SSL Decryption – MOP Website

CHAMELEON

FOR OUR SMARTER WORLD

LEON NETTO

1. Executive Summary

This security report outlines the findings of SSL/TLS decryption conducted on the MOP website. The purpose of this testing was to assess the security of the website's encrypted traffic and identify any potential vulnerabilities that could lead to data leakage or targeted attacks.

The decryption was performed using SSLKEYLOG and Wireshark, aiming to analyse the encrypted traffic for any signs of weak cipher suites or exploitable web servers. The report concludes that the security measures implemented on the MOP website, particularly through Google Cloud Platform (GCP), effectively safeguard against unauthorised access and data breaches.

2. Purpose

The purpose of this security assessment was to evaluate the effectiveness of the encryption protocols and security measures employed by the MOP website in protecting sensitive information transmitted over the network. By decrypting the SSL/TLS traffic, the goal was to identify any potential weaknesses or vulnerabilities that could compromise the confidentiality and integrity of data, thereby mitigating the risk of cyber-attacks and unauthorised access.

3. Scope

The scope of the assessment encompassed the following key activities:

1. Utilising SSLKEYLOG and Wireshark to decrypt and analyse the encrypted traffic of the MOP website.
2. Testing conducted to identify any weak cipher suites that could be exploited by malicious actors to intercept or manipulate data.
3. Analysis aimed at detecting any vulnerabilities in the web server configuration that could be leveraged for tailored attacks.
4. Utilising IP lookup tools to identify the IP address of the MOP website.
5. Detailed examination of network packets in Wireshark to determine if any sensitive information was leaked during transmission.

4. Findings

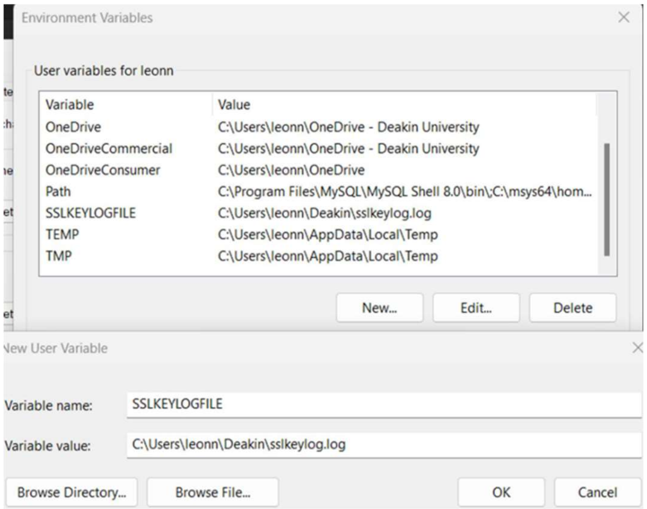
The findings of the security assessment are as follows:

1. **SSL/TLS encryption:** The encryption protocols utilised by the MOP website effectively protected all transmitted data, with no evidence of decryption or data leakage during the assessment.
2. **Cipher suite strength:** No weak cipher suites were identified during the testing, indicating robust encryption mechanisms in place.
3. **Web server security:** The web server hosting the MOP website appeared to be securely configured, with no apparent vulnerabilities detected that could be exploited for malicious purposes.
4. **Network traffic analysis:** Despite thorough examination of network packets in Wireshark, no sensitive information or exploitable data was found, affirming the efficacy of the security measures implemented.

In conclusion, the security measures implemented for the MOP website, particularly through GCP, are commendable and effectively safeguard against potential cyber threats. The SSL/TLS encryption, strong cipher suites, secure web server configuration, and proactive monitoring contribute to a robust defence posture, ensuring the confidentiality, integrity, and availability of data transmitted over the network. As a result, users can have confidence in the security of their interactions with the MOP website, mitigating the risk of unauthorised access and data breaches.

