

Analyzing Network Protocols with Wireshark

WHY ARE CORE NETWORK PROTOCOLS SO IMPORTANT TO UNDERSTAND?



Chris Greer

NETWORK ANALYST

@packetpioneer www.packetpioneer.com



Module Overview



Wireshark can be daunting

Focus quickly on what matters

What do we mean by core protocols?

Hands-on practice



Wireshark can be daunting



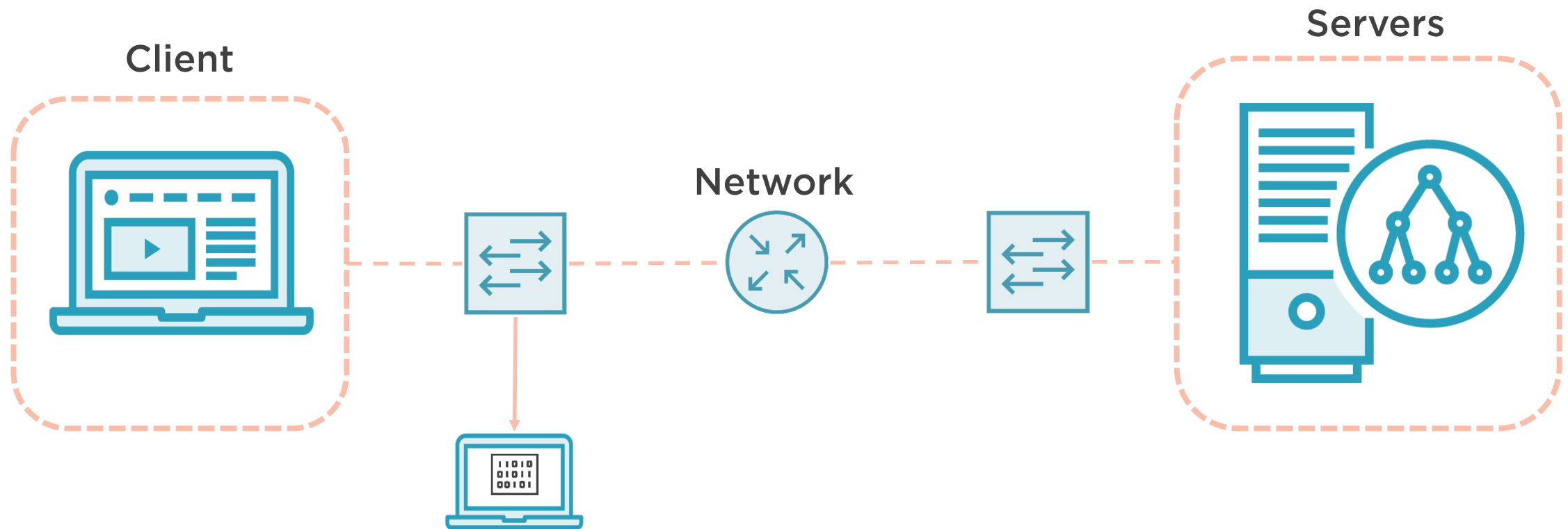
Packet Analysis



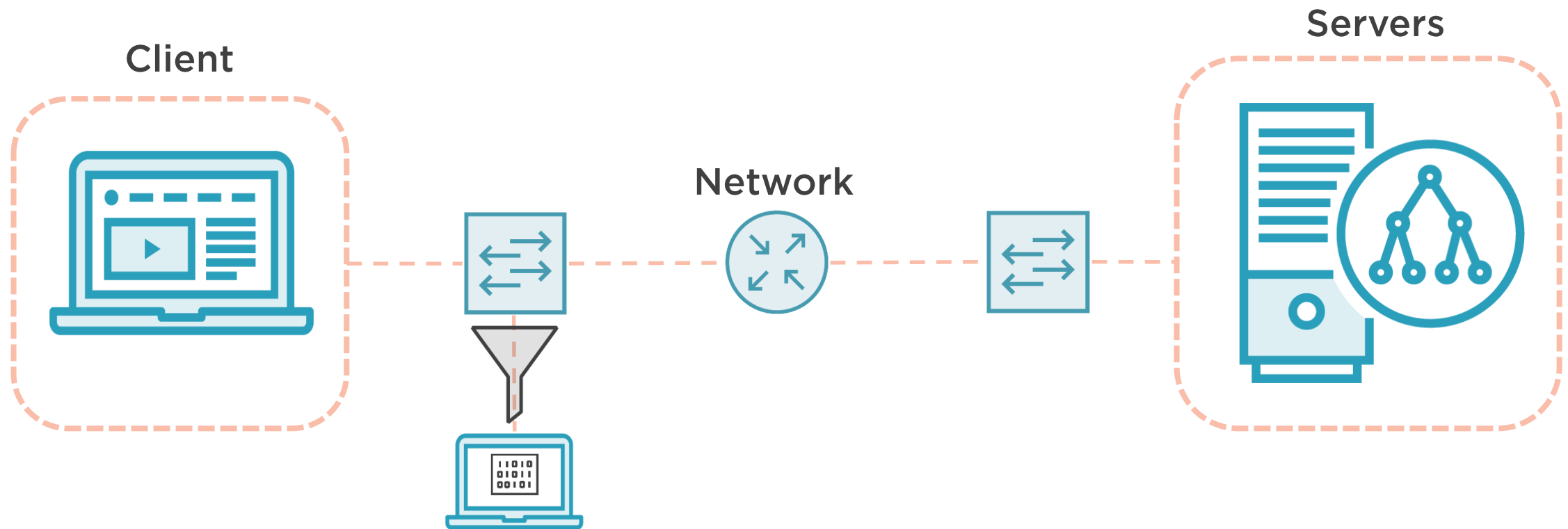
Focus Quickly on What Matters



Create a Smaller Haystack



Create a Smaller Haystack



Create Protocol Profiles

Web Drive to PluralSight.pcapng

Apply a display filter ... <96/>

No.	Time	Delta	Source	Destination	Length	Time to live	Info
1	0.000000	0.000000	173.194.68.188	192.168.10.1...	66	101	hvpvroom(5228) → 60348 [ACK] Seq=1 Ack=1 Wi
2	1.360433	1.360433	BelkinIn_9d:0...	Apple_e7:ce:...	42		Who has 192.168.10.108? Tell 192.168.10.1
3	1.360479	0.000046	Apple_e7:ce:6d	BelkinIn_9d:...	42		192.168.10.108 is at a4:5e:60:e7:ce:6d
4	2.854471	1.493992	192.168.10.108	192.168.10.1	79	64	Standard query 0x0767 A www.pluralsight.co
5	2.854614	0.000143	192.168.10.108	192.168.10.1	79	64	Standard query 0x9c30 A app.pluralsight.co
6	2.854750	0.000136	192.168.10.108	192.168.10.1	77	64	Standard query 0x2f72 A s.pluralsight.com
