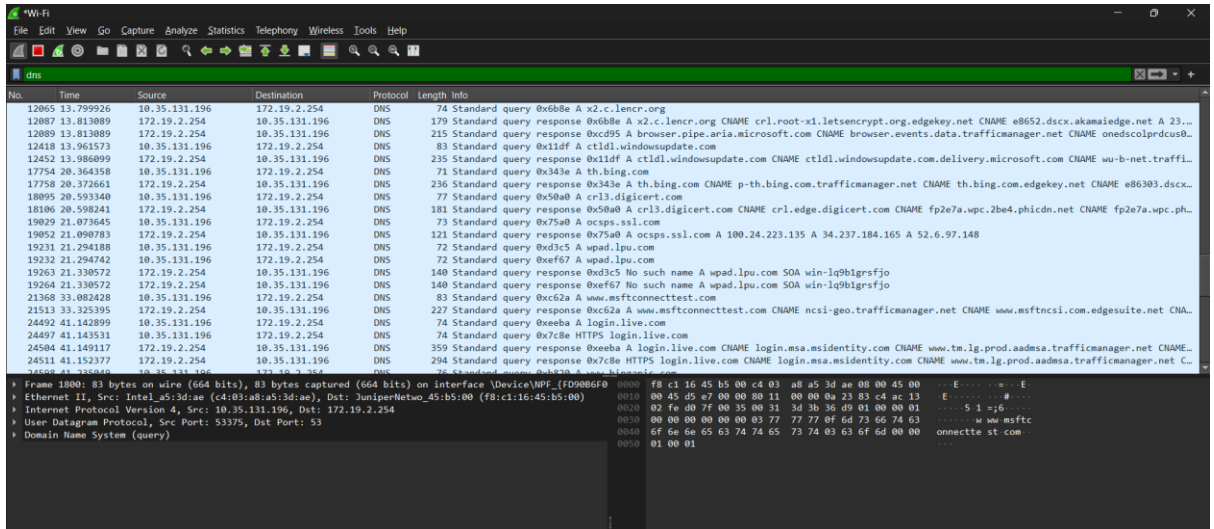
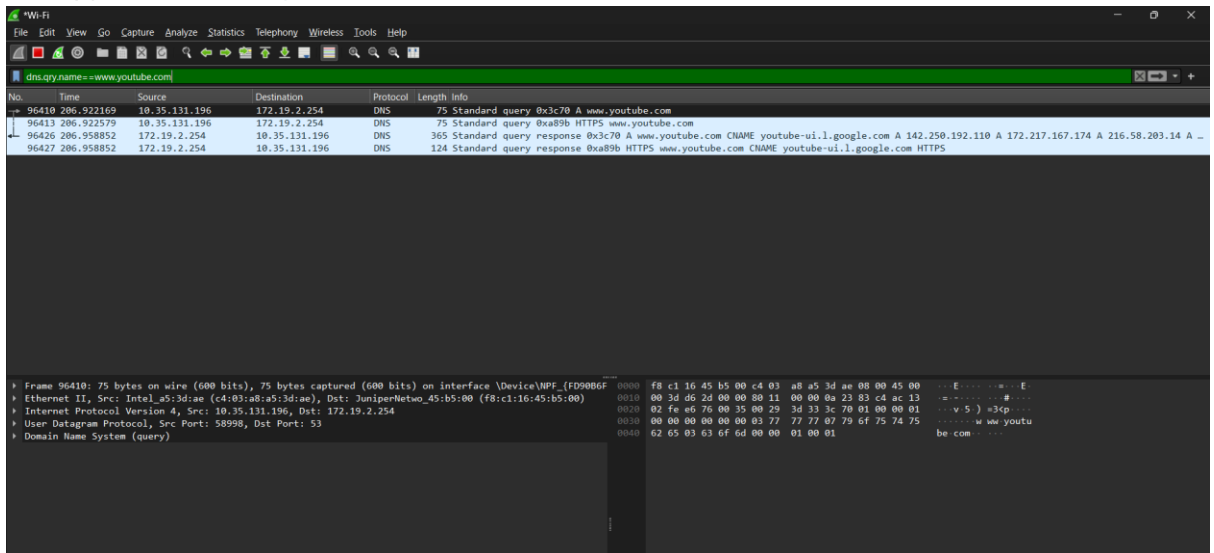


1. Dns



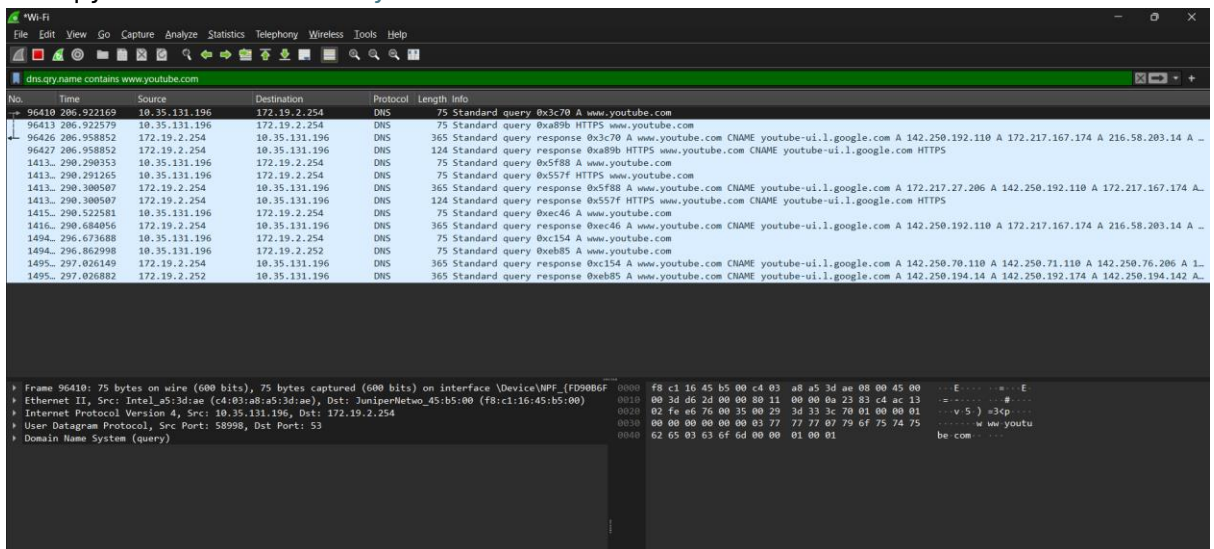
No.	Time	Source	Destination	Protocol	Length	Info
12065	13.799926	10.35.131.196	172.19.2.254	DNS	74	Standard query 0x6b8e A x2.c.lencr.org
12087	13.813089	172.19.2.254	10.35.131.196	DNS	179	Standard query response 0x6b8e A x2.c.lencr.org CNAME crl.root-x1.letsencrypt.org.edgekey.net CNAME e8652.dscx.akamaiedge.net A 23...
12089	13.813089	172.19.2.254	10.35.131.196	DNS	215	Standard query response 0xc095 A browser.pipe.aria.microsoft.com CNAME browser.events.data.trafficmanager.net CNAME onedscolprdcus0...
12418	13.961573	10.35.131.196	172.19.2.254	DNS	83	Standard query 0x11df A ctld1.windowsupdate.com
12452	13.966099	172.19.2.254	10.35.131.196	DNS	235	Standard query response 0x11df A ctld1.windowsupdate.com CNAME ctld1.windowsupdate.com.delivery.microsoft.com CNAME wu-b-net-traffic...
17754	20.364358	10.35.131.196	172.19.2.254	DNS	71	Standard query 0x343e A th.bing.com
17758	20.372661	172.19.2.254	10.35.131.196	DNS	236	Standard query response 0x343e A th.bing.com CNAME p-th.bing.com.trafficmanager.net CNAME th.bing.com.edgekey.net CNAME e86303.dscx...
18095	20.593340	10.35.131.196	172.19.2.254	DNS	77	Standard query 0x50a0 A crl3.digicert.com
18106	20.598241	172.19.2.254	10.35.131.196	DNS	181	Standard query response 0x50a0 A crl3.digicert.com CNAME crl.edge.digicert.com CNAME fp2e7a.upc.2be4.phicdn.net CNAME fp2e7a.upc.ph...