5. Conducting SSL Decryption

Step 1: Extract the SSLKEYLOGFILE from the settings in Windows 11. This can done in *System* > *About* > *Advanced System Settings* > *Environment Variables*. Select **New** and save the file as SSLKEYLOGFILE and select the directory in which the file will be saved in.



Environment Variables

User variables for leonn

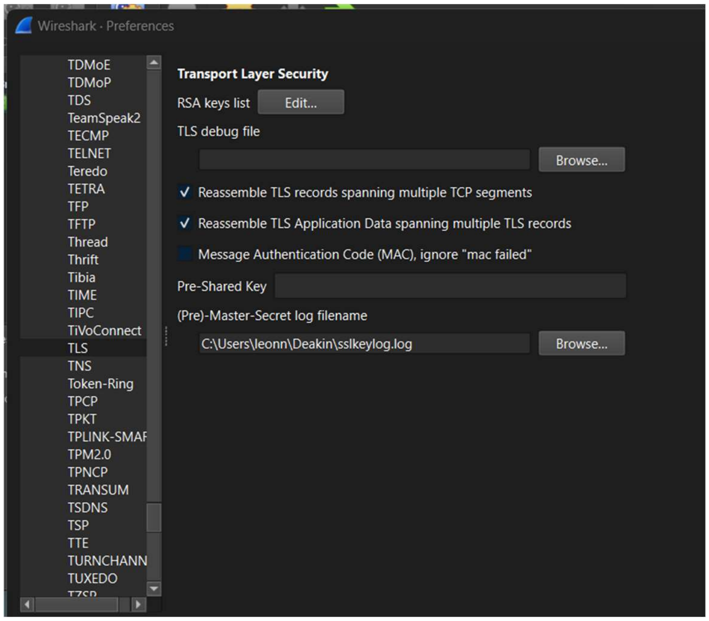
Variable	Value
OneDrive	C:\Users\leonn\OneDrive - Deakin University
OneDriveCommercial	C:\Users\leonn\OneDrive - Deakin University
OneDriveConsumer	C:\Users\leonn\OneDrive
Path	C:\Program Files\MySQL\MySQL Shell 8.0\bin\;C:\msys64\hom...
SSLKEYLOGFILE	C:\Users\leonn\Deakin\sslkeylog.log
TEMP	C:\Users\leonn\AppData\Local\Temp
TMP	C:\Users\leonn\AppData\Local\Temp

New User Variable

Variable name: SSLKEYLOGFILE

Variable value: C:\Users\leonn\Deakin\sslkeylog.log

Step 2: Open Wireshark and start monitoring the traffic. The SSLKEYLOGFILE will then need to be uploaded to Wireshark to decrypt the traffic. In Wireshark navigate to *Edit* > *Preferences* > *Protocols* > *TILS* and select **Browse** under Pre-Master-Secret log filename to upload the file.



Wireshark · Preferences

Transport Layer Security

RSA keys list Edit...

