HackerFrogs Afterschool Digital Forensics: Network Traffic

Class:
Digital Forensics

Workshop Number:
AS-FOR-03

Document Version:
1.75

Special Requirements:
Registered account at tryhackme.com

Welcome to HackerFrogs Afterschool!

Hey there HackerFrogs!

This is the third intro to Digital Forensics workshop.

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

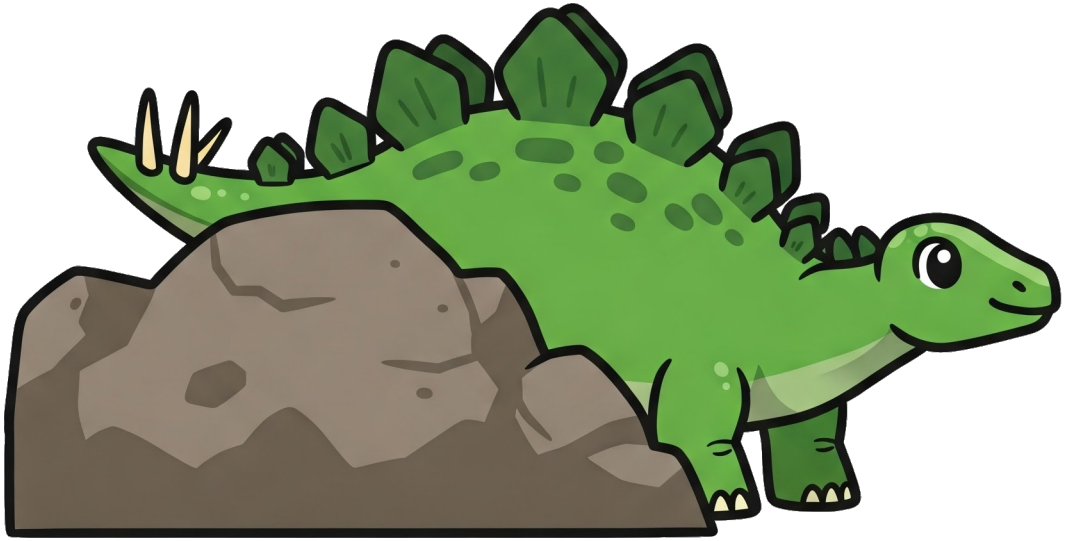
Steganography

Stegranography is the process of hiding information in another medium. E.g., hiding a hidden message in a picture

Steganography

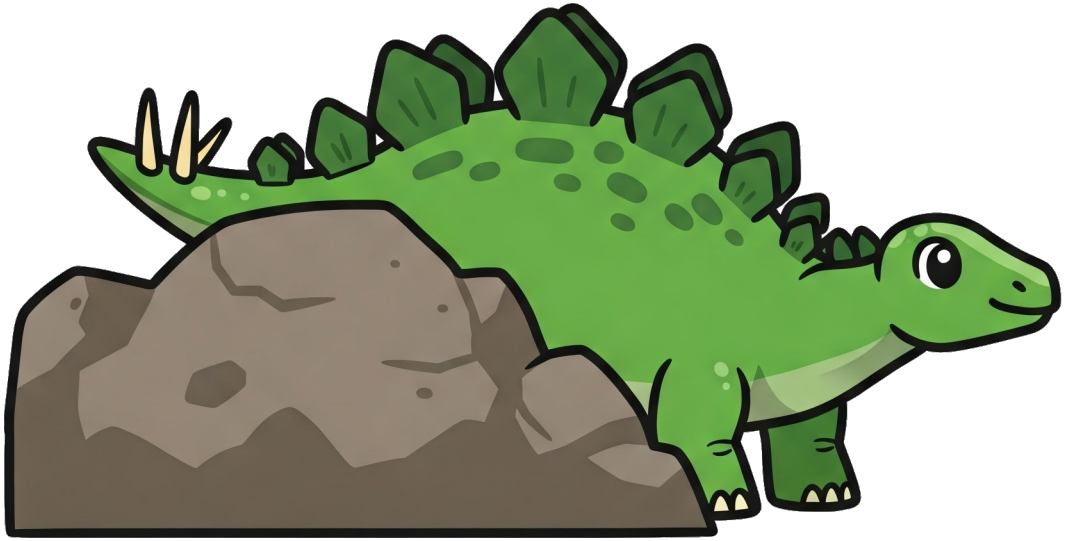
When dealing with digital files, steganography can be used to embed files or messages into different media files, like pictures, videos, and audio files

Steghide



Steghide is a program which can be used to embed files into certain types of picture and audio files

Steghide



Embedding files with Steghide can use password protection, for added security

This Workshop's Topics

- network logs

- packet capture files

- Wireshark

Network Traffic

This workshop's topic is computer networking log forensics.

