Monitoring Protokol ICMP menggunakan Wireshark

Annisa Cahyaningtyas
annisacahyaningtyas@gmail.com
http://annisacahyaningtyas.blogspot.com

1. Internet Control Message Protocol (ICMP)

Internet Control Message Protocol (ICMP) adalah salah satu protokol inti dari protokol internet. ICMP utamanya digunakan oleh sistem operasi komputer jaringan untuk mengirim pesan kesalahan yang menyatakan, sebagai contoh, bahwa komputer tujuan tidak bisa dijangkau.

ICMP berbeda tujuan dengan TCP dan UDP dalam hal ICMP tidak digunakan secara langsung oleh aplikasi jaringan milik pengguna. salah satu pengecualian adalah aplikasi ping yang mengirim pesan ICMP *Echo Request* (dan menerima *Echo Reply*) untuk menentukan apakah komputer tujuan dapat dijangkau dan berapa lama paket yang dikirimkan dibalas oleh komputer tujuan.

Internet Control Message Protocol (ICMP) adalah protokol yang digunakan untuk membantu error handling dan prosedur pengaturan (control procedure). Protokol ini bekerja pada network layer dan berurusan dengan layanan koneksi (connection services). Tugas dari ICMP adalah menyediakan *error control* dan *flow control* pada network layer.

Kegiatan yang berjalan di Internet dimonitor secara teliti oleh router. Jika terjadi seseuatu yang tidak diinginkan, kejadian tersebut akan dilaporkan oleh ICMP. ICMP mendeteksi kondisi error seperti kongesti/kemacetan internetwork (*internetwork congestion*) dan hubungan yang putus, lalu memberitahukan IP (Internet Protocol) dan protokol pada layer atas sehingga paket-paket dapat dikirimkan disekeliling area yang bermasalah.

Pesan/paket ICMP dikirim jika terjadi masalah pada layer IP dan layer atasnya (TCP/UDP). Pada konsisi normal, protokol IP berjalan dengan baik. Namun ada beberapa kondisi dimana koneksi IP terganggu, misalnya karena Router crash, putusnya kabel, atau matinya host tujuan. Pada saat ini ICMP membantu menstabilkan kondisi jaringan, dengan memberikan pesan-pesan tertentu sebagai respons atas kondisi tertentu yang terjadi pada jaringan tersebut.

2. Tipe Pesan ICMP

Ada dua tipe pesan yang dapat dihasilkan ICMP :

a. ICMP Error Message (dihasilkan jika terjadi kesalahan jaringan)
b. ICMP Query Message (dihasilkan jika pengirim paket mengirimkan informasi tertentu yang berkaitan dengan kondisi jaringan.

ICMP Error Message dibagi menjadi beberapa jenis :

1. Destination Unreachable, dihasilkan oleh router jika pengirim paket mengalami kegagalan akibat masalah putusnya jalur baik secara fisik maupun logic. Destination Unreacheable dibagi lagi menjadi beberapa jenis :
    a) Network Unreacheable, jika jaringan tujuan tak dapat dihubungi
    b) Host Unreacheable, jika host tujuan tak bisa dihubungi
    c) Protocol At Destination is Unreacheable, jika di tujuan tak tersedia protokol tersebut.
    d) Destination Host is Unknown, jika host tujuan tidak diketahui
    e) Destination Network is Unknown, jika network tujuan tidak diketahui

2. Time Exceeded, dikirimkan jika isi field TTL dalam paket IP sudah habis dan paket belum juga sampai ke tujuannya. Tiap kali sebuah paket IP melewati satu router, nilai TTL dalam paket tsb, dikurangi satu. TTL ini diterapkan untuk mencegah timbulnya paket IP yang terus menerus berputar-putar di network karena suatu kesalahan tertentu. sehingga menghabiskan sumber daya yang ada.
   Field TTL juga digunakan oleh program traceroute untuk melacak jalannya paket dari satu host ke host lain. Program traceroute dapat melakukan pelacakan rute berjalannya IP dengan cara mengirimkan paket kecil UDP ke IP tujuan, dengan TTL yang di set membesar.

