TUGAS

KEAMANAN JARINGAN KOMPUTER

“SNORT”

Devi Purnama

09011281320016

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

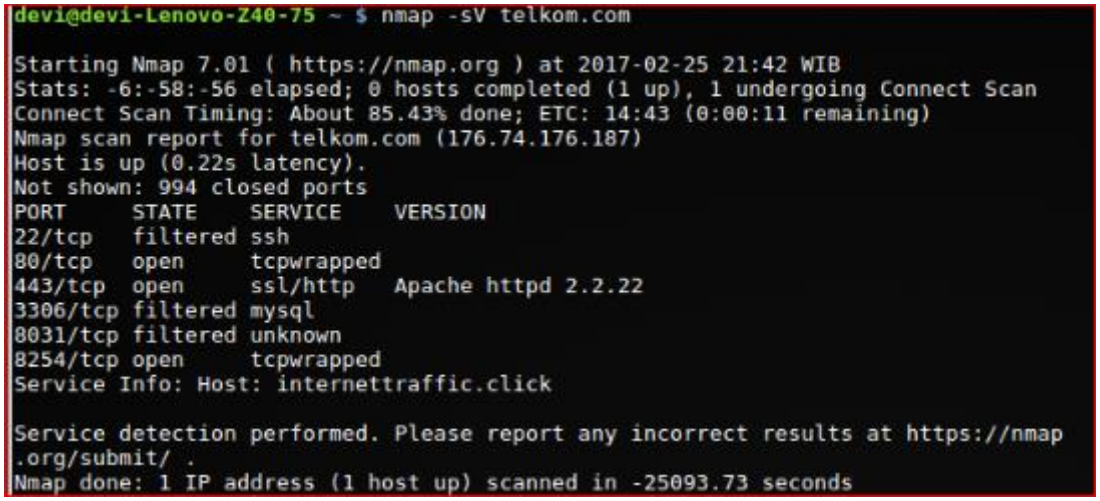
2017

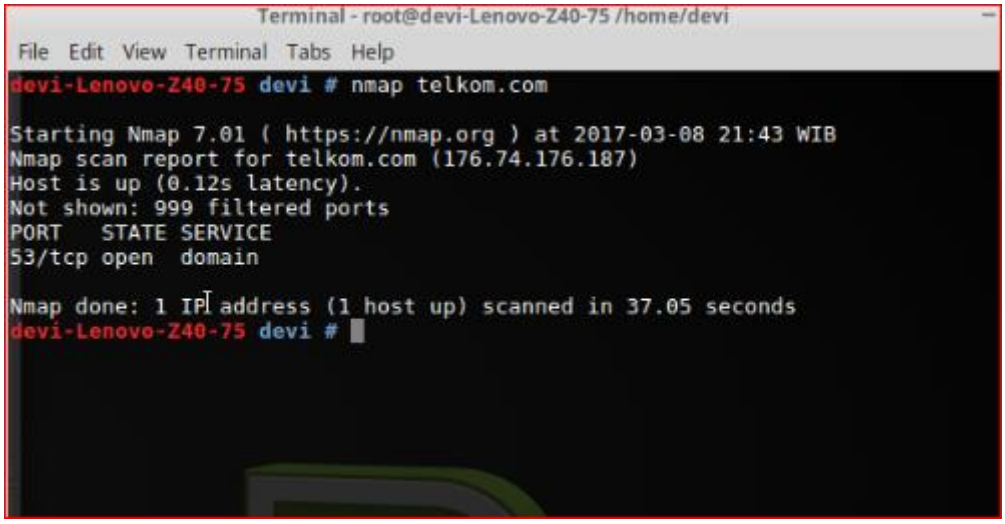
Domain : telkom.com

IP Address : 176.74.176.187

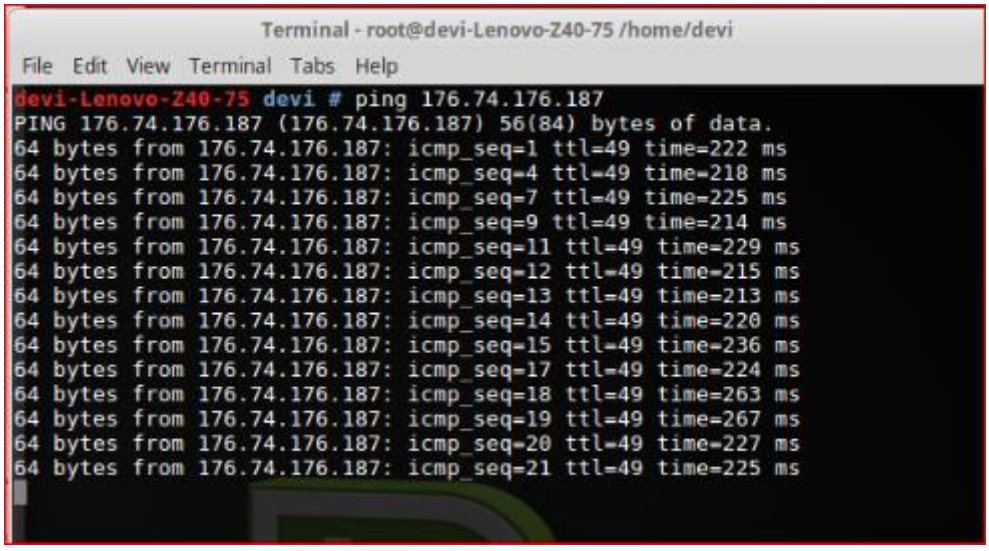
Hasil scanning yang di lakukan dengan target telkom.com, dengan menggunakan tools Xprobe dan Nmap, dengan melakukan scanning lebih kurang 20 menit. Berikut adalah hasil dari scanning, dan snort dengan menggunakan wireshark. Snort merupakan software yang digunakan untuk mengamati aktivitas dalam sebua jaringan komputer, snort dapat digunakan dlaam suatu NIDS(Networt Intrusion Detection System). Wireshark merupakan perangkat lunak yang spesifik untuk melakukan analisa paket data pada jaringan secara real time dan menampilkan hasil analisa paket data tersebut dalam format yang dipahami oleh pengguna. Wireshark dapat melakukan paket filtering, paket color coding, dan fitur-fitur lain yang dapat mengizinkan untuk melihat detail network traffic dan inspeksi paket data secara individu, Wireshark dapat menganalisis paket data secara real time. Artinya, aplikasi wireshark akan mengawasi semua paket data yang keluar masuk melalui antarmuka yang telah ditentukan dan selanjutnya akan menampilkan hasil paket datanya.

