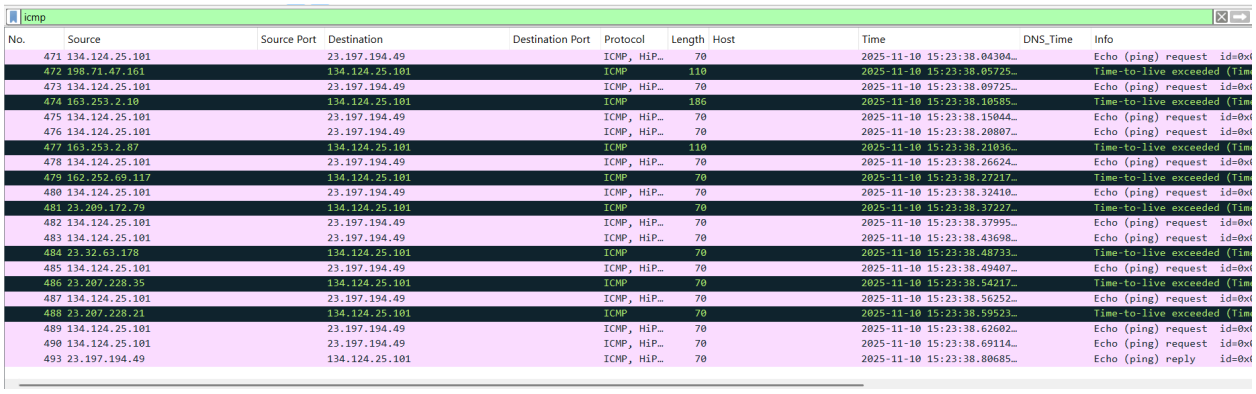
Lab Assignment 3

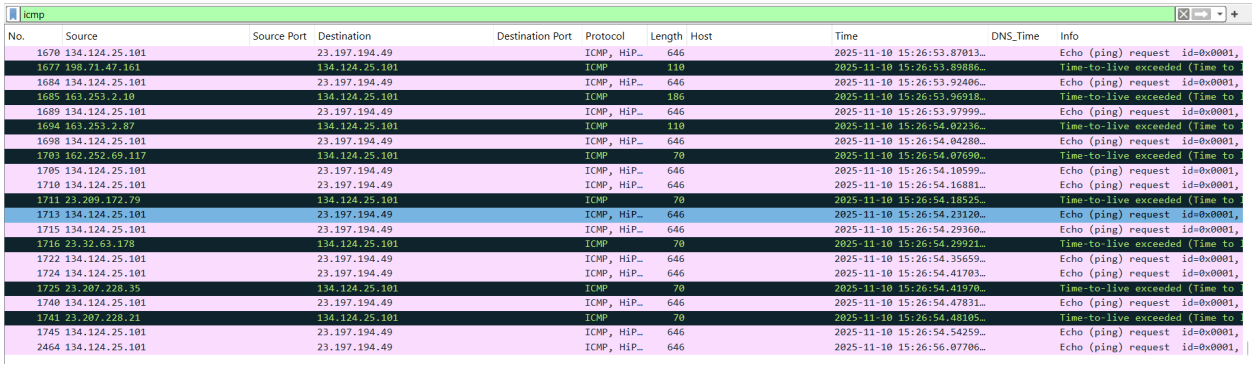
Trace56:



icmp

No.	Source	Source Port	Destination	Destination Port	Protocol	Length	Host	Time	DNS_Time	Info
471	134.124.25.101		23.197.194.49		ICMP, HiP…	70		2025-11-10 15:23:38.04304…		Echo (ping) request id=0x
472	198.71.47.161		134.124.25.101		ICMP	110		2025-11-10 15:23:38.05725…		Time-to-live exceeded (Tim
473	134.124.25.101		23.197.194.49		ICMP, HiP…	70		2025-11-10 15:23:38.09725…		Echo (ping) request id=0x
474	163.253.2.10		134.124.25.101		ICMP	186		2025-11-10 15:23:38.10585…		Time-to-live exceeded (Tim
475	134.124.25.101		23.197.194.49		ICMP, HiP…	70		2025-11-10 15:23:38.15044…		Echo (ping) request id=0x
476	134.124.25.101		23.197.194.49		ICMP, HiP…	70		2025-11-10 15:23:38.20807…		Echo (ping) request id=0x
477	163.253.2.87		134.124.25.101		ICMP	110		2025-11-10 15:23:38.21036…		Time-to-live exceeded (Tim
478	134.124.25.101		23.197.194.49		ICMP, HiP…	70		2025-11-10 15:23:38.26624…		Echo (ping) request id=0x
479	162.252.69.117		134.124.25.101		ICMP	70		2025-11-10 15:23:38.27217…		Time-to-live exceeded (Tim
480	134.124.25.101		23.197.194.49		ICMP, HiP…	70		2025-11-10 15:23:38.32410…		Echo (ping) request id=0x
481	23.209.172.79		134.124.25.101		ICMP	70		2025-11-10 15:23:38.37227…		Time-to-live exceeded (Tim
482	134.124.25.101		23.197.194.49		ICMP, HiP…	70		2025-11-10 15:23:38.37995…		Echo (ping) request id=0x
483	134.124.25.101		23.197.194.49		ICMP, HiP…	70		2025-11-10 15:23:38.43698…		Echo (ping) request id=0x
484	23.32.63.178		134.124.25.101		ICMP	70		2025-11-10 15:23:38.48733…		Time-to-live exceeded (Tim
485	134.124.25.101		23.197.194.49		ICMP, HiP…	70		2025-11-10 15:23:38.49407…		Echo (ping) request id=0x
486	23.207.228.35		134.124.25.101		ICMP	70		2025-11-10 15:23:38.54217…		Time-to-live exceeded (Tim
487	134.124.25.101		23.197.194.49		ICMP, HiP…	70		2025-11-10 15:23:38.56252…		Echo (ping) request id=0x
488	23.207.228.21		134.124.25.101		ICMP	70		2025-11-10 15:23:38.59523…		Time-to-live exceeded (Tim
489	134.124.25.101		23.197.194.49		ICMP, HiP…	70		2025-11-10 15:23:38.62602…		Echo (ping) request id=0x
490	134.124.25.101		23.197.194.49		ICMP, HiP…	70		2025-11-10 15:23:38.69114…		Echo (ping) request id=0x
493	23.197.194.49		134.124.25.101		ICMP, HiP…	70		2025-11-10 15:23:38.80685…		Echo (ping) reply id=0x

