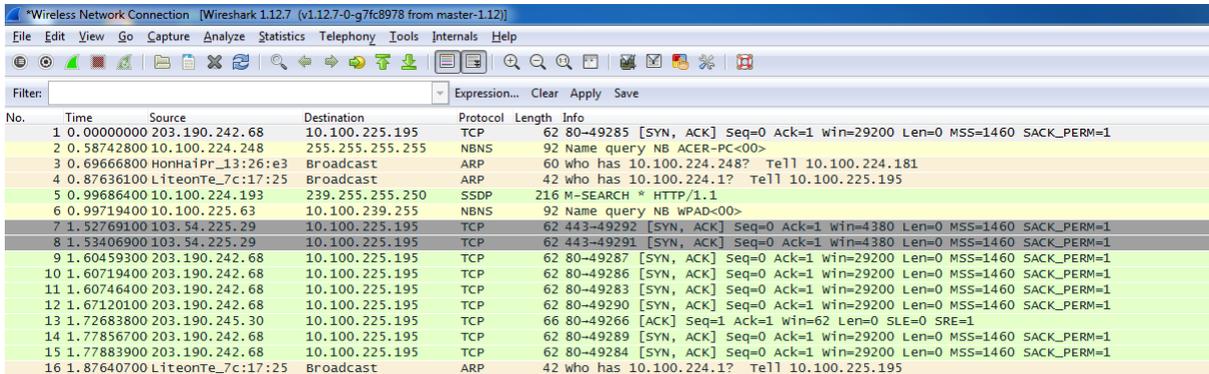
Sedangkan saat menggunakan command prompt perintah yang saya gunakan adalah (netstat -a). Netstat (Network Statistic) adalah program berbasis teks yang berfungsi untuk memantau koneksi jaringan pada suatu komputer, baik jaringan lokal (LAN) maupun jaringan internet. Perintah (netstat -a) akan menampilkan semua koneksi baik yang listening maupun tidak.

Setelah dijelaskan sedikit mengenai software aplikasi wireshark dan command prompt yang akan saya analisis maka sekarang saya akan menganalisis Protocol dan Request Method yang saya dapatkan dari capture data yang telah dilakukan sebelumnya. Pada capture data di software aplikasi wireshark saya mendapatkan 10 jenis protokol berbeda dimana dari setiap protokol tersebut memiliki banyak jenis protocol yang sama dengan alamat IP yang berbeda-beda. 10 protocol tersebut antara lain:

1. TCP (Transmission Control Protocol)
2. NBNS (Netbios Name Service)
3. ARP (Address Resolution Protocol)
4. SSDP (Simple Service Discovery Protocol)
5. DNS (Domain Name System)
6. OCSP (Online Certificate Status Protocol)
7. HTTP (Hyper Text Transfer Protocol)
8. LLMNR (Link-Local Multicast Name Resolution)
9. TLSV1.2 (Transport Layer Security)
10. DHCP (Dynamic Host Configuration Protokol)
11. UDP (User Datagram Protocol)

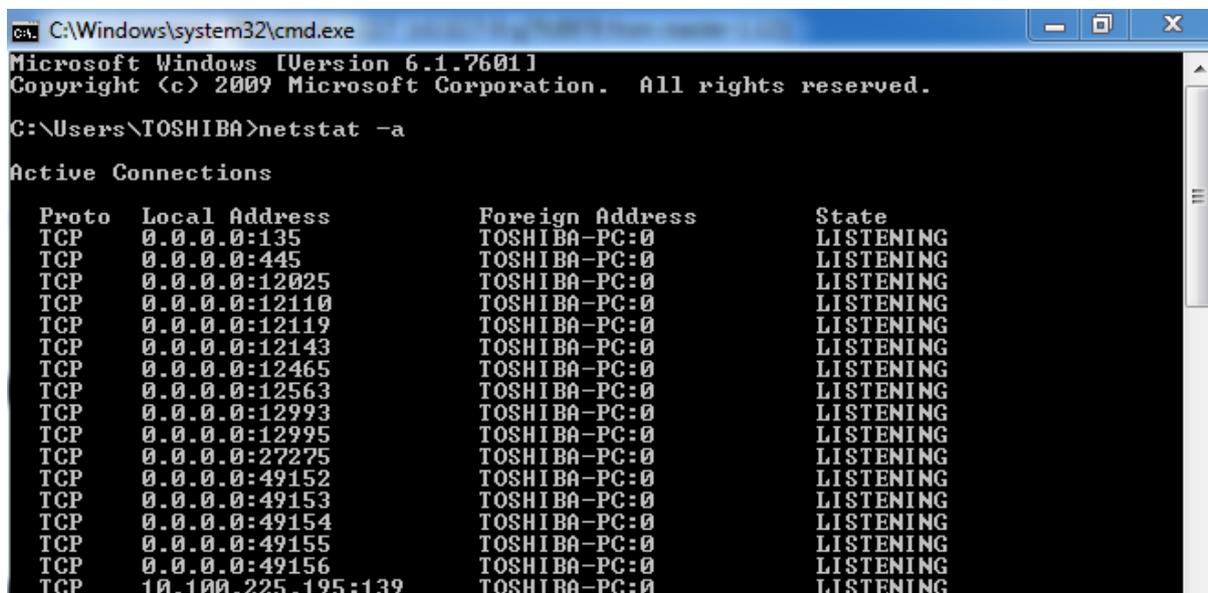
Sedangkan pada command prompt hanya ada dua jenis protocol yang muncul yaitu:

1. TCP (Transmission Control Protocol)
2. UDP (User Datagram Protocol)



No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	203.190.242.68	10.100.225.195	TCP	62	80->49285 [SYN, ACK] Seq=0 Ack=1 win=29200 Len=0 MSS=1460 SACK_PERM=1
2	0.58742800	10.100.224.248	255.255.255.255	NBNS	92	Name query NB ACER-PC<00>
3	0.69666800	HonHaiPr_13:26:e3	Broadcast	ARP	60	who has 10.100.224.248? Tell 10.100.224.181
4	0.87636100	LiteonTe_7c:17:25	Broadcast	ARP	42	who has 10.100.224.1? Tell 10.100.225.195
5	0.99686400	10.100.224.193	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
6	0.99719400	10.100.225.63	10.100.239.255	NBNS	92	Name query NB WPAD<00>
7	1.52769100	103.54.225.29	10.100.225.195	TCP	62	443->49292 [SYN, ACK] Seq=0 Ack=1 win=4380 Len=0 MSS=1460 SACK_PERM=1
8	1.53406900	103.54.225.29	10.100.225.195	TCP	62	443->49291 [SYN, ACK] Seq=0 Ack=1 win=4380 Len=0 MSS=1460 SACK_PERM=1
9	1.60459300	203.190.242.68	10.100.225.195	TCP	62	80->49287 [SYN, ACK] Seq=0 Ack=1 win=29200 Len=0 MSS=1460 SACK_PERM=1
10	1.60719400	203.190.242.68	10.100.225.195	TCP	62	80->49286 [SYN, ACK] Seq=0 Ack=1 win=29200 Len=0 MSS=1460 SACK_PERM=1
11	1.60746400	203.190.242.68	10.100.225.195	TCP	62	80->49283 [SYN, ACK] Seq=0 Ack=1 win=29200 Len=0 MSS=1460 SACK_PERM=1
12	1.67120100	203.190.242.68	10.100.225.195	TCP	62	80->49290 [SYN, ACK] Seq=0 Ack=1 win=29200 Len=0 MSS=1460 SACK_PERM=1
