

Praktikum 13

ANALISA PAKET DENGAN WIRESHARK & TCPDUMP

A. TUJUAN PEMBELAJARAN

1. Siswa mampu melakukan sniffing dengan wireshark dan tcpdump dan tahu keuntungan dan kelemahan kedua software tersebut
2. Siswa mampu melakukan analisa paket layer transport OSI (TCP dan UDP)
3. Siswa mampu melakukan analisa paket layer aplikasi Telnet dan SSH

B. DASAR TEORI

1. Sniffing

Menangkap atau mengendus(sniffing) trafik jaringan sangat berguna bagi administrator untuk menyelesaikan masalah-masalah yang muncul di jaringan, termasuk masalah keamanan. Hal ini berdasarkan fakta bahwa sejumlah penyerangan dimulai dengan penggunaan penyadap untuk melihat trafik jaringan dengan harapan melihat data-data penting yang ditransmisikan oleh user. Karena itu mempelajari kapabilitas dan keterbatasan software-software packet sniffing menjadi bagian yang penting dari kemampuan admin.

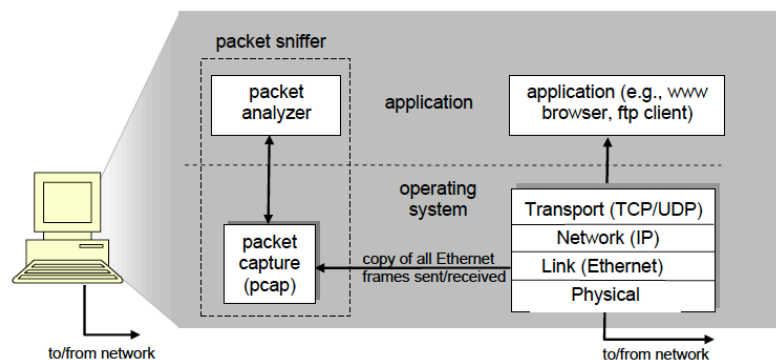


Gambar 13.1 Sniffing pada jaringan antara router 1 dan 2

Software Open Source Sniffing

Beberapa software open source yang digunakan untuk melakukan sniffing adalah :

1. TCP dump adalah tools UNIX/Linux yang banyak digunakan untuk merekam trafik jaringan berdasarkan kriteria user dan mampu menyimpan trafik dalam berbagai format yang berbeda. TCPdump umumnya digunakan pada kebanyakan distribusi linux dan dapat diperoleh di <http://www.tcpdump.org>.
2. Wireshark adalah aplikasi grafis yang banyak digunakan untuk monitoring dan analisis. Wireshark adalah opensource dan berjalan pada banyak platform OS termasuk Windows, Linux dan UNIX. Wireshark dapat didownload di <http://www.wireshark.org>.



Gambar 13.2 Blok Diagram Paket Sniffer

Bagaimana Sniffing Bekerja ?

Dalam menentukan bagaimana menyetting sniffer, topologi dan tipe jaringan harus menjadi pertimbangan. Secara lebih detail, perbedaan antara jaringan berbasis switch dan hub menjadi penentu trafik yang visible ketika sniffing dilakukan.

Ketika satu host butuh untuk berkomunikasi dengan host lain, host tersebut akan mengirim ARP request secara broadcast ke seluruh host dalam jaringan baik switch dan hub. Hanya host yang dicari akan menjawab dengan ARP reply yang berisi MAC address host tersebut. Pada jaringan berbasis switch, ketika komunikasi berjalan antara dua host, trafik diantaranya akan diisolasi oleh switch pada link fisik. Namun, pada jaringan berbasis hub, komunikasi antara kedua host dapat didengar oleh semua host yang lain pada jaringan tersebut, walaupun tidak diperhatikan.

Pasif dan Aktif Sniffing

Passive sniffing menempatkan NIC host pada mode promiscuous mode, yang artinya menangkap semua trafik yang dapat dilihat, termasuk trafik antara host yang berbeda terutama pada jaringan berbasis hub. Pada jaringan berbasis switch, passive sniffing dapat dilakukan pada switch yang melakukan SPAN atau mirror port dimana trafik secara dapat dikopikan dengan meletakkan sniffer pada port yang dimirror. Jika yang diinginkan adalah trafik yang masuk dan keluar jaringan, maka sniffer dapat diletakkan pada gateway.

Active Sniffing adalah alternative metode sniffing. Aktif sniffer mencoba mencari celah dari protocol ARP dengan melakukan ARP spoofing dengan menjawab request ARP dari host. Aktif sniffing secara aktif akan berusaha agar pemilik MAC address asli diabaikan atau dibuang dalam proses komunikasi antara host dan sniffer. Salah satu metode yang digunakan untuk active sniffing adalah MAC flooding.