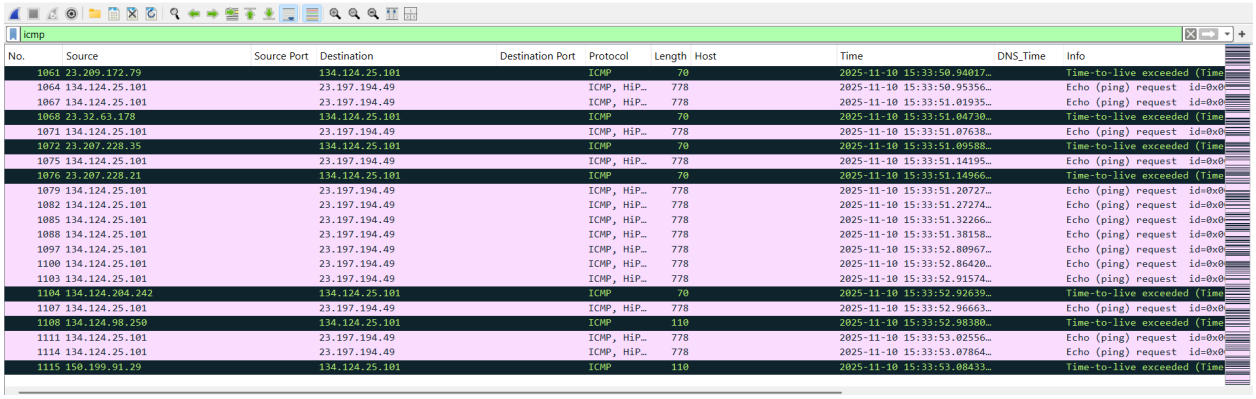
Trace2000:



icmp

No.	Source	Source Port	Destination	Destination Port	Protocol	Length	Host	Time	DNS_Time	Info
1670	134.124.25.101		23.197.194.49		ICMP, HiP…	646		2025-11-10 15:26:53.87013…		Echo (ping) request id=0x0001,
1677	198.71.47.161		134.124.25.101		ICMP	110		2025-11-10 15:26:53.89886…		Time-to-live exceeded (Time to
1684	134.124.25.101		23.197.194.49		ICMP, HiP…	646		2025-11-10 15:26:53.92406…		Echo (ping) request id=0x0001,
1685	163.253.2.10		134.124.25.101		ICMP	186		2025-11-10 15:26:53.96918…		Time-to-live exceeded (Time to
1689	134.124.25.101		23.197.194.49		ICMP, HiP…	646		2025-11-10 15:26:53.97999…		Echo (ping) request id=0x0001,
1694	163.253.2.87		134.124.25.101		ICMP	110		2025-11-10 15:26:54.02236…		Time-to-live exceeded (Time to
1698	134.124.25.101		23.197.194.49		ICMP, HiP…	646		2025-11-10 15:26:54.04280…		Echo (ping) request id=0x0001,
1703	162.252.69.117		134.124.25.101		ICMP	70		2025-11-10 15:26:54.07690…		Time-to-live exceeded (Time to
1705	134.124.25.101		23.197.194.49		ICMP, HiP…	646		2025-11-10 15:26:54.10599…		Echo (ping) request id=0x0001,
1710	134.124.25.101		23.197.194.49		ICMP, HiP…	646		2025-11-10 15:26:54.16881…		Echo (ping) request id=0x0001,
1711	23.209.172.79		134.124.25.101		ICMP	70		2025-11-10 15:26:54.18525…		Time-to-live exceeded (Time to
1713	134.124.25.101		23.197.194.49		ICMP, HiP…	646		2025-11-10 15:26:54.23120…		Echo (ping) request id=0x0001,
1715	134.124.25.101		23.197.194.49		ICMP, HiP…	646		2025-11-10 15:26:54.29360…		Echo (ping) request id=0x0001,
1716	23.32.63.178		134.124.25.101		ICMP	70		2025-11-10 15:26:54.29921…		Time-to-live exceeded (Time to
1722	134.124.25.101		23.197.194.49		ICMP, HiP…	646		2025-11-10 15:26:54.35659…		Echo (ping) request id=0x0001,
1724	134.124.25.101		23.197.194.49		ICMP, HiP…	646		2025-11-10 15:26:54.41703…		Echo (ping) request id=0x0001,
1725	23.207.228.35		134.124.25.101		ICMP	70		2025-11-10 15:26:54.41970…		Time-to-live exceeded (Time to
1740	134.124.25.101		23.197.194.49		ICMP, HiP…	646		2025-11-10 15:26:54.47831…		Echo (ping) request id=0x0001,
1741	23.207.228.21		134.124.25.101		ICMP	70		2025-11-10 15:26:54.48105…		Time-to-live exceeded (Time to
1745	134.124.25.101		23.197.194.49		ICMP, HiP…	646		2025-11-10 15:26:54.54259…		Echo (ping) request id=0x0001,
2464	134.124.25.101		23.197.194.49		ICMP, HiP…	646		2025-11-10 15:26:56.07706…		Echo (ping) request id=0x0001,

