# ANALISA PERFORMANSI *INTERNET CONTROL MESSAGE PROTOCOL* (ICMP) DALAM KAITANNYA DENGAN SISTEM KEAMANAN JARINGAN KOMPUTER PADA PROTOKOL TCP/IP

**Iskandar Ikbal**
*Jurusan Teknik Informatika, F.T. Universitas Komputer Indonesia.*
*JL. Dipati Ukur No: 112-114 Bandung 40132*

## ABSTRAK

*Internet Control Message Protocol* (ICMP) adalah protokol yang bertugas mengirimkan pesan-pesan kesalahan dan kondisi lain yang memerlukan perhatian khusus. Dengan menganalisa performansi ICMP dalam kaitannya dengan sistem keamanan jaringan komputer pada protokol TCP/IP maka dapat diperoleh karakteristiknya yang terdiri dari format paket datagram IP dan format paket datagram ICMP.

Hasil dari penelitian menunjukkan bahwa format paket datagram ICMP khususnya ICMP *Query Message* untuk *Echo Request* dan *Echo Reply* pada protokol TCP/IP yang berhasil ditangkap oleh *Sniffer Ethereal* dapat memberikan informasi yang sangat berguna bagi seorang *hacker* untuk mengeksploitasi suatu sistem jaringan komputer minimal pada jaringan *Local Area Network* (LAN).

Kata Kunci : TCP/IP, ICMP, *Sniffer Ethereal.*

## I. PENDAHULUAN

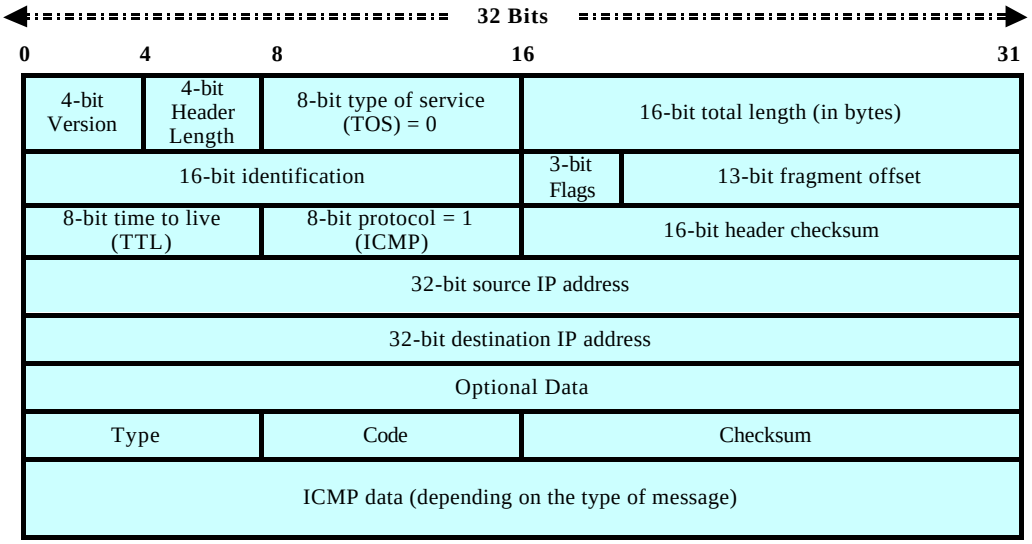
Paket pesan protokol ICMP terdiri dari dua jenis yaitu ICMP *Error Message* dan ICMP *Query Message*[1]. Masing-masing pesan memiliki spesifikasi yang berbeda-beda, untuk ICMP *Error Message* terbagi atas *Destination Unreachable, Time Exceeded, Parameter Problem, Source Quench,* dan *Redirect.* Sedangkan ICMP *Query Message* terdiri atas *Echo Request/Echo Reply, Timestamp/Timestamp Reply,* dan *Address Mask*[2].

Paket pesan ICMP muncul apabila terjadi masalah pada *layer Internet Protocol* (IP) dan *layer* di atasnya yaitu *Transport Control Protocol* (TCP) atau *User Datagram Protocol* (UDP)[3].

ICMP *message* dikirimkan di dalam paket datagram IP. Format paket datagram ICMP *message* dapat dilihat pada Gambar 1[4, 5].

Setiap ICMP *Error Message* terdiri dari *Internet Protocol* (IP) *header* dan sekurangnya delapan data oktet *(byte)* pada datagram. Pada kolom *Type* menspesifikasikan tipe dari *message,* kesalahan kode pada datagram dilaporkan oleh ICMP message pada kolom *Code.* Pengertian setiap kode bergantung dari tipe *message*[6].

Tujuan dari penelitian ini adalah untuk mengamati dan menganalisa karakteristik format paket datagram ICMP pada protokol TCP/IP.