Saat paket pertama dikirim, TTL diset satu, sehingga router pertama akan membuang paket ini dan mengirimkan paket ICMP Time Exceeded, kemudian paket kedua dikirim, dengan TTL dinaikan. Dengan naiknya TTL paket ini sukses melewati router pertama namun dibuang oleh router kedua, router ini pun mengirim paket ICMP time Exceeded.

3. Parameter Problem, paket ini dikirim jika terdapat kesalahan parameter pada header paket IP.
4. Source Quench, Paket ICMP ini dikirimkan jika router tujuan mengalami kongesti. Sebagai respons atas paket ini pihak pengirim paket harus memperlambat pengiriman paketnya.
5. Redirect, paket ini dikirimkan jika router merasa host mengirimkan paket IP melalui router yang salah. Paket ini seharusnya dikirimkan melalui router lain.

Sedangkan ICMP Query Message Terdiri atas :

1. Echo dan Echo Reply, Bertujuan untuk memeriksa apakah sistem tujuan dalam keadaan aktif. Program ping merupakan program pengisi paket ini. Respondet harus mengembalikan data yang sama dengan data yang dikirimkan.
2. Timestamp dan Timestamp Reply, Menghasilkan informasi waktu yang diperlukan sistem tujuan untuk memproses suatu paket.
3. Address mask, untuk mengetahui beberapa netmask yang harus digunakan suatu host dalam suatu network.

Sebagai paket pengatur kelancaran jaringan paket ICMP tidak diperbolehkan membebani network. Karenanya paket ICMP tidak boleh dikirim saat terjadi problem yang disebabkan oleh :

a. Kegagalan pengiriman paket ICMP
b. Kegagalan pengiriman paket broadcast atau multicast.

ICMP merupakan sebuah protokol manajemen dan penyedia layanan messaging untuk IP. ICMP berfungsi untuk melaporkan jika terjadi suatu masalah dalam pengiriman data. Berbagai hal yang dilaporkan adalah:

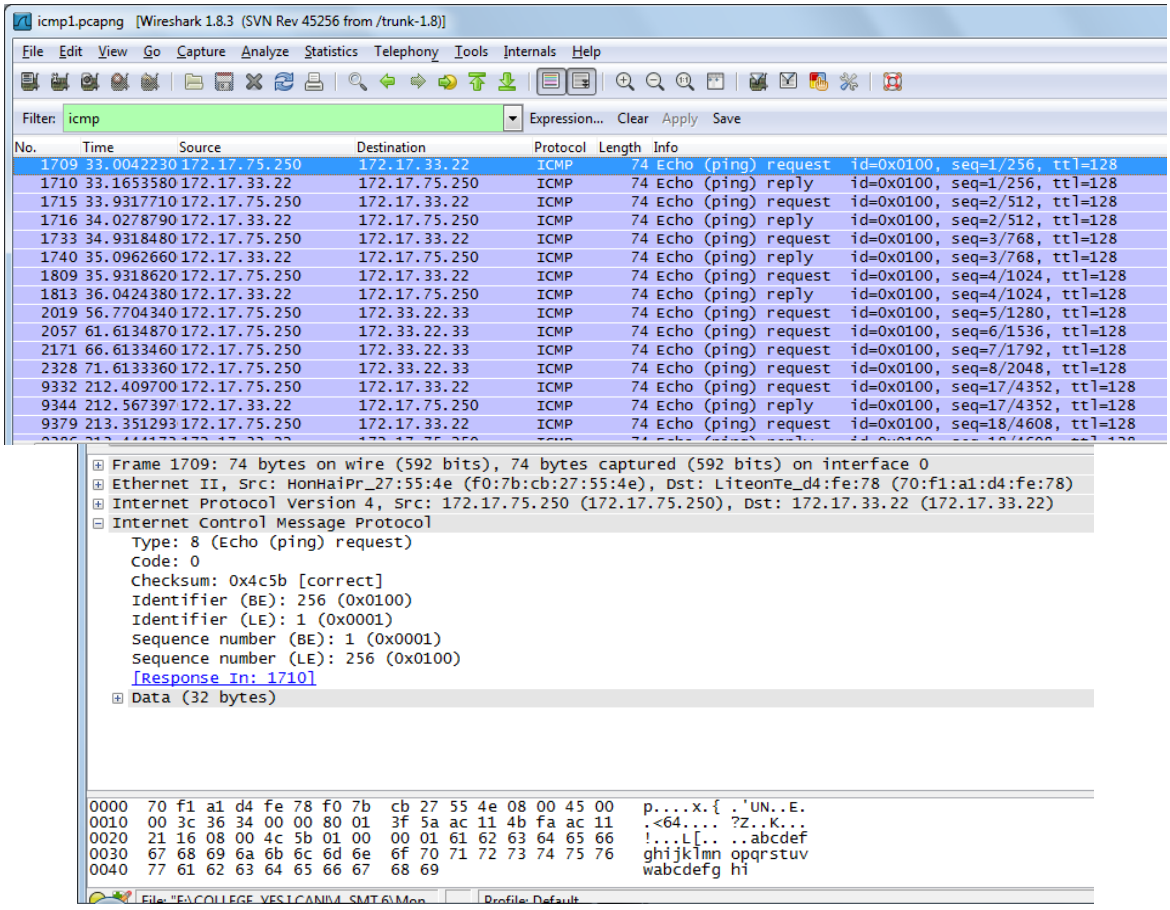
a. Destination Unreachable, merupakan laporan yang mengindikasikan bahwa tujuan tidak dapat dijangkau.