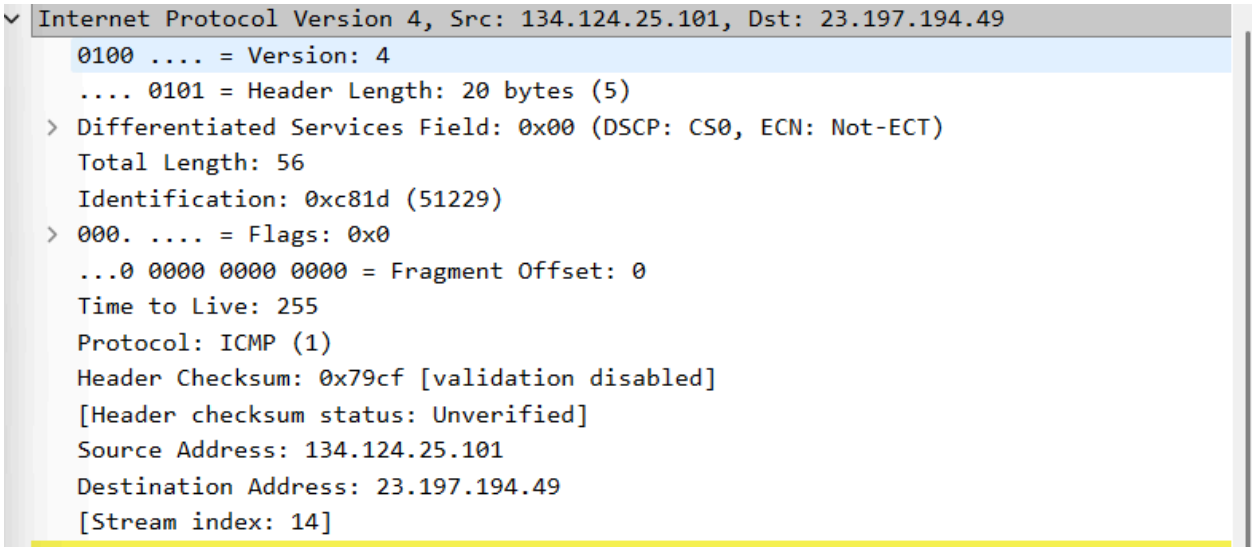
Trace3500:



icmp

No.	Source	Source Port	Destination	Destination Port	Protocol	Length	Host	Time	DNS_Time	Info
1061	23.209.172.79		134.124.25.101		ICMP	70		2025-11-10 15:33:50.94017…		Time-to-live exceeded (Time
1064	134.124.25.101		23.197.194.49		ICMP, HiP…	778		2025-11-10 15:33:50.95356…		Echo (ping) request id=0x0
1067	134.124.25.101		23.197.194.49		ICMP, HiP…	778		2025-11-10 15:33:51.01935…		Echo (ping) request id=0x0
1068	23.32.63.178		134.124.25.101		ICMP	70		2025-11-10 15:33:51.04730…		Time-to-live exceeded (Time
1071	134.124.25.101		23.197.194.49		ICMP, HiP…	778		2025-11-10 15:33:51.07638…		Echo (ping) request id=0x0
1072	23.207.228.35		134.124.25.101		ICMP	70		2025-11-10 15:33:51.09588…		Time-to-live exceeded (Time
1075	134.124.25.101		23.197.194.49		ICMP, HiP…	778		2025-11-10 15:33:51.14195…		Echo (ping) request id=0x0
1076	23.207.228.21		134.124.25.101		ICMP	70		2025-11-10 15:33:51.14966…		Time-to-live exceeded (Time
1079	134.124.25.101		23.197.194.49		ICMP, HiP…	778		2025-11-10 15:33:51.20727…		Echo (ping) request id=0x0
1082	134.124.25.101		23.197.194.49		ICMP, HiP…	778		2025-11-10 15:33:51.27274…		Echo (ping) request id=0x0
1085	134.124.25.101		23.197.194.49		ICMP, HiP…	778		2025-11-10 15:33:51.32266…		Echo (ping) request id=0x0
1088	134.124.25.101		23.197.194.49		ICMP, HiP…	778		2025-11-10 15:33:51.38158…		Echo (ping) request id=0x0
1097	134.124.25.101		23.197.194.49		ICMP, HiP…	778		2025-11-10 15:33:52.80967…		Echo (ping) request id=0x0
1100	134.124.25.101		23.197.194.49		ICMP, HiP…	778		2025-11-10 15:33:52.86420…		Echo (ping) request id=0x0
1103	134.124.25.101		23.197.194.49		ICMP, HiP…	778		2025-11-10 15:33:52.91574…		Echo (ping) request id=0x0
1104	134.124.204.242		134.124.25.101		ICMP	70		2025-11-10 15:33:52.92639…		Time-to-live exceeded (Time
1107	134.124.25.101		23.197.194.49		ICMP, HiP…	778		2025-11-10 15:33:52.96663…		Echo (ping) request id=0x0
1108	134.124.98.250		134.124.25.101		ICMP	110		2025-11-10 15:33:52.98380…		Time-to-live exceeded (Time
1111	134.124.25.101		23.197.194.49		ICMP, HiP…	778		2025-11-10 15:33:53.02556…		Echo (ping) request id=0x0
1114	134.124.25.101		23.197.194.49		ICMP, HiP…	778		2025-11-10 15:33:53.07864…		Echo (ping) request id=0x0
1115	150.199.91.29		134.124.25.101		ICMP	110		2025-11-10 15:33:53.08433…		Time-to-live exceeded (Time

