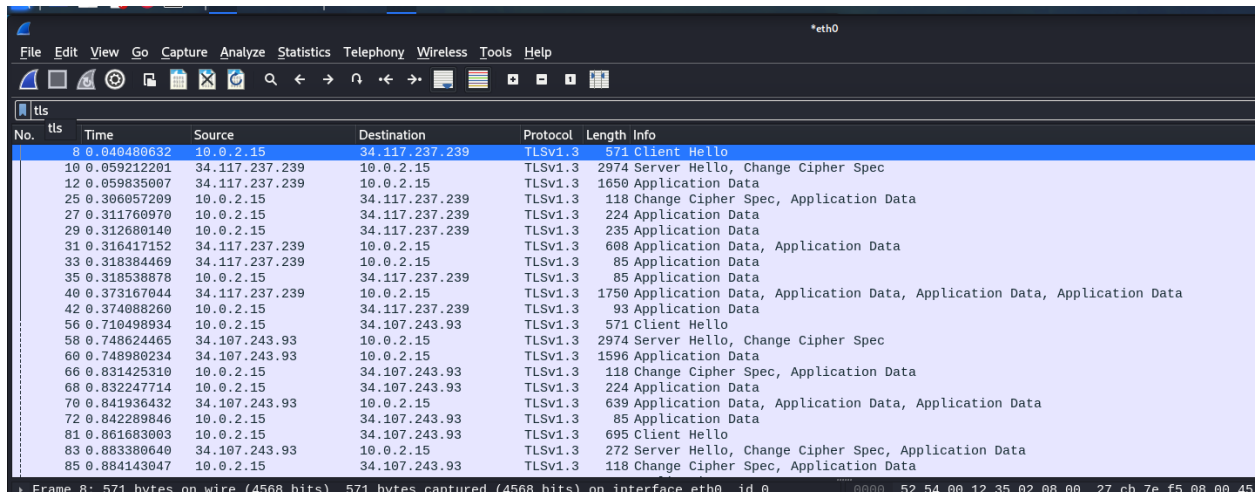


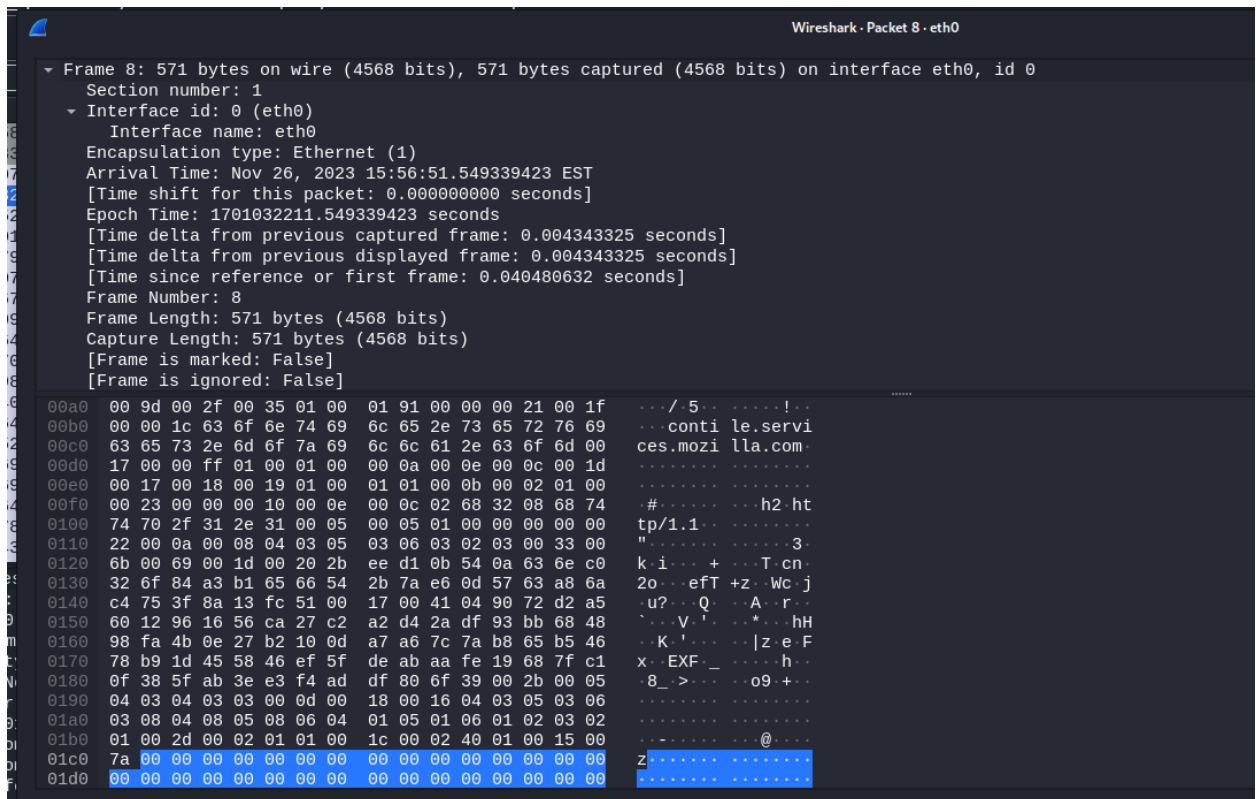
Lab 2: Privacy with Wireshark and TLS

Wireshark output after visiting unt.edu



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|----------------|----------------|----------|--------|--|
| 8 | 0.040480632 | 10.0.2.15 | 34.117.237.239 | TLSv1.3 | 571 | Client Hello |
| 10 | 0.059212201 | 34.117.237.239 | 10.0.2.15 | TLSv1.3 | 2974 | Server Hello, Change Cipher Spec |
| 12 | 0.059835007 | 34.117.237.239 | 10.0.2.15 | TLSv1.3 | 1650 | Application Data |
| 25 | 0.306057209 | 10.0.2.15 | 34.117.237.239 | TLSv1.3 | 118 | Change Cipher Spec, Application Data |
| 27 | 0.311760970 | 10.0.2.15 | 34.117.237.239 | TLSv1.3 | 224 | Application Data |
| 29 | 0.312680140 | 10.0.2.15 | 34.117.237.239 | TLSv1.3 | 235 | Application Data |
| 31 | 0.316417152 | 34.117.237.239 | 10.0.2.15 | TLSv1.3 | 608 | Application Data, Application Data |
| 33 | 0.318384469 | 34.117.237.239 | 10.0.2.15 | TLSv1.3 | 85 | Application Data |
| 35 | 0.318538878 | 10.0.2.15 | 34.117.237.239 | TLSv1.3 | 85 | Application Data |