7	2.858333	0.003583	192.168.10.108	104.25.218.21	54	64	60516 → https(443) [FIN, ACK] Seq=1 Ack=1
8	2.858579	0.000246	192.168.10.108	192.0.73.2	54	64	60520 → https(443) [FIN, ACK] Seq=1 Ack=1
9	2.858652	0.000073	192.168.10.108	172.217.10.72	66	64	60521 → https(443) [FIN, ACK] Seq=1 Ack=1
10	2.858784	0.000132	192.168.10.108	104.25.218.21	54	64	60518 → https(443) [FIN, ACK] Seq=1 Ack=1
11	2.858815	0.000031	192.168.10.108	172.217.10.72	66	64	60522 → https(443) [FIN, ACK] Seq=1 Ack=1
12	3.018467	0.159652	192.168.10.1	192.168.10.1...	253	64	Standard query response 0x0767 A www.plura
13	3.018469	0.000002	192.168.10.1	192.168.10.1...	301	64	Standard query response 0x9c30 A app.plura
14	3.018469	0.000000	192.168.10.1	192.168.10.1...	494	64	Standard query response 0x2f72 A s.plurals
15	3.018797	0.000328	192.168.10.108	104.16.242.2...	78	64	60533 → https(443) [SYN] Seq=0 Win=65535 L
16	3.019535	0.000738	192.168.10.108	104.16.211.40	78	64	60534 → https(443) [SYN] Seq=0 Win=65535 L

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (5...)

Ethernet II, Src: BelkinIn_9d:02:73 (94:10:3e:9d:02:73), D...

Internet Protocol Version 4, Src: 173.194.68.188, Dst: 192...

Transmission Control Protocol, Src Port: hvpvroom (5228), D...