13	1.72683800	203.190.245.30	10.100.225.195	TCP	66	80->49266 [ACK] Seq=1 Ack=1 win=62 Len=0 SLE=0 SRE=1
14	1.77856700	203.190.242.68	10.100.225.195	TCP	62	80->49289 [SYN, ACK] Seq=0 Ack=1 win=29200 Len=0 MSS=1460 SACK_PERM=1
15	1.77883900	203.190.242.68	10.100.225.195	TCP	62	80->49284 [SYN, ACK] Seq=0 Ack=1 win=29200 Len=0 MSS=1460 SACK_PERM=1
16	1.87640700	LiteonTe_7c:17:25	Broadcast	ARP	42	who has 10.100.224.1? Tell 10.100.225.195

Pada gambar diatas akan saya analisa capture data pada nomor 1 source beralamatkan IP 203.190.242.68 dan destination beralamatkan IP 10.100.225.195. pada alamat IP ini memiliki alamat source port dan destination port yaitu TCP (Transmission Control Protocol), protocol ini akan menjamin data yang dikirimkan agar terjaga/terkirim seutuhnya sehingga apabila pada saat pengiriman data terjadi error data, maka data akan dikirim kembali hingga data benar-benar sampai seutuhnya dipenerima. Server akan menerima TCP SYN dan membalasnya dengan ACK yang menyatakan bahwa SYN telah diterima. Begitu juga dengan alamat-alamat IP selanjutnya yang menggunakan protocol TCP memiliki proses yang sama, hanya saja alamat source to destination nya yang berbeda.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\TOSHIBA>netstat -a

Active Connections

Proto Local Address Foreign Address State
TCP 0.0.0.0:135 TOSHIBA-PC:0 LISTENING
TCP 0.0.0.0:445 TOSHIBA-PC:0 LISTENING
TCP 0.0.0.0:12025 TOSHIBA-PC:0 LISTENING
TCP 0.0.0.0:12110 TOSHIBA-PC:0 LISTENING
TCP 0.0.0.0:12119 TOSHIBA-PC:0 LISTENING
TCP 0.0.0.0:12143 TOSHIBA-PC:0 LISTENING
TCP 0.0.0.0:12465 TOSHIBA-PC:0 LISTENING
TCP 0.0.0.0:12563 TOSHIBA-PC:0 LISTENING
TCP 0.0.0.0:12993 TOSHIBA-PC:0 LISTENING
TCP 0.0.0.0:12995 TOSHIBA-PC:0 LISTENING
TCP 0.0.0.0:27275 TOSHIBA-PC:0 LISTENING
TCP 0.0.0.0:49152 TOSHIBA-PC:0 LISTENING
TCP 0.0.0.0:49153 TOSHIBA-PC:0 LISTENING
TCP 0.0.0.0:49154 TOSHIBA-PC:0 LISTENING
TCP 0.0.0.0:49155 TOSHIBA-PC:0 LISTENING
TCP 0.0.0.0:49156 TOSHIBA-PC:0 LISTENING
TCP 10.100.225.195:139 TOSHIBA-PC:0 LISTENING
```

Pada command prompt setelah diberi perintah (netstat -a) maka ada beberapa output yang ada seperti: Protocol,Local address,Foreign address, dan State. Protocol pertama yang akan saya analisis adalah TCP, dapat dilihat diatas ada banyak protocol TCP yang ada dengan alamat dan nomor port yang berbeda serta koneksi yang dituju oleh local address pun berbeda-beda. Pada gambar diatas Protocol TCP memiliki status “LISTENING” dimana

status ini artinya adalah bahwa protocol siap untuk melakukan koneksi ke web browser yang akan saya tuju yaitu www.cnnindonesia.com. Pada gambar diatas dapat dilihat pada protocol TCP ke 1 dan ke 2 memiliki Port 135 dan 445 dimana Port ini selalu mempresentasikan layanan yang sama. Sedangkan pada Port ke 12025-49156 merupakan port yang digunakan jaringan komputer yang berbeda untuk mendukung aplikasi dan sistem operasi yang dibuat.

