Packet Analysis Using Wireshark

What is *Packet* Analysis?

- Look at and understand network traffic
- Also known as analyzing packets, also known as network traffic analysis, also known as packet sniffing, also known as protocol analysis, also known as packet tracing

Why Packet Analysis?

- Troubleshoot networking issues
- Record communications (e.g., email, voice, chat)
- Record and analyze web traffic

- Reconstruct images and other data transmitted on network
- Catch usernames and passwords, personal information, and other sensitive information that were sent insecurely, in plaintext

Source: https://www.wired.com/story/miraibotnet-minecraft-scam-brought-down-theinternet/

Adding to the complexity, DDoS itself is a notoriously difficult crime to prove—even simply proving the crime ever happened can be extraordinarily challenging after the fact. "DDoS can happen in a vacuum, unless a company captures logs in the right way," Peterson says. Klein, a former UNIX administrator who grew up playing with Linux, spent weeks piecing together evidence and reassembling data to show how the DDoS attacks unfolded.

On the compromised devices, they had to carefully reconstruct the network traffic data, and study how the Mirai code launched so-called "packets" against its targets—a little-understood forensic process, known as analyzing PCAP (packet capture) data. Think of it as the digital equivalent of testing for fingerprints or gunshot residue. "It was the most complex DDoS software I've run across," Klein says.

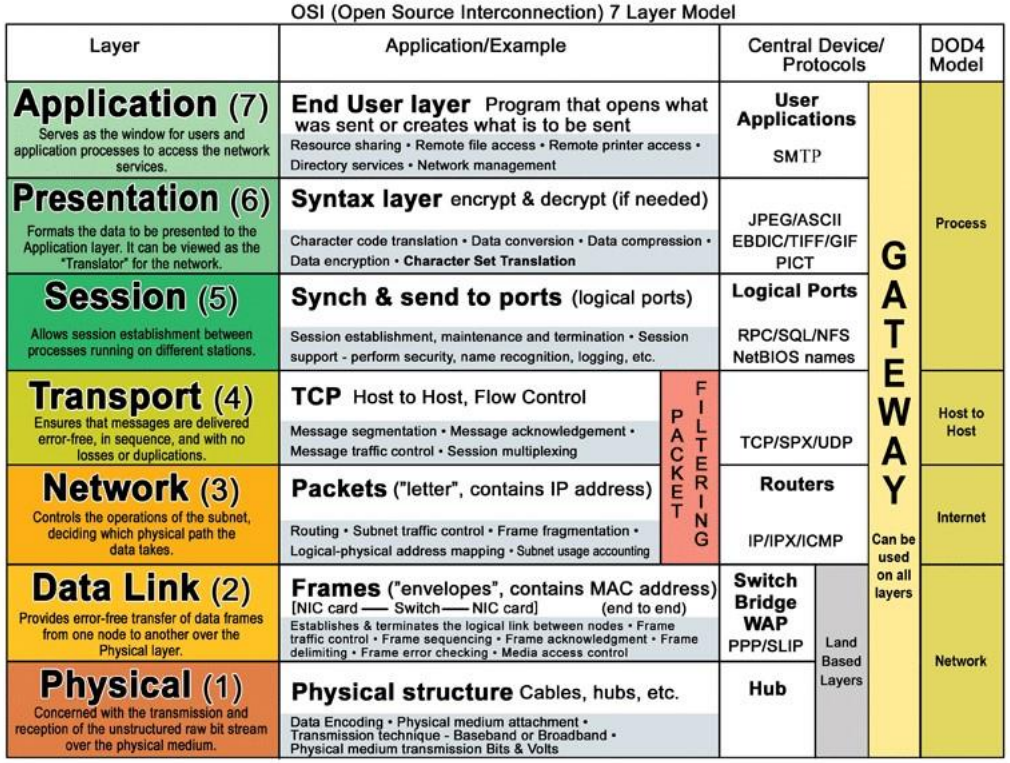
The FBI zeroed in on the suspects by the end of the year: Photos of the three hung for months on the wall in the Anchorage field office, where agents dubbed them the "Cub Scout Pack," a nod to their youthfulness. (Another older female suspect in an unrelated case, whose photo also hung on the board, was nicknamed the "Den Mother.")

What is a Packet?

- A unit of data
- A data stream (e.g., video, a web page) is comprised of many packets
- In general, a single packet contains the following information:
- Source and destination IP addresses and ports
- MAC address
- Time To Live (TTL)
- Protocol (e.g., TCP, UDP, IMCP)
- Payload
- A packet encapsulates all layers of the *Open Systems Interconnection (OSI) model*

What is the OSI Model?

- “A conceptual framework that describes the functions of a networking or telecommunication system.”
- 7 layers
- Each layer is abstracted from the other
- Sources:
- https://www.networkworld.com/article/3239677/lan-wan/the-osi-modelexplained-how-to-understand-andremember-the-7-layer-networkmodel.html
- https://buildingautomationmonthly.com/what-is-the-osi-model/



What is a PCAP File?

