

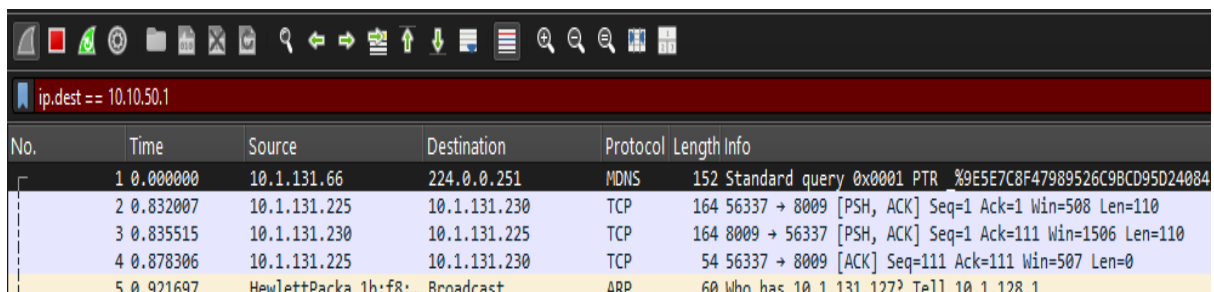
Network Security Lab

Name: Rooshan Riaz

Reg No: 2022506

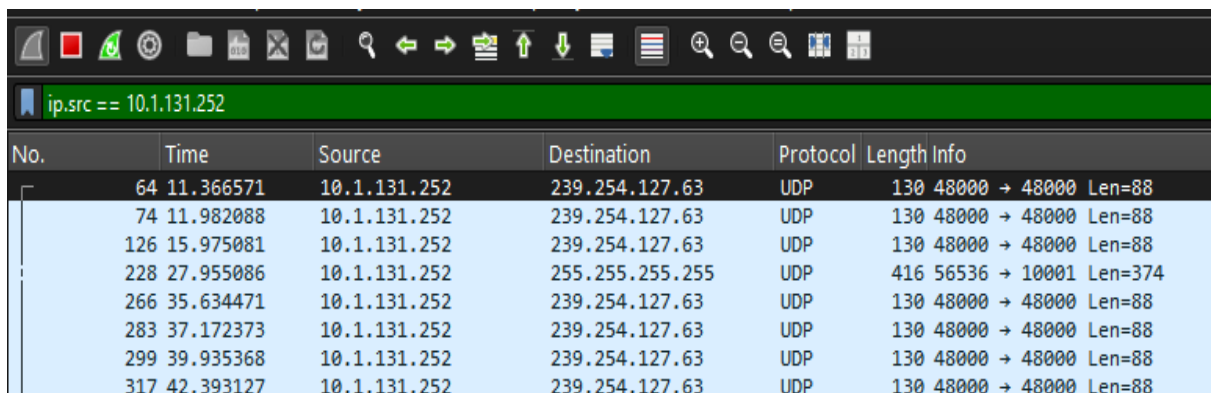
Lab-02: Packet Filtering Using Wireshark

Filter by Destination IP:



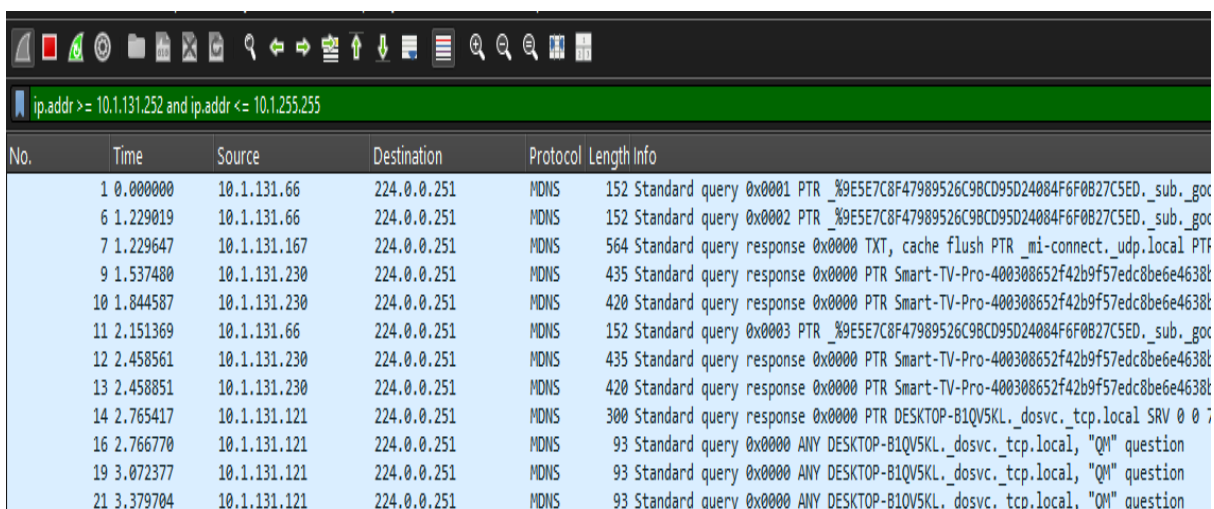
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.1.131.66	224.0.0.251	MDNS	152	Standard query 0x0001 PTR %9E5E7C8F47989526C9BCD95D24084
2	0.832007	10.1.131.225	10.1.131.230	TCP	164	56337 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=508 Len=110
3	0.835515	10.1.131.230	10.1.131.225	TCP	164	8009 → 56337 [PSH, ACK] Seq=1 Ack=111 Win=1506 Len=110
4	0.878306	10.1.131.225	10.1.131.230	TCP	54	56337 → 8009 [ACK] Seq=111 Ack=111 Win=507 Len=0
5	0.921697	HewlettPacka	1b:f8:: Broadcast	ARP	60	Who has 10.1.131.127? Tell 10.1.128.1