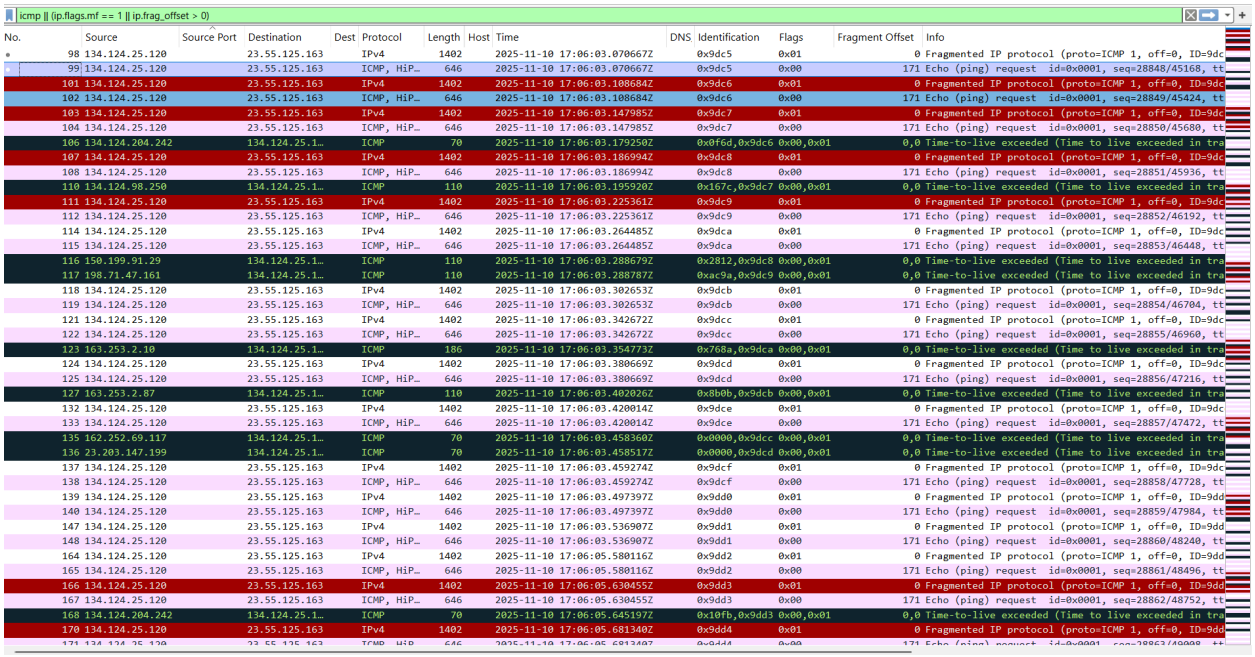
Screenshot for a-c:



a. Protocol: ICMP (1)
b. IP header = 20 bytes
   Payload = 36 bytes
   Determined by subtracting the header length from the total length field in the IP header (56 − 20 = 36).
c. No, this datagram has not been fragmented. You can tell because the Flags field is 0x0 (no fragmentation bits set) and the Fragment Offset is 0.
d. I observed TTL, Identification, and the Header checksum change on every Echo Request as I step through them.
e. Constant: Version, Header Length, Protocol, Source, Destination, Flags, Fragment Offset, DSCP/ECN, and (for the 56-byte run) Total Length.
   Must change: TTL (traceroute increments it to discover each hop), Identification (distinct datagram id for reassembly), and Header checksum (recomputed because header fields changed).
f. The IP ID increases by 1 each Echo Request
g. Identification values: 0x7203, 0x7384, 0x7545, 0x76d7, 0x785c, 0x79d8 … etc.
   TTL = 255
h. The Identification field changes for each ICMP “Time-to-Live exceeded” reply, but the TTL value remains constant at 255.

   This occurs because I was connected through the Cisco AnyConnect Secure Mobility Client, which routes all my traffic through a Cisco VPN gateway. Cisco devices typically use a default initial TTL of 255 for outbound packets, unlike Linux-based routers (which often start at 64) or Windows hosts (which usually start at 128).

Fragmentation:



No.	Source	Source Port	Destination	Dest	Protocol	Length	Host	Time	DNS	Identification	Flags	Fragment Offset	Info
98	134.124.25.120		23.55.125.163		IPv4	1402		2025-11-10 17:06:03.070667Z		0x9dc5	0x01	0	Fragmented IP protocol (proto=ICMP 1, off=0, ID=9dc
99	134.124.25.120		23.55.125.163		ICMP, HiP…	646		2025-11-10 17:06:03.070667Z		0x9dc5	0x00	171	Echo (ping) request id=0x0001, seq=28848/45168, tt
101	134.124.25.120		23.55.125.163		IPv4	1402		2025-11-10 17:06:03.108684Z		0x9dc6	0x01	0	Fragmented IP protocol (proto=ICMP 1, off=0, ID=9dc
102	134.124.25.120		23.55.125.163		ICMP, HiP…	646		2025-11-10 17:06:03.108684Z		0x9dc6	0x00	171	Echo (ping) request id=0x0001, seq=28849/45424, tt
103	134.124.25.120		23.55.125.163		IPv4	1402		2025-11-10 17:06:03.147985Z		0x9dc7	0x01	0	Fragmented IP protocol (proto=ICMP 1, off=0, ID=9dc
104	134.124.25.120		23.55.125.163		ICMP, HiP…	646		2025-11-10 17:06:03.147985Z		0x9dc7	0x00	171	Echo (ping) request id=0x0001, seq=28850/45680, tt
106	134.124.204.242		134.124.25.1…		ICMP	70		2025-11-10 17:06:03.179250Z		0x0f6d,0x9dc6	0x00,0x01	0,0	Time-to-live exceeded (Time to live exceeded in tra
107	134.124.25.120		23.55.125.163		IPv4	1402		2025-11-10 17:06:03.186994Z		0x9dc8	0x01	0	Fragmented IP protocol (proto=ICMP 1, off=0, ID=9dc
108	134.124.25.120		23.55.125.163		ICMP, HiP…	646		2025-11-10 17:06:03.186994Z		0x9dc8	0x00	171	Echo (ping) request id=0x0001, seq=28851/45936, tt
110	134.124.98.250		134.124.25.1…		ICMP	110		2025-11-10 17:06:03.195920Z		0x167c,0x9dc7	0x00,0x01	0,0	Time-to-live exceeded (Time to live exceeded in tra
111	134.124.25.120		23.55.125.163		IPv4	1402		2025-11-10 17:06:03.225361Z		0x9dc9	0x01	0	Fragmented IP protocol (proto=ICMP 1, off=0, ID=9dc
112	134.124.25.120		23.55.125.163		ICMP, HiP…	646		2025-11-10 17:06:03.225361Z		0x9dc9	0x00	171	Echo (ping) request id=0x0001, seq=28852/46192, tt
114	134.124.25.120		23.55.125.163		IPv4	1402		2025-11-10 17:06:03.264485Z		0x9dca	0x01	0	Fragmented IP protocol (proto=ICMP 1, off=0, ID=9dc
115	134.124.25.120		23.55.125.163		ICMP, HiP…	646		2025-11-10 17:06:03.264485Z		0x9dca	0x00	171	Echo (ping) request id=0x0001, seq=28853/46448, tt
116	150.199.91.29		134.124.25.1…		ICMP	110		2025-11-10 17:06:03.288679Z		0x2812,0x9dc8	0x00,0x01	0,0	Time-to-live exceeded (Time to live exceeded in tra
117	198.71.47.161		134.124.25.1…		ICMP	110		2025-11-10 17:06:03.288787Z		0xac9a,0x9dc9	0x00,0x01	0,0	Time-to-live exceeded (Time to live exceeded in tra
118	134.124.25.120		23.55.125.163		IPv4	1402		2025-11-10 17:06:03.302653Z		0x9dcb	0x01	0	Fragmented IP protocol (proto=ICMP 1, off=0, ID=9dc
119	134.124.25.120		23.55.125.163		ICMP, HiP…	646		2025-11-10 17:06:03.302653Z		0x9dcb	0x00	171	Echo (ping) request id=0x0001, seq=28854/46704, tt
121	134.124.25.120		23.55.125.163		IPv4	1402		2025-11-10 17:06:03.342672Z		0x9dcc	0x01	0	Fragmented IP protocol (proto=ICMP 1, off=0, ID=9dc
122	134.124.25.120		23.55.125.163		ICMP, HiP…	646		2025-11-10 17:06:03.342672Z		0x9dcc	0x00	171	Echo (ping) request id=0x0001, seq=28855/46960, tt
123	163.253.2.10		134.124.25.1…		ICMP	186		2025-11-10 17:06:03.354773Z		0x768a,0x9dca	0x00,0x01	0,0	Time-to-live exceeded (Time to live exceeded in tra
124	134.124.25.120		23.55.125.163		IPv4	1402		2025-11-10 17:06:03.380669Z		0x9dcd	0x01	0	Fragmented IP protocol (proto=ICMP 1, off=0, ID=9dc
125	134.124.25.120		23.55.125.163		ICMP, HiP…	646		2025-11-10 17:06:03.380669Z		0x9dcd	0x00	171	Echo (ping) request id=0x0001, seq=28856/47216, tt
127	163.253.2.87		134.124.25.1…		ICMP	110		2025-11-10 17:06:03.402026Z		0x8b0b,0x9dcb	0x00,0x01	0,0	Time-to-live exceeded (Time to live exceeded in tra
132	134.124.25.120		23.55.125.163		IPv4	1402		2025-11-10 17:06:03.420014Z		0x9dce	0x01	0	Fragmented IP protocol (proto=ICMP 1, off=0, ID=9dc
133	134.124.25.120		23.55.125.163		ICMP, HiP…	646		2025-11-10 17:06:03.420014Z		0x9dce	0x00	171	Echo (ping) request id=0x0001, seq=28857/47472, tt
135	162.252.69.117		134.124.25.1…		ICMP	70		2025-11-10 17:06:03.458360Z		0x0000,0x9dcc	0x00,0x01	0,0	Time-to-live exceeded (Time to live exceeded in tra
136	23.203.147.199		134.124.25.1…		ICMP	70		2025-11-10 17:06:03.458517Z		0x0000,0x9dcd	0x00,0x01	0,0	Time-to-live exceeded (Time to live exceeded in tra
137	134.124.25.120		23.55.125.163		IPv4	1402		2025-11-10 17:06:03.459274Z		0x9dcf	0x01	0	Fragmented IP protocol (proto=ICMP 1, off=0, ID=9dc
138	134.124.25.120		23.55.125.163		ICMP, HiP…	646		2025-11-10 17:06:03.459274Z		0x9dcf	0x00	171	Echo (ping) request id=0x0001, seq=28858/47728, tt
139	134.124.25.120		23.55.125.163		IPv4	1402		2025-11-10 17:06:03.497397Z		0x9dd0	0x01	0	Fragmented IP protocol (proto=ICMP 1, off=0, ID=9dd
140	134.124.25.120		23.55.125.163		ICMP, HiP…	646		2025-11-10 17:06:03.497397Z		0x9dd0	0x00	171	Echo (ping) request id=0x0001, seq=28859/47984, tt
147	134.124.25.120		23.55.125.163		IPv4	1402		2025-11-10 17:06:03.536907Z		0x9dd1	0x01	0	Fragmented IP protocol (proto=ICMP 1, off=0, ID=9dd
148	134.124.25.120		23.55.125.163		ICMP, HiP…	646		2025-11-10 17:06:03.536907Z		0x9dd1	0x00	171	Echo (ping) request id=0x0001, seq=28860/48240, tt
164	134.124.25.120		23.55.125.163		IPv4	1402		2025-11-10 17:06:05.580116Z		0x9dd2	0x01	0	Fragmented IP protocol (proto=ICMP 1, off=0, ID=9dd
165	134.124.25.120		23.55.125.163		ICMP, HiP…	646		2025-11-10 17:06:05.580116Z		0x9dd2	0x00	171	Echo (ping) request id=0x0001, seq=28861/48496, tt
166	134.124.25.120		23.55.125.163		IPv4	1402		2025-11-10 17:06:05.630455Z		0x9dd3	0x01	0	Fragmented IP protocol (proto=ICMP 1, off=0, ID=9dd
167	134.124.25.120		23.55.125.163		ICMP, HiP…	646		2025-11-10 17:06:05.630455Z		0x9dd3	0x00	171	Echo (ping) request id=0x0001, seq=28862/48752, tt
168	134.124.204.242		134.124.25.1…		ICMP	70		2025-11-10 17:06:05.645197Z		0x10fb,0x9dd3	0x00,0x01	0,0	Time-to-live exceeded (Time to live exceeded in tra
170	134.124.25.120		23.55.125.163		IPv4	1402		2025-11-10 17:06:05.681340Z		0x9dd4	0x01	0	Fragmented IP protocol (proto=ICMP 1, off=0, ID=9dc