1. Lakukan Nmap pada telkom.com untuk mengtahui ip target.

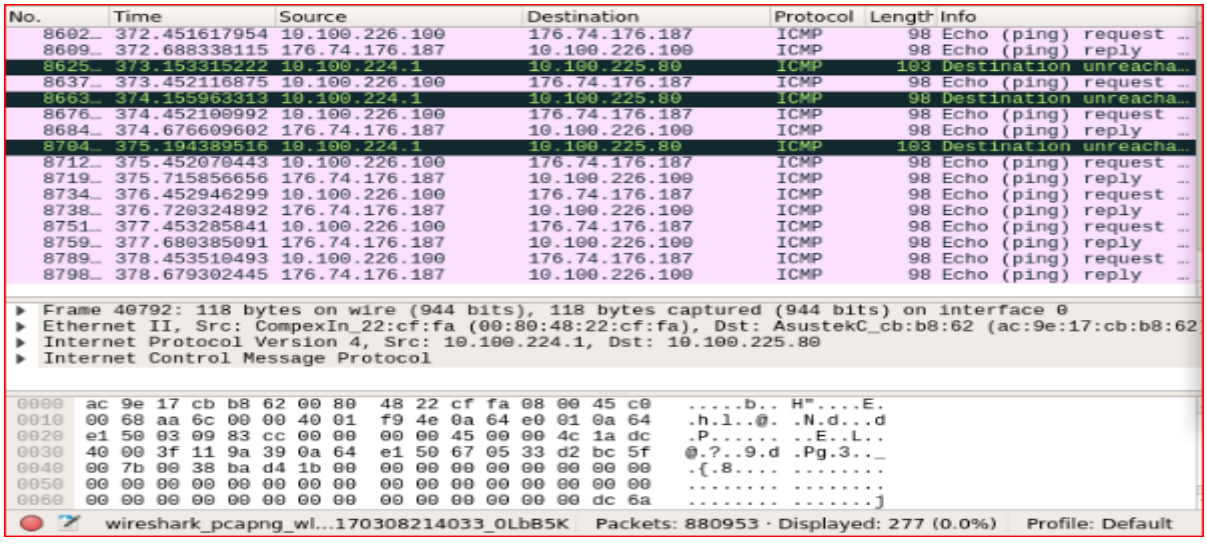


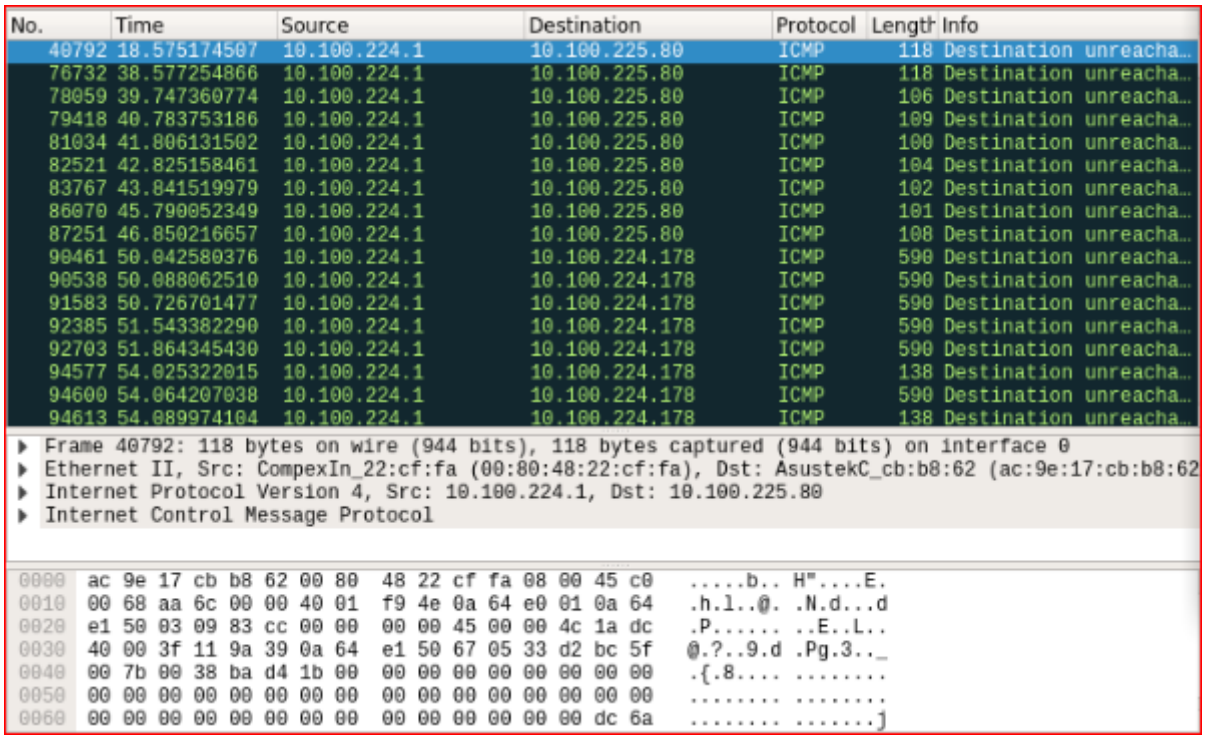


2. Lakukan Ping pada Ip Target



3. Hasil dari Wereshark yang dikukan pada saat ping pada ip target, yang berfungsi untuk merekam aktivitas pertukaran data yang di lakukan.



