HackerFrogs Afterschool
Digital Forensics: Wireshark

Class:
Digital Forensics

Workshop Number:
AS-FOR-04

Document Version:
1.75

Special Requirements:
Registered account at tryhackme.com

Welcome to HackerFrogs Afterschool!

Hey there HackerFrogs!

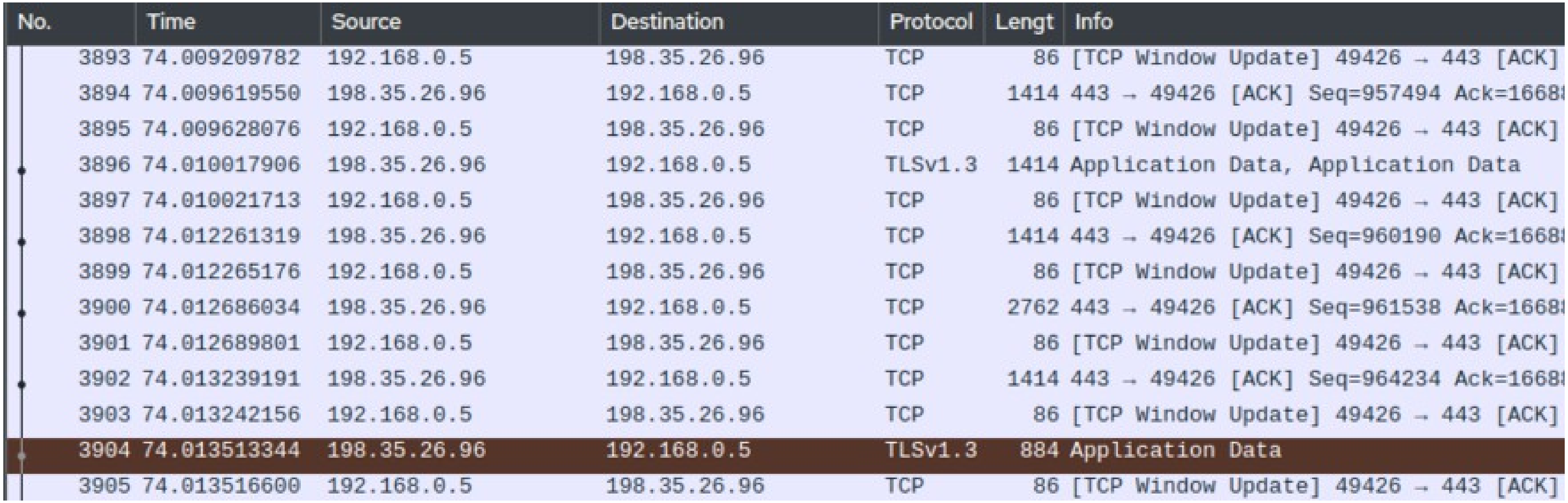
This is the fourth intro to Digital Forensics workshop.

In the previous workshop we learned about the following Digital Forensic concepts:

Network Traffic

Any time a network device sends data from one device to another, network traffic is generated as network packets are sent back and forth

PCAP Files



No.	Time	Source	Destination	Protocol	Lengt	Info
3893	74.009209782	192.168.0.5	198.35.26.96	TCP	86	[TCP Window Update] 49426 → 443 [ACK]
3894	74.009619550	198.35.26.96	192.168.0.5	TCP	1414	443 → 49426 [ACK] Seq=957494 Ack=1668
3895	74.009628076	192.168.0.5	198.35.26.96	TCP	86	[TCP Window Update] 49426 → 443 [ACK]
3896	74.010017906	198.35.26.96	192.168.0.5	TLSv1.3	1414	Application Data, Application Data
3897	74.010021713	192.168.0.5	198.35.26.96	TCP	86	[TCP Window Update] 49426 → 443 [ACK]
3898	74.012261319	198.35.26.96	192.168.0.5	TCP	1414	443 → 49426 [ACK] Seq=960190 Ack=1668
3899	74.012265176	192.168.0.5	198.35.26.96	TCP	86	[TCP Window Update] 49426 → 443 [ACK]
3900	74.012686034	198.35.26.96	192.168.0.5	TCP	2762	443 → 49426 [ACK] Seq=961538 Ack=1668
3901	74.012689801	192.168.0.5	198.35.26.96	TCP	86	[TCP Window Update] 49426 → 443 [ACK]
3902	74.013239191	198.35.26.96	192.168.0.5	TCP	1414	443 → 49426 [ACK] Seq=964234 Ack=1668
3903	74.013242156	192.168.0.5	198.35.26.96	TCP	86	[TCP Window Update] 49426 → 443 [ACK]
3904	74.013513344	198.35.26.96	192.168.0.5	TLSv1.3	884	Application Data
3905	74.013516600	192.168.0.5	198.35.26.96	TCP	86	[TCP Window Update] 49426 → 443 [ACK]

Files which contain a collection of network traffic are called packet capture (PCAP) files, and one specialty of digital forensics is the analysis of network traffic and PCAP files.