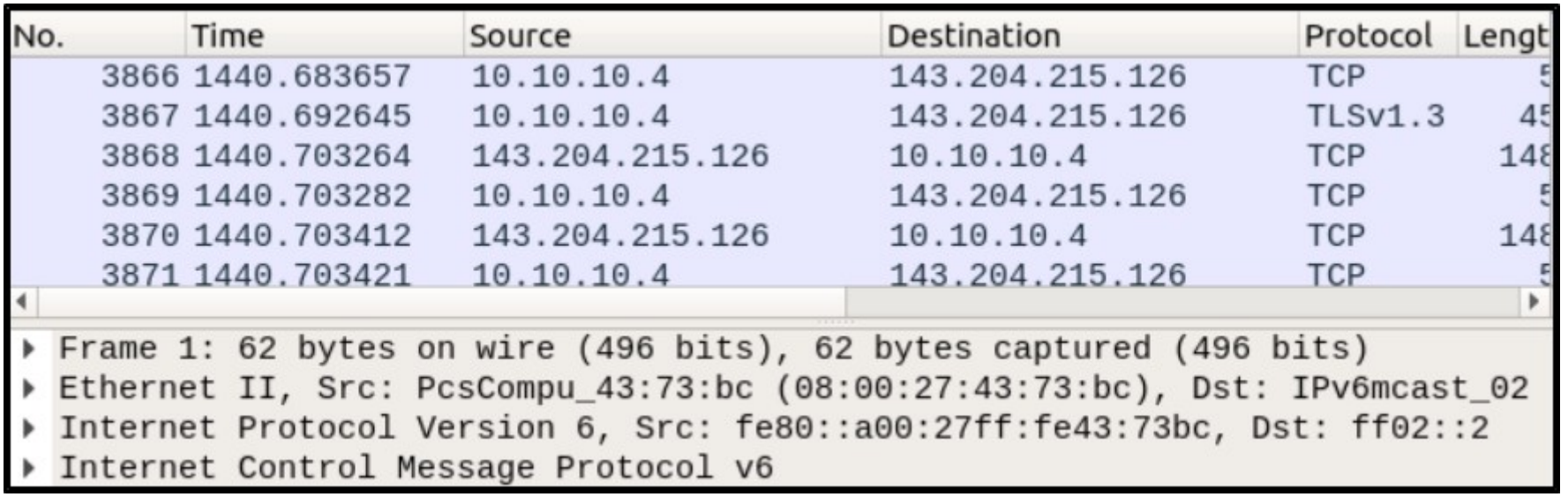
Network Traffic

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

What is a Network Device?

What is a network device? Any device that connects to a computer network: PCs, phones, tablets, cars, other IoT devices, etc, etc.

Network Packets and Traffic



No.	Time	Source	Destination	Protocol	Lengt
3866	1440.683657	10.10.10.4	143.204.215.126	TCP	5
3867	1440.692645	10.10.10.4	143.204.215.126	TLSv1.3	45
3868	1440.703264	143.204.215.126	10.10.10.4	TCP	148
3869	1440.703282	10.10.10.4	143.204.215.126	TCP	5
3870	1440.703412	143.204.215.126	10.10.10.4	TCP	148
3871	1440.703421	10.10.10.4	143.204.215.126	TCP	5

Network packets contain a number of elements, such as...

Network Packets and Traffic

Source	Destination
10.10.10.4	143.204.215.126
10.10.10.4	143.204.215.126
143.204.215.126	10.10.10.4
10.10.10.4	143.204.215.126

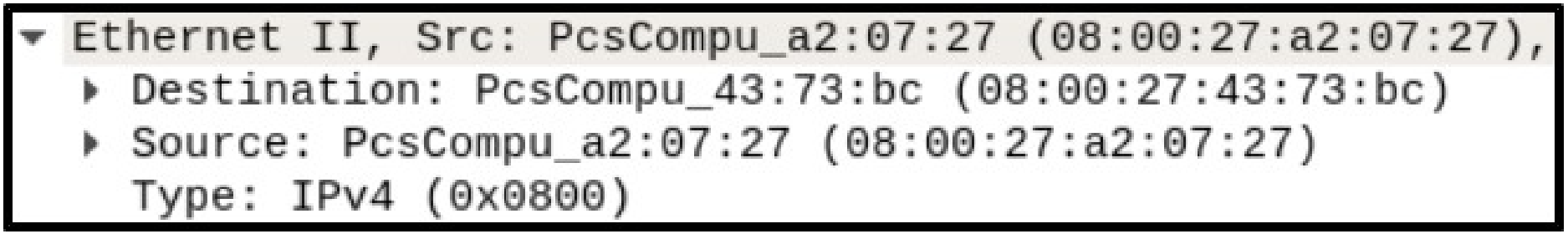
Source and **Destination**: the network addresses of both the source and destination devices (IP address)

Network Traffic

```
<html>\n
    <head>\n
        <title>[Simple Login Page! TryHackMe]</title>\n
        <link rel="stylesheet" media="screen" href="css/bootstrap.css"
        <link rel="stylesheet" media="screen" href="css/tryhackme.css"
</head>\n
```

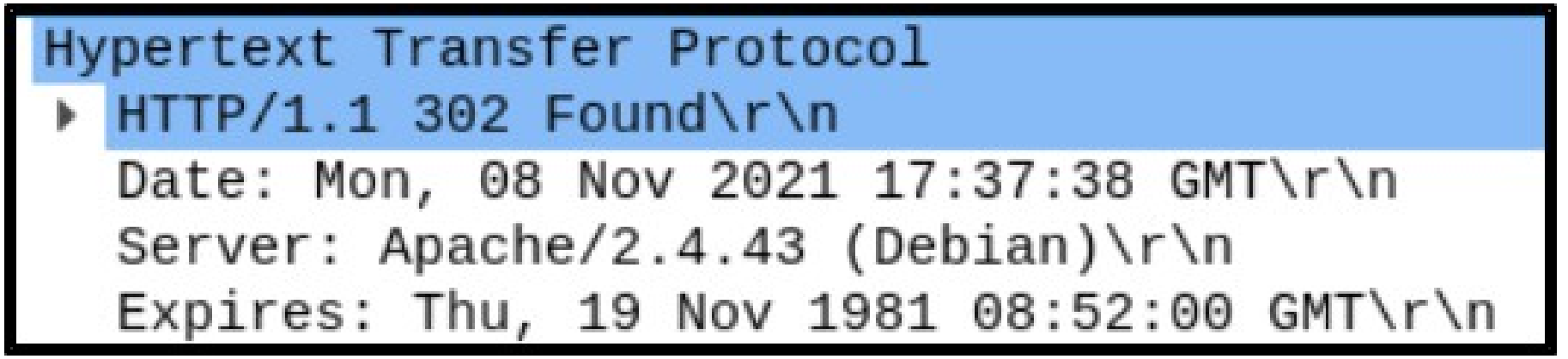
The “payload”: the actual data being sent

