JARINGAN KOMPUTER

NAMA : KARYN VUSVYTA

NIM : 09011181419007

KELAS : SK5A

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

FAKULTAS ILMU KOMPUTER

JURUSAN SISTEM KOMPUTER

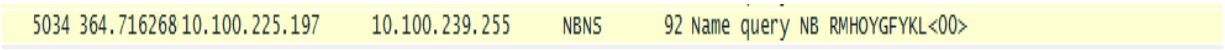
UNIVERSITAS SRIWIJAYA

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 mozila. Web browser yang saya pakai adalah www.cnnindonesia.com. Kemudian sya 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.



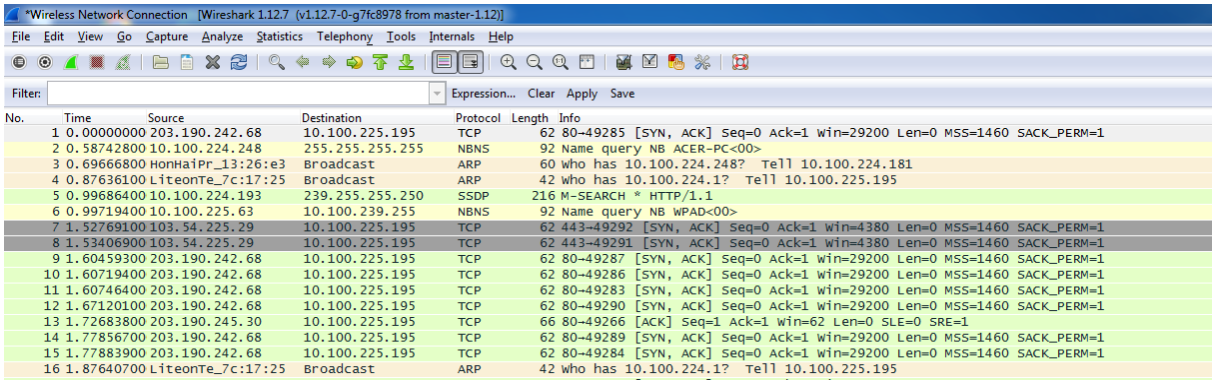
Sedangkan saat saat menggunakan command prompt perintah yang saya gunakan adalah (netstat –a). Netstat (Network Statistic) adalak program berbasis teks yang berfungsi untuk memantau koneksi jaringan pada suatu komputer, baik jaringan lokal (LAN) maupun jaringan internet. Perintah (netstat –a) akan menampilkan 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 sebelumya. Pada acapture 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:

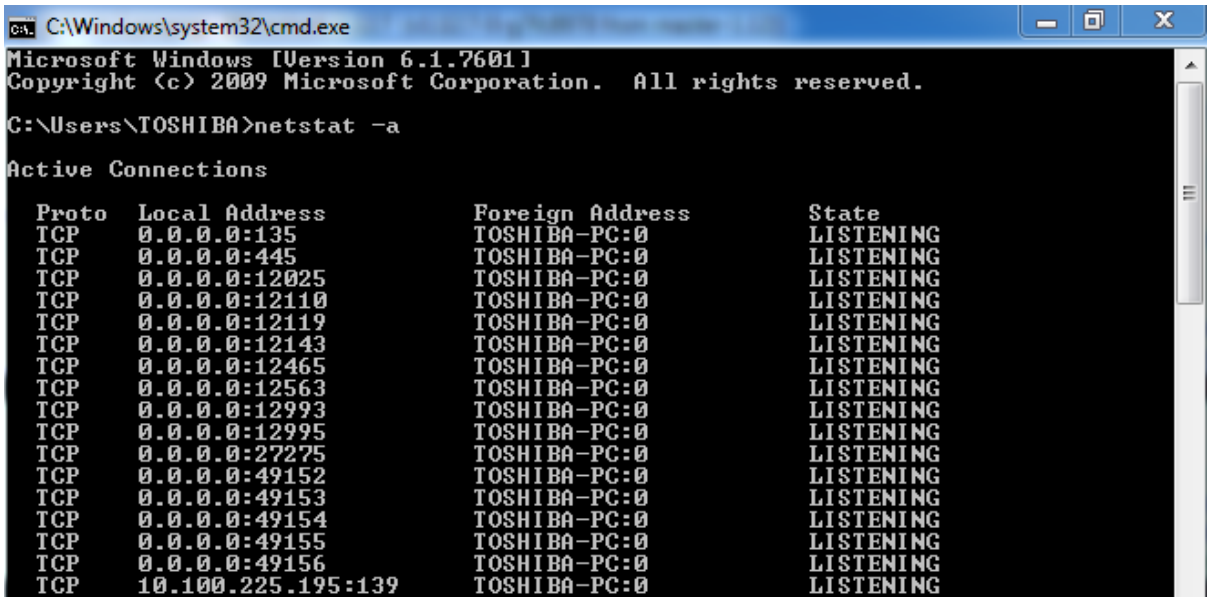
1. TCP (Transmission Control Protocol)
2. NBNS (Netbios Name Service)
3. ARP (Address Resolution Protocol)
4. SSDP (Simple Service Discovery Protocol)
5. DNS (Domain Name System)
6. OCSP (Online Certificate Status Protocol)
7. HTTP (Hyper Text Transfer Protocol)
8. LLMNR (Link-Local Multicast Name Resolution)
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)