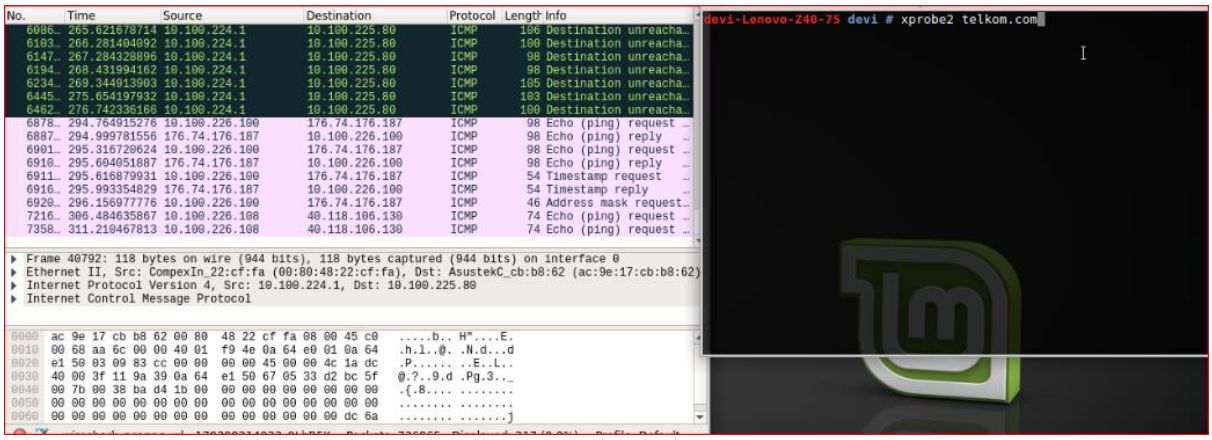


No.	Time	Source	Destination	Protocol	Length	Info
40792	18.575174507	10.100.224.1	10.100.225.80	ICMP	118	Destination unreacha…
76732	38.577254866	10.100.224.1	10.100.225.80	ICMP	118	Destination unreacha…
78059	39.747360774	10.100.224.1	10.100.225.80	ICMP	106	Destination unreacha…
79418	40.783753186	10.100.224.1	10.100.225.80	ICMP	109	Destination unreacha…
81034	41.806131502	10.100.224.1	10.100.225.80	ICMP	100	Destination unreacha…
82521	42.825158461	10.100.224.1	10.100.225.80	ICMP	104	Destination unreacha…
83767	43.841519979	10.100.224.1	10.100.225.80	ICMP	102	Destination unreacha…
86070	45.790052349	10.100.224.1	10.100.225.80	ICMP	101	Destination unreacha…
87251	46.850216657	10.100.224.1	10.100.225.80	ICMP	108	Destination unreacha…
90461	50.042580376	10.100.224.1	10.100.224.178	ICMP	590	Destination unreacha…
90538	50.088062510	10.100.224.1	10.100.224.178	ICMP	590	Destination unreacha…
91583	50.726701477	10.100.224.1	10.100.224.178	ICMP	590	Destination unreacha…
92385	51.543382290	10.100.224.1	10.100.224.178	ICMP	590	Destination unreacha…
92703	51.864345430	10.100.224.1	10.100.224.178	ICMP	590	Destination unreacha…
94577	54.025322015	10.100.224.1	10.100.224.178	ICMP	138	Destination unreacha…
94600	54.064207038	10.100.224.1	10.100.224.178	ICMP	590	Destination unreacha…
94613	54.089974104	10.100.224.1	10.100.224.178	ICMP	138	Destination unreacha…