19029	21.073645	10.35.131.196	172.19.2.254	DNS	73	Standard query 0x75a0 A ocsp.ssl.com
19052	21.090783	172.19.2.254	10.35.131.196	DNS	121	Standard query response 0x75a0 A ocsp.ssl.com A 100.24.223.135 A 34.237.184.105 A 52.6.97.148
19231	21.294188	10.35.131.196	172.19.2.254	DNS	72	Standard query 0xd3c5 A upad.lpu.com
19232	21.294742	10.35.131.196	172.19.2.254	DNS	72	Standard query 0xef67 A upad.lpu.com
19263	21.330572	172.19.2.254	10.35.131.196	DNS	140	Standard query response 0xd3c5 No such name A upad.lpu.com SOA win-lq9lgrsfjo
19264	21.330572	172.19.2.254	10.35.131.196	DNS	140	Standard query response 0xef67 No such name A upad.lpu.com SOA win-lq9lgrsfjo
21368	33.082428	10.35.131.196	172.19.2.254	DNS	83	Standard query 0xc62a A www.msftconnecttest.com
21513	33.325395	172.19.2.254	10.35.131.196	DNS	227	Standard query response 0xc62a A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNA...
24492	41.142899	10.35.131.196	172.19.2.254	DNS	74	Standard query 0xe0ba A login.live.com
24497	41.143531	10.35.131.196	172.19.2.254	DNS	74	Standard query 0x7c8e HTTPS login.live.com
24504	41.149117	172.19.2.254	10.35.131.196	DNS	359	Standard query response 0xe0ba A login.live.com CNAME login.msa.msidentity.com CNAME www.tm.lg.prod.aadmsa.trafficmanager.net CNAME...
24511	41.152377	172.19.2.254	10.35.131.196	DNS	294	Standard query response 0x7c8e HTTPS login.live.com CNAME login.msa.msidentity.com CNAME www.tm.lg.prod.aadmsa.trafficmanager.net C...

2. Dns qry.name==www.youtube.com



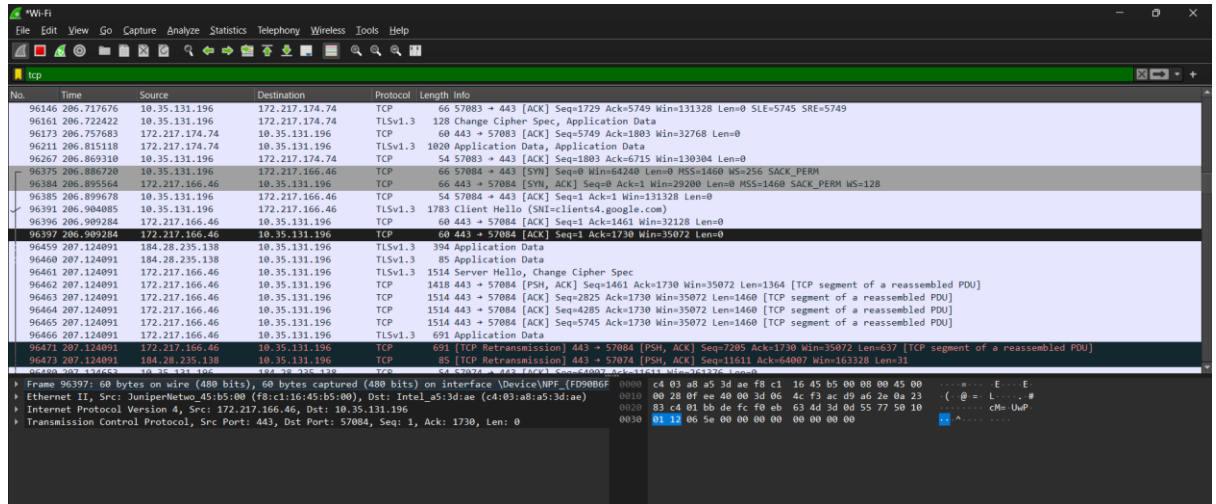
No.	Time	Source	Destination	Protocol	Length	Info
96410	206.922169	10.35.131.196	172.19.2.254	DNS	75	Standard query 0x3c70 A www.youtube.com
96413	206.922579	10.35.131.196	172.19.2.254	DNS	75	Standard query response 0x3c70 A www.youtube.com CNAME youtube-ui.l.google.com A 142.250.192.110 A 172.217.167.174 A 216.58.203.14 A ...