Gambar 1. Format Paket Datagram ICMP *Message*

## II. PROSEDUR EKSPERIMEN

Penelitian dilakukan di Jurusan Teknik Informatika, Fakultas Teknik, Universitas Komputer Indonesia (UNIKOM). Instrumen yang digunakan dalam penelitian ini adalah tiga buah *Personal Computer* (PC) yang dihubungkan dengan *Router* PC menggunakan metode *peer to peer.*

Spesifikasi untuk masing-masing PC sebagai berikut:

PC 1

CPU : AMD Athlon XP 1700+ 1,5 GHz
Memory : DDR 256 MB /PC 2700
Harddisk : 40 GHz / 7200 RPM
VGA : 64 MB / Nvidia GeForce 2 MX200
NIC : Gigafast NC 100
OS : Windows XP Professional
IP Address : 192.168.0.3
Subnet Mask : 255.255.255.0
Tool/Software :
- Ethereal
- Ping

PC 2

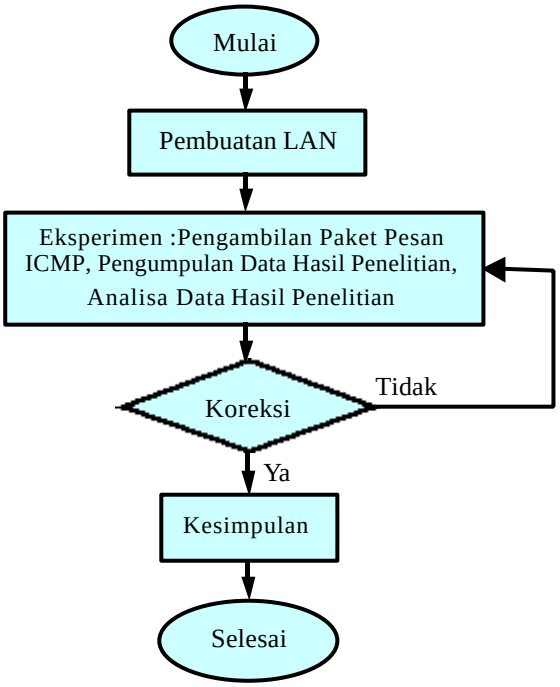
CPU : Intel Pentium IV 2,4 GHz
Memory : DDR 256 MB /PC 2700
Harddisk : 40 GHz / 7200 RPM
VGA : 64 MB / Nvidia GeForce 4 MX440
NIC : Realtek RTL 8129
OS : Windows XP Professional
IP Address : 196.168.0.2
Subnet Mask : 255.255.255.0
Tool/Software :
- Ethereal
- Ping

PC 3

| | |
|---|---|
| CPU | : Intel Pentium II 450 MHz |
| Memory | : SDR 128 MB /PC 2100 |
| Harddisk | : 20 GHz / 5400 RPM |
| VGA | : 32 MB / Nvidia GeForce 2 MX200 |
| NIC | : Compeq |
| OS | : Windows XP Professional |
| IP Address | : 192.168.0.1 |
| Subnet Mask | : 255.255.255.0 |
| Tool/Software | : |

- Ethereal
- Ping

Gambar 2 menunjukkan tahapan penelitian yang dilakukan.




Gambar 2. Tahapan Penelitian

## III. HASIL PERCOBAAN

Hasil penelitian yang dilakukan dengan mengirimkan *file Installer Flash* MX sebesar 56,3 MB tanpa disertai *error* dan dengan disertai *error* untuk menganalisa performansi ICMP dalam kaitannya dengan sistem keamanan jaringan komputer pada protokol TCP/IP meliputi karakteristik format datagram IP dan ICMP dapat dilihat pada Gambar 3, 4, 5, 6, 7 dan Gambar 8 di bawah ini:

### 1. Format Datagram IP pada transmisi data tanpa Disertai *Error* :

| | | | | |
|---|---|---|---|---|
| 4 | 20 bytes | 0 | 164 bytes | |
| 0x0587 | | | 0x04 | 0 |
| 128 | | 0x06 | 0x7344 | |
| 192.168.0.1 | | | | |
| 192.168.0.3 | | | | |
| Transaction Request | | | | |
| 32 bytes | | | | |

Gambar 3. Format Datagram IP untuk *Transaction Request*

| | | | | |
|---|---|---|---|---|
| 4 | 20 bytes | 0 | 164 bytes | |
| 0x3fbf | | | 0x04 | 0 |
| 128 | | 0x06 | 0x3955 | |
| 192.168.0.3 | | | | |
| 192.168.0.1 | | | | |
| Close Response | | | | |
| 32 bytes | | | | |

Gambar 4. Format Datagram IP untuk *Close Response*

## 2. Format Datagram IP pada transmisi data dengan Disertai *Error* :

| 4 | 20 bytes | 0 | 164 bytes |
|---|---|---|---|
| 0x7754 | | 0x04 | 0 |
| 128 | 0x06 | 0x01ab | |
| 192.168.0.1 | | | |
| 192.168.0.3 | | | |
| Transaction Request | | | |
| 32 bytes | | | |

