Övning 4
ETS052 Datorkommuniktion - 2014
Wireshark

September 11, 2014

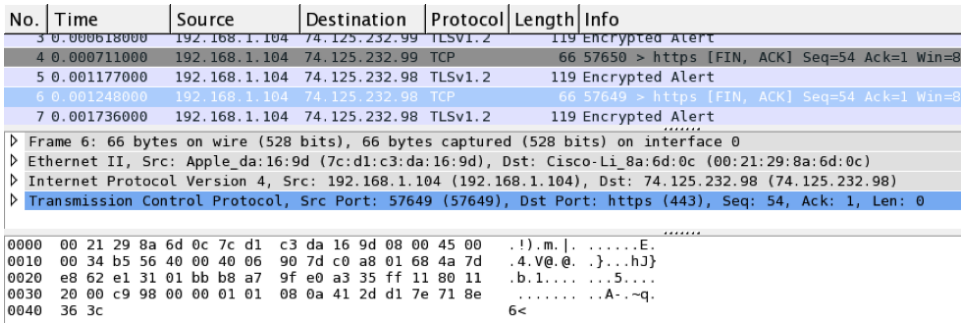
You can do the following exercise either on your own computer at home or in class. You will need to have Wireshark installed before you begin. Instructions on how to install and use Wireshark can be found in lab Y manual and in this guide.

1 What is Wireshark, and why would I ever need to use it?

Wireshark is an application that records/sniffs packets sent from, and received by your computer on a particular interface, but never sends any packets of its own. Wireshark records each packet from OSI level 2-7, and allows you to dissect and inspect each protocol the packet is composed of. Wireshark is aware of most protocols and is therefore able to isolate each parameter in their headers. Wireshark is even able to understand some application protocols, such as HTTP. Additionally, it allows you to filer out certain types of packets, transmissions, and applications. It is often used to monitor traffic, to analyze and debug application communication, and to see if there is any malicious communication emanating from a particular application. You will use Wireshark in some of the labs to analyze the traffic coming in and out of a specific application.

2 Prerequisite

An Internet connection over Wi-Fi or Ethernet, Wireshark installed and running on your computer.



3 Getting started

Open Wireshark and select the interface you wish to monitor. Start the capture by clicking the green shark fin. Wireshark will now capture and display every packet passing through the selected interface. Start the application or process that you wish to observe. Wireshark will now display the packets in sequence as they are transmitted and received. In order to be able to make more sense out of the torrent of packets, you can apply a filter to the output. For example, after applying the filter ip.src==192.168.1.20 Wireshark will only display the packets that originate from 192.168.1.20. Filters can also be applied to discern between different applications, ports, and protocols. For more on filters, visit the filter guide. Each packets will be displayed in a list, with an associated and by now familiar packet dump. Each packet is dissected into its constituent protocols and parameters. After your done capture the event(s), stop the trace capture.

1. When your computer is first connected to a network, using Wireshark, determine which packets are sent and to whom they are sent. Disconnect your Wi-Fi and/or Ethernet connection, leaving your computer without Internet. Start a Wireshark trace and reconnect your Internet interface.

2. Using Wireshark, try to determine which applications that are running on your computer by observing the packets these applications produce.

3. Try to turn off all Internet-dependent application on your computer such as Skype, your web browser, etc.

4. Determine the address of your router by using the trace from Problem 1. Which packet(s) reveal this information?

5. Determine, using Wireshark, which when you browser requests a web page. Proceed by opening your browser and start a new Wireshark trace, query www.vecka.nu.

6. Now try a website of your own choice. preferably one with lots of content.

7. Filter for the packets that are associated with the request. Which parameters did you use?

8. Determine the bitrate of the HTTP request. Try using a filer to isolate the traffic, or have a look at Statistics->IO Graph or Analyze->Follow TCP Stream, there are numerous ways to do this, be creative and use what you have learned!