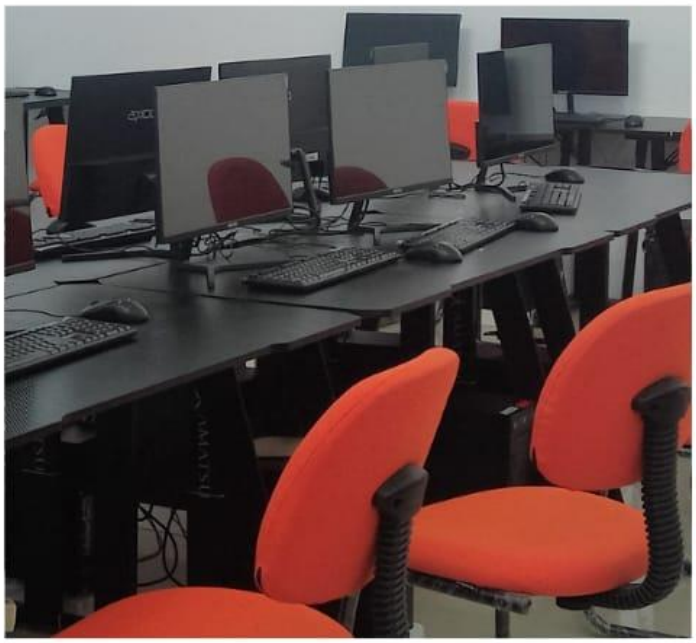
INSTITUT TEKNOLOGI
BACHARUDDIN JUSUF HABIBIE

MODUL PRAKTIKUM

JARINGAN KOMPUTER



LABORATORIUM
KOMPUTER
2023/2024

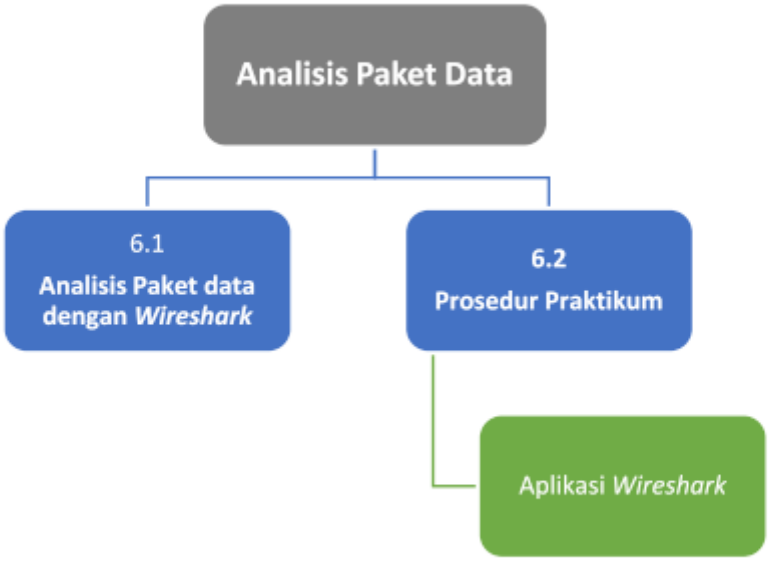
MODUL 6 ANALISIS PAKET DATA

TUJUAN

Setelah mempelajari materi pada pembelajaran modul ini, mahasiswa diharapkan dapat:

1. Memahami Analisis Paket Data pada Jaringan Komputer
2. Melakukan Konfigurasi pada Aplikasi Analisis Paket Data
3. Melakukan Analisis Jenis-Jenis Paket Data pada Aplikasi Wireshark

PETA MATERI



Modul berikut menjelaskan tentang Analisis Paket Data atau sering disebut dengan network forensic. Dalam jaringan komputer dan komunikasi data yang terhubung baik secara lokal ataupun secara luas, terdapat sebuah jalur lalu lintas transmisi dan data yang terkemas rapih dan baik oleh Network Protocol sehingga setiap transmisi dan data tersebut hanya berupa sinyal dalam bentuk kode binari. Sebuah paket data jaringan adalah satuan informasi dasar yang dapat ditransmisikan di atas jaringan atau melalui saluran komunikasi digital. Sebuah paket data berisi packet header yang berisi informasi mengenai protokol tersebut yang berhubungan dengan jenis, sumber, tujuan, atau informasi lainnya. Data yang hendak ditransmisikan disebut dengan data payload dan packet trailer yang bersifat opsional. Sebuah paket memiliki struktur logis yang dibentuk olch protokol yang digunakannya. Ukuran setiap paket juga dapat bervariasi, tergantung struktur yang dibentuk oleh arsitektur jaringan yang digunakan.

Pada saat berinteraksi dengan internet, komputer yang digunakan diistilahkan sebagai sebuah entitas yang dikenal juga sebagai Host. Banyak sekali proses komunikasi data antara komputer host dengan komputer lainnya yang berinteraksi pada jaringan tersebut. Ketika komputer host mengirim paket data melalui jaringan komputer, paket data tersebut akan disebar keseluruh jaringan hingga sampai ke alamat yang dituju. Berdasarkan hal tersebut, maka dibutuhkan suatu perangkat atau tool untuk memantau dan menganalisa lalu lintas paket data secara real time dan selengkap mungkin pada jaringan. Salah satu perangkat atau tool open source yang dapat digunakan untuk menganalisa kinerja jaringan internet adalah Wireshark.

6.1 Analisa Paket Data dengan Wireshark

Wireshark merupakan salah satu aplikasi open source untuk mengetahui lalu lintas komunikasi data dalam jaringan dengan cara memantau dan menganalisa melalui protokol dan port-port jaringan yang digunakan. Wireshark adalah salah satu dari sekian banyak tool Network Analyzer yang banyak digunakan oleh Network administrator untuk menganalisa kinerja jaringannya. Wireshark sudah menggunakan Graphical User Interface (GUI) dan mampu menangkap paket-paket data/informasi yang saling berinteraksi dalam jaringan. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa. Untuk menggunakan tool ini cukup memasukkan sebuah perintah untuk mendapatkan informasi yang ingin di-capture atau yang ingin diperoleh dari jaringan dan menganalisanya.