TLS debug file

✓ Reassemble TLS records spanning multiple TCP segments

✓ Reassemble TLS Application Data spanning multiple TLS records

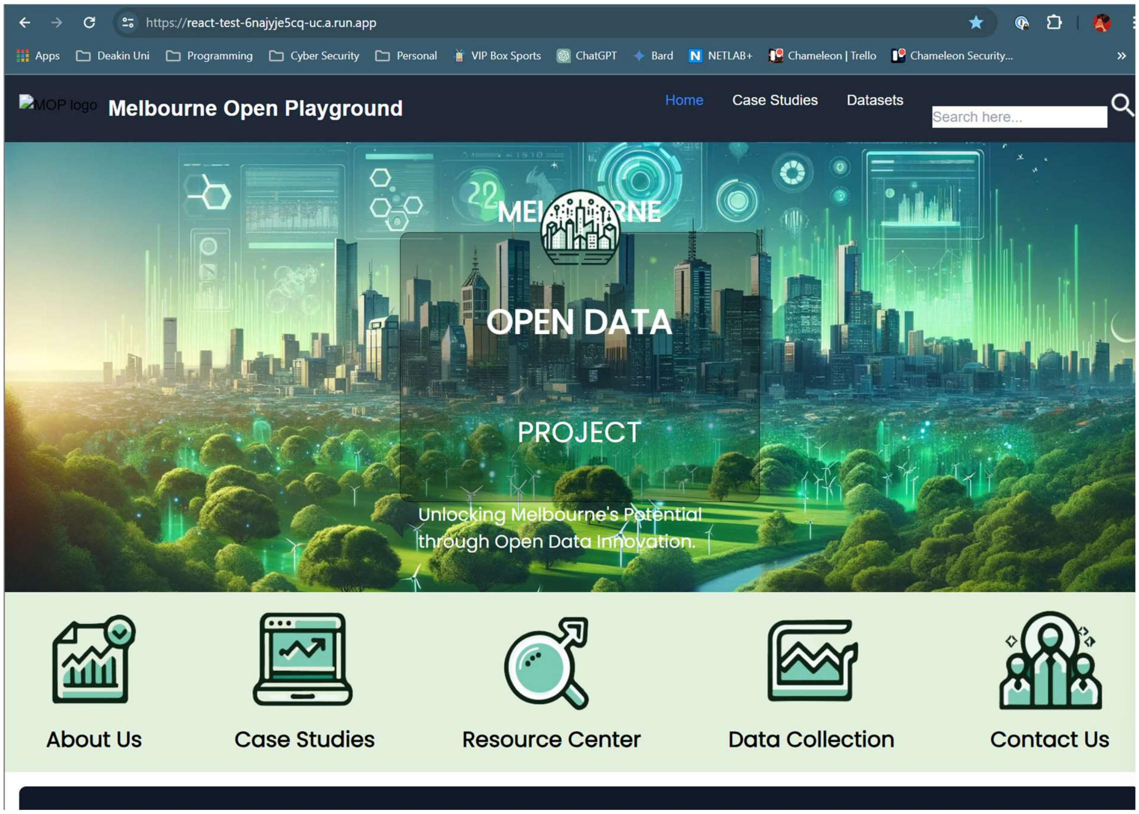
□ Message Authentication Code (MAC), ignore "mac failed"

Pre-Shared Key

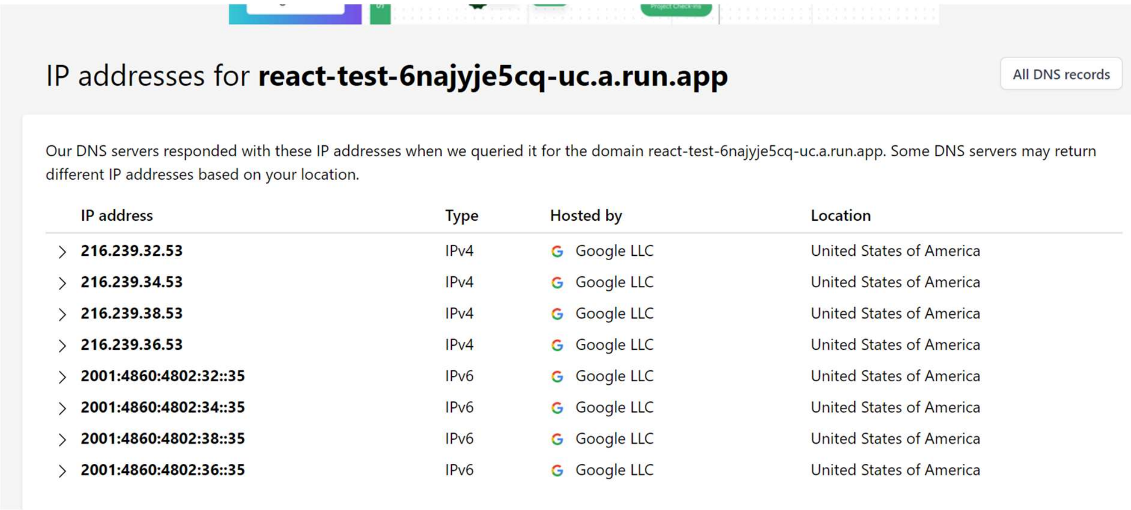
(Pre)-Master-Secret log filename

C:\Users\leonn\Deakin\sslkeylog.log

Step 3: Navigate to the MOP website in your browser of choice.