96426	206.958852	172.19.2.254	10.35.131.196	DNS	365	Standard query response 0x3c70 A www.youtube.com CNAME youtube-ui.l.google.com A 142.250.192.110 A 172.217.167.174 A 216.58.203.14 A ...
96427	206.958852	172.19.2.254	10.35.131.196	DNS	124	Standard query response 0xa89b HTTPS www.youtube.com CNAME youtube-ui.l.google.com HTTPS

3. Dns qry.name contains www.youtube.com



No.	Time	Source	Destination	Protocol	Length	Info
96410	206.922169	10.35.131.196	172.19.2.254	DNS	75	Standard query 0x3c70 A www.youtube.com
96413	206.922579	10.35.131.196	172.19.2.254	DNS	75	Standard query response 0xa89b HTTPS www.youtube.com CNAME youtube-ui.l.google.com A 142.250.192.110 A 172.217.167.174 A 216.58.203.14 A ...
96426	206.958852	172.19.2.254	10.35.131.196	DNS	365	Standard query response 0x3c70 A www.youtube.com CNAME youtube-ui.l.google.com A 142.250.192.110 A 172.217.167.174 A 216.58.203.14 A ...
96427	206.958852	172.19.2.254	10.35.131.196	DNS	124	Standard query response 0xa89b HTTPS www.youtube.com CNAME youtube-ui.l.google.com HTTPS
1413.	200.290353	10.35.131.196	172.19.2.254	DNS	75	Standard query 0x5f88 A www.youtube.com
1413.	200.291265	10.35.131.196	172.19.2.254	DNS	75	Standard query 0x557f HTTPS www.youtube.com
1413.	200.300507	172.19.2.254	10.35.131.196	DNS	365	Standard query response 0x5f88 A www.youtube.com CNAME youtube-ui.l.google.com A 172.217.27.206 A 142.250.192.110 A 172.217.167.174 A ...
1413.	200.300507	172.19.2.254	10.35.131.196	DNS	124	Standard query response 0x557f HTTPS www.youtube.com CNAME youtube-ui.l.google.com HTTPS
1415.	200.522581	10.35.131.196	172.19.2.254	DNS	75	Standard query 0xec46 A www.youtube.com
1416.	200.684056	172.19.2.254	10.35.131.196	DNS	365	Standard query response 0xec46 A www.youtube.com CNAME youtube-ui.l.google.com A 142.250.192.110 A 172.217.167.174 A 216.58.203.14 A ...
1494.	206.673608	10.35.131.196	172.19.2.254	DNS	75	Standard query 0xc154 A www.youtube.com
1494.	206.862988	10.35.131.196	172.19.2.252	DNS	75	Standard query 0xeb85 A www.youtube.com
1495.	297.026149	172.19.2.254	10.35.131.196	DNS	365	Standard query response 0xc154 A www.youtube.com CNAME youtube-ui.l.google.com A 142.250.70.110 A 142.250.71.110 A 142.250.76.206 A 1...
1495.	297.026882	172.19.2.252	10.35.131.196	DNS	365	Standard query response 0xeb85 A www.youtube.com CNAME youtube-ui.l.google.com A 142.250.194.14 A 142.250.192.174 A 142.250.194.142 A ...