Sebuah paket data mengandung segmen data yang menyimpan informasi yang digunakan seperti protokol, IP Address, MAC Address tujuan dan lain sebagainya. Dengan menggunakan wireshark Network administrator dapat men-capture atau merekam segala aktivitas lalu lintas yang terjadi pada jaringan ketika saat memulai browsing ke sebuah alamat URL. di internet dan dapat mendeteksi setiap paket data yang dikirim dan diterima melalui perangkat keras jaringan yang terhubung ke jaringan komputer.

6.2. Prosedur Praktikum

Analisa paket data merupakan langkah penting yang perlu dilakukan oleh seorang network administrator guna untuk melakukan pemantauan atau monitoring terhadap paket data atau informasi yang berlangsung pada sebuah jaringan komputer. Berikut langkah-langkah praktikum yang perlu dilakukan.

6.2.1 Persiapkan Alat dan Bahan

- 2 buah Komputer dilengkapi dengan aplikasi Wireshark.
- Kabel UTP dengan tipe Crossover
- witch/Hub (Optional), jika diperlukan.

6.2.2 Instalasi Aplikasi Wireshark

1. Pertama-tama unduh terlebih dahulu aplikasi wireshark pada situs resminya pada link berikut www.wireshark.org/download.
2. Pilih aplikasi wireshark sesuai arsitektur sistem operasi yang digunakan, sebagai contoh pada windows menggunakan Windows Installer (32-bit) atau Windows Installer (64-bit).

Gambar 6.1 Halaman Unduh *Wireshark*

3. Setelah diunduh maka selanjutnya lalukan instalasi pada aplikasi tersebut. Dengan cara klik ganda pada file tersebut.

4. Pada jendela Wireshark 2.0.1 (64-bit) Setup yang muncul, lalu tekan tombol Next.

5. Lanjutkan dengan menekan tombol I Agree

6. Pada jendela berikutnya, pilih secara default lalu tekan tombol Next.

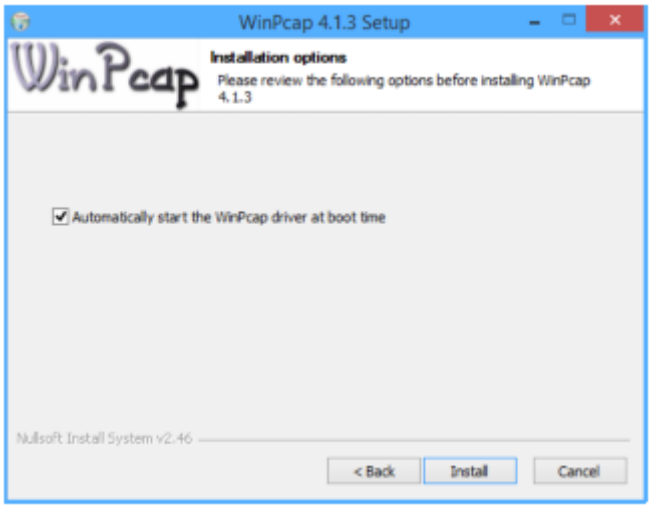
7. Selanjutnya secara dafault pada jendela Select Additional Task, tekan tombol Next.

8. Kemudian tentukan lokasi instalasi aplikasi, lalu tekan tombol Next. 9. Pada jendela Install WinPcup? pilihlah Install WinPrap 4.1.3, lalu tekan tombol Next.

10. Selanjutnya pada jendela Install USBPeap? pilihlah Install USBPcap 1.1.0, lalu tekan tombol Install. (pada langkah ini opsional).

11. Sesaat kemudian muncul jendela Win Peap 4.1.3 Setup, lalu tekan tombol Next.

12. Lanjutkan dengan menekan tombol I Agree 13. Pada jendela berikutnya secara default pilihlah Automatically start the WinPeap driver at boot time, lalu tekan tombol Install.



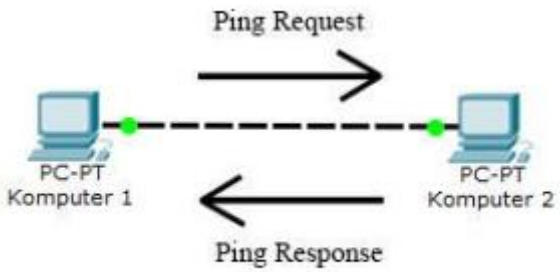
Gambar 6.2 Jendela Instalasi Aplikasi *WinPcap*

13. Selanjutnya tekan tombol Nexz, lala pada jendela berikutnya pilihlah Reboot Now dan tekan tombol Finish. Untuk melakukan restart pada sistem operasi.

6.2.3 Analisa Paket Data

1. Sebagai contoh menghubungkan 2 komputer secara peer to peer atau dalam jaringan client- server. Gambar 6.3 memiliki kriteria sebagai berikut:

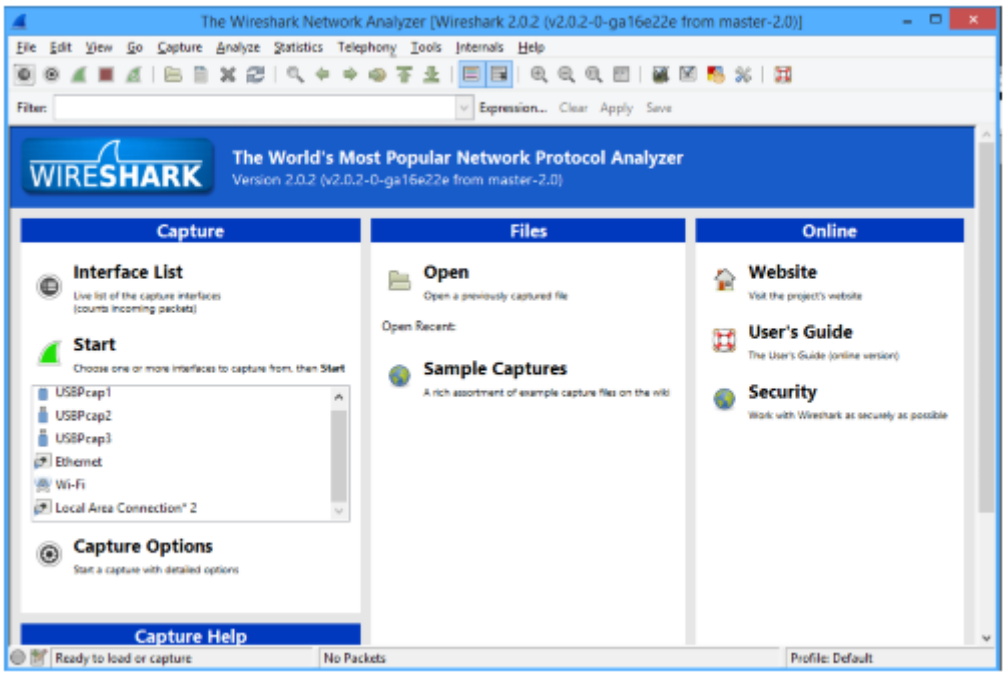
- Komputer ! :192.168.1.1/24
- Komputer 2 :192.168.1.2/24



Gambar 6.3 Permintaan Respon "ping" Ke Komputer 2

2.Selanjutnya setelah proses Reboot Now pada langkah sebelumnya, lakukan konfigurasi IP Address pada masing-masing laptop/komputer sesuai kriteria pada Gambar 6,3.

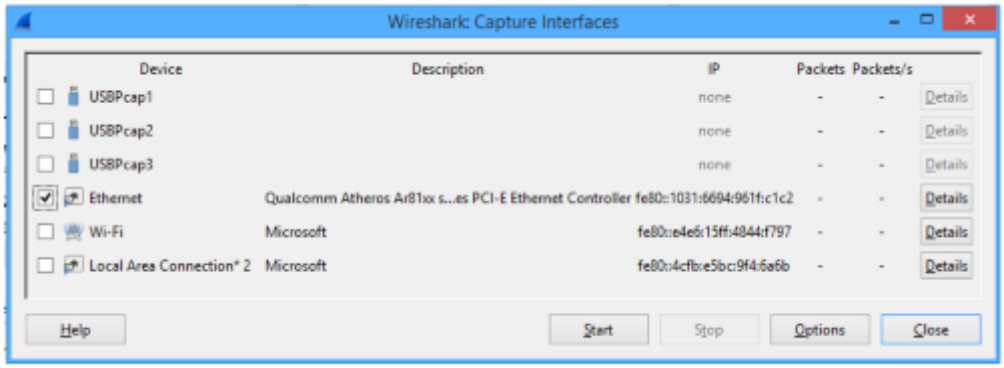
3. Kemudian jalankan aplikasi Wireshark yang sudah terinstall, maka muncul jendela seperti pada Gambar 6.4.



Gambar 6.4 Jendela *Interface Wireshark*

4. Pada jendela Wireshark pilihlah menu Interface List

5. Lanjutkan dengan memilih Interface yang ingin di-capture atau direkam, sebagai contoh pilih Ethernet lalu tekan tombol Start untuk memulai capture paket data.



Gambar 6.5 Jendela *Capture Interfaces*

Keterangan pada Gambar 6.5 sebagai berikut:

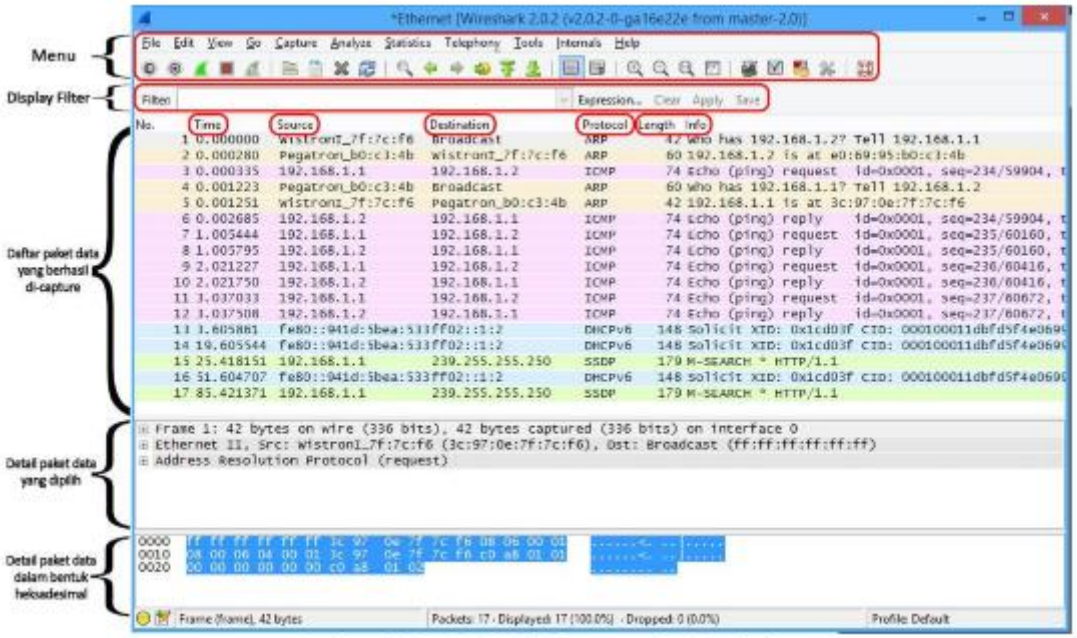
Ethernet merupakan kata lain dari interface LAN Card, sedangkan Wi-Fi kata lain dari Wireless Adapter.

