Wireshark Case Study

James Early
Randolph Odendahl
Bastian Tenbergen

November 2021

Wireshark Case Study

Background

A key element in network security is to have a keen sense of what type of traffic is transmitted inside of the network as well as between networks. For this purpose, network managers use certain tools to monitor, record, and analyse network traffic. Similarly, penetration testers may make use of the same tools during the "reconnaissance phase" of a penetration test to identify possible targets.

Case Study Overview

In this case study, we will use the common tool "Wireshark" to analyze a record of network traffic. Learners will develop some familiarity with the concepts involved in communicating over a network.

Student Instructions

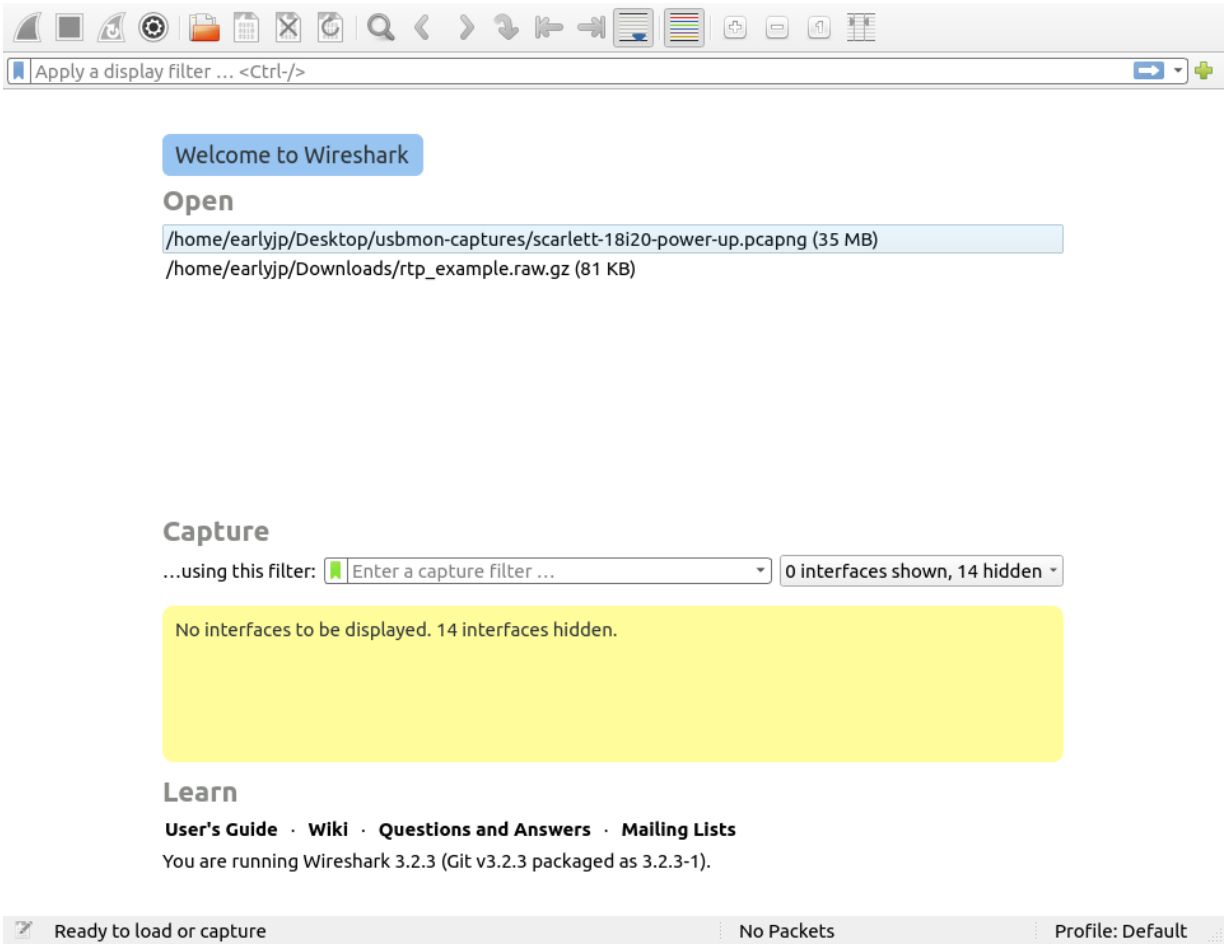
Setup

1. Launch a Web browser and visit https://www.wireshark.org/
2. Download and install the version of Wireshark required for your computer
3. Find the following files supplied with this case study and copy them to your computer:

   ```
   rtp_example.raw.gz
   dhcp.pcap
   ```

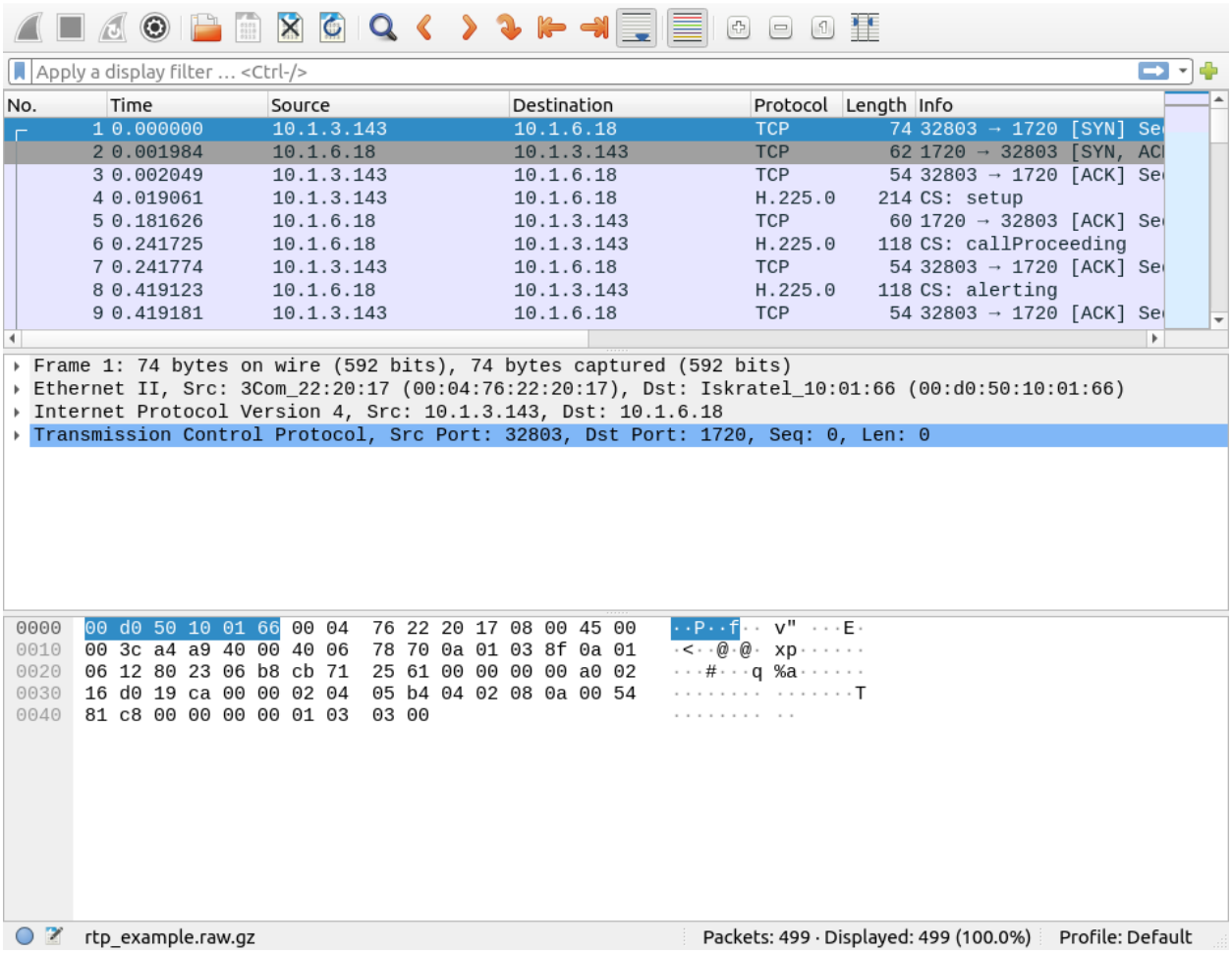
4. Launch the wireshark application

You should get an application window that looks like this (this example from Ubuntu Linux).



Investigate

1. Click on the Open folder icon (or choose "Open" from the "File" menu.)
2. Navigate to your Desktop folder and choose the file `rtp_example.raw.gz` from the open dialog
3. The captured session looks like this:



4. Answer each of the questions below and hand in a document with the questions and your answers. Be sure to retain the question number and sub-letter shown below.

