Lab 8. Dynamic Analysis

Dan Bruce, David Clark and Hector D. Menendez

Department of Computer Science
University College London

November 27, 2017

Network Analysis

Using the information of the network traffic, we can perform different kind of analysis:

- Conversation Analysis.
- Content Analysis.
- Identify the Malware origin.
- Data Mining Analysis

Wireshark

Wireshark is the world's foremost network protocol analyzer.

It lets you see what's happening on your network at a microscopic level.

It is the de facto (and often de jure) standard across many industries and educational institutions.

Working with Wireshark

Sniffing§

Filtering

Following

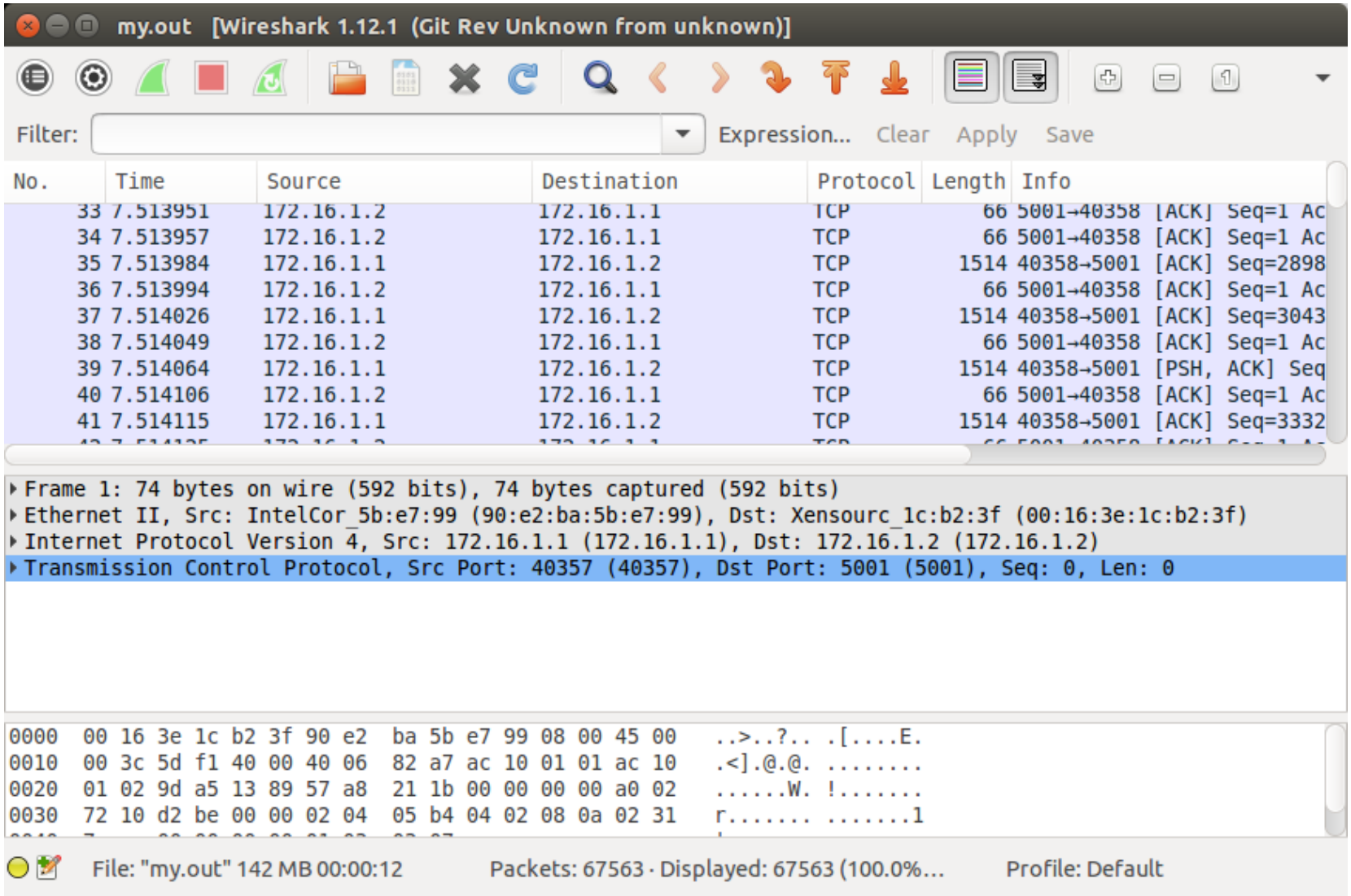
Analysing

Packer Sniffer

The basic tool for observing the messages exchanged between executing protocol entities is called a packet sniffer.

A packet sniffer receives a copy of packets that are sent / received from/by application and protocols executing on your machine.

Wireshark Interface



Capturing Packets

Run wireshark as an admin user.

Choose the capturing interface.

Run it until you want to stop.

Filtering

You can filter data according to the IP, Protocol.

You can follow a specific data stream.

You can analyse the information of the different protocol packages.

You can save the data in pcap files.

Following

Related to the Filtering process you can follow a specific stream.

With this you can follow specific conversations.

Also, it provides a good interfaces to see protocol exchanges.

Analysing

You can use the statistical tools from Wireshark

They provide different information about the packets such as timing, sender, receiver, etc.

It is interesting for having a general idea of the network.

Network Data

http://panda.gtisc.gatech.edu/malrec/

Exercise

1. Provide the statistics of the file (Packets, Time Span, Average pps, Average Packet size, Bytes, Average Bytes per second).
2. What percentage of packets are IRC packets?
3. What is the victim IP?
4. How many IRC conversations are? Who are the agents?
5. How many packets have been sent in every conversation?
6. Show a graph of packets per second for all packets in the pcap file.
7. Show an example of a conversation
8. Describe the information that can be extracted from the IRC conversations.