Jika pada gambar diatas status yang didapat dari protocol TCP adalah “LISTENING”, maka selanjutnya saya akan menjelaskan sedikit status protocol TCP lainnya, antara lain: “ESTABLISHED”, “CLOSING”, “TIME_WAIT”, “FIN_WAIT_2”.

TCP	10.100.225.195:49217	sea13:http	ESTABLISHED
TCP	10.100.225.195:49237	fe-self005:https	ESTABLISHED
TCP	10.100.225.195:49475	kul06s17-in-f3:https	ESTABLISHED
TCP	10.100.225.195:49484	sa-in-f139:https	ESTABLISHED
TCP	10.100.225.195:49514	sc-in-f155:https	CLOSING
TCP	10.100.225.195:49529	sc-in-f157:https	TIME_WAIT
TCP	10.100.225.195:49534	sc-in-f156:https	CLOSING
TCP	10.100.225.195:49633	104.244.42.72:https	FIN_WAIT_2
TCP	10.100.225.195:49634	sc-in-f156:http	TIME_WAIT
TCP	10.100.225.195:49642	sa-in-f94:https	TIME_WAIT
TCP	10.100.225.195:49671	70.39.184.114:http	TIME_WAIT
TCP	10.100.225.195:49683	sc-in-f113:https	ESTABLISHED
TCP	10.100.225.195:49686	sc-in-f113:https	ESTABLISHED
TCP	10.100.225.195:49692	a104-116-44-214:http	TIME_WAIT
TCP	10.100.225.195:49695	sa-in-f156:https	ESTABLISHED
TCP	10.100.225.195:49699	72.21.202.25:http	TIME_WAIT
TCP	10.100.225.195:49700	server-54-192-159-172:https	TIME_WAIT
TCP	10.100.225.195:49718	b2:http	TIME_WAIT
TCP	10.100.225.195:49719	8.37.229.50:http	ESTABLISHED
TCP	10.100.225.195:49720	b2:http	TIME_WAIT
TCP	10.100.225.195:49721	8.37.229.50:http	TIME_WAIT
TCP	10.100.225.195:49722	8.37.229.50:http	TIME_WAIT
TCP	10.100.225.195:49724	8.37.228.36:http	TIME_WAIT
TCP	10.100.225.195:49725	8.37.228.36:http	TIME_WAIT
TCP	10.100.225.195:49726	8.37.228.36:http	TIME_WAIT
TCP	10.100.225.195:49729	8.37.228.36:http	TIME_WAIT
TCP	10.100.225.195:49730	8.37.228.36:http	TIME_WAIT
TCP	10.100.225.195:49734	8.37.228.36:http	TIME_WAIT
TCP	10.100.225.195:49735	8.37.228.36:http	TIME_WAIT
TCP	10.100.225.195:49736	202.172.183.77:http	FIN_WAIT_2
TCP	10.100.225.195:49742	5.196.118.61:http	TIME_WAIT
TCP	10.100.225.195:49743	5.196.118.61:http	TIME_WAIT

Pada protocol TCP dengan status “ESTABLISHED” menandakan bahwa koneksi yang dijalankan telah dibangun dan client server siap untuk mengirim dan menerima data. Pada protocol TCP dengan status “CLOSING” menandakan bahwa proses terhenti dan pengirim sudah menutup proses selanjutnya. Pada protocol TCP dengan status “TIME_WAIT” merupakan waktu yang dibutuhkan untuk memastikan TCP menerima status acknowledgment pada saat menghentikan koneksi. Pada protocol TCP dengan status “FIN_WAIT_2” menandakan bahwa penerima sudah mendengar bahwa pengirim mempersilahkan untuk pergi, karena semua proses yang dilakukan sudah selesai. Sama halnya pada gambar sebelumnya pada gambar ini menunjukkan port dari range 49217-49743, port ini merupakan port yang ditetapkan oleh sistem operasi atau aplikasi yang digunakan untuk melayani request dari pengguna sesuai dengan kebutuhan. Port ini dapat digunakan dan dilepaskan sesuai kebutuhan.