| 40 | 0.373167044 | 34.117.237.239 | 10.0.2.15 | TLSv1.3 | 1750 | Application Data, Application Data, Application Data, Application Data |
| 42 | 0.374088260 | 10.0.2.15 | 34.117.237.239 | TLSv1.3 | 93 | Application Data |
| 56 | 0.710498934 | 10.0.2.15 | 34.107.243.93 | TLSv1.3 | 571 | Client Hello |
| 58 | 0.748624465 | 34.107.243.93 | 10.0.2.15 | TLSv1.3 | 2974 | Server Hello, Change Cipher Spec |
| 60 | 0.748980234 | 34.107.243.93 | 10.0.2.15 | TLSv1.3 | 1596 | Application Data |
| 66 | 0.831425310 | 10.0.2.15 | 34.107.243.93 | TLSv1.3 | 118 | Change Cipher Spec, Application Data |
| 68 | 0.832247714 | 10.0.2.15 | 34.107.243.93 | TLSv1.3 | 224 | Application Data |
| 70 | 0.841936432 | 34.107.243.93 | 10.0.2.15 | TLSv1.3 | 639 | Application Data, Application Data, Application Data |
| 72 | 0.842289846 | 10.0.2.15 | 34.107.243.93 | TLSv1.3 | 85 | Application Data |
| 81 | 0.861683003 | 10.0.2.15 | 34.107.243.93 | TLSv1.3 | 695 | Client Hello |
| 83 | 0.883380640 | 34.107.243.93 | 10.0.2.15 | TLSv1.3 | 272 | Server Hello, Change Cipher Spec, Application Data |
| 85 | 0.884143047 | 10.0.2.15 | 34.107.243.93 | TLSv1.3 | 118 | Change Cipher Spec, Application Data |

