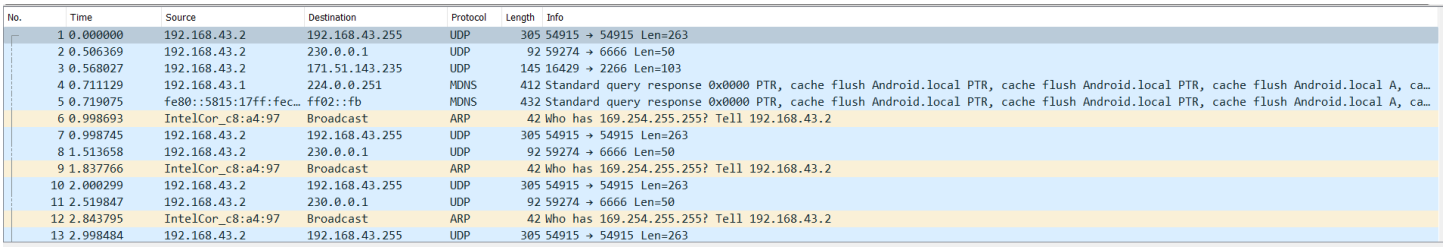
Name: Manav Doda

Roll No.: 195057

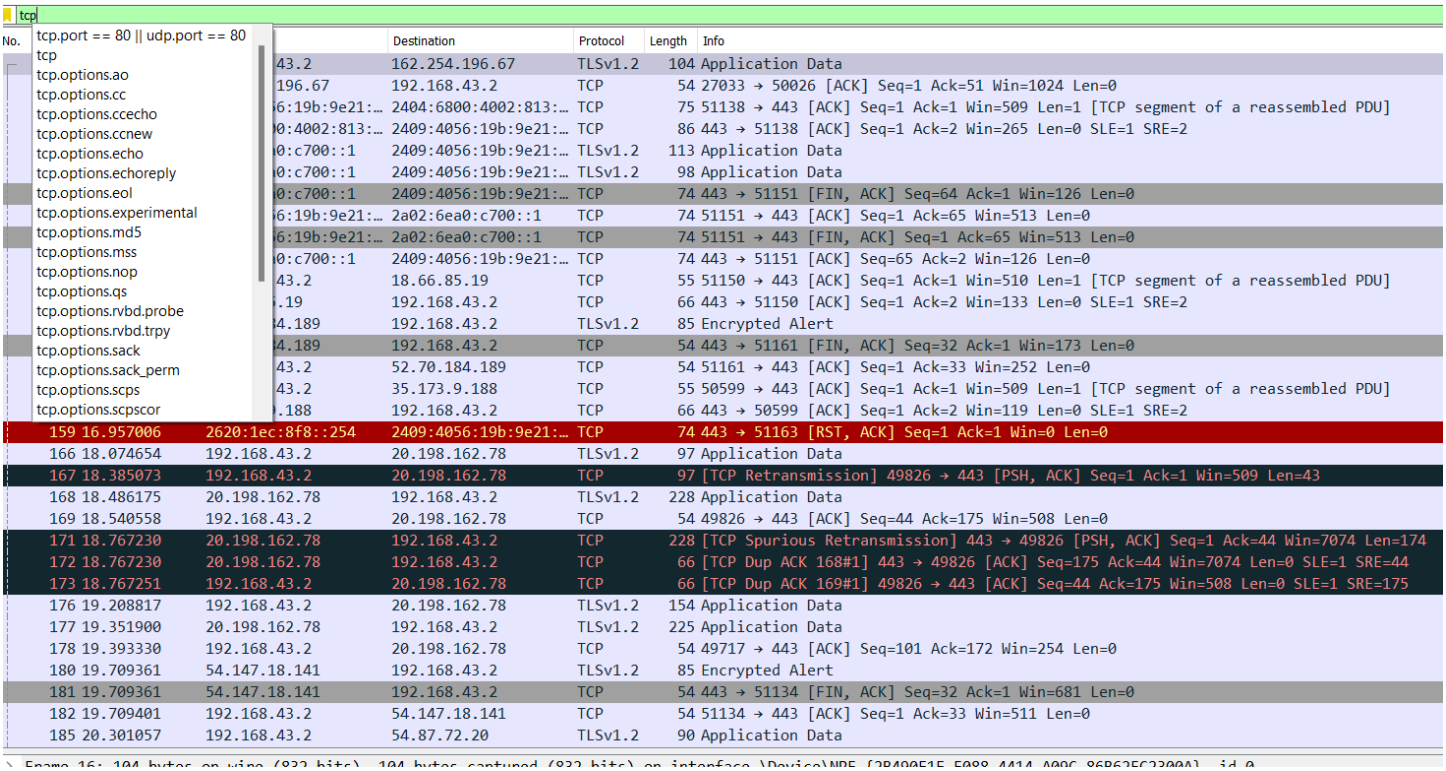
Computer Networks Lab 7

Install Ethereal on a computer. Set Ethereal to capture with a filter option of your choice. Load a webpage or send an email to a friend and stop capturing. Analyze the packets. See if you can read any or all of the data transmitted. Write down your findings.

We use wireshark:



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.43.2	192.168.43.255	UDP	305	54915 → 54915 Len=263
2	0.506369	192.168.43.2	230.0.0.1	UDP	92	59274 → 6666 Len=50
3	0.568027	192.168.43.2	171.51.143.235	UDP	145	16429 → 2266 Len=103
4	0.711129	192.168.43.1	224.0.0.251	MDNS	412	Standard query response 0x0000 PTR, cache flush Android.local PTR, cache flush Android.local PTR, cache flush Android.local A, ca…
5	0.719075	fe80::5815:17ff:fec…	ff02::fb	MDNS	432	Standard query response 0x0000 PTR, cache flush Android.local PTR, cache flush Android.local PTR, cache flush Android.local A, ca…
6	0.998693	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
7	0.998745	192.168.43.2	192.168.43.255	UDP	305	54915 → 54915 Len=263
8	1.513658	192.168.43.2	230.0.0.1	UDP	92	59274 → 6666 Len=50
9	1.837766	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
10	2.000299	192.168.43.2	192.168.43.255	UDP	305	54915 → 54915 Len=263
11	2.519847	192.168.43.2	230.0.0.1	UDP	92	59274 → 6666 Len=50
12	2.843795	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
13	2.998484	192.168.43.2	192.168.43.255	UDP	305	54915 → 54915 Len=263



tcp

tcp.port == 80 || udp.port == 80
tcp
tcp.options.ao
tcp.options.cc
tcp.options.ccecho
tcp.options.ccnew
tcp.options.echo
tcp.options.echoreply
tcp.options.eol
tcp.options.experimental
tcp.options.md5
tcp.options.mss
tcp.options.nop
tcp.options.qs
tcp.options.rvbd.probe
tcp.options.rvbd.trpy
tcp.options.sack
tcp.options.sack_perm
tcp.options.scps
tcp.options.scpscor