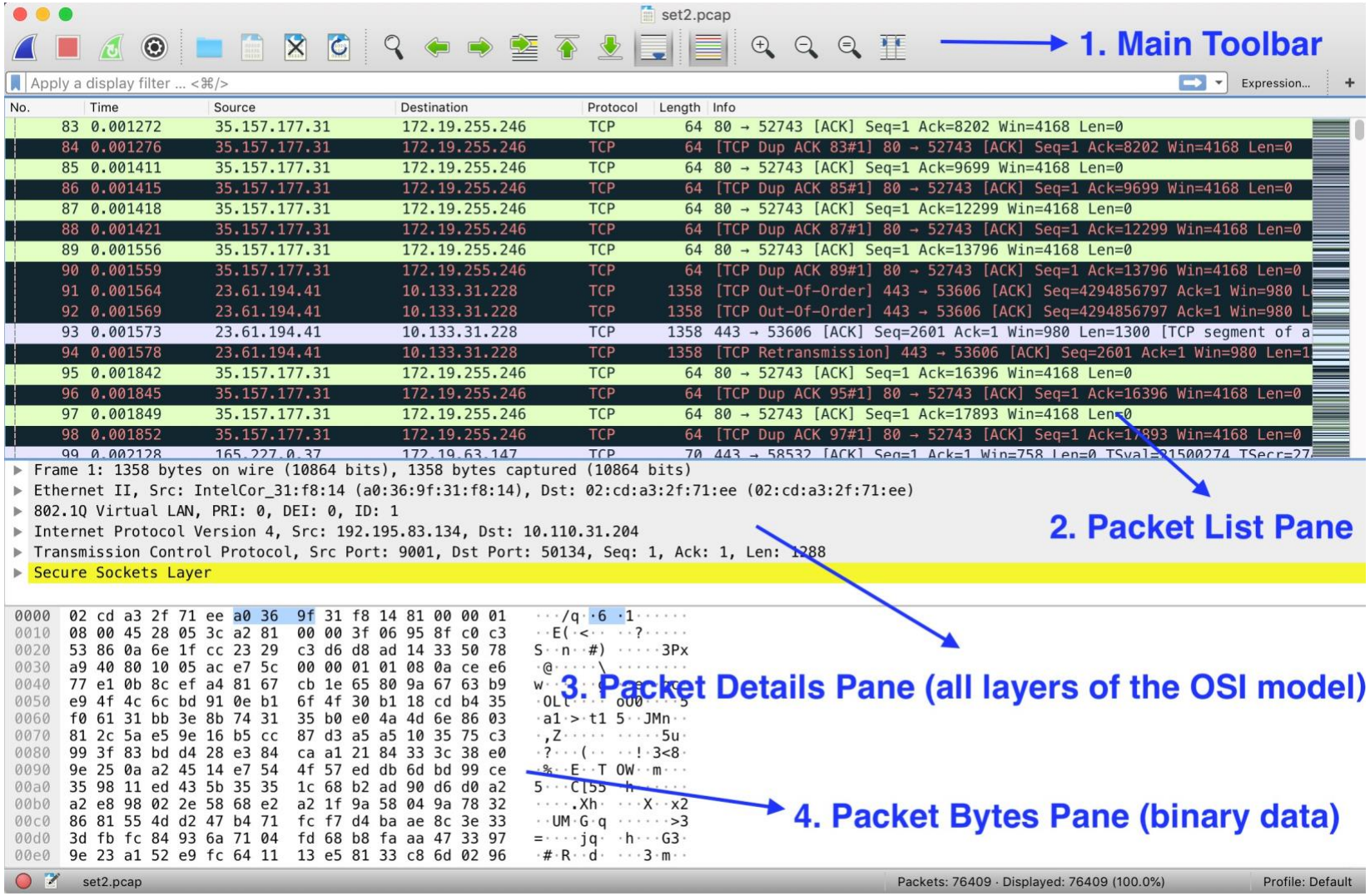
- PCAP stands for “packet capture”
- `.pcap`: The common file extension for packet captures and is commonly used in many applications such as *Wireshark*
- A 100 MB PCAP file contains tens of thousands of packets

What is Wireshark?