2. Wireshark

Wireshark, atau dulunya dikenal sebagai Ethereal, adalah salah satu tool yang sangat ampuh untuk senjata para analis keamanan jaringan. Sebagai analyzer packet jaringan, Wireshark dapat berlaku sebagai peer di jaringan dan mengamati trafik secara detail dalam berbagai level, mulai dari header packet hingga bit yang menyusun suatu paket. Karena wireshark menggunakan GUI, banyak pengguna memperoleh kemudahan grafis dalam menggunakan informasi yang terkandung di dalamnya.

Pemakaian warna

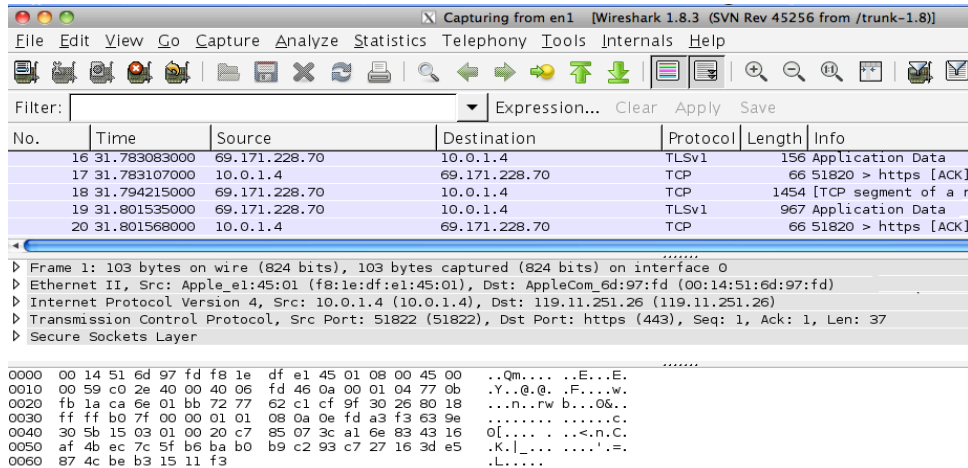
Salah satu fitur dari wireshark adalah penggunaan warna. Untuk jenis-jenis paket yang berbeda Paket-paket di wireshark diberi highlight warna hijau, biru dan hitam. Secara default, hijau adalah warna yang digunakan untuk trafik TCP, biru muda adalah warna yang digunakan untuk trafik UDP dan hitam menunjukkan paket TCP yang bermasalah (misalnya karena dikirim secara tidak berurutan)

Menggunakan hasil capture Wireshark

Bila tidak ada paket yang menarik untuk diamati, Wireshark memiliki sejumlah file

Pertemuan 12: Implementasi Lapisan Aplikasi

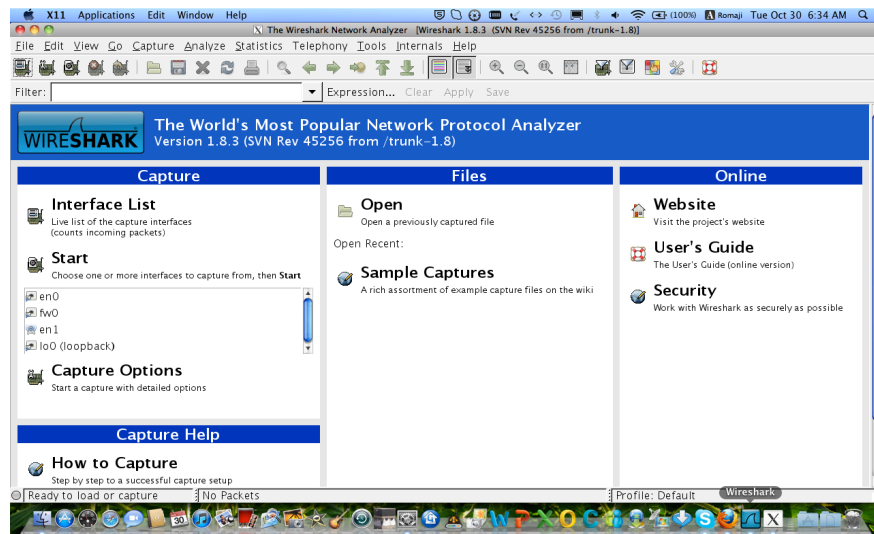
hasil capture yang dapat diload dan diinspeksi oleh user. Untuk membuka filenya mudah. Buka menu utama dan browse file yang diinginkan.