Wireshark

Wireshark is a program which is widely used for network traffic analysis, and we'll learn to use it to analyze PCAP files.

This Workshop's Topics

- Wireshark practice

- PicoCTF: Packets Primer

- PicoCTF: PcapPoisoning

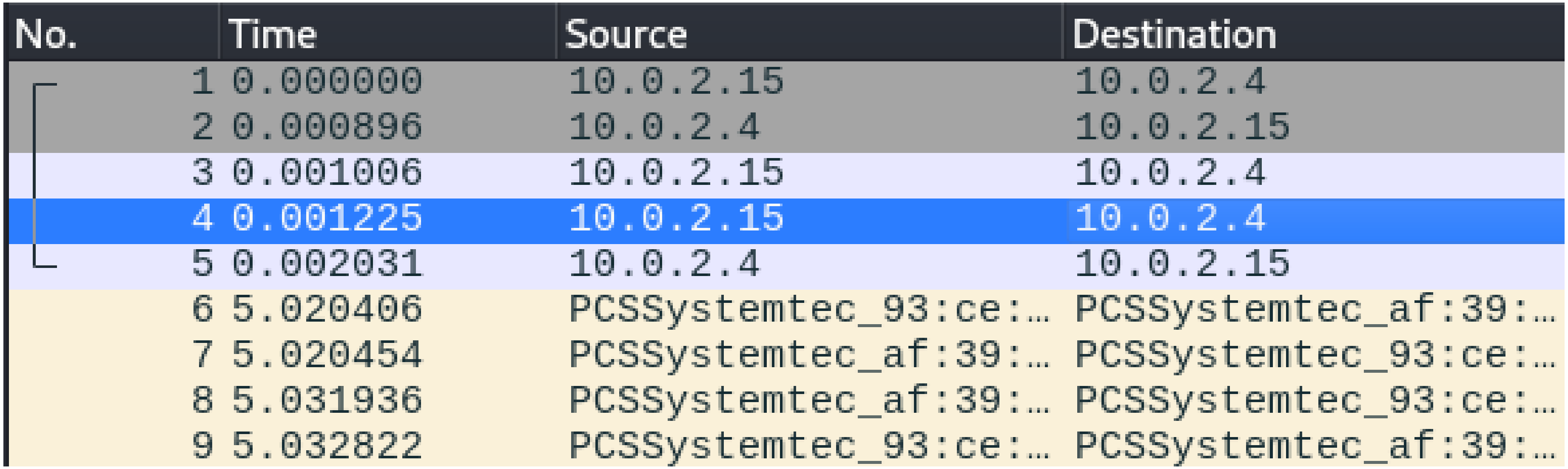
- PicoCTF: Wirehshark doo dooo do doo...

PicoCTF: Packets Primer

Let's begin our Wireshark practice with an easy challenge:

https://play.picoctf.org/practice/challenge/286?category=4&page=1&search=pack

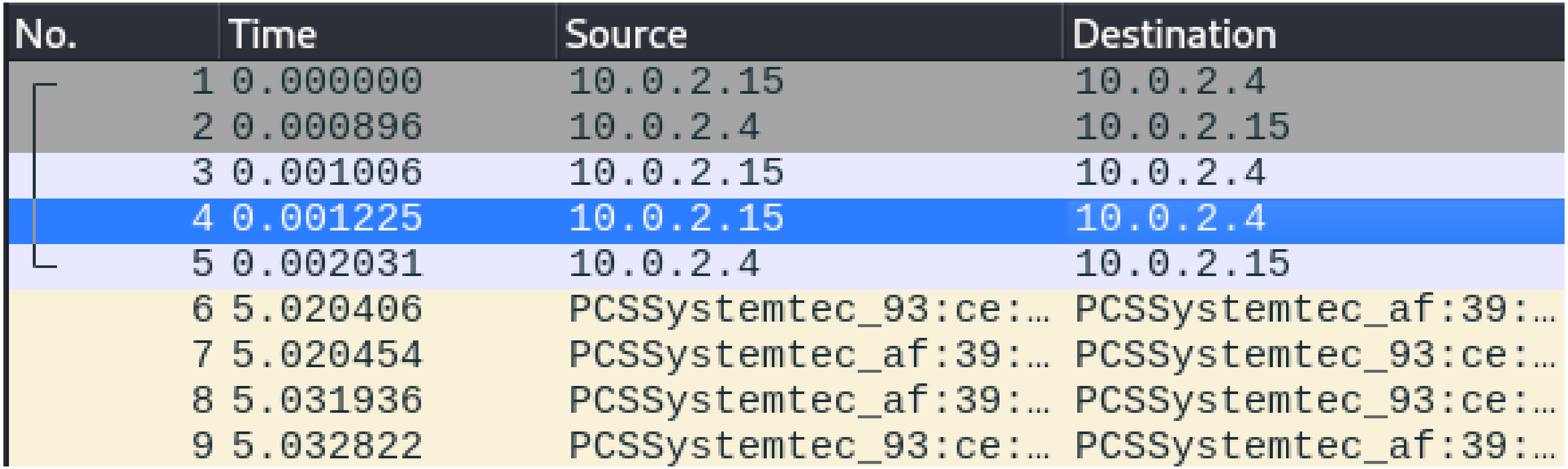
Manual Packet Inspection



No.	Time	Source	Destination
1	0.000000	10.0.2.15	10.0.2.4
2	0.000896	10.0.2.4	10.0.2.15
3	0.001006	10.0.2.15	10.0.2.4
4	0.001225	10.0.2.15	10.0.2.4
5	0.002031	10.0.2.4	10.0.2.15
6	5.020406	PCSSystemtec_93:ce:…	PCSSystemtec_af:39:…
7	5.020454	PCSSystemtec_af:39:…	PCSSystemtec_93:ce:…
8	5.031936	PCSSystemtec_af:39:…	PCSSystemtec_93:ce:…
9	5.032822	PCSSystemtec_93:ce:…	PCSSystemtec_af:39:…

Since there are very few packets in this PCAP file, it's possible to manually inspect their contents

Manual Packet Inspection



No.	Time	Source	Destination
1	0.000000	10.0.2.15	10.0.2.4
2	0.000896	10.0.2.4	10.0.2.15
3	0.001006	10.0.2.15	10.0.2.4
4	0.001225	10.0.2.15	10.0.2.4
5	0.002031	10.0.2.4	10.0.2.15
6	5.020406	PCSSystemtec_93:ce:…	PCSSystemtec_af:39:…
7	5.020454	PCSSystemtec_af:39:…	PCSSystemtec_93:ce:…
8	5.031936	PCSSystemtec_af:39:…	PCSSystemtec_93:ce:…
9	5.032822	PCSSystemtec_93:ce:…	PCSSystemtec_af:39:…

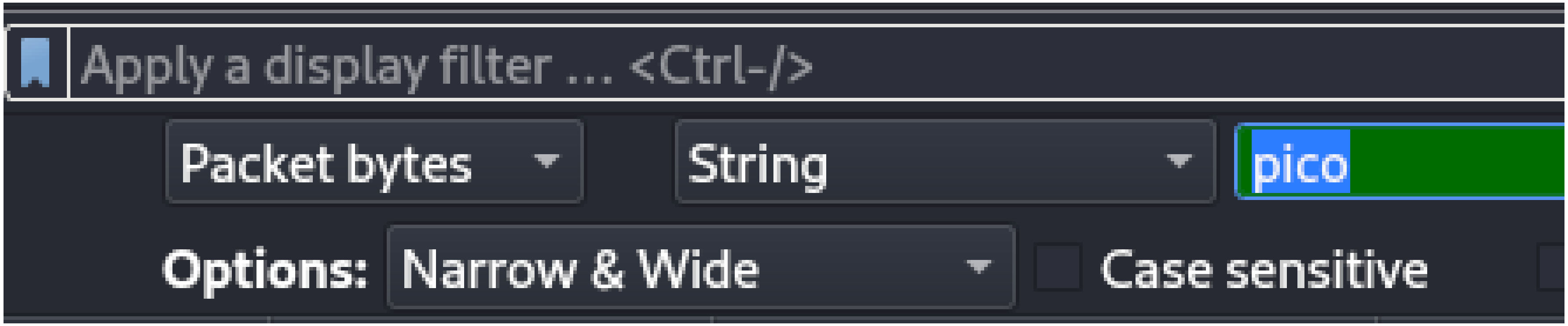
This is very unusual for a PCAP file, since most PCAPs contain hundreds or thousands of packets

PicoCTF: PcapPoisoning

Let's use the Wireshark string search functions with the next challenge:

https://play.picoctf.org/practice/challenge/362?category=4&page=1&search=pcap

Find Function: Strings



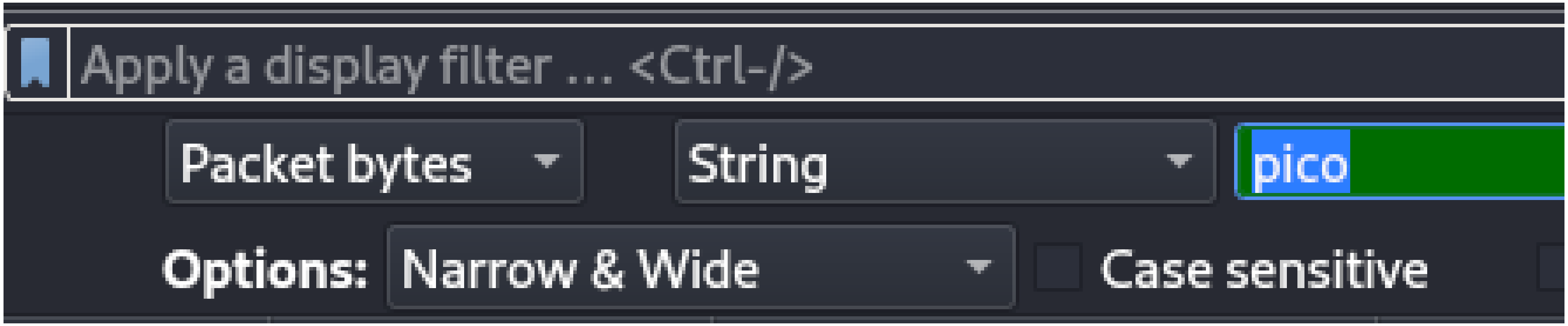
Apply a display filter … <Ctrl-/>

Packet bytes | String | pico

Options: Narrow & Wide □ Case sensitive

One important feature of Wireshark (especially for CTF challenges) is the ability to search for strings in packet contents