- Graphical and extensive packet analyzer
- Open source and free
- Platform independent (Windows, macOS, and Linux versions available)

- Features include filtering, reconstructing conversations, reconstructing files based on packets
- Website: https://www.wireshark.org/

The Wireshark User Interface

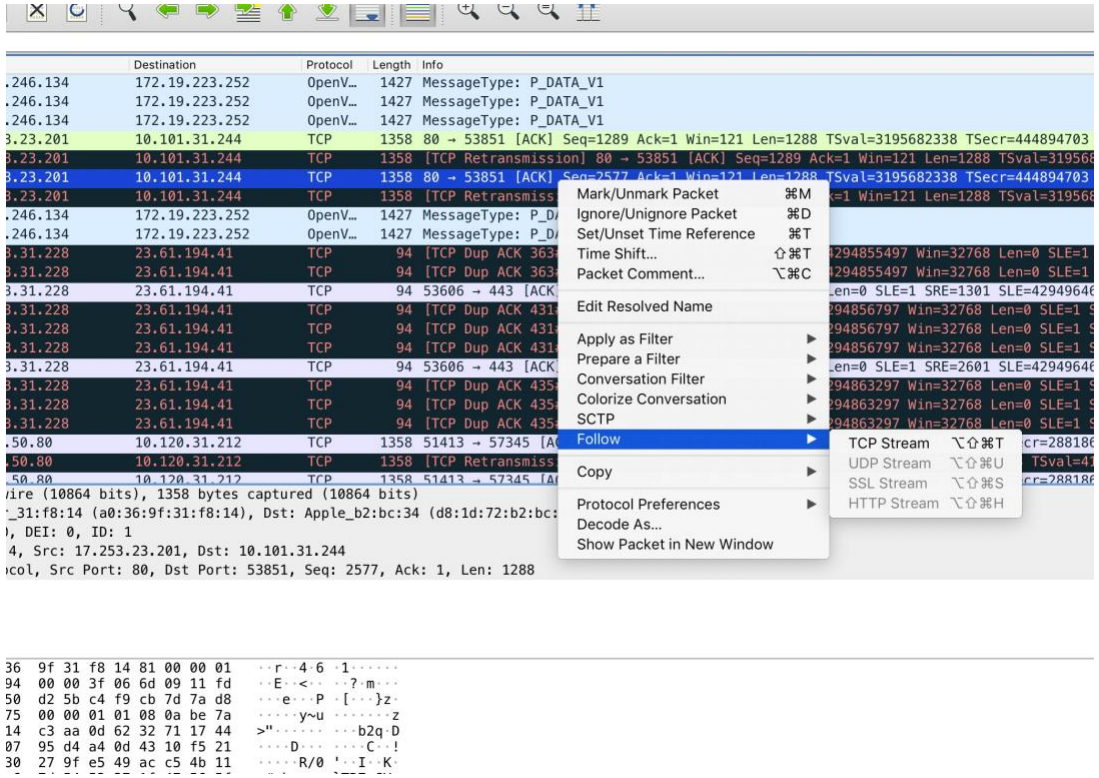


Exercise 1: Opening a Simple PCAP File in Wireshark

- Download: https://www.cs.tufts.edu/comp/116/simple.pcap
- Question 1: How many packets are there?
- Question 2: What networking protocol is used?
- Question 3: What is the source IP address?
- Question 4: What is the destination IP address?
- Question 5: What port number is the source using to communicate with the destination (or what port number is the destination listening on)?
- BONUS: Do you notice the “three-way handshake”?

Reconstructing a Conversation in Wireshark

1. Click on a packet (it will be highlighted in blue)
2. Right-click on packet
3. Go to “Follow”
4. Follow one of the following streams depending on protocol (TCP Stream is most common)



Exercise 2: Extracting Pictures

- Download: https://www.cs.tufts.edu/comp/116/set1.pcap
- Question 1: What insecure protocol was used to transmit pictures on network?
- Question 2: How many pictures were transmitted?
- Question 3: Extract one of the pictures that was transmitted. HINT: show and save the picture as “Raw” format.

Base64

- Base64 is an *encoding* scheme
- Used to represent binary data in ASCII text format
- Base64 is not encryption. Base64 is not encryption. Base64 is not encryption. Base64 is not encryption. Base64 is not encryption. Base64 is not encryption. Base64 is not encryption. Base64 is not encryption. Base64 is not encryption. Base64 is not encryption. Base64 is not encryption. Base64 is not encryption. https://sempf.net/post/base64-is-not-encryption
- Why is this important? “In basic HTTP authentication, a request contains a header field of the form `Authorization: Basic <credentials>`, where credentials is the Base64 encoding of id and password joined by a colon.” (source: https://en.wikipedia.org/wiki/Basic_access_authentication)

Exercise 3: Extracting Username:Password Pairs

- Download: https://www.cs.tufts.edu/comp/116/set3.pcap
- Question 1: What protocol was used to transmit the username:password pair (credentials)?
- Question 2: What is one username:password pair in this PCAP set? HINT: use Edit > Find Packet
- Question 3: Is the username:password pair valid? Why / why not?

(If time allows) Exercise 4: Extracting Username:Password Pairs

- Download: https://www.cs.tufts.edu/comp/116/set2.pcap
- This PCAP set is from the DEF CON conference. I am not responsible for the contents in this PCAP set.
- Question 1: How many packets are there in this PCAP set?
- Question 2: Find all the credentials in this PCAP set
- Question 3: Are the credentials valid?
- BONUS: Provide a list of all the domains and IP addresses in this PCAP set