TUGAS

“KEAMANAN JARINGAN KOMPUTER”

Disusun Oleh :

Nama : Nova Dyati Pradista

Nim : 09011181320005

JURUSAN SISTEM KOMPUTER

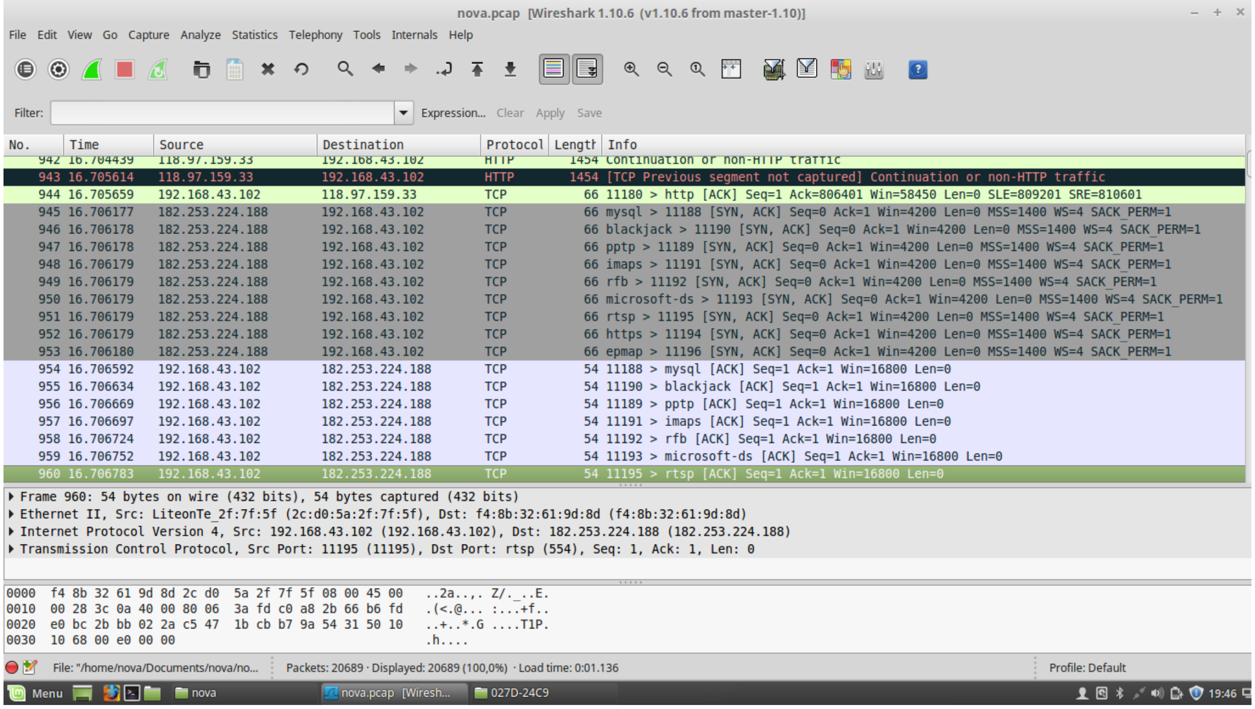
FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

