

Lab 1 - IoT Network Analysis

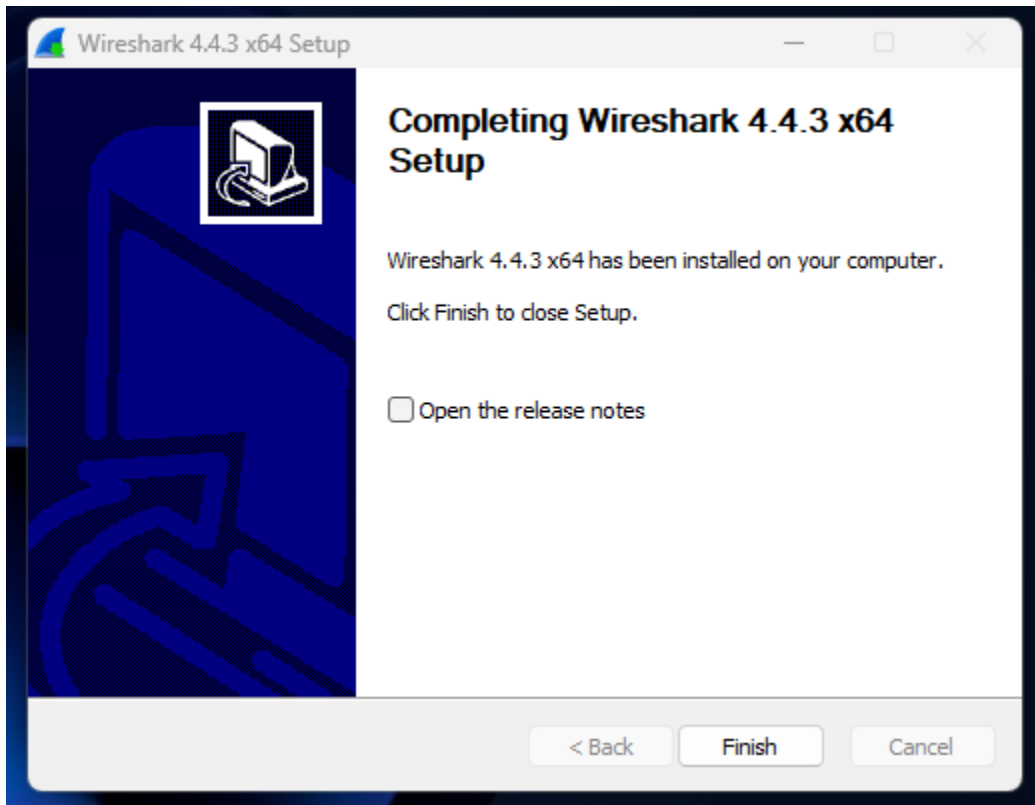
CS 466

2/2/2025

Patrick Hurley

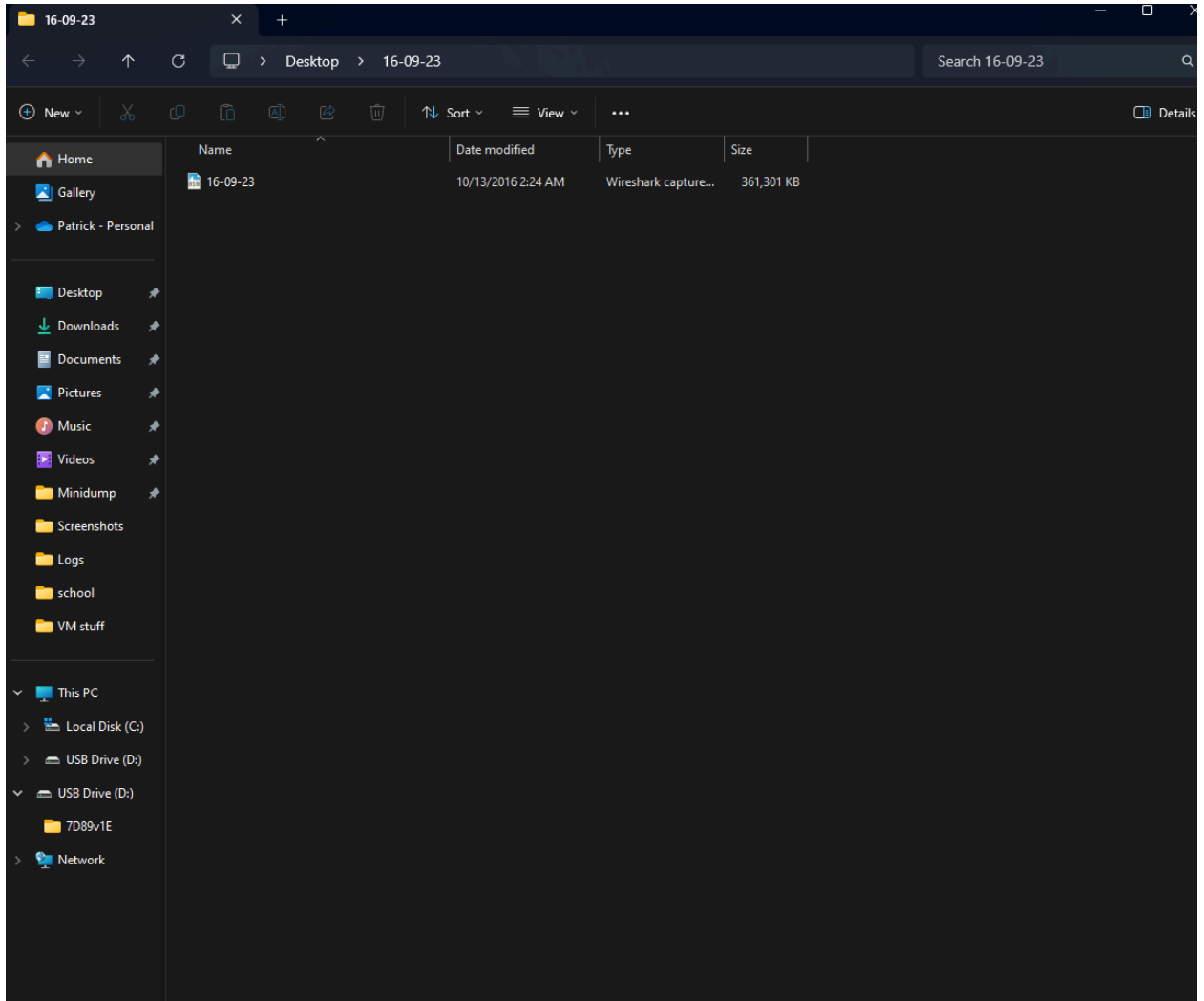
Part #1