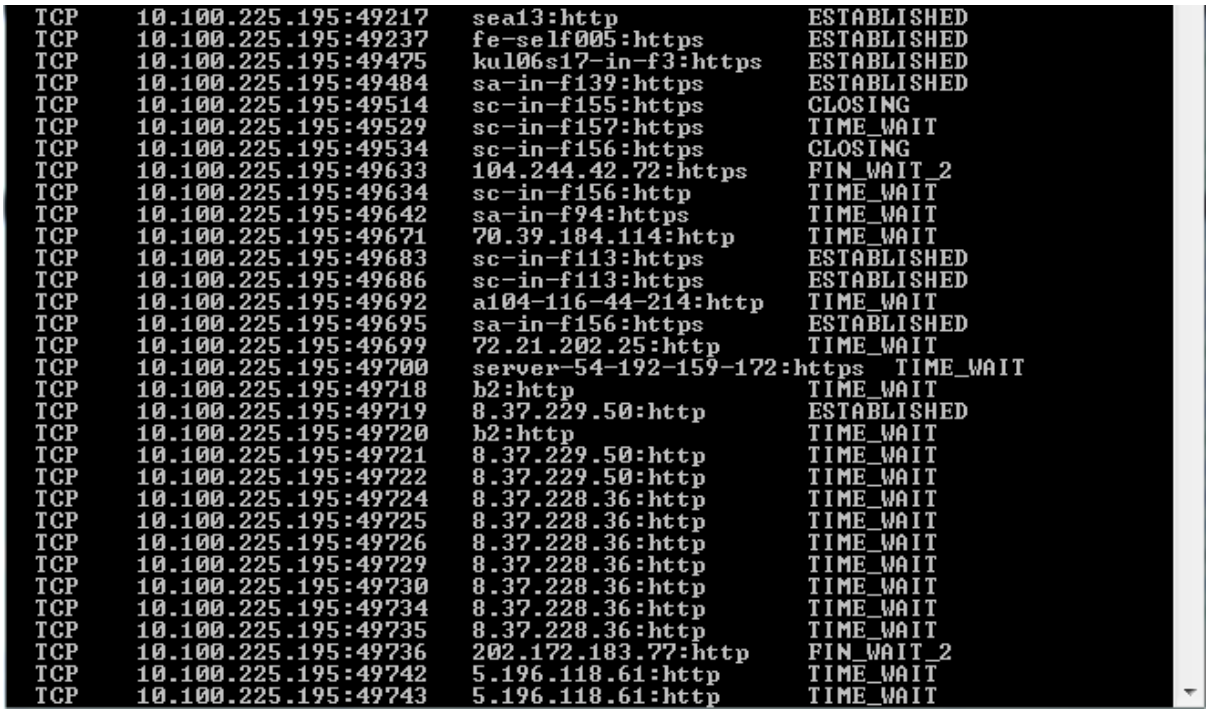
Pada gambar diatas akan saya analisa capture data pada nomor 1 source beralamatkan IP 203.190.242.68 dan destination beralamatkan IP 10.100.225.195. pada alamat IP ini memiliki alamat source port dan destination port yaitu TCP (Transmission Control Protocol), protocol ini akan menjamin data yang dikirimkan 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.