Gambar 13.3 GUI dari wireshark

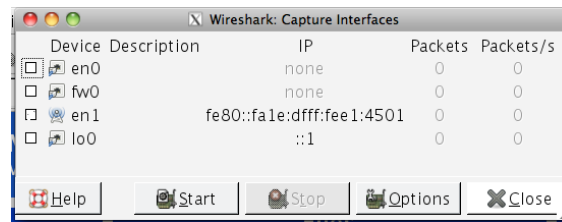
Cara Menjalankan Wireshark

1. Bukalah Wireshark



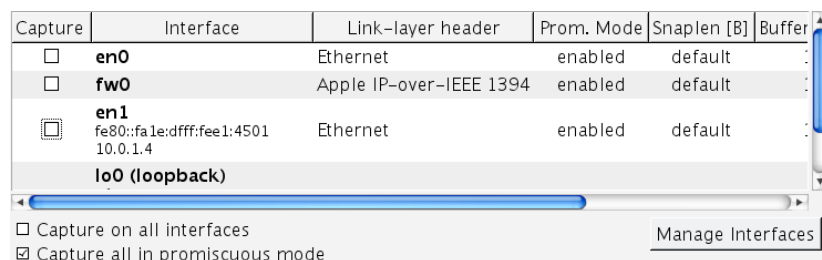
Gambar 13.4 Tampilan awal wireshark

2. Tentukan di interface mana wireshark berjalan. Pilih icon . Setelah itu akan muncul tampilan berikut :



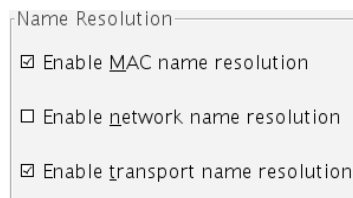
Gambar 13.5 Tampilan pilihan interface dimana wireshark beroperasi

- a. Pilih interface dimana anda melakukan sniffing.
- b. Pilih Option. Pilih Capture All in Promiscuous Mode



Gambar 13.6 Tampilan opsi capture

- c. Pada Name resolution, pilih dua opsi dari tiga, yaitu opsi enable MAC name resolution dan enable transport name resolution



Gambar 13.7 Tampilan Capture

3. Mulailah melakukan penangkapan packet. Pilih Start, pada tampilan Wireshark Capture Options
4. Akan muncul window seperti pada gambar 13.3 yang menunjukkan paket-paket yang ditangkap oleh wireshark pada subnet anda. Bagian yang paling atas, dibawah filter, disebut sebagai packet listing window. Bagian ini menunjukkan semua paket yang berhasil ditangkap oleh wireshark.

Pertemuan 12: Implementasi Lapisan Aplikasi

No.	Time	Source	Destination	Protocol	Length	Info
16	31.783083000	69.171.228.70	10.0.1.4	TLSv1	156	Applicati
17	31.783107000	10.0.1.4	69.171.228.70	TCP	66	51820 > h
18	31.794215000	69.171.228.70	10.0.1.4	TCP	1454	[TCP segm
19	31.801535000	69.171.228.70	10.0.1.4	TLSv1	967	Applicati
20	31.801568000	10.0.1.4	69.171.228.70	TCP	66	51820 > h

Gambar 13.8 Packet Listing Window

Bagian kedua adalah packet detail window, yang menunjukkan informasi paket secara detail. Detail packet window ini membedah paket dan menunjukkan field-field dari tiap layer, mulai dari Frame 1, Ethernet II, IPv4, TCP/UDP, dan aplikasi layer (SSH, Telnet, HTTP, dll)

```

> Frame 1: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface 0
> Ethernet II, Src: Apple_e1:45:01 (f8:1e:df:e1:45:01), Dst: AppleCom_6d:97:fd (00:14:51:6d:97:fd)
> Internet Protocol Version 4, Src: 10.0.1.4 (10.0.1.4), Dst: 119.11.251.26 (119.11.251.26)
> Transmission Control Protocol, Src Port: 51822 (51822), Dst Port: https (443), Seq: 1, Ack: 1, Len: 37
> Secure Sockets Layer

```

Gambar 13.9 Packet Detail Window

Bagian terakhir adalah packet content window yang berisi isi dari paket tersebut. Biasanya ditulis dalam hexa dan ascii.

```

0000  00 14 51 6d 97 fd f8 1e  df e1 45 01 08 00 45 00  ..Qm.... ..E...E.
0010  00 59 c0 2e 40 00 40 06  fd 46 0a 00 01 04 77 0b  .Y..@.@. .F....w.
0020  fb 1a ca 6e 01 bb 72 77  62 c1 cf 9f 30 26 80 18  ...n..rw b...0&..
0030  ff ff b0 7f 00 00 01 01  08 0a 0e fd a3 f3 63 9e  .....C.
0040  30 5b 15 03 01 00 20 c7  85 07 3c a1 6e 83 43 16  0[.... . ..<.n.C.

