

Mengintip Proses Request Data dengan Wireshark

Sekar Langit

Sekarlangit9312@gmail.com

<http://theflowerofsky.blogspot.com>

Lisensi Dokumen:

Copyright © 2003-2007 IlmuKomputer.Com

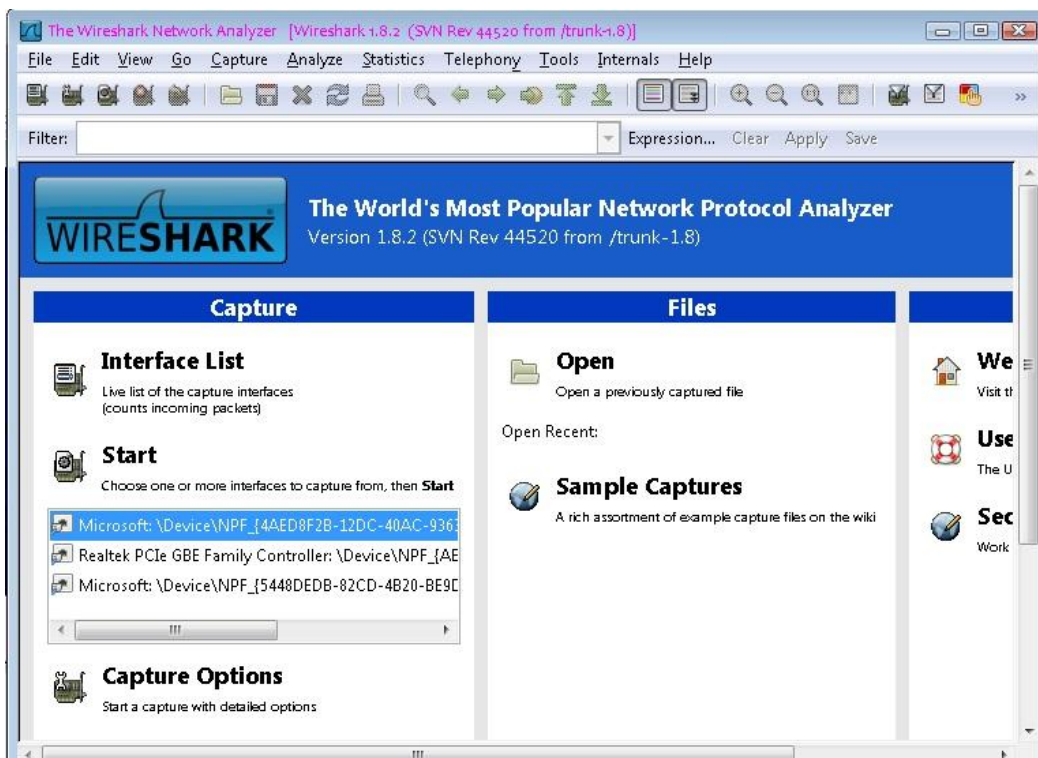
Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.

Dalam kehidupan sehari-hari anak muda jaman sekarang tentunya lekat sekali dengan teknologi yang bernama internet. Apapun yang kita cari dari mulai bahan kuliah, game-game terbaru, film-film box office, lagu yang sedang populer, resep masakan, sampai denah lokasi bisa kita temukan dengan mudah disana. Maka tidak heran kalau cara mengumpulkan informasi dengan mencari referensi di perpustakaan konvensional sudah mulai agak terlupakan dan digantikan dengan browsing di internet.

Tapi apakah kita pernah berpikir proses apa saja yang terjadi dalam “cloud” saat kita mencoba mengakses sebuah website di internet ??

Nah kali ini saya akan mengupas perjalanan data dari proses requesting sampai data tersebut muncul di layar komputer kita. Software yang saya gunakan adalah wireshark.

1. Jalankan aplikasi wireshark di komputer kita.



2. Klik 'interface list' lalu pilih interface yang aktif (bisa dilihat dari angka yang muncul di sebelah nama interface, jika 0 berarti tidak aktif.)
3. Setelah itu buka web browser dan coba mengakses sebuah situs. Sebagai contoh saya akan mencoba mengakses situs kampus saya yaitu www.polines.ac.id



4. Lihat paket yang tercapture di wireshark, disitu terlihat bahwa komputer saya dengan IP address 10.10.43.149 merequest alamat www.polines.ac.id. Karena komputer saya belum mengetahui alamat IP dari DNS tersebut maka terlebih dahulu request akan dikirimkan ke DNS server untuk mengetahui alamat IP dari website www.polines.ac.id.