Network Traffic



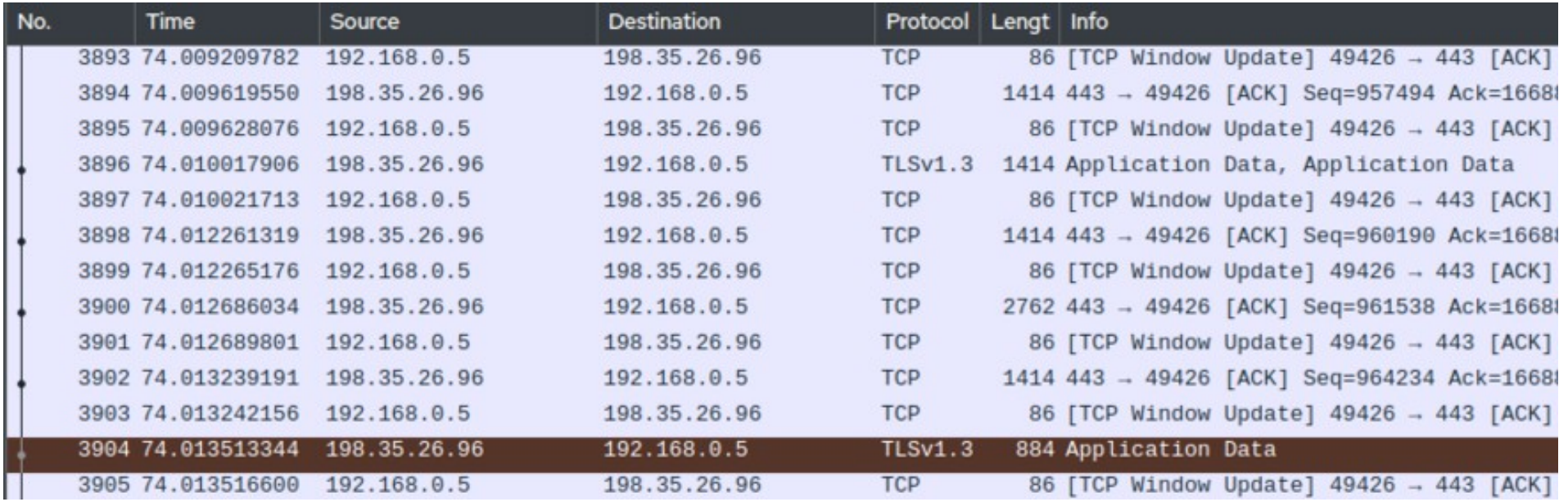
Header info: essential data for routing and processing the packet

Network Traffic



Protocol info: depending on the type of data packet (TCP, UDP, HTTP, etc), protocol-specific data can also be included in the packet

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.

Wireshark (Advent of Cyber Day 9)

We'll learn Wireshark through an interactive module on the TryHackMe website. Please navigate to the following URL:

https://tryhackme.com/r/room/adventofcyber3

Networking Basics: The OSI Model

Before we dive into how to use Wireshark, let's review the OSI model, which Wireshark uses to organize PCAP contents

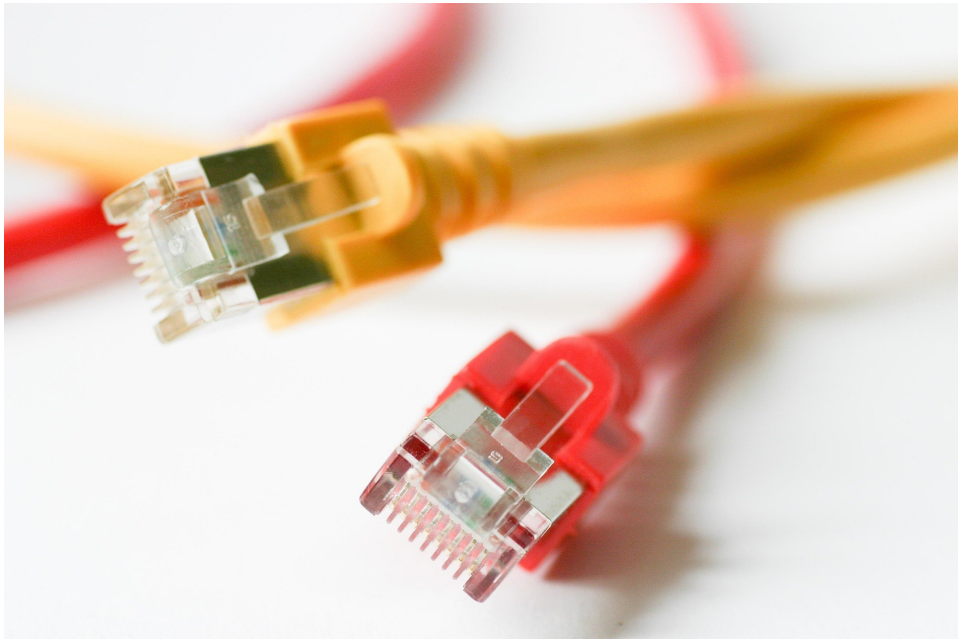
The OSI Model

The OSI model a system for organizing computer networking data into abstract layers. There are 7 layers in the OSI model:

The OSI Layers

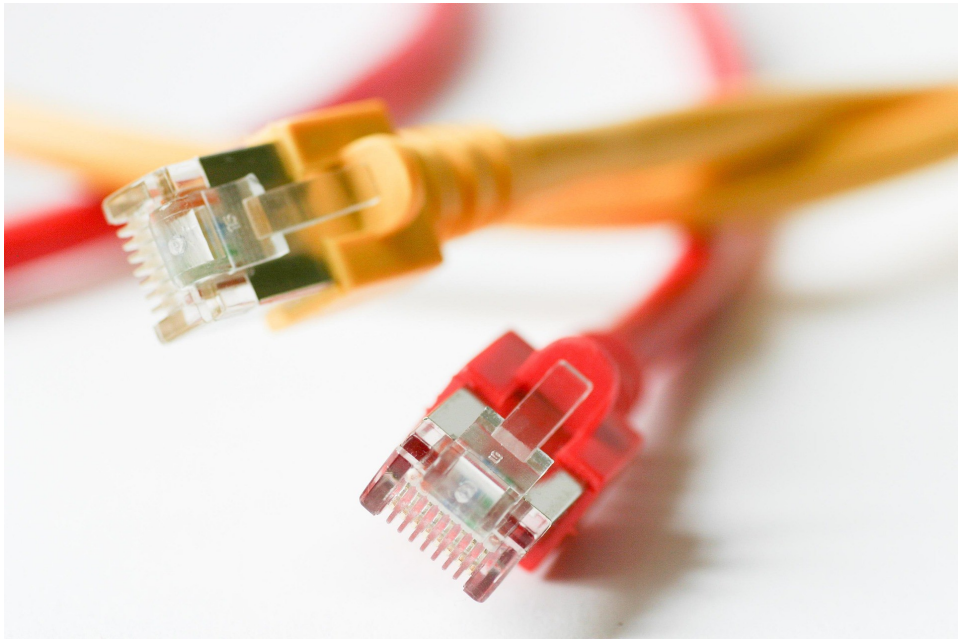
Layer 1 – Physical
Layer 2 – Data Link
Layer 3 – Network
Layer 4 – Transport
Layer 5 – Session
Layer 6 – Presentation
Layer 7 – Application