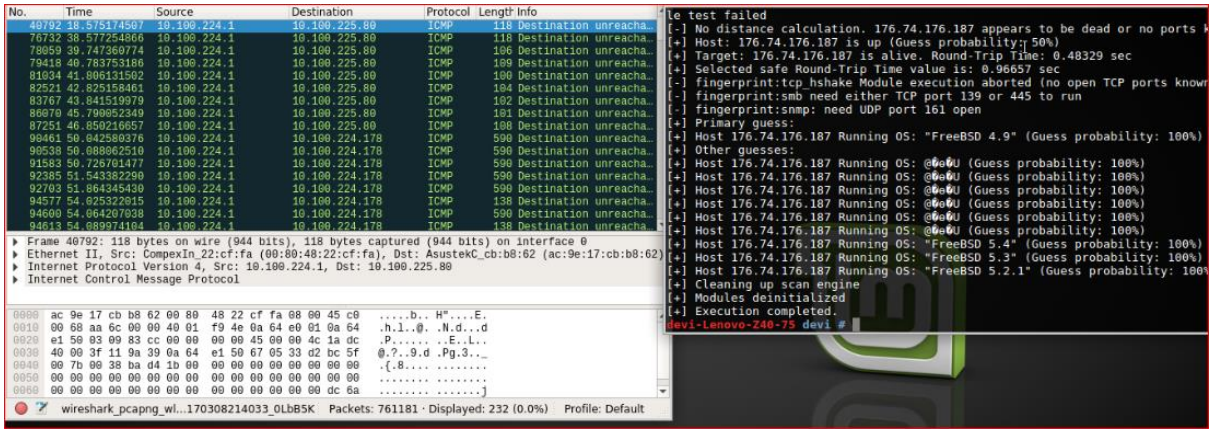
```
▸ Frame 40792: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0
▸ Ethernet II, Src: CompexIn_22:cf:fa (00:80:48:22:cf:fa), Dst: AsustekC_cb:b8:62 (ac:9e:17:cb:b8:62
▸ Internet Protocol Version 4, Src: 10.100.224.1, Dst: 10.100.225.80
▸ Internet Control Message Protocol
```

```
0000  ac 9e 17 cb b8 62 00 80  48 22 cf fa 08 00 45 c0   .....b.. H"....E.
0010  00 68 aa 6c 00 00 40 01  f9 4e 0a 64 e0 01 0a 64   .h.l..@. .N.d...d
0020  e1 50 03 09 83 cc 00 00  00 00 45 00 00 4c 1a dc   .P...... ..E..L..
0030  40 00 3f 11 9a 39 0a 64  e1 50 67 05 33 d2 bc 5f   @.?..9.d .Pg.3.._
0040  00 7b 00 38 ba d4 1b 00  00 00 00 00 00 00 00 00   .{.8.... ........
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 dc 6a   ........ .......j
```

