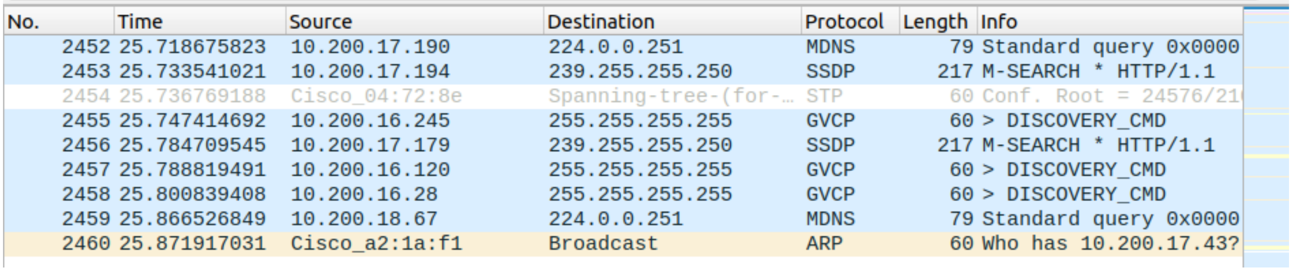
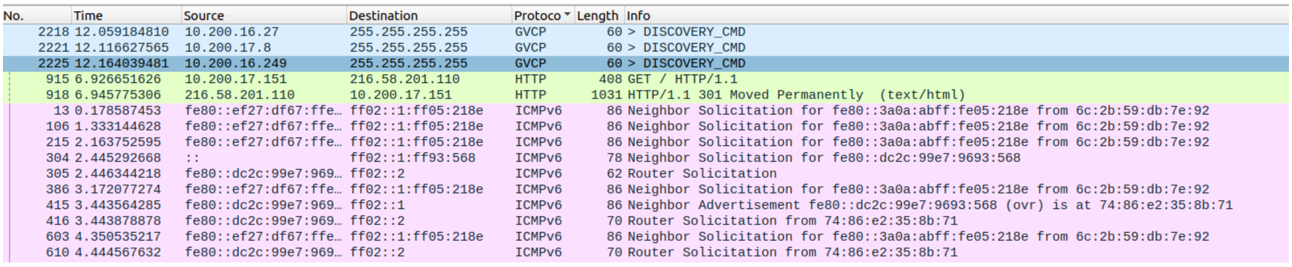
Joel Trainer
Assignment 1:



No.	Time	Source	Destination	Protocol	Length	Info
2452	25.718675823	10.200.17.190	224.0.0.251	MDNS	79	Standard query 0x0000
2453	25.733541021	10.200.17.194	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
2454	25.736769188	Cisco_04:72:8e	Spanning-tree-(for-…	STP	60	Conf. Root = 24576/21
2455	25.747414692	10.200.16.245	255.255.255.255	GVCP	60	> DISCOVERY_CMD
2456	25.784709545	10.200.17.179	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
2457	25.788819491	10.200.16.120	255.255.255.255	GVCP	60	> DISCOVERY_CMD
2458	25.800839408	10.200.16.28	255.255.255.255	GVCP	60	> DISCOVERY_CMD
2459	25.866526849	10.200.18.67	224.0.0.251	MDNS	79	Standard query 0x0000
2460	25.871917031	Cisco_a2:1a:f1	Broadcast	ARP	60	Who has 10.200.17.43?