TLS handshake packet data for :



Wireshark · Packet 8 · eth0

▼ Frame 8: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface eth0, id 0

Section number: 1

▼ Interface id: 0 (eth0)

Interface name: eth0

Encapsulation type: Ethernet (1)

Arrival Time: Nov 26, 2023 15:56:51.549339423 EST

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1701032211.549339423 seconds

[Time delta from previous captured frame: 0.004343325 seconds]

[Time delta from previous displayed frame: 0.004343325 seconds]

[Time since reference or first frame: 0.040480632 seconds]

Frame Number: 8

Frame Length: 571 bytes (4568 bits)

Capture Length: 571 bytes (4568 bits)

[Frame is marked: False]

[Frame is ignored: False]

00a0 00 9d 00 2f 00 35 01 00 01 91 00 00 00 21 00 1f ... / 5 ... ! ..

00b0 00 00 1c 63 6f 6e 74 69 6c 65 2e 73 65 72 76 69 ... conti le.servi

00c0 63 65 73 2e 6d 6f 7a 69 6c 6c 61 2e 63 6f 6d 00 ... ces.mozi lla.com

00d0 17 00 00 ff 01 00 01 00 00 0a 00 0e 00 0c 00 1d ...

00e0 00 17 00 18 00 19 01 00 01 01 00 0b 00 02 01 00 ...

00f0 00 23 00 00 00 10 00 0e 00 0c 02 68 32 08 68 74 ... # ... h2 ht

0100 74 70 2f 31 2e 31 00 05 00 05 01 00 00 00 00 00 ... tp/1.1 ...

0110 22 00 0a 00 08 04 03 05 03 06 03 02 03 00 33 00 ... " ... 3.

0120 6b 00 69 00 1d 00 20 2b ee d1 0b 54 0a 63 6e c0 ... k i ... + ... T.cn

0130 32 6f 84 a3 b1 65 66 54 2b 7a e6 0d 57 63 a8 6a ... 2o ... efT +z ... Wc.j

0140 c4 75 3f 8a 13 fc 51 00 17 00 41 04 90 72 d2 a5 ... u? ... Q ... A ... r ...

0150 60 12 96 16 56 ca 27 c2 a2 d4 2a df 93 bb 68 48 ... V ... ' ... * ... hH

0160 98 fa 4b 0e 27 b2 10 0d a7 a6 7c 7a b8 65 b5 46 ... K ... ' ... | z e F

0170 78 b9 1d 45 58 46 ef 5f de ab aa fe 19 68 7f c1 ... x ... EXF ... h ...

0180 0f 38 5f ab 3e e3 f4 ad df 80 6f 39 00 2b 00 05 ... 8 ... > ... o9 ... + ...

0190 04 03 04 03 03 00 0d 00 18 00 16 04 03 05 03 06 ...

01a0 03 08 04 08 05 08 06 04 01 05 01 06 01 02 03 02 ...

01b0 01 00 2d 00 02 01 01 00 1c 00 02 40 01 00 15 00 ... @ ...

01c0 7a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ... z ...

01d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...

After completing the handshake, view of application data packet:

Wireshark · Packet 12 · eth0

TCP payload (1596 bytes)
 TCP segment data (1596 bytes)
 [2 Reassembled TCP Segments (4383 bytes): #10(2787), #12(1596)]
 [Frame: 10, payload: 0-2786 (2787 bytes)]
 [Frame: 12, payload: 2787-4382 (1596 bytes)]
 [Segment count: 2]
 [Reassembled TCP length: 4383]
 [Reassembled TCP Data: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e2...]
 Transport Layer Security
 TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
 Opaque Type: Application Data (23)
 Version: TLS 1.2 (0x0303)
 Length: 4378
 Encrypted Application Data: 0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...
 [Application Data Protocol: Hypertext Transfer Protocol]