Filter by Source IP:



No.	Time	Source	Destination	Protocol	Length	Info
64	11.366571	10.1.131.252	239.254.127.63	UDP	130	48000 → 48000 Len=88
74	11.982088	10.1.131.252	239.254.127.63	UDP	130	48000 → 48000 Len=88
126	15.975081	10.1.131.252	239.254.127.63	UDP	130	48000 → 48000 Len=88
228	27.955086	10.1.131.252	255.255.255.255	UDP	416	56536 → 10001 Len=374
266	35.634471	10.1.131.252	239.254.127.63	UDP	130	48000 → 48000 Len=88
283	37.172373	10.1.131.252	239.254.127.63	UDP	130	48000 → 48000 Len=88
299	39.935368	10.1.131.252	239.254.127.63	UDP	130	48000 → 48000 Len=88
317	42.393127	10.1.131.252	239.254.127.63	UDP	130	48000 → 48000 Len=88

Filter by IP Range:



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.1.131.66	224.0.0.251	MDNS	152	Standard query 0x0001 PTR %9E5E7C8F47989526C9BCD95D24084F6F0827C5ED, _sub._goc
6	1.229019	10.1.131.66	224.0.0.251	MDNS	152	Standard query 0x0002 PTR %9E5E7C8F47989526C9BCD95D24084F6F0827C5ED, _sub._goc
7	1.229647	10.1.131.167	224.0.0.251	MDNS	564	Standard query response 0x0000 TXT, cache flush PTR _mi-connect, udp, local PTR
9	1.537480	10.1.131.230	224.0.0.251	MDNS	435	Standard query response 0x0000 PTR Smart-TV-Pro-400308652f42b9f57edc8be6e4638t
10	1.844587	10.1.131.230	224.0.0.251	MDNS	420	Standard query response 0x0000 PTR Smart-TV-Pro-400308652f42b9f57edc8be6e4638t
11	2.151369	10.1.131.66	224.0.0.251	MDNS	152	Standard query 0x0003 PTR %9E5E7C8F47989526C9BCD95D24084F6F0827C5ED, _sub._goc
12	2.458561	10.1.131.230	224.0.0.251	MDNS	435	Standard query response 0x0000 PTR Smart-TV-Pro-400308652f42b9f57edc8be6e4638t
13	2.458851	10.1.131.230	224.0.0.251	MDNS	420	Standard query response 0x0000 PTR Smart-TV-Pro-400308652f42b9f57edc8be6e4638t
14	2.765417	10.1.131.121	224.0.0.251	MDNS	300	Standard query response 0x0000 PTR DESKTOP-B1QV5KL, _dosvc._tcp.local, "QM" question
16	2.766770	10.1.131.121	224.0.0.251	MDNS	93	Standard query 0x0000 ANY DESKTOP-B1QV5KL, _dosvc._tcp.local, "QM" question
19	3.072377	10.1.131.121	224.0.0.251	MDNS	93	Standard query 0x0000 ANY DESKTOP-B1QV5KL, _dosvc._tcp.local, "QM" question
21	3.379704	10.1.131.121	224.0.0.251	MDNS	93	Standard query 0x0000 ANY DESKTOP-B1QV5KL, _dosvc._tcp.local, "QM" question

Filter Using XOR:

