CIS4204.01 **Brandon Thompson**
Dr. Ashokkumar Patel Due: 3/29/21

Lab Homework 6: Sniffing

In this lab we will be capturing and analyzing packets using Wireshark, TCPDump, and NetWitness Investigator

On Windows I am using Wireshark to capture packets, both time slots use the `WiFi` connection.

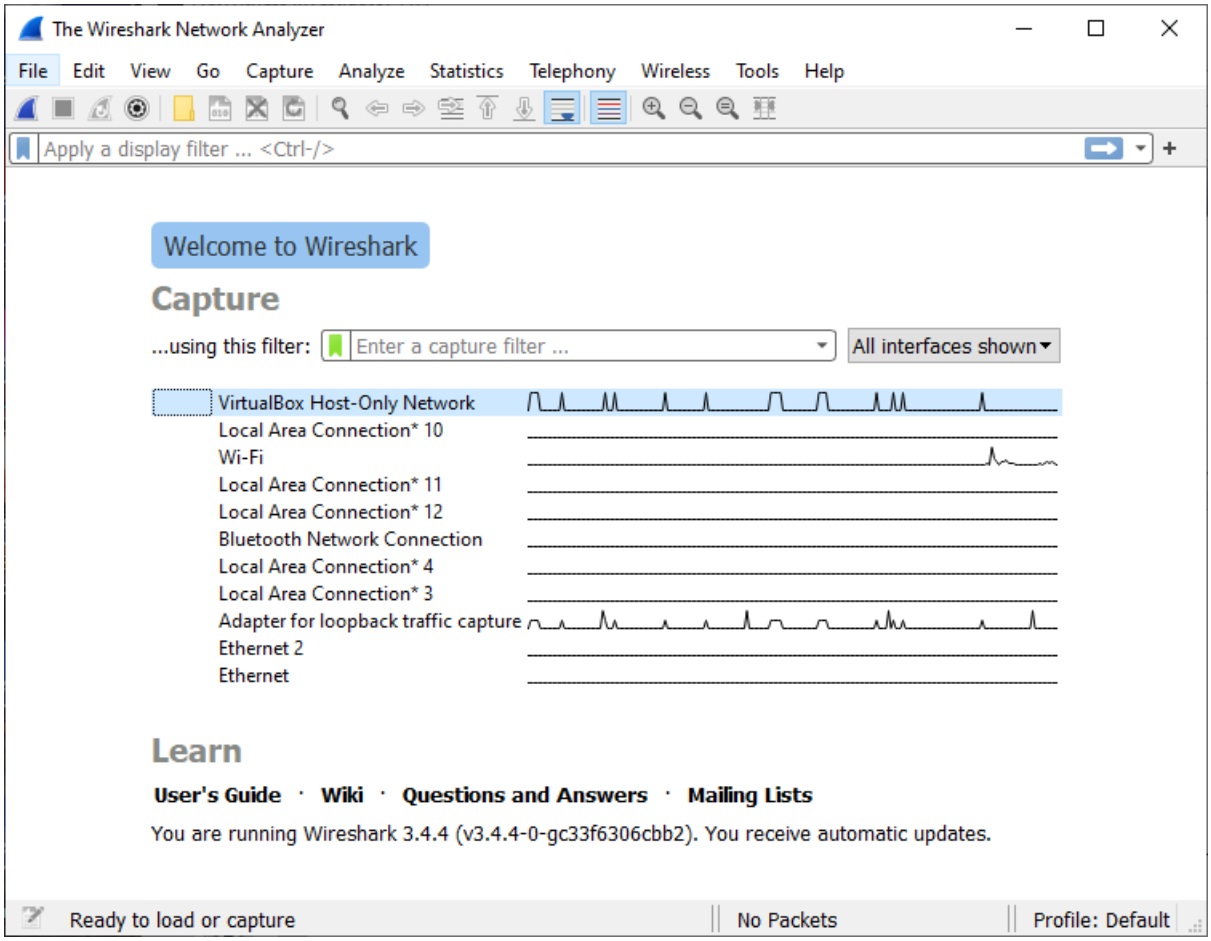

Figure 1: Start screen of Wireshark.

