2.4.3 Pengenalan Aplikasi

2.4.3.1 Wireshark

Wireshark adalah aplikasi penganalisa paket jaringan (Network Packet Analyzer). Sebuah software penganalisa paket jaringan yang bekerja dengan cara menangkap paket jaringan dan mencoba untuk menampilkan data paket yang tertangkap dengan detail. Wireshark bersifat open source.
Contoh penggunaan wireshark:

- Administrator jaringan menggunakan untuk melakukan penangan masalah jaringan
- Network security engineer menggunakan untuk memeriksa keamanan jaringan
- Developer menggunakan untuk melakukan debug pada implementasi protokol
- Umum digunakan untuk mempelajari internal protokol jaringan

Wireshark memiliki fitur:

- Tersedia untuk UNIX dan Windows.
- Menangkap paket data langsung dari network interface.
- Tampilan paket dengan informasi protokol yang sangat rinci.
- Open dan Save data paket yang dicapture.
- Import dan Eksport paket data dari dank e banyak program capture lainnya.
- Menyaring paket data dengan berbagai macam kriteria.
- Warnai layar paket berdasarkan filter.

2.4.3.2 Cara pemakaian aplikasi Wireshark

Langkah-langkah menggunakan Wireshark:

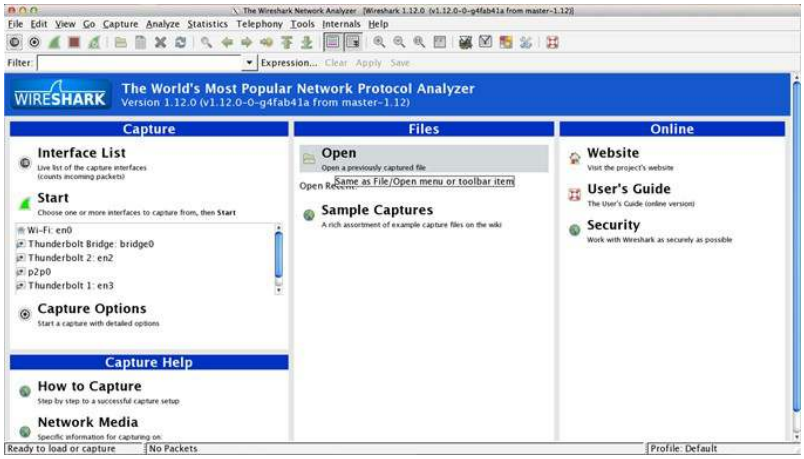
1. Klik ikon. . .