Here I have downloaded and installed Wireshark.



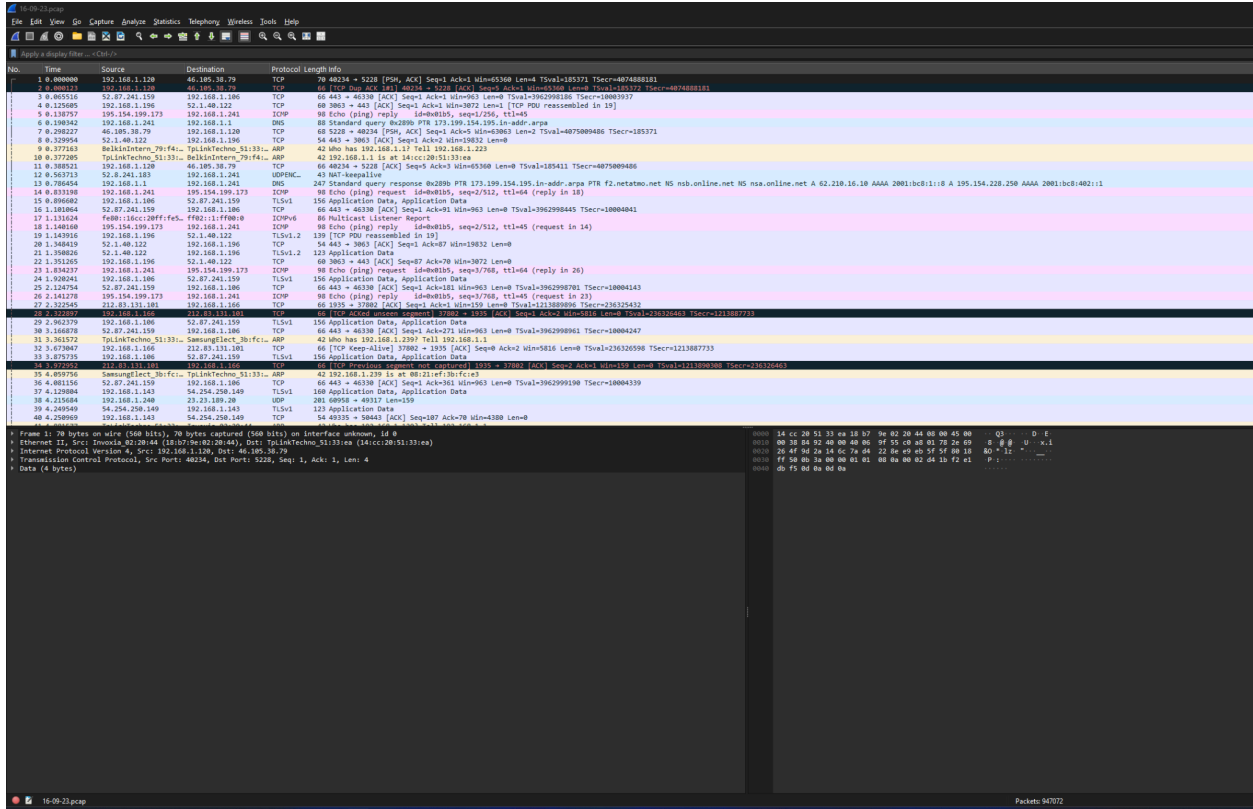
Part #2

Here is a screenshot of the extracted contents of the downloaded pcap file.