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
374	11.060174	Dell_e6:7e:a9	Broadcast	ARP	60	who has 10.10.43.90? Tell 10.10.42.6
375	11.126255	10.10.43.149	8.8.8.8	DNS	77	Standard query A www.polines.ac.id
376	11.260833	10.10.42.190	10.10.43.255	NBNS	92	Name query NB ISAIAP<00>
377	11.264019	10.10.41.238	10.10.43.255	NBNS	92	Name query NB ISATAP<00>
378	11.277295	169.254.75.39	169.254.255.255	NBNS	92	Name query NB ISATAP<00>
379	11.287396	10.10.41.159	10.10.43.255	NBNS	92	Name query NB ISATAP<00>
380	11.465293	10.10.41.44	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
381	11.470612	Azurewav_56:94:c1	Broadcast	ARP	60	who has 10.10.43.60? Tell 10.10.40.247
382	11.475407	10.10.43.14	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x3f3a63fc
383	11.479548	10.10.40.4	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x3f3a63fc
384	11.481298	192.168.1.185	224.0.0.252	LLMNR	64	Standard query A wpad
385	11.482785	10.10.43.14	10.10.43.255	NBNS	92	Name query NB WPAD<00>

Frame 375: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)

- Ethernet II, Src: WistronN_81:55:40 (90:a4:de:81:55:40), Dst: JuniperN_74:4e:c0 (88:e0:f3:74:4e:c0)
- Internet Protocol Version 4, Src: 10.10.43.149 (10.10.43.149), Dst: 8.8.8.8 (8.8.8.8)
- User Datagram Protocol, Src Port: 62846 (62846), Dst Port: domain (53)
- Domain Name System (query)
 - Transaction ID: 0x2723
 - Flags: 0x0100 (Standard query)
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - www.polines.ac.id: type A, class IN
 - Name: www.polines.ac.id
 - Type: A (Host address)
 - Class: IN (0x0001)

5. DNS server akan mengirimkan jawaban berupa IP address dari website www.polines.ac.id, yaitu 118.98.43.233

No.	Time	Source	Destination	Protocol	Length	Info
387	11.489989	10.10.43.149	Broadcast	ARP	60	who has 169.254.75.39? Tell 10.10.43.51
388	11.489989	D-Link_8b:f2:6e	Broadcast	ARP	60	who has 169.254.75.39? Tell 10.10.43.51
389	11.490612	8.8.8.8	10.10.43.149	DNS	107	Standard query response CNAME polines.ac.id A 118.98.43.233
390	11.490398	10.10.43.149	118.98.43.233	TCP	60	4972 > 8192 [STN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
391	11.565466	192.168.1.185	224.0.0.252	LLMNR	64	Standard query A wpad
392	11.566331	Hewlett_-36:ef:29	Broadcast	ARP	60	who has 10.10.40.1? Tell 10.10.43.52
393	11.567826	Hewlett_-36:ef:29	Broadcast	ARP	60	who has 10.10.40.1? Tell 10.10.43.52
394	11.570123	Hewlett_-36:ef:29	Broadcast	ARP	60	who has 10.10.40.1? Tell 10.10.43.52
395	11.571241	Hewlett_-36:ef:29	Broadcast	ARP	60	who has 10.10.40.1? Tell 10.10.43.52
396	11.572213	Dell_e6:77:5c	Broadcast	ARP	60	who has 10.10.42.109? Tell 10.10.42.11
397	11.667746	GemtekTe_ca:20:0b	Broadcast	ARP	42	who has 169.254.75.39? Tell 10.10.41.31
398	11.770780	192.168.1.185	192.168.1.255	NBNS	92	Name query NB WPAD<00>
399	11.772157	10.10.43.60	10.10.43.255	NBNS	92	Name query NB WPAD<00>

Type: A (Host address)
Class: IN (0x0001)