```

Gambar 13.10 Packet Content Window

5. Stoplah penangkapan paket bila anda telah mendapatkan paket yang dibutuhkan

dengan memilih 

3. TCP DUMP

Tcpdump adalah tool console yang memungkinkan anda untuk menangkap trafik raw di jaringan dan mendisplay header dari paket yang tertangkap tadi. TCPdump banyak digunakan untuk mencari masalah-masalah di jaringan atau untuk memonitor aktivitas jaringan, Tcpdump menggunakan API pcap (packet capture) yaitu , LibPcap

(Unix) atau winPcap(pada windows) untuk menangkap paket. Data hasil capture tcpdump sering disebut sebagai dumpfile.

Perbedaan utama Tcpdump dengan Wireshark adalah tcpdump tidak melakukan analisa terhadap data, namun hanya melakukan copy paket secara keseluruhan (dump raw packet data). Karena itu beban analisis terletak sepenuhnya pada user, namun demikian, kesalahan analisa yang disebabkan oleh software (semisal wireshark) dapat dihindari.

Tcpdump dapat bekerja dengan baik bila dipasang pada jaringan yang menggunakan hub. Bila tcpdump diletakkan pada jaringan berbasis switch, maka tcpdump tersebut hanya dapat melihat trafik antara user yang menggunakan tcpdump dan switch tersebut.

Tcpdump dijalankan dengan mencocokkan packet dengan opsi yang diberikan oleh user. Format penulisan tcpdump :

```
tcpdump [ -adeflnNOPqRStuvxX ] [ -c count ] [ -C file_size ] [ -F  
file ] [ -i interface ] [ -m module ] [ -r file ] [ -s snaplen ]  
[ -T type ] [ -w file ] [-E algo:secret ] [ expression ]
```

Opsi – opsi dari tcp dump ditunjukkan tabel dibawah :

Tabel 13.1 Opsi Tcpdump

-D	Melisting semua interface jaringan yang ada di system dimana tcp dump dapat menangkap paket.
-n	: Memberitahu tcpdump agar tidak melakukan konversi alamat (IP atau port address atau alamat lain) untuk menghemat waktu dan dapat beroperasi lebih cepat.
-i	memberi tahu tcp dump agar menempatkan interface jaringan dalam promiscuous mode dan memerintahkan interface jaringan untuk mendengar semua trafik yang datang.
-vvv	Menambah jumlah informasi yang didapat
-c	Berhenti menangkap paket setelah jumlah pakatnya sudah mencukupi
-C	Menspesifikasi agar ukuran file dari dumpfile harus mencapai ukuran tertentu

	sebelum membuat file baru. Ukuran file dinyatakan dalam orde jutaan byte (1,000,000 bytes, bukan 1,048,576 bytes).
-F	Menggunakan file sebagai input untuk operasi filter,
-S	Men-print absolute sequence numbers.
-p	Jangan meletakkan interface pada promiscuous mode.
-r	Membaca packet dari file (yang diciptakan sebelumnya dengan opsi -w)
-t	Jangan mengeprint timestamp pada dump file
-X	Ketika parsing dan printing, selain mengeprint header tiap paket, juga mengeprint data tiap paket, (kecuali link level header)I dalam hex dan ASCII. Opsi ini sangat berguna untuk analisa protocol baru.
-XX	Ketika parsing dan printing, selain mengeprint header tiap paket, juga mengeprint data tiap paket, termasuk link levelheader, dalam hex dan ASCII.
-E	Print header link-level header pada tiap dump line.
-z	Menghilangkan privileges (jika root) dan mengubah user ID ke user and group ID ke primary group dari user

Mengkombinasikan Opsi-Opsi dengan Operator Boolean

Tcpdump menggunakan operator boolean (AND,NOT,OR) sehingga mampu menciptakan beragam opsi gabungan yang anda butuhkan. Operator Boolean bisa bernilai TRUE atau FALSE tergantung kemampuan tcp dump untuk menterjemahkan perintah tersebut.

Tabel 13.2 Operator boolean Tcpdump

	Notasi	Arti
AND	&&	akan bernilai TRUE bila dan hanya bila kedua pernyataan/opsi bernilai TRUE.
NOT	!	akan bernilai TRUE bila pernyataan bernilai FALSE atau sebaliknya
OR		akan bernilai FALSE bila dan hanya bila salah satu atau kedua pernyataan FALSE.

