CSCD 433/533 Lab 1
Advanced Wireshark
Winter 2017

Background

In this lab we are going to explore more in-depth with Wireshark. We will look at some of the features that we have not covered in previous labs. Wireshark is a great tool for exploring networks. We will first look at an existing .pcap file in Part 1 of the lab and then, you have the opportunity to look at your own traffic at home using Wireshark.

Goals for this Lab

Previously, we have used the basic features of Wireshark such as capturing packets, analyzing packets from previous pcap files, identifying protocols and looking at TCP conversations. Now, we are going to delve more in-depth into:

- Statistics
- More complicated filtering
- Color packet analysis
- Conversation summaries for different protocols

Part 1 – Examining a Previously Captured .pcap file

Procedure

Start Wireshark.
Open a previously saved .pcap file, link to the file is on the Lab web page. You can save it to the desktop.
The file name is: tcp-ssh-capture1.pcap

Steps

Click on the ***Statistics*** tab of the main menu.
Click on the ***Summary*** tab and answer the questions below.

Questions

1. How many packets were captured in this file?
2. How much time between the first and last packet?
3. Looking at the majority of the packets captured in this file, what is the main protocol displayed?
4. Can you guess the purpose of the network connection and application used by looking at the packets captured in this file?

Now run another ***Statistics*** summary, ***Protocol Hierarchy***.

Answer more Questions

5. Are there DNS packets in the captured file? What percentage are they?
6. How many packets contain data from the captured packets?
7. Was this file captured from a Windows machine? How can you tell?

Packet Filters
In Question 5, you were asked if there were DNS packets in the file.
Set up a filter to see if these packets can be found in the file.

In the filter bar, enter **dns** and then hit apply.

8. How many packets did you find? What was the purpose of the dns packets?

Another way to filter this set of packets is to set the ip address to the dns server.
Type into the filter: **ip.addr==146.187.134.22**

9. What happens when you type this filter?

Type another filter, **arp** and then hit apply.

10. What response did you get, how many packets?
11. Arp is for mapping an IP address to a hardware Mac address.
In the Arp packets you filtered, was there a successful mapping of an IP address to a MAC address?
If yes, what was the MAC address found?

Colorizing Packets
In the ***View*** main menu choice, there are several Color menu items.
Click on the ***Coloring Rules*** and view all the different colors and associated protocols.
Then, click on ***Colorize Packet*** list and observe how the displayed packets are mapped to colors.

12. Look through the packet list and find any black colored packets.
List them – packet numbers and protocol.
What is the purpose of the black coloring?

Find the yellow colored packets. Name the protocol. What is the purpose of these packets?
You may have to use Google to find the answer.

13. What is the purpose of the dark grey color in this file? How many packets are dark grey?

Conversations
Lets go back to the ***Statistics*** menu tab and look at the conversations for each protocol.
Click on the ***Statistics*** menu tab and then the ***Conversations*** tab.
This brings up a table with Conversations listed by main protocol.
Click on the ***Ipv4*** tab.

14. How many conversations are listed in the window?
15. Click on the ***TCP*** tab. How many conversations are listed? Does the information in this window confirm the purpose of this conversation guessed at the beginning of this lab? What did you look at to

figure out the purpose of the TCP conversation?

Part 2 – Do this at Home

In this part of the lab you will be using wireshark on your home network.

Task 1 – Examining your own traffic

Likely you will be using the wlan0 interface for your wireless connection, unless you use wired Ethernet at home. Once you have selected this interface, start the capture.
Surf the web or do things you normally do like check email or even go to a game server.
Stop the capture after a short while. You will have lots of packets.

Use some of the tools we examined under the ***Statistics*** menu tab in Part 1 of the lab.

Create a short report listing:
a. the protocol composition of your captured packets.
b. the number of TCP conversations in your capture.
c. the number of UDP conversations in your capture.
d. Research one protocol you observed that is unfamiliar to you. Look up what it does and report on this.

Task 2 – Examining Others Traffic

Finally, if a member of your household was surfing unsavory websites, how could you capture their traffic to show that they were visiting these websites using Wireshark. Explain how you could do this. Typically, you will only be able to see your own traffic. However, wireshark can be used for network forensics in a spying capacity but takes a little more effort and special setup in order to do this. Write a brief summary of how you could accomplish this. Use Google.

Turning in the Lab
1. Put **CSCD433-Lab1** in the subject line.
2. Email the lab to me by the due date.

Finish.