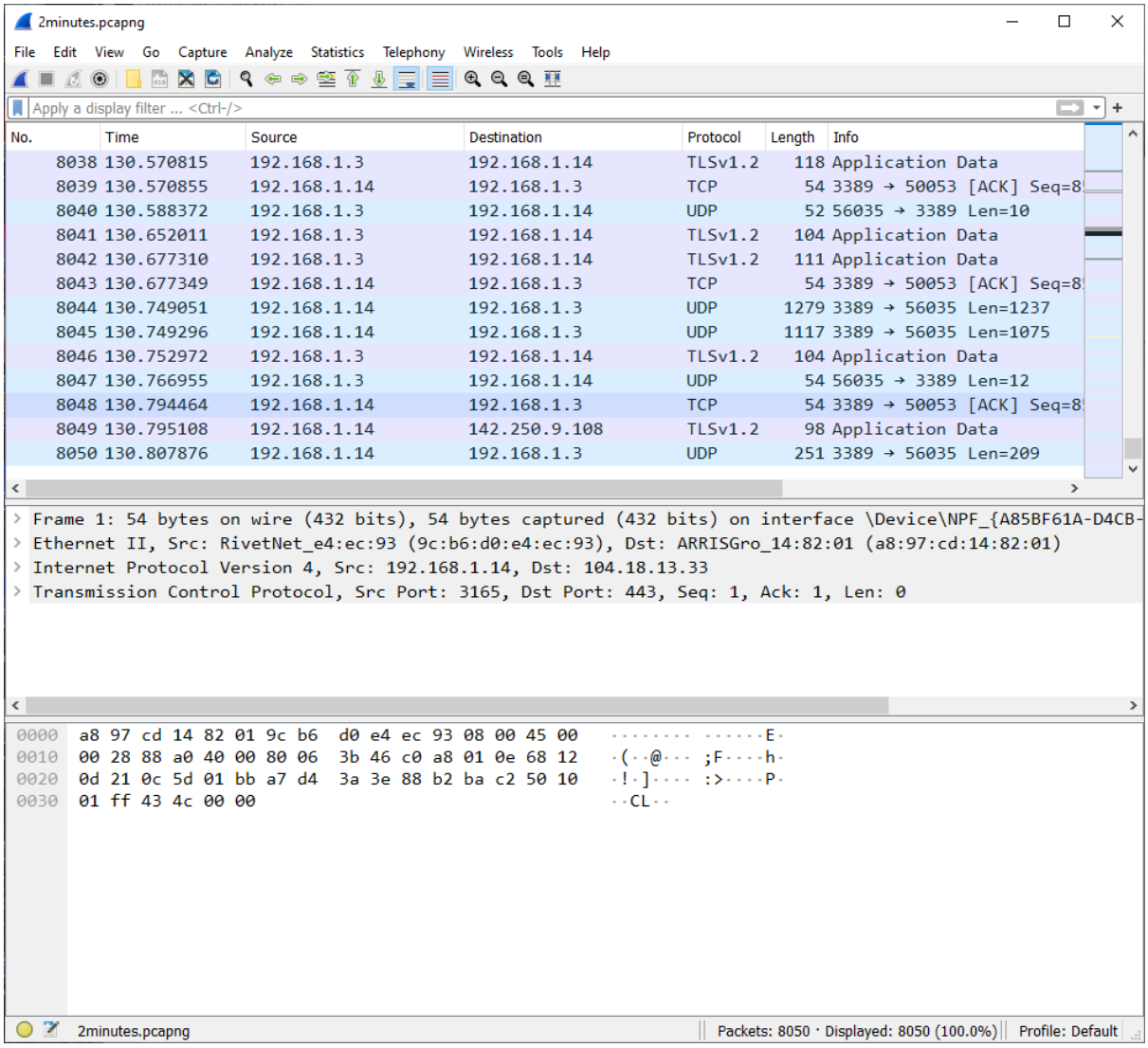

Figure 2: Capture for 2 minutes.