Selanjutnya pada software aplikasi wireshark saya akan menganalisis protocol HTTP.

47	2.90059800	10.100.225.195	203.190.245.30	TCP	55	49240-80	[ACK]	Seq=1 Ack=1 win=68 Len=1
48	3.18760300	10.100.225.195	203.190.242.68	TCP	54	49283-80	[FIN, ACK]	Seq=1 Ack=1 win=17520 Len=0
49	3.18987000	10.100.225.195	203.190.242.68	TCP	54	49284-80	[FIN, ACK]	Seq=1 Ack=1 win=17520 Len=0
50	3.19080500	10.100.225.195	203.190.242.68	TCP	54	49285-80	[FIN, ACK]	Seq=1 Ack=1 win=17520 Len=0
51	3.19133700	10.100.225.195	203.190.242.68	TCP	54	49282-80	[FIN, ACK]	Seq=1 Ack=1 win=17520 Len=0
52	3.42008900	Complex_22:cf:fa	LiteonTe_7c:17:25	ARP	60	10.100.224.1	is at	00:80:48:22:cf:fa
53	3.42265900	203.190.245.30	10.100.225.195	TCP	66	80-49293	[SYN, ACK]	Seq=0 Ack=1 win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=256
54	3.42266500	203.190.245.30	10.100.225.195	TCP	66	80-49294	[SYN, ACK]	Seq=0 Ack=1 win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=256
55	3.42266700	203.190.242.68	10.100.225.195	TCP	54	80-49283	[ACK]	Seq=1 Ack=2 win=29200 Len=0
56	3.42266800	203.190.242.68	10.100.225.195	TCP	54	80-49283	[FIN, ACK]	Seq=1 Ack=2 win=29200 Len=0
57	3.42267000	203.190.245.30	10.100.225.195	TCP	66	80-49295	[SYN, ACK]	Seq=0 Ack=1 win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=256
58	3.42411000	10.100.225.195	203.190.242.68	TCP	54	49283-80	[ACK]	Seq=2 Ack=2 win=17520 Len=0
59	3.42450700	10.100.225.195	203.190.245.30	TCP	54	49293-80	[ACK]	Seq=1 Ack=1 win=17408 Len=0
60	3.42463800	10.100.225.195	203.190.245.30	TCP	54	49294-80	[ACK]	Seq=1 Ack=1 win=17408 Len=0
61	3.42476300	10.100.225.195	203.190.245.30	TCP	54	49295-80	[ACK]	Seq=1 Ack=1 win=17408 Len=0
62	3.43609000	10.100.225.195	203.190.245.30	TCP	66	49297-80	[SYN]	Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
63	3.45458200	203.190.245.30	10.100.225.195	TCP	66	80-49296	[SYN, ACK]	Seq=0 Ack=1 win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=256
64	3.45458700	10.100.130.10	10.100.225.195	DNS	83	Standard query	response	0x7483
65	3.45459000	10.100.130.5	10.100.225.195	DNS	83	Standard query	response	0x7483
66	3.45501600	10.100.225.195	203.190.245.30	TCP	54	49296-80	[ACK]	Seq=1 Ack=1 win=17408 Len=0
67	3.45874600	10.100.225.195	203.190.245.30	HTTP	408	GET / HTTP/1.1		

Pada capture data nomor 67 pada gambar diatas, dapat dilihat bahwa protocol HTTP ditangkap saat meload situs cnnindoneisa. Protocol HTTP didapat karena data yang sedang diakses melalui world wide web. Jika ada request maka sesegera mungkin server akan merespon permintaan client. Dan respon yang diterima yaitu GET, dimana pada proses ini GET akan mengambil data dari web server dengan menentukan parameter dibagian URL dari permintaan. Pada capture data yang saya lakukan munculnya protocol HTTP tidak banyak seperti TCP dan yang lainnya.