OSI Layer 1: Physical



OSI Layer 1 is the **Physical** layer, which represents the physical connection between devices and the sending / receiving of raw data bits over a physical medium

OSI Layer 1: Physical



Examples of things that transmit data over OSI layer 1 include cables, connectors, network interface cards (NICs), and modems.

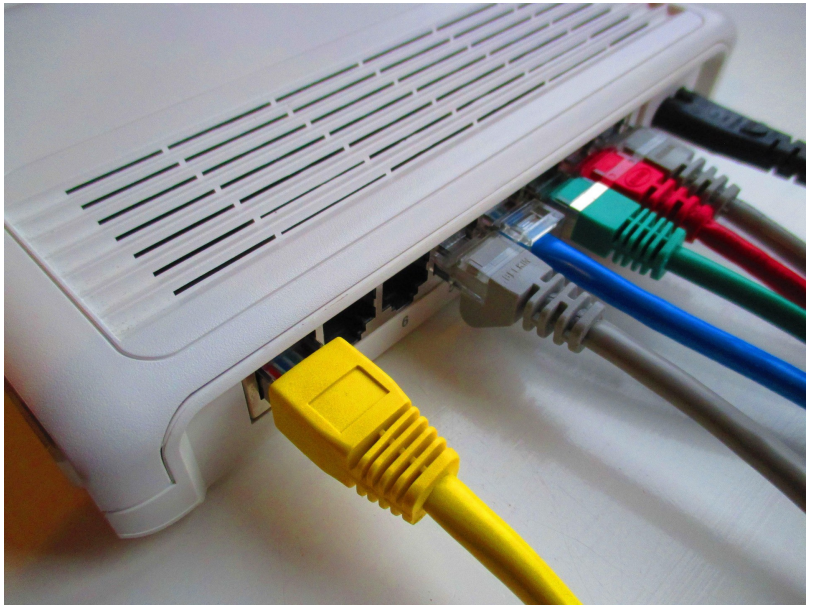
OSI Layer 2: Data Link

OSI Layer 2 is the **Data Link** layer, which provides reliable communication between directly connected nodes on a network. Data transmitted over the Data Link layer are called frames

OSI Layer 2: Data Link

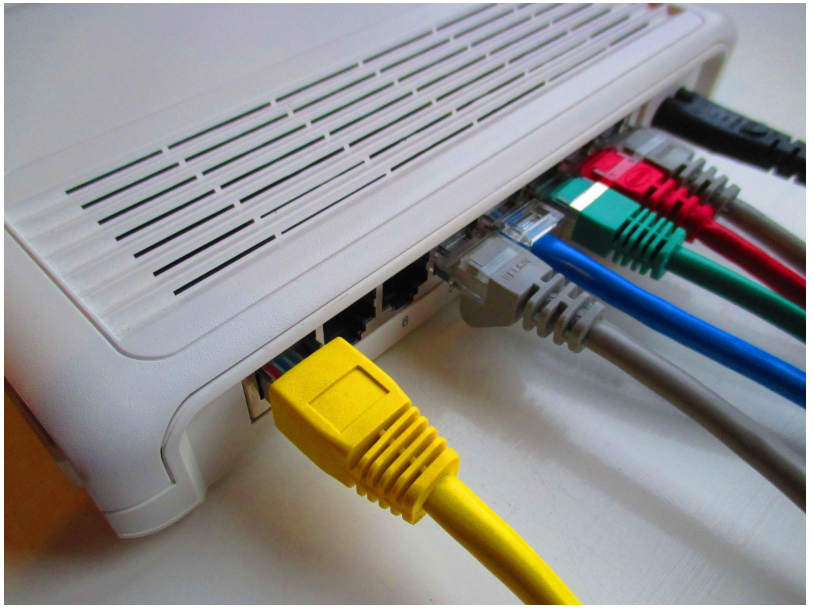
Examples of things that transmit data over OSI layer 2 include ethernet switches, wireless access points (WAPs), virtual LANs (VLANs), and MAC addresses

OSI Layer 3: Network



OSI Layer 3 is the **Network** layer, which covers logical addressing, routing, creation, and forwarding of packets between devices across different networks. Data transmitted over the Network layer are called packets

OSI Layer 3: Network



Examples of things that transmit data over OSI layer 3 are Firewalls, IPv4 / IPv6, ICMP, Network Address Translation (NAT) devices, and routers

OSI Layer 4: Transport

OSI Layer 4 is the **Transport** layer, which handles end-to-end communication, error detection / correction, and flow control in a network. Data transmitted over the Transport layer are called segments

OSI Layer 4: Transport

Examples of things that transmit data over OSI layer 4 are Transmission Control Protocol (TCP), User Datagram Protocol (UDP), port numbers, multiplexing, and socket programming