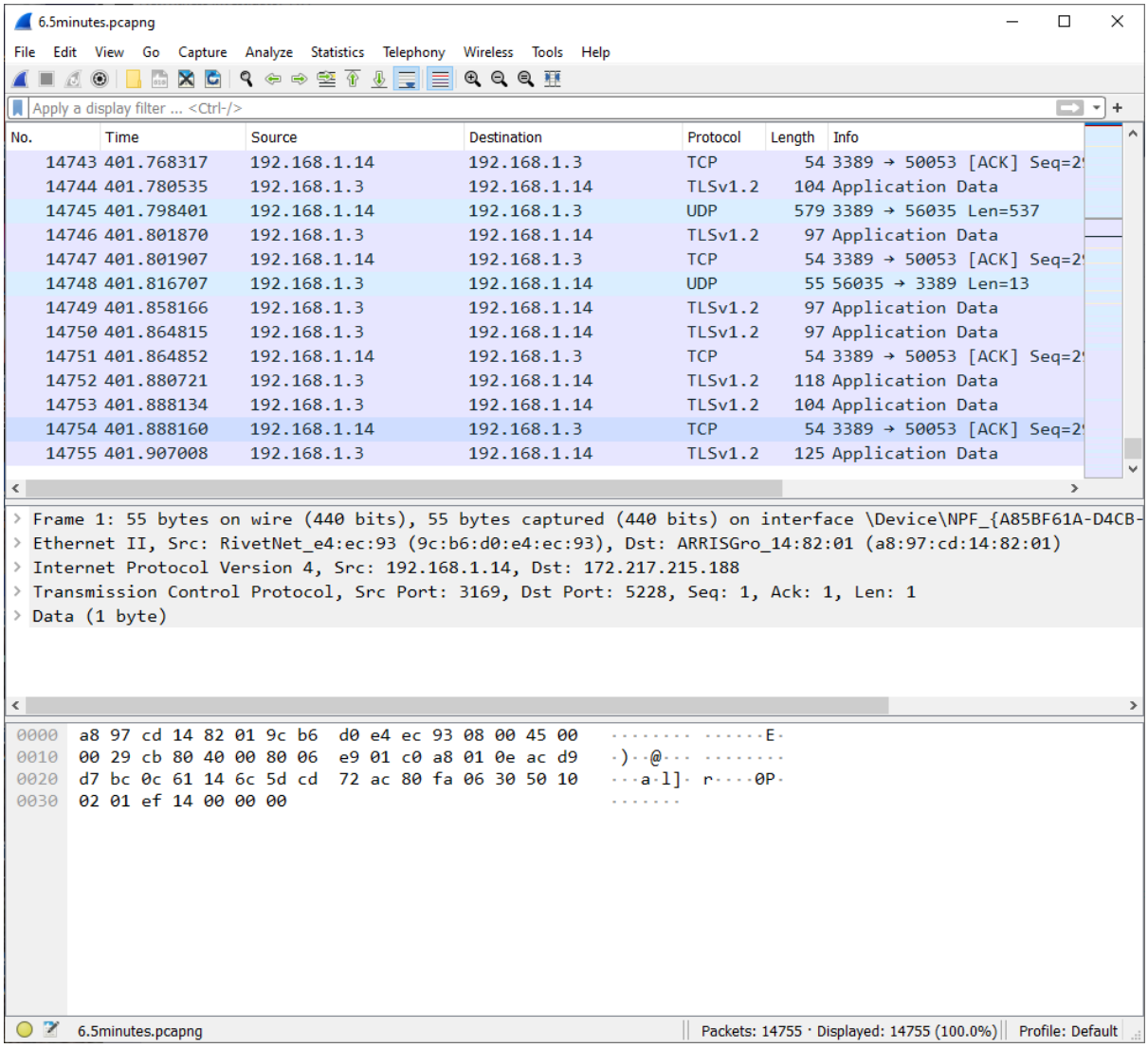

Figure 3: Capture for 6.5 minutes

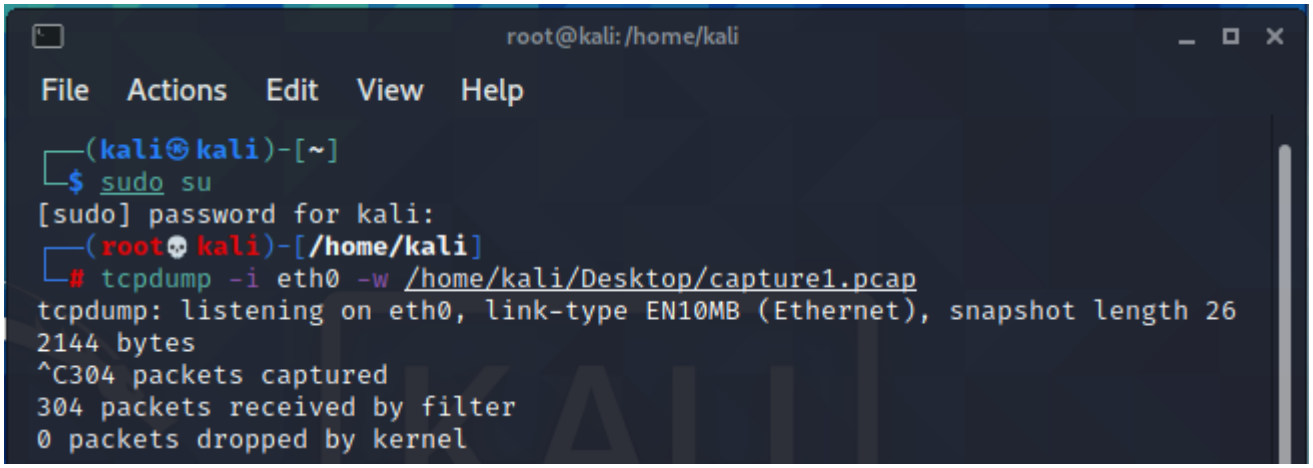

Figure 4: Fast TCPDump session, number of packets is because of a ping flood attack.

Figure 5: Netwitness summary of 2 minute scan.