Part #3

This screenshot shows the pcap file had ben opened in Wireshark.



Part #4

Below is a screenshot of the list of mac addresses in the endpoints tab. The first two MAC addresses listed below belong to the Samsung Smart Cam (00:16:6c:ab:6b:88) and the Withings Smart Baby Monitor (00:24:e4:11:18:a8).

Wireshark - Endpoints - 16-09-23.pcap

Endpoint Settings

- Name resolution
- Limit to display filter

Copy

Map

Protocol

- Bluetooth
- BPv7
- DCCP
- Ethernet
- FC
- FDDI
- IEEE 802.11
- IEEE 802.15.4
- IPv4
- IPv6
- IPX
- JXTA
- LTP
- MPTCP
- NCP
- openSAFETY
- RSVP
- SCTP
- SLL
- TCP
- Token-Ring
- UDP
- USB
- ZigBee

Filter list for specific type

Ethernet - 61	IPv4 - 668	IPv6 - 48	TCP - 7721	UDP - 6464		
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
00:16:6c:ab:6b:88	85,273	28 MB	67,650	26 MB	17,623	2 MB
00:24:e4:11:18:a8	46,905	4 MB	23,961	2 MB	22,944	2 MB
00:24:e4:1b:6f:96	376	80 kB	197	61 kB	179	19 kB
01:00:5e:00:00:01	689	32 kB	0	0 bytes	689	32 kB
01:00:5e:00:00:16	110	6 kB	0	0 bytes	110	6 kB
01:00:5e:00:00:fb	742	44 kB	0	0 bytes	742	44 kB
01:00:5e:00:00:fc	155	9 kB	0	0 bytes	155	9 kB
01:00:5e:00:01:3c	685	32 kB	0	0 bytes	685	32 kB
01:00:5e:02:00:fc	20	2 kB	0	0 bytes	20	2 kB
01:00:5e:7fff:fa	24,028	11 MB	0	0 bytes	24,028	11 MB
08:21:ef:3b:fc:e3	33,164	7 MB	16,752	2 MB	16,412	5 MB
14:cc:20:51:33:e9	3,404	398 kB	0	0 bytes	3,404	398 kB
14:cc:20:51:33:ea	792,836	289 MB	427,012	230 MB	365,824	59 MB
18:b4:30:25:b:e4	204	47 kB	110	33 kB	94	14 kB
18:b7:9e:02:20:44	8,959	995 kB	5,000	528 kB	3,959	468 kB
30:8c:fb:2f:e4:b2	242,703	30 MB	121,562	22 MB	121,141	8 MB
33:33:00:00:00:01	748	71 kB	0	0 bytes	748	71 kB
33:33:00:00:00:02	1,424	122 kB	0	0 bytes	1,424	122 kB
33:33:00:00:00:0c	22,139	11 MB	0	0 bytes	22,139	11 MB
33:33:00:00:00:16	52	5 kB	0	0 bytes	52	5 kB
33:33:00:00:00:fb	746	66 kB	0	0 bytes	746	66 kB
33:33:00:01:00:02	694	60 kB	0	0 bytes	694	60 kB
33:33:00:01:00:03	1,444	124 kB	0	0 bytes	1,444	124 kB
33:33:ff:00:00:00	1,401	120 kB	0	0 bytes	1,401	120 kB
33:33:ff:00:00:01	688	59 kB	0	0 bytes	688	59 kB
33:33:ff:00:0e:e2	685	59 kB	0	0 bytes	685	59 kB
33:33:ff:00:0f:8d	90	8 kB	0	0 bytes	90	8 kB
33:33:ff:18:34:43	681	59 kB	0	0 bytes	681	59 kB
33:33:ff:25:b:e4	3	258 bytes	0	0 bytes	3	258 bytes
33:33:ff:33:bb:85	684	59 kB	0	0 bytes	684	59 kB
33:33:ff:3b:fc:e3	95	8 kB	0	0 bytes	95	8 kB
33:33:ff:42:49:61	92	8 kB	0	0 bytes	92	8 kB
33:33:ff:46:69:72	2	172 bytes	0	0 bytes	2	172 bytes
33:33:ff:47:a0:a9	19	2 kB	0	0 bytes	19	2 kB
33:33:ff:51:33:ea	746	64 kB	0	0 bytes	746	64 kB
33:33:ff:79:f4:89	658	57 kB	0	0 bytes	658	57 kB
33:33:ff:83:28:11	661	57 kB	0	0 bytes	661	57 kB
33:33:ff:87:16:44	90	8 kB	0	0 bytes	90	8 kB
33:33:ff:99:e7:24	99	9 kB	0	0 bytes	99	9 kB
33:33:ff:a7:a3:c2	23	2 kB	0	0 bytes	23	2 kB
33:33:ff:a8:e6:db	3	250 bytes	0	0 bytes	3	250 bytes
33:33:ff:ab:6b:88	668	57 kB	0	0 bytes	668	57 kB
33:33:ff:ae:c2:e3	5	422 bytes	0	0 bytes	5	422 bytes
33:33:ff:c9:a7:81	2	164 bytes	0	0 bytes	2	164 bytes
33:33:ff:d4:f4:b7	680	58 kB	0	0 bytes	680	58 kB
33:33:ff:e4:9b:c0	696	60 kB	0	0 bytes	696	60 kB
44:65:0d:56:cc:d3	52,614	6 MB	31,503	4 MB	21,111	2 MB
50:c7:bf:00:56:39	2,775	345 kB	1,682	179 kB	1,093	166 kB
70:5a:0f:e4:9b:c0	14,241	4 MB	9,005	2 MB	5,236	2 MB
70:ee:50:03:b8:ac	13,508	2 MB	6,184	1 MB	7,314	1 MB
70:ee:50:18:34:43	38,749	14 MB	21,228	12 MB	17,521	2 MB
74:2f:68:81:69:42	255,653	213 MB	97,202	15 MB	158,451	198 MB
74:6a:89:00:2e:25	59	7 kB	33	3 kB	26	4 kB
b4:ce:ff:6a:7a:3c:2	19,789	10 MB	9,050	2 MB	10,739	9 MB
d0:52:a8:00:67:5e	29,623	2 MB	15,172	1 MB	14,451	1 MB
d0:a6:37:df:a1:e1	686	143 kB	391	39 kB	295	104 kB
e0:76:d0:33:bb:85	7,575	1 MB	4,572	502 kB	3,003	903 kB
ea:1a:50:70:f4:80	68,747	17 MB	36,848	14 MB	31,899	2 MB