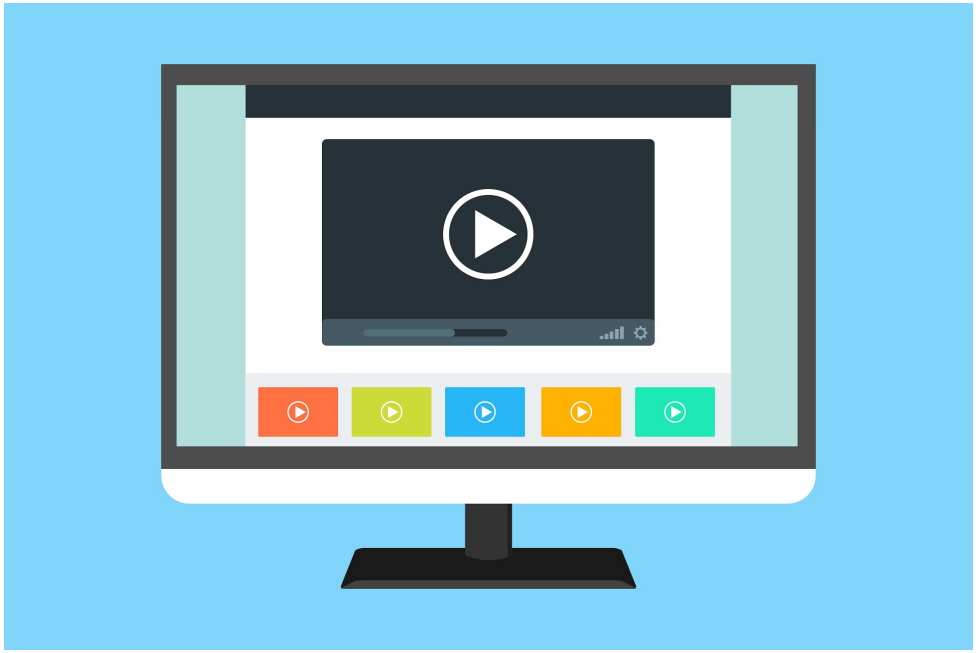
OSI Layer 5: Session

OSI Layer 5 is the **Session** layer, which manages communication sessions, and the orderly exchange of data between devices. Data transmitted over the Session layer is called data units or session data

OSI Layer 5: Session

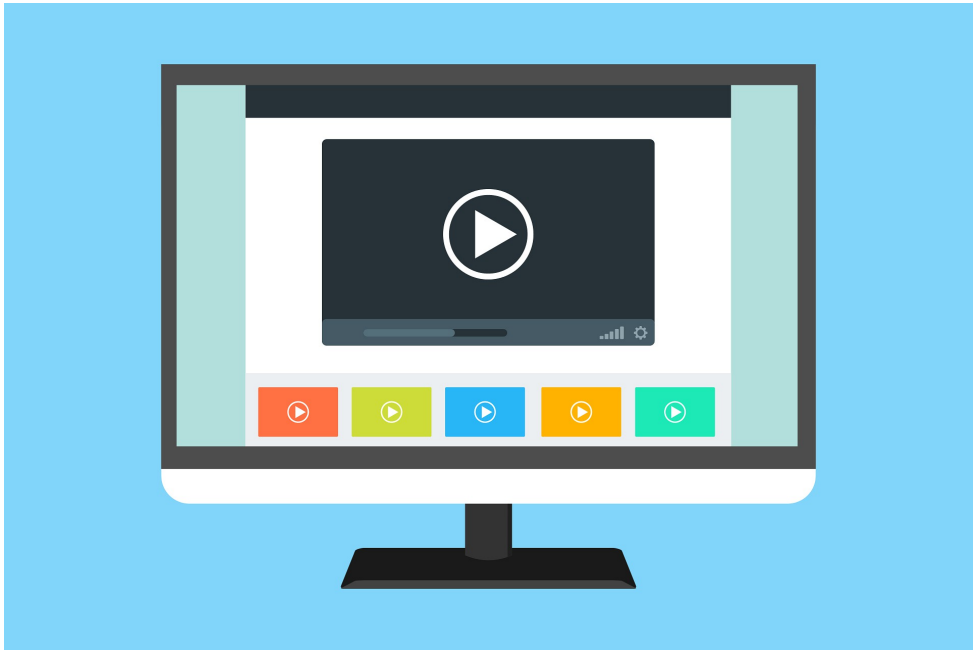
Examples of things that transmit data over OSI layer 5 are web browsers / web servers, remote desktop protocol (RDP), and network printing

OSI Layer 6: Presentation



OSI Layer 6 is the **Presentation** layer, and deals with encryption, character encoding, data compression, and format conversion. Data transmitted over the Presentation layer is called data units or presentation data

OSI Layer 6: Presentation



Examples of things that transmit data over OSI layer 6 are media players, transport layer security (TLS) protocols, file format converters, encoding libraries, and encryption / decryption software.