0000 a4 5e 60 e7 ce 6d 94 10 3e 9d 02 73 08 00 45 00

0010 00 34 34 c7 00 00 65 06 63 6a ad c2 44 bc c0 a8

0020 0a 6c 14 6c eb bc 75 84 36 cf d3 5a 09 32 80 10

0030 00 f4 da f4 00 00 01 01 08 0a 36 c9 28 28 38 28

0040 bd 1e

Web Drive to PluralSight.pcapng

Packets: 1123 · Displayed: 1123 (100.0%)

Profile: TCP Plain

Create Protocol Profiles

Web Drive to PluralSight.pcapng

Apply a display filter ... <96/>

No.	Time	Delta	Source	Destination	Length	Time to live	Info
1	0.000000	0.000000	173.194.68.188	192.168.10.108	60	101	hqvroom(5228) → 60548 [ACK] Seq=1 Ack=1 Win=0 Len=0
2	1.360433	1.360433	BelkinIn_9d:02:73	Apple_e7:ce:6d	42		Who has 192.168.10.108? Tell 192.168.10.108 is at a4:5e:60:e7:ce:6d
3	1.360479	0.000046	Apple_e7:ce:6d	BelkinIn_9d:02:73	42		192.168.10.108 is at a4:5e:60:e7:ce:6d
4	2.854471	1.493992	192.168.10.108	192.168.10.1	79	64	Standard query 0x0767 A www.pluralsight.com
5	2.854614	0.000143	192.168.10.108	192.168.10.1	79	64	Standard query 0x9c30 A app.pluralsight.com
6	2.854750	0.000136	192.168.10.108	192.168.10.1	77	64	Standard query 0x2f72 A s.pluralsight.com
7	2.858333	0.003583	192.168.10.108	104.25.218.21	54	64	60516 → https(443) [FIN, ACK] Seq=1 Ack=1 Win=0 Len=0
8	2.858579	0.000246	192.168.10.108	192.0.73.2	54	64	60520 → https(443) [FIN, ACK] Seq=1 Ack=1 Win=0 Len=0
9	2.858652	0.000073	192.168.10.108	172.217.10.72	66	64	60521 → https(443) [FIN, ACK] Seq=1 Ack=1 Win=0 Len=0
10	2.858784	0.000132	192.168.10.108	104.25.218.21	54	64	60518 → https(443) [FIN, ACK] Seq=1 Ack=1 Win=0 Len=0
11	2.858815	0.000031	192.168.10.108	172.217.10.72	66	64	60522 → https(443) [FIN, ACK] Seq=1 Ack=1 Win=0 Len=0
12	3.018467	0.159652	192.168.10.1	192.168.10.1...	253	64	Standard query response 0x0767 A www.plura
13	3.018469	0.000002	192.168.10.1	192.168.10.1...	301	64	Standard query response 0x9c30 A app.plura
14	3.018469	0.000000	192.168.10.1	192.168.10.1...	494	64	Standard query response 0x2f72 A s.plurals
15	3.018797	0.000328	192.168.10.108	104.16.242.2...	78	64	60533 → https(443) [SYN] Seq=0 Win=65535 Len=0
16	3.019535	0.000738	192.168.10.108	104.16.211.40	78	64	60534 → https(443) [SYN] Seq=0 Win=65535 Len=0

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (5184 bits) on 0

Ethernet II, Src: BelkinIn_9d:02:73 (94:10:3e:9d:02:73), Dst: Apple_e7:ce:6d (08:00:27:08:00:45)

Internet Protocol Version 4, Src: 173.194.68.188, Dst: 192.168.10.108

Transmission Control Protocol, Src Port: hqvroom (5228), Dst Port: 60548

0000 a4 5e 60 e7 ce 6d 94 10 3e 9d 02 73 08 00 45 00
0010 00 34 34 c7 00 00 65 06 63 6a ad c2 44 bc c0 a8
0020 0a 6c 14 6c eb bc 75 84 36 cf d3 5a 09 32 80 10
0030 00 f4 da f4 00 00 01 01 08 0a 36 c9 28 28 38 28
0040 bd 1e

Web Drive to PluralSight.pcapng

Packets: 1123 · Displayed: 1123 (100.0%)

Profile: TCP Plain



Create Protocol Profiles

The image shows a Wireshark packet capture interface. The top toolbar includes icons for file operations, network analysis, and search. Below the toolbar is a filter bar with the text "Apply a display filter ... <%%/>" and a search icon. The main packet list table has columns: No., Time, Delta, Source, Destination, Length, Time to live, and Info. The table contains 16 rows of captured packets. The 15th packet is highlighted in green. Below the packet list, the "Packet Details" pane shows the structure of the selected packet (Frame 15): Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The "Packet Bytes" pane shows the raw hex and ASCII data of the packet. A red rectangle highlights the hex data from offset 0000 to 0040.