Part #5

I will continue using the two MAC addresses from the previous question, the Samsung Smart Cam (00:16:6c:ab:6b:88) and the Withings Smart Baby Monitor (00:24:e4:11:18:a8).

The first screenshot below shows that the Samsung Smart Cam is the destination. Through this, we can figure out the destination IP address, which is **192.168.1.249**.

```
Wireshark · Packet 123 · 16-09-23.pcap
▶ Frame 123: 252 bytes on wire (2016 bits), 252 bytes captured (2016 bits) on interface unknown, id 0
▼ Ethernet II, Src: BelkinIntern_83:28:11 (ec:1a:59:83:28:11), Dst: SamsungElect_ab:6b:88 (00:16:6c:ab:6b:88)
  ▶ Destination: SamsungElect_ab:6b:88 (00:16:6c:ab:6b:88)
  ▶ Source: BelkinIntern_83:28:11 (ec:1a:59:83:28:11)
  Type: IPv4 (0x0800)
  [Stream index: 14]
▼ Internet Protocol Version 4, Src: 192.168.1.193, Dst: 192.168.1.249
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 238
  Identification: 0x5bf3 (23539)
  ▶ 010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: TCP (6)
  Header Checksum: 0x590c [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.193
  Destination Address: 192.168.1.249
  [Stream index: 12]
▶ Transmission Control Protocol, Src Port: 4981, Dst Port: 49152, Seq: 1, Ack: 1, Len: 186
▶ Hypertext Transfer Protocol

0000 00 16 6c ab 6b 88 ec 1a 59 83 28 11 08 00 45 00  ..l k... Y (...E-
0010 00 ee 5b f3 40 00 40 06 59 0c c0 a8 01 c1 c0 a8  ..[ @ @ Y.....
0020 01 f9 13 75 c0 00 f6 68 f5 69 02 b0 98 19 80 18  ...u...h i.....
0030 0b 68 46 9d 00 00 01 01 08 0a 0d 28 ae 9b 00 b8  ..hF..... (....
0040 25 48 47 45 54 20 2f 72 6f 6f 74 44 65 73 63 2e  %HGGET /r ootDesc.
0050 78 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 4f  xml HTTP /1.1 HO
0060 53 54 3a 20 31 39 32 2e 31 36 38 2e 31 2e 32 34  ST: 192. 168.1.24
0070 39 3a 34 39 31 35 32 0d 0a 44 41 54 45 3a 20 46  9:49152  DATE: F
0080 72 69 2c 20 32 33 20 53 65 70 20 32 30 31 36 20  ri, 23 S ep 2016
0090 30 30 3a 30 30 3a 30 37 20 47 4d 54 0d 0a 43 4f  00:00:07 GMT CO
00a0 4e 4e 45 43 54 49 4f 4e 3a 20 63 6c 6f 73 65 0d  NNECTION : close
00b0 0a 55 53 45 52 2d 41 47 45 4e 54 3a 20 4c 69 6e  -USER-AG ENT: Lin
```