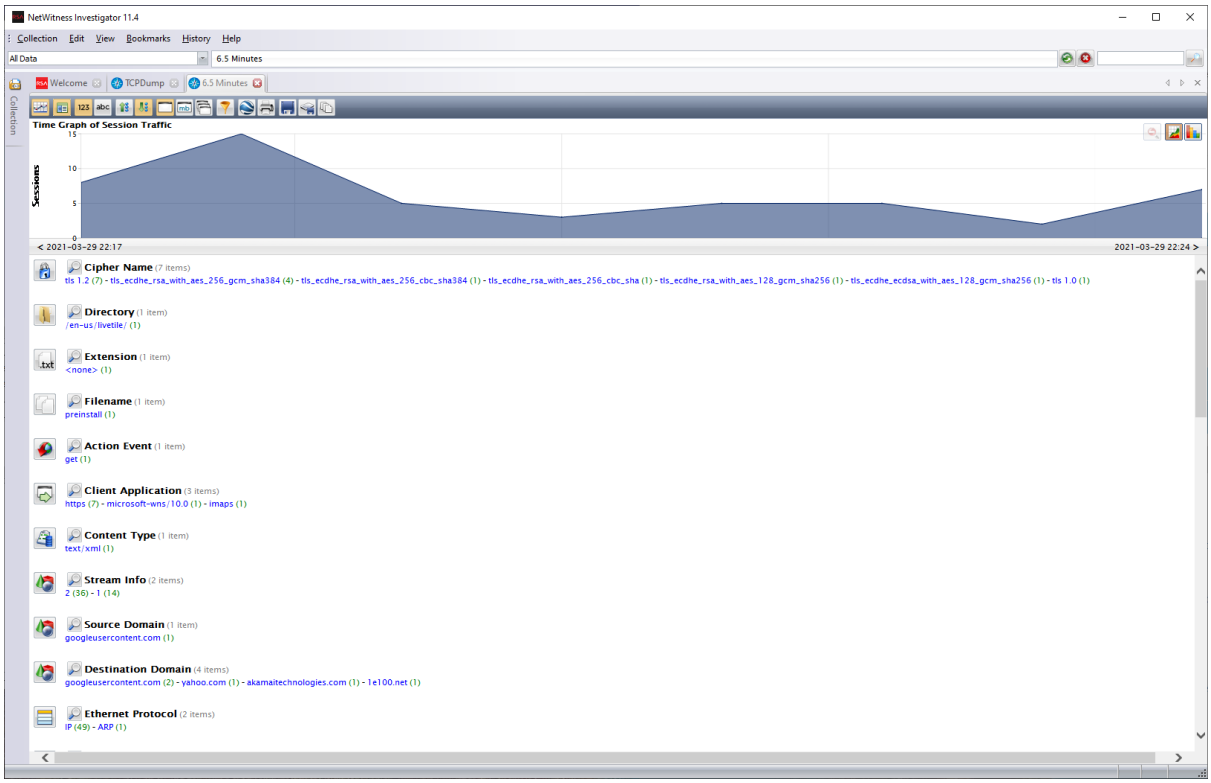

Figure 6: Netwitness summary of 6.5 minute scan