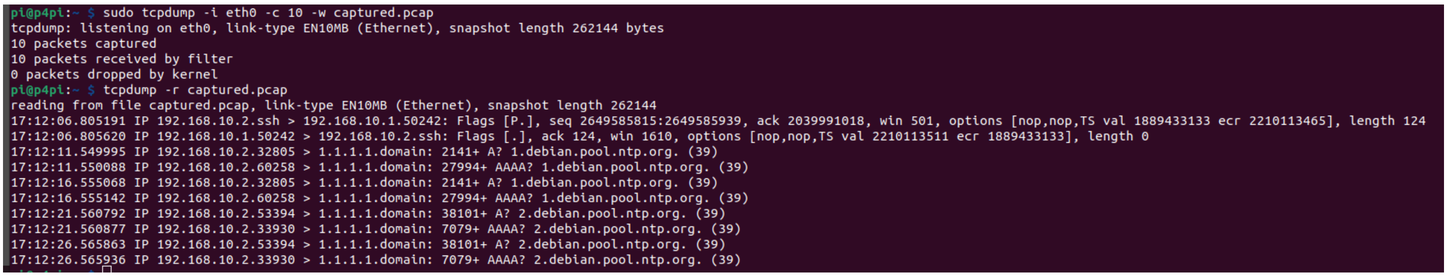
The packets captured are using a lot of different protocols. I think most are for making connections.



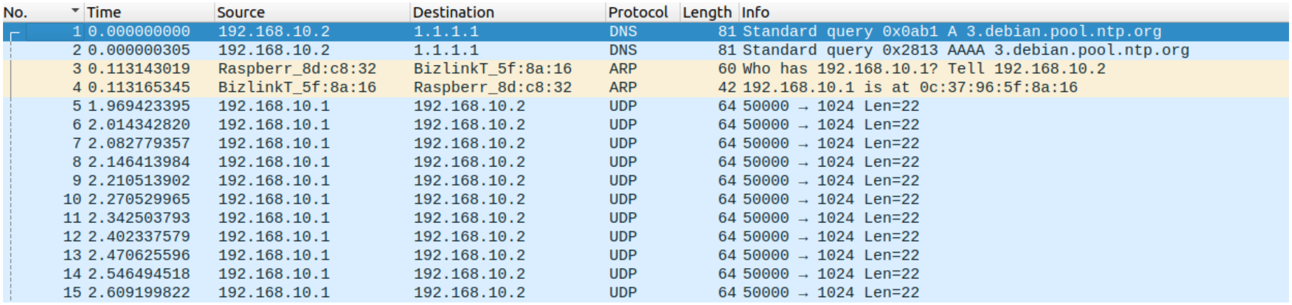
No.	Time	Source	Destination	Protoco	Length	Info
2218	12.059184810	10.200.16.27	255.255.255.255	GVCP	60	> DISCOVERY_CMD
2221	12.116627565	10.200.17.8	255.255.255.255	GVCP	60	> DISCOVERY_CMD
2225	12.164039481	10.200.16.249	255.255.255.255	GVCP	60	> DISCOVERY_CMD
915	6.926651626	10.200.17.151	216.58.201.110	HTTP	408	GET / HTTP/1.1
918	6.945775306	216.58.201.110	10.200.17.151	HTTP	1031	HTTP/1.1 301 Moved Permanently (text/html)
13	0.178587453	fe80::ef27:df67:ffe…	ff02::1:ff05:218e	ICMPv6	86	Neighbor Solicitation for fe80::3a0a:abff:fe05:218e from 6c:2b:59:db:7e:92
106	1.333144628	fe80::ef27:df67:ffe…	ff02::1:ff05:218e	ICMPv6	86	Neighbor Solicitation for fe80::3a0a:abff:fe05:218e from 6c:2b:59:db:7e:92
215	2.163752595	fe80::ef27:df67:ffe…	ff02::1:ff05:218e	ICMPv6	86	Neighbor Solicitation for fe80::3a0a:abff:fe05:218e from 6c:2b:59:db:7e:92
304	2.445292668	::	ff02::1:ff93:568	ICMPv6	78	Neighbor Solicitation for fe80::dc2c:99e7:9693:568
305	2.446344218	fe80::dc2c:99e7:969…	ff02::2	ICMPv6	62	Router Solicitation
386	3.172077274	fe80::ef27:df67:ffe…	ff02::1:ff05:218e	ICMPv6	86	Neighbor Solicitation for fe80::3a0a:abff:fe05:218e from 6c:2b:59:db:7e:92
415	3.443564285	fe80::dc2c:99e7:969…	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::dc2c:99e7:9693:568 (ovr) is at 74:86:e2:35:8b:71
416	3.443878878	fe80::dc2c:99e7:969…	ff02::2	ICMPv6	70	Router Solicitation from 74:86:e2:35:8b:71
603	4.350535217	fe80::ef27:df67:ffe…	ff02::1:ff05:218e	ICMPv6	86	Neighbor Solicitation for fe80::3a0a:abff:fe05:218e from 6c:2b:59:db:7e:92
610	4.444567632	fe80::dc2c:99e7:969…	ff02::2	ICMPv6	70	Router Solicitation from 74:86:e2:35:8b:71