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”.



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 acknowladgment pada saat menhentikan konkesi. 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 malayani request dari pengguna sesuai dengan kebutuhan. Port ini dapat digunakan dan dilepaskan sesuai kebutuhan.

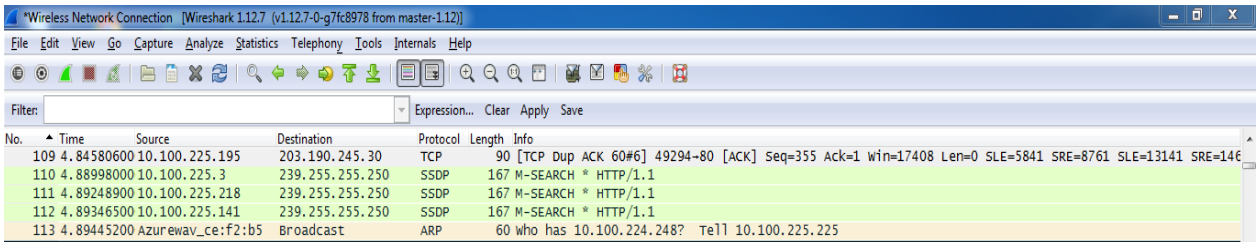
Selanjutnya pada software aplikasi wireshark saya akan menganalisis protocol HTTP.

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	Compex_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.

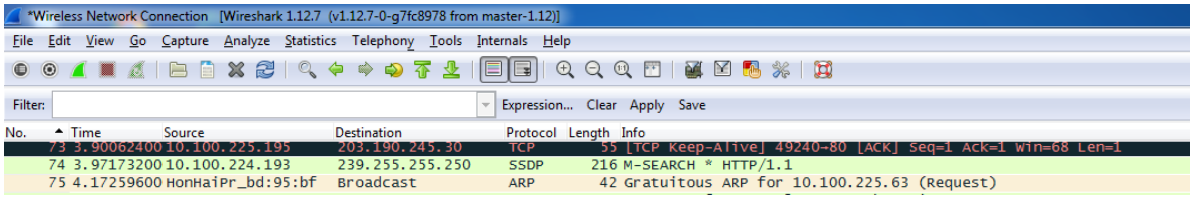
Protocol lainnya yang akan saya analisis adalah protocol SSDP.



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.

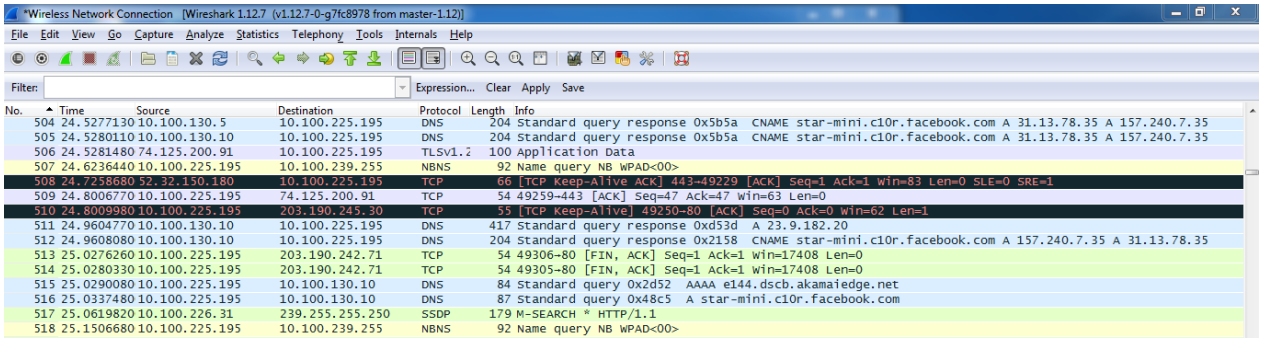
Protocol lainnya yang akan saya analisis adalah protocol ARP.



