

Wireshark um eigene Protokolle erweitern

Jiří Kraml
Backend Engineer



Wireshark

The screenshot displays the Wireshark interface with a list of captured network packets. The packet list pane shows various protocols including UDP, TCP, and TLSv1.2. The selected packet (No. 32) is a TLSv1.2 record, which is expanded in the packet details pane to show its structure: Content Type (Application Data), Version (TLS 1.2), Length (34), and Encrypted Application Data. The packet bytes pane shows the raw hex and ASCII data of the selected packet.

No.	Time	Source	SPort	Destination	DPort	Protocol	Length	Info
2024-09-21 10:13:54.839257	19.0	284299033	192.168.98.229	36988 142.250.186.106	443	UDP	76	36988 → 443 Len=32
2024-09-21 10:13:54.930878	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	420909527	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	420435209	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	432775918	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	658996003	192.168.98.229	54940 142.250.184.195	80	TCP	68	54940 → 80 [ACK] Seq=1 Win=487 Len=0 TSval=27
2024-09-21 10:13:55.262424	30.0	787465835	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	40930 142.250.186.133	443	TLSv1.2	107	Application Data
2024-09-21 10:13:57.359394	32.2	804399944	142.250.186.133	443 192.168.98.229	40930	TLSv1.2	107	Application Data
2024-09-21 10:13:57.359396	33.2	804432601	192.168.98.229	40930 142.250.186.133	443	TCP	68	40930 → 443 [ACK] Seq=40 Ack=40 Win=496 Len=0 TSval=17
2024-09-21 10:13:58.784367	34.4	229489262	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=17
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=17
2024-09-21 10:13:59.166666	40.4	611702370	Intel_b9:9d:08			IPv4	3	[Malformed Packet]
2024-09-21 10:14:00.615296	41.0	96937894	3.65.102.105	443 192.168.98.229	40256	TLSv1.2	109	Application Data
2024-09-21 10:14:00.615244	42.0	969366034	192.168.98.229	40256 3.65.102.105	443	TCP	68	40256 → 443 [ACK] Seq=55 Ack=149 Win=488 Len=0 TSval=17
2024-09-21 10:14:00.642043	43.0	687084804	142.250.185.110	443 192.168.98.229	37963	UDP	83	443 → 37963 Len=39
2024-09-21 10:14:00.642044	44.0	687085806	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 0000
▼ 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: 40930, 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: 0c0f519ae0b3f233ce536e2ee46b4c2ac3052c10ca11ea67236a6760c
[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

The screenshot displays the Wireshark interface with a list of captured packets and a detailed view of a selected packet (Frame 32).

Packet List:

No.	Time	Source	SPort	Destination	DPort	Protocol	Length	Info
2024-09-21 10:13:54.839257	19.0	284299983	192.168.98.229	36988	142.250.186.106	43 UDP	76	36988 → 443 Len=32
2024-09-21 10:13:54.930878	20.0	375912238	192.168.98.229	37963	142.250.185.110	43 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	43 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	43 UDP	699	37963 → 443 Len=655
2024-09-21 10:13:54.975053	23.0	420909527	142.250.185.110	443	192.168.98.229	37 TCP	79	443 → 37963 Len=35
2024-09-21 10:13:54.975411	24.0	420435209	192.168.98.229	37963	142.250.185.110	43 UDP	77	37963 → 443 Len=33
2024-09-21 10:13:54.987056	25.0	432097407	142.250.185.110	443	192.168.98.229	37 TCP	161	443 → 37963 Len=117
2024-09-21 10:13:54.987056	26.0	432098307	142.250.185.110	443	192.168.98.229	37 TCP	88	443 → 37963 Len=44
2024-09-21 10:13:54.987733	27.0	432775918	192.168.98.229	37963	142.250.185.110	43 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	37 TCP	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 Win=487 Len=0 TSval=27
2024-09-21 10:13:55.262424	30.0	787465835	142.250.184.195	80	192.168.98.229	54 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	40930	142.250.186.133	43 TLSv1.2	107	Application Data
2024-09-21 10:13:57.359354	32.2	804395944	142.250.186.133	443	192.168.98.229	40 TCP	107	Application Data
2024-09-21 10:13:57.359396	33.2	804432661	192.168.98.229	40930	142.250.186.133	43 TCP	68	40930 → 443 [ACK] Seq=40 Ack=40 Win=496 Len=0 TSval=
2024-09-21 10:13:58.784367	34.4	229489262	184.18.42.130	443	192.168.98.229	36 UDP	94	Application Data
2024-09-21 10:13:58.785633	35.4	230674924	192.168.98.229	36350	184.18.42.130	43 TLSv1.2	98	Application Data
2024-09-21 10:13:58.811139	36.4	256180936	184.18.42.130	443	192.168.98.229	36 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	43 TLSv1.2	122	Application Data
2024-09-21 10:13:58.943416	38.4	388457994	3.65.102.105	443	192.168.98.229	40 TCP	124	Application Data
2024-09-21 10:13:58.943450	39.4	388492743	192.168.98.229	40256	3.65.102.105	43 TCP	68	40256 → 443 [ACK] Seq=55 Ack=57 Win=488 Len=0 TSval=
2024-09-21 10:13:59.166666	40.4	611782370	Intel_b9:9d:08			IPv4	16	[Malformed Packet]
2024-09-21 10:14:00.615296	41.0	969327894	3.65.102.105	443	192.168.98.229	40 TCP	108	Application Data
2024-09-21 10:14:00.615244	42.0	969306834	192.168.98.229	40256	3.65.102.105	43 TCP	68	40256 → 443 [ACK] Seq=55 Ack=149 Win=488 Len=0 TSval=
2024-09-21 10:14:00.642843	43.0	687084804	142.250.185.110	443	192.168.98.229	37 UDP	83	443 → 37963 Len=39
2024-09-21 10:14:00.642844	44.0	687085806	142.250.185.110	443	192.168.98.229	37 UDP	82	443 → 37963 Len=38

Frame 32: 167 bytes on wire (856 bits), 167 bytes captured (856 bits) on interface any, 1d

- 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: 40930, 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: 0x5f19a0e03f233ce536e2ee46b4c2ac3052c10ca11ea67236a6769c [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

The screenshot displays the Wireshark network protocol analyzer interface. The main packet list pane shows a series of network packets. Packet 32 is highlighted in green, indicating it is the selected packet. The 'Info' column for this packet shows '36688 - 443 Len=32'. The packet details pane below shows the structure of the selected packet, which is a TLSv1.2 record. The details pane is expanded to show the 'Encrypted Application Data' field, which contains a large block of hexadecimal data. The status bar at the bottom of the window indicates that the record layer version is 'tls.record.version' and is 2 bytes long. It also shows that 88 packets are displayed, which is 100.0% of the total 88 packets, and that 0 packets were dropped.

No.	Time	Source	SPort	Destination	DPport	Protocol	Length	Info
2024-09-21 10:13:54.839257	19.0	284299033	192.168.98.229	36688	142.250.186.106	443	UDP	36688 - 443 Len=32
2024-09-21 10:13:54.930878	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	420099527	142.250.185.110	443	192.168.98.229	37963	UDP	37963 - 443 Len=35
2024-09-21 10:13:54.975411	24.0	420433529	192.168.98.229	37963	142.250.185.110	443	UDP	37963 - 443 Len=33
2024-09-21 10:13:54.987056	25.0	432097407	142.250.185.110	443	192.168.98.229	37963	UDP	37963 - 443 Len=117
2024-09-21 10:13:54.987056	26.0	432098307	142.250.185.110	443	192.168.98.229	37963	UDP	37963 - 443 Len=44
2024-09-21 10:13:54.987733	27.0	432775918	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	37963 - 443 Len=28
2024-09-21 10:13:55.213955	29.0	658996003	192.168.98.229	54940	142.250.184.195	80	TCP	54940 - 80 [ACK] Seq=1 Win=487 Len=0 TSval=27
2024-09-21 10:13:55.262424	30.0	787465835	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	40930	142.250.186.133	443	TLSv1.2	Application Data
2024-09-21 10:13:57.359394	32.2	804399944	142.250.186.133	443	192.168.98.229	40930	TLSv1.2	Application Data
2024-09-21 10:13:57.359396	33.2	804432601	192.168.98.229	40930	142.250.186.133	443	TCP	40930 - 443 [ACK] Seq=40 Ack=40 Win=496 Len=0 TSval=
2024-09-21 10:13:58.784367	34.4	229489262	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	36350 - 443 [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_b9:90:08			IPv4	5	[Malformed Packet]
2024-09-21 10:14:00.615296	41.0	969327894	3.65.102.105	443	192.168.98.229	40256	TLSv1.2	Application Data
2024-09-21 10:14:00.615344	42.0	969306034	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	43.0	6087084004	142.250.185.110	443	192.168.98.229	37963	UDP	37963 - 443 Len=39
2024-09-21 10:14:00.642044	44.0	6087085006	142.250.185.110	443	192.168.98.229	37963	UDP	37963 - 443 Len=38