- Answers
 - www.polines.ac.id: type CNAME, class IN, cname polines.ac.id
 - Name: www.polines.ac.id
 - Type: CNAME (Canonical name for an alias)
 - Class: IN (0x0001)
 - Time to live: 13 minutes, 59 seconds
 - Data length: 2
 - Primaryname: polines.ac.id
 - polines.ac.id: type A, class IN, addr 118.98.43.233
 - Name: polines.ac.id
 - Type: A (Host address)
 - Class: IN (0x0001)
 - Time to live: 13 minutes, 59 seconds
 - Data length: 4
 - Addr: 118.98.43.233 (118.98.43.233)

6. Setelah mengetahui IP address dari www.polines.ac.id, maka barulah komputer saya dengan alamat IP 10.10.43.149 akan merequest ke alamat IP website yaitu 118.98.43.233 dengan menggunakan protokol TCP.

Protocol TCP ini adalah protocol yang terletak pada lapisan transport yang digunakan untuk melakukan browsing. Tapi sebelumnya saya akan sedikit menjelaskan tentang flag-flag pada TCP serta fungsi dari flag-flag yang ada pada program Wireshark.

- ✓ Flag URG (urgent) berfungsi untuk mengidentifikasi bahwa bagian dari TCP mengandung data yang sangat penting.
- ✓ Flag ACK (acknowledgment) berfungsi untuk mengetahui apakah data yang dikirimkan sudah diterima atau belum di komputer client.
- ✓ Flag PSH (push) berfungsi untuk mengindikasikan isi dari TCP yang diterima di komputer client. Jika PSH bernilai 1 maka data tidak boleh satu byte pun hilang, jika hilang maka data akan dikirim ulang.
- ✓ Flag RST (reset) berfungsi untuk mengidentifikasi jika koneksi yang dibuat gagal. Untuk sebuah koneksi TCP yang sedang berjalan (aktif), sebuah segmen dengan flag RST diset ke nilai 1 akan dikirimkan sebagai respons terhadap sebuah segmen TCP yang diterima yang ternyata segmen tersebut bukan yang diminta, sehingga koneksi pun menjadi gagal.
- ✓ Flag SYN berfungsi untuk mengindikasikan bahwa segmen TCP yang bersangkutan mengandung Initial Sequence Number (ISN). Selama proses pembuatan sesi koneksi TCP, jika melakukan request maka akan memberikan nilai SYN bernilai 1.
- ✓ Flag FIN (Finish) berfungsi untuk menandakan bahwa pengirim segmen TCP telah selesai dalam mengirimkan data dalam sebuah koneksi TCP. Ketika sebuah koneksi TCP akhirnya dihentikan (akibat sudah tidak ada data yang dikirimkan lagi), setiap host TCP akan mengirimkan sebuah segmen TCP dengan flag FIN diset ke nilai 1.

7. Sekarang saya akan menjelaskan proses 'three way handshake'. Pada bagian ini komputer saya dengan alamat IP 10.10.43.149 mengirimkan request ke website polines dengan alamat IP 118.98.43.233 yang ditunjukkan dengan nilai '1' pada flag SYN.

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
388	11.489989	D-Link_8b:f2:6e	Broadcast	ARP	60	who has 169.254.75.39? Tell 10.10.43.51
389	11.490612	8.8.8.8	10.10.43.149	DNS	107	Standard query response CNAME pdlines.ac.id A 118.98.43.233
390	11.496398	10.10.43.149	118.98.43.233	TCP	66	49772 > http [SYN] seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
391	11.565466	192.168.1.185	224.0.0.252	LLMNR	64	standard query A wpad
392	11.566331	Hewlett-_36:ef:29	Broadcast	ARP	60	who has 10.10.40.1? Tell 10.10.43.52
393	11.567826	Hewlett-_36:ef:29	Broadcast	ARP	60	who has 10.10.40.1? Tell 10.10.43.52
394	11.570123	Hewlett-_36:ef:29	Broadcast	ARP	60	who has 10.10.40.1? Tell 10.10.43.52
395	11.571241	Hewlett-_36:ef:29	Broadcast	ARP	60	who has 10.10.40.1? Tell 10.10.43.52
396	11.572213	Dell_e6:77:5c	Broadcast	ARP	60	who has 10.10.42.109? Tell 10.10.42.11
397	11.667746	GemtekTe_ca:20:0b	Broadcast	ARP	42	who has 169.254.75.39? Tell 10.10.41.31
398	11.770780	192.168.1.185	192.168.1.255	NBNS	92	Name query NB WPAD<00>
399	11.772157	10.10.43.60	10.10.43.255	NBNS	92	Name query NB WPAD<00>

