

TUGAS KEAMANAN JARINGAN KOMPUTER
“IDS SNORT”



NAMA : AGUS JULAINSYAH

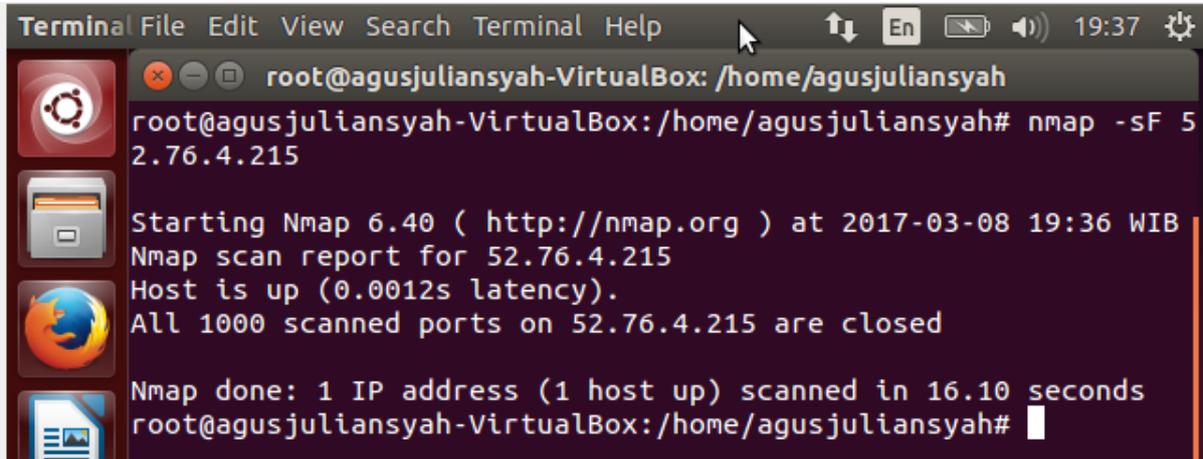
NIM :09011181320034

KELAS : SK8A

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

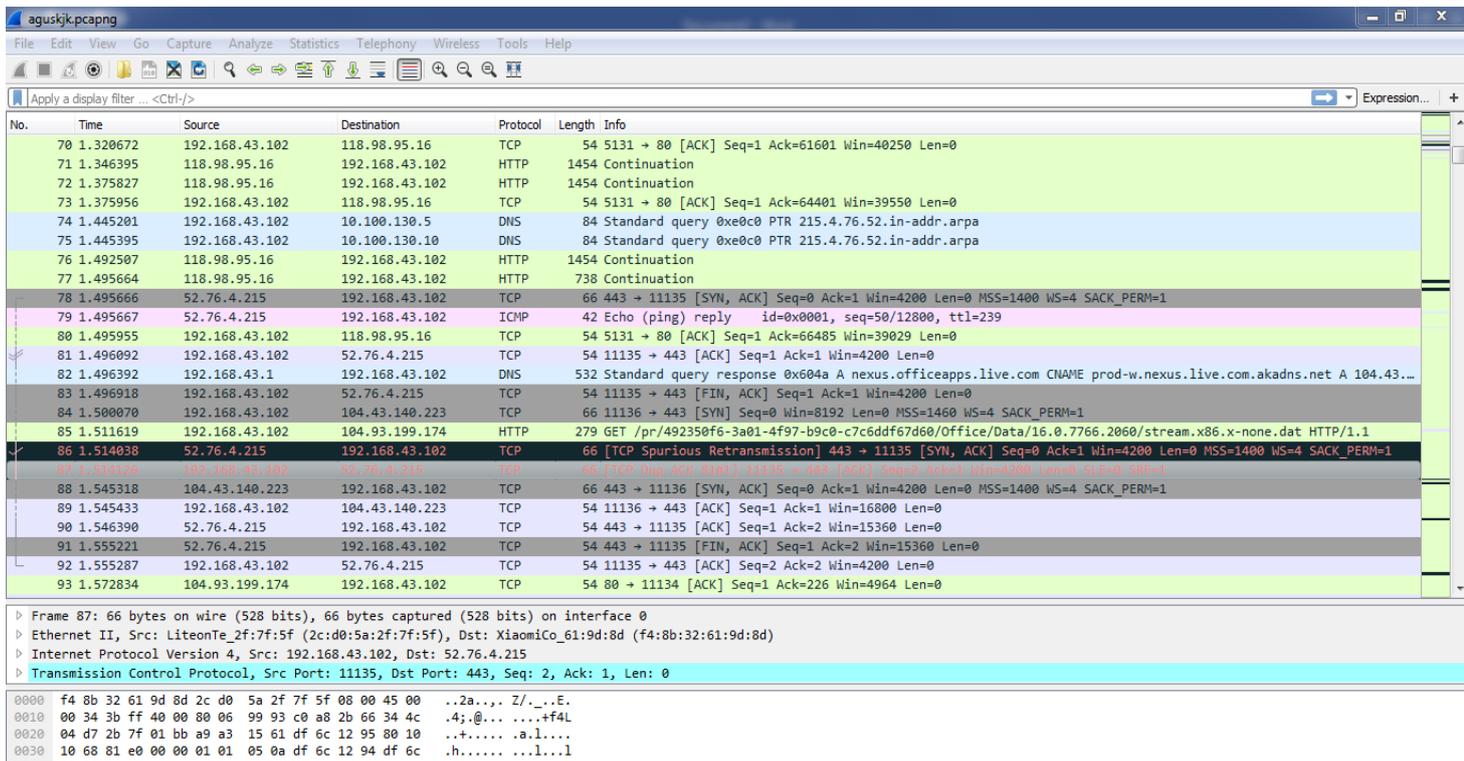
1. Domain (Target) : Vidio.com (52.76.4.215)

- Tampilan Scanning pada Nmap dan Wireshark :



```
Terminal File Edit View Search Terminal Help
root@agusjuliansyah-VirtualBox: /home/agusjuliansyah
root@agusjuliansyah-VirtualBox:/home/agusjuliansyah# nmap -sF 52.76.4.215

Starting Nmap 6.40 ( http://nmap.org ) at 2017-03-08 19:36 WIB
Nmap scan report for 52.76.4.215
Host is up (0.0012s latency).
All 1000 scanned ports on 52.76.4.215 are closed
Nmap done: 1 IP address (1 host up) scanned in 16.10 seconds
root@agusjuliansyah-VirtualBox:/home/agusjuliansyah#
```



No.	Time	Source	Destination	Protocol	Length	Info
70	1.320672	192.168.43.102	118.98.95.16	TCP	54	5131 → 80 [ACK] Seq=1 Ack=61601 Win=40250 Len=0
71	1.346395	118.98.95.16	192.168.43.102	HTTP	1454	Continuation
72	1.375827	118.98.95.16	192.168.43.102	HTTP	1454	Continuation
73	1.375956	192.168.43.102	118.98.95.16	TCP	54	5131 → 80 [ACK] Seq=1 Ack=64401 Win=39550 Len=0
74	1.445201	192.168.43.102	10.100.130.5	DNS	84	Standard query 0xe0c0 PTR 215.4.76.52.in-addr.arpa
75	1.445395	192.168.43.102	10.100.130.10	DNS	84	Standard query 0xe0c0 PTR 215.4.76.52.in-addr.arpa
76	1.492507	118.98.95.16	192.168.43.102	HTTP	1454	Continuation
77	1.495664	118.98.95.16	192.168.43.102	HTTP	738	Continuation
78	1.495666	52.76.4.215	192.168.43.102	TCP	66	443 → 11135 [SYN, ACK] Seq=0 Ack=1 Win=4200 Len=0 MSS=1400 WS=4 SACK_PERM=1
79	1.495672	52.76.4.215	192.168.43.102	ICMP	42	Echo (ping) reply id=0x0001, seq=50/12800, ttl=239
80	1.495955	192.168.43.102	118.98.95.16	TCP	54	5131 → 80 [ACK] Seq=1 Ack=66485 Win=39029 Len=0
81	1.496092	192.168.43.102	52.76.4.215	TCP	54	11135 → 443 [ACK] Seq=1 Ack=1 Win=4200 Len=0
82	1.496392	192.168.43.1	192.168.43.102	DNS	532	Standard query response 0x604a A nexus.officeapps.live.com CNAME prod-w.nexus.live.com.akadns.net A 104.43...
83	1.496918	192.168.43.102	52.76.4.215	TCP	54	11135 → 443 [FIN, ACK] Seq=1 Ack=1 Win=4200 Len=0
84	1.500070	192.168.43.102	104.43.140.223	TCP	66	11136 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1400 WS=4 SACK_PERM=1
85	1.511619	192.168.43.102	104.93.199.174	HTTP	279	GET /pr/492350f6-3a01-4f97-b9c0-c7c6ddf67d60/Office/Data/16.0.7766.2060/stream.x86.x-none.dat HTTP/1.1
86	1.514038	52.76.4.215	192.168.43.102	TCP	66	[TCP Spurious Retransmission] 443 → 11135 [SYN, ACK] Seq=0 Ack=1 Win=4200 Len=0 MSS=1400 WS=4 SACK_PERM=1
87	1.514106	192.168.43.102	52.76.4.215	TCP	66	[TCP Dup ACK (RSEQ)] 11135 → 443 [ACK] Seq=2 Ack=1 Win=4200 Len=0 MSS=1400 WS=4 SACK_PERM=1
88	1.545318	104.43.140.223	192.168.43.102	TCP	66	443 → 11136 [SYN, ACK] Seq=0 Ack=1 Win=4200 Len=0 MSS=1400 WS=4 SACK_PERM=1
89	1.545433	192.168.43.102	104.43.140.223	TCP	54	11136 → 443 [ACK] Seq=1 Ack=1 Win=16000 Len=0
90	1.546390	52.76.4.215	192.168.43.102	TCP	54	443 → 11135 [ACK] Seq=1 Ack=2 Win=15360 Len=0
91	1.555221	52.76.4.215	192.168.43.102	TCP	54	443 → 11135 [FIN, ACK] Seq=1 Ack=2 Win=15360 Len=0
92	1.555287	192.168.43.102	52.76.4.215	TCP	54	11135 → 443 [ACK] Seq=2 Ack=2 Win=4200 Len=0
93	1.572834	104.93.199.174	192.168.43.102	TCP	54	80 → 11134 [ACK] Seq=1 Ack=226 Win=4964 Len=0

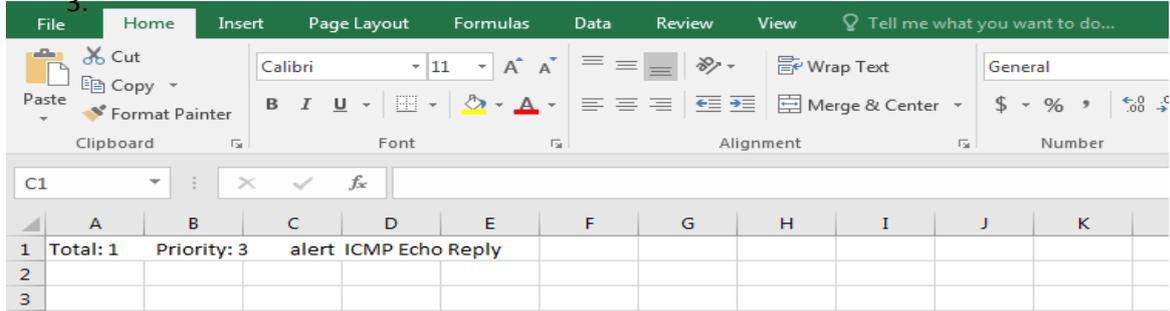
▶ Frame 87: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▶ Ethernet II, Src: LiteonTe_2f:7f:5f (2c:d0:5a:2f:7f:5f), Dst: XiaomiCo_61:9d:8d (f4:8b:32:61:9d:8d)
▶ Internet Protocol Version 4, Src: 192.168.43.102, Dst: 52.76.4.215
▶ Transmission Control Protocol, Src Port: 11135, Dst Port: 443, Seq: 2, 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 34 3b ff 40 00 80 06 99 93 c0 a8 2b 66 34 4c .4;.@... ..+f4L
0020 04 d7 2b 7f 01 bb a9 a3 15 61 df 6c 12 95 80 10 ..+..... a.l....
0030 10 68 81 e0 00 01 01 05 0a df 6c 12 94 df 6c .h..... ...l...
0040 ..
```

Tampilan pada gambar diatas dapat saya analisa bahwa langkah pertama kita harus membuka nmapnya terlebih dahulu atau dengan membuka nmap menggunakan Ubuntu 14.04 ataupun dengan linux , lalu selanjutnya saya memasukan IP atau domain target yang telah di tuju dengan cara melakukan perintah seperti berikut : nmap -sF lalu masukan domain atau IP target misalnya saya di atas memasukan IP 52.76.4.215 sesuai target yang telah saya tuju pada tugas kemarin , lalu lihat tampilan pada wireshark apakah IP target yang sudah saya scanning itu akan muncul, dan terlihat IP dengan 52.76.4.215 yang saya scanning ternyata muncul maka hasil scanningnya berhasil lalu saya stop wiresharknya saya stop untuk di save as dan melakukan langkah berikutnya yaitu mengambil data alert snort.

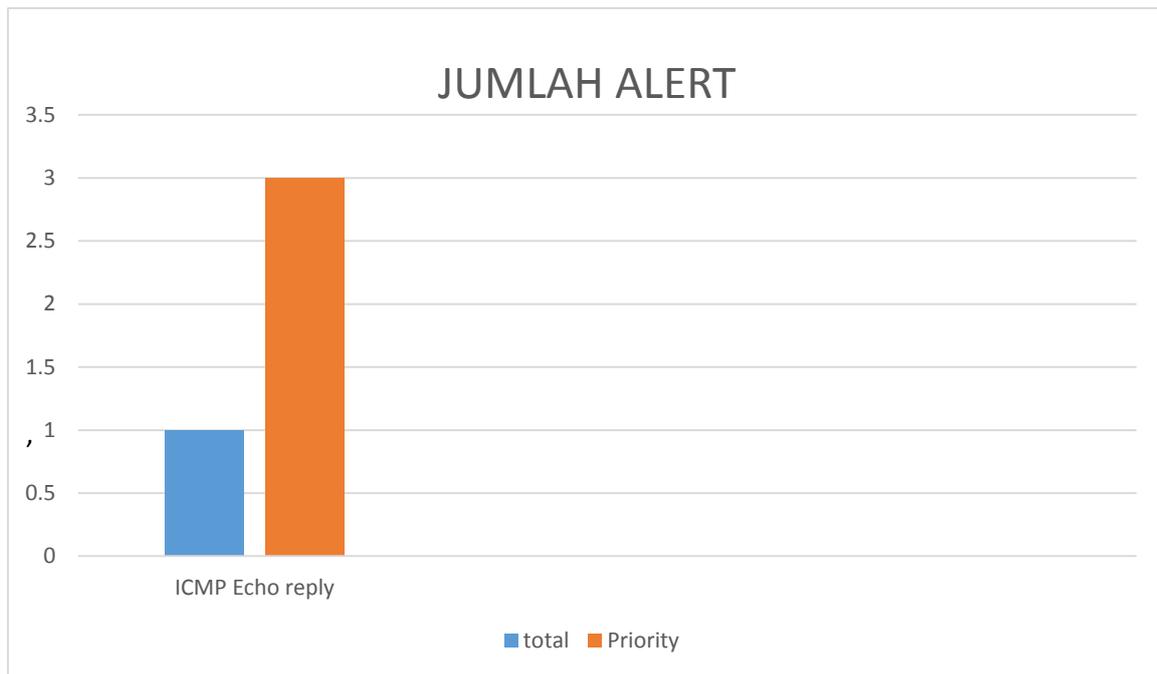
2. Hasil Alert menggunakan snort:

3.



The screenshot shows the Microsoft Excel interface with the following data in the table:

	A	B	C	D	E	F	G	H	I	J	K
1	Total: 1	Priority: 3	alert ICMP Echo Reply								
2											
3											



Tampilan pada gambar di atas menunjukkan bahwa hasil ekstrakan dari scanning menggunakan nmap dan wireshark secara bersama yang telah saya lakukan pada langkah pertama tadi, lalu langkah berikut melakukan ekstrakan tersebut dengan menggunakan snort untuk mendapatkan data alertnya, data yang saya dapat dari IP target yaitu 52.76.4.215 hanya 1 data alert yaitu ICMP Echo reply yang total di tunjukan pada warna biru hanya 1 dan prioritynya yang di tunjukan oleh warna orange hanya 3 jumlahnya , itu hasil scanning saya dari langkah pertama sampai langkah kedua.