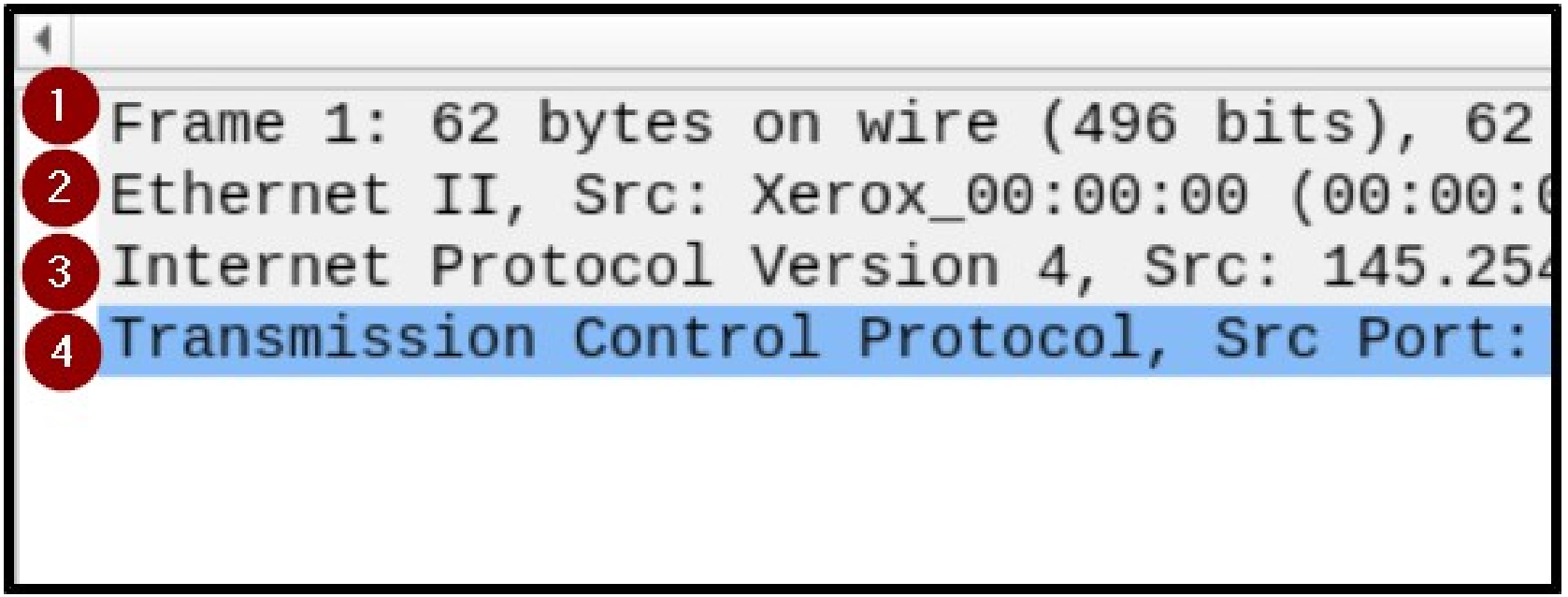
OSI Layer 7: Application

OSI Layer 7 is the **Application** layer, deals with end-user applications and offers a standardized interface for diverse apps across a network. Data transmitted over the Application layer is called application data, or messages

OSI Layer 7: Application

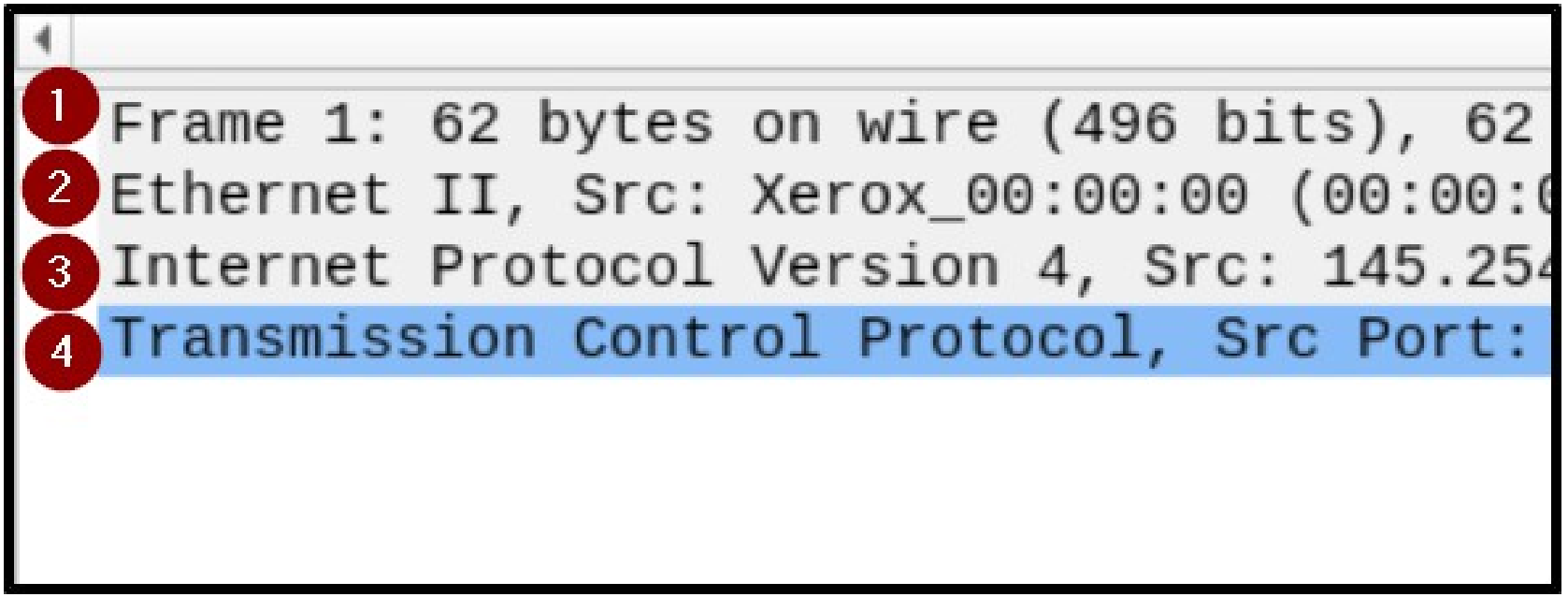
Examples of things that transmit data over OSI layer 7 are web browsers, HTTP, email clients, messaging apps, DNS, and database management systems (DBMS)