To get HTTP I needed to search for a website in the browser.

Here is a screenshot of captured packets

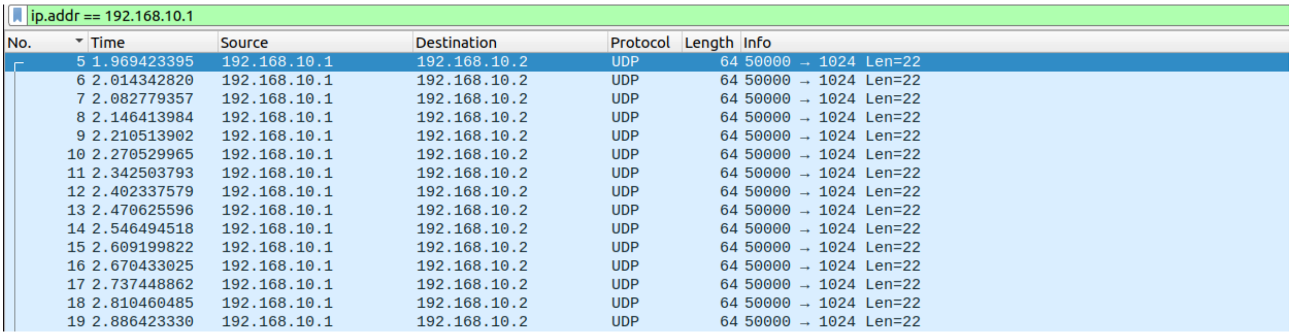


```
pi@p4pi:~ $ sudo tcpdump -i eth0 -c 10 -w captured.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10 packets captured
10 packets received by filter
0 packets dropped by kernel
pi@p4pi:~ $ tcpdump -r captured.pcap
reading from file captured.pcap, link-type EN10MB (Ethernet), snapshot length 262144
17:12:06.805191 IP 192.168.10.2.ssh > 192.168.10.1.50242: Flags [P.], seq 2649585815:2649585939, ack 2039991018, win 501, options [nop,nop,TS val 1889433133 ecr 2210113465], length 124
17:12:06.805620 IP 192.168.10.1.50242 > 192.168.10.2.ssh: Flags [.], ack 124, win 1610, options [nop,nop,TS val 2210113511 ecr 1889433133], length 0
17:12:11.549995 IP 192.168.10.2.32805 > 1.1.1.1.domain: 2141+ A? 1.debian.pool.ntp.org. (39)
17:12:11.550088 IP 192.168.10.2.60258 > 1.1.1.1.domain: 27994+ AAAA? 1.debian.pool.ntp.org. (39)
17:12:16.555068 IP 192.168.10.2.32805 > 1.1.1.1.domain: 2141+ A? 1.debian.pool.ntp.org. (39)
17:12:16.555142 IP 192.168.10.2.60258 > 1.1.1.1.domain: 27994+ AAAA? 1.debian.pool.ntp.org. (39)
17:12:21.560792 IP 192.168.10.2.53394 > 1.1.1.1.domain: 38101+ A? 2.debian.pool.ntp.org. (39)
17:12:21.560877 IP 192.168.10.2.33930 > 1.1.1.1.domain: 7079+ AAAA? 2.debian.pool.ntp.org. (39)
17:12:26.565863 IP 192.168.10.2.53394 > 1.1.1.1.domain: 38101+ A? 2.debian.pool.ntp.org. (39)
17:12:26.565936 IP 192.168.10.2.33930 > 1.1.1.1.domain: 7079+ AAAA? 2.debian.pool.ntp.org. (39)
```