6. Selanjutnya biarkan jendela Wireshark tetap berjalan untuk melakukan capturing atau perekaman data.

7. Kemudian untuk mendapatkan informasi dari paket data, lakukan perintah "ping" pada komputer 1 ke tujuan atau komputer 2 dengan cara menggunakan aplikasi Command Prompt

Perintah "ping" merupakan salah satu contoh yang mudah untuk komunikasi data antar komputer pada jaringan

7. Pada aplikasi Run yang muncul, ketikan perintah "cmd" lalu tekan tombol OK.
8. Selanjutnya ketikan perintah "ping" diikuti dengan IP Address komputer yang dituju di dalam jaringan, misalnya masukkan IP Address komputer 2 yakni 192.168.1.2. Lalu tekanlah tombol Enter.
9. Jika pada jendela "cmd" atau Command Prompt muncul tampilan Reply from IP address atau Request Time Out, maka paket data sudah terkirim, jadi informasi tersebut sudah dapat di analisa.
10. Kemudian kembali pada jendela Wireshark tekan tombol Stop pada Tab Capture, maka muncul informasi-informasi dari paket data hasil dari perintah "ping" yang dilakukan sebelumnya dari komputer I ke tujuan atau komputer 2.



Gambar 6.6 Jendela Hasil *Capture* pada *Wireshark*

Keterangan pada Gambar 6.6 sebagai berikut:

Menu : Sekumpulan menu-menu yang tersedia di Wireshark yang memiliki fungsi tersendiri.

Display Filter : Kolom yang diisi dengan perintah-perintah untuk mem-filter paket-paket apa saja yang ditampilkan pada daftar paket data. Tampilan paket-paket data yang berhasil di-capture oleh Wireshark.

Daftar Paket Data: berurutan mulai dari paket pertama yang ditangkap, dan seterusnya. Sebuah paket tentunya membawa informasi tertentu yang bisa berbeda-beda antur paket yang lain, di kolom ini akan ditampilkan detail paket yang terpilih pada daftar paket data di atasnya. Biasanya

Detail Paket Data : terdiri dari 3 sampai 5 informasi. : Detail paket yang terpilih akan ditampilkan dalam bentuk beksu, terkadang akan lebih mudah mendapatkan informasi dari bagian ini.

Pada bagian Daftar Paket Data, terdapat kolom-kolom seperti berikut ini:

No : Menampilkan jumlah paket data.

Time : Menampilkan waktu saat paket tersebut tertangkap.

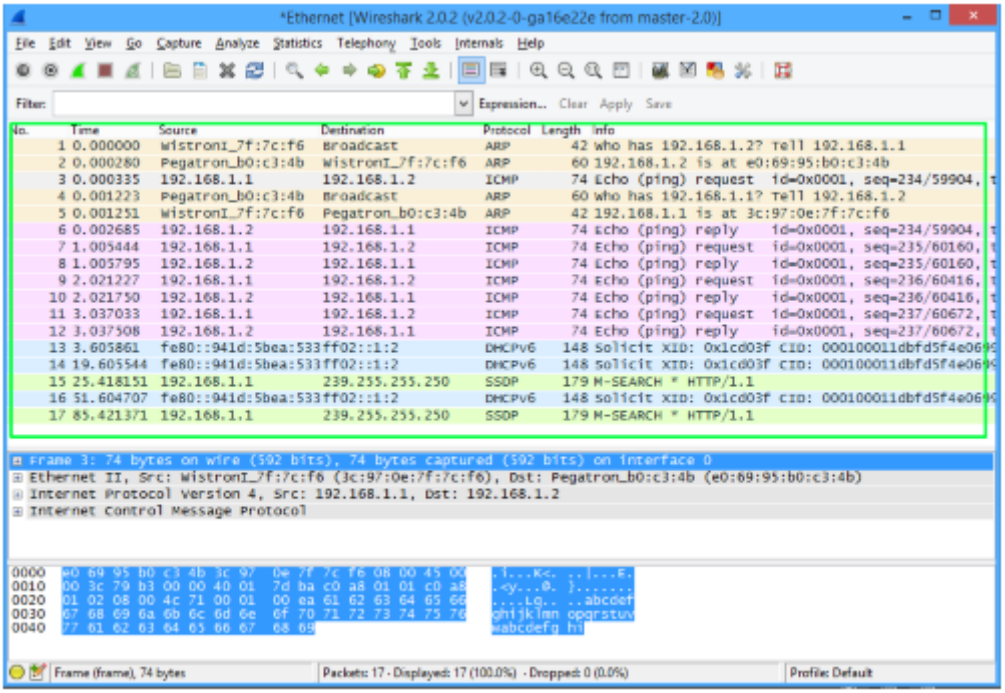
Source : Menampilkan alamas IP sumber dari paket data tersebut.

Destination : Menampilkan alamat IP majuan dari paket data tersebut.

Protocol :Menampilkan protokol apa yang dipakai sebuah paket data.

Info : Menampilkan informasi mendetil tentang paket data tersebut.

12. Selanjutnya didapatkan hasil capture yang dilakukan dengan perintah "ping" terlihat pada Gambar 6.7 didapatkan informasi dari paket data sebagai berikut:



Gambar 6.7 Hasil *Capture* Komputer 1 Ke Komputer 2

Jumlah Frame : Terdiri dari 17 Frume

Time/Waktu : Masing-masing frame memiliki rentang waktu yang berbeda-beda saat transmisi data

Source/ Sumber : Merupakan komputer sumber atau komputer yang melakukan perintah "ping" terhadap komputer yang dituju atau komputer 2. Sebagai contoh:

Frame 1 Melakukan broadcast atau menyebarkan informasi MAC Address komputer | "Wistron" melalui protocol ARP terhadap jaringan, lalu di jawablah pada frame 2 bahwa MAC Address di terima oleh Komputer 2 "Pegatron", kemudian dibalas informasi tersebut ke komputer 1 pada kolom Destinasion.