Find Function: Strings



Apply a display filter … <Ctrl-/>

Packet bytes ▾ String ▾ pico

Options: Narrow & Wide ▾ □ Case sensitive

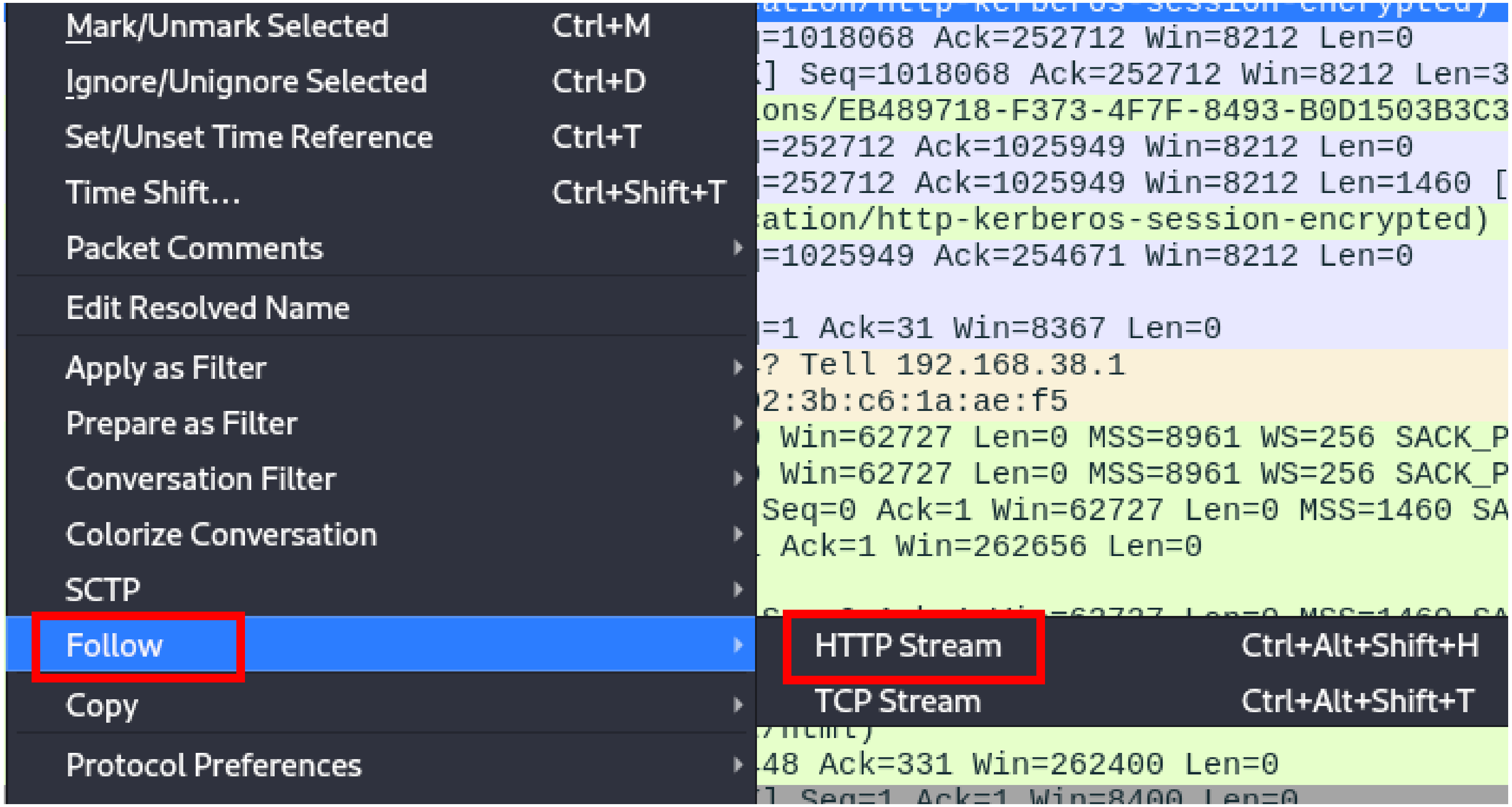
Make sure to search for “Packet bytes” and “Strings” before submitting the search term

PicoCTF: Wireshark doo dooo do doo...