4. Scanning target dengan menggunakan xprobe



```
devi-Lenovo-Z40-75 devi # xprobe2 telkom.com
```



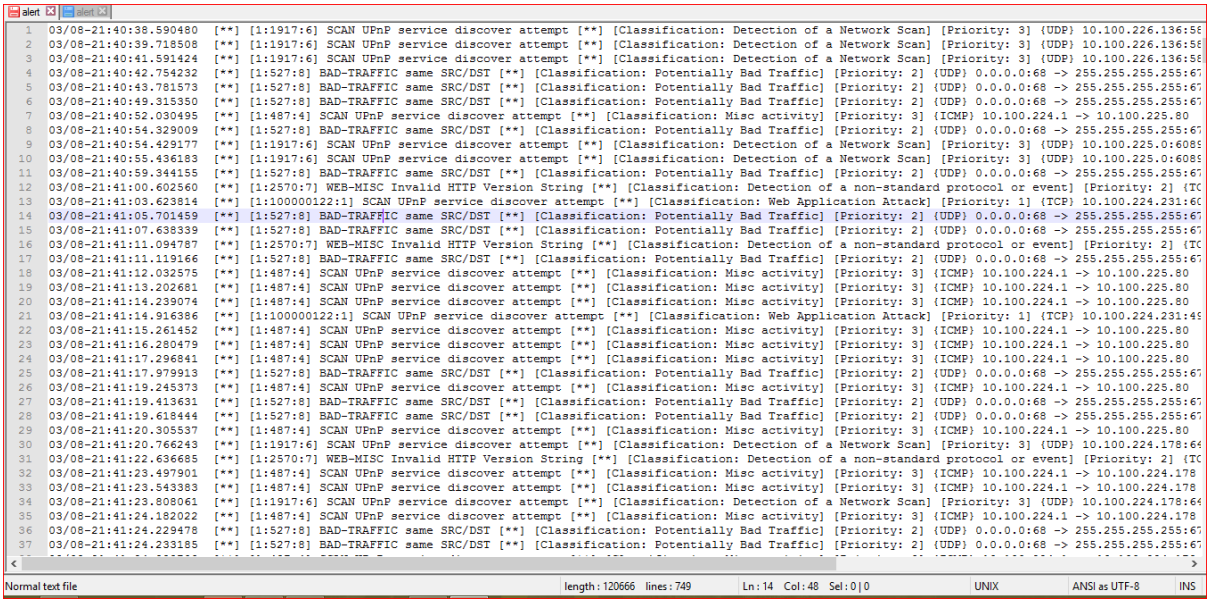
```
le test failed
[-] No distance calculation. 176.74.176.187 appears to be dead or no ports k
[+] Host: 176.74.176.187 is up (Guess probability: 50%)
[+] Target: 176.74.176.187 is alive. Round-Trip Time: 0.48329 sec
[+] Selected safe Round-Trip Time value is: 0.96657 sec
[-] fingerprint:tcp_hshake Module execution aborted (no open TCP ports known
[-] fingerprint:smb need either TCP port 139 or 445 to run
[-] fingerprint:snmp: need UDP port 161 open
[+] Primary guess:
[+] Host 176.74.176.187 Running OS: "FreeBSD 4.9" (Guess probability: 100%)
[+] Other guesses:
[+] Host 176.74.176.187 Running OS: @@@@U (Guess probability: 100%)
[+] Host 176.74.176.187 Running OS: @@@@U (Guess probability: 100%)
[+] Host 176.74.176.187 Running OS: @@@@U (Guess probability: 100%)
[+] Host 176.74.176.187 Running OS: @@@@U (Guess probability: 100%)
[+] Host 176.74.176.187 Running OS: @@@@U (Guess probability: 100%)
[+] Host 176.74.176.187 Running OS: @@@@U (Guess probability: 100%)
[+] Host 176.74.176.187 Running OS: "FreeBSD 5.4" (Guess probability: 100%)
[+] Host 176.74.176.187 Running OS: "FreeBSD 5.3" (Guess probability: 100%)
[+] Host 176.74.176.187 Running OS: "FreeBSD 5.2.1" (Guess probability: 100%
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
devi-Lenovo-Z40-75 devi #
```