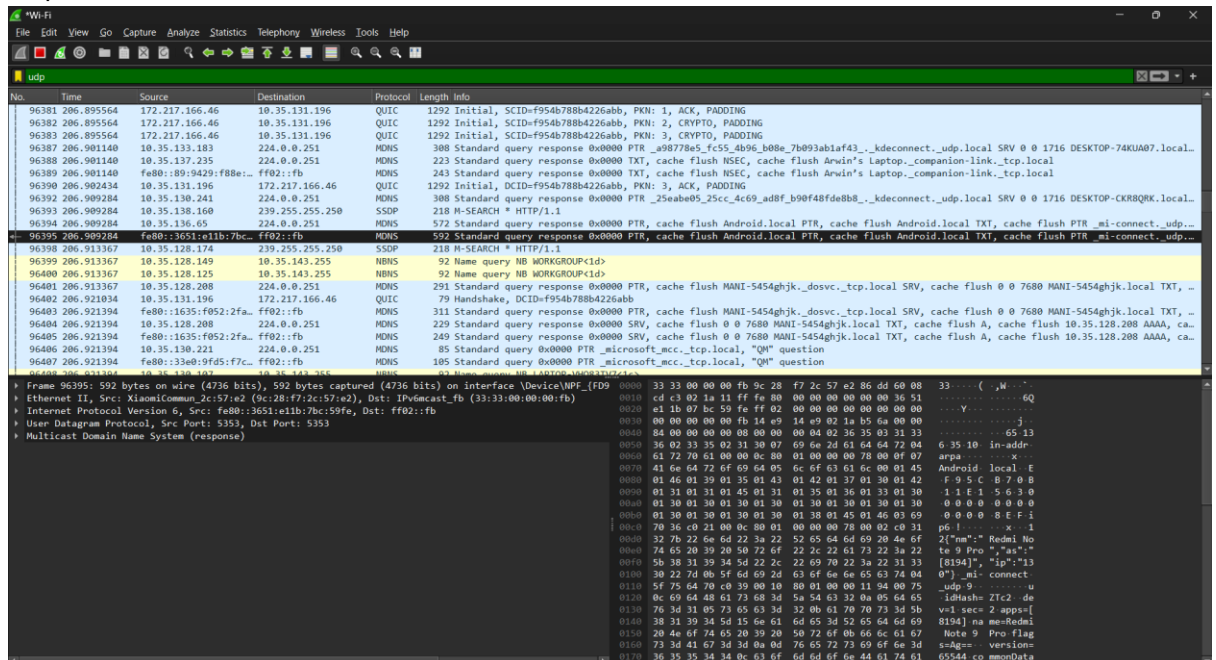
4. Tcp



The screenshot shows a Wireshark capture of TCP traffic. The packet list on the left shows several packets, with packet 96397 selected. The packet details pane on the right shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
96146	206.717676	10.35.131.196	172.217.174.74	TCP	66	57083 → 443 [ACK] Seq=1729 Ack=5749 Win=131328 Len=0 SLE=5745 SRE=5749
96161	206.722422	10.35.131.196	172.217.174.74	TLSv1.3	128	Change Cipher Spec, Application Data
96173	206.757683	172.217.174.74	10.35.131.196	TCP	60	443 → 57083 [ACK] Seq=5749 Ack=1803 Win=32768 Len=0
96211	206.815118	172.217.174.74	10.35.131.196	TLSv1.3	1020	Application Data, Application Data
96267	206.869310	10.35.131.196	172.217.174.74	TCP	54	57083 → 443 [ACK] Seq=1803 Ack=6715 Win=130304 Len=0
96375	206.889720	10.35.131.196	172.217.166.46	TCP	66	57084 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
96384	206.895564	172.217.166.46	10.35.131.196	TCP	66	443 → 57084 [SYN, ACK] Seq=0 Ack=1 Win=29280 Len=0 MSS=1460 SACK_PERM WS=128
96385	206.899678	10.35.131.196	172.217.166.46	TCP	54	57084 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
96391	206.904085	10.35.131.196	172.217.166.46	TLSv1.3	1783	Client Hello (SNI=clients4.google.com)
96396	206.909284	172.217.166.46	10.35.131.196	TCP	60	443 → 57084 [ACK] Seq=1 Ack=1463 Win=32128 Len=0
96397	206.909284	172.217.166.46	10.35.131.196	TCP	60	443 → 57084 [ACK] Seq=1 Ack=1730 Win=35072 Len=0
96459	207.124091	184.28.235.138	10.35.131.196	TLSv1.3	394	Application Data
96460	207.124091	184.28.235.138	10.35.131.196	TLSv1.3	85	Application Data
96461	207.124091	172.217.166.46	10.35.131.196	TLSv1.3	1514	Server Hello, Change Cipher Spec