No.			Destination	Protocol	Length	Info
		43.2	162.254.196.67	TLSv1.2	104	Application Data
		196.67	192.168.43.2	TCP	54	27033 → 50026 [ACK] Seq=1 Ack=51 Win=1024 Len=0
		6:19b:9e21:…	2404:6800:4002:813:…	TCP	75	51138 → 443 [ACK] Seq=1 Ack=1 Win=509 Len=1 [TCP segment of a reassembled PDU]
		0:4002:813:…	2409:4056:19b:9e21:…	TCP	86	443 → 51138 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
		0:c700::1	2409:4056:19b:9e21:…	TLSv1.2	113	Application Data
		0:c700::1	2409:4056:19b:9e21:…	TLSv1.2	98	Application Data
		0:c700::1	2409:4056:19b:9e21:…	TCP	74	443 → 51151 [FIN, ACK] Seq=64 Ack=1 Win=126 Len=0
		6:19b:9e21:…	2a02:6ea0:c700::1	TCP	74	51151 → 443 [ACK] Seq=1 Ack=65 Win=513 Len=0
		6:19b:9e21:…	2a02:6ea0:c700::1	TCP	74	51151 → 443 [FIN, ACK] Seq=1 Ack=65 Win=513 Len=0
		0:c700::1	2409:4056:19b:9e21:…	TCP	74	443 → 51151 [ACK] Seq=65 Ack=2 Win=126 Len=0
		43.2	18.66.85.19	TCP	55	51150 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]
		.19	192.168.43.2	TCP	66	443 → 51150 [ACK] Seq=1 Ack=2 Win=133 Len=0 SLE=1 SRE=2
		4.189	192.168.43.2	TLSv1.2	85	Encrypted Alert
		4.189	192.168.43.2	TCP	54	443 → 51161 [FIN, ACK] Seq=32 Ack=1 Win=173 Len=0
		43.2	52.70.184.189	TCP	54	51161 → 443 [ACK] Seq=1 Ack=33 Win=252 Len=0
		43.2	35.173.9.188	TCP	55	50599 → 443 [ACK] Seq=1 Ack=1 Win=509 Len=1 [TCP segment of a reassembled PDU]
		.188	192.168.43.2	TCP	66	443 → 50599 [ACK] Seq=1 Ack=2 Win=119 Len=0 SLE=1 SRE=2
159	16.957006	2620:1ec:8f8::254	2409:4056:19b:9e21:…	TCP	74	443 → 51163 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
166	18.074654	192.168.43.2	20.198.162.78	TLSv1.2	97	Application Data
167	18.385073	192.168.43.2	20.198.162.78	TCP	97	[TCP Retransmission] 49826 → 443 [PSH, ACK] Seq=1 Ack=1 Win=509 Len=43
168	18.486175	20.198.162.78	192.168.43.2	TLSv1.2	228	Application Data
169	18.540558	192.168.43.2	20.198.162.78	TCP	54	49826 → 443 [ACK] Seq=44 Ack=175 Win=508 Len=0
171	18.767230	20.198.162.78	192.168.43.2	TCP	228	[TCP Spurious Retransmission] 443 → 49826 [PSH, ACK] Seq=1 Ack=44 Win=7074 Len=174
172	18.767230	20.198.162.78	192.168.43.2	TCP	66	[TCP Dup ACK 168#1] 443 → 49826 [ACK] Seq=175 Ack=44 Win=7074 Len=0 SLE=1 SRE=44
173	18.767251	192.168.43.2	20.198.162.78	TCP	66	[TCP Dup ACK 169#1] 49826 → 443 [ACK] Seq=44 Ack=175 Win=508 Len=0 SLE=1 SRE=175
176	19.208817	192.168.43.2	20.198.162.78	TLSv1.2	154	Application Data
177	19.351900	20.198.162.78	192.168.43.2	TLSv1.2	225	Application Data
178	19.393330	192.168.43.2	20.198.162.78	TCP	54	49717 → 443 [ACK] Seq=101 Ack=172 Win=254 Len=0
180	19.709361	54.147.18.141	192.168.43.2	TLSv1.2	85	Encrypted Alert
181	19.709361	54.147.18.141	192.168.43.2	TCP	54	443 → 51134 [FIN, ACK] Seq=32 Ack=1 Win=681 Len=0
182	19.709401	192.168.43.2	54.147.18.141	TCP	54	51134 → 443 [ACK] Seq=1 Ack=33 Win=511 Len=0
185	20.301057	192.168.43.2	54.87.72.20	TLSv1.2	90	Application Data