Step 4: Navigate to www.nslookup.io to search for the MOP website IP addresses. Enter the MOP website domain name and select **Find DNS records** and this should provide you with the IPv4 and IPv6 addresses as below.



IP addresses for **react-test-6najyje5cq-uc.a.run.app**

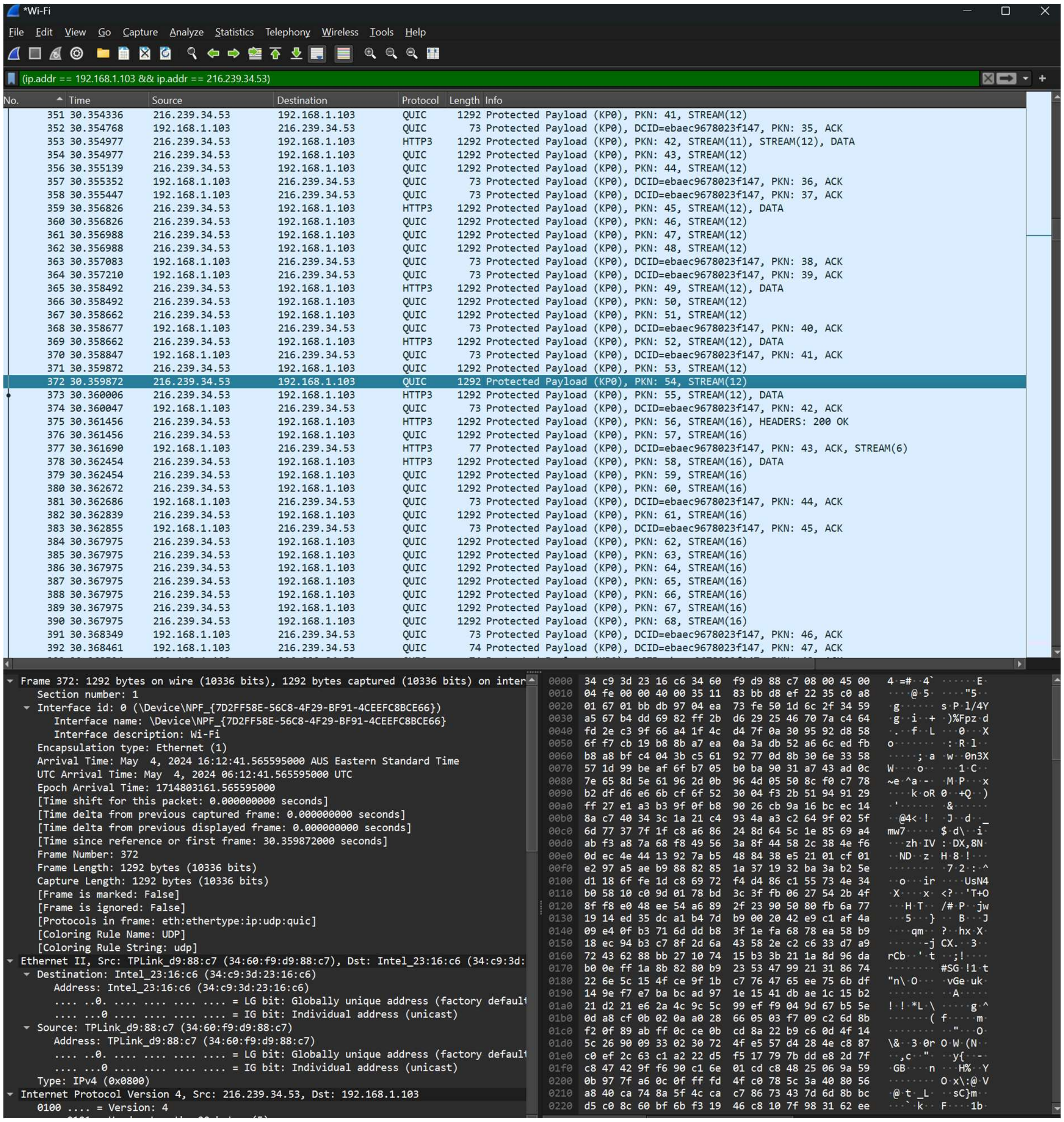
Our DNS servers responded with these IP addresses when we queried it for the domain react-test-6najyje5cq-uc.a.run.app. Some DNS servers may return different IP addresses based on your location.