Pada frame 3 komputer 1 melakukan permintaan request dengan perintah "ping" dengan IP 192.168.1.1 ke IP 192.168.1.2 melalui protocol ICMP, maka frame 4 dan frame 5 melakukan hal yang sama seperti komputer I pada frame 1 dan frame 2

Pada frame 6 komputer 2 melakukan balasan dengan dengan jawaban reply melalui protocol ICMP. Selanjutnya pada frame 7. komputer 1 melakukan permintaan / request kembali, kemudian di balas oleh komputer 2 pada frume 8. dst.

Tujuan : Merupakan destinasi yang tuju oleh komputer sumber yang berisi tentang IP Address versi 4, IP Address versi 6 dan MAC Address.

Protokol : Merupakan jalur transmisi data atau porr-port yang dilalui oleh sebuah paket data dalam jaringan.ICMP (Internet Control Message Protocol) merupakan protokol yang bertugas mengirimkan pesan-pesan kesalahan dan kondisi lain yang memerlukan perhatian khusus, sepeni Echo dan Echo Reply. ARP Address Resolution Protocol) merupakan protokol untuk mendapatkan informasi MAC address berdasarkan informasi P Address. Ketika suatu how mengirim paket menggunakan IP Address host tujuan, switch akan memeriksa daftar pada tabel ARP untuk mencocokan IP Address dengan MAC address tujuan. Tabel ARP berisi informasi pemetaan antara IP Address dengan MAC address.

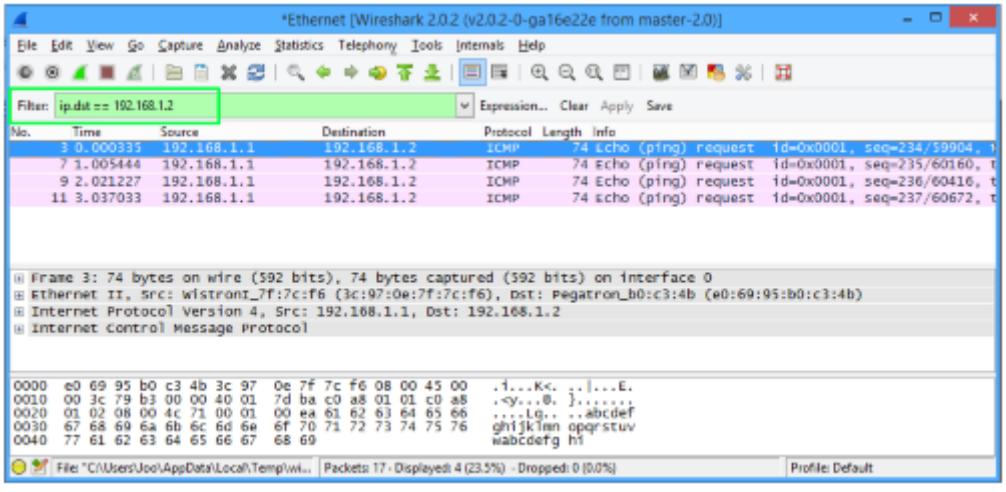
Info : Merupakan keterangan detil saat paket data melakukan transmisi data.

13. Analisis dan catat hasil percobaan analisa paket data pada komputer I dan komputer 2.

6.2.4 Analisa Paket Data dengan Perintah Wireshark

Aplikasi Network Analyzer salah satunya adalah Wireshark. Di dalam Wireshark terdapat perintah-perintah yang dapat digunakan untuk mempermudah seorang network administrator untuk menyaring / mem-filter informasi dari masing-masing paket data yang di transmisikan dalam sebuah jaringan komputer. Berikut perintah yang digunakan dalam Wireshark:

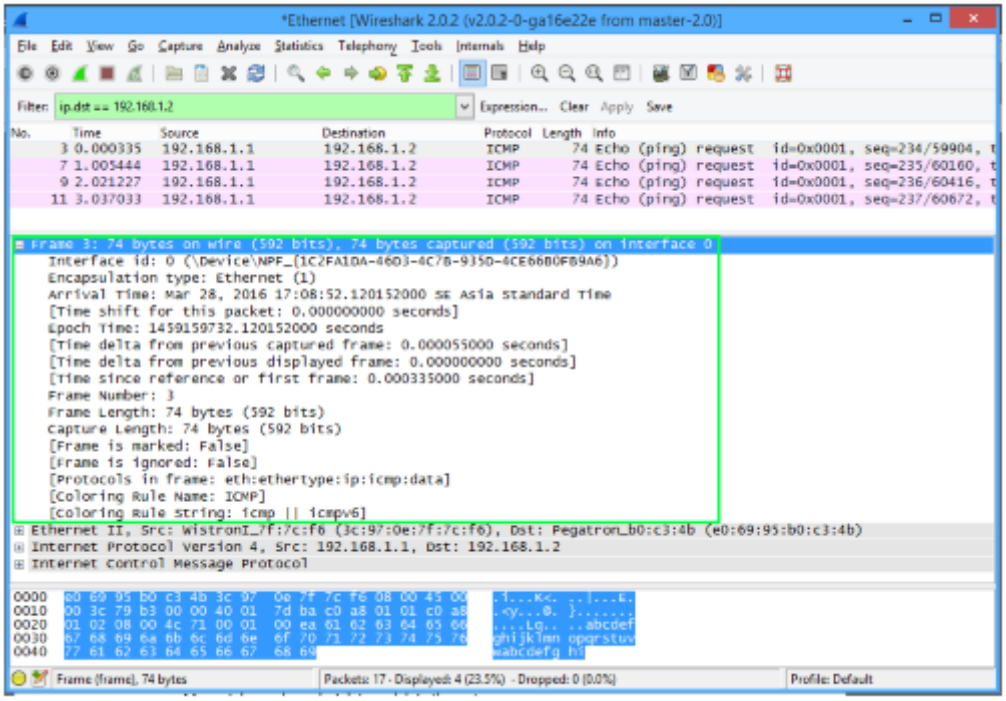
1.Pada Gambar 6.8 merupakan hasil capture yang dapat tersaring/ter-filter dengan perintah **"ip.dst-IP Address Tujuan".** Lalu ketikan perintah **"ip.dst-192.168.1.2"** pada kolom Display Filter yang bertujuan untuk memeriksa informasi yang dikirimkan dari komputer I ke komputer tujuan atau komputer 2.