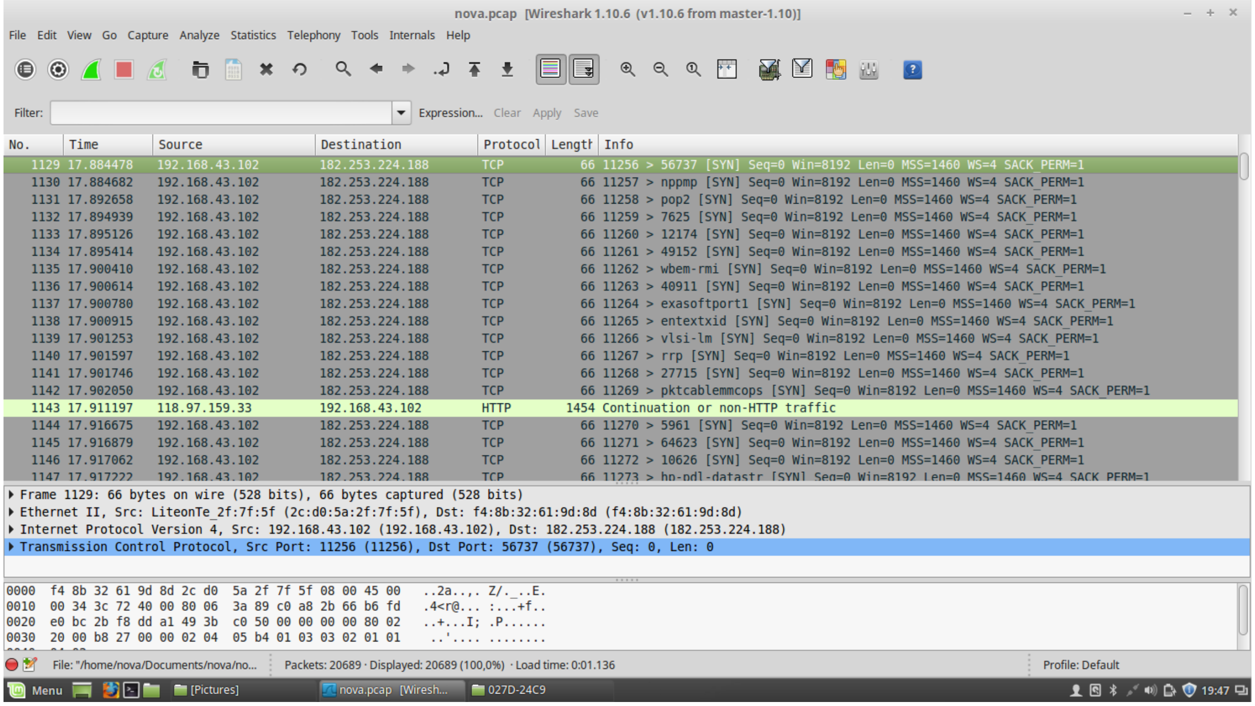
2017

Domain : www.tokopedia.com

Berikut tampilan hasil dari scanning yang direkam menggunakan wireshark dengan domain 182.253.224.188 :


nova.pcap [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
Menu
nova
nova.pcap [Wiresh...
027D-24C9
19:46