Cara Menjalankan TCP dump :

Cobalah melakukan perintah-perintah ini :

1. [root@akane ~]# **tcpdump -D**

Perintah ini akan mengeprint semua NIC yang dapat digunakan tcpdump

2. [root@akane~]#**tcpdump -nnXX -i eth0 -w tcpdumpku -C 3**

Perintah ini akan menangkap semua trafik pada eth0 dan menulisnya dalam file tcpdumpku dan mengeset ukuran file sekitar 3M tanpa melakukan translasi nama dari alamat IP atau nomer port

3. [root@akane: ~]#**tcpdump -nnvvv -i eth0 host 10.0.2.2**

Perintah ini akan mengeprint semua paket yang menuju atau keluar dari ip 10.0.2.2

4. [root@akane: ~]#**tcpdump tcp and dst port 23**

Perintah ini akan mengeprint semua trafik telnet yang berada pada port 23

5. [root@akane: ~]# **tcpdump -r rawfile > textfile**

Perintah ini akan mengubah rawfile menjadi textfile

Hasil packet tracing pada tcpdump :

```
tcpdump -nn host 192.168.2.165 and port 23 tcpdump: listening on eth0
19:20:00.804501 192.168.2.10.1221 > 192.168.2.165.23:
S2565655403:2565655403(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
```

Arti masing-masing field ditunjukkan tabel dibawah :

Tabel 13.3 Deskripsi hasil trace tcpdump

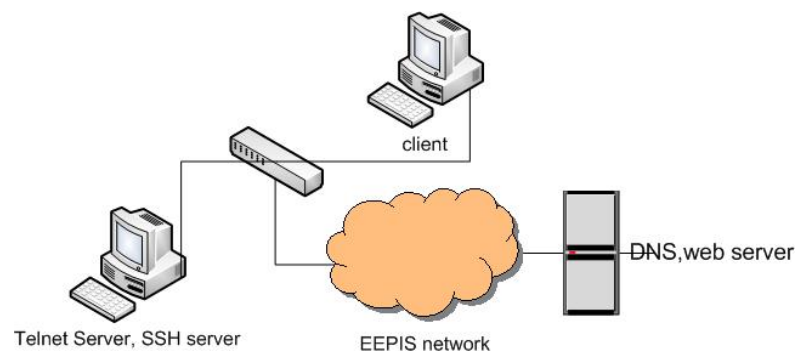
Field-Field	Deskripsi
19:20:0.804501	Timestamp dari paket. Menunjukkan jam 19, lebih 20 menit, 0.804501 detik
192.168.2.10.1221	source IP address dengan no port
192.168.2.165.23	Destinasi IP address dengan no port
S	flag
2565655403	data sequence numbers
win 16384	window size

C. TUGAS PENDAHULUAN

1. Apa tujuan sniffing ?
2. Apa beda passive sniffing dan aktif sniffing ?
3. Terangkan apa yang disebut enkapsulasi dan dekapsulasi paket dan sebutkan nama paket pada tiap layer OSI
4. Gambarkan format datagram TCP dan UDP. Sebutkan fungsi masing-masing fieldnya
5. Bagaimana perintah agar tcpdump melakukan filter paket http pada computer dengan IP 192.168.34.23/24
6. Salah satu perbedaan protocol ssh dan telnet adalah dalam hal keamanan dari proses sniffing. Jelaskan pernyataan ini.
7. Bagaimana mengatur agar Wireshark hanya mengambil paket http dari user 10.252.130.45/24 ?

D. PERCOBAAN

Percobaan ini dibagi dalam tiga bagian yaitu mengamati paket UDP, TCP dan melakukan sniffing koneksi telnet dan ssh. Karena itu perhatikan baik-baik agar waktu mencukupi untuk semua percobaan. Simpan hasil percobaan anda dan lakukan analisa dengan menjawab pertanyaan pada tiap percobaan. Sebagai langkah awal, buatlah konfigurasi jaringan sebagai berikut.