Frame 32: 167 bytes on wire (856 bits), 167 bytes captured (856 bits) on interface any, id 0000
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: 40930, 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: 0c0f519ae0b3f233ce536e46b46c2ac3052c10ca11ea67236a6700
[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

The screenshot displays the Wireshark interface with a list of network packets and a detailed view of a selected packet (Frame 32).

Packet List:

No.	Time	Source	SPort	Destination	DPort	Protocol	Length	Info
2024-09-21 10:13:54.839257	19	0.284299833	192.168.98.229	36988 142.250.186.106	443	UDP	76	36988 → 443 Len=32
2024-09-21 10:13:54.930878	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	0.420989527	142.250.185.110	443 192.168.98.229	37963	UDP	79	443 → 37963 Len=35
2024-09-21 10:13:54.975411	24	0.420435229	192.168.98.229	37963 142.250.185.110	443	UDP	77	37963 → 443 Len=33
2024-09-21 10:13:54.987055	25	0.42097467	142.250.185.110	443 192.168.98.229	37963	UDP	161	443 → 37963 Len=117
2024-09-21 10:13:54.987056	26	0.42098307	142.250.185.110	443 192.168.98.229	37963	UDP	88	443 → 37963 Len=44
2024-09-21 10:13:54.987733	27	0.432775918	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 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	40930 142.250.186.133	443	TLSv1.2	107	Application Data
2024-09-21 10:13:57.359394	32	2.804395944	142.250.186.133	443 192.168.98.229	40930	TLSv1.2	107	Application Data
2024-09-21 10:13:57.359396	33	2.804432661	192.168.98.229	40930 142.250.186.133	443	TCP	68	40930 → 443 [ACK] Seq=40 Ack=40 Win=496 Len=0 TSval=
2024-09-21 10:13:58.784367	34	4.229489262	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 10:13:59.166666	40	4.611702370	Intel_b9:9d:08			IPv4	36	[Malformed Packet]
2024-09-21 10:14:00.615296	41	6.969372894	3.65.102.105	443 192.168.98.229	40256	TLSv1.2	109	Application Data
2024-09-21 10:14:00.615244	42	6.969368634	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	6.987084804	142.250.185.110	443 192.168.98.229	37963	UDP	83	443 → 37963 Len=39
2024-09-21 10:14:00.642044	44	6.987085806	142.250.185.110	443 192.168.98.229	37963	UDP	82	443 → 37963 Len=38

Frame 32 Details:

- Frame 32: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface any, id 3
- 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: 40930, 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: 0c5f19a0e803f233c5536a2ee46b4c2ac3052c10ca11ea67236a6709e [Application Data Protocol: Hypertext Transfer Protocol]