IP address	Type	Hosted by	Location
216.239.32.53	IPv4	Google LLC	United States of America
216.239.34.53	IPv4	Google LLC	United States of America
216.239.38.53	IPv4	Google LLC	United States of America
216.239.36.53	IPv4	Google LLC	United States of America
2001:4860:4802:32::35	IPv6	Google LLC	United States of America
2001:4860:4802:34::35	IPv6	Google LLC	United States of America
2001:4860:4802:38::35	IPv6	Google LLC	United States of America
2001:4860:4802:36::35	IPv6	Google LLC	United States of America

Step 5: Go back to Wireshark. You will need to filter the IP ranges. The source IP will be your workstation's IP and the MOP website IP(s).

In the filter tab enter (ip.addr == yourIP && ip.addr == 216.239.34.53) and hit Enter. This should provide you with the network packets between your IP and the MOP website's IPv4 IP - you can analyse all four IP addresses should you wish.

Inspect the packets for any sensitive data. As noted, the packets are well protected within GCP, and nothing provided in the payloads can be used to exploit the web application. This was the result for all four IP addresses.



```
(ip.addr == 192.168.1.103 && ip.addr == 216.239.34.53)
```

```
No.      Time        Source          Destination     Protocol Length Info
    351 30.354336    216.239.34.53   192.168.1.103   QUIC     1292 Protected Payload (KP0), PKN: 41, STREAM(12)
    352 30.354768    192.168.1.103   216.239.34.53   QUIC       73 Protected Payload (KP0), DCID=ebaec9678023f147, PKN: 35, ACK
    353 30.354977    216.239.34.53   192.168.1.103   HTTP3    1292 Protected Payload (KP0), PKN: 42, STREAM(11), STREAM(12), DATA
    354 30.354977    216.239.34.53   192.168.1.103   QUIC     1292 Protected Payload (KP0), PKN: 43, STREAM(12)
    356 30.355139    216.239.34.53   192.168.1.103   QUIC     1292 Protected Payload (KP0), PKN: 44, STREAM(12)
    357 30.355352    192.168.1.103   216.239.34.53   QUIC       73 Protected Payload (KP0), DCID=ebaec9678023f147, PKN: 36, ACK
    358 30.355447    192.168.1.103   216.239.34.53   QUIC       73 Protected Payload (KP0), DCID=ebaec9678023f147, PKN: 37, ACK
    359 30.356826    216.239.34.53   192.168.1.103   HTTP3    1292 Protected Payload (KP0), PKN: 45, STREAM(12), DATA
    360 30.356826    216.239.34.53   192.168.1.103   QUIC     1292 Protected Payload (KP0), PKN: 46, STREAM(12)
    361 30.356988    216.239.34.53   192.168.1.103   QUIC     1292 Protected Payload (KP0), PKN: 47, STREAM(12)
    362 30.356988    216.239.34.53   192.168.1.103   QUIC     1292 Protected Payload (KP0), PKN: 48, STREAM(12)