Let's learn more about the stream follow function with this challenge:

https://play.picoctf.org/practice/challenge/115?category=4&page=1&search=wire

Stream Follow Conversation



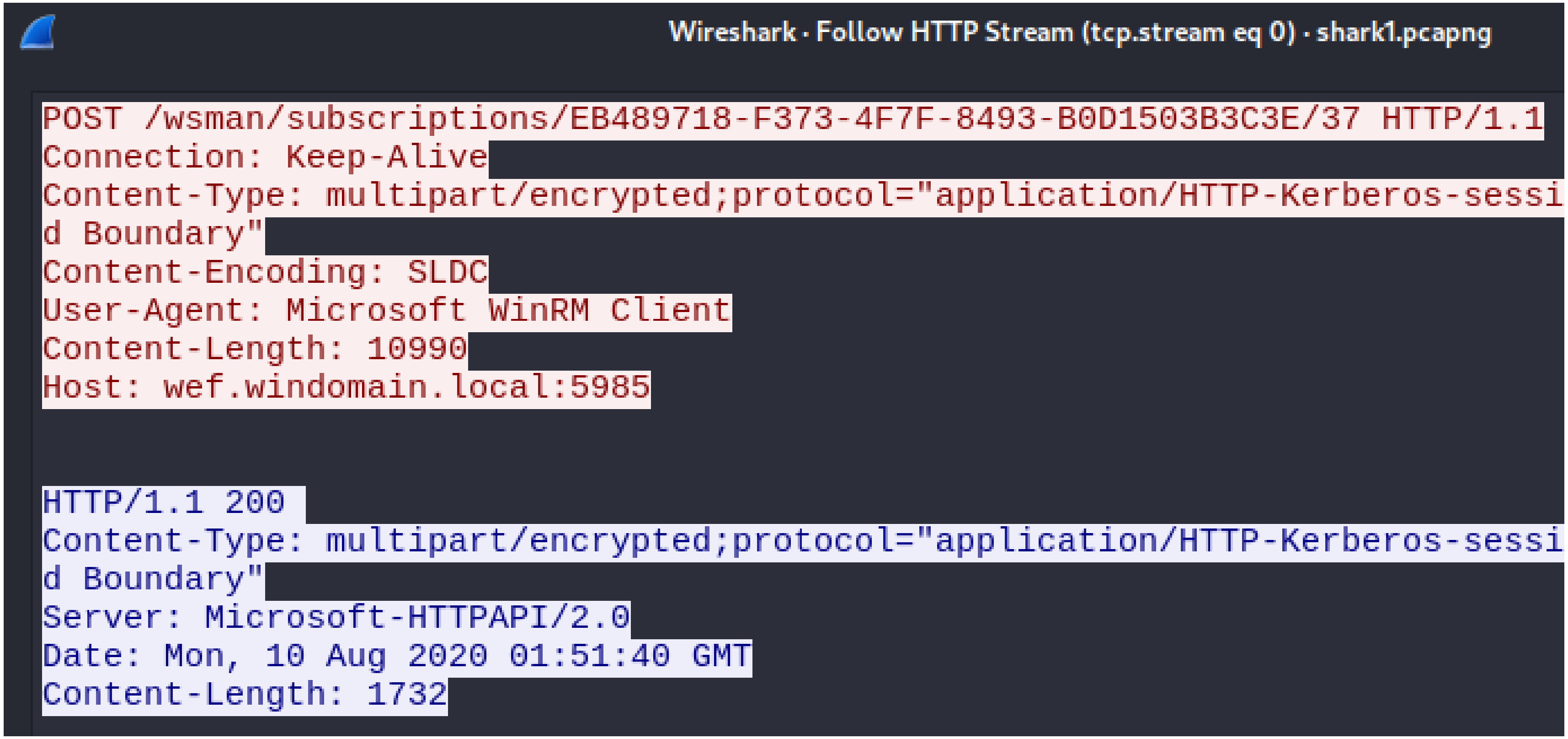
```
ation/http-kerberos-session-encrypted)
=1018068 Ack=252712 Win=8212 Len=0
] Seq=1018068 Ack=252712 Win=8212 Len=3
ons/EB489718-F373-4F7F-8493-B0D1503B3C3
=252712 Ack=1025949 Win=8212 Len=0
=252712 Ack=1025949 Win=8212 Len=1460 [
ation/http-kerberos-session-encrypted)
=1025949 Ack=254671 Win=8212 Len=0

=1 Ack=31 Win=8367 Len=0
? Tell 192.168.38.1
2:3b:c6:1a:ae:f5
 Win=62727 Len=0 MSS=8961 WS=256 SACK_P
 Win=62727 Len=0 MSS=8961 WS=256 SACK_P
Seq=0 Ack=1 Win=62727 Len=0 MSS=1460 SA
 Ack=1 Win=262656 Len=0

/html)
48 Ack=331 Win=262400 Len=0
] Seq=1 Ack=1 Win=8400 Len=0
```

A useful function for following packets sent between two servers is the “follow conversation” function

