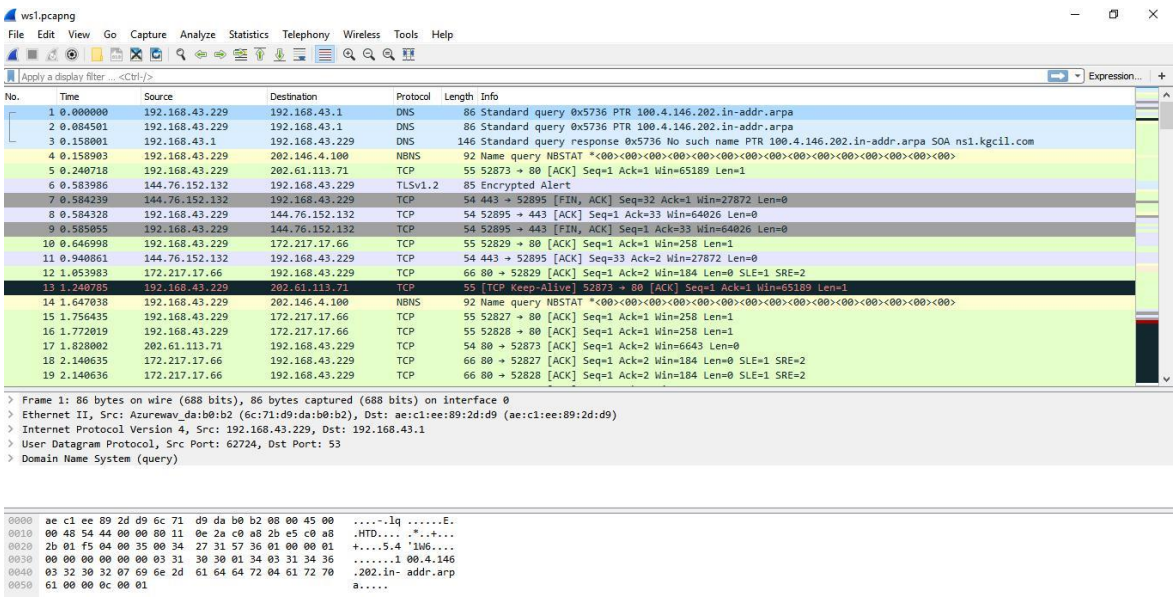
Nama : Rizky Soufi Gustiawan

NIM : 09011281520111
Kelas : SK 5C

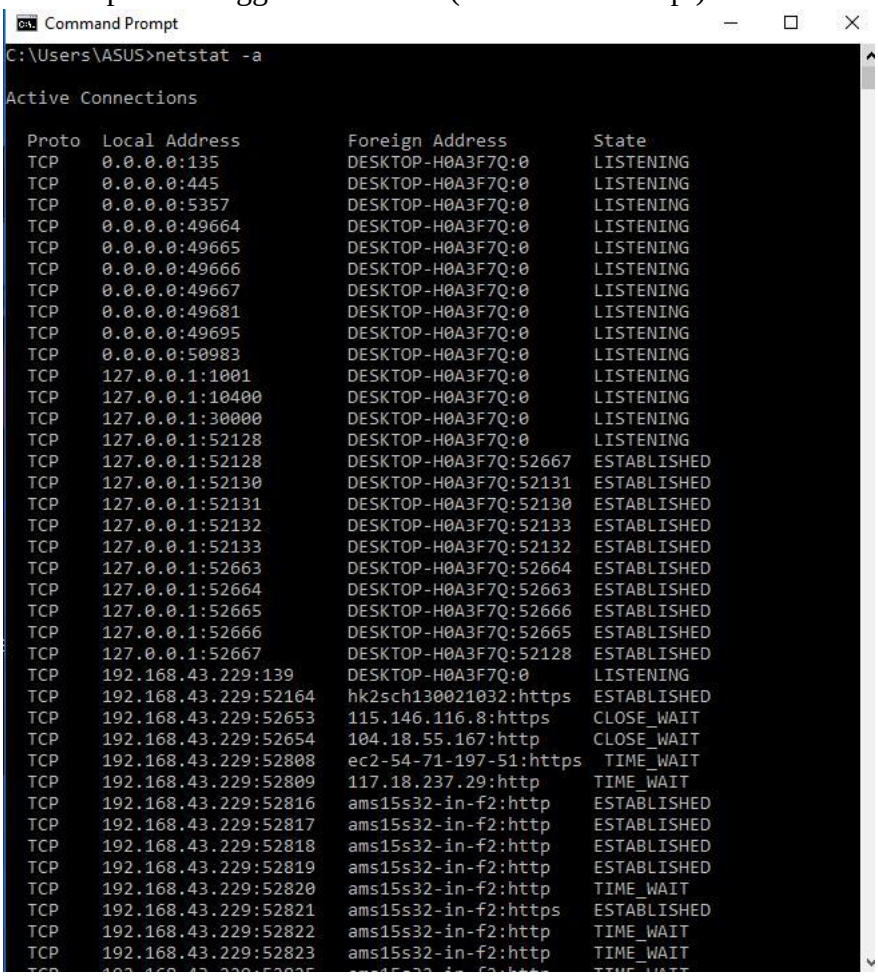
Tugas Jarkom

- Capture data dari www.kompas.com Hasil

  capture data menggunakan Wireshark



Hasil capture menggunakan CMD (Command Prompt)



Source :

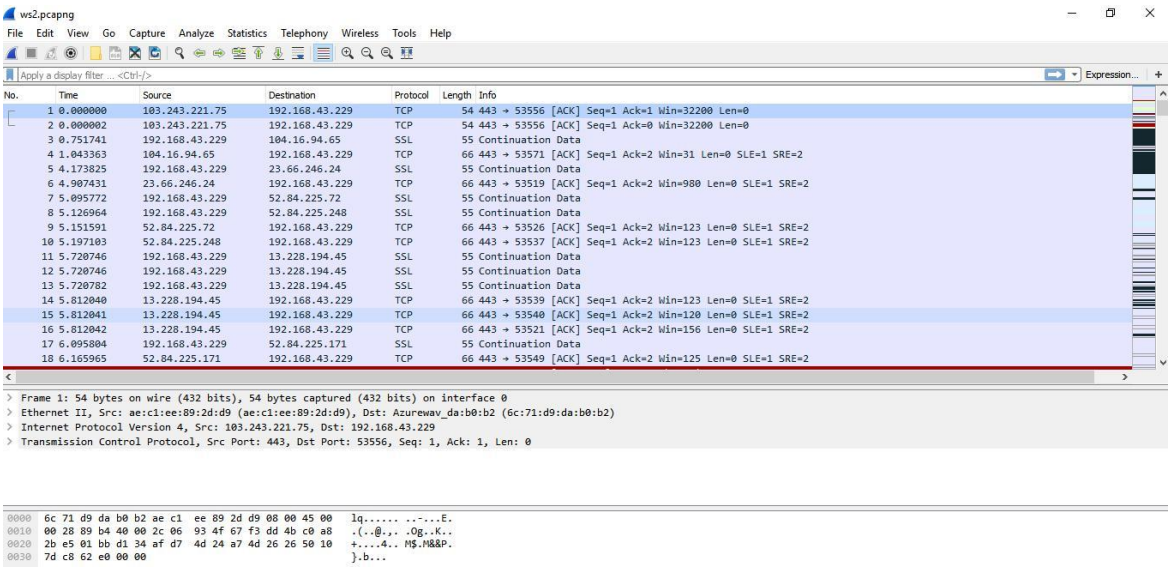
IP	Info
192.168.43.229	Standard query 0x5736 PTR 100.4.146.202.in-addr.arpa
192.168.43.1	Standard query response 0x5736 No such name PTR 100.4.146.202.in-addr.arpa SOA ns1.kgcil.com
144.76.152.132	Encrypted Alert
172.217.17.66	80 → 52829 [ACK] Seq=1 Ack=2 Win=184 Len=0 SLE=1 SRE=2
202.61.113.71	80 → 52873 [ACK] Seq=1 Ack=2 Win=6643 Len=0

Destination :