ip.addr == 20.190.146.35 xor tcp						
No.	Time	Source	Destination	Protocol	Length	Info
112	15.881035	20.24.249.45	10.1.131.225	TCP	1454	443 → 56480 [ACK] Seq=1 Ack=306 Win=262656 Len=1400 [TCP PDU reassembled in 116]
113	15.881035	20.24.249.45	10.1.131.225	TCP	1454	443 → 56480 [ACK] Seq=1401 Ack=306 Win=262656 Len=1400 [TCP PDU reassembled in 116]
114	15.881035	20.24.249.45	10.1.131.225	TCP	1454	443 → 56480 [ACK] Seq=2801 Ack=306 Win=262656 Len=1400 [TCP PDU reassembled in 116]
115	15.881035	20.24.249.45	10.1.131.225	TCP	1454	443 → 56480 [ACK] Seq=4201 Ack=306 Win=262656 Len=1400 [TCP PDU reassembled in 116]
128	16.214464	20.24.249.45	10.1.131.225	TCP	60	443 → 56480 [ACK] Seq=6378 Ack=2334 Win=263168 Len=0
188	15.713966	20.24.249.45	10.1.131.225	TCP	66	443 → 56480 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
147	20.404481	10.1.131.129	10.1.131.225	TCP	54	52687 → 7680 [ACK] Seq=5 Ack=5 Win=512 Len=0
460	67.702311	10.1.131.129	10.1.131.225	TCP	54	53198 → 7680 [ACK] Seq=1 Ack=1 Win=131328 Len=0
464	67.706758	10.1.131.129	10.1.131.225	TCP	54	53198 → 7680 [ACK] Seq=76 Ack=77 Win=131072 Len=0
465	67.707162	10.1.131.129	10.1.131.225	TCP	54	53198 → 7680 [FIN, ACK] Seq=76 Ack=77 Win=131072 Len=0
458	67.698312	10.1.131.129	10.1.131.225	TCP	66	53198 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
109	15.714111	10.1.131.225	20.24.249.45	TCP	54	56480 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
129	16.214571	10.1.131.225	20.24.249.45	TCP	54	56480 → 443 [ACK] Seq=2334 Ack=6378 Win=261888 Len=0
132	16.247182	10.1.131.225	20.24.249.45	TCP	54	56480 → 443 [ACK] Seq=2334 Ack=6941 Win=261376 Len=0
117	15.881190	10.1.131.225	20.24.249.45	TCP	54	56480 → 443 [ACK] Seq=306 Ack=6220 Win=262144 Len=0
122	16.050287	10.1.131.225	20.24.249.45	TCP	54	56480 → 443 [ACK] Seq=464 Ack=6340 Win=261888 Len=0
125	16.059662	10.1.131.225	20.24.249.45	TCP	1494	56480 → 443 [ACK] Seq=589 Ack=6340 Win=261888 Len=1440 [TCP PDU reassembled in 126]
104	15.557901	10.1.131.225	20.24.249.45	TCP	66	56480 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
110	15.718082	10.1.131.225	10.1.131.129	TCP	54	7680 → 52687 [ACK] Seq=1 Ack=5 Win=4099 Len=0
466	67.707193	10.1.131.225	10.1.131.129	TCP	54	7680 → 53198 [ACK] Seq=77 Ack=77 Win=1049600 Len=0
463	67.703611	10.1.131.225	10.1.131.129	TCP	54	7680 → 53198 [FIN, ACK] Seq=76 Ack=76 Win=1049600 Len=0
459	67.698532	10.1.131.225	10.1.131.129	TCP	66	7680 → 53198 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
121	16.050185	20.24.249.45	10.1.131.225	TLSv1.2	123	Application Data
123	16.059086	10.1.131.225	20.24.249.45	TLSv1.2	141	Application Data
124	16.059258	10.1.131.225	20.24.249.45	TLSv1.2	92	Application Data
126	16.059662	10.1.131.225	20.24.249.45	TLSv1.2	359	Application Data
127	16.214464	20.24.249.45	10.1.131.225	TLSv1.2	92	Application Data
130	16.247146	20.24.249.45	10.1.131.225	TLSv1.2	579	Application Data
131	16.247146	20.24.249.45	10.1.131.225	TLSv1.2	92	Application Data
120	16.050185	20.24.249.45	10.1.131.225	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
111	15.722215	10.1.131.225	20.24.249.45	TLSv1.2	359	Client Hello (SNI=fd.api.icris.microsoft.com)

Filtering IP Address by != (Not Equal):

ip.addr != 10.1.131.255						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.1.131.66	224.0.0.251	MDNS	152	Standard query 0x0001 PTR _90E5E7C8F47989526C9BCD95D24084F6F0827C5ED._sub._googlecast._tcp.local, "QU" quest
2	0.832087	10.1.131.225	10.1.131.230	TCP	164	56337 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=508 Len=110 [TCP PDU reassembled in 270]
3	0.835515	10.1.131.230	10.1.131.225	TCP	164	8009 → 56337 [PSH, ACK] Seq=1 Ack=111 Win=1506 Len=110 [TCP PDU reassembled in 271]
4	0.878306	10.1.131.225	10.1.131.230	TCP	54	56337 → 8009 [ACK] Seq=111 Ack=111 Win=507 Len=0
6	1.229019	10.1.131.66	224.0.0.251	MDNS	152	Standard query 0x0002 PTR _90E5E7C8F47989526C9BCD95D24084F6F0827C5ED._sub._googlecast._tcp.local, "QM" quest
7	1.229647	10.1.131.167	224.0.0.251	MDNS	564	Standard query response 0x0000 TXT, cache flush PTR _mi-connect._udp.local PTR ("nm";"POCO X3 NFC","as");"B19
9	1.537480	10.1.131.230	224.0.0.251	MDNS	435	Standard query response 0x0000 PTR Smart-TV-Pro-400308652f42b9f57edc8be6e4638b59._googlecast._tcp.local TXT,
10	1.844587	10.1.131.230	224.0.0.251	MDNS	420	Standard query response 0x0000 PTR Smart-TV-Pro-400308652f42b9f57edc8be6e4638b59._googlecast._tcp.local TXT,
11	2.151369	10.1.131.66	224.0.0.251	MDNS	152	Standard query 0x0003 PTR _90E5E7C8F47989526C9BCD95D24084F6F0827C5ED._sub._googlecast._tcp.local, "QM" quest
12	2.458561	10.1.131.230	224.0.0.251	MDNS	435	Standard query response 0x0000 PTR Smart-TV-Pro-400308652f42b9f57edc8be6e4638b59._googlecast._tcp.local TXT,
13	2.458851	10.1.131.230	224.0.0.251	MDNS	420	Standard query response 0x0000 PTR Smart-TV-Pro-400308652f42b9f57edc8be6e4638b59._googlecast._tcp.local TXT,
14	2.765417	10.1.131.121	224.0.0.251	MDNS	300	Standard query response 0x0000 PTR DESKTOP-B1QVSKL._dosvc._tcp.local SRV 0 0 7680 DESKTOP-B1QVSKL.local TXT
16	2.766770	10.1.131.121	224.0.0.251	MDNS	93	Standard querv 0x0000 ANY DESKTOP-B1QVSKL._dosvc._tcp.local. "QM" question

