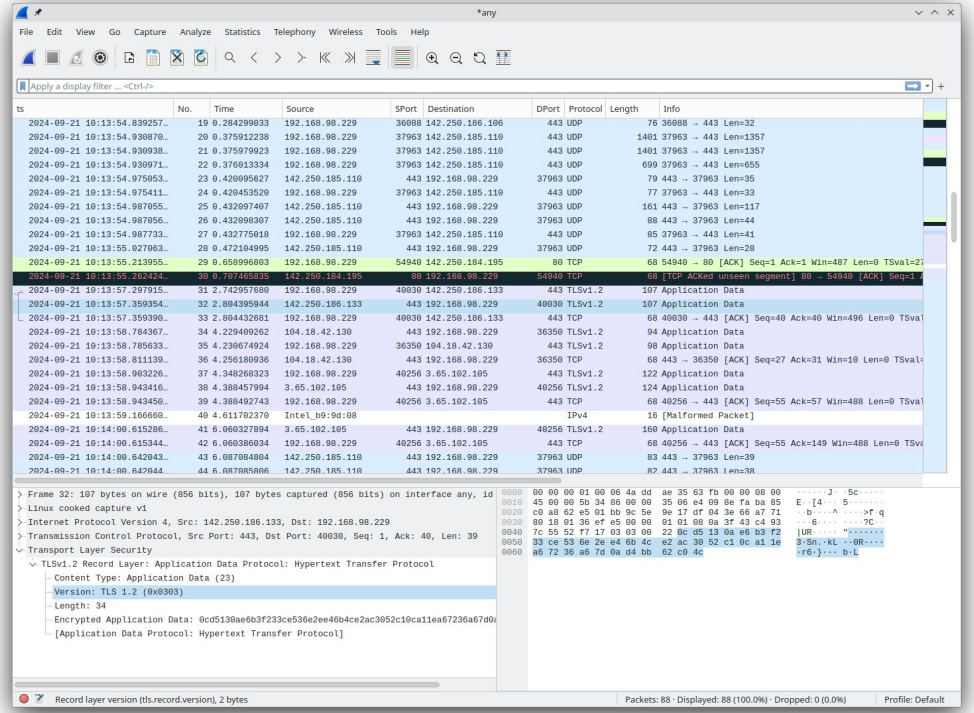
Staffbase

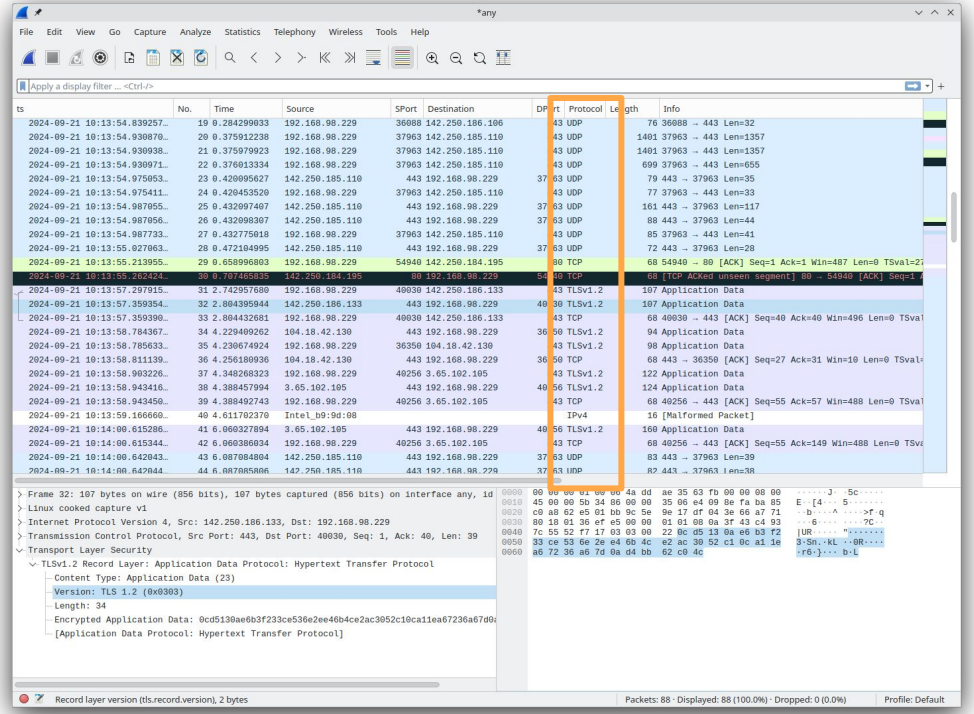
Wireshark um eigene Protokolle erweitern