Wireshark and the OSI Model



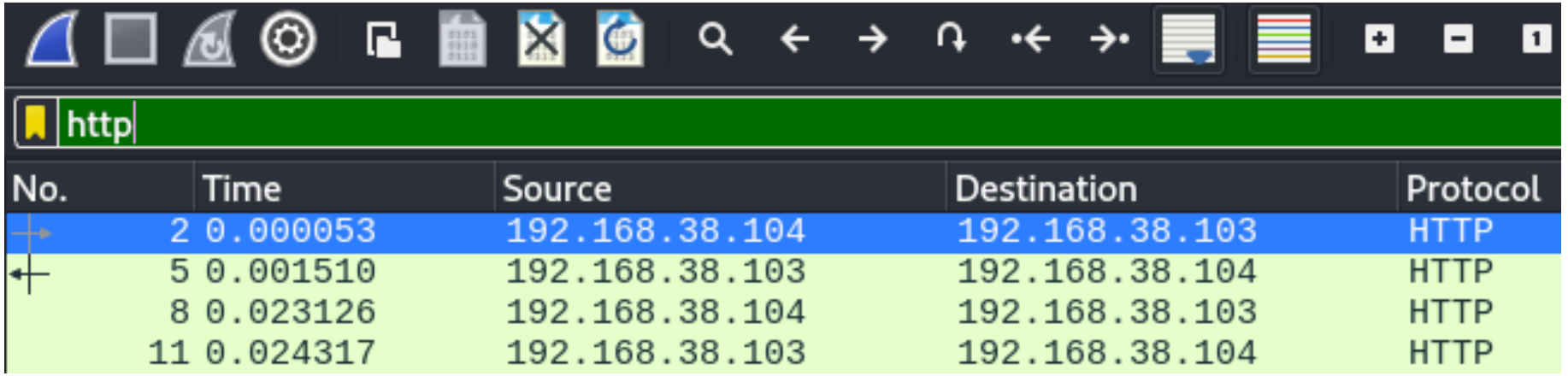
The Wireshark packet details pane organizes its expandable tabs according to OSI layers. Note that not all packets will contain layers in a sequence.

Wireshark and the OSI Model



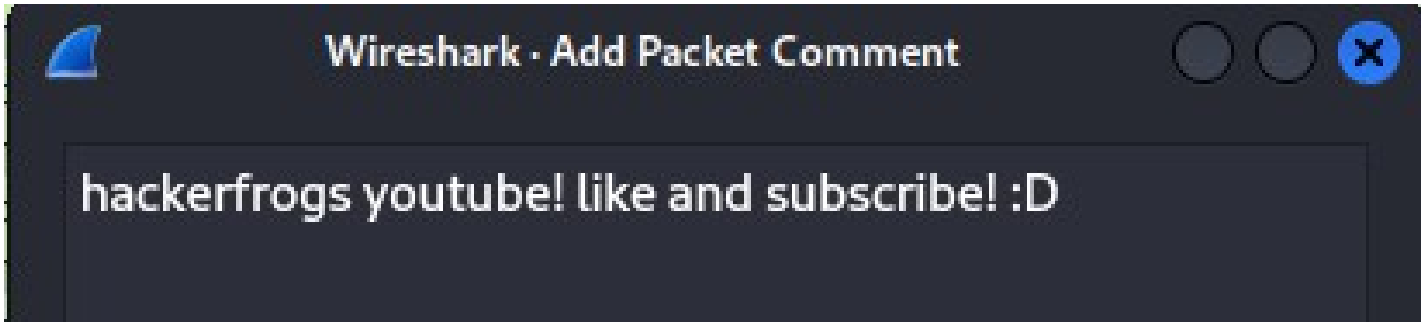
But most packets will contain data for OSI layers 1, 2, and 3.

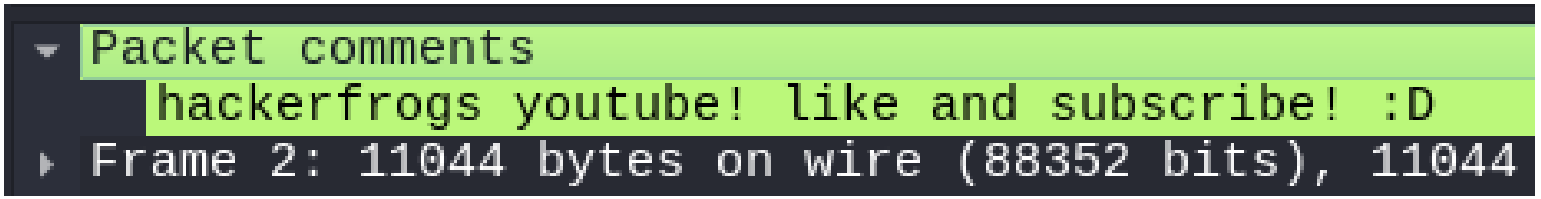
Display Filter



The display filter is an important tool for managing large numbers of packets, and can be fine-tuned to display only packets with specific properties.