Jika pada software aplikasi wireshark terdapat protocol HTTP yang muncul maka pada command prompt tidak ada satupun protocol HTTP yang muncul.

Protocol lainnya yang akan saya analisis adalah protocol SSDP.

No.	Time	Source	Destination	Protocol	Length	Info
109	4.84580600	10.100.225.195	203.190.245.30	TCP	90	[TCP Dup ACK #0#6] 49294-80 [ACK] Seq=355 Ack=1 win=17408 Len=0 SLE=5841 SRE=8761 SLE=13141 SRE=146
110	4.88998000	10.100.225.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
111	4.89248900	10.100.225.218	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
112	4.89346500	10.100.225.141	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
113	4.89445200	Azurewav_ce:f2:b5	Broadcast	ARP	60	who has 10.100.224.248? Te1l 10.100.225.225

Pada nomor 110-112 terdapat protocol SSDP yang muncul pada saat capture data. Sebenarnya tidak hanya ini protocol SSDP yang muncul tapi masih banyak lagi SSDP yang muncul saat capture data namun saya memberikan beberapa protocol SSDP yang ada saja. Adanya protocol SSDP disini adalah sebuah protocol yang universal yang biasa digunakan dalam beberapa perangkat jaringan komputer, seperti sistem operasi yang saya gunakan yaitu Windows 7. SSDP menggunakan notifikasi pengumuman yang ditawarkan oleh protocol HTTP yang memberikan URI (Universal Resource Identifier) untuk tipe layanan dan juga USN (Unique Service Name). SSDP juga didukung oleh banyak perangkat firewall, dimana host komputer yang berada dibelakangnya bisa membuka lubang untuk beberapa aplikasi. SSDP disini juga sebagai media pertukaran antara komputer dan media center.

Jika pada software aplikasi wireshark terdapat protocol SSDP yang muncul maka pada command prompt tidak ada satupun protocol SSDP yang muncul.

Protocol lainnya yang akan saya analisis adalah protocol ARP.

No.	Time	Source	Destination	Protocol	Length	Info
73	3.80062400	10.100.225.195	203.190.245.30	TCP	55	[TCP Keep-Alive] 49240-80 [ACK] Seq=1 Ack=1 Win=68 Len=1
74	3.97173200	10.100.224.193	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
75	4.17259600	HonHaiPr_bd:95:bf	Broadcast	ARP	42	Gratuitous ARP for 10.100.225.63 (Request)

Pada capture data nomor 75 pada gambar diatas, dapat dilihat bahwa protocol ARP ditangkap saat meload situs cnnindoneisa. Dari capture data yang saya lakukan, munculnya protocol ARP tidak hanya 1 atau 2 saja namun banyak protocol ARP yang didapat. Protocol ARP merupakan protocol yang penting dalam jaringan. (Request) yang terdapat pada gambar pada protocol ini adalah host yang bergabung atau terhubung dalam jaringan LAN saling berkomunikasi menggunakan alat fisik (MAC Address) dan tidak menggunakan IP address. Jadi sebuah host yang ingin berkomunikasi dengan host lain harus mengetahui MAC address yang dimiliki oleh host tujuannya tersebut. Host bisa mendapatkan informasi mengenai MAC address dari host tujuannya ketika tahapan transfer data dilakukan. Sebelum sebuah data diberikan MAC address, terlebih dahulu data tersebut diberi alamat logis berupa IP address. IP address yang ditambahkan ini merupakan IP address dari host pengirim dan penerima. Baru kemudian menentukan alamat fisik MAC address dari host tujuan. Dapat disimpulkan bahwa protocol ARP ini bertugas sebagai penerjemah alamat logis berupa IP address menjadi alamat fisik yaitu MAC address.