Jiří Kraml
Backend Engineer

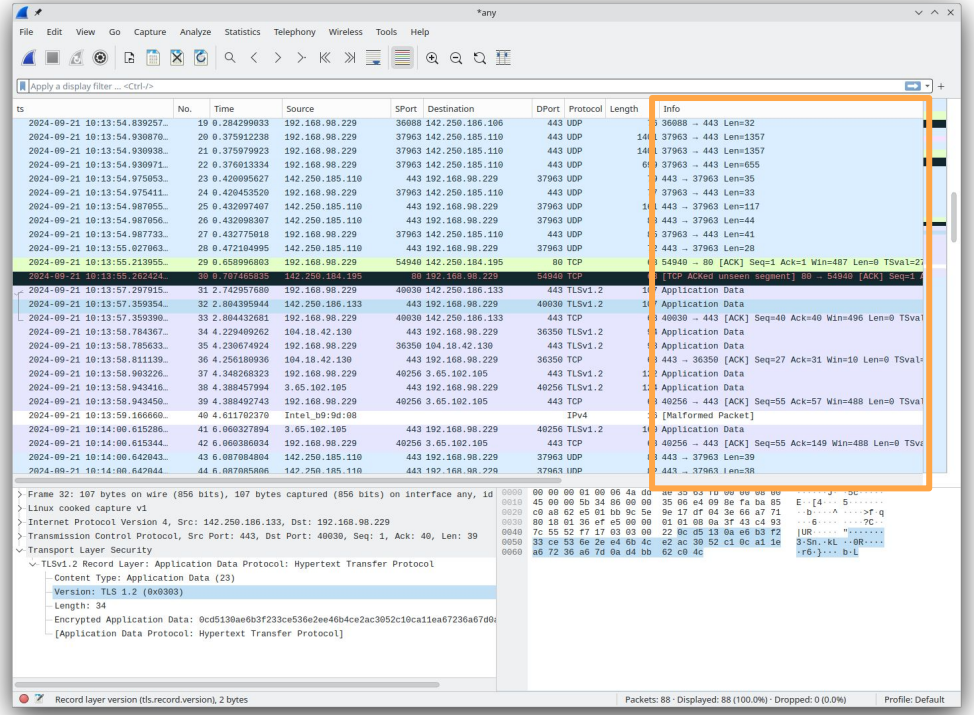
Wireshark


*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
ts No. Time Source SPort Destination DPort Protocol Length Info
2024-09-21 10:13:54.839257… 19 0.284299033 192.168.98.229 36088 142.250.186.106 443 UDP 76 36088 → 443 Len=32
2024-09-21 10:13:54.930870… 20 0.375912238 192.168.98.229 37963 142.250.185.110 443 UDP 1401 37963 → 443 Len=1357
2024-09-21 10:13:54.930938… 21 0.375979923 192.168.98.229 37963 142.250.185.110 443 UDP 1401 37963 → 443 Len=1357
2024-09-21 10:13:54.930971… 22 0.376013334 192.168.98.229 37963 142.250.185.110 443 UDP 699 37963 → 443 Len=655
2024-09-21 10:13:54.975053… 23 0.420095627 142.250.185.110 443 192.168.98.229 37963 UDP 79 443 → 37963 Len=35
2024-09-21 10:13:54.975411… 24 0.420453520 192.168.98.229 37963 142.250.185.110 443 UDP 77 37963 → 443 Len=33
2024-09-21 10:13:54.987055… 25 0.432097407 142.250.185.110 443 192.168.98.229 37963 UDP 161 443 → 37963 Len=117
2024-09-21 10:13:54.987056… 26 0.432098307 142.250.185.110 443 192.168.98.229 37963 UDP 88 443 → 37963 Len=44
2024-09-21 10:13:54.987733… 27 0.432775018 192.168.98.229 37963 142.250.185.110 443 UDP 85 37963 → 443 Len=41
2024-09-21 10:13:55.027063… 28 0.472104995 142.250.185.110 443 192.168.98.229 37963 UDP 72 443 → 37963 Len=28
2024-09-21 10:13:55.213955… 29 0.658996803 192.168.98.229 54940 142.250.184.195 80 TCP 68 54940 → 80 [ACK] Seq=1 Ack=1 Win=487 Len=0 TSval=27
2024-09-21 10:13:55.262424… 30 0.707465835 142.250.184.195 80 192.168.98.229 54940 TCP 68 [TCP ACKed unseen segment] 80 → 54940 [ACK] Seq=1
2024-09-21 10:13:57.297915… 31 2.742957680 192.168.98.229 40030 142.250.186.133 443 TLSv1.2 107 Application Data
2024-09-21 10:13:57.359354… 32 2.804395944 142.250.186.133 443 192.168.98.229 40030 TLSv1.2 107 Application Data
2024-09-21 10:13:57.359390… 33 2.804432681 192.168.98.229 40030 142.250.186.133 443 TCP 68 40030 → 443 [ACK] Seq=40 Ack=40 Win=496 Len=0 TSval
2024-09-21 10:13:58.784367… 34 4.229409262 104.18.42.130 443 192.168.98.229 36350 TLSv1.2 94 Application Data
2024-09-21 10:13:58.785633… 35 4.230674924 192.168.98.229 36350 104.18.42.130 443 TLSv1.2 98 Application Data
