

Filtering p-cap to examine MAC Address, DNS, & TCP data

Next, I'll filter by a specific Ethernet MAC Address; by selecting the first packet and drilling into the Eth II subtree, the MAC will display as either the source or destination MAC address:

The screenshot shows the Wireshark interface with a packet capture file named 'sample.pcap'. The filter bar at the top contains the filter 'eth.addr == 42:01:ac:15:e0:02'. The packet list shows several packets, with packet 26 selected. The packet details pane for packet 26 is expanded, showing the Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol layers. The Ethernet II layer shows the source MAC address as 42:01:ac:15:e0:01 and the destination MAC address as 42:01:ac:15:e0:02. The Internet Protocol Version 4 layer shows the source IP as 142.250.1.139 and the destination IP as 172.21.224.2. The Internet Control Message Protocol layer shows the type as Echo (ping) reply.

No.	Time	Source	Destination	Protocol	Length	Info
26	9.645078	142.250.1.139	172.21.224.2	ICMP	98	Echo (ping) reply
27	9.645214	172.21.224.2	169.254.169.254	DNS	86	Standard query 0x3cd
28	9.645859	169.254.169.254	172.21.224.2	DNS	120	Standard query respo
29	9.646069	172.21.224.2	35.235.244.34	SSH	210	Server: Encrypted pa
30	9.646203	35.235.244.34	172.21.224.2	TCP	66	35193 → 22 [ACK] Seq
31	10.646049	172.21.224.2	142.250.1.139	ICMP	98	Echo (ping) request
32	10.646563	142.250.1.139	172.21.224.2	ICMP	98	Echo (ping) reply

Wireshark · Packet 26 · sample.pcap

- > Frame 26: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
- ▼ Ethernet II, Src: 42:01:ac:15:e0:01 (42:01:ac:15:e0:01), Dst: 42:01:ac:15:e0:02
 - > Destination: 42:01:ac:15:e0:02 (42:01:ac:15:e0:02)
 - > Source: 42:01:ac:15:e0:01 (42:01:ac:15:e0:01)
 - > Type: IPv4 (0x0800)
- > Internet Protocol Version 4, Src: 142.250.1.139, Dst: 172.21.224.2
- > Internet Control Message Protocol

0000 42 01 ac 15 e0 02 42 01 ac 15 e0 01 08 00 45 00 B...B... ..E
0010 00 54 00 00 00 00 73 01 2b 0c 8e fa 01 8b ac 15 T... +...
0020 e0 02 00 00 72 f5 68 31 00 02 42 14 7e 63 00 00 ...r·h1 ·B·nc·
0030 00 00 a2 8c 03 00 00 00 00 00 10 11 12 13 14 15 !"#\$\$%
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 &'()*+,-./012345
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,-./012345
0060 36 37 67

No.: 26 · Time: 9.645078 · Source: 142.250.1.139 · Destination: 172.21.224.2 · Echo (ping) reply id=0x6831, seq=2/512, ttl=115 (request in 25)

Filtering in Wireshark to explore DNS packets using port 53, and by drilling into the DNS subtree through Queries it shows the website that was queried:

sample.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port == 53

No.	Time	Source	Destination	Protocol	Length	Info
9	8.637619	172.21.224.2	169.254.169.254	DNS	81	Standard query 0xc2
10	8.637625	172.21.224.2	169.254.169.254	DNS	81	Standard query 0xd63
11	8.641838	169.254.169.254	172.21.224.2	DNS	193	Standard query respo
12	8.641978	169.254.169.254	172.21.224.2	DNS	177	Standard query respo
19	8.644093	172.21.224.2	169.254.169.254	DNS	86	Standard query 0xb54
20	8.647339	169.254.169.254	172.21.224.2	DNS	120	Standard query respo
27	9.645214	172.21.224.2	169.254.169.254	DNS	86	Standard query 0x3cd
28	9.645859	169.254.169.254	172.21.224.2	DNS	120	Standard query respo
33	10.646715	172.21.224.2	169.254.169.254	DNS	86	Standard query 0x94d
34	10.647413	169.254.169.254	172.21.224.2	DNS	120	Standard query respo
60	18.031311	172.21.224.2	169.254.169.254	DNS	81	Standard query 0xae2

> Internet Protocol Version 4, Src: 172.21.224.2, Dst: 169.254.169.254
 > User Datagram Protocol, Src Port: 59398, Dst Port: 53
 > Domain Name System (query)
 Transaction ID: 0xc26
 Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 > Queries
 > opensource.google.com: type A, class IN
 [Response In: 12]

0000 42 01 ac 15 e0 01 42 01 ac 15 e0 02 08 00
 0010 00 43 6b da 40 00 40 11 ee ba ac 15 e0 02
 0020 a9 fe e8 06 00 35 00 2f e0 55 0c 26 01 00
 0030 00 00 00 00 00 00 0a 6f 70 65 6e 73 6f 75
 0040 65 06 67 6f 6f 67 6c 65 03 63 6f 6d 00 00
 0050 01