Gambar 13.11 Konfigurasi jaringan

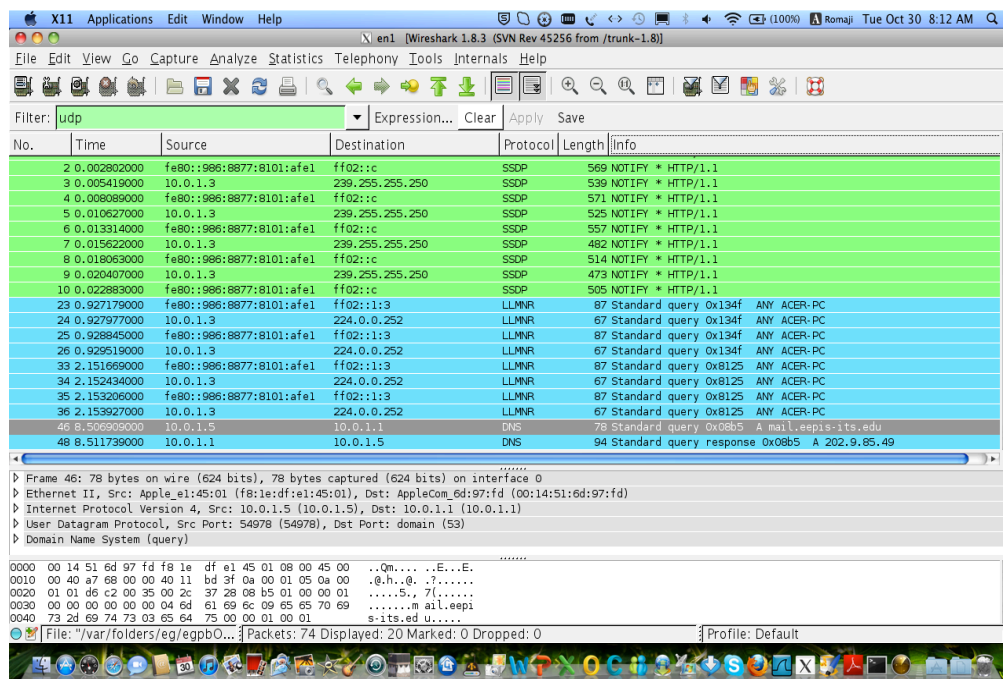
Pertemuan 12: Implementasi Lapisan Aplikasi

1. Mengamati paket User Datagram Protocol (UDP)

Pada percobaan pertama ini kita akan mencoba melihat format paket UDP pada protokol DNS dengan menggunakan wireshark. Kerjakan langkah-langkah praktikum dibawah dan jawablah pertanyaan-pertanyaanya.

1. Siapkan server DNS agar siap menerima query dari client atau gunakan DNS dari PENS. Catat no IP computer anda, default gateway dan server DNS.
2. Nyalakan Wireshark dan mulailah mengcapture packet
3. Lakukan nslookup pada computer anda untuk melakukan query ke name server secara interaktif. Contoh :

```
C:/> nslookup mail.eepis-its.edu
```
4. Tunggu sekitar 30 detik.
5. Lakukan filtering dengan memasukkan : udp pada kolom Filter:
6. Pilih paket udp. Lihat ke kolom ke 5 yaitu Protocol. Cari DNS. Klik.



Gambar 13.12 Filtering paket UDP dengan protocol DNS

6. Jika mungkin, ketika menjawab pertanyaan dibawah, print hasil capture untuk menunjukkan alasan anda menjawab pertanyaan tersebut. Pilih *File -> Print*, pilih *Selected packet only*. Lanjutkan dengan memilih *Packet Summary line*. Setelah itu pilih sejumlah

informasi yang ingin anda print.

7. Jawab pertanyaan dibawah .

Pertanyaan :

1. Pada jendela listing packet, pilih satu paket pada protocol DNS. Lihat pada details paket (lihat gambar 13.3) Dari paket ini lihatlah berapa jumlah field di udp header. Sebutkan field-field ini
2. Dari field isi packet (packet content field, lihat gambar 13.3) . Berapa panjang (dalam bytes) field UDP.
3. Nilai yang ada pada length field (pada detail packet window) ini adalah nilai apa? (Petunjuk, bandingkan dengan field content)
4. Berapa byte maksimum yang dapat dimasukkan dalam payload UDP?
5. Berapa no port source? Berapa jumlah port maksimum pada source ?
6. Berapa nomor protocol untuk UDP? Beri jawaban anda dalam notasi heksadesimal dan decimal (untuk ini lihat ke header IP)
7. Apa yang disebut field checksum. Apa fungsinya? Jelas bagaima nilai UDP checksum ini diperoleh (lihat google bila perlu)
8. Lihat paket kedua yang dikirim dari DNS server, yaitu DNS reply. Cobalah tarik hubungan antara DNS request dan reply.

