

Wireshark Case Study

James Early
Randolph Odendahl
Bastian Tenbergen

November 2021

Copyright 2021 James Early, Randolph Odendahl, Bastian Tenbergen. All Rights Reserved.

NO WARRANTY

THIS MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. THE AUTHORS MAKE NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. THE AUTHORS DO NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this report is not intended in any way to infringe on the rights of the trademark holder.

Internal use. Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

External use. This document may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the authors.

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

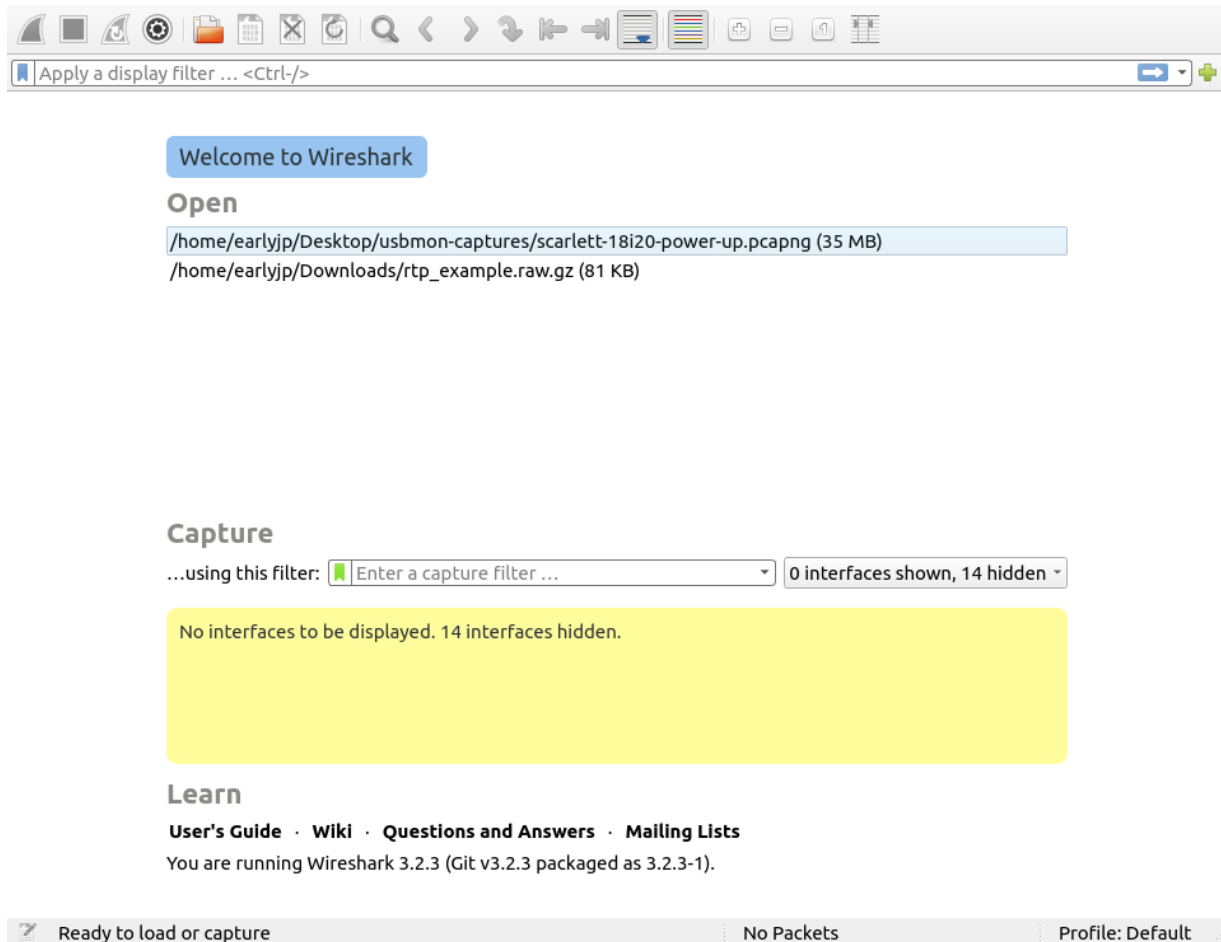
In this case study, we will use the common tool “Wireshark” to analyze a record of network traffic. Learners will develop some familiarity with the concepts involved in communicating over a network.

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:

The image shows a Wireshark interface with a packet capture of 'rtp_example.raw.gz'. The top pane displays a list of 9 packets. The middle pane shows the details of the first packet (No. 1), which is a TCP SYN packet from 10.1.3.143 to 10.1.6.18. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.1.3.143	10.1.6.18	TCP	74	32803 → 1720 [SYN] Seq: 0
2	0.001984	10.1.6.18	10.1.3.143	TCP	62	1720 → 32803 [SYN, ACK] Seq: 1720
3	0.002049	10.1.3.143	10.1.6.18	TCP	54	32803 → 1720 [ACK] Seq: 1720
4	0.019061	10.1.3.143	10.1.6.18	H.225.0	214	CS: setup
5	0.181626	10.1.6.18	10.1.3.143	TCP	60	1720 → 32803 [ACK] Seq: 1720
6	0.241725	10.1.6.18	10.1.3.143	H.225.0	118	CS: callProceeding
7	0.241774	10.1.3.143	10.1.6.18	TCP	54	32803 → 1720 [ACK] Seq: 1720
8	0.419123	10.1.6.18	10.1.3.143	H.225.0	118	CS: alerting
9	0.419181	10.1.3.143	10.1.6.18	TCP	54	32803 → 1720 [ACK] Seq: 1720

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

Ethernet II, Src: 3Com_22:20:17 (00:04:76:22:20:17), Dst: Iskratel_10:01:66 (00:d0:50:10:01:66)

Internet Protocol Version 4, Src: 10.1.3.143, Dst: 10.1.6.18

Transmission Control Protocol, Src Port: 32803, Dst Port: 1720, Seq: 0, Len: 0

```

0000  00 d0 50 10 01 66 00 04 76 22 20 17 08 00 45 00  ..P..f..v" ...E.
0010  00 3c a4 a9 40 00 40 06 78 70 0a 01 03 8f 0a 01  .<..@.@.xp.....
0020  06 12 80 23 06 b8 cb 71 25 61 00 00 00 00 a0 02  .#...q %a.....
0030  16 d0 19 ca 00 00 02 04 05 b4 04 02 08 0a 00 54  .....T
0040  81 c8 00 00 00 00 01 03 03 00                      .....

```

- 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

- How many packets (frames) are there in this capture?
- Choose the first frame in the top pane. Expand the Internet Protocol triangle of this frame in the middle pane.
 - What are the source and destination addresses of this packet?
 - To what entities do these numbers refer?
- Expand the Transmission Control Protocol triangle of the packet.
 - What are the source and destination ports of this packet?
 - To what entities do these numbers refer?
- 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