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.

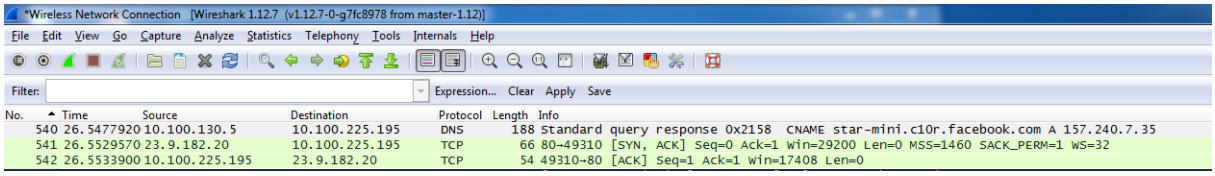
Protocol lainnya yang akan saya analisis adalah NBNS.



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.

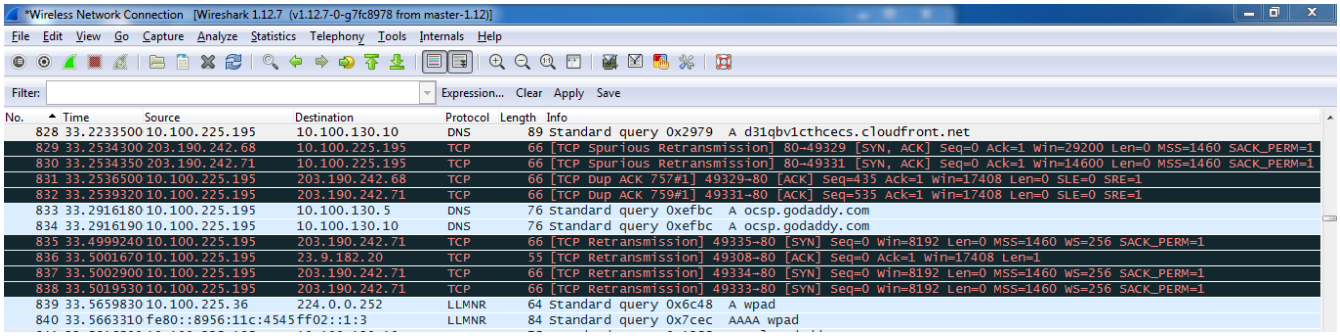
Protocol lainnya yang akan saya analisis adalah DNS.



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.

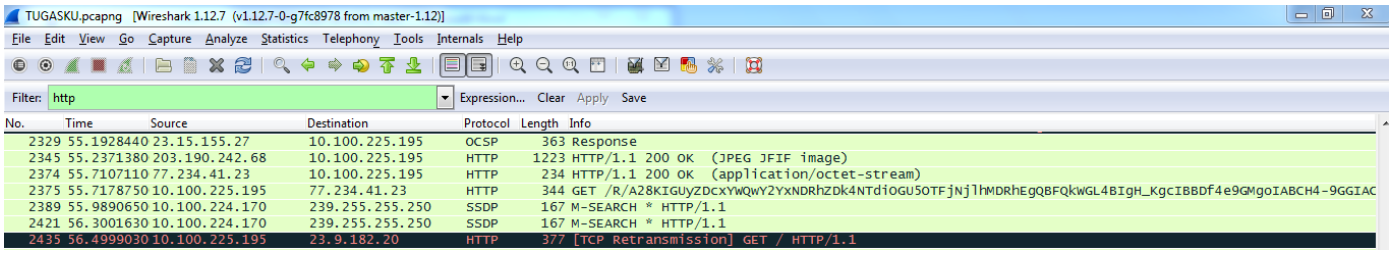
Protocol lainnya yang akan saya analisis adalah LLMNR.



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.