2. Mengamati paket Transport Control Protocol (TCP)

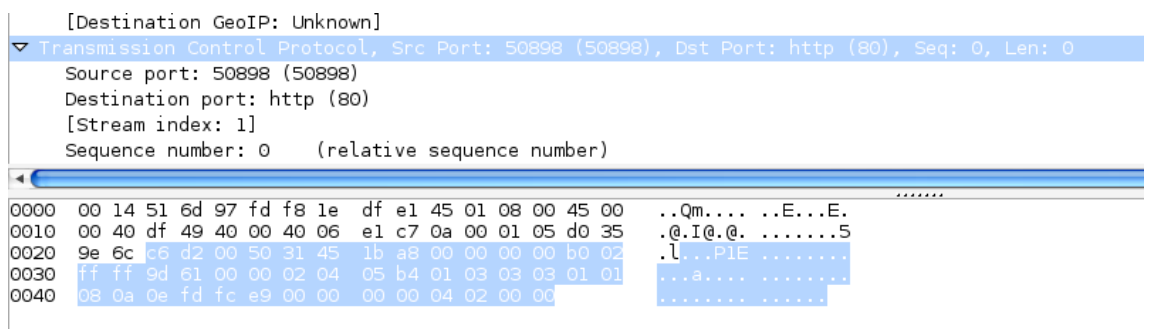
Pada percobaan kedua ini, kita akan mencoba mengamati paket TCP pada protocol HTTP. Untuk itu anda perlu terkoneksi ke jaringan luar atau menyiapkan web server sederhana pada subnet anda. Kerjakan langkah-langkah berikut dan jawab pertanyaan dibawah dengan seksama.

1. Buka Wireshark dan mulailah mengcapture packet
2. Catat IP computer anda. Bukalah browser. Sebelumnya pastikan bahwa cache browser kosong
3. Jika halaman web sudah terbuka, tunggu 30 detik, kemudian tutup halaman web tersebut.
4. Hentikan capture dengan menekan Stop.

5. Filterlah hanya menunjukkan tcp paket pada kolom filter . Isi dengan tcp.
Klik lah paket tcp di listing packet window (lihat gambar 13.3)
6. Klik pada detail packet window dan packet content window(cek gambar 13.3).
Jawablah pertanyaan dibawah .

Pertanyaan :

1. Lihatlah paket yang berasal dari computer anda menuju web server dari halaman web yang dituju.
2. Coba buka detail packet window. Berapa source port dan destination port ? Berapa no ip source dan destinasi?
3. Klik pada TCP. Lihat pada packet content window. Ini adalah header packet TCP. Capture bagian ini sebagai laporan. Berapa header lengthnya (dalam bytes) dan dalam heksa decimal pada packet content window?



Gambar 13.13 Header paket TCP dalam heksa decimal (kolom tengah) dan dalam ascii(kolom kanan) di jendela packet-content-wireshark

4. Berapa nilai field sequence number? Apa nilai flagnya ?
5. Apa fungsi MSS field, Win. Len dan timestamp ?
6. Perhatikan 2 paket berikutnya (antara source dan destinasi yang sama) setelah paket tersebut Jawab pertanyaan no 2 dan 4., Perhatikan bahwa ini adalah proses 3 way handshake untuk paket TCP. Gambarkan proses ini.
7. Bandingkan field-field TCP dan nilainya pada 3 paket tersebut. Apakah sama field-fieldnya dan isinya,jika ada bedanya, dimana ?

3. Sniffing koneksi telnet dan ssh

Siapkan sebuah telnet server dan ssh server pada subnet anda. Pada konfigurasi ini, telnet dan ssh server, ip addressnya 10.0.1.3/24Siapkan username dan password untuk keduanya. Baca baik-baik langkah percobaan dan pertanyaan sebelum menjalankan praktikum.Jalankan langkah-langkah seperti dibawah :

1. Coba ping server telnet untuk mengecek konektivitas.
2. Cek interface apa saja yang bisa dipakai oleh tcpdump
`#tcpdump-D`
3. Jalankan tcpdump pada salah satu interface misalnya en0 dan mulailah menangkap paket yang meuju dan meninggalkan telnet server, yaitu port 23. Server telnet memiliki no IP 10.0.1.3. Hasil tracing disimpan dengan nama filedump.
`#tcpdump-i en0-X -s 0 -w filedump host 10.0.1.3 and port 23`
4. Buka terminal baru. Untuk melihat MAC address, tambahkan opsi e:
`#tcpdump-i en0-e -wfiledump2 host 10.0.1.3 and port 23`
5. Mulailah melakukan telnet dari client.
`#telnet10.0.1.3`
Masukkan username dan passwordnya
6. Tcpdump akan merekam paket-paket yang dikirim, termasuk username dan password telnet. Peristiwa ini disebut sniffing packet
7. Stop menangkap paket dengan Ctrl Z atau Ctrl C
8. Gunakan perintah dibawah untuk membaca filedump dan mengubahnya menjadi txt file.
`#sudo tcpdump -r filedump -s 0 -X >filedump.txt`
`#sudo tcpdump -r filedump2 -s 0 -eX >filedump2.txt`
9. Amati paket-paket yang anda tangkap tadi dan jawablah pertanyaan dibawah dibawah dengan menggunakan tcpdump
10. Ulangilah langkah diatas untuk SSH server. Cobalah melakukan sniffing username dan password pada protokol SSH

Pertanyaan

Gunakan tcpdump untuk menjawab pertanyaan ini !Jika perlu tunjukkan hasil printout dari tcpdump untuk mendasari jawabanmu.