Stream Follow Conversation



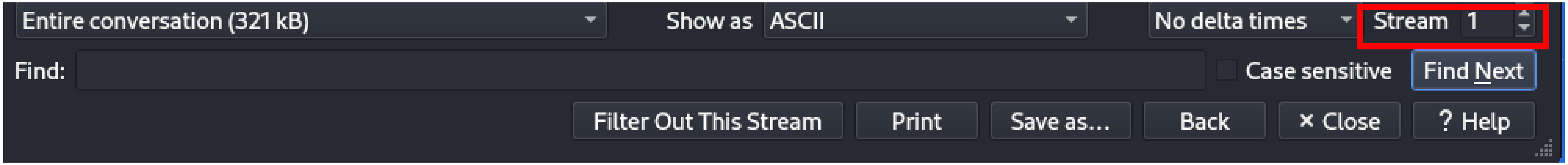
Wireshark · Follow HTTP Stream (tcp.stream eq 0) · shark1.pcapng

```
POST /wsman/subscriptions/EB489718-F373-4F7F-8493-B0D1503B3C3E/37 HTTP/1.1
Connection: Keep-Alive
Content-Type: multipart/encrypted;protocol="application/HTTP-Kerberos-sessi
d Boundary"
Content-Encoding: SLDC
User-Agent: Microsoft WinRM Client
Content-Length: 10990
Host: wef.windomain.local:5985


HTTP/1.1 200
Content-Type: multipart/encrypted;protocol="application/HTTP-Kerberos-sessi
d Boundary"
Server: Microsoft-HTTPAPI/2.0
Date: Mon, 10 Aug 2020 01:51:40 GMT
Content-Length: 1732
```

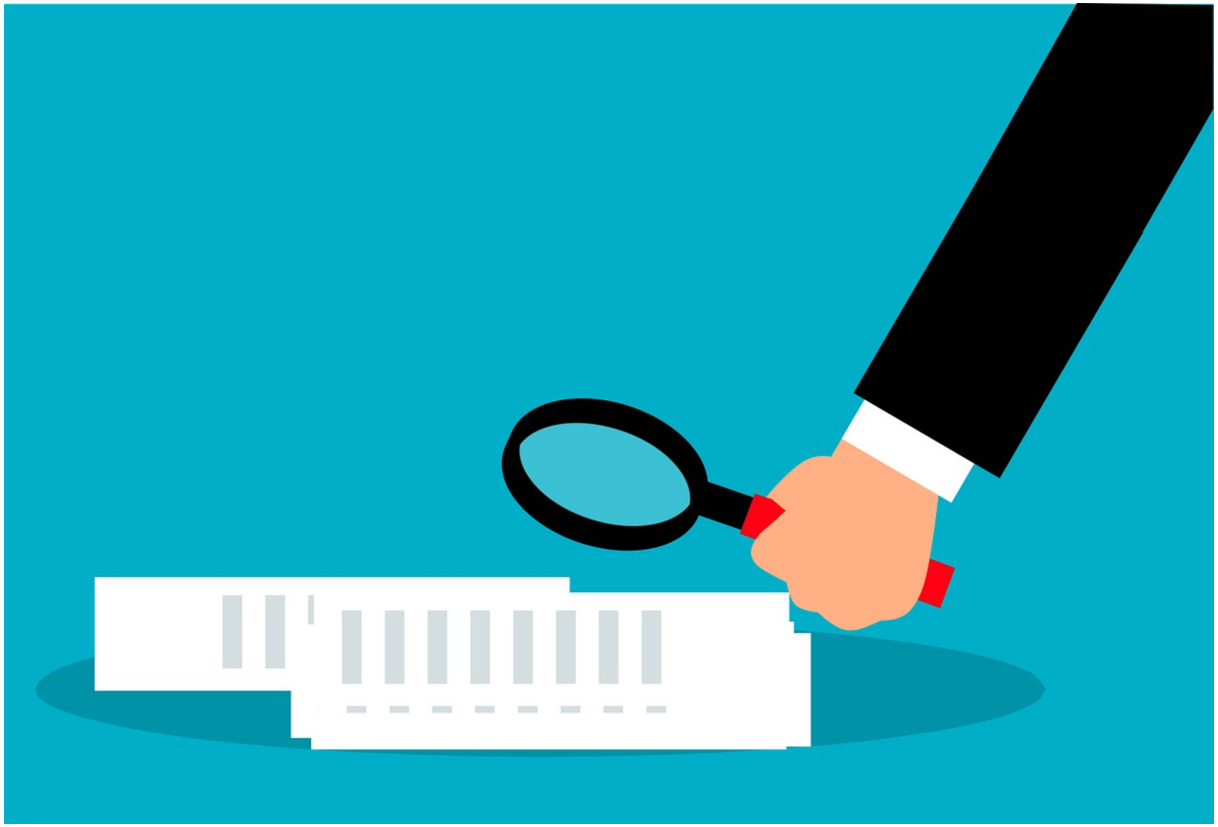
In this window, you will see the data sent between the two servers, but if the data is encrypted, you will not be able to read it