The second screenshot below shows that the Withings Smart Baby Monitor is the source this time. The source Ip address for the baby monitor is **192.168.1.166**.

```
▶ Frame 32: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface unknown, id 0
▼ Ethernet II, Src: Withings_11:18:a8 (00:24:e4:11:18:a8), Dst: TpLinkTechno_51:33:ea (14:cc:20:51:33:ea)
  ▶ Destination: TpLinkTechno_51:33:ea (14:cc:20:51:33:ea)
  ▶ Source: Withings_11:18:a8 (00:24:e4:11:18:a8)
  Type: IPv4 (0x0800)
  [Stream index: 6]
▼ Internet Protocol Version 4, Src: 192.168.1.166, Dst: 212.83.131.101
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 52
  Identification: 0x395a (14682)
  ▶ 010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: TCP (6)
  Header Checksum: 0xe762 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.166
  Destination Address: 212.83.131.101
  [Stream index: 6]
▶ Transmission Control Protocol, Src Port: 37802, Dst Port: 1935, Seq: 0, Ack: 2, Len: 0
```

Part #6

In the screenshot below, I used the given MAC address for the router to search for it on Wireshark. From this screenshot I can see that the router is the source, because of this I can then use that to see that the IP address of the router is **52.87.241.159**

```

Wireshark · Packet 257 · 16-09-23.pcap
▶ Frame 257: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface unknown, id 0
▼ Ethernet II, Src: TpLinkTechno_51:33:ea (14:cc:20:51:33:ea), Dst: Dropcam_2f:e4:b2 (30:8c:fb:2f:e4:b2)
  ▶ Destination: Dropcam_2f:e4:b2 (30:8c:fb:2f:e4:b2)
  ▶ Source: TpLinkTechno_51:33:ea (14:cc:20:51:33:ea)
  Type: IPv4 (0x0800)
  [Stream index: 1]
▼ Internet Protocol Version 4, Src: 52.87.241.159, Dst: 192.168.1.106
  0100 .... = Version: 4
  ... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 52
  Identification: 0xd586 (54662)
  ▶ 010. .... = Flags: 0x2, Don't fragment
  ... 0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 224
  Protocol: TCP (6)
  Header Checksum: 0xdd33 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 52.87.241.159
  Destination Address: 192.168.1.106
  [Stream index: 1]
▶ Transmission Control Protocol, Src Port: 443, Dst Port: 46330, Seq: 1, Ack: 541, Len: 0

0000  30 8c fb 2f e4 b2 14 cc  20 51 33 ea 08 00 45 00  0 / ... Q3...E
0010  00 34 d5 86 40 00 e0 06  dd 33 34 57 f1 9f c0 a8  4 @ ... 34W ...
0020  01 6a 01 bb b4 fa ce 1d  70 7a f7 32 c4 58 80 10  j ... pz 2 X ...
0030  03 c3 b1 69 00 00 01 01  08 0a ec 36 93 9c 00 98  i ... 6 ...
0040  a8 42                                B

```

Part #7

The first IOS device I searched for was the Amazon Echo by using its MAC address, and I was able to see many different protocols it used. Below is a screen showing protocols like **UDP, TCP, and NTP**.