Packet Bytes:

```
00 00 00 01 00 06 4a dd ae 35 63 fb 00 00 00 00 ..... J Sc .....
45 00 00 5b 34 06 00 00 35 06 64 09 Be Fa ba 85 E [4 ..... 5 .....
c0 a8 62 e5 01 bb 0c 5e 9e 17 d7 04 3e 06 a7 71 b ..... 0 ..... r f q
80 18 36 ef e5 00 00 01 01 08 0a 3f 43 c4 93 .. 6 ..... 7c .....
7c 55 27 f7 03 03 00 22 0c 05 13 0a 06 b3 f2 [UR ..... 0 .....
33 c5 53 6e 2e 04 00 4c e2 ac 30 52 c1 0c a1 1e 3-Sn ..... kl ..... 0R .....
06 72 36 a6 7d 0a 04 0b 62 c9 4c ..... 0 ..... b k
```

Wireshark

The screenshot displays the Wireshark interface with a list of captured packets and a detailed view of a selected packet (Frame 32).

Packet List:

No.	Time	Source	SPort	Destination	DPort	Protocol	Length	Info
2024-09-21 10:13:54.839257	19.0	284299933	192.168.98.229	36988 142.250.186.106	443	UDP	76	36988 → 443 Len=32
2024-09-21 10:13:54.930876	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	420909527	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	420433529	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	432775918	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 Win=487 Len=0 TSval=27
2024-09-21 10:13:55.262424	30.0	767465835	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	40930 142.250.186.133	443	TLSv1.2	107	Application Data
2024-09-21 10:13:57.359394	32.2	804399944	142.250.186.133	443 192.168.98.229	40930	TLSv1.2	107	Application Data
2024-09-21 10:13:57.359396	33.2	804432661	192.168.98.229	40930 142.250.186.133	443	TCP	68	40930 → 443 [ACK] Seq=40 Ack=40 Win=496 Len=0 TSval=17
2024-09-21 10:13:58.784367	34.4	229489262	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=17
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=17
2024-09-21 10:13:59.166666	40.4	611702370	Intel_b9:9d:08			IPv4	36	[Malformed Packet]
2024-09-21 10:14:00.615296	41.0	969327894	3.65.102.105	443 192.168.98.229	40256	TLSv1.2	109	Application Data
2024-09-21 10:14:00.615244	42.0	969306694	192.168.98.229	40256 3.65.102.105	443	TCP	68	40256 → 443 [ACK] Seq=55 Ack=149 Win=488 Len=0 TSval=17
2024-09-21 10:14:00.642043	43.0	687084804	142.250.185.110	443 192.168.98.229	37963	UDP	83	443 → 37963 Len=39
2024-09-21 10:14:00.642044	44.0	687085806	142.250.185.110	443 192.168.98.229	37963	UDP	82	443 → 37963 Len=38

Packet 32 Details:

- Frame 32: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface any, id 0000
- Linux cooked capture v1 0010
- Internet Protocol Version 4, Src: 142.250.186.133, Dst: 192.168.98.229 0020
- Transmission Control Protocol, Src Port: 443, Dst Port: 40930, Seq: 1, Ack: 40, Len: 39 0030
- Transport Layer Security 0040
 - TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol 0050
 - Content Type: Application Data (23) 0060
 - Version: TLS 1.2 (0x0303) 0070
 - Length: 34 0080
 - Encrypted Application Data: 0x5f19a0e0b3f233ce536e2ee46b4c2ac3052c10ca11ea67236a6769c [Application Data Protocol: Hypertext Transfer Protocol] 0090

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

The screenshot displays the Wireshark interface with the following details:

- Packet List:** Shows a list of captured packets. The selected packet (No. 32) is a TLSv1.2 record from source 192.168.98.229 to destination 142.250.186.133.
- Packet Details:** Shows the structure of the selected packet:
 - Frame 32: 167 bytes on wire (856 bits), 167 bytes captured (856 bits) on interface any, id 3
 - 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: 49030, 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: 0xc5f510aeb03f233ce536e2ee46b4ce2ac3052c10ca11ea67236a6769e
 - [Application Data Protocol: Hypertext Transfer Protocol]
- Packet Bytes:** Shows the raw hex and ASCII data of the selected packet, including the TLS record structure.

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!