Filtering Out by Subnet:

ip.addr == 10.1.131.121/24						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.1.131.113	224.0.0.251	MDNS	278	Standard query response 0x0000 PTR DESKTOP-M32KR2E._dosvc._tcp.local SRV 0 0 7680 DESKTOP-M32KR2E.local TXT
3	0.000591	10.1.131.113	224.0.0.251	MDNS	93	Standard query 0x0000 ANY DESKTOP-M32KR2E._dosvc._tcp.local, "QM" question
5	0.001115	10.1.131.143	224.0.0.251	MDNS	97	Standard query 0x0000 PTR lb._dns-sd._udp.local, "QU" question PTR _atc._tcp.local, "QU" question
7	0.001906	10.1.131.88	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
9	0.002261	10.1.131.88	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
11	0.307140	10.1.131.113	224.0.0.251	MDNS	93	Standard query 0x0000 ANY DESKTOP-M32KR2E._dosvc._tcp.local, "QM" question
13	0.307902	10.1.131.113	224.0.0.251	MDNS	93	Standard query 0x0000 ANY DESKTOP-M32KR2E._dosvc._tcp.local, "QM" question

Filter by IP Address and Protocol:

ip.addr == 10.1.131.129 and tcp						
No.	Time	Source	Destination	Protocol	Length	Info
107	15.674762	10.1.131.129	10.1.131.225	MS-DO	58	KeepAlive Message
110	15.718082	10.1.131.225	10.1.131.129	TCP	54	7680 → 52687 [ACK] Seq=1 Ack=5 Win=4099 Len=0
146	20.347694	10.1.131.225	10.1.131.129	MS-DO	58	KeepAlive Message
147	20.404481	10.1.131.129	10.1.131.225	TCP	54	52687 → 7680 [ACK] Seq=5 Ack=5 Win=512 Len=0
458	67.698312	10.1.131.129	10.1.131.225	TCP	66	53198 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
459	67.698532	10.1.131.225	10.1.131.129	TCP	66	7680 → 53198 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
460	67.702311	10.1.131.129	10.1.131.225	TCP	54	53198 → 7680 [ACK] Seq=1 Ack=1 Win=131328 Len=0
461	67.703139	10.1.131.129	10.1.131.225	MS-DO	129	Handshake Message (Request)
462	67.703377	10.1.131.225	10.1.131.129	MS-DO	129	Handshake Message (Reply)
463	67.703611	10.1.131.225	10.1.131.129	TCP	54	7680 → 53198 [FIN, ACK] Seq=76 Ack=76 Win=1049600 Len=0
464	67.706758	10.1.131.129	10.1.131.225	TCP	54	53198 → 7680 [ACK] Seq=76 Ack=77 Win=131072 Len=0
465	67.707162	10.1.131.225	10.1.131.129	TCP	54	53198 → 7680 [FIN, ACK] Seq=76 Ack=77 Win=131072 Len=0
466	67.707193	10.1.131.225	10.1.131.129	TCP	54	7680 → 53198 [ACK] Seq=77 Ack=77 Win=1049600 Len=0

Filter SYN Flag:

tcp.flags.syn == 1						
No.	Time	Source	Destination	Protocol	Length Info	
63	14.772044	10.1.131.225	20.190.146.35	TCP	66 56479 → 443 [SYN]	Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
64	14.853171	20.190.146.35	10.1.131.225	TCP	66 443 → 56479 [SYN, ACK]	Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
104	15.557901	10.1.131.225	20.24.249.45	TCP	66 56480 → 443 [SYN]	Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
108	15.713966	20.24.249.45	10.1.131.225	TCP	66 443 → 56480 [SYN, ACK]	Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
458	67.698312	10.1.131.129	10.1.131.225	TCP	66 53198 → 7680 [SYN]	Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
459	67.698532	10.1.131.225	10.1.131.129	TCP	66 7680 → 53198 [SYN, ACK]	Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM

tcp.flags.syn == 1 and tcp.flags.ack == 0						
No.	Time	Source	Destination	Protocol	Length Info	
63	14.772044	10.1.131.225	20.190.146.35	TCP	66 56479 → 443 [SYN]	Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
104	15.557901	10.1.131.225	20.24.249.45	TCP	66 56480 → 443 [SYN]	Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
458	67.698312	10.1.131.129	10.1.131.225	TCP	66 53198 → 7680 [SYN]	Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

Filter Out IP Address:

!(ip.addr == 10.1.131.59)						
No.	Time	Source	Destination	Protocol	Length Info	
1	0.000000	10.1.131.129	10.1.131.255	NBNS	92	Name query NB DESKTOP-INV3IOF8<1c>
3	0.921742	fe80::1002:d7b:7e32::ff02::fb		MDNS	120	Standard query 0x0000 PTR _companion-link_tcp.local, "QM" question PTR _rdlink_tcp.local, "QM" question
4	1.228696	10.1.131.129	10.1.131.255	NBNS	92	Name query NB DESKTOP-INV3IOF8<1c>
5	1.228936	Dell_3c31:9e	Broadcast	ARP	60	Who has 10.1.131.127? Tell 10.1.131.72
6	1.228936	HewlettPacka_1b:f8::	Broadcast	ARP	60	Who has 10.1.131.27? Tell 10.1.128.1
7	1.228936	HewlettPacka_1b:f8::	Broadcast	ARP	60	Who has 10.1.131.50? Tell 10.1.128.1
8	1.536157	10.1.131.129	10.1.131.255	NBNS	92	Name query NB DESKTOP-INV3IOF8<1c>
9	1.843063	CloudNetwork_f2:ab::	Broadcast	ARP	42	Who has 10.1.131.222? Tell 10.1.131.166
10	2.457750	CloudNetwork_f2:ab::	Broadcast	ARP	42	Who has 10.1.131.222? Tell 10.1.131.166
11	3.379343	CloudNetwork_f2:ab::	Broadcast	ARP	42	Who has 10.1.131.222? Tell 10.1.131.166
13	3.379615	fe80::1002:d7b:7e32::ff02::fb		MDNS	120	Standard query 0x0000 PTR _companion-link_tcp.local, "QM" question PTR _rdlink_tcp.local, "QM" question
14	3.993725	Dell_3c31:9e	Broadcast	ARP	60	Who has 10.1.131.127? Tell 10.1.131.72
15	4.607909	CloudNetwork_f2:ab::	Broadcast	ARP	42	Who has 10.1.131.197? Tell 10.1.131.68
16	4.917329	Dell_3c31:9e	Broadcast	ARP	60	Who has 10.1.131.127? Tell 10.1.131.72
17	4.918347	10.1.131.252	255.255.255.255	UDP	416	51744 → 10001 Len=374

Filter by time stamp:

frame.time >= "September 24, 2024 4:00:00"						
No.	Time	Source	Destination	Protocol	Length Info	
1	0.000000	10.1.131.129	10.1.131.255	NBNS	92	Name query NB DESKTOP-INV3IOF8<1c>
2	0.614540	10.1.131.59	224.0.0.251	MDNS	100	Standard query 0x0000 PTR _companion-link_tcp.local, "QM" question PTR _rdlink_tcp.local, "QM" question
3	0.921742	fe80::1002:d7b:7e32::ff02::fb		MDNS	120	Standard query 0x0000 PTR _companion-link_tcp.local, "QM" question PTR _rdlink_tcp.local, "QM" question
4	1.228696	10.1.131.129	10.1.131.255	NBNS	92	Name query NB DESKTOP-INV3IOF8<1c>
5	1.228936	Dell_3c31:9e	Broadcast	ARP	60	Who has 10.1.131.127? Tell 10.1.131.72
6	1.228936	HewlettPacka_1b:f8::	Broadcast	ARP	60	Who has 10.1.131.27? Tell 10.1.128.1
7	1.228936	HewlettPacka_1b:f8::	Broadcast	ARP	60	Who has 10.1.131.50? Tell 10.1.128.1
8	1.536157	10.1.131.129	10.1.131.255	NBNS	92	Name query NB DESKTOP-INV3IOF8<1c>
9	1.843063	CloudNetwork_f2:ab::	Broadcast	ARP	42	Who has 10.1.131.222? Tell 10.1.131.166
10	2.457750	CloudNetwork_f2:ab::	Broadcast	ARP	42	Who has 10.1.131.222? Tell 10.1.131.166
11	3.379343	CloudNetwork_f2:ab::	Broadcast	ARP	42	Who has 10.1.131.222? Tell 10.1.131.166
12	3.379343	10.1.131.59	224.0.0.251	MDNS	100	Standard query 0x0000 PTR _companion-link_tcp.local, "QM" question PTR _rdlink_tcp.local, "QM" question
13	3.379615	fe80::1002:d7b:7e32::ff02::fb		MDNS	120	Standard query 0x0000 PTR _companion-link_tcp.local, "QM" question PTR _rdlink_tcp.local, "QM" question
14	3.993725	Dell_3c31:9e	Broadcast	ARP	60	Who has 10.1.131.127? Tell 10.1.131.72
15	4.607909	CloudNetwork_f2:ab::	Broadcast	ARP	42	Who has 10.1.131.197? Tell 10.1.131.68
16	4.917329	Dell_3c31:9e	Broadcast	ARP	60	Who has 10.1.131.127? Tell 10.1.131.72