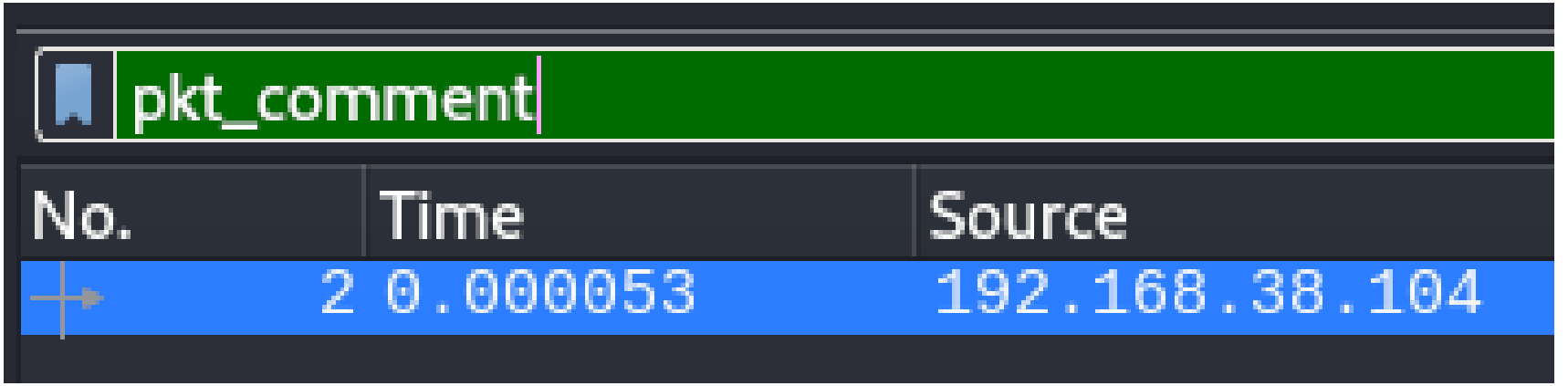
Packet Comments





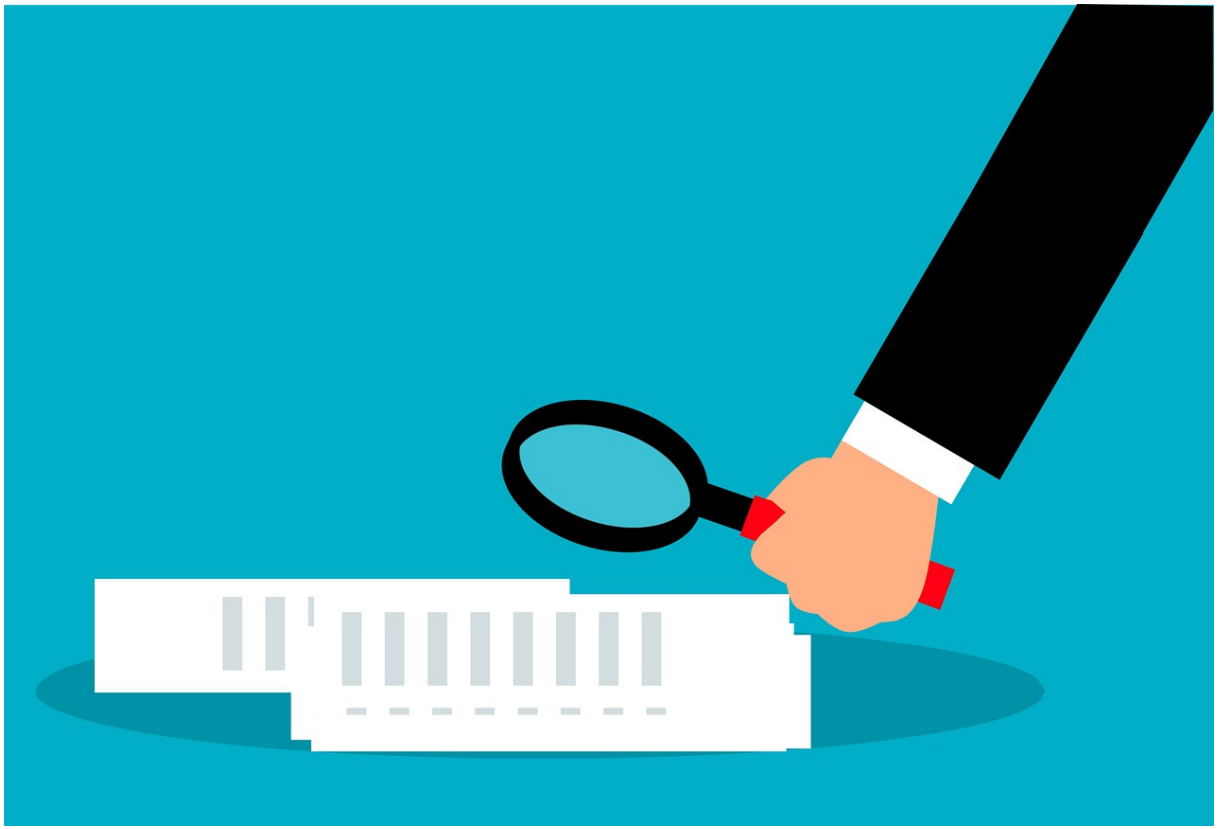
Packet comments are a way for analysts to attach notes to specific packets. The keyboard shortcut for packet comments is **Ctrl+Alt+C**.

Packet Comments



We can also filter packets by only those containing comments with the Display Filter “pkt_comment”

Summary

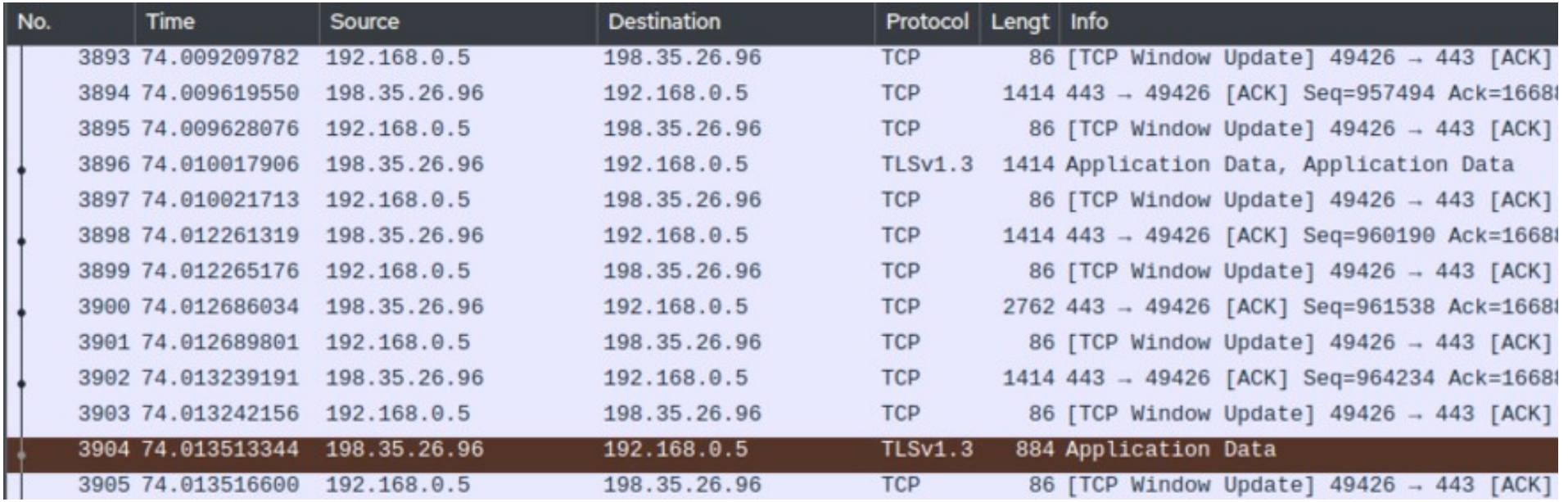


Let's review the digital forensics concepts we learned in this workshop:

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.

What's Next?

In the next digital forensics workshop, we'll practice more network traffic analysis with the TryHackMe platform

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!