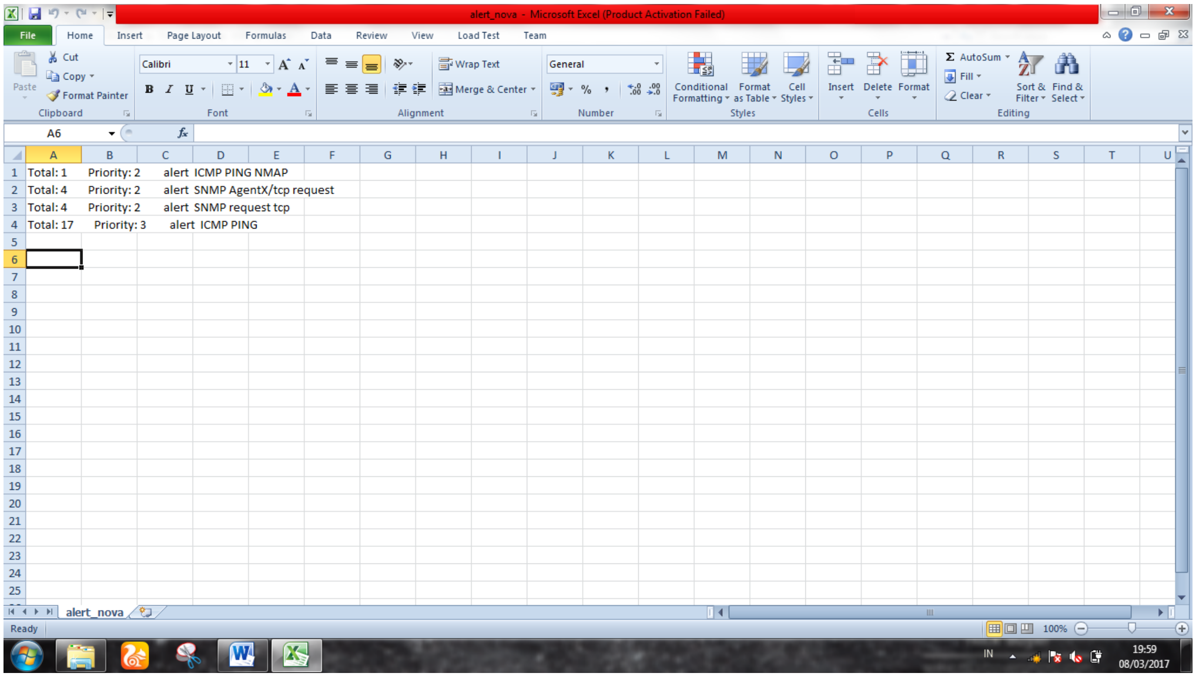
```
No.   Time       Source          Destination     Protocol Length Info
  942 16.704439  118.97.159.33   192.168.43.102  HTTP     1454 Continuation or non-HTTP traffic
  943 16.705614  118.97.159.33   192.168.43.102  HTTP     1454 [TCP Previous segment not captured] Continuation or non-HTTP traffic
  944 16.705659  192.168.43.102  118.97.159.33   TCP        66 11180 > http [ACK] Seq=1 Ack=806401 Win=58450 Len=0 SLE=809201 SRE=810601
  945 16.706177  182.253.224.188 192.168.43.102  TCP        66 mysql > 11188 [SYN, ACK] Seq=0 Ack=1 Win=4200 Len=0 MSS=1400 WS=4 SACK_PERM=1
  946 16.706178  182.253.224.188 192.168.43.102  TCP        66 blackjack > 11190 [SYN, ACK] Seq=0 Ack=1 Win=4200 Len=0 MSS=1400 WS=4 SACK_PERM=1
  947 16.706178  182.253.224.188 192.168.43.102  TCP        66 pptp > 11189 [SYN, ACK] Seq=0 Ack=1 Win=4200 Len=0 MSS=1400 WS=4 SACK_PERM=1
  948 16.706179  182.253.224.188 192.168.43.102  TCP        66 imaps > 11191 [SYN, ACK] Seq=0 Ack=1 Win=4200 Len=0 MSS=1400 WS=4 SACK_PERM=1
  949 16.706179  182.253.224.188 192.168.43.102  TCP        66 rfb > 11192 [SYN, ACK] Seq=0 Ack=1 Win=4200 Len=0 MSS=1400 WS=4 SACK_PERM=1
  950 16.706179  182.253.224.188 192.168.43.102  TCP        66 microsoft-ds > 11193 [SYN, ACK] Seq=0 Ack=1 Win=4200 Len=0 MSS=1400 WS=4 SACK_PERM=1
  951 16.706179  182.253.224.188 192.168.43.102  TCP        66 rtsp > 11195 [SYN, ACK] Seq=0 Ack=1 Win=4200 Len=0 MSS=1400 WS=4 SACK_PERM=1
  952 16.706179  182.253.224.188 192.168.43.102  TCP        66 https > 11194 [SYN, ACK] Seq=0 Ack=1 Win=4200 Len=0 MSS=1400 WS=4 SACK_PERM=1