Filter by Length greater than 100:

frame.len > 100						
No.	Time	Source	Destination	Protocol	Length	
3	0.921742	fe80::1002:d7b:7e32::ff02::fb		MDNS	120	
13	3.379615	fe80::1002:d7b:7e32::ff02::fb		MDNS	120	
17	4.918347	10.1.131.252	255.255.255.255	UDP	416	
19	5.226426	10.1.131.130	224.0.0.251	MDNS	278	
20	5.226958	fe80::5794:ed1:e2ae::ff02::fb		MDNS	298	
22	5.227594	fe80::5794:ed1:e2ae::ff02::fb		MDNS	113	
24	5.529884	fe80::5794:ed1:e2ae::ff02::fb		MDNS	113	
27	5.836859	fe80::5794:ed1:e2ae::ff02::fb		MDNS	113	
30	6.146160	10.1.131.130	224.0.0.251	MDNS	343	
31	6.147051	fe80::5794:ed1:e2ae::ff02::fb		MDNS	363	
32	6.147630	10.1.131.130	224.0.0.251	MDNS	279	
33	6.147630	fe80::5794:ed1:e2ae::ff02::fb		MDNS	299	
39	7.987715	fe80::4f1:31e7:c595::ff02::fb		MDNS	103	
54	12.595622	fe80::1002:d7b:7e32::ff02::fb		MDNS	120	
55	12.902140	10.1.131.54	224.0.0.251	MDNS	291	
58	13.516794	10.1.131.101	10.1.131.255	BROWSER	243	
60	14.772044	10.1.131.225	20.190.146.35	TCP	256	

Filter by Length equal to 100:

frame.len == 92					
No.	Time	Source	Destination	Protocol	Length
1	0.000000	10.1.131.129	10.1.131.255	NBNS	92
4	1.228696	10.1.131.129	10.1.131.255	NBNS	92
8	1.536157	10.1.131.129	10.1.131.255	NBNS	92
29	6.145687	10.1.131.146	10.1.131.255	NBNS	92
34	6.760857	10.1.131.146	10.1.131.255	NBNS	92
37	7.372487	10.1.131.146	10.1.131.255	NBNS	92
45	9.523220	10.1.131.61	10.1.131.255	NBNS	92
49	11.059354	10.1.131.61	10.1.131.255	NBNS	92
59	13.823874	10.1.131.126	10.1.131.255	NBNS	92
60	14.437779	10.1.131.126	10.1.131.255	NBNS	92
72	15.052805	10.1.131.126	10.1.131.255	NBNS	92
124	16.059258	10.1.131.225	20.24.249.45	TLSv1.2	92
127	16.214464	20.24.249.45	10.1.131.225	TLSv1.2	92
131	16.247146	20.24.249.45	10.1.131.225	TLSv1.2	92
134	16.688647	10.1.131.225	10.1.131.255	NBNS	92
136	17.438670	10.1.131.225	10.1.131.255	NBNS	92
139	18.204079	10.1.131.225	10.1.131.255	NBNS	92
231	28.568944	10.1.131.150	10.1.131.255	NBNS	92
236	28.877975	10.1.131.213	10.1.131.255	NBNS	92
241	29.184916	10.1.131.150	10.1.131.255	NBNS	92
247	29.492511	10.1.131.213	10.1.131.255	NBNS	92
250	30.412461	10.1.131.150	10.1.131.255	NBNS	92
251	30.719669	10.1.131.213	10.1.131.255	NBNS	92
261	34.405811	10.1.131.213	10.1.131.255	NBNS	92
262	35.327791	10.1.131.213	10.1.131.255	NBNS	92
266	36.249361	10.1.131.213	10.1.131.255	NBNS	92
291	47.000918	10.1.131.146	10.1.131.255	NBNS	92
305	48.536809	10.1.131.146	10.1.131.255	NBNS	92
357	55.602430	10.1.131.146	10.1.131.255	NBNS	92
366	56.217522	10.1.131.146	10.1.131.255	NBNS	92
371	56.832606	10.1.131.146	10.1.131.255	NBNS	92

Broadcast Filter:

eth.dst == ff:ff:ff:ff:ff:ff					
No.	Time	Source	Destination	Protocol	Length Info
1	0.000000	10.1.131.129	10.1.131.255	NBNS	92 Name query NB DESKTOP-MV3I0F8<1c>
4	1.228696	10.1.131.129	10.1.131.255	NBNS	92 Name query NB DESKTOP-MV3I0F8<1c>
5	1.228936	Dell_3c:31:9e	Broadcast	ARP	60 Who has 10.1.131.127? Tell 10.1.131.72
6	1.228936	HewlettPacka_1b:f8:...	Broadcast	ARP	60 Who has 10.1.131.27? Tell 10.1.128.1
7	1.228936	HewlettPacka_1b:f8:...	Broadcast	ARP	60 Who has 10.1.131.50? Tell 10.1.128.1
8	1.536157	10.1.131.129	10.1.131.255	NBNS	92 Name query NB DESKTOP-MV3I0F8<1c>
9	1.843063	CloudNetwork_f2:ab:...	Broadcast	ARP	42 Who has 10.1.131.222? Tell 10.1.131.166
10	2.457750	CloudNetwork_f2:ab:...	Broadcast	ARP	42 Who has 10.1.131.222? Tell 10.1.131.166
11	3.379343	CloudNetwork_f2:ab:...	Broadcast	ARP	42 Who has 10.1.131.222? Tell 10.1.131.166
14	3.993725	Dell_3c:31:9e	Broadcast	ARP	60 Who has 10.1.131.127? Tell 10.1.131.72
15	4.607909	CloudNetwork_f2:ab:...	Broadcast	ARP	42 Who has 10.1.131.197? Tell 10.1.131.68
16	4.917329	Dell_3c:31:9e	Broadcast	ARP	60 Who has 10.1.131.127? Tell 10.1.131.72