2024-09-21 10:13:58.811139… 36 4.256180936 104.18.42.130 443 192.168.98.229 36350 TCP 68 443 → 36350 [ACK] Seq=27 Ack=31 Win=10 Len=0 TSval=
2024-09-21 10:13:58.903226… 37 4.348268323 192.168.98.229 40256 3.65.102.105 443 TLSv1.2 122 Application Data
2024-09-21 10:13:58.943416… 38 4.388457994 3.65.102.105 443 192.168.98.229 40256 TLSv1.2 124 Application Data
2024-09-21 10:13:58.943450… 39 4.388492743 192.168.98.229 40256 3.65.102.105 443 TCP 68 40256 → 443 [ACK] Seq=55 Ack=57 Win=488 Len=0 TSval
2024-09-21 10:13:59.166660… 40 4.611702370 Intel_b9:9d:08 IPv4 16 [Malformed Packet]
2024-09-21 10:14:00.615286… 41 6.060327894 3.65.102.105 443 192.168.98.229 40256 TLSv1.2 160 Application Data
2024-09-21 10:14:00.615344… 42 6.060386034 192.168.98.229 40256 3.65.102.105 443 TCP 68 40256 → 443 [ACK] Seq=55 Ack=149 Win=488 Len=0 TSval
2024-09-21 10:14:00.642043… 43 6.087084804 142.250.185.110 443 192.168.98.229 37963 UDP 83 443 → 37963 Len=39
2024-09-21 10:14:00.642044… 44 6.087085806 142.250.185.110 443 192.168.98.229 37963 UDP 82 443 → 37963 Len=38
Frame 32: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface any, id
Linux cooked capture v1
Internet Protocol Version 4, Src: 142.250.186.133, Dst: 192.168.98.229
Transmission Control Protocol, Src Port: 443, Dst Port: 40030, Seq: 1, Ack: 40, Len: 39
Transport Layer Security
TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
Content Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 34
Encrypted Application Data: 0cd5130ae6b3f233ce536e2ee46b4ce2ac3052c10ca11ea67236a67d0a
[Application Data Protocol: Hypertext Transfer Protocol]
0000 00 00 00 01 00 06 4a dd ae 35 63 fb 00 00 08 00 ·····J· ·5c·····
0010 45 00 00 5b 34 86 00 00 35 06 e4 09 8e fa ba 85 E··[4··· 5·····
0020 c0 a8 62 e5 01 bb 9c 5e 9e 17 df 04 3e 66 a7 71 ··b····^ ····>f·q
0030 80 18 01 36 ef e5 00 00 01 01 08 0a 3f 43 c4 93 ···6···· ····?C··
0040 7c 55 52 f7 17 03 03 00 22 0c d5 13 0a e6 b3 f2 |UR····· "·v·····
0050 33 ce 53 6e 2e e4 6b 4c e2 ac 30 52 c1 0c a1 1e 3·Sn·kL ··0R····
0060 a6 72 36 a6 7d 0a d4 bb 62 c0 4c ·r6·}··· b·L
Record layer version (tls.record.version), 2 bytes
Packets: 88 · Displayed: 88 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