Questions - Part 1

1. How many packets (frames) are there in this capture?
2. Choose the first frame in the top pane. Expand the Internet Protocol triangle of this frame in the middle pane.
    a. What are the source and destination addresses of this packet?
    b. To what entities do these numbers refer?
3. Expand the Transmission Control Protocol triangle of the packet.
    a. What are the source and destination ports of this packet?
    b. To what entities do these numbers refer?
4. Note that wireshark is smart enough to "know" which ports are typically used by internet applications. What service is the host at IP 10.1.3.143 trying to access on the host with IP 10.1.6.18? [hint]

5. Read this discussion excerpted from the previous hint and answer the questions that follow as best you can:

> H.323 uses a single fixed TCP port (1720) to start a call using the H.225 protocol (defined by H.323 suite) for call control. Once that protocol is complete, it then uses a dynamic TCP port for the H.245 protocol (also defined by the H.323 suite) for capabilities exchange (caps exchange) and channel control. Finally, it opens up two dynamic UDP ports for each type of media that was negotiated for the call (audio, video, far-end camera control, etc.). This first port carries the RTP protocol data (defined by the H.225 specification) and the second one carries the RTCP data (defined by the H.225 specification).

   a. Which frame first accesses port 1720 and, hence, initiates the exchange?
   b. At which frame do the parties shift to using another pair of ports (for the H.245 protocol)?
   c. At which frame do they begin the real-time protocol (RTP) specified by H.225?

Questions - Part 2

These questions are based on the `dhcp.pcap` file. Open the file in Wireshark and examine its contents to answer these questions:

1. Frame 1 - client is requesting an IP address. Expand the Bootstrap Protocol.
   a. What does **DHCP** stand for?
   b. What do you think **DHCP Discover** means?
2. Frame 2 - expand the Bootstrap Protocol.
   a. What do you think **DHCP Offer** means?
3. Frame 3 - expand the Bootstrap Protocol.
   a. What has the "client" requested of the DHCP server?
4. Frame 4 - The client now has an IP address.
   a. What is this address?

Instructor Notes

This case study should be made available as an individual assignment with a few days of preparation time. Alternatively, this case study could be used as an in-class exercise in a unit on network traffic monitoring.

Example solution

Questions - Part 1

1. How many packets (frames) are there in this capture?

A: There are 499 frames in this capture.

2. Choose the first frame in the top pane. Expand the Internet Protocol triangle of this frame in the middle pane.
    a) What are the source and destination addresses of this packet?
    A: Source: 10.1.3.143, Destination: 10.1.6.18

    b) To what entities do these numbers refer?
    A: These represent Internet Protocol addresses of computers on a private network

3. Expand the Transmission Control Protocol triangle of the packet.
    a) What are the source and destination ports of this packet?
    A: Source: 32803, Destination: 1720

    b) To what entities do these numbers refer?
    A: These represent the port numbers that the applications are using to establish a connection.

4. Note that wireshark is smart enough to "know" which ports are typically used by internet applications. What service is the host at IP 10.1.3.143 trying to access on the host with IP 10.1.6.18? [hint]
    A: The host is trying to access the H.323 Video Conferencing service

5. Read this discussion excerpted from the previous hint and answer the questions that follow as best you can:

    H.323 uses a single fixed TCP port (1720) to start a call using the H.225 protocol (defined by H.323 suite) for call control. Once that protocol is complete, it then uses a dynamic TCP port for the H.245 protocol (also defined by the H.323 suite) for capabilities exchange (caps exchange) and channel control. Finally, it opens up two dynamic UDP ports for each type of media that was negotiated for the call (audio, video, far-end camera control, etc.). This first port carries the RTP protocol data (defined by the H.225 specification) and the second one carries the RTCP data (defined by the H.225 specification).

    a) Which frame first accesses port 1720 and, hence, initiates the exchange?
    A: Frame 1

    b) At which frame do the parties shift to using another pair of ports (for the H.245 protocol)?
    A: Frame 15

    c) At which frame do they begin the real-time protocol (RTP) specified by H.225?
    A: Frame 34

Questions - Part 2

These questions are based on the dhcp.pcap file. Open the file in Wireshark and examine its contents to answer these questions:

6. Frame 1 - client is requesting an IP address. Expand the Bootstrap Protocol.
    a) What does **DHCP** stand for?
    A: Dynamic Host Configuration Protocol

    b) What do you think **DHCP Discover** means?
    A: DHCP Discover is a host attempting to locate a DHCP server from which to lease a local IP address

7. Frame 2 - expand the Bootstrap Protocol.
    a) What do you think **DHCP Offer** means?
    A: DHCP Offer contains the network information offered by the DHCP server in response to a request

8. Frame 3 - expand the Bootstrap Protocol.
    a) What has the "client" requested of the DHCP server?
    A: The client requested a local IP address for the network

9. Frame 4 - The client now has an IP address.
    a) What is this address?
    A: The address given was 192.168.0.10