16-09-23.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

eth.addr==44:65:0d:56:cc:d3

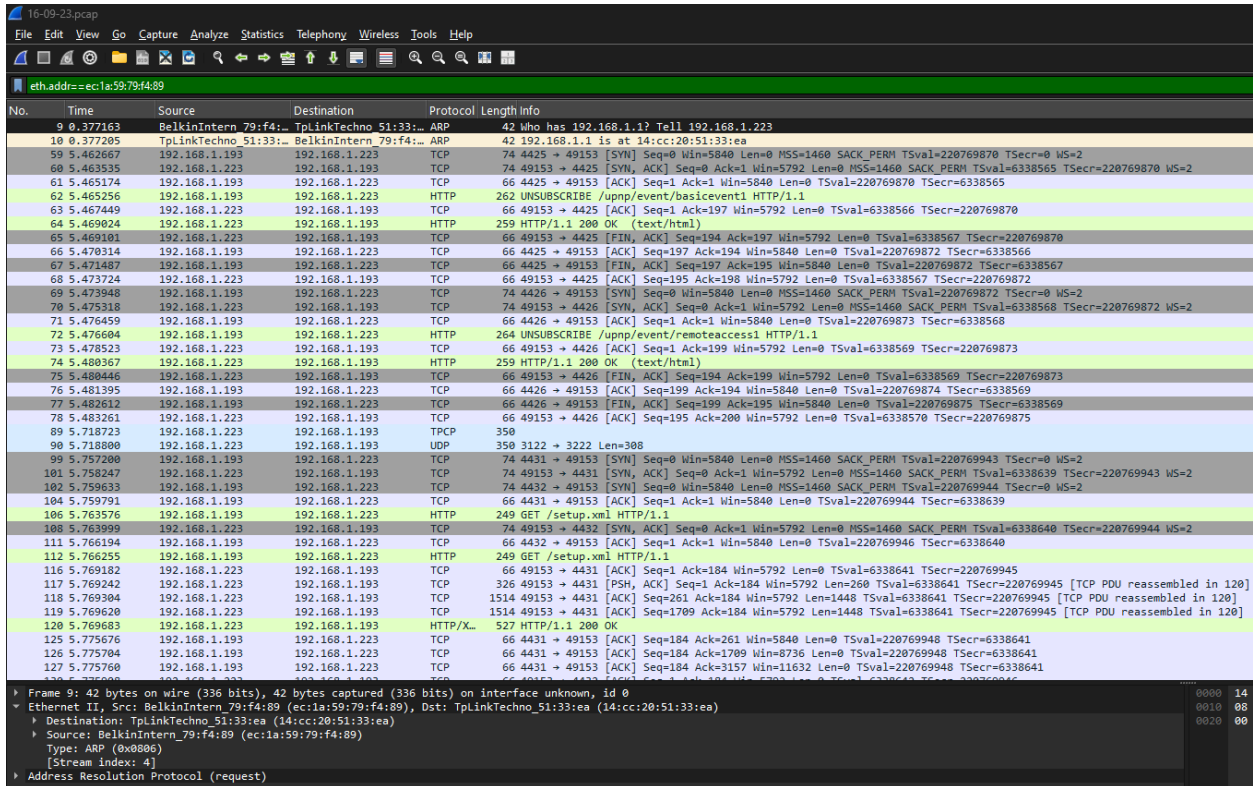
No.	Time	Source	Destination	Protocol	Length	Info
38	4.215684	192.168.1.240	23.23.189.20	UDP	201	60958 → 49317 Len=159
258	6.348524	192.168.1.240	23.23.189.20	UDP	191	37244 → 33434 Len=149
308	18.643506	54.239.29.231	192.168.1.240	TLSv1.2	95	Application Data
309	18.654095	192.168.1.240	54.239.29.231	TCP	54	46369 → 443 [ACK] Seq=1 Ack=42 Win=1734 Len=0
310	18.654208	192.168.1.240	54.239.29.231	TLSv1.2	95	Application Data
311	18.907551	54.239.29.231	192.168.1.240	TCP	54	443 → 46369 [ACK] Seq=42 Ack=42 Win=544 Len=0
328	22.006867	192.168.1.240	67.18.187.111	NTP	90	NTP Version 4, client
329	22.186663	67.18.187.111	192.168.1.240	NTP	90	NTP Version 4, server
336	23.651574	TpLinkTechno_51:33:...	AmazonTechno_56:cc:...	ARP	42	Who has 192.168.1.240? Tell 192.168.1.1
337	23.653157	AmazonTechno_56:cc:...	TpLinkTechno_51:33:...	ARP	42	192.168.1.240 is at 44:65:0d:56:cc:d3
357	31.248144	192.168.1.240	23.23.189.20	UDP	201	60958 → 49317 Len=159
375	33.375311	192.168.1.240	23.23.189.20	UDP	191	37244 → 33434 Len=149
444	48.681181	192.168.1.240	54.239.29.231	TLSv1.2	95	Application Data
447	48.897459	54.239.29.231	192.168.1.240	TCP	54	443 → 46369 [ACK] Seq=42 Ack=83 Win=544 Len=0
448	48.897578	54.239.29.231	192.168.1.240	TLSv1.2	95	Application Data
455	49.357557	54.239.29.231	192.168.1.240	TCP	95	[TCP Retransmission] 443 → 46369 [PSH, ACK] Seq=42 Ack=83 Win=544 Len=41
456	49.406854	192.168.1.240	54.239.29.231	TCP	54	46369 → 443 [ACK] Seq=83 Ack=83 Win=1734 Len=0
478	54.361577	TpLinkTechno_51:33:...	AmazonTechno_56:cc:...	ARP	42	Who has 192.168.1.240? Tell 192.168.1.1
479	54.371887	AmazonTechno_56:cc:...	TpLinkTechno_51:33:...	ARP	42	192.168.1.240 is at 44:65:0d:56:cc:d3