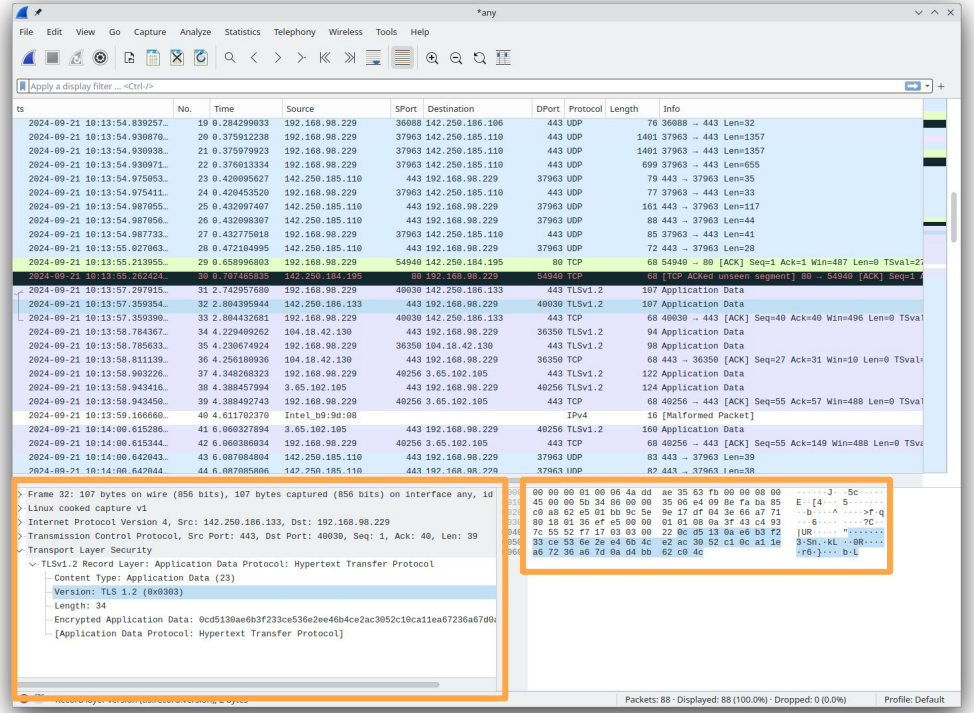
Wireshark


*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Frame 32: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface any, id
Linux cooked capture v1
Internet Protocol Version 4, Src: 142.250.186.133, Dst: 192.168.98.229
Transmission Control Protocol, Src Port: 443, Dst Port: 40030, Seq: 1, Ack: 40, Len: 39
Transport Layer Security
TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
Content Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 34
Encrypted Application Data: 0cd5130ae6b3f233ce536e2ee46b4ce2ac3052c10ca11ea67236a67d0a
[Application Data Protocol: Hypertext Transfer Protocol]
Record layer version (tls.record.version), 2 bytes
Packets: 88 · Displayed: 88 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