1. Sebutkan no IP telnet server-client ; serta no IP ssh server-client
2. Berapa MAC address dari telnet dan ssh; server dan client
3. Berapa nomor port telnet dan ssh ; server dan client
4. Telnet paket menggunakan datagram TCP atau UDP ?
5. Apa arti opsi-opsi yang diberikan tcpdump yaitu :s,X,D,w,r, e
6. Dapatkah anda melihat user name dan password yang diberikan user ketika koneksi lewat telnet dan ssh ke server? Jika iya, tunjukkan user name dan password dengan menunjukkan printout line dari tcp dump.Petunjuk. Coba cari kata login dan password ini dikolom ascii hasil tracing tcpdump. User yang digunakan adalah 'srini' dan password: 'student' .

```
02:11:27.709795 IP fitri-VirtualBox.telnet > 10.0.1.4.49423: Flags [P.], seq 66
0x0000: 4510 0040 a34f 4000 4006 8152 0a00 0103 E..@.0@..R....
0x0010: 0a00 0104 0017 c10f 1e6b e3ac 936c 0f9e .....k...l..
0x0020: 5018 00b7 1639 0000 6669 7472 692d 5669 P...9..fitri-Vi
0x0030: 7274 7561 6c42 6f78 206c 6f67 696e 3a20 rtualBox.login:..
```

Gambar 13.14 Server mempersilahkan client untuk login

Untuk username, perhatikan huruf s pada kolom ascii sebelah kanan Ini adalah awal dari huruf username (srini).

```
02:11:29.913981 IP 10.0.1.4.49423 > fitri-VirtualBox.telnet: Flags [P.], seq
0x0000: 4500 0029 0337 4000 8006 e191 0a00 0104 E..).7@.....
0x0010: 0a00 0103 c10f 0017 936c 0f9e 1e6b e3c4 .....l...k..
0x0020: 5018 0044 c01f 0000 7300 0000 0000 P..D....s....
```

Gambar 13.15 Client mulai mengirim username ke server

Server menjawab dengan paket berikut. Perhatikan bahwa huruf s dikirim kembali ke client

```
02:11:29.920213 IP fitri-VirtualBox.telnet > 10.0.1.4.49423: Flags [P.], seq
0x0000: 4510 0029 a350 4000 4006 8168 0a00 0103 E..).P@.@..h....
0x0010: 0a00 0104 0017 c10f 1e6b e3c4 936c 0f9f .....k...l..
0x0020: 5018 00b7 1622 0000 73 P....".s
```

Gambar 13.16 Respon dari server terhadap jawaban user name dari client

Pertemuan 12: Implementasi Lapisan Aplikasi

```
02:11:32.580437 IP fitri-VirtualBox.telnet > 10.0.1.4.49423: Flags [P.], seq 97:107, ack 84, win 183, length 10
  0x0000: 4510 0032 a35a 4000 4006 8155 0a00 0103  E..2.Z@..U....
  0x0010: 0a00 0104 0017 c10f 1e6b e3cb 936c 0fa5  ....k...l..
  0x0020: 5018 00b7 162b 0000 5061 7373 776f 7264  P....+..Password
  0x0030: 3a20                                     :.
```

Gambar 13.17 Server meminta telnet password

Untuk password, perhatikan huruf s pada kolom ascii sebelah paling kanan. Ini adalah awal dari Huruf password berikutnya dikirim satu persatu untuk tiap paket.

```
02:11:34.222322 IP 10.0.1.4.49423 > fitri-VirtualBox.telnet: Flags [P.], seq 84:85,
  0x0000: 4500 0029 0343 4000 8006 e185 0a00 0104  E..).C@.....
  0x0010: 0a00 0103 c10f 0017 936c 0fa5 1e6b e3d5  ....l...k..
  0x0020: 5018 0044 c007 0000 7300 0000 0000      P..D....s....
```

Gambar 13.18 Client memberikan password ke server

E. LAPORAN RESMI

Kumpulkan hasil percobaan di atas berserta capture konfigurasinya