500	58.275338	192.168.1.240	23.23.189.20	UDP	201	60958 → 49317 Len=159
515	60.401675	192.168.1.240	23.23.189.20	UDP	191	37244 → 33434 Len=149
566	68.235096	192.168.1.240	207.171.178.6	NTP	90	NTP Version 4, client
567	68.379046	207.171.178.6	192.168.1.240	NTP	90	NTP Version 4, server
579	72.393442	192.168.1.240	67.18.187.111	NTP	90	NTP Version 4, client
580	72.573293	67.18.187.111	192.168.1.240	NTP	90	NTP Version 4, server
587	74.204330	AmazonTechno_56:cc:...	TpLinkTechno_51:33:...	ARP	42	Who has 192.168.1.1? Tell 192.168.1.240
588	74.204371	TpLinkTechno_51:33:...	AmazonTechno_56:cc:...	ARP	42	192.168.1.1 is at 14:cc:20:51:33:ea
604	78.643442	54.239.29.231	192.168.1.240	TLSv1.2	95	Application Data
605	78.646079	192.168.1.240	54.239.29.231	TCP	54	46369 → 443 [ACK] Seq=83 Ack=124 Win=1734 Len=0
606	78.646185	192.168.1.240	54.239.29.231	TLSv1.2	95	Application Data
609	78.897643	54.239.29.231	192.168.1.240	TCP	54	443 → 46369 [ACK] Seq=124 Ack=124 Win=544 Len=0
638	85.299592	192.168.1.240	23.23.189.20	UDP	201	60958 → 49317 Len=159
656	87.426655	192.168.1.240	23.23.189.20	UDP	191	37244 → 33434 Len=149
744	108.674189	192.168.1.240	54.239.29.231	TLSv1.2	95	Application Data
745	108.890415	54.239.29.231	192.168.1.240	TCP	54	443 → 46369 [ACK] Seq=124 Ack=165 Win=544 Len=0
746	108.890537	54.239.29.231	192.168.1.240	TLSv1.2	95	Application Data
748	109.129560	192.168.1.240	54.239.29.231	TCP	95	[TCP Spurious Retransmission] 46369 → 443 [PSH, ACK] Seq=124 Ack=124 Win=1734 Len=41
750	109.345730	54.239.29.231	192.168.1.240	TCP	54	[TCP Dup ACK 745#1] 443 → 46369 [ACK] Seq=165 Ack=165 Win=544 Len=0
751	109.357641	54.239.29.231	192.168.1.240	TCP	95	[TCP Retransmission] 443 → 46369 [PSH, ACK] Seq=124 Ack=165 Win=544 Len=41
752	109.402851	192.168.1.240	54.239.29.231	TCP	54	46369 → 443 [ACK] Seq=165 Ack=165 Win=1734 Len=0