Gambar 6.8 Hasil Perintah "ip.dst == 192.168.1.2"

2. Maka didapatkan 4 frume yang memiliki informasi pada kolom Info dengan keterangan bahwa IP Address 192.168.1.1 melakukan perintah "ping" atau permintaan/request.

3. Kemudian melakukan analisa pada paket data, sebagai contoh pada no.3 atau frame ke 3 didapatkan informasi data pada gambar 6.9, sebagai berikut:



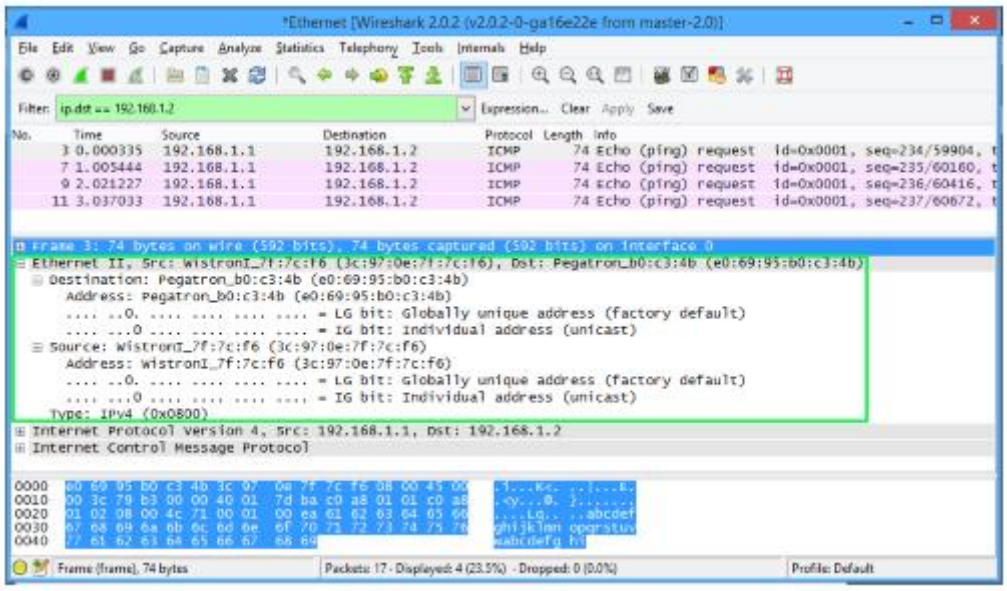
Gambar 6.9 *Detail* Paket Data *Frame*

Pada detail paket data frame terdapat informasi sebagai berikut:

- Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
- Arrival Time: Mar 28, 2016 17:08-52.120152000 SE Asia Standard Time
  Menunjukkan pada frame ke 3 mempunyai data berukuran 74 Bytes melalui media kabel atau ethernet.
- Encapsulation type: Ethernet (1) Menunjukan enkapsulasi data melalui ethernet.
- Protocols in frame: eth.ethertype:ipticmp:data
  Menunjukkan transmisi data pada interface ethernet menggunakan protokol ICMP

Kesimpulan frame 3 adalah transmisi data dilakukan pada ethernet, pada waktu 17:05 menggunakan protokol ICMP.

4. Selanjutnya melakukan analisa pada frame ke 3 bagian Ethernet 11. didapatkan informasi data pada gambar 6.10. sebagai berikut:



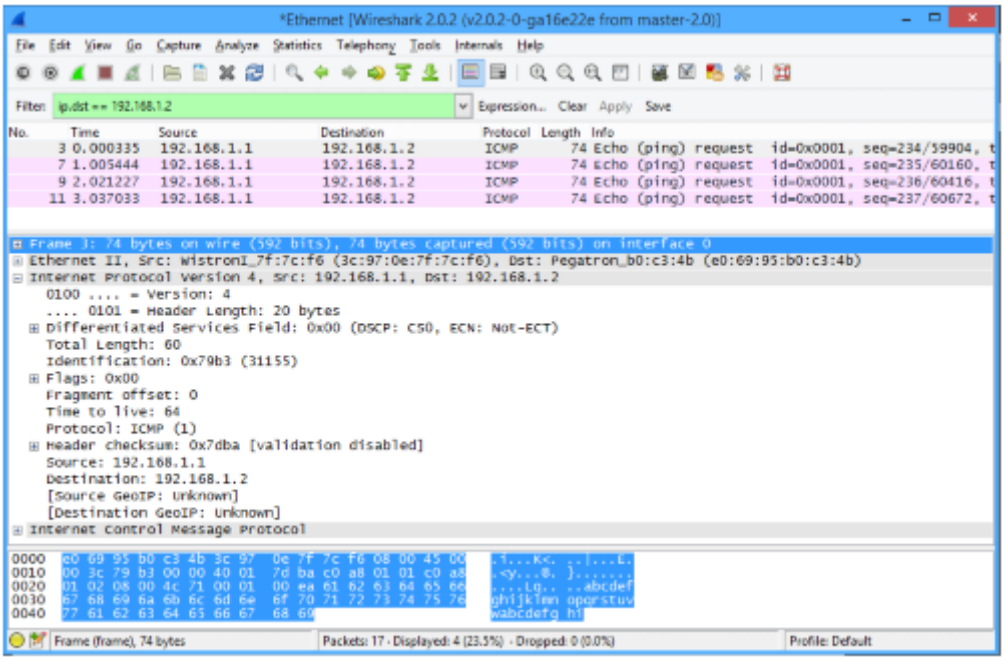
Gambar 6.10 *Detail* Paket Data *Ethernet* II