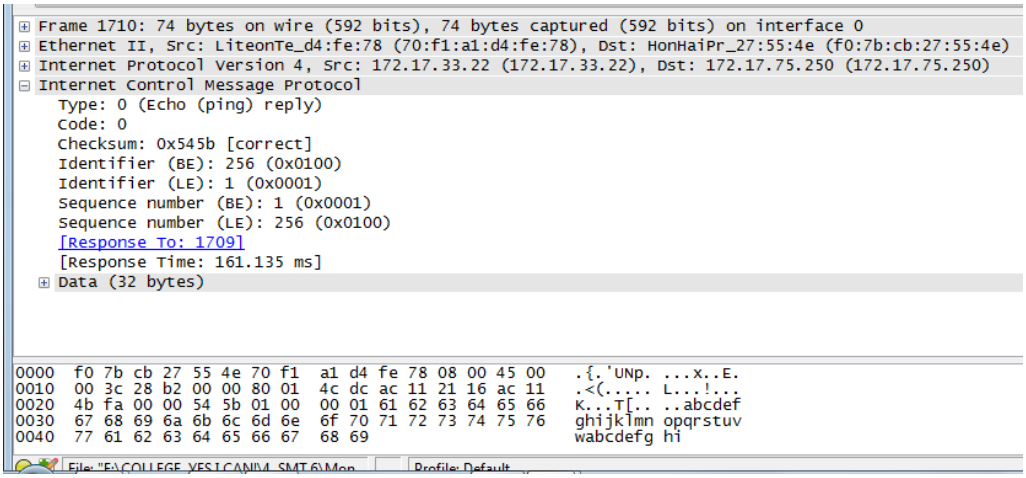
b. Buffer Bull, memberitahukan kepada pengirim jika memori penuh.
c. Hops, memberitahu pengirim bahwa paket telah melalui jumlah hop maksimum dan akan diabaikan.
d. Ping, menggunakan ICMP echo untuk memeriksa hubungan.

