# CIT 430/530 – Forensic Activity #1.9 - Wireshark Review

## Introduction

In the provided capture, answer the following questions related to normal network communications. Based on the capture and your analysis, you should be able to write-up a brief, but descriptive brief analysis of what happened. In other words, you are to put into words what the device being analyzed actually did. Your explanation should include pertinent information from the capture. For example, it should include frame numbers, protocols used, IP addresses, traffic flow, etc.

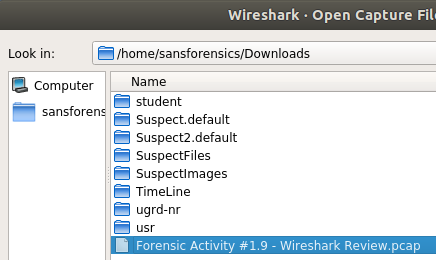
|  |  |
| --- | --- |
| Analyzed Device Info | |
| Platform | Linux |
| Device Name | Host1 |
| Background | New desktop for recently hired staff member |

## Getting Started

From the terminal, open Wireshark with the following command.

**# sudo wireshark**

In Wireshark, select File, then Open and navigate to the .pcap file downloaded from Canvas.



### Initial Communication

***Note: Use a filter of 'bootp' to see DHCP frames***

1. What is Host1’s IPv4 address **after** connecting to the network and obtaining an IPv4 address from the DHCP server?
   * 10.2.56.12
2. What is Host1’s MAC address?
   * 

### Secure Transmissions

Host1 securely communicated with the organizations local server, kosh.nku.edu. After providing the proper credentials, the user of Host1 was able to download a document from the server. Answer the following questions based on the information from the capture.

1. What secure TCP/IP layer 5 protocol was used to connect to this server?
   * ssh
2. What is the IP address of the server Host1 accessed?
   * 172.31.108.200
3. What frames show Host1 ending the session to the server?
   * 110,111,112,113  
     ***Note: A Google search of "TCP/IP connection termination sequence" can be helpful***
4. Do you see any evidence of the file downloaded to Host1 from the server? If so, what frame(s)? If not, why do you think this is?
   * We cannot know if a file is downloaded due to the encrypted data, all we can see is a lot of communication between the two address, it could be possible but we don’t know.

### Internet Communications

During lunch, the user of Host1 went to a common sports website. Answer the following questions based on the information from the capture.

1. What protocol was most likely used when Host1 visited this website?
   * hhtp
2. What website did the user visit?
   * Espn.com
3. What is the destination IP listed in the GET request to the website?
   * 34.204.66.190
4. What frame contains the corresponding GET response back to Host1?
   * 159
5. How did you determine this is the correct frame?
   * By searching for the requested frame in 146, due to the source IP
   * Table

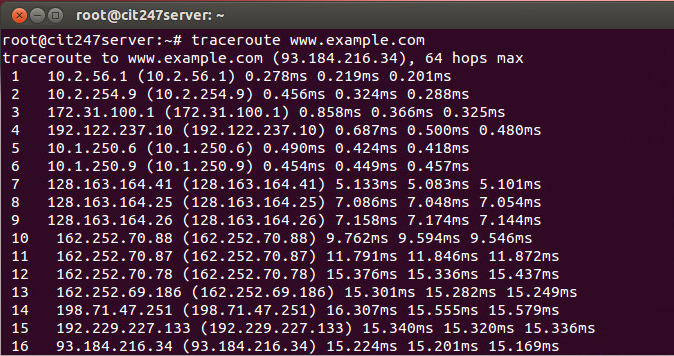
     Description automatically generated

### Network Connectivity Test

At one-point the user at Host1 wanted to see the path to the website [www.example.com](http://www.example.com). The following image shows the output from the traceroute command. ***Note: If you are unfamiliar with traceroute, use the following links*.**

* [Linux traceroute command](https://www.computerhope.com/unix/utracero.htm) - *Computer Hope*
* [Traceroute Linux command / Unix Command](https://www.lifewire.com/traceroute-linux-command-4092586) – *Lifewire*

Based on the image and Wireshark capture, answer the following questions.



1. What protocol needs to be supplied in the filter textbox to see the frames captured while traceroute ran?
   * icmp
2. What is the range of these frames in Wireshark?
   * 3708-3803
3. Why are there more frames in the capture file than what is listed as traceroute output?
4. These are the actual packets used in the traceroute command. Each icmp will send a ping request 3 times to whoever their neighbor is and so on. Wireshark has 95 more packets because it is capturing the time to live value of 1,2,3 and zero.
5. How many networks (i.e. default gateway devices) are seen before finally reaching [www.example.com](http://www.example.com)?
   * 16