> Frame 16: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface \Device\NPF_{2B400F15-F088-4414-A00C-86B62FC2300A}, id 0

http

No.	Time	Source	Destination	Protocol	Length	Info
	930278	192.168.43.2	45.113.119.130	HTTP	208	GET /control/feature/tags/ut.json HTTP/1.1
	014998	45.113.119.130	192.168.43.2	HTTP/J…	708	HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
1084	58.130116	192.168.43.2	45.113.119.1	HTTP	276	GET /helper_ui/helper_web_ui.btinstall HTTP/1.1
1086	58.212271	45.113.119.1	192.168.43.2	HTTP	227	HTTP/1.1 304 Not Modified
1098	58.587775	192.168.43.2	45.113.119.1	HTTP	224	GET /control/tags/ut.json HTTP/1.1
1118	58.670864	45.113.119.1	192.168.43.2	HTTP/J…	945	HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
1572	69.562494	192.168.43.147	192.168.43.2	HTTP	140	GET / HTTP/1.1
1573	69.562840	192.168.43.2	192.168.43.147	HTTP	162	HTTP/1.1 400 ERROR (text/html)
7545	85.777914	192.168.43.2	117.18.237.29	HTTP	294	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTPJvUY%2Bs1%2Bj4yzQuAcL2oQno5fCgQUUWj%2FkK8CB3U8zNllZGKiErhZcjsCEA%2F6bQK5DKEZnVbQQLO8AOY%3D
7554	85.921333	117.18.237.29	192.168.43.2	OCSP	852	Response
9559	122.968930	2409:4056:19b:9e21:…	2600:140f:d800:2a3:…	HTTP	301	GET / HTTP/1.1
9562	123.058772	2600:140f:d800:2a3:…	2409:4056:19b:9e21:…	HTTP	337	HTTP/1.1 304 Not Modified
9572	123.239180	2409:4056:19b:9e21:…	2600:140f:d800:2a3:…	HTTP	301	GET / HTTP/1.1
9576	123.329026	2600:140f:d800:2a3:…	2409:4056:19b:9e21:…	HTTP	337	HTTP/1.1 304 Not Modified
9586	123.509036	2409:4056:19b:9e21:…	2405:200:1630:1200:…	HTTP	327	GET /DSTROOTCAX3CRL.crl HTTP/1.1
9591	123.620404	2405:200:1630:1200:…	2409:4056:19b:9e21:…	HTTP	342	HTTP/1.1 304 Not Modified

arp

No.	Time	Source	Destination	Protocol	Length	Info
402	29.850142	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
407	31.043616	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
413	31.843901	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
635	32.847945	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
659	34.036595	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
665	34.848502	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
719	35.843661	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
754	37.030199	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
767	37.839364	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
770	38.853225	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
774	40.032774	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
777	40.057387	5a:15:17:c2:6b:9e	IntelCor_c8:a4:97	ARP	42	Who has 192.168.43.2? Tell 192.168.43.1
778	40.057405	IntelCor_c8:a4:97	5a:15:17:c2:6b:9e	ARP	42	192.168.43.2 is at a0:51:0b:c8:a4:97
780	40.852817	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
783	41.844424	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
788	43.030294	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
804	43.846688	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
813	44.842015	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
835	46.034892	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
844	46.844477	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
851	47.850455	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
855	49.035001	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
864	49.841871	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
883	50.848683	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
903	52.032452	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
918	52.850398	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
952	53.839317	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
984	55.039981	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
995	55.246776	5a:15:17:c2:6b:9e	IntelCor_c8:a4:97	ARP	42	Who has 192.168.43.2? Tell 192.168.43.1
996	55.246790	IntelCor_c8:a4:97	5a:15:17:c2:6b:9e	ARP	42	192.168.43.2 is at a0:51:0b:c8:a4:97
1027	55.847588	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2
1057	56.844331	IntelCor_c8:a4:97	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.43.2