| | | |
|------|---|-----------------------|
| 0000 | 17 03 03 11 1a 0b b2 da cd 92 21 87 d8 65 09 4c |!..e.L |
| 0010 | 89 da 68 60 f9 52 fe e2 4b 9b 76 62 89 c4 56 bf | ..h..R.. K.vb..V. |
| 0020 | ae b6 17 e2 57 55 14 6b 65 b4 1c 06 36 bf d7 6f | ...WU.k e...6..o |
| 0030 | 80 ae 95 45 28 e9 4d e0 a7 5f 7f 16 ee 21 53 e0 | ...E(.M.!S. |
| 0040 | 14 fd 43 f2 30 86 28 5f 3f 4e cd 6f 14 19 b8 69 | ..C.0.(_ ?N.o...i |
| 0050 | 97 a9 3f 71 43 2c 49 dc 60 80 e8 18 c3 20 9b 0e | ..?qC,I- |
| 0060 | 83 d0 18 90 a2 df ea 4f 0e 17 7e 2e bb 9e 2e b4 |0 ..~..... |
| 0070 | 94 a9 28 2d 2c 81 8e a4 94 ef 3a 17 3e 32 3b f8 | ..(-,.... :>2;.. |
| 0080 | 1c 79 46 62 08 a9 54 71 91 30 3c eb 4e 5f b5 08 | ..yFb..Tq ..0<_N.. |
| 0090 | 0d 36 b0 66 7d 59 0e 8e 4c 48 36 e5 d8 c3 9a 76 | ..6.f}Y.. LH6...v |
| 00a0 | 8b 18 f9 74 21 69 ca 5a 01 bb d1 e1 a4 eb c0 03 | ...tli.Z |
| 00b0 | 18 4b 30 43 5c 69 b4 f4 ad 87 ce aa 38 d9 d7 ba | ..K0C\i..8... . |
| 00c0 | e2 6a 24 23 55 5e b6 2f 12 8b f3 ec 67 91 e2 13 | ..j\$#U^./g... . |
| 00d0 | 46 bb df 72 eb 8e 6a b5 21 0d 64 db e0 8c d4 ad | F..r..j. !.d..... |
| 00e0 | 29 5c 9a b2 3e 03 ef 94 e6 e8 53 97 55 ec 4a d9 |)\...>... ..S.U.J. |
| 00f0 | 39 fc e2 2d 2d 88 fc 0f cc 97 a3 5f 7c 0e cb f3 | 9..... .._ |
| 0100 | b5 ad 63 34 0e 0a d5 88 11 ff 91 2d 30 30 a6 91 | ..c4....00.. . |
| 0110 | 9b 3b c7 88 96 70 23 30 5e 16 df 12 2f 53 29 d2 | .;...p#0 ^.../S).. |

Frame (1650 bytes) Reassembled TCP (4383 bytes)

Bytes 5-4382: Encrypted Application Data (tls.app_data)

✓ Show packet bytes

TLS stream:

Wireshark · Follow TLS Stream (tcp.stream eq 0) · eth0

Follow TLS Stream (tcp.stream eq 0) · eth0

Stream 0: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 1: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 2: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 3: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 4: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 5: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 6: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 7: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 8: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 9: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 10: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 11: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 12: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 13: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 14: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 15: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 16: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 17: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 18: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 19: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 20: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 21: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 22: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 23: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 24: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 25: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 26: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 27: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 28: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 29: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 30: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 31: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 32: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 33: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 34: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 35: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 36: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 37: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 38: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 39: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 40: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 41: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 42: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 43: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 44: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 45: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 46: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 47: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 48: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 49: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 50: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 51: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 52: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 53: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 54: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 55: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 56: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 57: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 58: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 59: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 60: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 61: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 62: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 63: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 64: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 65: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 66: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 67: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 68: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 69: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 70: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 71: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 72: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 73: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 74: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 75: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 76: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 77: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 78: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 79: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 80: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 81: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 82: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 83: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 84: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 85: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 86: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 87: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 88: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 89: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 90: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 91: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 92: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 93: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 94: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 95: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 96: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 97: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 98: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 99: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 100: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 101: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 102: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 103: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 104: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 105: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 106: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 107: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 108: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 109: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 110: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 111: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 112: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 113: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 114: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 115: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 116: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