  953 16.706180  182.253.224.188 192.168.43.102  TCP        66 epmap > 11196 [SYN, ACK] Seq=0 Ack=1 Win=4200 Len=0 MSS=1400 WS=4 SACK_PERM=1
  954 16.706592  192.168.43.102  182.253.224.188 TCP        54 11188 > mysql [ACK] Seq=1 Ack=1 Win=16800 Len=0
  955 16.706634  192.168.43.102  182.253.224.188 TCP        54 11190 > blackjack [ACK] Seq=1 Ack=1 Win=16800 Len=0
  956 16.706669  192.168.43.102  182.253.224.188 TCP        54 11189 > pptp [ACK] Seq=1 Ack=1 Win=16800 Len=0
  957 16.706697  192.168.43.102  182.253.224.188 TCP        54 11191 > imaps [ACK] Seq=1 Ack=1 Win=16800 Len=0
  958 16.706724  192.168.43.102  182.253.224.188 TCP        54 11192 > rfb [ACK] Seq=1 Ack=1 Win=16800 Len=0
  959 16.706752  192.168.43.102  182.253.224.188 TCP        54 11193 > microsoft-ds [ACK] Seq=1 Ack=1 Win=16800 Len=0
  960 16.706783  192.168.43.102  182.253.224.188 TCP        54 11195 > rtsp [ACK] Seq=1 Ack=1 Win=16800 Len=0

▸ Frame 960: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
▸ Ethernet II, Src: LiteonTe_2f:7f:5f (2c:d0:5a:2f:7f:5f), Dst: f4:8b:32:61:9d:8d (f4:8b:32:61:9d:8d)
▸ Internet Protocol Version 4, Src: 192.168.43.102 (192.168.43.102), Dst: 182.253.224.188 (182.253.224.188)
▸ Transmission Control Protocol, Src Port: 11195 (11195), Dst Port: rtsp (554), Seq: 1, Ack: 1, Len: 0

0000  f4 8b 32 61 9d 8d 2c d0  5a 2f 7f 5f 08 00 45 00   ..2a..,. Z/._..E.
0010  00 28 3c 0a 40 00 80 06  3a fd c0 a8 2b 66 b6 fd   .(<.@... :...+f..
0020  e0 bc 2b bb 02 2a c5 47  1b cb b7 9a 54 31 50 10   ..+..*.G ....T1P.
0030  10 68 00 e0 00 00                                  .h....

File: "/home/nova/Documents/nova/no...   Packets: 20689 · Displayed: 20689 (100,0%) · Load time: 0:01.136   Profile: Default
```