Filtering Packets with TCP Port greater than 100:

all tcp.port > 100						
No.	Time	Source	Destination	Protocol	Length	Info
63	14.772044	10.1.131.225	20.190.146.35	TCP	66	56479 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
64	14.853171	20.190.146.35	10.1.131.225	TCP	66	443 → 56479 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
65	14.853221	10.1.131.225	20.190.146.35	TCP	54	56479 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
66	14.854384	10.1.131.225	20.190.146.35	TLSv1.2	348	Client Hello (SNI=login.live.com)
67	14.937851	20.190.146.35	10.1.131.225	TCP	1454	443 → 56479 [ACK] Seq=1 Ack=295 Win=4194048 Len=1400 [TCP PDU reassembled in 69]
68	14.937851	20.190.146.35	10.1.131.225	TCP	1454	443 → 56479 [ACK] Seq=1401 Ack=295 Win=4194048 Len=1400 [TCP PDU reassembled in 69]
69	14.937851	20.190.146.35	10.1.131.225	TLSv1.2	1211	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
70	14.937951	10.1.131.225	20.190.146.35	TCP	54	56479 → 443 [ACK] Seq=295 Ack=3958 Win=132352 Len=0
71	14.963714	10.1.131.225	20.190.146.35	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
73	15.053316	20.190.146.35	10.1.131.225	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
74	15.058604	10.1.131.225	20.190.146.35	TLSv1.2	333	Application Data
75	15.058807	10.1.131.225	20.190.146.35	TCP	1494	56479 → 443 [ACK] Seq=732 Ack=4009 Win=132352 Len=1440 [TCP PDU reassembled in 79]
76	15.058807	10.1.131.225	20.190.146.35	TCP	1494	56479 → 443 [ACK] Seq=2172 Ack=4009 Win=132352 Len=1440 [TCP PDU reassembled in 79]
77	15.058807	10.1.131.225	20.190.146.35	TCP	1494	56479 → 443 [ACK] Seq=3612 Ack=4009 Win=132352 Len=1440 [TCP PDU reassembled in 79]
78	15.058807	10.1.131.225	20.190.146.35	TCP	1494	56479 → 443 [ACK] Seq=5052 Ack=4009 Win=132352 Len=1440 [TCP PDU reassembled in 79]
79	15.058807	10.1.131.225	20.190.146.35	TLSv1.2	892	Application Data
80	15.140992	20.190.146.35	10.1.131.225	TCP	60	443 → 56479 [ACK] Seq=4009 Ack=2172 Win=4194304 Len=0
81	15.140992	20.190.146.35	10.1.131.225	TCP	60	443 → 56479 [ACK] Seq=4009 Ack=5052 Win=4194304 Len=0
82	15.140992	20.190.146.35	10.1.131.225	TCP	60	443 → 56479 [ACK] Seq=4009 Ack=7330 Win=4194304 Len=0
85	15.393902	20.190.146.35	10.1.131.225	TCP	1454	443 → 56479 [ACK] Seq=4009 Ack=7330 Win=4194304 Len=1400 [TCP PDU reassembled in 97]
86	15.393902	20.190.146.35	10.1.131.225	TCP	1454	443 → 56479 [ACK] Seq=5409 Ack=7330 Win=4194304 Len=1400 [TCP PDU reassembled in 97]
87	15.393902	20.190.146.35	10.1.131.225	TCP	1454	443 → 56479 [ACK] Seq=6809 Ack=7330 Win=4194304 Len=1400 [TCP PDU reassembled in 97]
88	15.393902	20.190.146.35	10.1.131.225	TCP	1454	443 → 56479 [ACK] Seq=8209 Ack=7330 Win=4194304 Len=1400 [TCP PDU reassembled in 97]
89	15.393902	20.190.146.35	10.1.131.225	TCP	1454	443 → 56479 [ACK] Seq=9609 Ack=7330 Win=4194304 Len=1400 [TCP PDU reassembled in 97]
90	15.393902	20.190.146.35	10.1.131.225	TCP	1454	443 → 56479 [ACK] Seq=11009 Ack=7330 Win=4194304 Len=1400 [TCP PDU reassembled in 97]
91	15.393902	20.190.146.35	10.1.131.225	TCP	1454	443 → 56479 [ACK] Seq=12409 Ack=7330 Win=4194304 Len=1400 [TCP PDU reassembled in 97]
92	15.393902	20.190.146.35	10.1.131.225	TCP	1454	443 → 56479 [ACK] Seq=13809 Ack=7330 Win=4194304 Len=1400 [TCP PDU reassembled in 97]
93	15.394044	10.1.131.225	20.190.146.35	TCP	54	56479 → 443 [ACK] Seq=7330 Ack=15209 Win=132352 Len=0
94	15.394612	20.190.146.35	10.1.131.225	TCP	1454	443 → 56479 [ACK] Seq=15209 Ack=7330 Win=4194304 Len=1400 [TCP PDU reassembled in 97]
95	15.394612	20.190.146.35	10.1.131.225	TCP	1454	443 → 56479 [ACK] Seq=16609 Ack=7330 Win=4194304 Len=1400 [TCP PDU reassembled in 97]
96	15.394612	20.190.146.35	10.1.131.225	TCP	1454	443 → 56479 [ACK] Seq=18009 Ack=7330 Win=4194304 Len=1400 [TCP PDU reassembled in 97]