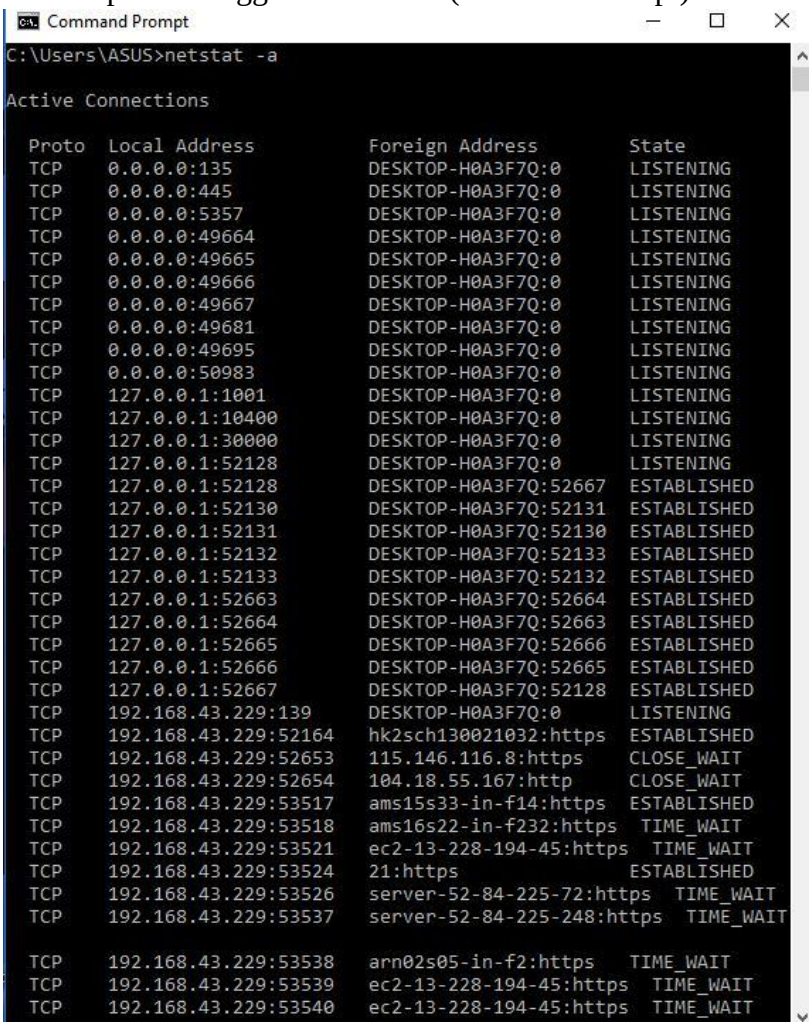
IP	Info
192.168.43.1	Standard query 0x5736 PTR 100.4.146.202.in-addr.arpa
192.168.43.229	Standard query response 0x5736 No such name PTR 100.4.146.202.in-addr.arpa SOA ns1.kgcil.com
202.61.113.71	52873 → 80 [ACK] Seq=1 Ack=1 Win=65189 Len=1
144.76.152.132	52895 → 443 [ACK] Seq=1 Ack=33 Win=64026 Len=0
172.217.17.66	52829 → 80 [ACK] Seq=1 Ack=1 Win=258 Len=1

- Capture data dari www.vidio.com

Hasil capture dengan Wireshark



Hasil capture menggunakan CMD (Commad Prompt)



Source :

IP	Info
103.243.221.75	443 → 53556 [ACK] Seq=1 Ack=1 Win=32200 Len=0
192.168.43.229	[TCP segment of a reassembled PDU]
104.16.94.65	443 → 53571 [ACK] Seq=1 Ack=2 Win=31 Len=0 SLE=1 SRE=2
23.66.246.24	443 → 53519 [ACK] Seq=1 Ack=2 Win=980 Len=0 SLE=1 SRE=2
52.84.225.72	443 → 53526 [ACK] Seq=1 Ack=2 Win=123 Len=0 SLE=1 SRE=2
52.84.225.248	443 → 53537 [ACK] Seq=1 Ack=2 Win=123 Len=0 SLE=1 SRE=2
13.228.194.45	443 → 53539 [ACK] Seq=1 Ack=2 Win=123 Len=0 SLE=1 SRE=2
52.84.225.171	443 → 53549 [ACK] Seq=1 Ack=2 Win=125 Len=0 SLE=1 SRE=2
38.72.130.155	443 → 53560 [RST, ACK] Seq=1 Ack=1 Win=25617 Len=0

Destination :

IP	Info
192.168.43.229	443 → 53556 [ACK] Seq=1 Ack=1 Win=32200 Len=0
104.16.94.65	[TCP segment of a reassembled PDU]
23.66.246.24	[TCP segment of a reassembled PDU]
52.84.225.72	[TCP segment of a reassembled PDU]
52.84.225.248	Continuation Data
13.228.194.45	[TCP segment of a reassembled PDU]
52.84.225.171	[TCP segment of a reassembled PDU]
23.41.75.27	53562 → 80 [ACK] Seq=1 Ack=1 Win=257 Len=1

- Perbedaan Capture Data menggunakan Wireshark dan Cmd;

  Analisis paket data dengan menggunakan Wireshark lebih lengkap dan terinci dibandingkan dengan menggunakan Cmd, selain itu juga Cmd hanya dapat membaca protocol TCP sedangkan pada Wireshark dapat membaca berbagai jenis protocol sehingga banyak data yang muncul, termasuk berbagai jenis data error yang terjadi saat pembacaan data.

- Capture Filters