96462	207.124091	172.217.166.46	10.35.131.196	TCP	1418	443 → 57084 [PSH, ACK] Seq=1461 Ack=1730 Win=35072 Len=1364 [TCP segment of a reassembled PDU]
96463	207.124091	172.217.166.46	10.35.131.196	TCP	1514	443 → 57084 [ACK] Seq=2825 Ack=1730 Win=35072 Len=1460 [TCP segment of a reassembled PDU]
96464	207.124091	172.217.166.46	10.35.131.196	TCP	1514	443 → 57084 [ACK] Seq=4285 Ack=1730 Win=35072 Len=1460 [TCP segment of a reassembled PDU]
96465	207.124091	172.217.166.46	10.35.131.196	TCP	1514	443 → 57084 [ACK] Seq=5745 Ack=1730 Win=35072 Len=1460 [TCP segment of a reassembled PDU]
96466	207.124091	172.217.166.46	10.35.131.196	TLSv1.3	691	Application Data
96471	207.124091	172.217.166.46	10.35.131.196	TCP	691	[TCP Retransmission] 443 → 57084 [PSH, ACK] Seq=7205 Ack=1730 Win=35072 Len=637 [TCP segment of a reassembled PDU]
96472	207.124091	184.28.235.138	10.35.131.196	TCP	85	[TCP Retransmission] 443 → 57074 [PSH, ACK] Seq=11611 Ack=64007 Win=163328 Len=31

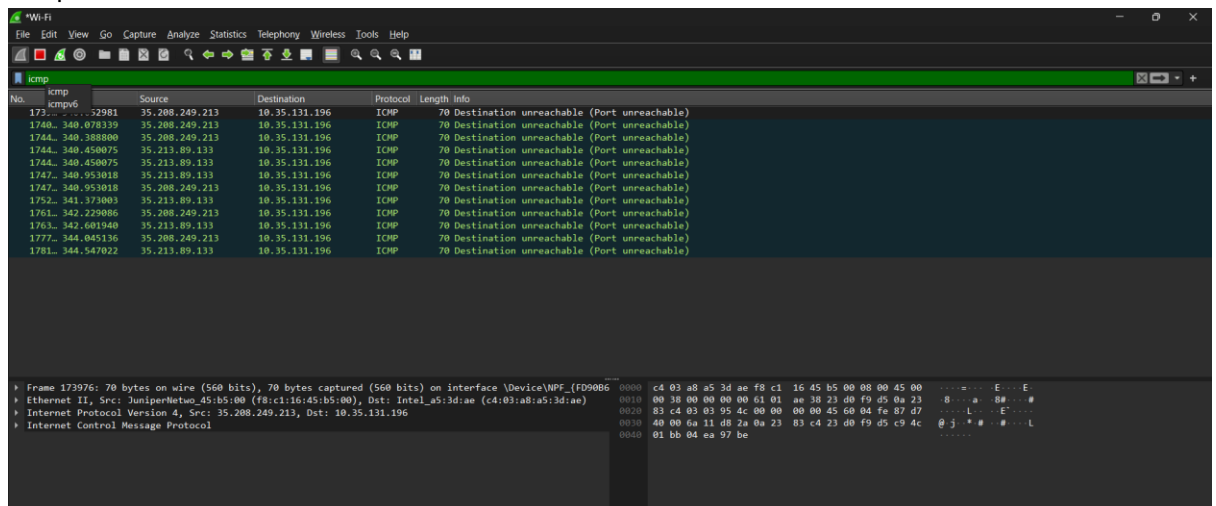
5. Udp



The screenshot shows a Wireshark capture of UDP traffic. The packet list on the left shows several packets, with packet 96395 selected. The packet details pane on the right shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and User Datagram Protocol. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
96381	206.895564	172.217.166.46	10.35.131.196	QUIC	1292	Initial, SCID=F954b788b4226abb, PKN: 1, ACK, PADDING
96382	206.895564	172.217.166.46	10.35.131.196	QUIC	1292	Initial, SCID=F954b788b4226abb, PKN: 2, CRYPTO, PADDING
96383	206.895564	172.217.166.46	10.35.131.196	QUIC	1292	Initial, SCID=F954b788b4226abb, PKN: 3, CRYPTO, PADDING
96387	206.901140	10.35.133.183	224.0.0.251	MDNS	308	Standard query response 0x0000 PTR _a98778a5_fc55_4b96_b08e_7b093abfa43_._kdeconnect_udp.local SRV 0 0 1716 DESKTOP-74XU07.local..