Sequence number: 0 (relative sequence number)
 Header length: 32 bytes

Flags: 0x02 (SYN)

- 000. = Reserved: Not set
- ...0 = Nonce: Not set
- 0... = Congestion Window Reduced (CWR): Not set
-0.. = ECN-Echo: Not set
-0. = Urgent: Not set
-0 = Acknowledgement: Not set
-0.. = Push: Not set
-0 = Reset: Not set
-**.1.** = **Syn: Set**
-0 = FIN: Not set

Window size value: 8192
 [calculated window size: 8192]

Checksum: 0x0a3f [validation disabled]

8. Setelah itu server dari 118.98.43.233 membalas request dengan mengirimkan flag 'ACK' bernilai '1' yang artinya menyatakan persetujuan akses website dan mengkonfirmasi apakah tanda persetujuan telah sampai di komputer client. Terlihat pada gambar di bawah flag 'ACK' dan flag 'SYN' bernilai '1'.

No.	Time	Source	Destination	Protocol	Length	Info
405	11.888078	169.254.75.39	169.254.255.255	NBNS	92	Name query NB ISATAP<00>
406	11.889164	De11_e6:7e:1e	Broadcast	ARP	60	who has 169.254.254.254? Tell 10.10.40.87
407	11.890239	118.98.43.233	10.10.43.149	TCP	66	http > 49772 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=8
408	11.890391	10.10.43.149	118.98.43.233	TCP	54	49772 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
409	11.890994	10.10.43.149	118.98.43.233	HTTP	602	GET / HTTP/1.1
410	11.981908	De11_e6:7e:a9	Broadcast	ARP	60	who has 10.10.43.90? Tell 10.10.42.6
411	11.983186	fe80::4d82:4267:72eff02::1:3		LLMNR	90	Standard query A dirqsyoert
412	11.984286	fe80::4d82:4267:72eff02::1:3		LLMNR	90	Standard query A ccxdbvgkxx
413	11.985548	10.10.41.158	224.0.0.252	LLMNR	70	Standard query A dirqsyoert
414	11.986841	10.10.41.158	224.0.0.252	LLMNR	70	Standard query A ccxdbvgkxx
415	11.987851	fe80::4d82:4267:72eff02::1:3		LLMNR	90	Standard query A csskatyekj
416	11.988963	10.10.41.158	224.0.0.252	LLMNR	70	Standard query A csskatyekj
417	11.989070	De11_e6:7e:7f	Broadcast	ARP	60	who has 172.172.171.?? Tell 172.172.172.17

Sequence number: 0 (relative sequence number)
 Acknowledgement number: 1 (relative ack number)
 Header length: 32 bytes

Flags: 0x12 (SYN, 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. = Acknowledgement: Set
- 0.. = Push: Not set
-0.. = Reset: Not set
-1. = Syn: Set
-0 = Fin: Not set

Window size value: 5840

9. Client yang disini berarti adalah komputer saya dengan alamat IP 10.10.43.149 membalas dengan mengirimkan flag 'ACK' bernilai '1' yang berarti memberitahukan bahwa data telah diterima di komputer client. Inilah akhir dari proses three way handshake yang menghasilkan output terbangunnya hubungan antara komputer saya dengan komputer server website polines.