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x0ab1 A 3.debian.pool.ntp.org
2	0.000000305	192.168.10.2	1.1.1.1	DNS	81	Standard query 0x2813 AAAA 3.debian.pool.ntp.org
3	0.113143019	Raspberr_8d:c8:32	BizlinkT_5f:8a:16	ARP	60	Who has 192.168.10.1? Tell 192.168.10.2
4	0.113165345	BizlinkT_5f:8a:16	Raspberr_8d:c8:32	ARP	42	192.168.10.1 is at 0c:37:96:5f:8a:16
5	1.969423395	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
6	2.014342820	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
7	2.082779357	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
8	2.146413984	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
9	2.210513902	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
10	2.270529965	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
11	2.342503793	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
12	2.402337579	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
13	2.470625596	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
14	2.546494518	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
15	2.609199822	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22

The packets sent used UDP, length 86.

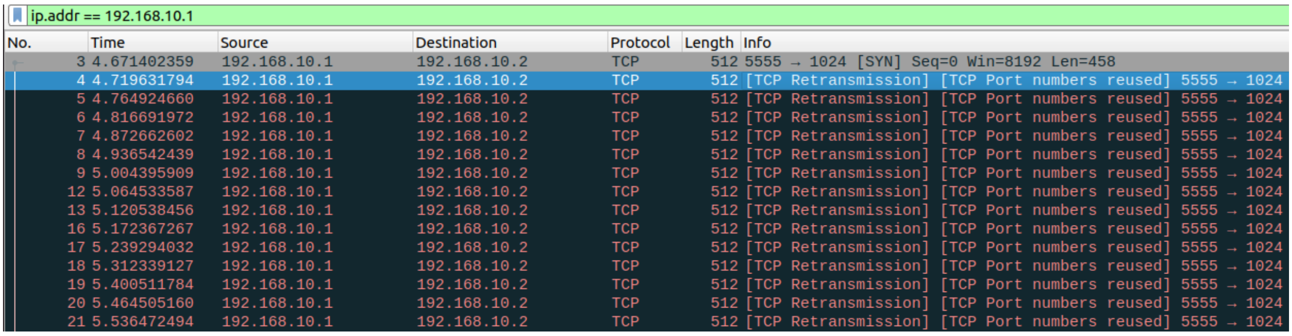


ip.addr == 192.168.10.1

No.	Time	Source	Destination	Protocol	Length	Info
5	1.969423395	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
6	2.014342820	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
7	2.082779357	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
8	2.146413984	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
9	2.210513902	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
10	2.270529965	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
11	2.342503793	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
12	2.402337579	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
13	2.470625596	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
14	2.546494518	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
15	2.609199822	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
16	2.670433025	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
17	2.737448862	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
18	2.810460485	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22
19	2.886423330	192.168.10.1	192.168.10.2	UDP	64	50000 → 1024 Len=22

This is filtered to only see packets form ip address 192.168.10.1

Here is a screenshot of captured packets after modifying the code



ip.addr == 192.168.10.1

No.	Time	Source	Destination	Protocol	Length	Info
3	4.671402359	192.168.10.1	192.168.10.2	TCP	512	5555 → 1024 [SYN] Seq=0 Win=8192 Len=458
4	4.719631794	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024
5	4.764924660	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024
6	4.816691972	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024
7	4.872662602	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024
8	4.936542439	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024
9	5.004395909	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024
12	5.064533587	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024
13	5.120538456	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024
16	5.172367267	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024
17	5.239294032	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024
18	5.312339127	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024
19	5.400511784	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024
20	5.464505160	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024
21	5.536472494	192.168.10.1	192.168.10.2	TCP	512	[TCP Retransmission] [TCP Port numbers reused] 5555 → 1024