Gambar 5. Format Datagram IP untuk *Transaction Request*

| 4 | 20 bytes | 0 | 60 bytes |
|---|---|---|---|
| 0x7799 | | 0x00 | 0 |
| 128 | 0x01 | 0x41d3 | |
| 192.168.0.1 | | | |
| 192.168.0.3 | | | |
| Internet Control Message Protocol (ICMP) | | | |
| 8 | 0 | 0xff2a | |
| 32 bytes | | | |

Gambar 6. Format Datagram ICMP *Genarally* untuk *Echo Request*

| 4 | 20 bytes | 0 | 60 bytes |
|---|---|---|---|
| 0xbc00 | | 0x00 | 0 |
| 128 | 0x01 | 0xfd6b | |
| 192.168.0.3 | | | |
| 192.168.0.1 | | | |
| Internet Control Message Protocol | | | |
| 0 | 0 | 0x072b | |
| 32 bytes | | | |

Gambar 7. Format Datagram ICMP *Generally* untuk *Echo Reply*

| 4 | 20 bytes | 0 | 79 bytes |
|---|---|---|---|
| 0x3fbf | | 0x04 | 0 |
| 128 | 6 | 0x9f55 | |
| 192.168.0.3 | | | |
| 192.168.0.1 | | | |
| Close Response | | | |
| 32 bytes | | | |

Gambar 8. Format Datagram IP untuk *Close Response*

Hasil penelitian yang telah dilakukan menunjukkan paket pesan datagram ICMP *Query Message* baik *Echo Request* ataupun *Echo Reply* tersebut selalu berada di dalam paket datagram IP, karena semua format paket datagram memiliki *header* IP yang besarnya 20 *bytes*, artinya ICMP merupakan bagian *internal* dari IP dan diimplementasikan di setiap modul IP.

## IV. KESIMPULAN DAN SARAN

**Kesimpulan :**

Dari penelitian di atas dapat ditarik kesimpulan yaitu :

1. Dengan menganalisa karakteristik dari format paket datagram IP, kita dapat memperoleh informasi-informasi yang sangat bermanfaat dalam hubungannya dengan sistem keamanan jaringan komputer pada protokol TCP/IP antara lain:
   - IP *Address* komputer/*host* asal.
   - IP *Address* komputer/*host* tujuan.
   - *Header* dari paket datagram IP berupa *versi, header length, type of service, total length, identification, flags, fragment offset, time to live, protocol, header checksum, source IP address,* dan *destination IP address.*
   - protokol yang dibawa oleh protokol IP yaitu protokol TCP, UDP, NBSS, dan SMB pada saat proses transmisi data pada penelitian ini.
2. Informasi lain yang bisa diperoleh adalah informasi mengenai paket datagram ICMP khususnya *Echo Request* (*type*=8) dan *Echo Reply* (*type*=0), yaitu mengetahui tipe, kode, *checksum,* identifikasi, *sequence number* dan data dari ICMP *Query Message.*
3. Dari keseluruhan penelitian di atas merupakan informasi yang sering kali dianggap tidak penting, tetapi sangat berguna bagi siapapun yang ingin mengeksploitasi suatu jaringan komputer baik dalam bentuk LAN, MAN, WAN bahkan GAN.

**Saran :**

Saran penulis dalam tugas akhir ini adalah:

1. Untuk dapat menggali lebih banyak dan untuk mengetahui karakteristik yang lebih baik dari protokol ICMP ini, penulis menyarankan untuk melakukan penelitian dengan konfigurasi jaringan komputer yang memiliki banyak *router*.
2. Penelitian yang dilakukan dan informasi yang diperoleh dari kegiatan tugas akhir ini masih belum sempurna dan ada beberapa kekurangan sebagai akibat dari keterbatasan fasilitas dan ilmu yang penulis miliki.
3. Apabila ada pihak lain yang akan melanjutkan dan menyempurnakan penelitian ini, maka tugas akhir ini dapat dijadikan sebagai bahan referensi dan pertimbangan untuk mendapatkan hasil yang lebih baik lagi.

## V. DAFTAR PUSTAKA


1. K. Jamsa and K. Cope. *Internet Programming*. Jamsa Press. ISBN 1-884133-12-6, page 564 (1995).
2. M. G. Naugle. *Network Protocol Handbook*. McGraw-Hill, Inc., ISBN 0-07-046461-8, page 256 (1994).
3. D. Maryanto. *Pedoman Instalasi & Penggunaan FreeBSD.* FreeBSD Maniac Press, halaman 14 (2000).
4. L. Tanutama. *Jaringan Komputer*. Elex Media Komputindo. ISBN 979-637-423-4, halaman 39 (1996).
5. O. Arkin. *ICMP Usage in Scanning*. Sys-Security Group., page 1-218 (2001)
6. F. Halsall. *Data Communications, Computer Network and Open Systems.* Addison-Wesley Publishing Company, page 755 (1996).