nova.pcap [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
Menu
[Pictures]
nova.pcap [Wiresh...
027D-24C9
19:47

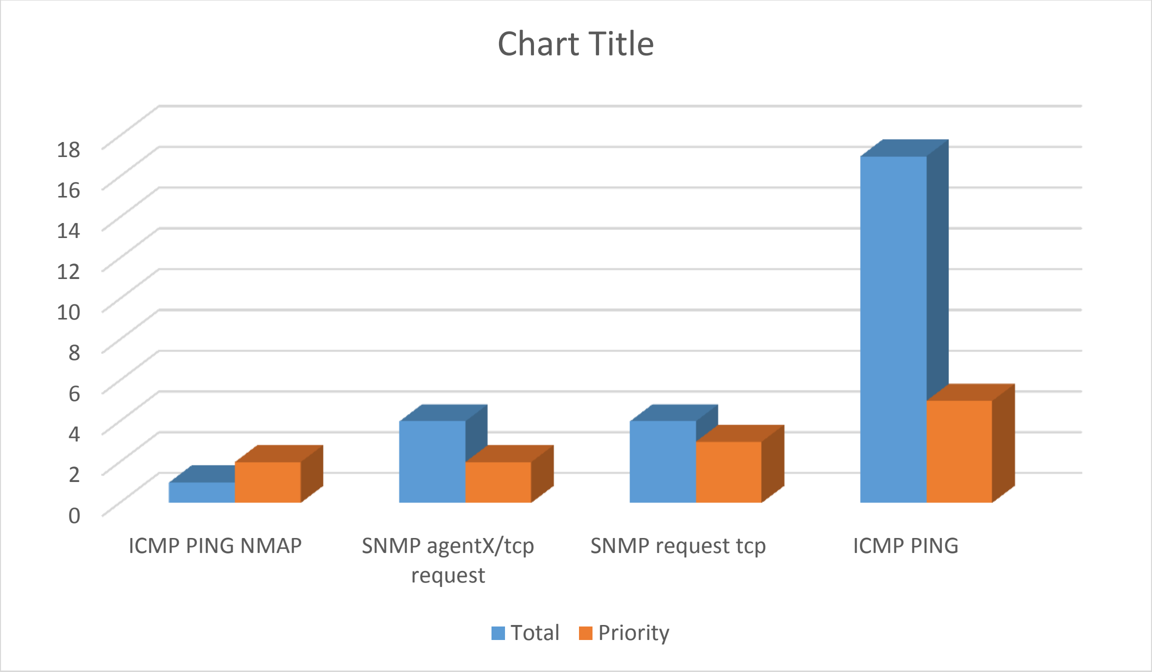
```
No.   Time       Source          Destination     Protocol Length Info
 1129 17.884478  192.168.43.102  182.253.224.188 TCP        66 11256 > 56737 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
 1130 17.884682  192.168.43.102  182.253.224.188 TCP        66 11257 > nppmp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
 1131 17.892658  192.168.43.102  182.253.224.188 TCP        66 11258 > pop2 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
 1132 17.894939  192.168.43.102  182.253.224.188 TCP        66 11259 > 7625 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
 1133 17.895126  192.168.43.102  182.253.224.188 TCP        66 11260 > 12174 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
 1134 17.895414  192.168.43.102  182.253.224.188 TCP        66 11261 > 49152 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
 1135 17.900410  192.168.43.102  182.253.224.188 TCP        66 11262 > wbem-rmi [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
 1136 17.900614  192.168.43.102  182.253.224.188 TCP        66 11263 > 40911 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
 1137 17.900780  192.168.43.102  182.253.224.188 TCP        66 11264 > exasoftport1 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
 1138 17.900915  192.168.43.102  182.253.224.188 TCP        66 11265 > entextxid [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
 1139 17.901253  192.168.43.102  182.253.224.188 TCP        66 11266 > vlsi-lm [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
 1140 17.901597  192.168.43.102  182.253.224.188 TCP        66 11267 > rrp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
 1141 17.901746  192.168.43.102  182.253.224.188 TCP        66 11268 > 27715 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
 1142 17.902050  192.168.43.102  182.253.224.188 TCP        66 11269 > pktcablemmcops [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
 1143 17.911197  118.97.159.33   192.168.43.102  HTTP     1454 Continuation or non-HTTP traffic
 1144 17.916675  192.168.43.102  182.253.224.188 TCP        66 11270 > 5961 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
 1145 17.916879  192.168.43.102  182.253.224.188 TCP        66 11271 > 64623 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
 1146 17.917062  192.168.43.102  182.253.224.188 TCP        66 11272 > 10626 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
 1147 17.917222  192.168.43.102  182.253.224.188 TCP        66 11273 > hp-pdl-datastr [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1

▸ Frame 1129: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▸ Ethernet II, Src: LiteonTe_2f:7f:5f (2c:d0:5a:2f:7f:5f), Dst: f4:8b:32:61:9d:8d (f4:8b:32:61:9d:8d)
▸ Internet Protocol Version 4, Src: 192.168.43.102 (192.168.43.102), Dst: 182.253.224.188 (182.253.224.188)
▸ Transmission Control Protocol, Src Port: 11256 (11256), Dst Port: 56737 (56737), Seq: 0, Len: 0

0000  f4 8b 32 61 9d 8d 2c d0  5a 2f 7f 5f 08 00 45 00   ..2a..,. Z/._..E.
0010  00 34 3c 72 40 00 80 06  3a 89 c0 a8 2b 66 b6 fd   .4<r@... :...+f..
0020  e0 bc 2b f8 dd a1 49 3b  c0 50 00 00 00 00 80 02   ..+...I; .P......
0030  20 00 b8 27 00 00 02 04  05 b4 01 03 03 02 01 01    ..'.... ........

File: "/home/nova/Documents/nova/no...   Packets: 20689 · Displayed: 20689 (100,0%) · Load time: 0:01.136   Profile: Default
```

Pada tampilan wireshark diatas dapat dilihat time, source, destination, protocol, length, dan info, dengan alamat ip targetnya 182.253.224.188 dengan menggunakan banyak protokol TCP.

Berikut hasil compile dengan snort –r sehingga menghasilkan alert dan grafik seperti gambar dibawah ini :



	A	B	C
1	Total: 1	Priority: 2	alert ICMP PING NMAP
2	Total: 4	Priority: 2	alert SNMP AgentX/tcp request
3	Total: 4	Priority: 2	alert SNMP request tcp
4	Total: 17	Priority: 3	alert ICMP PING



Pada Tampilan hasil Alert diatas terdapat 4 Alert, dari grafik yang tertinggi hingga grafik yang terendah. Grafik tertinggi yaitu pada alert *ICMP PING* dengan total alert 17 dan priority nya 3, sedangkan grafik yang terendah yaitu pada alert *ICMP PING NMAP* dengan total 1 dan priority nya 2.