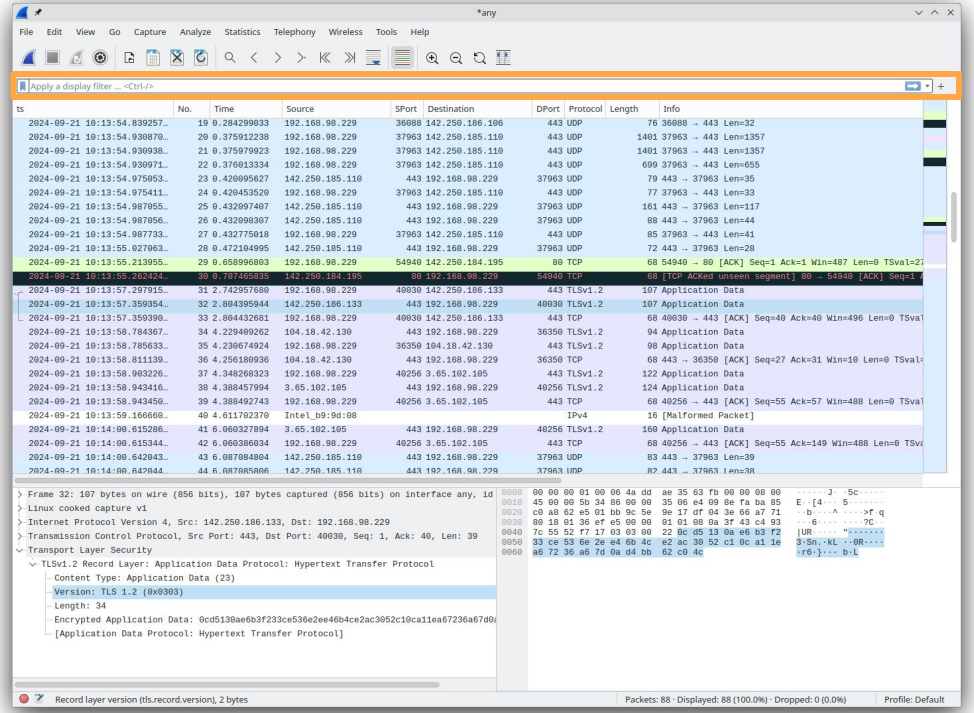
Wireshark


*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
ts No. Time Source SPort Destination DPort Protocol Length Info
2024-09-21 10:13:54.839257… 19 0.284299033 192.168.98.229 36088 142.250.186.106 443 UDP 36088 → 443 Len=32
2024-09-21 10:13:54.930870… 20 0.375912238 192.168.98.229 37963 142.250.185.110 443 UDP 37963 → 443 Len=1357
2024-09-21 10:13:54.930938… 21 0.375979923 192.168.98.229 37963 142.250.185.110 443 UDP 37963 → 443 Len=1357
2024-09-21 10:13:54.930971… 22 0.376013334 192.168.98.229 37963 142.250.185.110 443 UDP 37963 → 443 Len=655
2024-09-21 10:13:54.975053… 23 0.420095627 142.250.185.110 443 192.168.98.229 37963 UDP 443 → 37963 Len=35
2024-09-21 10:13:54.975411… 24 0.420453520 192.168.98.229 37963 142.250.185.110 443 UDP 37963 → 443 Len=33
2024-09-21 10:13:54.987055… 25 0.432097407 142.250.185.110 443 192.168.98.229 37963 UDP 443 → 37963 Len=117
2024-09-21 10:13:54.987056… 26 0.432098307 142.250.185.110 443 192.168.98.229 37963 UDP 443 → 37963 Len=44
2024-09-21 10:13:54.987733… 27 0.432775018 192.168.98.229 37963 142.250.185.110 443 UDP 37963 → 443 Len=41
2024-09-21 10:13:55.027063… 28 0.472104995 142.250.185.110 443 192.168.98.229 37963 UDP 443 → 37963 Len=28
2024-09-21 10:13:55.213955… 29 0.658996803 192.168.98.229 54940 142.250.184.195 80 TCP 54940 → 80 [ACK] Seq=1 Ack=1 Win=487 Len=0 TSval=27
2024-09-21 10:13:55.262424… 30 0.707465835 142.250.184.195 80 192.168.98.229 54940 TCP [TCP ACKed unseen segment] 80 → 54940 [ACK] Seq=1
2024-09-21 10:13:57.297915… 31 2.742957680 192.168.98.229 40030 142.250.186.133 443 TLSv1.2 Application Data
2024-09-21 10:13:57.359354… 32 2.804395944 142.250.186.133 443 192.168.98.229 40030 TLSv1.2 Application Data
2024-09-21 10:13:57.359390… 33 2.804432681 192.168.98.229 40030 142.250.186.133 443 TCP 40030 → 443 [ACK] Seq=40 Ack=40 Win=496 Len=0 TSval
2024-09-21 10:13:58.784367… 34 4.229409262 104.18.42.130 443 192.168.98.229 36350 TLSv1.2 Application Data
2024-09-21 10:13:58.785633… 35 4.230674924 192.168.98.229 36350 104.18.42.130 443 TLSv1.2 Application Data
2024-09-21 10:13:58.811139… 36 4.256180936 104.18.42.130 443 192.168.98.229 36350 TCP 443 → 36350 [ACK] Seq=27 Ack=31 Win=10 Len=0 TSval
2024-09-21 10:13:58.903226… 37 4.348268323 192.168.98.229 40256 3.65.102.105 443 TLSv1.2 Application Data
2024-09-21 10:13:58.943416… 38 4.388457994 3.65.102.105 443 192.168.98.229 40256 TLSv1.2 Application Data
2024-09-21 10:13:58.943450… 39 4.388492743 192.168.98.229 40256 3.65.102.105 443 TCP 40256 → 443 [ACK] Seq=55 Ack=57 Win=488 Len=0 TSval
2024-09-21 10:13:59.166660… 40 4.611702370 Intel_b9:9d:08 IPv4 [Malformed Packet]
2024-09-21 10:14:00.615286… 41 6.060327894 3.65.102.105 443 192.168.98.229 40256 TLSv1.2 Application Data
2024-09-21 10:14:00.615344… 42 6.060386034 192.168.98.229 40256 3.65.102.105 443 TCP 40256 → 443 [ACK] Seq=55 Ack=149 Win=488 Len=0 TSval
2024-09-21 10:14:00.642043… 43 6.087084804 142.250.185.110 443 192.168.98.229 37963 UDP 443 → 37963 Len=39
Frame 32: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface any, id
Linux cooked capture v1
Internet Protocol Version 4, Src: 142.250.186.133, Dst: 192.168.98.229
Transmission Control Protocol, Src Port: 443, Dst Port: 40030, Seq: 1, Ack: 40, Len: 39
Transport Layer Security
TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
Content Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 34
Encrypted Application Data: 0cd5130ae6b3f233ce536e2ee46b4ce2ac3052c10ca11ea67236a67d0
[Application Data Protocol: Hypertext Transfer Protocol]
0000 00 00 00 01 00 06 4a dd
0010 45 00 00 5b 34 86 00 00 35 06 e4 09 8e fa ba 85
0020 c0 a8 62 e5 01 bb 9c 5e 9e 17 df 04 3e 66 a7 71
0030 80 18 01 36 ef e5 00 00 01 01 08 0a 3f 43 c4 93
0040 7c 55 52 f7 17 03 03 00 22 0c d5 13 0a e6 b3 f2
0050 33 ce 53 6e 2e e4 6b 4c e2 ac 30 52 c1 0c a1 1e
0060 a6 72 36 a6 7d 0a d4 bb 62 c0 4c
Record layer version (tls.record.version), 2 bytes
Packets: 88 · Displayed: 88 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