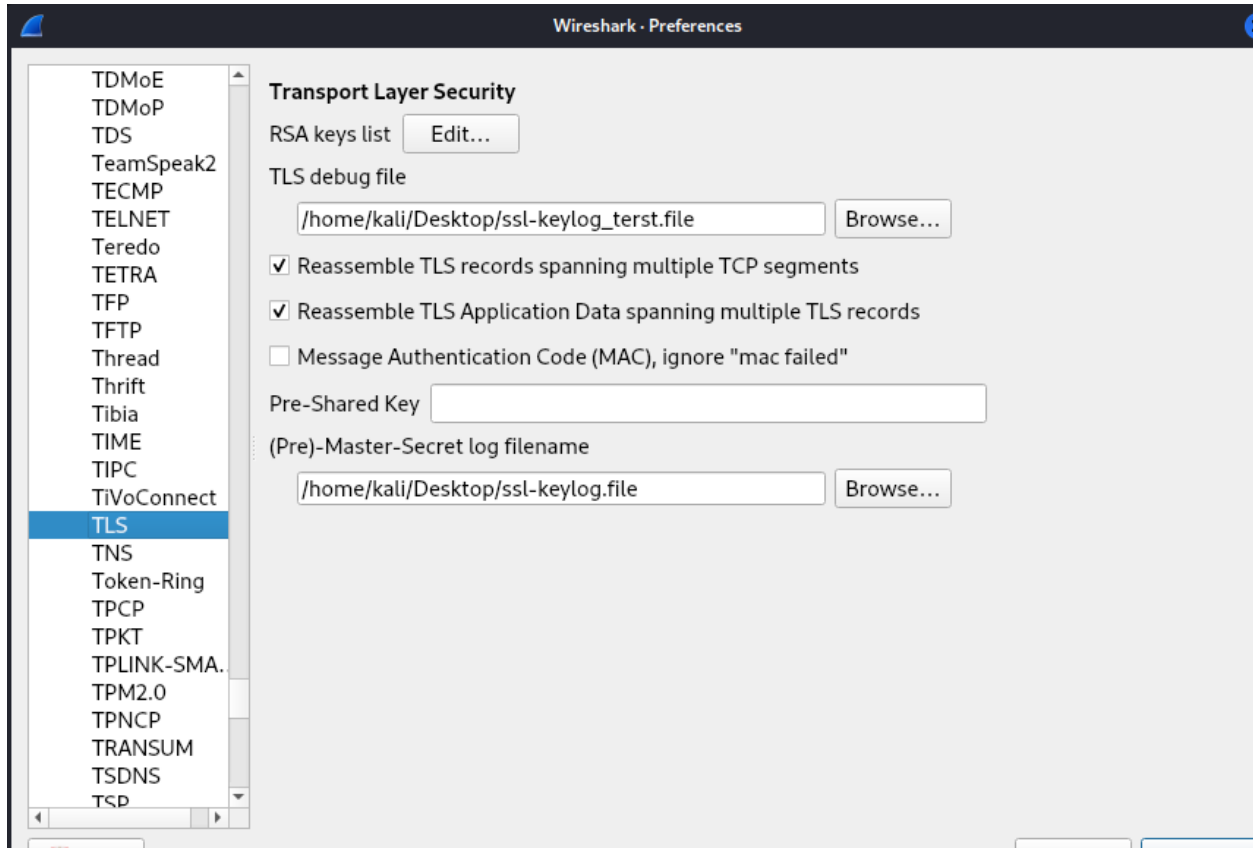
Stream 117: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 118: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