Jika pada software aplikasi wireshark terdapat protocol ARP yang muncul maka pada command prompt tidak ada satupun protocol ARP yang muncul.

Protocol lainnya yang akan saya analisis adalah NBNS.

No.	Time	Source	Destination	Protocol	Length	Info
504	24.5277130	10.100.130.5	10.100.225.195	DNS	204	Standard query response 0x5b5a CNAME star-mini.c10r.facebook.com A 31.13.78.35 A 157.240.7.35
505	24.5280110	10.100.130.10	10.100.225.195	DNS	204	Standard query response 0x5b5a CNAME star-mini.c10r.facebook.com A 31.13.78.35 A 157.240.7.35
506	24.5281480	74.125.200.91	10.100.225.195	TLSv1.2	100	Application Data
507	24.6236440	10.100.225.195	10.100.239.255	NBNS	92	Name query NB WPAD<00>
508	24.7258680	52.32.150.180	10.100.225.195	TCP	66	[TCP Keep-Alive ACK] 443-49229 [ACK] Seq=1 Ack=1 Win=83 Len=0 SLE=0 SRE=1
509	24.8006770	10.100.225.195	74.125.200.91	TCP	54	49259-443 [ACK] Seq=47 Ack=47 Win=63 Len=0
510	24.8009980	10.100.225.195	203.190.245.30	TCP	55	[TCP Keep-Alive] 49250-80 [ACK] Seq=0 Ack=0 Win=62 Len=1
511	24.9604770	10.100.130.10	10.100.225.195	DNS	417	Standard query response 0xd53d A 23.9.182.20
512	24.9608080	10.100.130.10	10.100.225.195	DNS	204	Standard query response 0x2158 CNAME star-mini.c10r.facebook.com A 157.240.7.35 A 31.13.78.35
513	25.0276260	10.100.225.195	203.190.242.71	TCP	54	49306-80 [FIN, ACK] Seq=1 Ack=1 Win=17408 Len=0
514	25.0280330	10.100.225.195	203.190.242.71	TCP	54	49305-80 [FIN, ACK] Seq=1 Ack=1 Win=17408 Len=0
515	25.0290080	10.100.225.195	10.100.130.10	DNS	84	Standard query 0x2d52 AAAA e144.dscb.akamaiedge.net
516	25.0337480	10.100.225.195	10.100.130.10	DNS	87	Standard query 0x48c5 A star-mini.c10r.facebook.com
517	25.0619820	10.100.226.31	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
518	25.1506680	10.100.225.195	10.100.239.255	NBNS	92	Name query NB WPAD<00>

Pada capture data nomor 518 pada gambar diatas, dapat dilihat bahwa protocol NBNS ditangkap saat meload situs cnnindoneisa. Dari capture data yang saya lakukan, munculnya protocol NBNS tidak hanya 1 atau 2 saja namun banyak protocol NBNS yang didapat. Pada protocol NBNS adalah protocol Netbios yang digunakan oleh aplikasi di OS window untuk digunakan pada protocol TCP/IP, maka ketika OS window melakukan koneksi internet protocol NBNS akan muncul di capture data wireshark.

Jika pada software aplikasi wireshark terdapat protocol NBNS yang muncul maka pada command prompt tidak ada satupun protocol NBNS yang muncul.

Protocol lainnya yang akan saya analisis adalah DNS.

No.	Time	Source	Destination	Protocol	Length	Info
540	26.5477920	10.100.130.5	10.100.225.195	DNS	188	standard query response 0x2158 CNAME star-mini.c10r.facebook.com A 157.240.7.35
541	26.5529570	23.9.182.20	10.100.225.195	TCP	66	80-49310 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=32
542	26.5533900	10.100.225.195	23.9.182.20	TCP	54	49310-80 [ACK] Seq=1 Ack=1 Win=17408 Len=0

Pada capture data nomor 540 pada gambar diatas, dapat dilihat bahwa protocol DNS ditangkap saat meload situs cnnindoneisa. Dari capture data yang saya lakukan, munculnya protocol DNS tidak hanya 1 atau 2 saja namun banyak protocol DNS yang didapat. DNS merupakan sebuah sistem yang berfungsi untuk menerjemahkan alamat IP ke nama domain atau sebaliknya, dari nama domain ke alamat IP. Jadi host komputer mengirimkan queries berupa nama komputer dan domain name server yang kemudian dipetakan dalam alamat IP oleh DNS. Seperti gambar diatas ketika mengetikkan alamat website cnnindonesia.com maka DNS akan menerjemahkannya kedalam alamat IP: 10.100.130.5 agar dapat dimengerti oleh komputer.