No.	Time	Delta	Source	Destination	Length	Time to live	Info
1	0.000000	0.000000	173.194.68.188	192.168.10.1...	66	101	hvpvroom(5228) → 60348 [ACK] Seq=1 Ack=1 Wi
2	1.360433	1.360433	BelkinIn_9d:0...	Apple_e7:ce:...	42		Who has 192.168.10.108? Tell 192.168.10.1
3	1.360479	0.000046	Apple_e7:ce:6d	BelkinIn_9d:...	42		192.168.10.108 is at a4:5e:60:e7:ce:6d
4	2.854471	1.493992	192.168.10.108	192.168.10.1	79	64	Standard query 0x0767 A www.pluralsight.co
5	2.854614	0.000143	192.168.10.108	192.168.10.1	79	64	Standard query 0x9c30 A app.pluralsight.co
6	2.854750	0.000136	192.168.10.108	192.168.10.1	77	64	Standard query 0x2f72 A s.pluralsight.com
7	2.858333	0.003583	192.168.10.108	104.25.218.21	54	64	60516 → https(443) [FIN, ACK] Seq=1 Ack=1
8	2.858579	0.000246	192.168.10.108	192.0.73.2	54	64	60520 → https(443) [FIN, ACK] Seq=1 Ack=1
9	2.858652	0.000073	192.168.10.108	172.217.10.72	66	64	60521 → https(443) [FIN, ACK] Seq=1 Ack=1
10	2.858784	0.000132	192.168.10.108	104.25.218.21	54	64	60518 → https(443) [FIN, ACK] Seq=1 Ack=1
11	2.858815	0.000031	192.168.10.108	172.217.10.72	66	64	60522 → https(443) [FIN, ACK] Seq=1 Ack=1
12	3.018467	0.159652	192.168.10.1	192.168.10.1...	253	64	Standard query response 0x0767 A www.plura
13	3.018469	0.000002	192.168.10.1	192.168.10.1...	301	64	Standard query response 0x9c30 A app.plura
14	3.018469	0.000000	192.168.10.1	192.168.10.1...	494	64	Standard query response 0x2f72 A s.plurals
15	3.018797	0.000328	192.168.10.108	104.16.242.2...	78	64	60533 → https(443) [SYN] Seq=0 Win=65535 L
16	3.019535	0.000738	192.168.10.108	104.16.211.40	78	64	60534 → https(443) [SYN] Seq=0 Win=65535 Len=0 M

Frame 15: 66 bytes on wire (528 bits), 66 bytes captured (516 bits) on interface 0

- Ethernet II, Src: BelkinIn_9d:02:73 (94:10:3e:9d:02:73), Dst: 192.168.10.1 (08:00:27:00:00:00)
- Internet Protocol Version 4, Src: 173.194.68.188, Dst: 192.168.10.1
- Transmission Control Protocol, Src Port: hvpvroom (5228), Dst Port: 443

0000 a4 5e 60 e7 ce 6d 94 10 3e 9d 02 73 08 00 45 00
0010 00 34 34 c7 00 00 65 06 63 6a ad c2 44 bc c0 a8
0020 0a 6c 14 6c eb bc 75 84 36 cf d3 5a 09 32 80 10
0030 00 f4 da f4 00 00 01 01 08 0a 36 c9 28 28 38 28
0040 bd 1e



Create Protocol Profiles

The image shows the Wireshark network protocol analyzer interface. The top toolbar includes various icons for file operations, search, and display. Below the toolbar is a filter bar with the text "Apply a display filter ... <%%/>" and a button to apply the filter. To the right of the filter bar is a tabbed interface for packet classification, with tabs labeled "Bad TCP", "No Broadcast/Chatter", "Slow HTTP", "Any IP Broadcast", and "MilkFilter". The main packet list table displays the following data:

No.	Time	Delta	Source	Destination	Length	Time to live	Info
1	0.000000	0.000000	173.194.68.188	192.168.10.1...	66	101	hvpvroom(5228) → 60348 [ACK] Seq=1 Ack=1 Wi
2	1.360433	1.360433	BelkinIn_9d:0...	Apple_e7:ce:...	42		Who has 192.168.10.108? Tell 192.168.10.1
3	1.360479	0.000046	Apple_e7:ce:6d	BelkinIn_9d:...	42		192.168.10.108 is at a4:5e:60:e7:ce:6d
4	2.854471	1.493992	192.168.10.108	192.168.10.1	79	64	Standard query 0x0767 A www.pluralsight.co
5	2.854614	0.000143	192.168.10.108	192.168.10.1	79	64	Standard query 0x9c30 A app.pluralsight.co
6	2.854750	0.000136	192.168.10.108	192.168.10.1	77	64	Standard query 0x2f72 A s.pluralsight.com
7	2.858333	0.003583	192.168.10.108	104.25.218.21	54	64	60516 → https(443) [FIN, ACK] Seq=1 Ack=1
8	2.858579	0.000246	192.168.10.108	192.0.73.2	54	64	60520 → https(443) [FIN, ACK] Seq=1 Ack=1
9	2.858652	0.000073	192.168.10.108	172.217.10.72	66	64	60521 → https(443) [FIN, ACK] Seq=1 Ack=1
10	2.858784	0.000132	192.168.10.108	104.25.218.21	54	64	60518 → https(443) [FIN, ACK] Seq=1 Ack=1
11	2.858815	0.000031	192.168.10.108	172.217.10.72	66	64	60522 → https(443) [FIN, ACK] Seq=1 Ack=1
12	3.018467	0.159652	192.168.10.1	192.168.10.1...	253	64	Standard query response 0x0767 A www.plura
13	3.018469	0.000002	192.168.10.1	192.168.10.1...	301	64	Standard query response 0x9c30 A app.plura
14	3.018469	0.000000	192.168.10.1	192.168.10.1...	494	64	Standard query response 0x2f72 A s.plurals
15	3.018797	0.000328	192.168.10.108	104.16.242.2...	78	64	60533 → https(443) [SYN] Seq=0 Win=65535 L
16	3.019535	0.000738	192.168.10.108	104.16.211.40	78	64	60534 → https(443) [SYN] Seq=0 Win=65535 L

Below the packet list, the detailed view of the selected packet (No. 15) is shown. It includes a list of packet details and a hex dump of the packet data.

Frame 15: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
Ethernet II, Src: BelkinIn_9d:02:73 (94:10:3e:9d:02:73), Dst: 192.168.10.1 (08:00:27:00:00:00)
Internet Protocol Version 4, Src: 173.194.68.188, Dst: 192.168.10.1
Transmission Control Protocol, Src Port: hvpvroom (5228), Dst Port: 60533

The hex dump shows the following data:

```
0000  a4 5e 60 e7 ce 6d 94 10 3e 9d 02 73 08 00 45 00  
0010  00 34 34 c7 00 00 65 06 63 6a ad c2 44 bc c0 a8  
0020  0a 6c 14 6c eb bc 75 84 36 cf d3 5a 09 32 80 10  
0030  00 f4 da f4 00 00 01 01 08 0a 36 c9 28 28 38 28  
0040  bd 1e
```



What Do We Mean by Core Protocols?



Core Protocols Support Applications

Application Data

UDP

TCP

TLS

IPv6

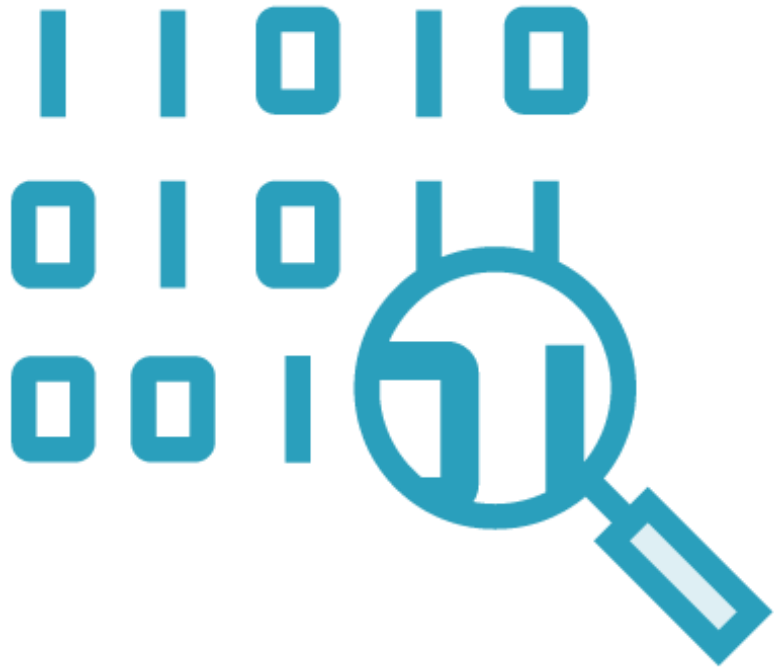
DNS

ARP

IP

ICMP





A skilled network analyst is able to quickly
read and exonerate these protocols

Or use them to pinpoint the issue



Demo



Create a protocol profile in Wireshark