Frame 38: 201 bytes on wire (1608 bits), 201 bytes captured (1608 bits) on interface unknown, id 0

Ethernet II, Src: AmazonTechno_56:cc:d3 (44:65:0d:56:cc:d3), Dst: TpLinkTechno_51:33:ea (14:cc:20:51:33:ea)

- Destination: TpLinkTechno_51:33:ea (14:cc:20:51:33:ea)
- Source: AmazonTechno_56:cc:d3 (44:65:0d:56:cc:d3)
- Type: IPv4 (0x0800)
- [Stream index: 9]

The second IOT device I chose was the Belkin Wemo switch. The screenshot below shows multiple protocols including **ARP**, **TCP**, **HTTP**, and **UDP**.

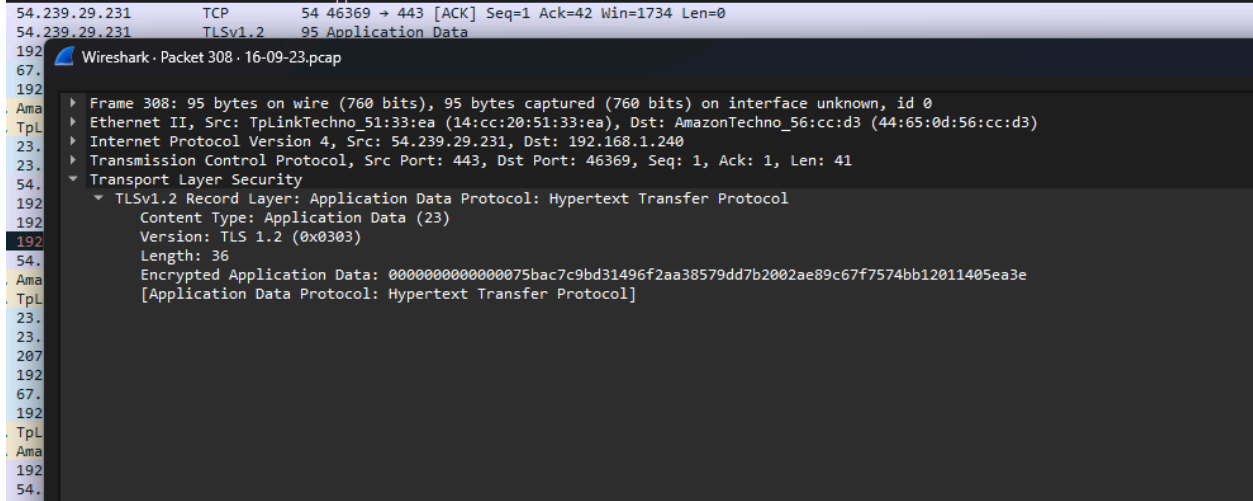


Part #8

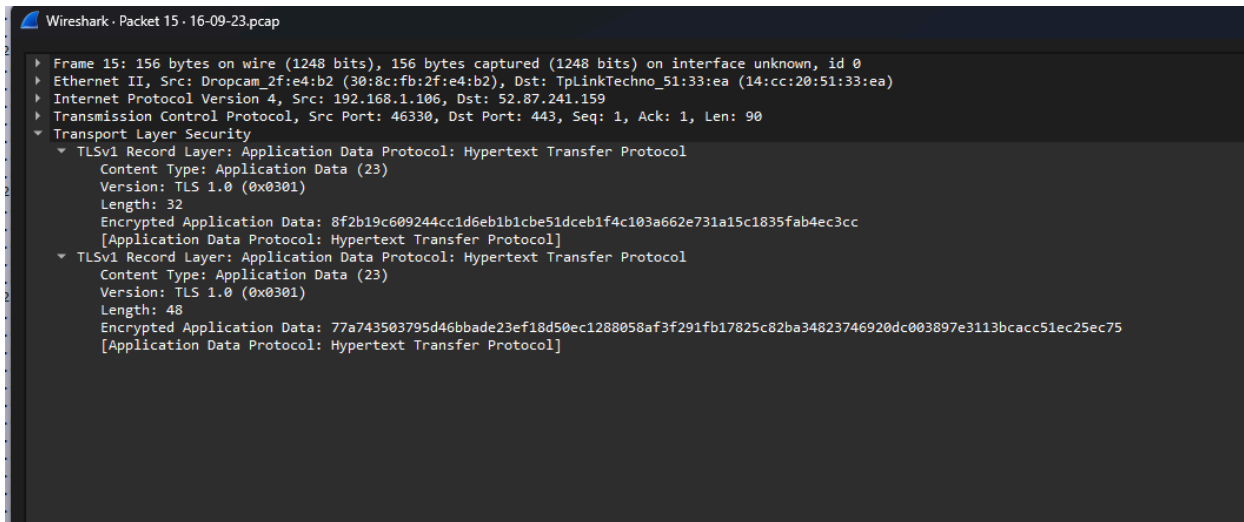
Elephant flow is talking about the flow of very large amounts of packets. Mice flow is talking about smaller amounts of packets being sent

Part #9

The first IoT device I chose was the Amazon Echo. The screenshot below shows that the Amazon Echo has **Transport Layer Security version 1.2**.

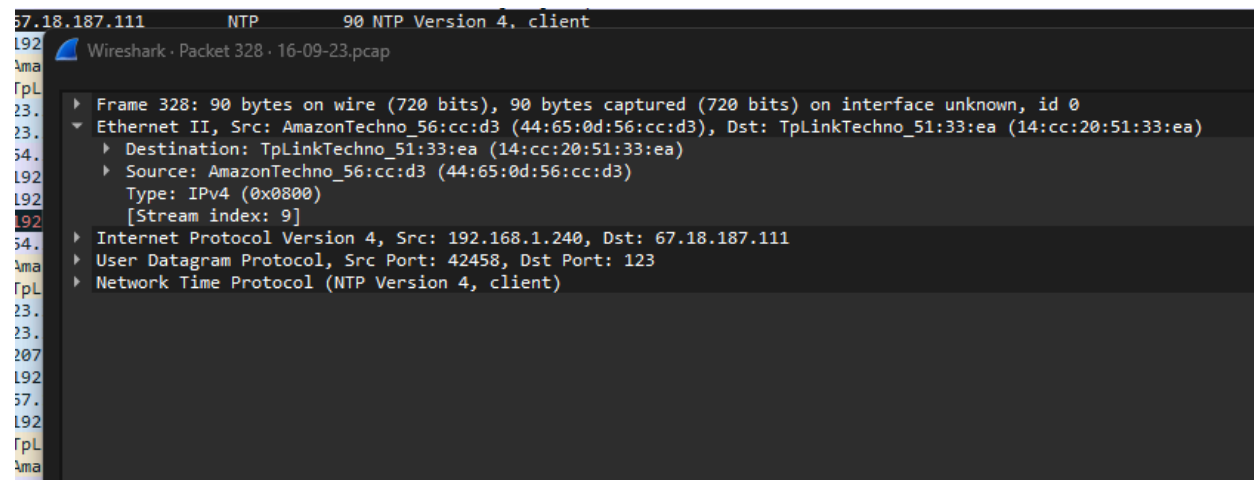


The second IOT device i chose was the DropCam. The screenshot below shows that the DropCam has **TLS version 1**.



Part #10

Below is a screenshot that shows the Amazon Echo device is communicating with an external IP address of **67.18.187.111**, because if it was communicating with internal addresses it would start with 192.168.xxx.xxx



The Below screenshot is of the Netatmo Welcome. The Netatmo is receiving information from an external IP address **52.8.241.183**.