Stream Follow Conversation



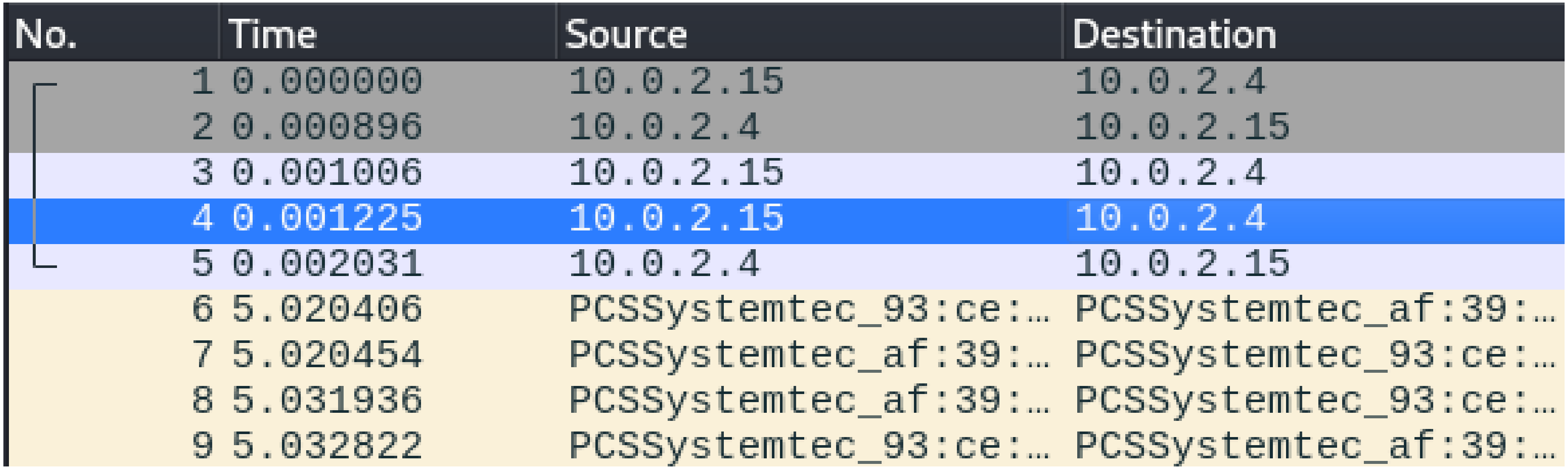
To switch between different conversation streams, click on the arrow keys in the bottom-right corner of the window

Summary



Let's review the digital forensics concepts we learned in this workshop:

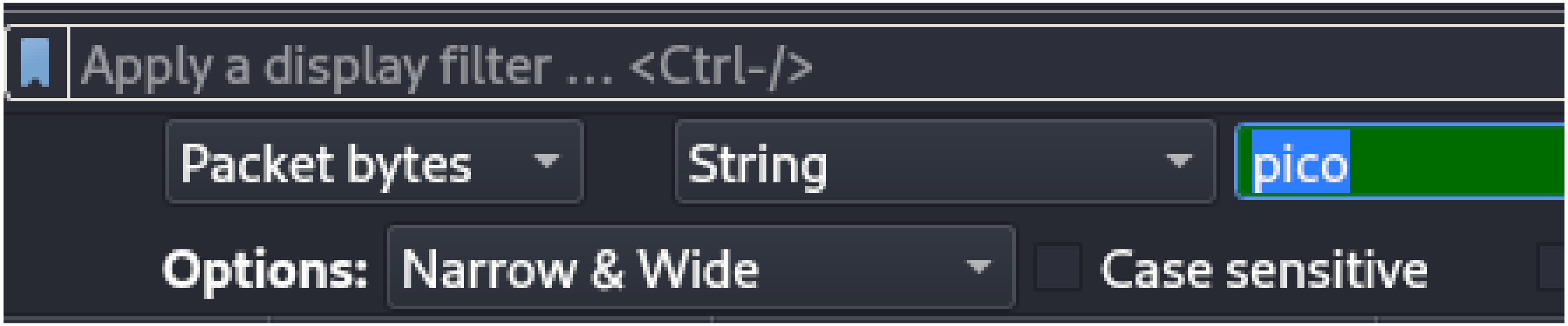
Manual Packet Inspection



No.	Time	Source	Destination
1	0.000000	10.0.2.15	10.0.2.4
2	0.000896	10.0.2.4	10.0.2.15
3	0.001006	10.0.2.15	10.0.2.4
4	0.001225	10.0.2.15	10.0.2.4
5	0.002031	10.0.2.4	10.0.2.15
6	5.020406	PCSSystemtec_93:ce:…	PCSSystemtec_af:39:…
7	5.020454	PCSSystemtec_af:39:…	PCSSystemtec_93:ce:…
8	5.031936	PCSSystemtec_af:39:…	PCSSystemtec_93:ce:…
9	5.032822	PCSSystemtec_93:ce:…	PCSSystemtec_af:39:…

If there are very few packets in a PCAP, it's possible to manually inspect them without too much trouble