i. Yes, the 2000-byte Echo Request was fragmented across multiple IP datagrams. I observed several packets with the same Identification (e.g., 0x9dc5) and MF=1, along with others having non-zero Fragment Offsets, confirming that the original datagram was split into smaller fragments for transmission.

j. The first fragment (ID 0x9dc5) has Fragment Offset = 0 and More Fragments = Set (MF = 1), which indicates fragmentation. All fragments share the same Identification value, showing that they belong to the same original datagram.

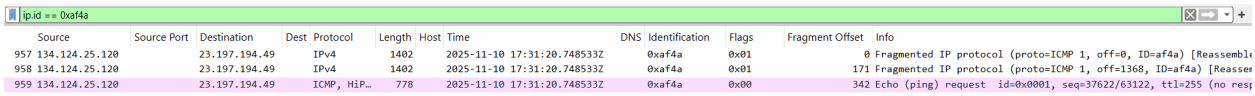
k. The Fragment Offset field indicates a fragment's position:
0 → first fragment
>0 → later fragment

The More Fragments (MF) flag tells whether more fragments follow:
MF = 1 → not the last fragment
MF = 0 → last fragment
All fragments share the same Identification number.

l. Between the first and second fragments of my 2000-byte Echo Request (ID 0x9dc5), the IP header fields that changed were Total Length (1402 → 646 bytes), the More Fragments flag (MF = 1 → 0), the Fragment Offset (0 → 1368), and the Header Checksum (recalculated).
Fields that remained constant included Version 4, IHL 20 bytes, DSCP/ECN 0x00, Identification 0x9dc5, Protocol ICMP (1), TTL 255, and both Source and Destination addresses.

These differences confirm normal IPv4 fragmentation: the first fragment starts at offset 0 and signals more fragments to follow, while the second (last) fragment has a non-zero offset and clears the MF bit.

m. .



	Source	Source Port	Destination	Dest	Protocol	Length	Host	Time	DNS	Identification	Flags	Fragment Offset	Info
957	134.124.25.120		23.197.194.49		IPv4	1402		2025-11-10 17:31:20.748533Z		0xaf4a	0x01	0	Fragmented IP protocol (proto=ICMP 1, off=0, ID=af4a) [Reassembl
958	134.124.25.120		23.197.194.49		IPv4	1402		2025-11-10 17:31:20.748533Z		0xaf4a	0x01	171	Fragmented IP protocol (proto=ICMP 1, off=1368, ID=af4a) [Reasse
959	134.124.25.120		23.197.194.49		ICMP, HiP…	778		2025-11-10 17:31:20.748533Z		0xaf4a	0x00	342	Echo (ping) request id=0x0001, seq=37622/63122, ttl=255 (no resp

For the 3500-byte Echo Request (IP ID = 0xAF4A), Wireshark shows three fragments created from the original datagram.
• The first fragment has Fragment Offset = 0 and MF = 1.
• The second fragment has Fragment Offset = 1368 and MF = 1.
• The final fragment has Fragment Offset = 2736 and MF = 0.
Each fragment carries part of the same ICMP packet (total lengths ≈ 1402, 1402, and 778 bytes).

This three-way split occurs because the Cisco AnyConnect VPN path enforces an MTU of about 1400 bytes; any packet larger than that is automatically fragmented to traverse the VPN tunnel.