Pada detail paket data Ethernet II terdapat informasi sebagai berikut:

- Ethernet 11. Sre: Wistronl 71:7e:f6 (3e:97:0c:7f7e:fb), Dst: Pegatron b0:03:46 (e0:69:95:b0:e3:46)
- Destination: Pegatron_b0c3:4b (et:69:95;b0:c3:4b)
- Address: Pegatron b0c3:4b (c0:69-95:60x3:46)
- Source: Wistronl 71:7c:f6 (3c:970e7f7c:f6)
- Address: Wistront 78.7c:f6 (3e:97:0e:717:16)
  Menunjukkan sumber "Sre" interface pada ethernet memiliki MAC Address/ alamat fisik "3e:97:06:76-7c:16" atau komputer 1. Sedangkan tujuan "Dst" memiliki MAC Address alamat fisik "e0:69:95:b0:c3:4b" atau komputer 2.
- Type: IPv4 (0x0800)
  Menunjukkan protokol yang dilalui menggunakan IP Address versi 4.

Kesimpulan Ethernet II adalah transmisi data yang dilakukan dikirim dari MAC Address c0.69.95:60:23:4b atau komputer 1 ke MAC Address 30:97-0e:71;70:6 atau komputer 2 melalui IP Address versi 4.

5. Kemudian melakukan analisa pada rame ke 3 bagian Internet Protocol Version 4. didapatkan informasi data pada gambar 6.11. sebagai berikut:



Gambar 6.11 *Detail* Paket Data *Internet Protocol Version* 4

Pada detail paket data Internet Protocol Version 4 terdapat informasi sebagai berikut:

- Internet Protocol Version 4, Stu: 192.168.1.1. Dst: 192.168.1.2
- Time to live: 64
- Protocol: ICMP (1)

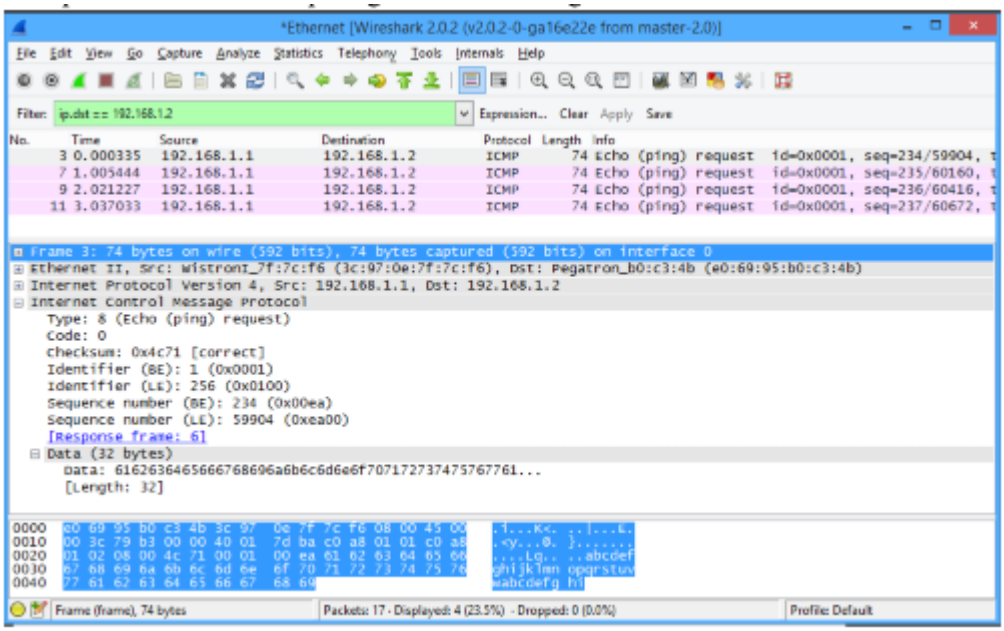
Menunjukkan IP protokol versi 4 dengan sumber "Src" 192.168.1.1 atau komputer 1. Sedangkan tujuan "Dst" 192.168.1.2 atau komputer 2. Dengan Time to live atau waktu koneksi 64ms, melalui protokol ICMP pada port 1.

- Header checksum: 0x7dba [validation disabled]
- Source: 192.168.1.1
- Destination: 192.168.1.2

Menunjukkan sumber alamat IP kompoter 1 ke tujuan yakni komputer 2,

Kesimpulan Internet Protocol Version 4 adalah transmisi data yang dilakukan dikirim dari 192.168.1.1 atau komputer 1 ke 192.168.1.2 atau komputer 2 dengan waktu 64ms melalui protokol ICMP pada port 1.