Jika pada software aplikasi wireshark terdapat protocol DNS yang muncul maka pada command prompt tidak ada satupun protocol DNS yang muncul.

Protocol lainnya yang akan saya analisis adalah LLMNR.

No.	Time	Source	Destination	Protocol	Length	Info
828	33.2233500	10.100.225.195	10.100.130.10	DNS	89	standard query 0x2979 A d31qbv1cthccecs.cloudfront.net
829	33.2534300	203.190.242.68	10.100.225.195	TCP	66	[TCP Spurious Retransmission] 80-49329 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1
830	33.2534350	203.190.242.71	10.100.225.195	TCP	66	[TCP Spurious Retransmission] 80-49331 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1
831	33.2536500	10.100.225.195	203.190.242.68	TCP	66	[TCP Dup ACK 737#1] 49329-80 [ACK] Seq=125 Ack=1 Win=17408 Len=0 SLE=0 SRE=1
832	33.2539320	10.100.225.195	203.190.242.71	TCP	66	[TCP Dup ACK 738#1] 49331-80 [ACK] Seq=325 Ack=1 Win=17408 Len=0 SLE=0 SRE=1
833	33.2916180	10.100.225.195	10.100.130.5	DNS	76	Standard query 0xf6bc A ocsip.godaddy.com
834	33.2916190	10.100.225.195	10.100.130.10	DNS	76	Standard query 0xf6bc A ocsip.godaddy.com
835	33.4999240	10.100.225.195	203.190.242.71	TCP	66	[TCP Retransmission] 49335-80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
836	33.5001670	10.100.225.195	23.9.182.20	TCP	55	[TCP Retransmission] 49308-80 [ACK] Seq=0 Ack=1 Win=17408 Len=1
837	33.5002900	10.100.225.195	203.190.242.71	TCP	66	[TCP Retransmission] 49334-80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
838	33.5019530	10.100.225.195	203.190.242.71	TCP	66	[TCP Retransmission] 49333-80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
839	33.5659830	10.100.225.36	224.0.0.252	LLMNR	64	Standard query 0x6c48 A wpad
840	33.5663310	fe80::8956:11c:4545:ff02::1:3		LLMNR	84	Standard query 0x7cec AAAA wpad

Pada capture data nomor 839,840 pada gambar diatas, dapat dilihat bahwa protocol LLMNR ditangkap saat meload situs cnnindoneisa. LLMNR merupakan protocol berdasarkan DNS (Domain Name System) yang memungkinkan kedua Ipv4 dan Ipv6 host untuk melakukan resolusi nama host pada link lokal yang sama. Seperti pada OS Windows 7 yang saya gunakan.

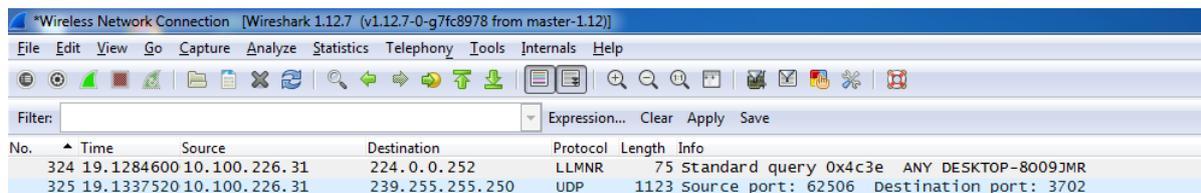
Jika pada software aplikasi wireshark terdapat protocol LLMNR yang muncul maka pada command prompt tidak ada satupun protocol LLMNR yang muncul.

Protocol lainnya yang akan saya analisis adalah protocol OCSP.