2. .
    a. .
    -D <decoy1,decoy2[,ME],...> — Cloaks the scan by injecting spoofed probes from multiple decoy IPs so your real IP is hidden among them.
    -f — Fragments probe packets into smaller pieces to try to evade simple packet filters or IDS signature matching.
    -sS — Performs a fast, “stealth” SYN scan that detects open TCP ports by sending SYNs without completing the TCP handshake.
    -sV — Probes open ports to determine the service and version running on them (useful for patching and triage).
    -O — Attempts OS detection by fingerprinting TCP/IP stack behavior to guess the target’s operating system.
    b. Perform the following:
        i. .

```
C:\Windows\System32>nmap -sS -v 134.124.1.234 -oN nmap_2bi_134.124.1.234.txt
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-10 13:07 -0600
Initiating Ping Scan at 13:07
Scanning 134.124.1.234 [4 ports]
Completed Ping Scan at 13:07, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:07
Completed Parallel DNS resolution of 1 host. at 13:07, 1.53s elapsed
Initiating SYN Stealth Scan at 13:07
Scanning WWW.umsl.edu (134.124.1.234) [1000 ports]
Discovered open port 443/tcp on 134.124.1.234
Discovered open port 80/tcp on 134.124.1.234
Completed SYN Stealth Scan at 13:07, 4.84s elapsed (1000 total ports)
Nmap scan report for WWW.umsl.edu (134.124.1.234)
Host is up (0.036s latency).
Not shown: 995 filtered tcp ports (no-response), 3 filtered tcp ports (host-prohibited)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 6.91 seconds
           Raw packets sent: 2001 (88.020KB) | Rcvd: 44 (4.776KB)
```

ii. .

```
C:\Windows\System32>nmap -sS -v 134.124.1.234 -oN nmap_2bi_134.124.1.234.txt
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-10 13:07 -0600
Initiating Ping Scan at 13:07
Scanning 134.124.1.234 [4 ports]
Completed Ping Scan at 13:07, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:07
Completed Parallel DNS resolution of 1 host. at 13:07, 1.53s elapsed
Initiating SYN Stealth Scan at 13:07
Scanning WWW.umsl.edu (134.124.1.234) [1000 ports]
Discovered open port 443/tcp on 134.124.1.234
Discovered open port 80/tcp on 134.124.1.234
Completed SYN Stealth Scan at 13:07, 4.84s elapsed (1000 total ports)
Nmap scan report for WWW.umsl.edu (134.124.1.234)
Host is up (0.036s latency).
Not shown: 995 filtered tcp ports (no-response), 3 filtered tcp ports (host-prohibited)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 6.91 seconds
           Raw packets sent: 2001 (88.020KB) | Rcvd: 44 (4.776KB)

C:\Windows\System32>nmap -sS -sV -O -p 22,80,443 www.umsl.edu -oN www_umsl_scan.txt
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-10 13:15 -0600
Failed to resolve "www.umsl.edu".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 5.83 seconds
```

iii. Done. Too much to screenshot.

iv. Scanning 192.168.1.0/24 found host 192.168.1.250 up; ports 80 (http) and 443 (https) were open (listening), 22/tcp was filtered, and 1021 other TCP ports were closed.

```
C:\Windows\System32>nmap -sS -T4 -p 1-1024 192.168.1.0/24 -oN local_network_scan.txt
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-10 13:23 -0600
Nmap scan report for 192.168.1.250
Host is up (0.0070s latency).
Not shown: 1021 closed tcp ports (reset)
PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  open     http
443/tcp open     https

Nmap done: 256 IP addresses (1 host up) scanned in 19.90 seconds
```

v. When scanning the top 100 common ports of 192.168.1.1, Nmap reported that the host appeared down, likely because it was blocking ICMP echo requests or ping probes. This differs from scanning 192.168.1.1–100, where Nmap detected at least one host up (192.168.1.250). The key difference is that the single-host scan checks for responses only from one address, while the range scan discovers active hosts even if some block ping replies.

```
C:\Windows\System32>nmap -sS -T4 -p 1-1024 192.168.1.0/24 -oN local_network_scan.txt
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-10 13:23 -0600
Nmap scan report for 192.168.1.250
Host is up (0.0070s latency).
Not shown: 1021 closed tcp ports (reset)
PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  open     http
443/tcp open     https

Nmap done: 256 IP addresses (1 host up) scanned in 19.90 seconds

C:\Windows\System32>nmap -sS --top-ports 100 192.168.1.1 -oN common_ports_scan.txt
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-10 13:29 -0600
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.24 seconds
```

vi. Owner: scanme.nmap.org — this host is run by the Nmap project (nmap.org).
Ports scanned: Nmap scanned its default 1000 TCP ports (output shows 987 closed ports + 13 shown).
Ports found (number — service — state):
19/tcp — chargen — filtered
22/tcp — ssh — open
25/tcp — smtp — filtered