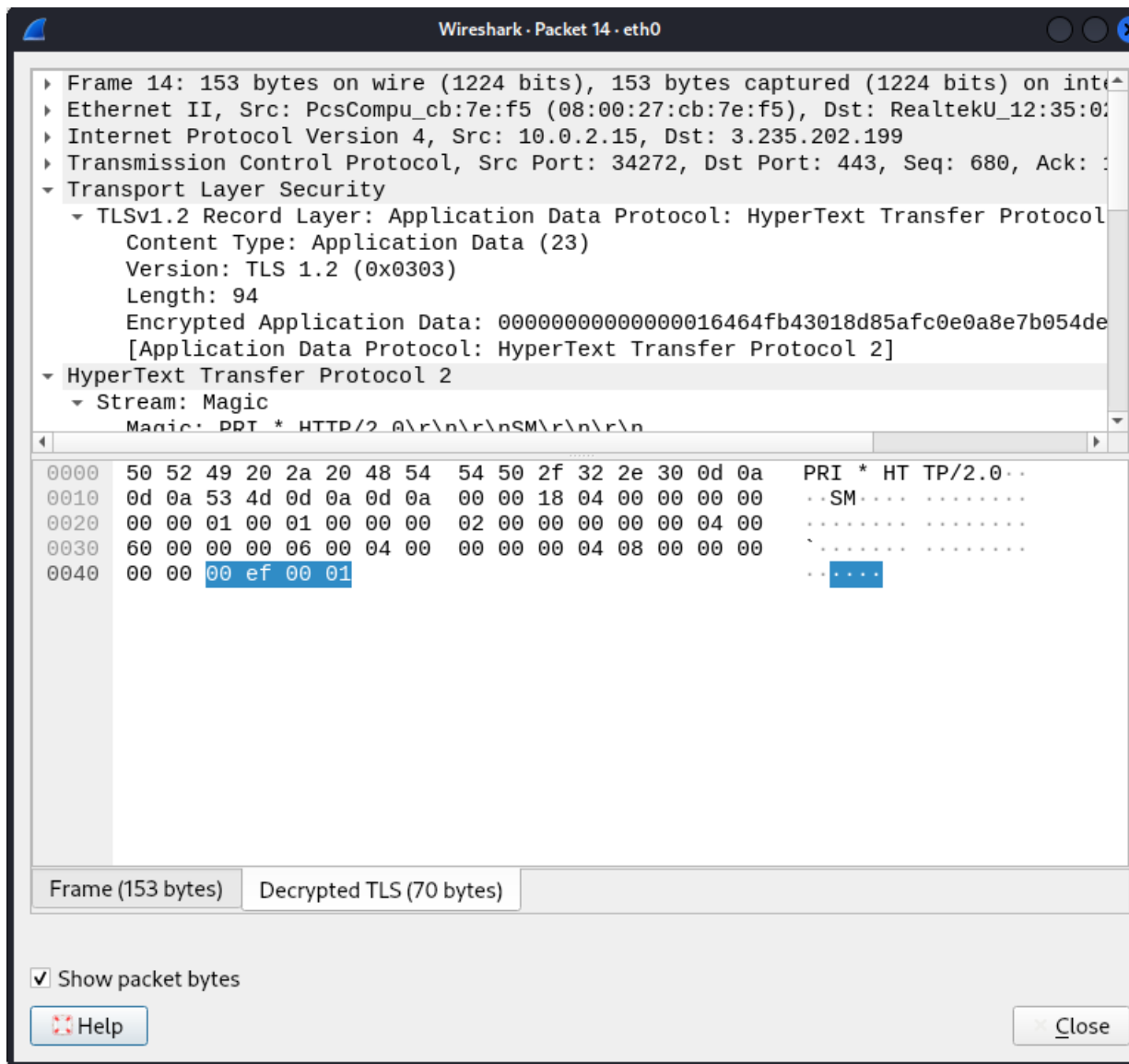
Stream 119: 170303111a0bb2dacd922187d865094c89da6860f952fee24b9b766289c456bfaeb617e25755146b65...

Stream 120: 170303111a0bb2dacd922187d865094c

Note: The SSL protocol (SSLv2 and SSLv3) hasn't been in use for several years, having been superseded by TLSv1. While some programs still start with SSLv2-compatible handshakes or occasionally use the SSLv2-style record format, they all generally use TLS nowadays and the Wireshark configuration page has been renamed accordingly. The display filter is `tls`.