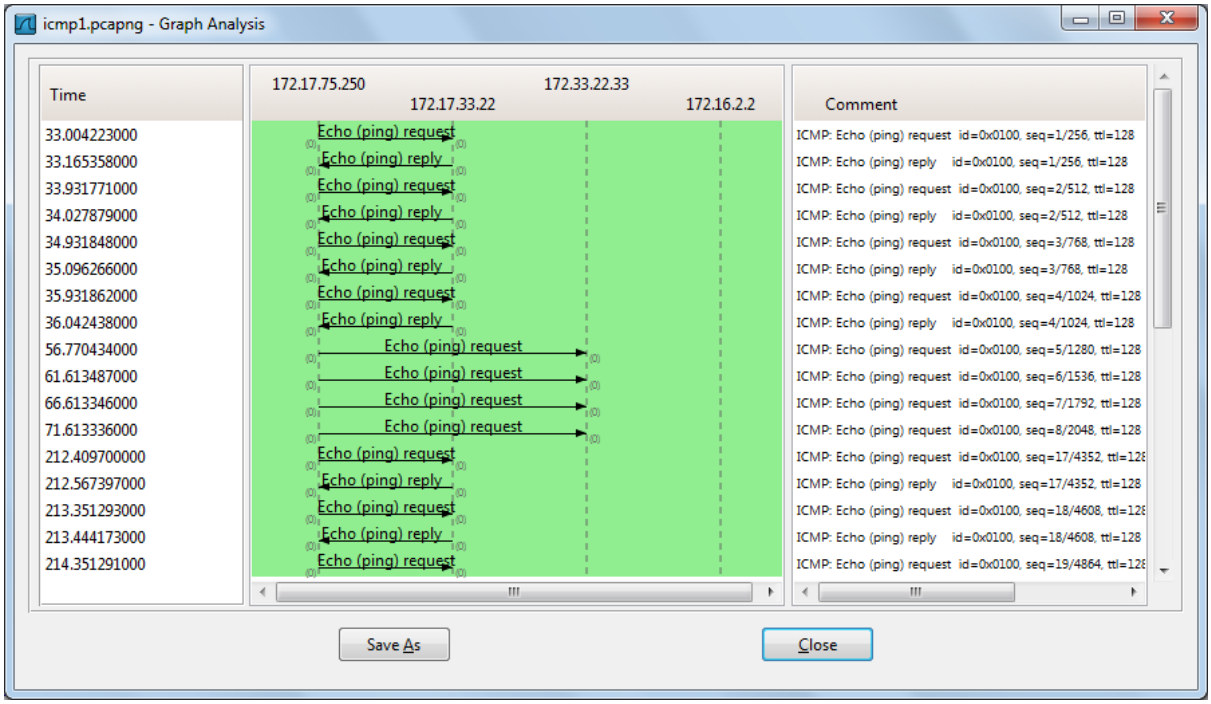
3. Monitoring ICMP menggunakan Wireshark

Dapat pula memonitoring protokol ICMP menggunakan Wireshark. Sebelumnya, kita sudah terhubung ke dalam suatu jaringan kemudian mengaktifkan terlebih dahulu aplikasi Wireshark lalu memilih Interfaces yang aktif kemudian dapat menuliskan ICMP pada kotak filter.

a. Tampilan Wireshark saat melakukan monitoring ICMP yang berhasil, hal tersebut dapat dilakukan dengan cara melakukan proses PING.