Wireshark

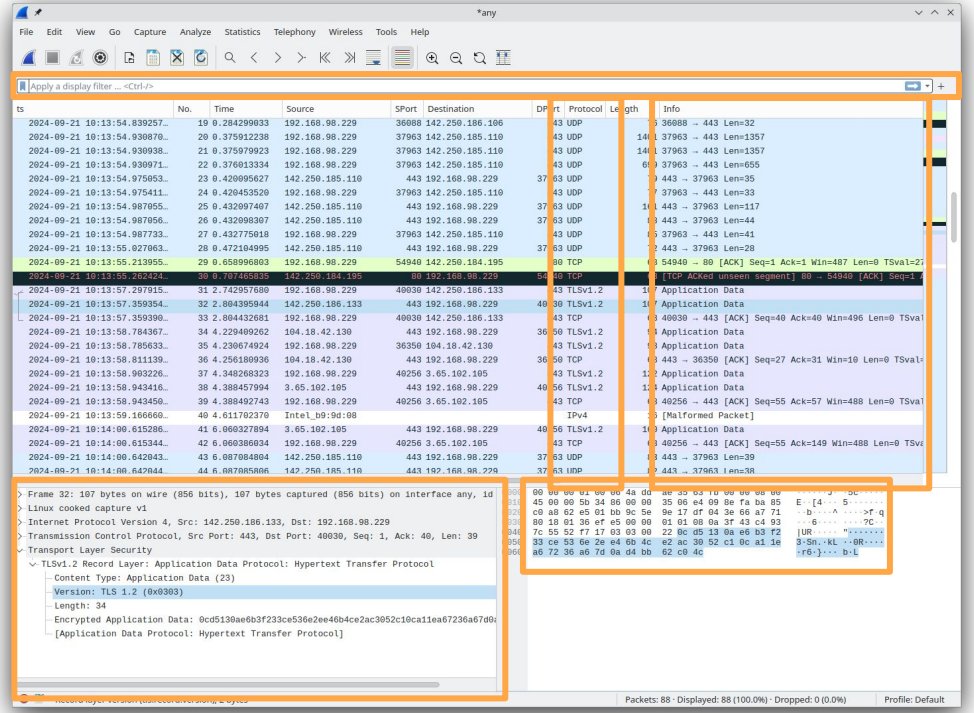

*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
ts No. Time Source SPort Destination DPort Protocol Length Info
2024-09-21 10:13:54.839257… 19 0.284299033 192.168.98.229 36088 142.250.186.106 443 UDP 76 36088 → 443 Len=32
2024-09-21 10:13:54.930870… 20 0.375912238 192.168.98.229 37963 142.250.185.110 443 UDP 1401 37963 → 443 Len=1357
2024-09-21 10:13:54.930938… 21 0.375979923 192.168.98.229 37963 142.250.185.110 443 UDP 1401 37963 → 443 Len=1357
2024-09-21 10:13:54.930971… 22 0.376013334 192.168.98.229 37963 142.250.185.110 443 UDP 699 37963 → 443 Len=655
2024-09-21 10:13:54.975053… 23 0.420095627 142.250.185.110 443 192.168.98.229 37963 UDP 79 443 → 37963 Len=35
2024-09-21 10:13:54.975411… 24 0.420453520 192.168.98.229 37963 142.250.185.110 443 UDP 77 37963 → 443 Len=33
2024-09-21 10:13:54.987055… 25 0.432097407 142.250.185.110 443 192.168.98.229 37963 UDP 161 443 → 37963 Len=117
2024-09-21 10:13:54.987056… 26 0.432098307 142.250.185.110 443 192.168.98.229 37963 UDP 88 443 → 37963 Len=44
2024-09-21 10:13:54.987733… 27 0.432775018 192.168.98.229 37963 142.250.185.110 443 UDP 85 37963 → 443 Len=41
2024-09-21 10:13:55.027063… 28 0.472104995 142.250.185.110 443 192.168.98.229 37963 UDP 72 443 → 37963 Len=28
2024-09-21 10:13:55.213955… 29 0.658996803 192.168.98.229 54940 142.250.184.195 80 TCP 68 54940 → 80 [ACK] Seq=1 Ack=1 Win=487 Len=0 TSval=27
2024-09-21 10:13:55.262424… 30 0.707465835 142.250.184.195 80 192.168.98.229 54940 TCP 68 [TCP ACKed unseen segment] 80 → 54940 [ACK] Seq=1
2024-09-21 10:13:57.297915… 31 2.742957680 192.168.98.229 40030 142.250.186.133 443 TLSv1.2 107 Application Data
2024-09-21 10:13:57.359354… 32 2.804395944 142.250.186.133 443 192.168.98.229 40030 TLSv1.2 107 Application Data
2024-09-21 10:13:57.359390… 33 2.804432681 192.168.98.229 40030 142.250.186.133 443 TCP 68 40030 → 443 [ACK] Seq=40 Ack=40 Win=496 Len=0 TSval
2024-09-21 10:13:58.784367… 34 4.229409262 104.18.42.130 443 192.168.98.229 36350 TLSv1.2 94 Application Data
2024-09-21 10:13:58.785633… 35 4.230674924 192.168.98.229 36350 104.18.42.130 443 TLSv1.2 98 Application Data
2024-09-21 10:13:58.811139… 36 4.256180936 104.18.42.130 443 192.168.98.229 36350 TCP 68 443 → 36350 [ACK] Seq=27 Ack=31 Win=10 Len=0 TSval=
2024-09-21 10:13:58.903226… 37 4.348268323 192.168.98.229 40256 3.65.102.105 443 TLSv1.2 122 Application Data
2024-09-21 10:13:58.943416… 38 4.388457994 3.65.102.105 443 192.168.98.229 40256 TLSv1.2 124 Application Data
2024-09-21 10:13:58.943450… 39 4.388492743 192.168.98.229 40256 3.65.102.105 443 TCP 68 40256 → 443 [ACK] Seq=55 Ack=57 Win=488 Len=0 TSval
2024-09-21 10:13:59.166660… 40 4.611702370 Intel_b9:9d:08 IPv4 16 [Malformed Packet]
2024-09-21 10:14:00.615286… 41 6.060327894 3.65.102.105 443 192.168.98.229 40256 TLSv1.2 160 Application Data
2024-09-21 10:14:00.615344… 42 6.060386034 192.168.98.229 40256 3.65.102.105 443 TCP 68 40256 → 443 [ACK] Seq=55 Ack=149 Win=488 Len=0 TSval
2024-09-21 10:14:00.642043… 43 6.087084804 142.250.185.110 443 192.168.98.229 37963 UDP 83 443 → 37963 Len=39
2024-09-21 10:14:00.642044… 44 6.087085806 142.250.185.110 443 192.168.98.229 37963 UDP 82 443 → 37963 Len=38
Frame 32: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface any, id
Linux cooked capture v1
Internet Protocol Version 4, Src: 142.250.186.133, Dst: 192.168.98.229
Transmission Control Protocol, Src Port: 443, Dst Port: 40030, Seq: 1, Ack: 40, Len: 39
Transport Layer Security
TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
Content Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 34
Encrypted Application Data: 0cd5130ae6b3f233ce536e2ee46b4ce2ac3052c10ca11ea67236a67d0
[Application Data Protocol: Hypertext Transfer Protocol]
00 00 00 01 00 06 4a dd ae 35 63 fb 00 00 08 00 ·····J· ·5c·····
45 00 00 5b 34 86 00 00 35 06 e4 09 8e fa ba 85 E··[4··· 5·····
c0 a8 62 e5 01 bb 9c 5e 9e 17 df 04 3e 66 a7 71 ··b····^ ····>f·q
80 18 01 36 ef e5 00 00 01 01 08 0a 3f 43 c4 93 ···6···· ····?C··
7c 55 52 f7 17 03 03 00 22 0c d5 13 0a e6 b3 f2 |UR····· "·v·····
33 ce 53 6e 2e e4 6b 4c e2 ac 30 52 c1 0c a1 1e 3·Sn.·kL ··0R····
a6 72 36 a6 7d 0a d4 bb 62 c0 4c ·r6·}··· b·L
Packets: 88 · Displayed: 88 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