Gambar 2.23: Ikon Wireshark

2. Kemudian akan tampil aplikasi wireshark dengan diawali spash screen.

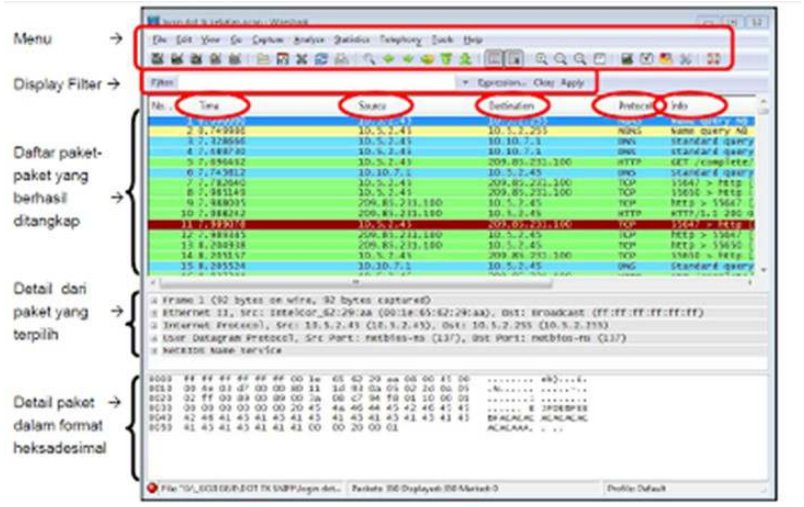
Gambar 2.24: Wireshark Splash

3. Tampilan awal program Wireshark.



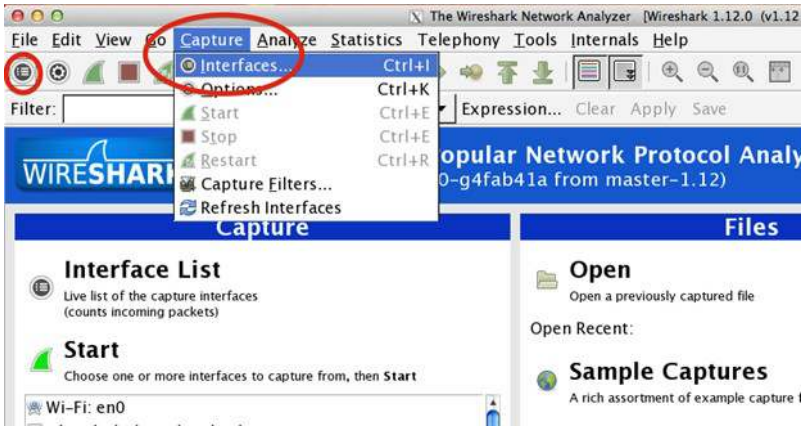
Gambar 2.25: Wireshark awal

4. Keterangan menu wireshark.



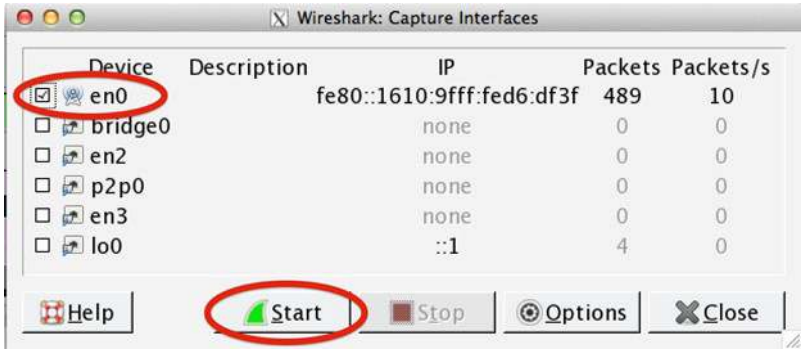
Gambar 2.26: Wireshark menu

5. Melakukan CAPTURE data menggunakan wireshark, pilih menu INTERFACE.



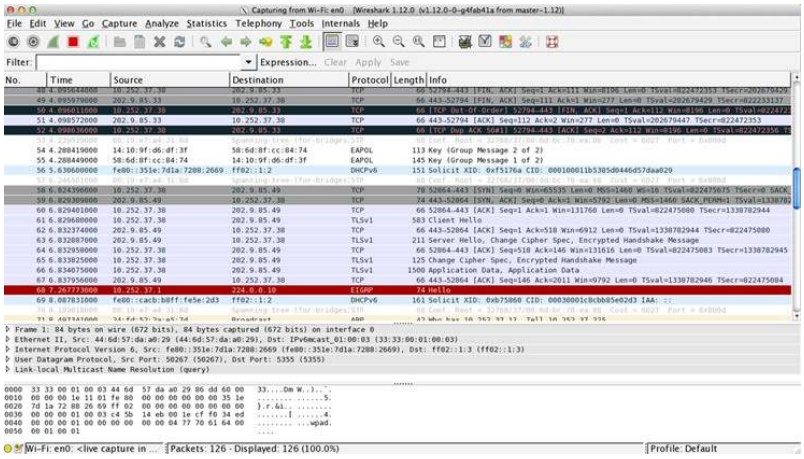
Gambar 2.27: Wireshark capture interface

6. Pilih interface yang kita gunakan, kemudian klik start.



Gambar 2.28: Wireshark pemilihan interface

7. Setelah mengaktifkan interfaces, Wireshark akan beraksi membaca semua data yang berada di jaringan. Terlihat banyak data yang dapat dicapture.

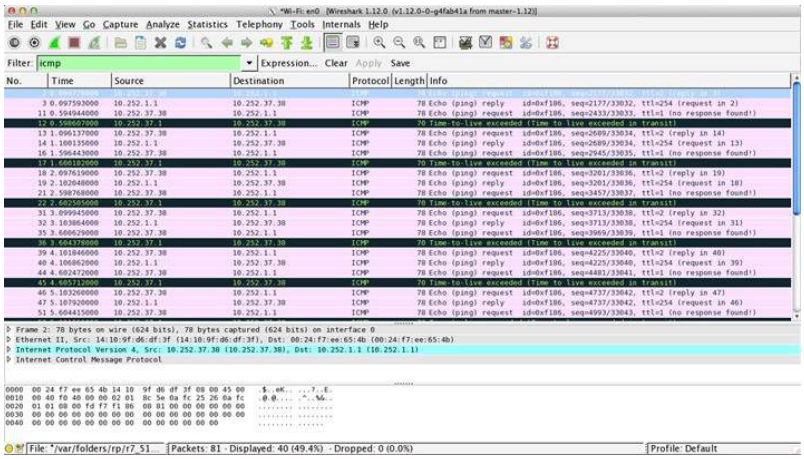


Gambar 2.29: Wireshark in action

Keterangan:

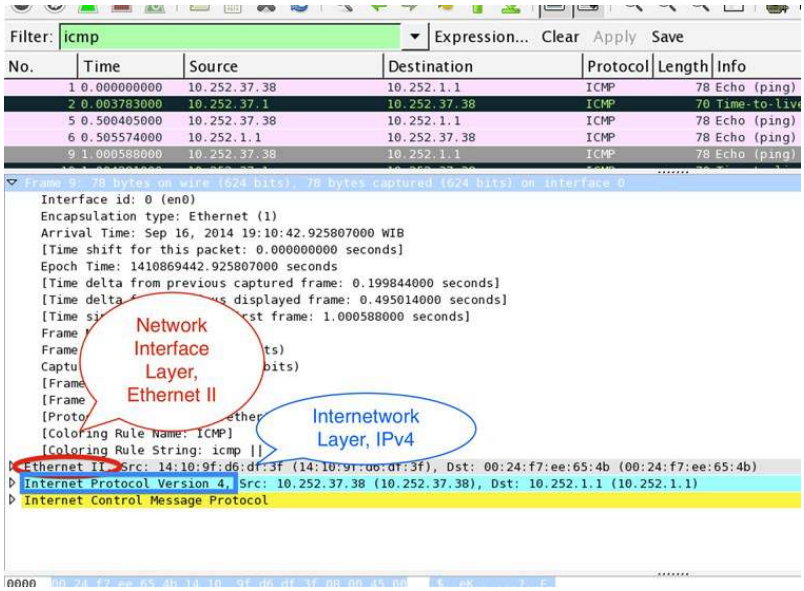
Source	Alamat IP pengirim
Destination	Alamat IP tujuan
Protocol	Jenis protokol yang digunakan, seperti TCP, DHCP, dll
Length	Panjang data yang dikirimkan
Info	Informasi isi data yang dikirimkan

8. Ketikkan ICMP pada filter box untuk melakukan penyaringan data yang akan ditampilkan sehingga hanya data PING yang akan ditampilkan.



Gambar 2.30: Wireshark melakukan filter

9. Penjelasan data.



Gambar 2.31: Wireshark hasil capture per layer

2.4.4 Persiapan Praktikum

Bahan-bahan yang dibutuhkan untuk melakukan praktikum, antara lain:

1. Modul praktikum
2. PC yang dilengkapi dengan aplikasi Wireshark
3. Jaringan aktif
4. Lembar Laporan Praktikum (Lampiran)
5. Koneksi LAN dan Internet

2.4.5 Langkah-langkah Praktikum

2.4.5.1 Menjalankan aplikasi wireshark

1. Mahasiswa melakukan pengecekan apakah pada PC yang dipakai sudah terinstall aplikasi wireshark ?!!
2. Apabila belum terinstall, mahasiswa harus melakukan installasi di PC yang digunakan !!!

```
Untuk OS Linux Debian/Ubuntu:
    dhoto@mypc $ su
    root@mypc # apt-get install wireshark

    Untuk OSX:
    - Download wireshark dan XQuartz
    - Lakukan konfigurasi XQuartz pada wireshark

    Untuk Windows:
    - Download wireshark
    - Klik 2x pada installer wireshark
```

3. Klik ikon Wireshark !!!
4. Klik pada menu CAPTURE dan memilih INTERFACES.
5. Pilih interface yang akan digunakan untuk mengrekam data.
6. Klik Start.
7. Pada OS linux, jalankan aplikasi TERMINAL dan ketik perintah PING yang digunakan untuk melakukan pengecekan jaringan (tanpa tanda $):

```
$ ping 8.8.8.8
```

8. Kembali ke aplikasi wireshark, hentikan rekam data dengan cara klik tombol merah pada wireshark. Ambil data untuk jenis tipe: icmp dengan cara memfilter di aplikasi wireshark dan lakukan screen shot pada tampilan wireshark yang kalian gunakan.

2.4.5.2 Melakukan rekam data untuk jenis protokol tertentu

1. Lakukan praktikum seperti kegiatan 2.5.1 dari nomer 4 s/d 8.
2. Ganti kegiatan pada no 7, dengan kegiatan berikut:
   - Jalankan aplikasi terminal dan ketik perintah NSLOOKUP yang digunakan untuk mengetahui IP dari suatu tujuan (tanpa tanda $):

     ```
     $ nslookup www.pens.ac.id
     ```

     Ambil data untuk jenis tipe: dns
   - Jalankan aplikasi web browser dan arahkan ke alamat: ftp://newfs.pens.ac.id, Download salah satu data yang ada di alamat tersebut !!!
     Ambil data untuk jenis tipe: ftp
   - Jalankan aplikasi web browser dan arahkan ke alamat: http://www.pens.ac.id
     Ambil data untuk jenis tipe: http
3. Untuk masing-masing kegiatan diatas, laporkan data yang telah direkam sesuai dengan layer pada TCP/IP model. Gunakan lembar Laporan praktikum 2. TCP/IP Model. (Lampiran 2.4.6)

2.4.6 Lampiran

Laporan praktikum TCP/IP Model
Kegiatan :
Nama :
NRP :

Data
Application Layer

Data:

Host-to-host Layer

Data:

Internetwork Layer

Data:

Network Interface Layer

Data: