

Nama : Ratih Filaresy
 Kelas : SI 4A
 NIM : 09031281520099
 Mata Kuliah : Komunikasi Data dan Jaringan Komputer
 Dosen Pembimbing : Deris Stiawan, Ph.D

Analisa Paket Data Menggunakan Wireshark

Aplikasi wireshark digunakan untuk menganalisa jaringan. Wireshark bisa digunakan untuk menangkap paket-paket data yang berlalu lalang. Situs web yang saya analisa diantaranya adalah dari situs web indonesia yaitu kaskus.co.id, dari situs web luar negeri subscane.com, dari media social nya ask.fm dan stacoverflow.com. Berikut ini adalah analisisnya.

Kaskus.co.id

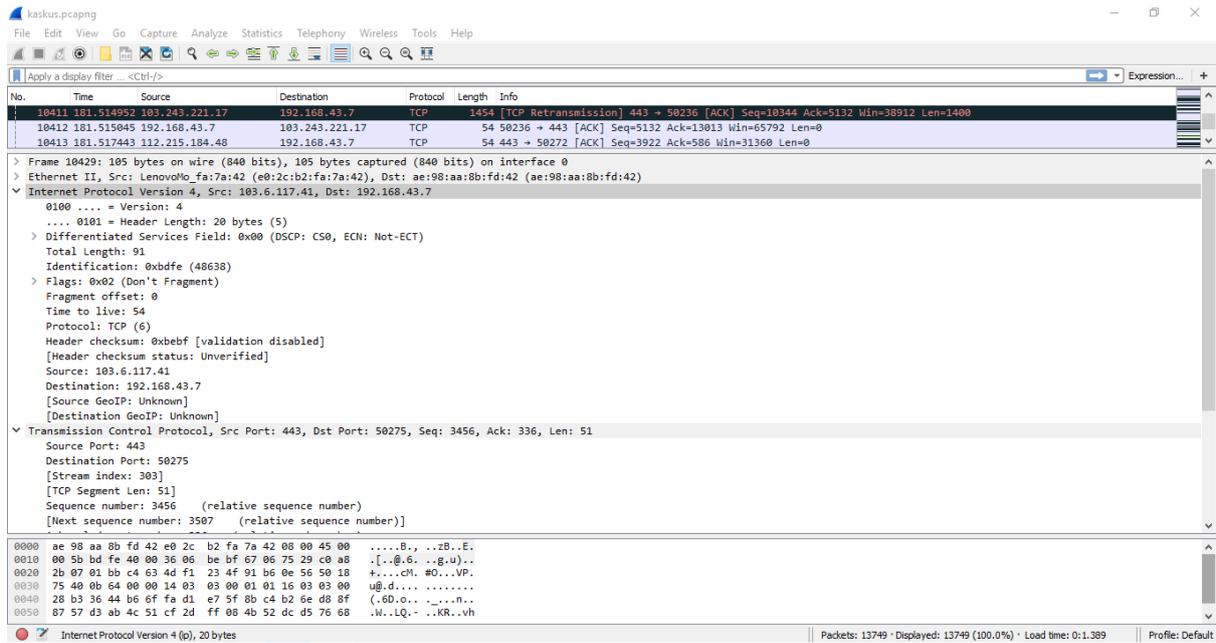
The screenshot shows the Wireshark interface with a list of network packets. Packet 10411 is highlighted in green. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
10411	181.514952	103.243.221.17	192.168.43.7	TCP	1454	[TCP Retransmission] 443 → 50236 [ACK] Seq=10344 Ack=5132 Win=38912 Len=1480
10412	181.515045	192.168.43.7	103.243.221.17	TCP	54	50236 → 443 [ACK] Seq=5132 Ack=13013 Win=65792 Len=0
10413	181.517443	112.215.184.48	192.168.43.7	TCP	54	443 → 50272 [ACK] Seq=3922 Ack=586 Win=31360 Len=0
10414	181.517445	112.215.184.48	192.168.43.7	TCP	54	443 → 50272 [ACK] Seq=3922 Ack=1725 Win=34048 Len=0
10415	181.517446	23.59.139.27	192.168.43.7	TCP	54	80 → 50219 [FIN, ACK] Seq=1965 Ack=234 Win=30272 Len=0
10416	181.517616	192.168.43.7	112.215.184.48	TCP	503	[TCP Retransmission] 50272 → 443 [PSH, ACK] Seq=1725 Ack=3922 Win=65792 Len=449
10417	181.517680	192.168.43.7	23.59.139.27	TCP	54	50219 → 80 [ACK] Seq=234 Ack=1966 Win=65792 Len=0
10418	181.518011	192.168.43.7	23.59.139.27	TCP	54	50219 → 80 [FIN, ACK] Seq=234 Ack=1966 Win=65792 Len=0
10419	181.520889	112.215.184.48	192.168.43.7	TLSv1.2	784	[TCP Previous segment not captured] Application Data, Application Data
10420	181.520464	192.168.43.7	112.215.184.48	TCP	66	[TCP Dup ACK 10283#1] 50272 → 443 [ACK] Seq=2174 Ack=3922 Win=65792 Len=0 SLE=4320 SRE=5050
10421	181.523475	112.215.184.48	192.168.43.7	TLSv1.2	92	Application Data
10422	181.523477	112.215.184.48	192.168.43.7	TLSv1.2	247	Application Data, Application Data
10423	181.523478	112.215.184.48	192.168.43.7	TLSv1.2	162	Application Data, Application Data
10424	181.523549	192.168.43.7	112.215.184.48	TCP	66	[TCP Dup ACK 10283#2] 50272 → 443 [ACK] Seq=2174 Ack=3922 Win=65792 Len=0 SLE=4320 SRE=5088
10425	181.523611	192.168.43.7	112.215.184.48	TCP	66	[TCP Dup ACK 10283#3] 50272 → 443 [ACK] Seq=2174 Ack=3922 Win=65792 Len=0 SLE=4320 SRE=5281
10426	181.523648	192.168.43.7	112.215.184.48	TCP	66	[TCP Dup ACK 10283#4] 50272 → 443 [ACK] Seq=2174 Ack=3922 Win=65792 Len=0 SLE=4320 SRE=5389
10427	181.547479	103.50.216.10	192.168.43.7	TLSv1.2	1454	Ignored Unknown Record
10428	181.547482	52.74.72.167	192.168.43.7	TCP	54	[TCP Previous segment not captured] 443 → 50254 [FIN, ACK] Seq=3037 Ack=336 Win=28160 Len=0
10429	181.547482	103.6.117.41	192.168.43.7	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
10430	181.547483	103.6.117.41	192.168.43.7	TLSv1.2	123	Application Data
10431	181.547550	192.168.43.7	103.50.216.10	TCP	68	[TCP Dup ACK 10287#1] 50180 → 443 [ACK] Seq=6244 Ack=21280 Win=64480 Len=0 SLE=215102 SRE=216502
10432	181.547637	192.168.43.7	52.74.72.167	TCP	54	[TCP Dup ACK 10082#1] 50254 → 443 [ACK] Seq=336 Ack=3006 Win=65536 Len=0
10433	181.547764	192.168.43.7	103.6.117.41	TCP	54	50275 → 443 [ACK] Seq=336 Ack=3576 Win=63625 Len=0
10434	181.583487	103.6.117.46	192.168.43.7	TCP	1454	[TCP segment of a reassembled PDU]

The detailed view for packet 10411 shows:

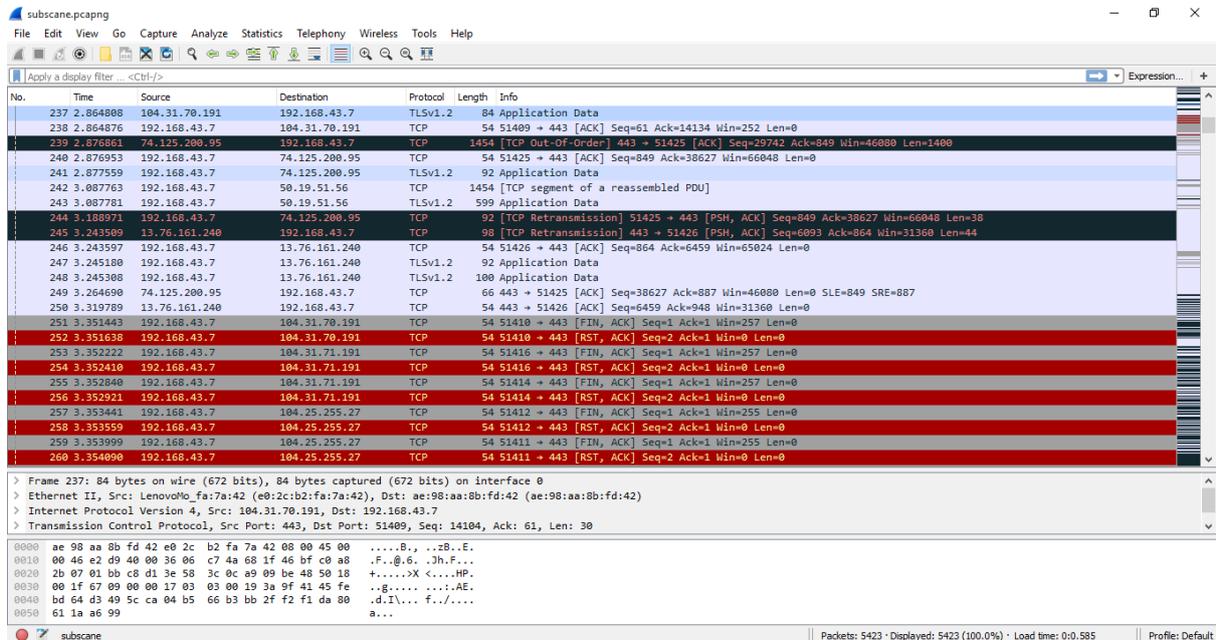
- Frame 10429: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface 0
- Ethernet II, Src: LenovoNo_fa:7a:42 (e8:2c:b2:fa:7a:42), Dst: ae:98:aa:8b:fd:42 (ae:98:aa:8b:fd:42)
- Internet Protocol Version 4, Src: 103.6.117.41, Dst: 192.168.43.7
- TCP, Src Port: 443, Dst Port: 50236, Seq: 10344, Len: 1480
- Application Data (1480 bytes)

Pada nomor **10411** pada source nya 103.243.221.17 , destination nya 192.168.43.7 pada protokolnya TCP dan legth nya 1454. Kembali lagi lagi pada no **10412** sourenya berubah menjadi 192.168.43.7 dan destinationnya 103.243.221.17.

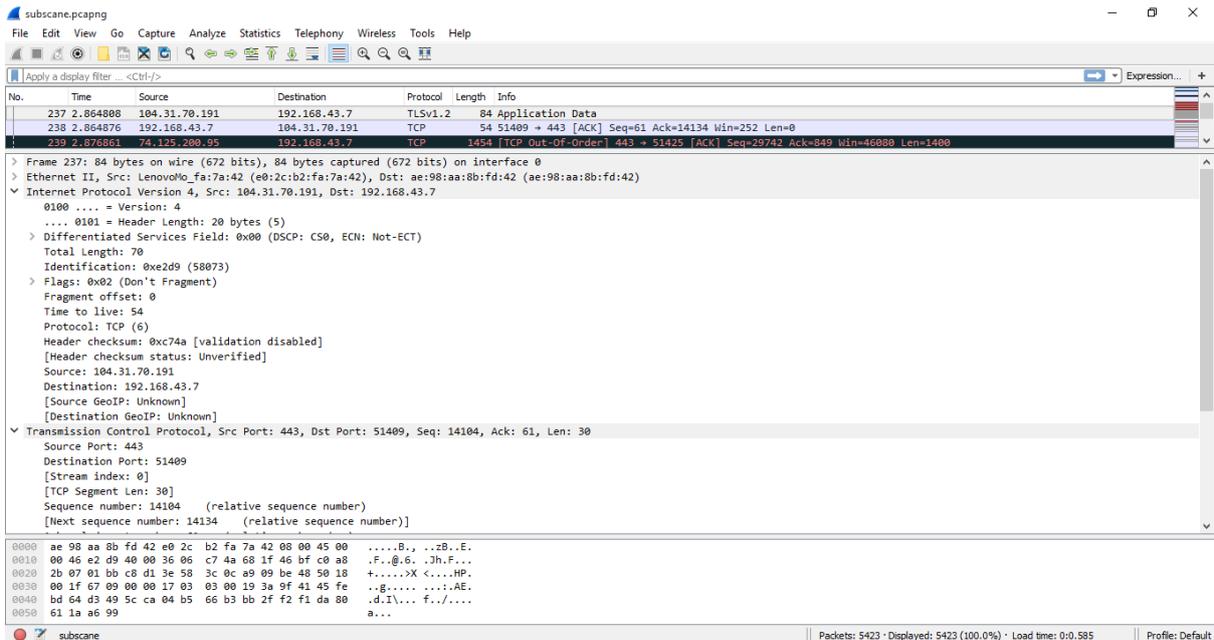


Pada gambar di atas, menunjukan bahwa ip address pada laptop yang saya gunakan adalah **192.168.43.7** yang ditunjukan pada bagian di internet protocol version di sourceny, dan terdapat ip address saat di source yaitu **103.6.117.41** ini adalah ip address dari kaskus.co.id . Bisa dilihat pada gambar di atas pada bagian ethernet II source memiliki mac address yaitu **e0:2c:b2:fa:7a:42** dan di bagian destination terdapat juga mac address yaitu **ae:98:aa:8b:fd:42**. Selanjutnya pada bagian di internet protocol version, hasil dari header length yaitu **20** bytes, source port **443** dan destination **50275**. Pada bagian transmission control protocol Sequence number yaitu **3456** dan next sequence number yaitu **3507**.

Subscane.com

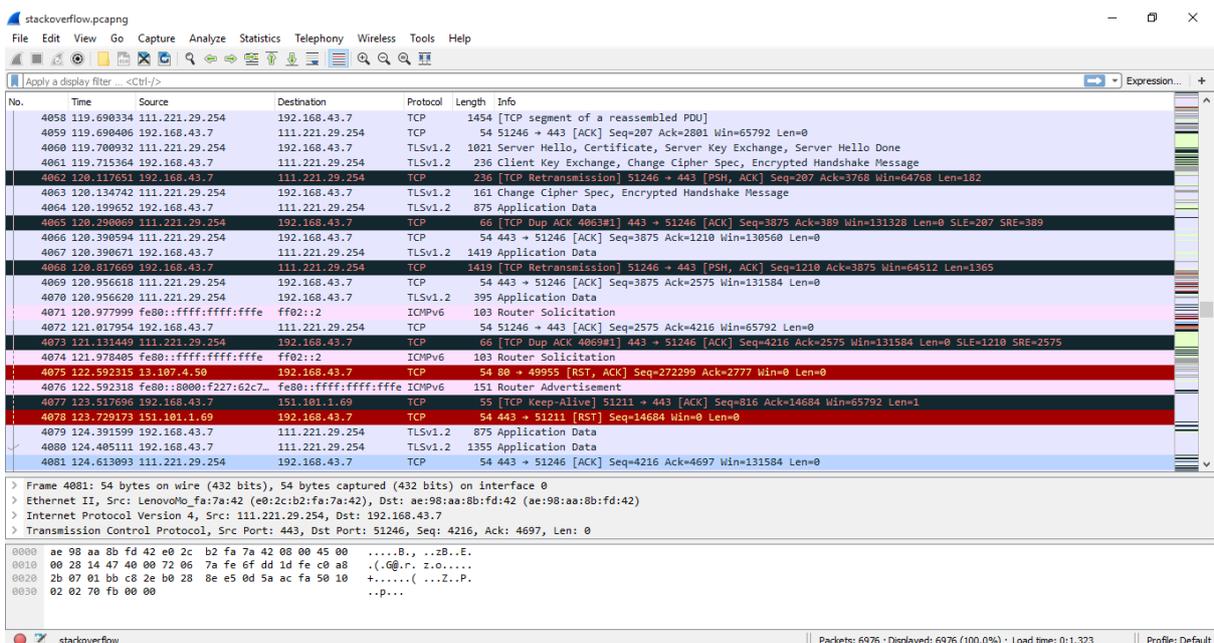


Pada nomor **237** pada source nya **104.31.70.191**, destination nya **192.168.43.7** pada protokolnya TCP. Kembali lagi lagi pada no **238** sourenya berubah menjadi **192.168.43.7** dan destinationnya **104.31.70.191**.

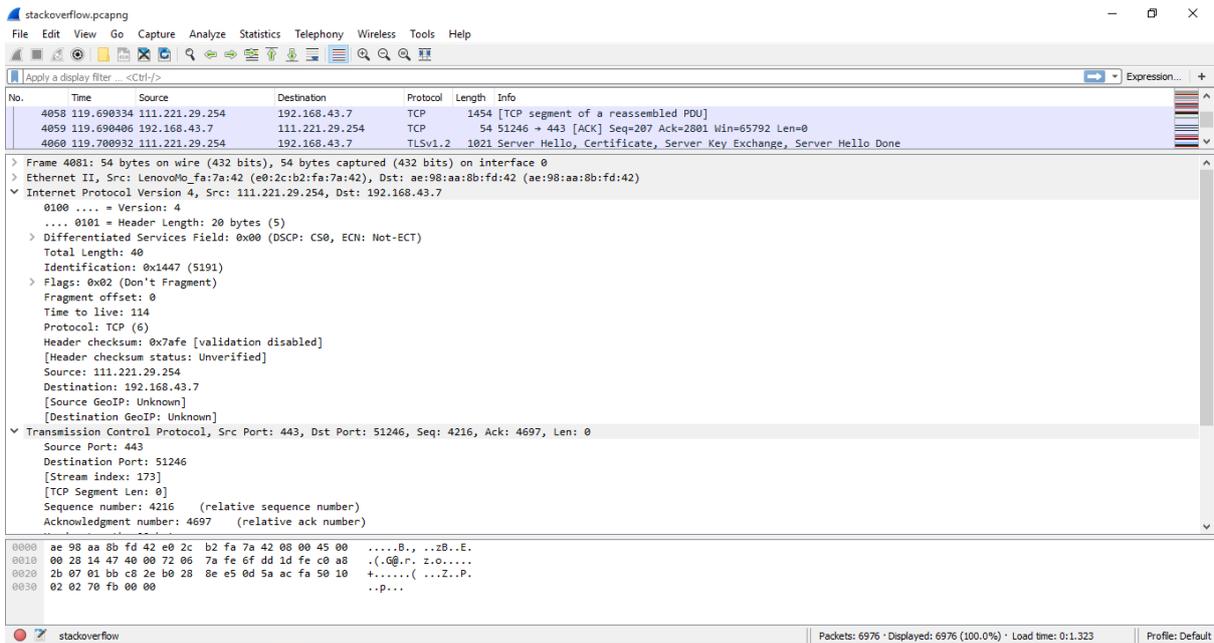


Pada gambar di atas, menunjukan bahwa ip address pada laptop yang saya gunakan adalah **192.168.43.7** yang ditunjukkan pada bagian di internet protocol version di sourceny, dan terdapat ip address saat di source yaitu **104.31.70.191** ini adalah ip address dari subscane.com . Bisa dilihat pada gambar di atas pada bagian ethernet II source memiliki mac address yaitu **e0:2c:b2:fa:7a:42** dan di bagian destination terdapat juga mac address yaitu **ae:98:aa:8b:fd:42**. Selanjutnya pada bagian di internet protocol version, hasil dari header length yaitu **20** bytes, source port **443** dan destination **51409**. Pada bagian transmission control protocol Sequence number yaitu **14104** dan next sequence number yaitu **14134**.

Stackoverflow.com

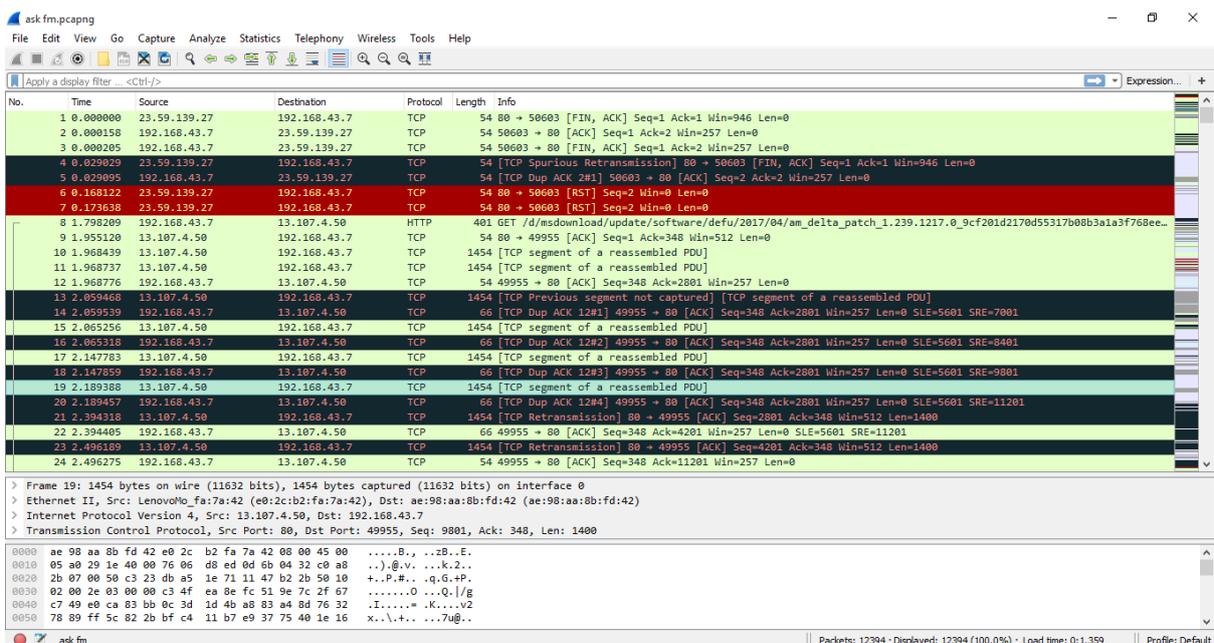


Pada nomor **4058** pada source nya 111.221.29.254 , destination nya 192.168.43.7 pada protokolnya TCP. Kembali lagi lagi pada no **4059** sourenya berubah menjadi 192.168.43.7 dan destinationnya 111.221.29.254.