    363 30.357083    192.168.1.103   216.239.34.53   QUIC       73 Protected Payload (KP0), DCID=ebaec9678023f147, PKN: 38, ACK
    364 30.357210    192.168.1.103   216.239.34.53   QUIC       73 Protected Payload (KP0), DCID=ebaec9678023f147, PKN: 39, ACK
    365 30.358492    216.239.34.53   192.168.1.103   HTTP3    1292 Protected Payload (KP0), PKN: 49, STREAM(12), DATA
    366 30.358492    216.239.34.53   192.168.1.103   QUIC     1292 Protected Payload (KP0), PKN: 50, STREAM(12)
    367 30.358662    216.239.34.53   192.168.1.103   QUIC     1292 Protected Payload (KP0), PKN: 51, STREAM(12)
    368 30.358677    192.168.1.103   216.239.34.53   QUIC       73 Protected Payload (KP0), DCID=ebaec9678023f147, PKN: 40, ACK
    369 30.358662    216.239.34.53   192.168.1.103   HTTP3    1292 Protected Payload (KP0), PKN: 52, STREAM(12), DATA
    370 30.358847    192.168.1.103   216.239.34.53   QUIC       73 Protected Payload (KP0), DCID=ebaec9678023f147, PKN: 41, ACK
    371 30.359872    216.239.34.53   192.168.1.103   QUIC     1292 Protected Payload (KP0), PKN: 53, STREAM(12)
    372 30.359872    216.239.34.53   192.168.1.103   QUIC     1292 Protected Payload (KP0), PKN: 54, STREAM(12)
    373 30.360006    216.239.34.53   192.168.1.103   HTTP3    1292 Protected Payload (KP0), PKN: 55, STREAM(12), DATA
    374 30.360047    192.168.1.103   216.239.34.53   QUIC       73 Protected Payload (KP0), DCID=ebaec9678023f147, PKN: 42, ACK
    375 30.361456    216.239.34.53   192.168.1.103   HTTP3    1292 Protected Payload (KP0), PKN: 56, STREAM(16), HEADERS: 200 OK
    376 30.361456    216.239.34.53   192.168.1.103   QUIC     1292 Protected Payload (KP0), PKN: 57, STREAM(16)
    377 30.361690    192.168.1.103   216.239.34.53   HTTP3      77 Protected Payload (KP0), DCID=ebaec9678023f147, PKN: 43, ACK, STREAM(6)
    378 30.362454    216.239.34.53   192.168.1.103   HTTP3    1292 Protected Payload (KP0), PKN: 58, STREAM(16), DATA
    379 30.362454    216.239.34.53   192.168.1.103   QUIC     1292 Protected Payload (KP0), PKN: 59, STREAM(16)
    380 30.362672    216.239.34.53   192.168.1.103   QUIC     1292 Protected Payload (KP0), PKN: 60, STREAM(16)
    381 30.362686    192.168.1.103   216.239.34.53   QUIC       73 Protected Payload (KP0), DCID=ebaec9678023f147, PKN: 44, ACK
    382 30.362839    216.239.34.53   192.168.1.103   QUIC     1292 Protected Payload (KP0), PKN: 61, STREAM(16)
    383 30.362855    192.168.1.103   216.239.34.53   QUIC       73 Protected Payload (KP0), DCID=ebaec9678023f147, PKN: 45, ACK