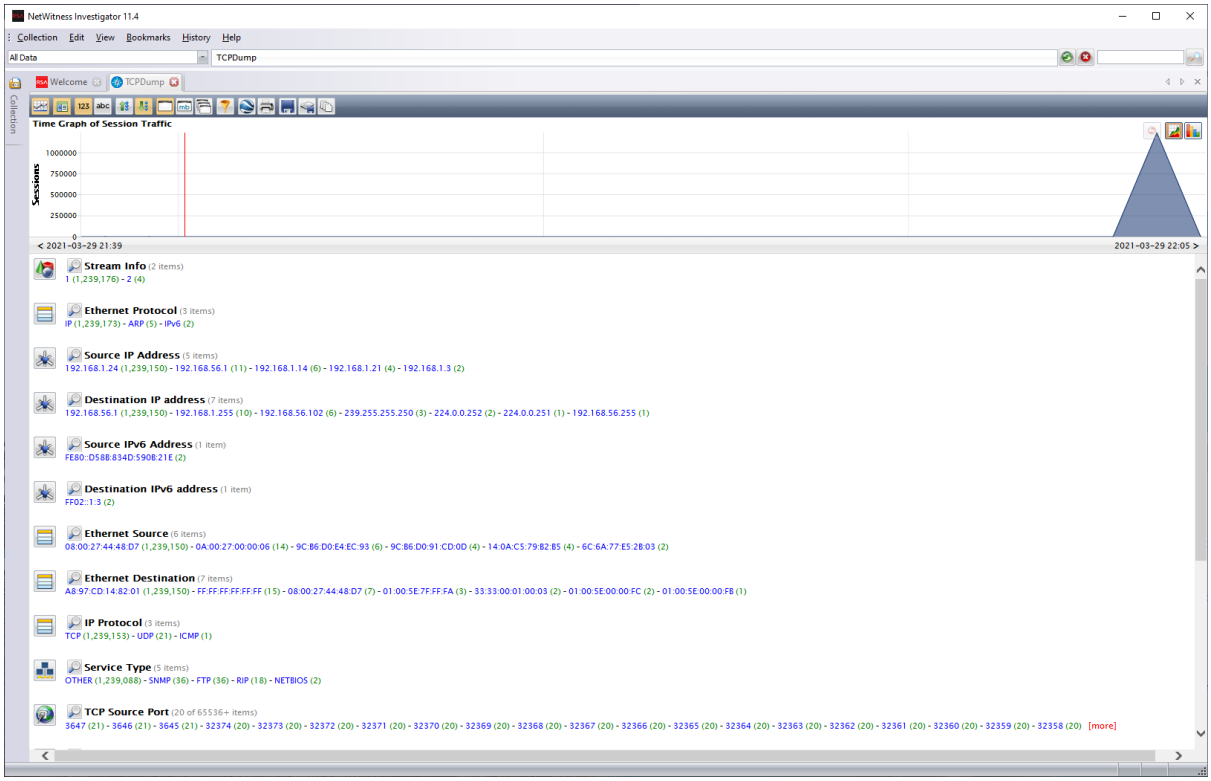

Figure 7: NetWitness summary of TCPDump.