Find Function: Strings

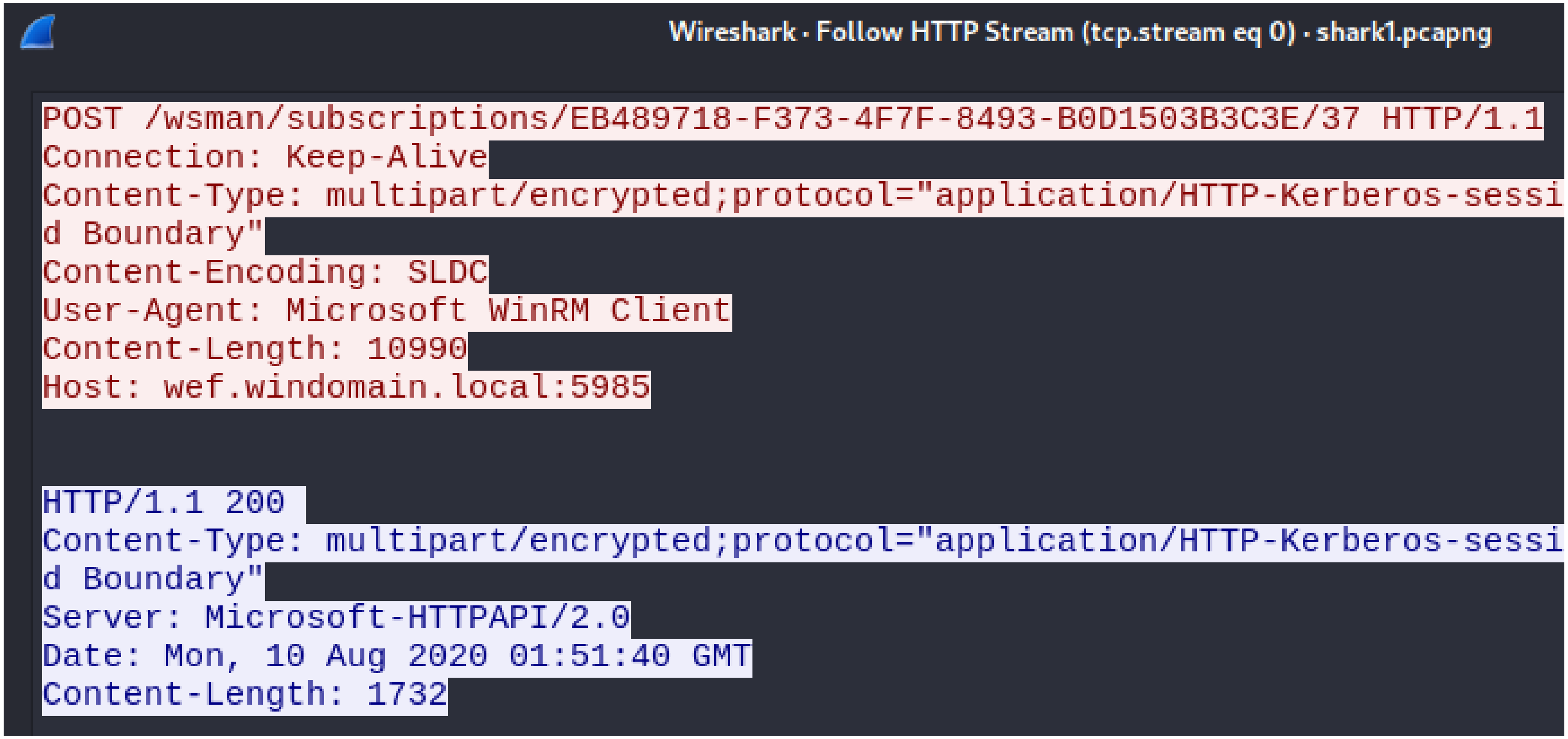

Apply a display filter … <Ctrl-/>

Packet bytes ▾ String ▾ pico

Options: Narrow & Wide ▾ □ Case sensitive

The Find function can let us return packets that only contain specified strings

Stream Follow Conversation


Wireshark · Follow HTTP Stream (tcp.stream eq 0) · shark1.pcapng

```
POST /wsman/subscriptions/EB489718-F373-4F7F-8493-B0D1503B3C3E/37 HTTP/1.1
Connection: Keep-Alive
Content-Type: multipart/encrypted;protocol="application/HTTP-Kerberos-sessi
d Boundary"
Content-Encoding: SLDC
User-Agent: Microsoft WinRM Client
Content-Length: 10990
Host: wef.windomain.local:5985


HTTP/1.1 200
Content-Type: multipart/encrypted;protocol="application/HTTP-Kerberos-sessi
d Boundary"
Server: Microsoft-HTTPAPI/2.0
Date: Mon, 10 Aug 2020 01:51:40 GMT
Content-Length: 1732
```

The “stream follow” function can be used to see all data sent between two servers in an easy-to-read format

What's Next?

In the next digital forensics workshop, we'll learn about a new topic, digital disk image forensics with PicoCTF!

Extra Credit

Looking for more study material on this workshop's topics?

See this video's description for links to supplemental documents and exercises!

Until Next Time, HackerFrogs!