No.	Time	Source	Destination	Protocol	Length	Info
405	11.888078	169.254.75.39	169.254.255.255	NBNS	92	Name query NB ISATAP<00>
406	11.889164	De11_e6:7e:1e	Broadcast	ARP	60	who has 169.254.254.254? Tell 10.10.40.87
407	11.890239	118.98.43.233	10.10.43.149	TCP	66	http > 49772 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=8
408	11.890391	10.10.43.149	118.98.43.233	TCP	54	49772 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
409	11.890994	10.10.43.149	118.98.43.233	HTTP	602	GET / HTTP/1.1
410	11.981908	De11_e6:7e:a9	Broadcast	ARP	60	who has 10.10.43.90? Tell 10.10.42.6
411	11.983186	fe80::4d82:4267:72eff02::1:3		LLMNR	90	Standard query A dirqsyoert
412	11.984286	fe80::4d82:4267:72eff02::1:3		LLMNR	90	Standard query A ccxdbvgkxx
413	11.985548	10.10.41.158	224.0.0.252	LLMNR	70	Standard query A dirqsyoert
414	11.986841	10.10.41.158	224.0.0.252	LLMNR	70	Standard query A ccxdbvgkxx
415	11.987851	fe80::4d82:4267:72eff02::1:3		LLMNR	90	Standard query A csskatyekj
416	11.988963	10.10.41.158	224.0.0.252	LLMNR	70	Standard query A csskatyekj
417	11.989070	De11_e6:7e:7f	Broadcast	ARP	60	who has 172.172.171.?? Tell 172.172.172.17

Sequence number: 1 (relative sequence number)
 Acknowledgement number: 1 (relative ack number)
 Header length: 20 bytes

Flags: 0x10 (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. = Acknowledgement: Set
- 0.. = Push: Not set
-0.. = Reset: Not set
-0. = Syn: Not set
-0 = Fin: Not set

Window size value: 4380

10. Akhirnya barulah komputer server mengirimkan data melalui protokol HTTP. Seperti yang terlihat pada gambar di bawah, flag yang aktif adalah flag ACK dan flag PSH. Flag PSH berarti mengindikasikan isi dari TCP yang diterima di komputer client, jika PSH bernilai 1 maka data tidak boleh satu byte pun hilang, jika hilang maka data akan dikirim ulang.

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
405	11.888078	169.254.75.39	169.254.255.255	NBNS	92	Name query NB ISATAP<00>
406	11.889164	0e11_e6:7e:1e	Broadcast	ARP	60	who has 169.254.254.254? Tell 10.10.40.87
407	11.890239	118.98.43.233	10.10.43.149	TCP	66	http > 49772 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=8
408	11.890391	10.10.43.149	118.98.43.233	TCP	54	49772 > http [ACK] Seq=1 Ack=1 win=17520 Len=0
409	11.890994	10.10.43.149	118.98.43.233	HTTP	602	GET / HTTP/1.1
410	11.981908	0e11_e6:7e:1e	Broadcast	ARP	60	who has 10.10.43.90? Tell 10.10.42.6
411	11.983186	fe80::4d82:4267:72eff02::1:3		LLMNR	90	Standard query A oirgqsyort
412	11.984286	fe80::4d82:4267:72eff02::1:3		LLMNR	90	Standard query A ccxdbvgkxx
413	11.985548	10.10.41.158	224.0.0.252	LLMNR	70	Standard query A oirgqsyort
414	11.986841	10.10.41.158	224.0.0.252	LLMNR	70	Standard query A ccxdbvgkxx
415	11.987851	fe80::4d82:4267:72eff02::1:3		LLMNR	90	Standard query A csskatyekj
416	11.988963	10.10.41.158	224.0.0.252	LLMNR	70	Standard query A csskatyekj
417	11.989070	0e11_e6:7e:1e	Broadcast	ARP	60	who has 172.172.171.?? Tell 172.172.172.17

Sequence number: 1 (relative sequence number)
 [Next sequence number: 549 (relative sequence number)]
 Acknowledgement number: 1 (relative ack number)
 Header length: 20 bytes
 Flags: 0x18 (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... = Acknowledgement: Set
1... = Push: set
U.. = Reset: Not set
0. = Syn: Not set
0 = Fin: Not set
 Window size value: 4380

Nah begitulah proses browsing yang biasa kita lakukan sehari-hari. Selama ini mungkin kita hanya duduk di depan komputer dan menunggu proses loading selesai tanpa tahu proses yang terjadi sebenarnya. Dan ternyata prosesnya tidak sesimple yang kita bayangkan.

Biografi Penulis



Sekar Langit. Menyelesaikan pendidikan Sekolah Dasar di SD Muktiharjo Kidul 02 Semarang, SMP di SMP PL Domenico Savio Semarang, dan SMA di SMAN 5 Semarang. Sekarang sedang menempuh pendidikan jenjang D4 di Politeknik Negeri Semarang jurusan Teknik Elektro dan prodi Teknik Telekomunikasi.