96388	206.901140	10.35.137.235	224.0.0.251	MDNS	223	Standard query response 0x0000 TXT, cache flush HSEC, cache flush Arwin's Laptop_companion-link_tcp.local
96389	206.901140	f80b:1635:f852:2fa::f	ff02::fb	MDNS	243	Standard query response 0x0000 TXT, cache flush HSEC, cache flush Arwin's Laptop_companion-link_tcp.local
96390	206.902434	10.35.131.196	172.217.166.46	QUIC	1292	Initial, DCID=F954b788b4226abb, PKN: 3, ACK, PADDING
96392	206.909284	10.35.130.241	224.0.0.251	MDNS	308	Standard query response 0x0000 PTR _25eab05_25cc_4c69_adbf_b90f48fde8b8_._kdeconnect_udp.local SRV 0 0 1716 DESKTOP-CRR8QRK.local..
96393	206.909284	10.35.138.160	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
96394	206.909284	10.35.136.65	224.0.0.251	MDNS	572	Standard query response 0x0000 PTR, cache flush Android.local PTR, cache flush Android.local TXT, cache flush PTR_mi-connect_udp...
96395	206.909284	f80b:1635:f852:2fa::f	ff02::fb	MDNS	592	Standard query response 0x0000 PTR, cache flush Android.local PTR, cache flush Android.local TXT, cache flush PTR_mi-connect_udp...
96398	206.913367	10.35.128.174	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
96399	206.913367	10.35.128.149	10.35.143.255	NBNS	92	Name query NB WORKGROUP<id>
96400	206.913367	10.35.128.125	10.35.143.255	NBNS	92	Name query NB WORKGROUP<id>
96401	206.913367	10.35.128.208	224.0.0.251	MDNS	291	Standard query response 0x0000 PTR, cache flush MANI-5454ghjk._dosvc_tcp.local SRV, cache flush 0 0 7680 MANI-5454ghjk.local TXT, _
96402	206.921034	10.35.131.196	172.217.166.46	QUIC	79	Handshake, DCID=F954b788b4226abb
96403	206.921394	f80b:1635:f852:2fa::f	ff02::fb	MDNS	311	Standard query response 0x0000 PTR, cache flush MANI-5454ghjk._dosvc_tcp.local SRV, cache flush 0 0 7680 MANI-5454ghjk.local TXT, _
96404	206.921394	10.35.128.208	224.0.0.251	MDNS	229	Standard query response 0x0000 SRV, cache flush 0 0 7680 MANI-5454ghjk.local TXT, cache flush A, cache flush 10.35.128.208 AAAA, ca..
96405	206.921394	f80b:1635:f852:2fa::f	ff02::fb	MDNS	249	Standard query response 0x0000 SRV, cache flush 0 0 7680 MANI-5454ghjk.local TXT, cache flush A, cache flush 10.35.128.208 AAAA, ca..
96406	206.921394	10.35.130.221	224.0.0.251	MDNS	85	Standard query 0x0000 PTR_microsoft_mcc_tcp.local, "QM" question
96407	206.921394	f80b:1635:f852:2fa::f	ff02::fb	MDNS	105	Standard query 0x0000 PTR_microsoft_mcc_tcp.local, "QM" question

6. Icmp



The screenshot shows a Wireshark capture of ICMP traffic. The packet list on the left shows several packets, with packet 173 selected. The packet details pane on the right shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
173	...	35.208.249.213	10.35.131.196	ICMP	70	Destination unreachable (Port unreachable)
1740	...	35.208.249.213	10.35.131.196	ICMP	70	Destination unreachable (Port unreachable)
1744	...	35.208.249.213	10.35.131.196	ICMP	70	Destination unreachable (Port unreachable)
1744	...	35.213.89.133	10.35.131.196	ICMP	70	Destination unreachable (Port unreachable)
1744	...	35.213.89.133	10.35.131.196	ICMP	70	Destination unreachable (Port unreachable)
1747	...	35.213.89.133	10.35.131.196	ICMP	70	Destination unreachable (Port unreachable)
1747	...	35.208.249.213	10.35.131.196	ICMP	70	Destination unreachable (Port unreachable)
1752	...	35.213.89.133	10.35.131.196	ICMP	70	Destination unreachable (Port unreachable)
1761	...	35.208.249.213	10.35.131.196	ICMP	70	Destination unreachable (Port unreachable)
1763	...	35.213.89.133	10.35.131.196	ICMP	70	Destination unreachable (Port unreachable)
1777	...	35.208.249.213	10.35.131.196	ICMP	70	Destination unreachable (Port unreachable)
1781	...	35.213.89.133	10.35.131.196	ICMP	70	Destination unreachable (Port unreachable)

