**Report for Lab 11: Network Analysis**

Lu Lin, Columbus State University

As we know, in the field of network administration, packet capture (pcap) is used for capturing network traffic. In this lab, the goal of the first step is to use tcpdump on the remote computer to capture network traffic. Then the captured traffic can be copied for analysis.

1. Capture traffic with tcpdump

tcpdump is a command line packet analyzer. When get connected, I run the commands as in the lab instructions to start capturing traffic with tcpdump, the commands capture all traffic and write it to a file named testdump.pcap that is compatible with Wireshark. Figure 1 is the screenshot when stop the running tcpdump, the capture size is 262144 bytes and 570 packets received:

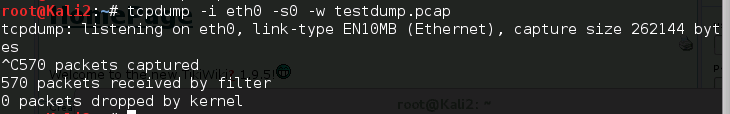


Figure 1. the end of part 1

1. Analyzing Traffic with Wireshark

Wireshark is easier to use than tcpdump, it is capable of extracting files which were downloaded and captured. Wireshark and tcpdump work well together, as in the lab instructions, with some simple command lines, the captured session exported by tcpdump can be analyzed in Wireshark as follows:

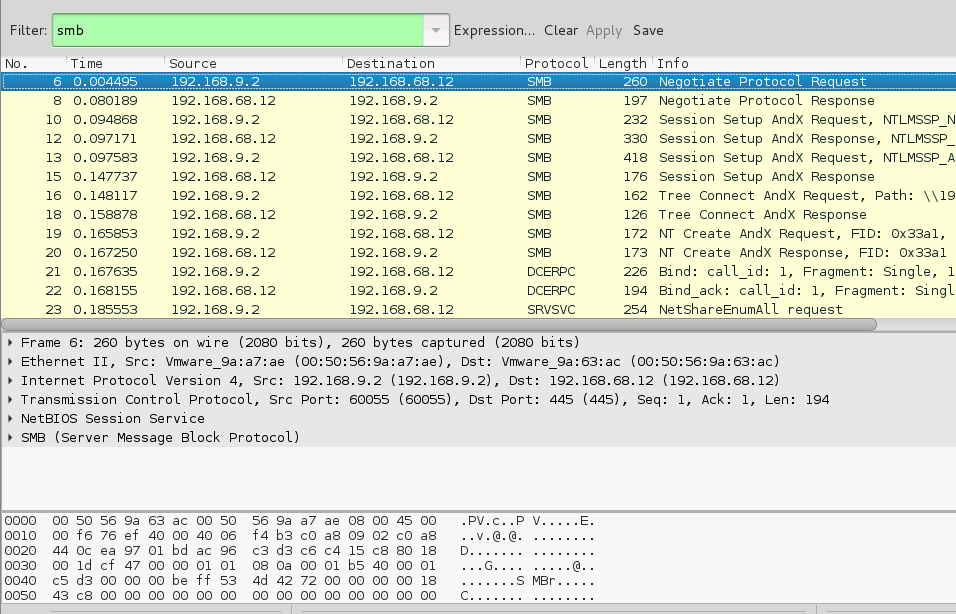


Figure 2. Screenshot of SMB traffic only

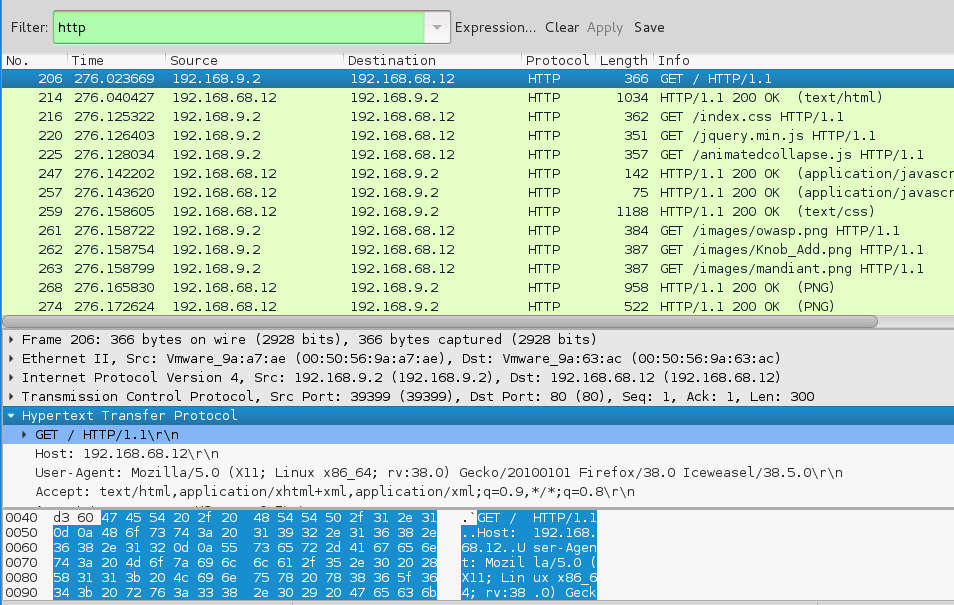


Figure 3. Screenshot of a GET packet from HTTP traffic

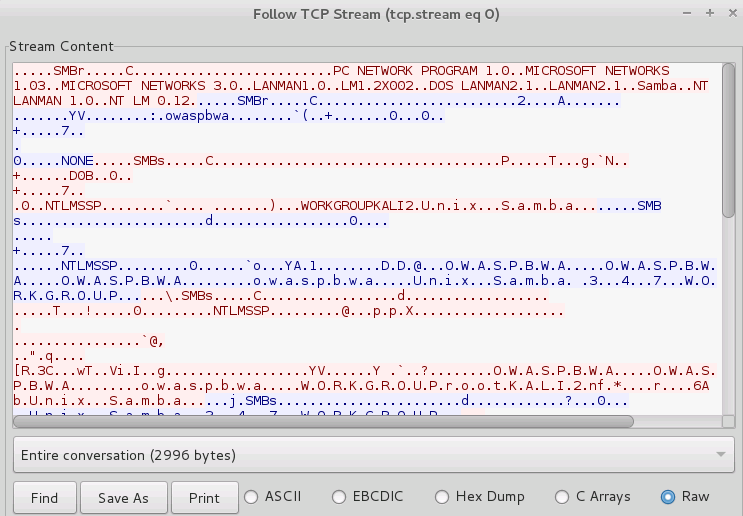


Figure 4. Follow TCP Stream from start to finish given the first TCP connection

1. Analyzing Traffic with Xplico

Xplico is an open source Network Forensic Analysis Tool (NFAT), Xplico isn't a network protocol analyzer, its goal is to extract all application data content from a network capture (i.e. pcap file). Following the lab instructions, Xplico extracts an image in the *dig* directory and *ARP* messages in the *arp* directory.

Figure 5. Files and directories in xdecode directory