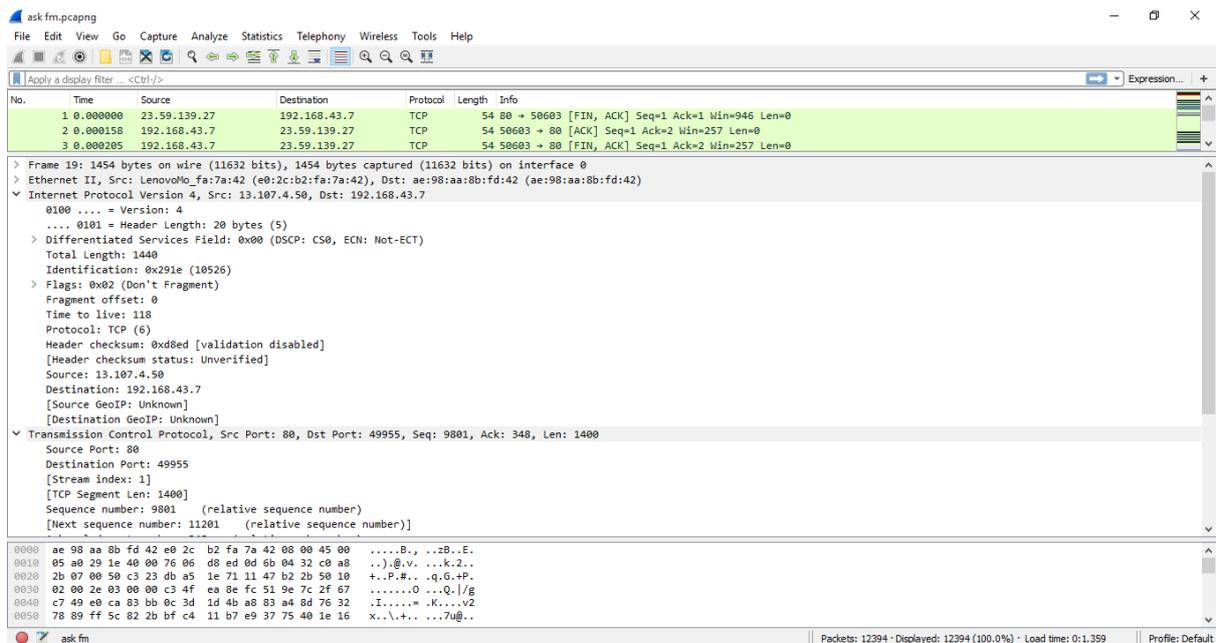


Pada gambar di atas, menunjukan bahwa ip address pada laptop yang saya gunakan adalah **192.168.43.7** yang ditunjukkan pada bagian di internet protocol version di sourcenya, dan terdapat ip address saat di source yaitu **111.221.29.254** ini adalah ip address dari stackoverflow.com. Bisa dilihat pada gambar di atas pada bagian ethernet II source memiliki mac address yaitu **e0:2c:b2:fa:7a:42** milik pc dan di bagian destination terdapat juga mac address yaitu **ae:98:aa:8b:fd:42** milik stackoverflow.com. Selanjutnya pada bagian di internet protocol version, hasil dari header length yaitu **20** bytes, source port **443** dan destination **51246**. Pada bagian transmission control protocol Sequence number yaitu **4216** dan acknowledgment number yaitu **4697**.

Ask.fm



Pada nomor **1** pada source nya **23.59.139.27**, destination nya **192.168.43.7** pada protokolnya **TCP**. Kembali lagi lagi pada no **2** sourenya berubah menjadi **192.168.43.7** dan destinationnya **23.59.139.27**.



Pada gambar di atas, menunjukan bahwa ip address pada laptop yang saya gunakan adalah **192.168.43.7** yang ditunjukan pada bagian di internet protocol version di sourcenya, dan terdapat ip address saat di source yaitu **13.107.4.50** ini adalah ip address dari ask.fm . Bisa dilihat pada gambar di atas pada bagian ethernet II source memiliki mac address yaitu **e0:2c:b2:fa:7a:42** dan di bagian destination terdapat juga mac address yaitu **ae:98:aa:8b:fd:42**. Selanjutnya pada bagian di internet protocol version, hasil dari header length yaitu **20** bytes, source port **80** dan destination **49955**. Pada bagian transmission control protocol Sequence number yaitu **9801** dan next sequence number yaitu **11201**.