80/tcp — http — open
111/tcp — rpcbind — filtered
135/tcp — msrpc — filtered
389/tcp — ldap — filtered
445/tcp — microsoft-ds — filtered
636/tcp — ldaps — filtered
1433/tcp — ms-sql-s — filtered
4444/tcp — krb524 — filtered
9929/tcp — nping-echo — open
31337/tcp — tcpwrapped — open
(Total shown = 13 ports; 987 other TCP ports were closed.)

```
C:\Windows\System32>nmap -sS -sV 45.33.32.156 -oN host_scan_45.33.32.156.txt
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-10 13:34 -0600
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.12s latency).
Not shown: 987 closed tcp ports (reset)
PORT      STATE    SERVICE      VERSION
19/tcp    filtered chargen
22/tcp    open     ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    open     http         Apache httpd 2.4.7 ((Ubuntu))
111/tcp   filtered rpcbind
135/tcp   filtered msrpc
389/tcp   filtered ldap
445/tcp   filtered microsoft-ds
636/tcp   filtered ldapssl
1433/tcp  filtered ms-sql-s
4444/tcp  filtered krb524
9929/tcp  open     nping-echo   Nping echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.93 seconds
```

vii. Scan for detecting OS and services on scanme.nmap.org.

```
C:\Windows\System32>nmap -A scanme.nmap.org -oN detect_os_services.txt
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-10 14:29 -0600
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.10s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 987 closed tcp ports (reset)
PORT      STATE    SERVICE      VERSION
19/tcp    filtered chargen
22/tcp    open     tcpwrapped
| ssh-hostkey:
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
25/tcp    filtered smtp
80/tcp    open     http         Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
111/tcp   filtered rpcbind
135/tcp   filtered msrpc
389/tcp   filtered ldap
445/tcp   filtered microsoft-ds
636/tcp   filtered ldapssl
1433/tcp  filtered ms-sql-s
4444/tcp  filtered krb524
9929/tcp  open     nping-echo   Nping echo
31337/tcp open     tcpwrapped
Aggressive OS guesses: Linux 4.19 - 5.15 (97%), Linux 4.15 (93%), Linux 2.6.32 (92%), Linux 3.10 - 3.12 (92%), IPFire 2.27 (Linux 5.15 - 6.1) (92%), Linux 5.4 (92%), Linux 2.6.39 (91%), Linux 3.10 - 3.16 (
91%), Linux 3.10 (90%), Linux 4.9 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 14 hops

TRACEROUTE (using port 587/tcp)
HOP RTT       ADDRESS
1   50.00 ms  134.124.204.242
2   51.00 ms  134.124.98.250
3   109.00 ms kc-core-01-he0-1-0-3-420.mo.more.net (150.199.91.29)
4   109.00 ms fourhundredge-0-0-0-10.1441.core2.kans.net.internet2.edu (198.71.47.161)
5   114.00 ms fourhundredge-0-0-0-1.4079.core2.denv.net.internet2.edu (163.253.1.250)
6   115.00 ms fourhundredge-0-0-0-3.4079.core2.salt.net.internet2.edu (163.253.1.169)
7   115.00 ms fourhundredge-0-0-0-2.4079.core2.sacr.net.internet2.edu (163.253.1.186)
8   115.00 ms fourhundredge-0-0-0-0.4079.core2.sunn.net.internet2.edu (163.253.1.191)
9   115.00 ms fourhundredge-0-0-0-49.4079.agg1.sanj.net.internet2.edu (163.253.2.42)
10  168.00 ms eqix-sv1.linode.com (206.223.116.196)
11  ... 13
14  118.00 ms scanme.nmap.org (45.33.32.156)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
```

viii. Try –f option for firewall evasion

```
C:\Windows\System32>nmap -sS -f 45.33.32.156 -oN nmap_evade_f.txt
Warning: Packet fragmentation selected on a host other than Linux, OpenBSD, FreeBSD, or NetBSD.  This may or may not work.
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-10 14:37 -0600
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.070s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 74.43 seconds
```

ix. Perform a half-open scan

```
C:\Windows\System32>nmap -sS -v www.qburst.com -oN qburst_halfopen.txt
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-10 14:44 -0600
Initiating Parallel DNS resolution of 1 host. at 14:44
Completed Parallel DNS resolution of 1 host. at 14:44, 1.63s elapsed
Initiating Ping Scan at 14:44
Scanning www.qburst.com (34.117.195.190) [4 ports]
Completed Ping Scan at 14:44, 0.12s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:44
Completed Parallel DNS resolution of 1 host. at 14:44, 1.70s elapsed
Initiating SYN Stealth Scan at 14:44
Scanning www.qburst.com (34.117.195.190) [1000 ports]
Discovered open port 443/tcp on 34.117.195.190
Discovered open port 80/tcp on 34.117.195.190
Completed SYN Stealth Scan at 14:44, 10.16s elapsed (1000 total ports)
Nmap scan report for www.qburst.com (34.117.195.190)
Host is up (0.10s latency).
rDNS record for 34.117.195.190: 190.195.117.34.bc.googleusercontent.com
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 13.82 seconds
           Raw packets sent: 2008 (88.328KB) | Rcvd: 63 (4.364KB)
```

x. Adding -sU produced UDP results in addition to the TCP results: TCP ports (80 and 443) remained open while 22 stayed filtered, but now Nmap also reported 53/udp closed and 161/udp open|filtered. The key difference is that UDP probing can return closed (ICMP port-unreachable) or the ambiguous open|filtered (no reply — could be an open silent service or a filtered/dropped packet), so the combined scan shows additional UDP entries and more ambiguous states compared with the clearer TCP-only SYN scan.

```
C:\Windows\System32>nmap -sS -sU -p T:80,443,22,U:53,161 --min-rate 50 -T4 www.qburst.com -oN combined_tcp_udp_qburst.txt
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-10 14:55 -0600
Nmap scan report for www.qburst.com (34.117.195.190)
Host is up (0.080s latency).
rDNS record for 34.117.195.190: 190.195.117.34.bc.googleusercontent.com

PORT    STATE         SERVICE
22/tcp  filtered      ssh
80/tcp  open          http
443/tcp open          https
53/udp  closed        domain
161/udp open|filtered snmp

Nmap done: 1 IP address (1 host up) scanned in 4.83 seconds
```