Wireshark


*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
ts No. Time Source SPort Destination DPort Protocol Length Info
2024-09-21 10:13:54.839257… 19 0.284299033 192.168.98.229 36088 142.250.186.106 443 UDP 76 36088 → 443 Len=32
2024-09-21 10:13:54.930870… 20 0.375912238 192.168.98.229 37963 142.250.185.110 443 UDP 1401 37963 → 443 Len=1357
2024-09-21 10:13:54.930938… 21 0.375979923 192.168.98.229 37963 142.250.185.110 443 UDP 1401 37963 → 443 Len=1357
2024-09-21 10:13:54.930971… 22 0.376013334 192.168.98.229 37963 142.250.185.110 443 UDP 699 37963 → 443 Len=655
2024-09-21 10:13:54.975053… 23 0.420095627 142.250.185.110 443 192.168.98.229 37963 UDP 79 443 → 37963 Len=35
2024-09-21 10:13:54.975411… 24 0.420453520 192.168.98.229 37963 142.250.185.110 443 UDP 77 37963 → 443 Len=33
2024-09-21 10:13:54.987055… 25 0.432097407 142.250.185.110 443 192.168.98.229 37963 UDP 161 443 → 37963 Len=117
2024-09-21 10:13:54.987056… 26 0.432098307 142.250.185.110 443 192.168.98.229 37963 UDP 88 443 → 37963 Len=44
2024-09-21 10:13:54.987733… 27 0.432775018 192.168.98.229 37963 142.250.185.110 443 UDP 85 37963 → 443 Len=41
2024-09-21 10:13:55.027063… 28 0.472104995 142.250.185.110 443 192.168.98.229 37963 UDP 72 443 → 37963 Len=28
2024-09-21 10:13:55.213955… 29 0.658996803 192.168.98.229 54940 142.250.184.195 80 TCP 68 54940 → 80 [ACK] Seq=1 Ack=1 Win=487 Len=0 TSval=27
2024-09-21 10:13:55.262424… 30 0.707465835 142.250.184.195 80 192.168.98.229 54940 TCP 68 [TCP ACKed unseen segment] 80 → 54940 [ACK] Seq=1
2024-09-21 10:13:57.297915… 31 2.742957680 192.168.98.229 40030 142.250.186.133 443 TLSv1.2 107 Application Data
2024-09-21 10:13:57.359354… 32 2.804395944 142.250.186.133 443 192.168.98.229 40030 TLSv1.2 107 Application Data
2024-09-21 10:13:57.359390… 33 2.804432681 192.168.98.229 40030 142.250.186.133 443 TCP 68 40030 → 443 [ACK] Seq=40 Ack=40 Win=496 Len=0 TSval
2024-09-21 10:13:58.784367… 34 4.229409262 104.18.42.130 443 192.168.98.229 36350 TLSv1.2 94 Application Data
2024-09-21 10:13:58.785633… 35 4.230674924 192.168.98.229 36350 104.18.42.130 443 TLSv1.2 98 Application Data
2024-09-21 10:13:58.811139… 36 4.256180936 104.18.42.130 443 192.168.98.229 36350 TCP 68 443 → 36350 [ACK] Seq=27 Ack=31 Win=10 Len=0 TSval=
2024-09-21 10:13:58.903226… 37 4.348268323 192.168.98.229 40256 3.65.102.105 443 TLSv1.2 122 Application Data
2024-09-21 10:13:58.943416… 38 4.388457994 3.65.102.105 443 192.168.98.229 40256 TLSv1.2 124 Application Data
2024-09-21 10:13:58.943450… 39 4.388492743 192.168.98.229 40256 3.65.102.105 443 TCP 68 40256 → 443 [ACK] Seq=55 Ack=57 Win=488 Len=0 TSval
2024-09-21 10:13:59.166660… 40 4.611702370 Intel_b9:9d:08 IPv4 16 [Malformed Packet]
2024-09-21 10:14:00.615286… 41 6.060327894 3.65.102.105 443 192.168.98.229 40256 TLSv1.2 160 Application Data
2024-09-21 10:14:00.615344… 42 6.060386034 192.168.98.229 40256 3.65.102.105 443 TCP 68 40256 → 443 [ACK] Seq=55 Ack=149 Win=488 Len=0 TSva
2024-09-21 10:14:00.642043… 43 6.087084804 142.250.185.110 443 192.168.98.229 37963 UDP 83 443 → 37963 Len=39
2024-09-21 10:14:00.642044… 44 6.087085806 142.250.185.110 443 192.168.98.229 37963 UDP 82 443 → 37963 Len=38
Frame 32: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface any, id
Linux cooked capture v1
Internet Protocol Version 4, Src: 142.250.186.133, Dst: 192.168.98.229
Transmission Control Protocol, Src Port: 443, Dst Port: 40030, Seq: 1, Ack: 40, Len: 39
Transport Layer Security
TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
Content Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 34
Encrypted Application Data: 0cd5130ae6b3f233ce536e2ee46b4ce2ac3052c10ca11ea67236a67d0a
[Application Data Protocol: Hypertext Transfer Protocol]
0000 00 00 00 01 00 06 4a dd ae 35 63 fb 00 00 08 00 ·····J· ·5c·····
0010 45 00 00 5b 34 86 00 00 35 06 e4 09 8e fa ba 85 E··[4··· 5·····
0020 c0 a8 62 e5 01 bb 9c 5e 9e 17 df 04 3e 66 a7 71 ··b····^ ····>f·q
0030 80 18 01 36 ef e5 00 00 01 01 08 0a 3f 43 c4 93 ···6···· ····?C··
0040 7c 55 52 f7 17 03 03 00 22 0c d5 13 0a e6 b3 f2 |UR····· "·v·····
0050 33 ce 53 6e 2e e4 6b 4c e2 ac 30 52 c1 0c a1 1e 3·Sn·kL ··0R····
0060 a6 72 36 a6 7d 0a d4 bb 62 c0 4c ·r6·}··· b·L
Record layer version (tls.record.version), 2 bytes
Packets: 88 · Displayed: 88 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