5. Hasil snort

```
snort -A fast -c /etc/snort/snort.conf -r tugas_snort.pcap
```

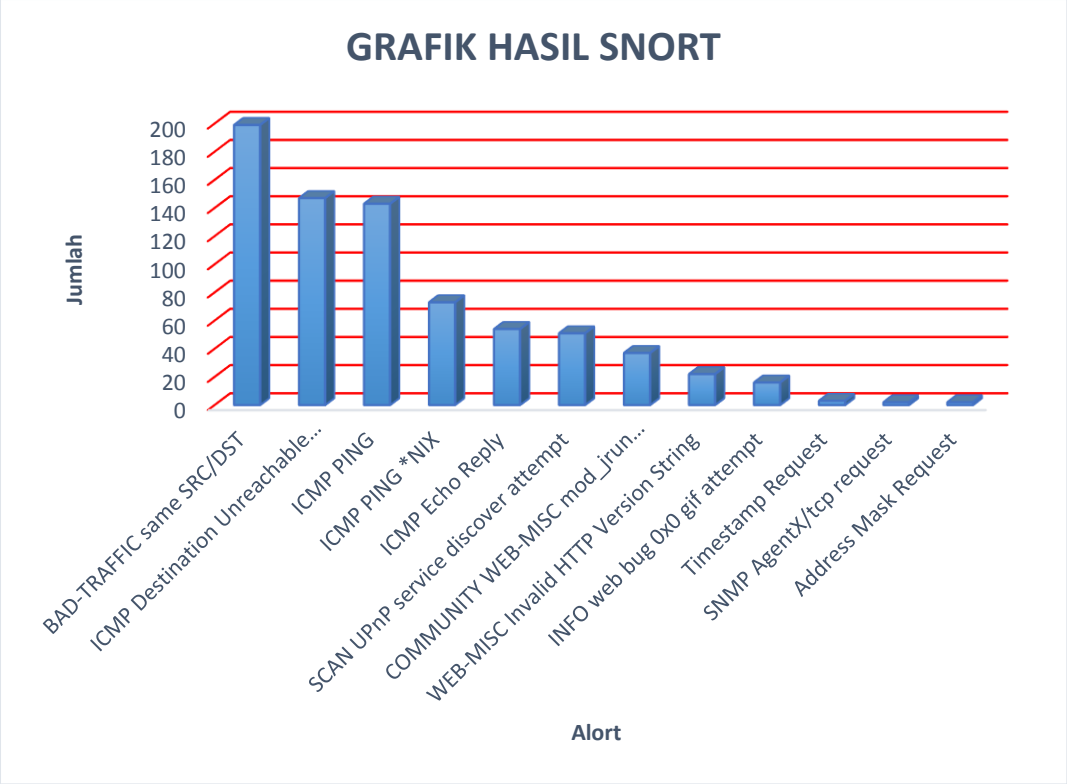
```
  Max concurrent sessions                          : 0
===============================================================================
dcerpc2 Preprocessor Statistics
  Total sessions: 3
  Total sessions aborted: 2

  Transports
    SMB
      Total sessions: 3
      Packet stats
        Packets: 32
        Ignored bytes: 730
        Maximum outstanding requests: 1
        SMB command requests/responses processed
          Transaction (0x25) : 2/0
          Tree Disconnect (0x71) : 1/1
          Negotiate (0x72) : 3/2
          Session Setup AndX (0x73) : 4/4
          Logoff AndX (0x74) : 1/1
          Tree Connect AndX (0x75) : 2/2
===============================================================================
SSL Preprocessor:
   SSL packets decoded: 24119
           Client Hello: 1100
           Server Hello: 619
            Certificate: 552
            Server Done: 1496
   Client Key Exchange: 458
   Server Key Exchange: 230
         Change Cipher: 1319
              Finished: 0
    Client Application: 2872
    Server Application: 468
                 Alert: 402
  Unrecognized records: 11848
  Completed handshakes: 0
       Bad handshakes: 146
      Sessions ignored: 393
    Detection disabled: 6987
===============================================================================
SIP Preprocessor Statistics
  Total sessions: 0
===============================================================================
Snort exiting
devi-Lenovo-Z40-75 Documents #
```

6. Hasil Snort yang telah dilakukan pada target, maka kita dapat menetahui daftar dari Alert yang telah di rekam pada wireshark.



7. **TABEL HASIL SNORT ALERT PADA WIRESHARK**

No	Alert	Jumlah
1	BAD-TRAFFIC same SRC/DST	199
2	ICMP Destination Unreachable Communication with Destination Network is Administratively Prohibited	147
3	ICMP PING	143
4	ICMP PING *NIX	73
5	ICMP Echo Reply	54
6	SCAN UPnP service discover attempt	51
7	COMMUNITY WEB-MISC mod_jrun overflow attempt	37
8	WEB-MISC Invalid HTTP Version String	22
9	INFO web bug 0x0 gif attempt	16
10	Timestamp Request	3
11	SNMP AgentX/tcp request	2
12	Address Mask Request	2


GRAFIK HASIL SNORT
Jumlah
200
180
160
140
120
100
80
60
40
20
0
BAD-TRAFFIC same SRC/DST
ICMP Destination Unreachable...
ICMP PING
ICMP PING *NIX
ICMP Echo Reply
SCAN UPnP service discover attempt
COMMUNITY WEB-MISC mod_jrun...
WEB-MISC Invalid HTTP Version String
INFO web bug 0x0 gif attempt
Timestamp Request
SNMP AgentX/tcp request
Address Mask Request
Alort