No.	Time	Source	Destination	Protocol	Length	Info
2329	55.1928440	23.15.155.27	10.100.225.195	OCSP	363	Response
2345	55.2371380	203.190.242.68	10.100.225.195	HTTP	1223	HTTP/1.1 200 OK (JPEG JFIF image)
2374	55.7107110	77.234.41.23	10.100.225.195	HTTP	234	HTTP/1.1 200 OK (application/octet-stream)
2375	55.718750	10.100.225.195	77.234.41.23	HTTP	344	GET /R/A28kIGuyZdcxvWQwY2YxNDRhZk4NTdi0GU50TFjNjIHMDRhEgQBfkwGL4BIgIh_KgcIBDDf4e9GmoIABCH4-9GGIAC
2389	55.9890650	10.100.224.170	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
2421	56.3001630	10.100.224.170	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
2435	56.4999030	10.100.225.195	23.9.182.20	HTTP	377	[TCP Retransmission] GET / HTTP/1.1

Pada capture data nomor 2329 pada gambar diatas, dapat dilihat bahwa protocol OCSP ditangkap saat meload situs cnnindoneisa. Protocol OCSP adalah protokol Internet yang digunakan untuk memperoleh status pencabutan suatu X.509 sertifikat digital. Hal ini dibuat sebagai alternatif untuk daftar pencabutan sertifikat (CRL), khusus menangani masalah-masalah tertentu yang terkait dengan penggunaan CRL dalam infrastruktur kunci publik (PKI). Pesan dikomunikasikan melalui OCSP dikodekan dalam ASN.1 dan biasanya dikomunikasikan melalui HTTP. Di "permintaan / tanggapan" sifat pesan ini mengarah ke OCSP server yang disebut responden OCSP. Dalam protocol ini terjadi proses response yang menandakan bahwa proses yang dijalankan protocol ini berjalan dengan baik.

Protocol lainnya yang akan saya analisis adalah UDP.



The screenshot shows a Wireshark capture of network traffic. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, Help), a toolbar with various icons, and a filter field. The main pane displays a list of captured packets with the following data:

No.	Time	Source	Destination	Protocol	Length	Info
324	19.1284600	10.100.226.31	224.0.0.252	LLMNR	75	Standard query 0x4c3e ANY DESKTOP-8009JMR
325	19.1337520	10.100.226.31	239.255.255.250	UDP	1123	Source port: 62506 Destination port: 3702

Pada capture data nomor 325 pada gambar diatas, dapat dilihat bahwa protocol UDP ditangkap saat meload situs cnnindoneisa. Pada capture data ini hanya sedikit protocol UDP yang didapat. Pada protocol UDP data yang dikirimkan dalam bentuk packet tidak harus melakukan call setup. Selain itu, data dalam protocol UDP akan dikirimkan sebagai datagram tanpa adanya nomor identifier. Pada gambar diatas dapat dilihat bahwa pada protocol UDP terdapat source port: 62506 dan destination port: 3702. Nomor port ini digunakan untuk mengelompokkan port-port untuk dapat digunakan sebagai server untuk UDP. Paket berisi port client dan port sumber berbentuk file text dikirimkan ke server dalam UDP header, UDP bertujuan untuk membaca nomor port tujuan dan memproses data.

```
C:\Windows\system32\cmd.exe
UDP 0.0.0.0:5355 ***
UDP 0.0.0.0:55628 ***
UDP 0.0.0.0:55639 ***
UDP 0.0.0.0:55641 ***
UDP 0.0.0.0:55643 ***
UDP 0.0.0.0:55645 ***
UDP 0.0.0.0:55647 ***
UDP 0.0.0.0:55649 ***
UDP 0.0.0.0:55651 ***
UDP 0.0.0.0:55653 ***
UDP 10.100.225.195:137 ***
UDP 10.100.225.195:138 ***
UDP 10.100.225.195:1900 ***
UDP 127.0.0.1:1900 ***
UDP 127.0.0.1:50817 ***
UDP 127.0.0.1:55638 ***
UDP 127.0.0.1:55640 ***
UDP 127.0.0.1:55642 ***
UDP 127.0.0.1:55644 ***
UDP 127.0.0.1:55646 ***
UDP 127.0.0.1:55648 ***
UDP 127.0.0.1:55650 ***
UDP 127.0.0.1:55652 ***
UDP 192.168.56.1:137 ***
UDP 192.168.56.1:138 ***
UDP 192.168.56.1:1900 ***
UDP [::1]:5355 ***
UDP [::1]:1900 ***
UDP [::1]:50816 ***
UDP [fe80::2ca9:523e:9e47:c5e1%16]:546 ***
UDP [fe80::2ca9:523e:9e47:c5e1%16]:1900 ***
UDP [fe80::e51b:8a5:b867:c99c%12]:546 ***
UDP [fe80::e51b:8a5:b867:c99c%12]:1900 ***
```

Pada command prompt protocol UDP memiliki port dari skala 5355-50826 dimana nomor-nomor port ini adalah ephemeral port, namun tetap saja tidak menutup kemungkinan nilai ephemeral port mempunyai nilai diluar range ini, hal tersebut bergantung dari sistem operasi yang digunakan.