Wireshark

- C?
- Lua Support!
- “Dissectoren” für das Verarbeiten von Paketen



Was Ihr heute lernt

- Ihr schreibt ein wenig Lua-Code
- Ihr implementiert Dissectoren für simple Demoprotokolle

Was Ihr heute lernt

- Ihr schreibt ein wenig Lua-Code
- Ihr implementiert Dissectoren für simple Demoprotokolle

- Ihr seht es live und traut euch die Umsetzung zu!

Lokales Setup

Lokales Setup

Wireshark installieren

Idealerweise über den Paketmanager

Packet Dumps runterladen

Siehe `github.com/jkraml-staffbase`

Lokales Setup

Scriptordner

Meistens `$HOME/.local/lib/wireshark/plugins`

Editor

Eure Wahl

Lokales Setup

Scriptordner

Meistens `$HOME/.local/lib/wireshark/plugins`

Editor

Eure Wahl

`workshop.lua`

Lokales Setup

Scriptordner

Meistens `$HOME/.local/lib/wireshark/plugins`

Editor

Eure Wahl

workshop.lua

```
print("hello world")
```

Protokoll #1: Temperaturmessung

Protokoll #1: Temperaturmessung

- UDP
- Konstante Länge
- Nur eine Messung pro UDP Paket

Uint8 (1 Byte)	Float32 (4 Byte, bigendian)
Sensor ID	Messwert

Basics: UDP/TCP

Basics: UDP/TCP

- PDU Protocol Data Unit

Basics: UDP/TCP

- PDU Protocol Data Unit

- UDP → Packet

Basics: UDP/TCP

- PDU Protocol Data Unit

- UDP → Packet

- TCP → Stream

Basics: UDP/TCP

- PDU Protocol Data Unit

- UDP → Packet

- TCP → Stream

Protokoll #2: Börsendaten

Protokoll #2: Börsendaten

- TCP
- Explizite Längenangabe

Uint8 (1 Byte)	Char[] (1-4 Bytes)	Float32 (4 Byte, bigendian)
Symbollänge	Tickersymbol	Preis

Protokoll #3:
Null-terminierter Text

Protokoll #3: Null-terminierter Text

- TCP
- Länge während Verarbeitung unbekannt

Char[] (n Bytes)	Endzeichen (1 Byte)
Text	Null-Byte

Protokoll #4:
Gebündelte Temperaturmessung

Protokoll #4: Gebündelte Temperaturmessung

- UDP
- Reserviertes Byte
- Halbwegs Rückwärtskompatibel

– (1 Byte)	Uint32 (4 B, be.)	n * PDU (n * 5 B)
0xFF	Anzahl	Einzelne Messungen

Weiterführende Links

- Wireshark: Dokumentation zu Lua [link]
- Wireshark: Wiki [link]
- Das Github Repository zu diesem Workshop [link]

Kommt ins Team!

Kommt einfach am Stand vorbei, wir sind da.

Oder meldet euch:

jiri.kraml@staffbase.com

LinkedIn

Danke!