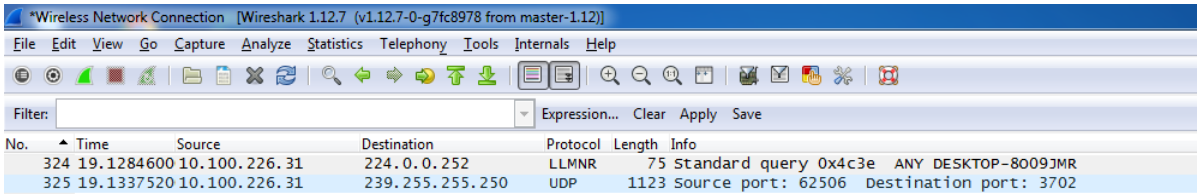
Jika pada software aplikasi wireshark terdapat protocol LLMNR yang muncul maka pada command prompt tidak ada satupun protocol LLMNR yang muncul.

Protocol lainnya yang akan saya analisis adalah protocol OCSP.

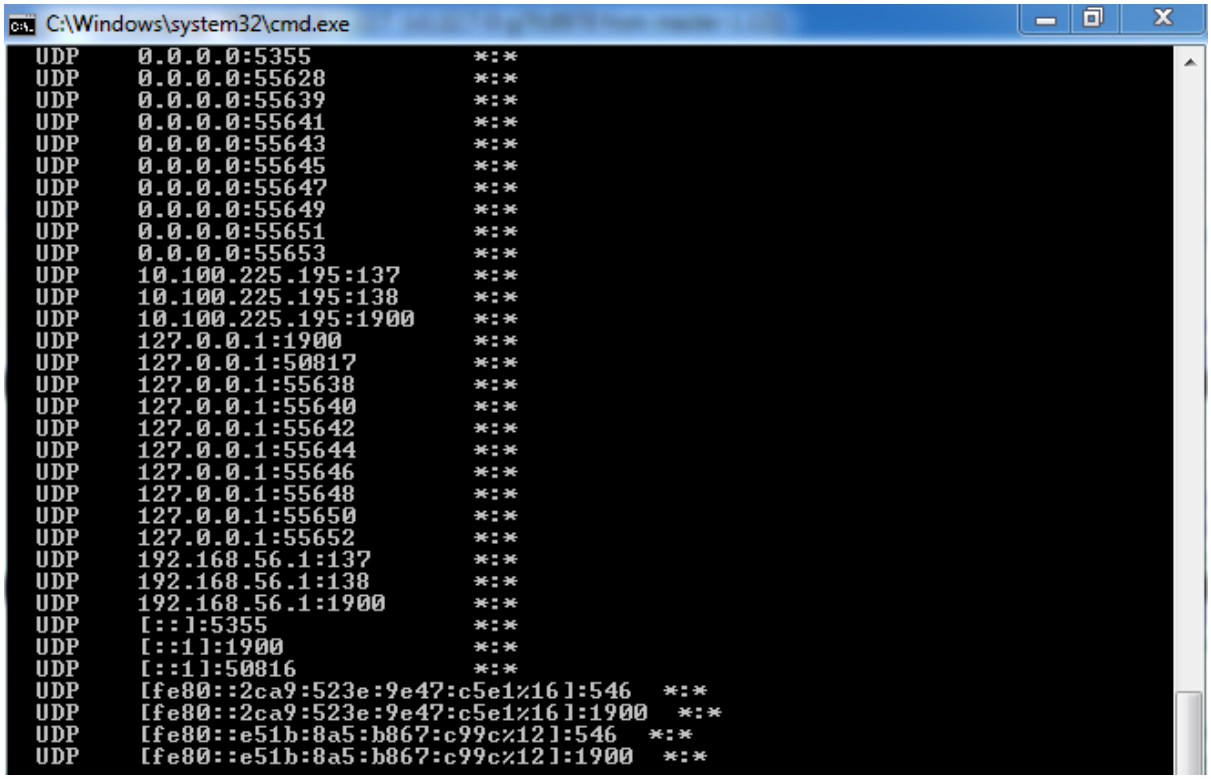


Pada capture data nomor 2329 pada gambar diatas, dapat dilihat bahwa protocol OCSP ditangkap saat meload situs cnnindoneisa. Protocol OCSP adalah protokol Internet yang digunakan untuk memperoleh status pencabutan suatu X.509 sertifikat digital. Hal ini dibuat sebagai alternatif untuk daftar pencabutan 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.



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.



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.