    384 30.367975    216.239.34.53   192.168.1.103   QUIC     1292 Protected Payload (KP0), PKN: 62, STREAM(16)
    385 30.367975    216.239.34.53   192.168.1.103   QUIC     1292 Protected Payload (KP0), PKN: 63, STREAM(16)
    386 30.367975    216.239.34.53   192.168.1.103   QUIC     1292 Protected Payload (KP0), PKN: 64, STREAM(16)
    387 30.367975    216.239.34.53   192.168.1.103   QUIC     1292 Protected Payload (KP0), PKN: 65, STREAM(16)
    388 30.367975    216.239.34.53   192.168.1.103   QUIC     1292 Protected Payload (KP0), PKN: 66, STREAM(16)
    389 30.367975    216.239.34.53   192.168.1.103   QUIC     1292 Protected Payload (KP0), PKN: 67, STREAM(16)
    390 30.367975    216.239.34.53   192.168.1.103   QUIC     1292 Protected Payload (KP0), PKN: 68, STREAM(16)
    391 30.368349    192.168.1.103   216.239.34.53   QUIC       73 Protected Payload (KP0), DCID=ebaec9678023f147, PKN: 46, ACK
    392 30.368461    192.168.1.103   216.239.34.53   QUIC       74 Protected Payload (KP0), DCID=ebaec9678023f147, PKN: 47, ACK
```

```
Frame 372: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on inter
   Section number: 1
   Interface id: 0 (\Device\NPF_{7D2FF58E-56C8-4F29-BF91-4CEEFC8BCE66})
      Interface name: \Device\NPF_{7D2FF58E-56C8-4F29-BF91-4CEEFC8BCE66}
      Interface description: Wi-Fi
   Encapsulation type: Ethernet (1)
   Arrival Time: May  4, 2024 16:12:41.565595000 AUS Eastern Standard Time
   UTC Arrival Time: May  4, 2024 06:12:41.565595000 UTC
   Epoch Arrival Time: 1714803161.565595000
   [Time shift for this packet: 0.000000000 seconds]
   [Time delta from previous captured frame: 0.000000000 seconds]
   [Time delta from previous displayed frame: 0.000000000 seconds]
   [Time since reference or first frame: 30.359872000 seconds]
   Frame Number: 372
   Frame Length: 1292 bytes (10336 bits)
   Capture Length: 1292 bytes (10336 bits)
   [Frame is marked: False]
   [Frame is ignored: False]
   [Protocols in frame: eth:ethertype:ip:udp:quic]
   [Coloring Rule Name: UDP]
   [Coloring Rule String: udp]
Ethernet II, Src: TPLink_d9:88:c7 (34:60:f9:d9:88:c7), Dst: Intel_23:16:c6 (34:c9:3d:
   Destination: Intel_23:16:c6 (34:c9:3d:23:16:c6)
      Address: Intel_23:16:c6 (34:c9:3d:23:16:c6)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
   Source: TPLink_d9:88:c7 (34:60:f9:d9:88:c7)
      Address: TPLink_d9:88:c7 (34:60:f9:d9:88:c7)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
   Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 216.239.34.53, Dst: 192.168.1.103
   0100 .... = Version: 4
```

```
0000  34 c9 3d 23 16 c6 34 60  f9 d9 88 c7 08 00 45 00   4·=#··4` ······E·