3. Selanjutnya melakukan analisa pada frame ke 3 bagian Internet Control Message Protocol, didapatkan informasi datu pada gambar 6.12. sebagai berikut:



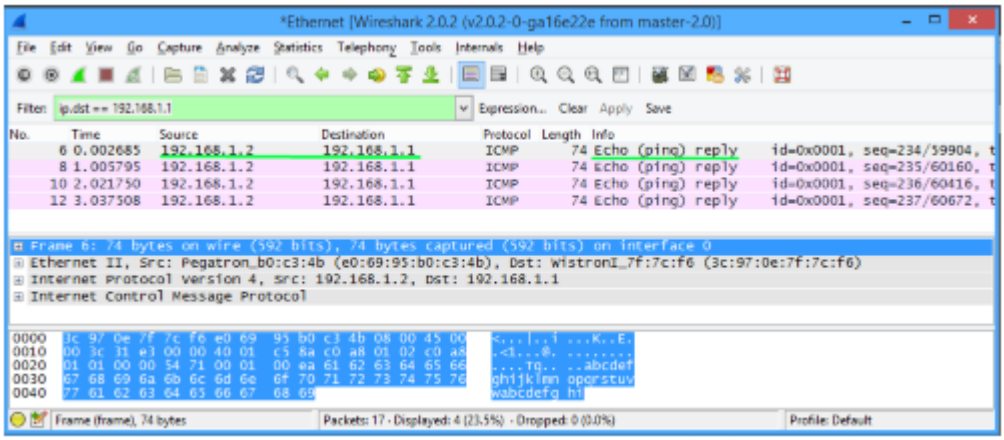
Gambar 6.12 ***Internet Control Message Control***

Pada detail paket Internet Control Message Protocol terdapat informasi sebagai berikut:

- Type: 8 (Echo (ping) request)
- Response frame: 6
  Menunjukkan pada ethernet melakukan perintah (echo) "ping" yang artinya request atau permintaan informasi. Dan di response atau dibalas pada permintaan tersebut pada frame ke 6 di daftar paket data,
- Data (32 bytes) Data: 6162636465666768696a6b6c6d6c60707172737475767761
  Menunjukkan ukuran data yang dikirim saat melakukan perintah "ping".

Kesimpulan Internet Control Message Control adalah transmisi data yang dilakukan ethernet menggunakan perintah "ping" dengan ukuran data sepanjang 32Bytes dan di response atau di balas pada frame ke 6 pada daftar paket data tersebut.

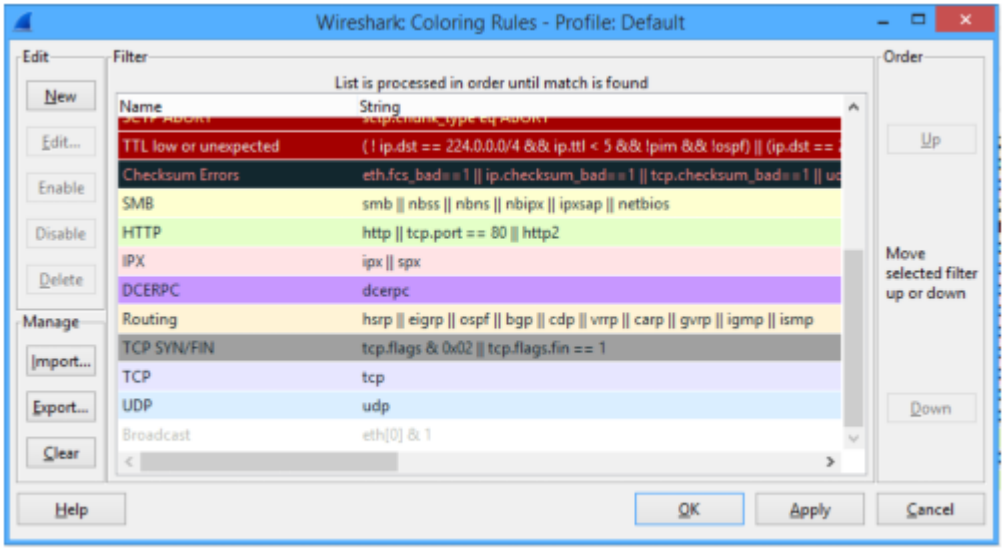
7. Pada Gambar 6.13 merupakan hasil capire yang dapat tersaring/ter-filter dengan perintah "ip.dst-IP Address Tujuan". Lalu ketikan perintah "ip.dst-192.168.1.1" pada kolom Display Filter yang bertujuan untuk memeriksa informasi yang dibalas oleh komputer 2 ke komputer peminta atau komputer 1.



Gambar 6.13 Hasil Perintah "ip.dst == 192.168.1.1"

8. Maka didapatkan 4 frame yang memiliki informasi pada kolom Info dengan keterangan bahwa IP Address 192.168.1.2 membalas perintah "ping" atau dengan status reply.

9. Selanjutnya untuk mengetahui fungsi dari masing-masing warna pada daftar paket data dengan memilim tab View, lalu tekan tombol Coloring Rules...



Gambar 6.14 Jendela Fungsi Warna Pada Daftar Paket Data

10. Analisis dan catat hasil percobaan analisis paket data pada Wireshark

Soal Latihan!

1. Lakukan analisis paket data (Application / Datagram , Transport / Segment , Internet / Packet , Network Access / Frame) pada profil siakad masing-masing pada *link* siakad.um.ac.id. Screenshot hasil *capture wireshark* dan analisa seperti prosedur praktikum sebelumnya.
   Catatan lakukan *capture* paket data sebelum *login* pada halaman siakad.um.ac.id

Jawaban:

1. .....
   .....
   .....
   .....

RANGKUMAN

Analisis paket data merupakan mekanisme yang penting dilakukan dalam jaringan komputer. Sebuah paket data jaringan adalah satuan informasi dasar yang dapat ditransmisikan di atas jaringan atau melalui saluran komunikasi digital. Sebuah paket data berisi packet header yang berisi informasi mengenai protokol tersebut yang berhubungan dengan jenis, sumber, tujuan, atau informasi lainnya

Wireshark merupakan salah satu aplikasi open source untuk mengetahui lalu lintas komunikasi data dalam jaringan dengan cara memantau dan menganalisa melalui protokol dan port-port jaringan yang digunakan. Wireshark adalah salah satu dari sekian banyak tool Network Analyzer yang banyak digunakan oleh Network administrator untuk menganalisa kinerja jaringannya. Wireshark sudah menggunakan Graphical User Interface (GUI) dan mampo menangkap paket-paket data dalam jaringan.