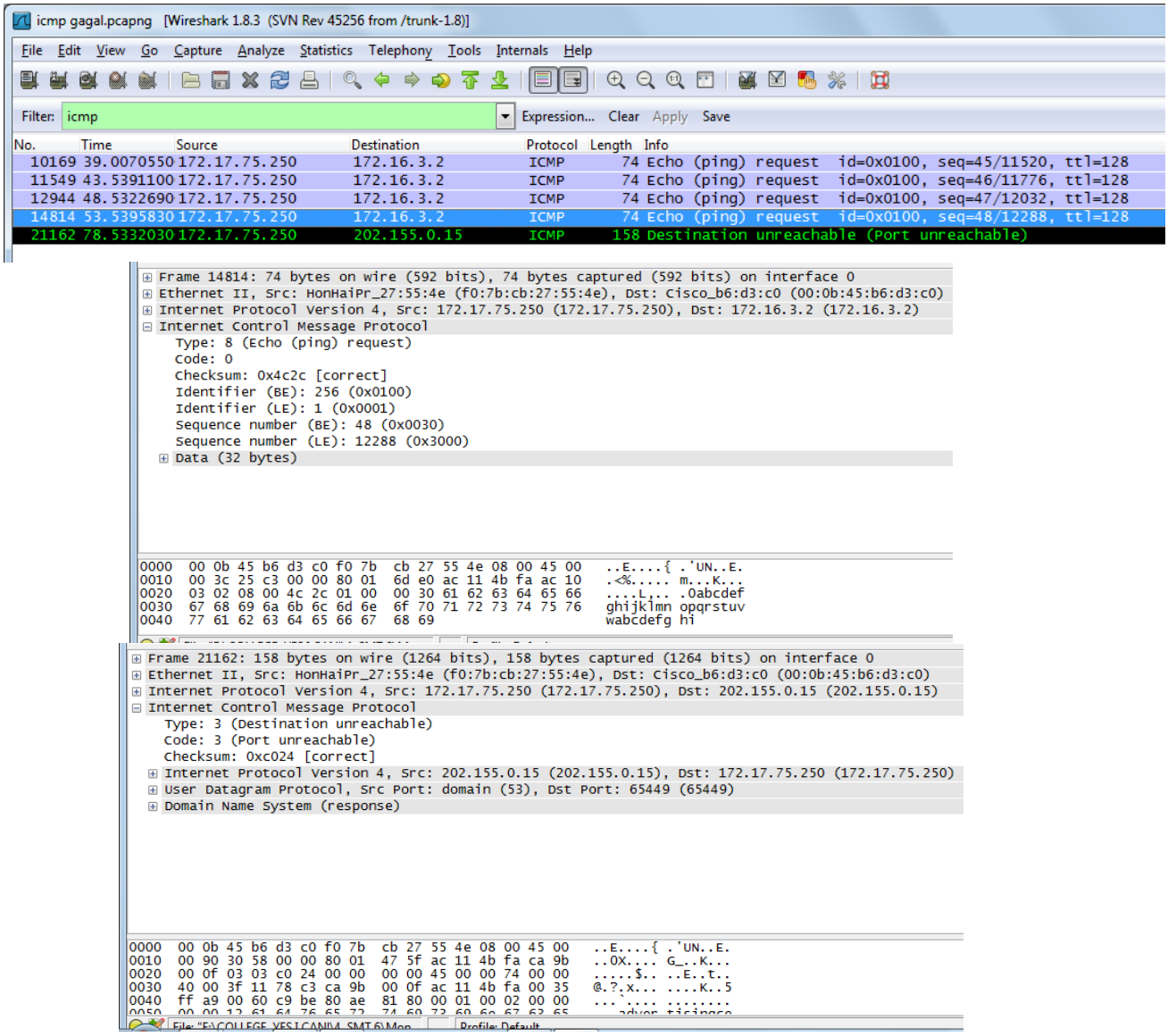
Terlihat bahwa pada saat proses aplikasi ping yang mengirim pesan ICMP *Echo Request* (dan menerima *Echo Reply*) untuk menentukan apakah komputer tujuan dapat dijangkau dan berapa lama paket yang dikirimkan dibalas oleh komputer tujuan, berhasil dilakukan seperti terlihat pada tampilan di atas.

