Analyzing Network Packets

Aruna Balasubramanian

CSE 534, Fall 2021

Packet Analysis is a very important skill

- Network administrators use it to troubleshoot network problems
- Network security engineers use it to examine security problems
- QA engineers use it to verify network applications
- Developers use it to debug protocol implementations
- People use it to learn network protocol internals

How to analyze network packets

- A packet comes in to the Network Interface Card (NIC) at the host machine
- Typically, you process the packet at each layer and send the packet up to the application layer
- Instead, operating systems provide a technique to capture the packets at the NIC
  - The packet is processed by the higher layers as before
  - A copy of the packet capture is stored for use
  - This captured file is called a PCAP file

PCAP file

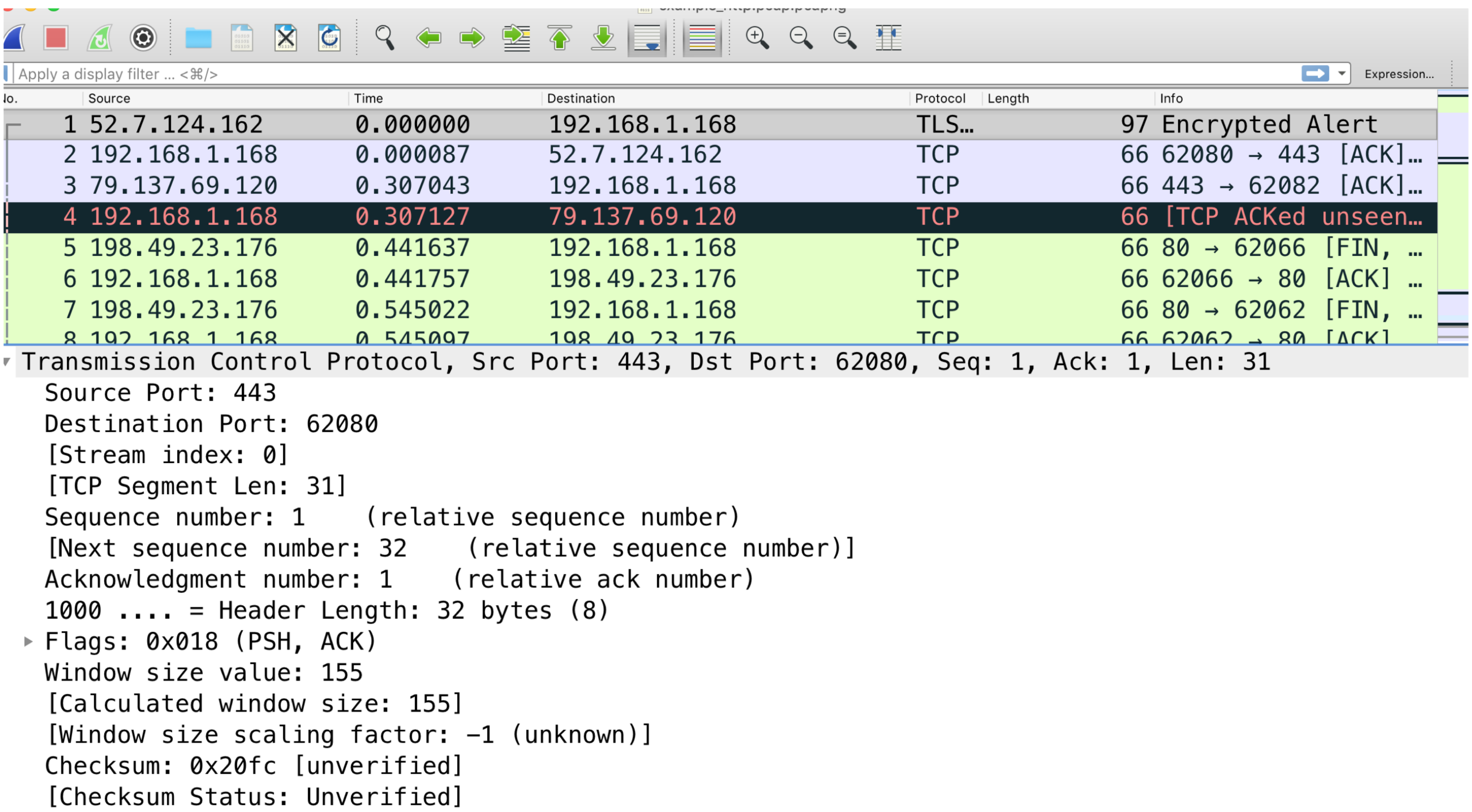
- PCAP stands for Packet Capture
- It has a .pcap extension
- To use the pcap file, you start your tool (that uses the pcap library that most Oses provide)
  - The tool will capture the raw packet information including all headers until you stop

Tools that are commonly used for pcap capture

- TCPDump: Command line tool
  - For example: sudo tcpdump --interface any

- More popular: Wireshark
  - Visual tool.
  - Already breaks down packet headers into different layers and helps you analyze packets

Wireshark



```
No.  Source         Time      Destination    Protocol Length Info
   1 52.7.124.162   0.000000  192.168.1.168  TLS…         97 Encrypted Alert
   2 192.168.1.168  0.000087  52.7.124.162   TCP          66 62080 → 443 [ACK]…
   3 79.137.69.120  0.307043  192.168.1.168  TCP          66 443 → 62082 [ACK]…
   4 192.168.1.168  0.307127  79.137.69.120  TCP          66 [TCP ACKed unseen…
   5 198.49.23.176  0.441637  192.168.1.168  TCP          66 80 → 62066 [FIN, …
   6 192.168.1.168  0.441757  198.49.23.176  TCP          66 62066 → 80 [ACK] …
   7 198.49.23.176  0.545022  192.168.1.168  TCP          66 80 → 62062 [FIN, …
   8 192.168.1.168  0.545097  198.49.23.176  TCP          66 62062 → 80 [ACK]
```

```
▾ Transmission Control Protocol, Src Port: 443, Dst Port: 62080, Seq: 1, Ack: 1, Len: 31
    Source Port: 443
    Destination Port: 62080
    [Stream index: 0]
    [TCP Segment Len: 31]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 32    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x018 (PSH, ACK)
    Window size value: 155
    [Calculated window size: 155]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x20fc [unverified]
    [Checksum Status: Unverified]
```