The graph at the top shows a large spike in network traffic. Before the spike there are virtually no packets transferred, however during the spike there were almost 1.25 million packets transferred.

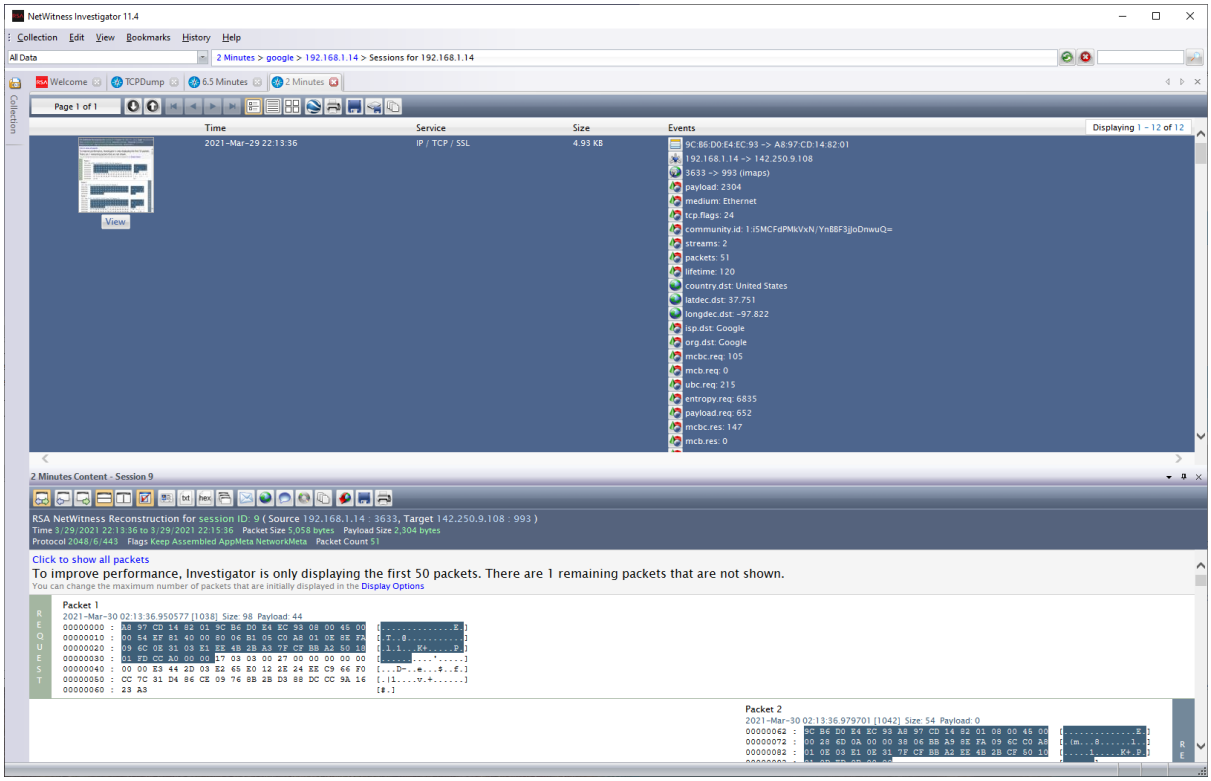

Figure 8: NetWitness also allows us to drill down into categories and view individual packet data.

In this lab i learned how to use Wireshark on Windows machines and TCPDump on Kali Linux to capture network traffic. Wireshark has filtering options available in the application but i chose to explore the NetWitness Investigator application. NetWitness categories packets much more thn Wireshark does. NetWitness gives consolidated lists of IP addresses that generate the most traffic. As seen in figure 7 the timeline is also an important tool to find times of large network traffic, or in this case, to view the packets in a ping flood attack.