Domain Name System (dns), 39 bytes

Packets: 200 · Displayed: 22 (11.0%) Profile: Default

Now to examine TCP packets using port 80:

sample.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 80

No.	Time	Source	Destination	Protocol	Length	Info
37	10.799238	172.21.224.2	169.254.169.254	TCP	54	56664 → 80 [ACK] Seq=1 Ack=1 Win=63814 Len=0
38	10.799668	169.254.169.254	172.21.224.2	TCP	54	[TCP ACKED unseen segment] 80 → 56664 [ACK] Seq=1 Ack=2 Win=65535 Len=0
52	16.943231	172.21.224.2	169.254.169.254	TCP	54	41208 → 80 [ACK] Seq=1 Ack=1 Win=63814 Len=0
53	16.943758	169.254.169.254	172.21.224.2	TCP	54	[TCP ACKED unseen segment] 80 → 41208 [ACK] Seq=1 Ack=2 Win=65535 Len=0
64	18.032768	172.21.224.2	142.250.1.139	TCP	74	49652 → 80 [SYN] Seq=0 Win=65320 Len=0 MSS=1420 SACK_PERM TSval=2804123006 TSecr=406
65	18.034210	142.250.1.139	172.21.224.2	TCP	74	80 → 49652 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1420 SACK_PERM TS
66	18.034238	172.21.224.2	142.250.1.139	TCP	66	49652 → 80 [ACK] Seq=1 Ack=1 Win=65408 Len=0 TSval=2804123006 TSecr=406
67	18.034291	172.21.224.2	142.250.1.139	HTTP	151	GET / HTTP/1.1
68	18.034724	142.250.1.139	172.21.224.2	TCP	66	80 → 49652 [ACK] Seq=1 Ack=86 Win=65536 Len=0 TSval=4069674931 TSecr=28
69	18.036927	142.250.1.139	172.21.224.2	HTTP	648	HTTP/1.1 301 Moved Permanently (text/html)
70	18.036941	172.21.224.2	142.250.1.139	TCP	66	49652 → 80 [ACK] Seq=86 Ack=583 Win=64896 Len=0 TSval=2804123009 TSecr=
79	18.037390	172.21.224.2	142.250.1.139	TCP	66	49652 → 80 [FIN, ACK] Seq=86 Ack=583 Win=64896 Len=0 TSval=2804123009 T

> Frame 37: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
 > Ethernet II, Src: 42:01:ac:15:e0:02 (42:01:ac:15:e0:02), Dst: 42:01:ac:15:e0:01 (42:01:ac:15:e0:01)
 > Internet Protocol Version 4, Src: 172.21.224.2, Dst: 169.254.169.254
 > Transmission Control Protocol, Src Port: 56664, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

0000 42 01 ac 15 e0 01 42 01 ac 15 e0 02 08 00 45 00
 0010 00 28 89 a2 40 00 40 06 d1 18 ac 15 e0 02 a9 fe
 0020 a9 fe dd 58 00 50 24 08 9f 5f 09 a3 39 73 50 10
 0030 f9 46 e0 2f 00 00

By selecting the first packet, I can drill into the subtrees to review anything I prefer, for instance Time to live (TTL) [max numbers of hops a packet is allowed to pass through before discarded], src & destination addresses, byte size, protocol, ect:

Wireshark · Packet 37 · sample.pcap

▼ Frame 37: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)

- Encapsulation type: Ethernet (1)
- Arrival Time: Nov 23, 2022 12:38:27.387163000 Greenwich Standard Time
- UTC Arrival Time: Nov 23, 2022 12:38:27.387163000 UTC
- Epoch Arrival Time: 1669207107.387163000
- [Time shift for this packet: 0.000000000 seconds]
- [Time delta from previous captured frame: 0.151417000 seconds]
- [Time delta from previous displayed frame: 0.000000000 seconds]
- [Time since reference or first frame: 10.799238000 seconds]
- Frame Number: 37
- Frame Length: 54 bytes (432 bits)
- Capture Length: 54 bytes (432 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: eth:ethertype:ip:tcp]
- [Coloring Rule Name: HTTP]
- [Coloring Rule String: http || tcp.port == 80 || http2]

> Ethernet II, Src: 42:01:ac:15:e0:02 (42:01:ac:15:e0:02), Dst: 42:01:ac:15:e0:01 (42:01:ac:15:e0:01)

▼ Internet Protocol Version 4, Src: 172.21.224.2, Dst: 169.254.169.254

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 40
- Identification: 0x89a2 (35234)
- > 010. = Flags: 0x2, Don't fragment
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 64
- Protocol: TCP (6)
- Header Checksum: 0xd118 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 172.21.224.2

0000	42 01 ac 15 e0 01 42 01	ac 15 e0 02 08 00 45 00	B.....B.....E.
0010	00 28 89 a2 40 00 40 06	d1 18 ac 15 e0 02 a9 fe	.(.@@@.....