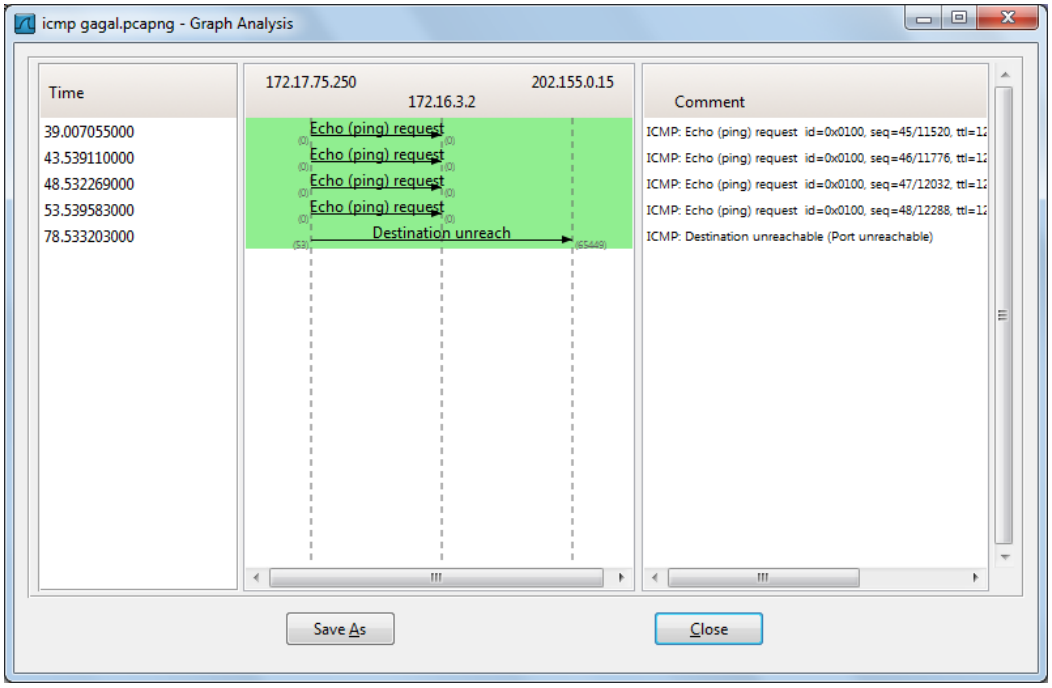
Secara teoritis, *echo request* dan *echo reply* adalah dua tipe pesan yang digunakan untuk melihat apakah tujuan (*destination*) dapat dicapai dan dalam keadaan hidup. Pada saat mengirim ECHO REQUEST, tujuan (*destination*) diharapkan untuk mengirim balik ECHO REPLY yang menandakan tujuan dapat dicapai dan dalam keadaan hidup.

Sesuai dengan tampilan capture dan flow graph, yang bertindak sebagai Source (sumber yang melakukan ping) memiliki IP 172.17.33.22 selalu mengirimkan Echo (ping) request pada proses awal, menuju Destination (tujuan dari ping yang diinginkan sumber)

memiliki IP 172.17.33.22 yang memberikan balasan Echo (ping) reply atau dengan kata lain ping yang dilakukan berhasil sebab sampai ke alamat tujuan.

b. Tampilan Wireshark saat melakukan monitoring ICMP yang tidak berhasil (destination unreachable), hal tersebut dapat dikarenakan saat melakukan proses PING terjadi error atau suatu proses terputusnya server pada suatu jaringan maka PING gagal.





Secara teoritis, Destination unreachable merupakan tipe pesan yang digunakan ketika subnet atau router tidak dapat menemukan tujuan, atau paket dengan DF bit tidak dapat dikirimkan, karena "paket-kecil" jaringan berada pada jalur.

Sesuai dengan tampilan capture dan flow graph, yang bertindak sebagai Source (sumber yang melakukan ping) memiliki IP 172.17.75.250 selalu mengirimkan Echo (ping) request pada proses awal, menuju Destination (tujuan dari ping yang diinginkan sumber) memiliki IP 172.17.3.2, namun belum juga memberikan balasan Echo (ping) reply seperti proses ping yang berhasil malah mendapat balasan Destination unreachable (port unreachable). Dapat diartikan bahwa seperti teori yang ada, bahwa balasan Destination Unreachable, mengindikasikan sebagai laporan bahwa tujuan tidak dapat dijangkau.

Dapat disimpulkan dari analisis menggunakan Wireshark, bahwa pada protokol ICMP memiliki empat jawaban, hal tersebut dapat dilihat lagi pada type dan code di tab Internet protokol, antara lain:

a. Request
   Type : 8
   Code : 0
b. Destination Unreacheble
   Type : 3
   Code : 3
c. Reply
   Type : 0
   Code : 0
d. Request Time Out
   Type : 0
   Code : 0

Biografi Penulis

Annisa Cahyaningtyas. Saat ini sedang menjalani studi D4 di Politeknik Negeri Semarang, Jurusan Teknik Elektro, Program Studi Teknik Telekomunikasi.