Decrypted TLS stream: As the ssl being



Other packet:

Wireshark · Packet 44 · eth0

- ▶ Frame 44: 1072 bytes on wire (8576 bits), 1072 bytes captured (8576 bits) on interface
- ▶ Ethernet II, Src: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: RealtekU_12:35:02
- ▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 20.225.32.183
- ▶ Transmission Control Protocol, Src Port: 56496, Dst Port: 443, Seq: 850, Ack: 36
- ▼ Transport Layer Security
 - ▼ TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
 - Content Type: Application Data (23)
 - Version: TLS 1.2 (0x0303)
 - Length: 1013
 - Encrypted Application Data: 00000000000000001ad5b4fffb981c14b19ce9f1a54b911f3
 - [Application Data Protocol: Hypertext Transfer Protocol]
 - ▶ Hypertext Transfer Protocol

| Offset | Hex | ASCII |
|--------|-------------------------|--|
| 0000 | 47 45 54 20 2f 20 48 54 | GET / HTTP/1.1 |
| 0010 | 48 6f 73 74 3a 20 77 77 | Host: www.unt.edu |
| 0020 | 75 0d 0a 43 6f 6e 6e 65 | User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:11.0) Gecko/20100101 Firefox/11.0 |
| 0030 | 65 65 70 2d 61 6c 69 76 | Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 |
| 0040 | 2d 43 6f 6e 74 72 6f 6c | Accept-Language: en-US,en;q=0.5 |
| 0050 | 65 3d 30 0d 0a 73 65 63 | Cache-Control: max-age=0 |
| 0060 | 22 43 68 72 6f 6d 69 75 | Connection: keep-alive |
| 0070 | 39 22 2c 20 22 4e 6f 74 | Sec-CH-UA: "Chromium";v="119", "Not A Brand";v="24" |
| 0080 | 22 3b 76 3d 22 32 34 22 | Sec-CH-UA-Mobile: ?0 |
| 0090 | 2d 75 61 2d 6d 6f 62 69 | Sec-CH-UA-Platform: "Linux" |
| 00a0 | 73 65 63 2d 63 68 2d 75 | Upgrade-Insecure-Requests: 1 |
| 00b0 | 72 6d 3a 20 22 4c 69 6e | Accept-Encoding: gzip, deflate, br |
| 00c0 | 72 61 64 65 2d 49 6e 73 | |
| 00d0 | 71 75 65 73 74 73 3a 20 | |
| 00e0 | 41 67 65 6e 74 3a 20 4d | |
| 00f0 | 2e 30 20 28 58 31 31 3b | |

Frame (1072 bytes) Decrypted TLS (989 bytes)

Now looking for the http packet:

Wireshark interface showing a TLS handshake and an HTTP GET request. The main packet list on the left shows packets 9 through 97. Packet 17 is selected, showing details for Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Transport Layer Security (TLSv1.2). The TLSv1.2 Record Layer details show the Content Type as Application Data (23), Version as TLS 1.2 (0x0303), Length as 527, and Encrypted Application Data as 00000000000000002c6c794a0e2bc7cdee44b7ae1af7563. The Hypertext Transfer Protocol 2 details show the Stream ID as 1, Length as 494, and the GET request for /heat.aspx?aid=8543&url=https%3A%2F%2Fwww.unt.edu%2F&uid=9da6ff-f8-47e0-bbdb-7a75-5eec3ec9e185&p=s%7C0%7C0&ww=92-8&wh=814&o=1&d=1-26&prev=9fafed0d-375e-c6.

Wireshark - Packet 17 - eth0

Frame 17: 586 bytes on wire (4688 bits), 586 bytes captured (4688 bits) on interface eth0
Ethernet II, Src: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: RealtekU_12:35:00:00:00:00
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 3.235.202.199
Transmission Control Protocol, Src Port: 34272, Dst Port: 443, Seq: 779, Ack: 123, Win: 0, Len: 0
Transport Layer Security
 TLSv1.2 Record Layer: Application Data Protocol: HyperText Transfer Protocol 2
 Content Type: Application Data (23)
 Version: TLS 1.2 (0x0303)
 Length: 527
 Encrypted Application Data: 00000000000000002c6c794a0e2bc7cdee44b7ae1af7563
 [Application Data Protocol: HyperText Transfer Protocol 2]
 Hypertext Transfer Protocol 2
 Stream: HEADERS, Stream ID: 1, Length 494, GET /heat.aspx?aid=8543&url=https%3A%2F%2Fwww.unt.edu%2F&uid=9da6ff-f8-47e0-bbdb-7a75-5eec3ec9e185&p=s%7C0%7C0&ww=92-8&wh=814&o=1&d=1-26&prev=9fafed0d-375e-c6

Frame (586 bytes) | Decrypted TLS (503 bytes) | Decompressed Header (809 bytes)