Filter TCP Packets with Ports 80, 443, 8080:

tcp.port in {80,443,8080}						
No.	Time	Source	Destination	Protocol	Length	Info
63	14.772044	10.1.131.225	20.190.146.35	TCP	66	56479 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
64	14.853171	20.190.146.35	10.1.131.225	TCP	66	443 → 56479 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
65	14.853221	10.1.131.225	20.190.146.35	TCP	54	56479 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
66	14.854384	10.1.131.225	20.190.146.35	TLSv1.2	348	Client Hello (SNI=login.live.com)
67	14.937851	20.190.146.35	10.1.131.225	TCP	1454	443 → 56479 [ACK] Seq=1 Ack=295 Win=4194048 Len=1400 [TCP PDU reassembled in 69]
68	14.937851	20.190.146.35	10.1.131.225	TCP	1454	443 → 56479 [ACK] Seq=1401 Ack=295 Win=4194048 Len=1400 [TCP PDU reassembled in 69]
69	14.937851	20.190.146.35	10.1.131.225	TLSv1.2	1211	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
70	14.937951	10.1.131.225	20.190.146.35	TCP	54	56479 → 443 [ACK] Seq=295 Ack=3958 Win=132352 Len=0
71	14.963714	10.1.131.225	20.190.146.35	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
73	15.053316	20.190.146.35	10.1.131.225	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
74	15.058604	10.1.131.225	20.190.146.35	TLSv1.2	333	Application Data
75	15.058807	10.1.131.225	20.190.146.35	TCP	1494	56479 → 443 [ACK] Seq=732 Ack=4009 Win=132352 Len=1440 [TCP PDU reassembled in 79]
76	15.058807	10.1.131.225	20.190.146.35	TCP	1494	56479 → 443 [ACK] Seq=2172 Ack=4009 Win=132352 Len=1440 [TCP PDU reassembled in 79]
77	15.058807	10.1.131.225	20.190.146.35	TCP	1494	56479 → 443 [ACK] Seq=3612 Ack=4009 Win=132352 Len=1440 [TCP PDU reassembled in 79]
78	15.058807	10.1.131.225	20.190.146.35	TCP	1494	56479 → 443 [ACK] Seq=5052 Ack=4009 Win=132352 Len=1440 [TCP PDU reassembled in 79]
79	15.058807	10.1.131.225	20.190.146.35	TLSv1.2	892	Application Data
80	15.140992	20.190.146.35	10.1.131.225	TCP	60	443 → 56479 [ACK] Seq=4009 Ack=2172 Win=4194304 Len=0
81	15.140992	20.190.146.35	10.1.131.225	TCP	60	443 → 56479 [ACK] Seq=4009 Ack=5052 Win=4194304 Len=0
82	15.140992	20.190.146.35	10.1.131.225	TCP	60	443 → 56479 [ACK] Seq=4009 Ack=7330 Win=4194304 Len=0
85	15.393902	20.190.146.35	10.1.131.225	TCP	1454	443 → 56479 [ACK] Seq=4009 Ack=7330 Win=4194304 Len=1400 [TCP PDU reassembled in 97]
86	15.393902	20.190.146.35	10.1.131.225	TCP	1454	443 → 56479 [ACK] Seq=5409 Ack=7330 Win=4194304 Len=1400 [TCP PDU reassembled in 97]
87	15.393902	20.190.146.35	10.1.131.225	TCP	1454	443 → 56479 [ACK] Seq=6809 Ack=7330 Win=4194304 Len=1400 [TCP PDU reassembled in 97]
88	15.393902	20.190.146.35	10.1.131.225	TCP	1454	443 → 56479 [ACK] Seq=8209 Ack=7330 Win=4194304 Len=1400 [TCP PDU reassembled in 97]
89	15.393902	20.190.146.35	10.1.131.225	TCP	1454	443 → 56479 [ACK] Seq=9609 Ack=7330 Win=4194304 Len=1400 [TCP PDU reassembled in 97]
90	15.393902	20.190.146.35	10.1.131.225	TCP	1454	443 → 56479 [ACK] Seq=11009 Ack=7330 Win=4194304 Len=1400 [TCP PDU reassembled in 97]
91	15.393902	20.190.146.35	10.1.131.225	TCP	1454	443 → 56479 [ACK] Seq=12409 Ack=7330 Win=4194304 Len=1400 [TCP PDU reassembled in 97]
92	15.393902	20.190.146.35	10.1.131.225	TCP	1454	443 → 56479 [ACK] Seq=13809 Ack=7330 Win=4194304 Len=1400 [TCP PDU reassembled in 97]
93	15.394044	10.1.131.225	20.190.146.35	TCP	54	56479 → 443 [ACK] Seq=7330 Ack=15209 Win=132352 Len=0
94	15.394612	20.190.146.35	10.1.131.225	TCP	1454	443 → 56479 [ACK] Seq=15209 Ack=7330 Win=4194304 Len=1400 [TCP PDU reassembled in 97]
95	15.394612	20.190.146.35	10.1.131.225	TCP	1454	443 → 56479 [ACK] Seq=16609 Ack=7330 Win=4194304 Len=1400 [TCP PDU reassembled in 97]
96	15.394612	20.190.146.35	10.1.131.225	TCP	1454	443 → 56479 [ACK] Seq=18009 Ack=7330 Win=4194304 Len=1400 [TCP PDU reassembled in 97]