0010  04 fe 00 00 40 00 35 11  83 bb d8 ef 22 35 c0 a8   ····@·5· ····"5··
0020  01 67 01 bb db 97 04 ea  73 fe 50 1d 6c 2f 34 59   ·g······ s·P·l/4Y
0030  a5 67 b4 dd 69 82 ff 2b  d6 29 25 46 70 7a c4 64   ·g··i··+ ·)%Fpz·d
0040  fd 2e c3 9f 66 a4 1f 4c  d4 7f 0a 30 95 92 d8 58   ·.··f··L ···0···X
0050  6f f7 cb 19 b8 8b a7 ea  0a 3a db 52 a6 6c ed fb   o······· ·:·R·l··
0060  b8 a8 bf c4 04 3b c5 61  92 77 0d 8b 30 6e 33 58   ·····;·a ·w··0n3X
0070  57 1d 99 be af 6f b7 05  b0 ba 90 31 a7 43 ad 0c   W····o·· ···1·C··
0080  7e 65 8d 5e 61 96 2d 0b  96 4d 05 50 8c f0 c7 78   ~e·^a·-· ·M·P···x
0090  b2 df d6 e6 6b cf 6f 52  30 04 f3 2b 51 94 91 29   ····k·oR 0··+Q··)
00a0  ff 27 e1 a3 b3 9f 0f b8  90 26 cb 9a 16 bc ec 14   ·'······ ·&······
00b0  8a c7 40 34 3c 1a 21 c4  93 4a a3 c2 64 9f 02 5f   ··@4<·!· ·J··d··_
00c0  6d 77 37 7f 1f c8 a6 86  24 8d 64 5c 1e 85 69 a4   mw7····· $·d\··i·
00d0  ab f3 a8 7a 68 f8 49 56  3a 8f 44 58 2c 38 4e f6   ···zh·IV :·DX,8N·
00e0  0d ec 4e 44 13 92 7a b5  48 84 38 e5 21 01 cf 01   ··ND··z· H·8·!···
00f0  e2 97 a5 ae b9 88 82 85  1a 37 19 32 ba 3a b2 5e   ········ ·7·2·:·^
0100  d1 18 6f fe 1d c8 69 72  f4 d4 86 c1 55 73 4e 34   ··o···ir ····UsN4
0110  b0 58 10 c0 9d 01 78 bd  3c 3f fb 06 27 54 2b 4f   ·X····x· <?··'T+O
0120  8f f8 e0 48 ee 54 a6 89  2f 23 90 50 80 fb 6a 77   ···H·T·· /#·P··jw
0130  19 14 ed 35 dc a1 b4 7d  b9 00 20 42 e9 c1 af 4a   ···5···} ·· B···J
0140  09 e4 0f b3 71 6d dd b8  3f 1e fa 68 78 ea 58 b9   ····qm·· ?··hx·X·
0150  18 ec 94 b3 c7 8f 2d 6a  43 58 2e c2 c6 33 d7 a9   ······-j CX.··3··
0160  72 43 62 88 bb 27 10 74  15 b3 3b 21 1a 8d 96 da   rCb··'·t ··;!····
0170  b0 0e ff 1a 8b 82 80 b9  23 53 47 99 21 31 86 74   ········ #SG·!1·t
0180  22 6e 5c 15 4f ce 9f 1b  c7 76 47 65 ee 75 6b df   "n\·O··· ·vGe·uk·
0190  14 9e f7 e7 ba bc ad 97  1e 15 41 db ae 1c 15 b2   ········ ··A·····
01a0  21 d2 21 e6 2a 4c 9c 5c  99 ef f9 04 9d 67 b5 5e   !·!·*L·\ ·····g·^
01b0  0d a8 cf 0b 02 0a a0 28  66 05 03 f7 09 c2 6d 8b   ·······( f·····m·
01c0  f2 0f 89 ab ff 0c ce 0b  cd 8a 22 b9 c6 0d 4f 14   ········ ··"···O·
01d0  5c 26 90 09 33 02 30 72  4f e5 57 d4 28 4e c8 87   \&··3·0r O·W·(N··
01e0  c0 ef 2c 63 c1 a2 22 d5  f5 17 79 7b dd e8 2d 7f   ··,c··"· ··y{··-·
01f0  c8 47 42 9f f6 90 c1 6e  01 cd c8 48 25 06 9a 59   ·GB····n ···H%··Y
0200  0b 97 7f a6 0c 0f ff fd  4f c0 78 5c 3a 40 80 56   ········ O·x\:@·V
0210  a8 40 ca 74 8a 5f 4c ca  c7 86 73 43 7d 6d 8b bc   ·@·t·_L· ··sC}m··
0220  d5 c0 8c 60 bf 6b f3 19  46 c8 10 7f 98 31 62 ee   ···`·k·· F····1b·
```