**EXPERIMENT NO-2**

**Aim:** Study of packet sniffer tools like wireshark(ethereal) and tcpdump

**Title:** Study and use various commands and interface of wireshark(ethereal) and tcpdump.

**Theory:**

**Wireshark:**

Wireshark is a free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues.

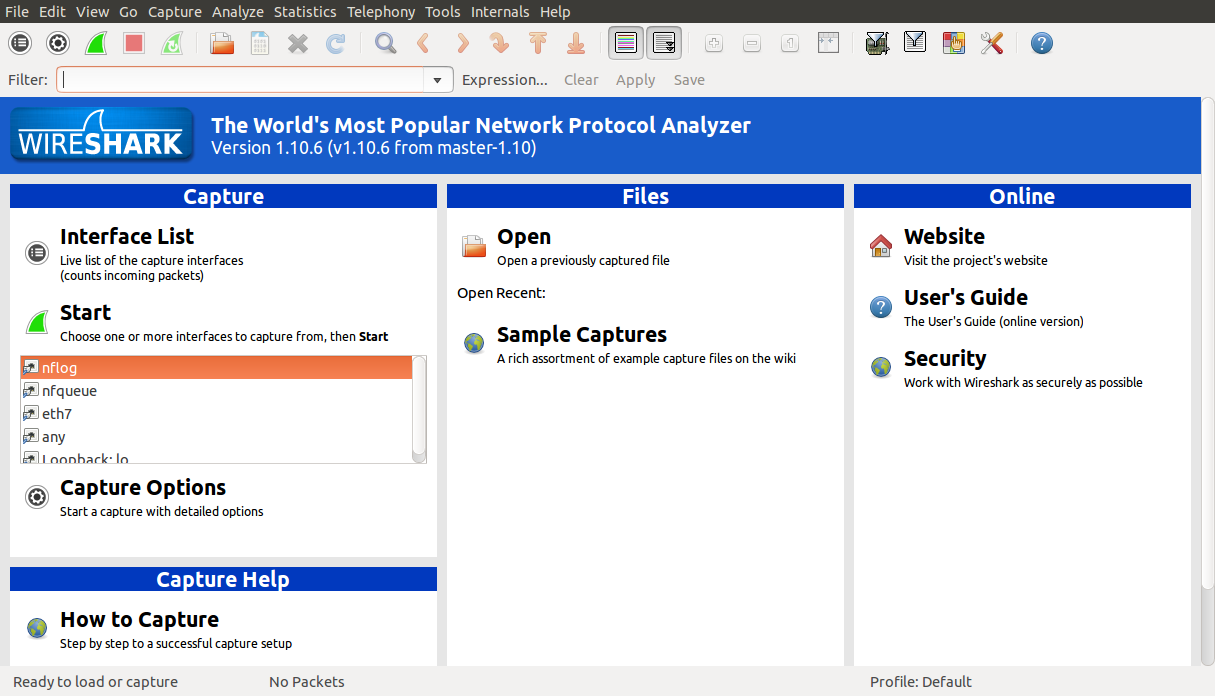
Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets; it runs on Linux, OS X, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows. There is also a terminal-based (non-GUI) version called TShark. Wireshark, and the other programs distributed with it such as TShark, are free software, released under the terms of the GNU General Public License.

**Features:**

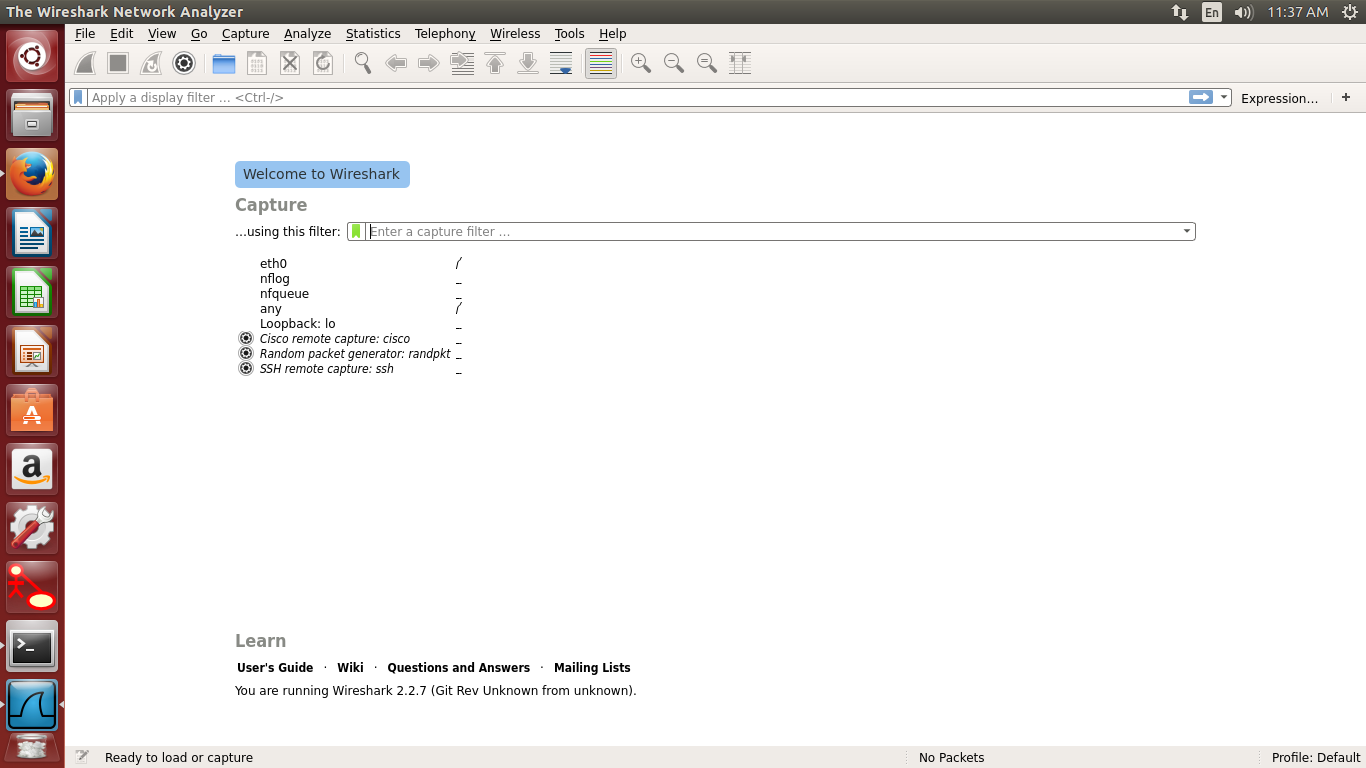
* Data can be captured "from the wire" from a live network connection or read from a file of already-captured packets.
* Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, TShark.
* Data display can be refined using a display filter.
* Plug-ins can be created for dissecting new protocols.
* Raw USB traffic can be captured.
* Wireless connections can also be filtered as long as they transverse the monitored Ethernet.
* Various settings, timers, and filters can be set that ensure only triggered traffic appear.

**Capturing packets**

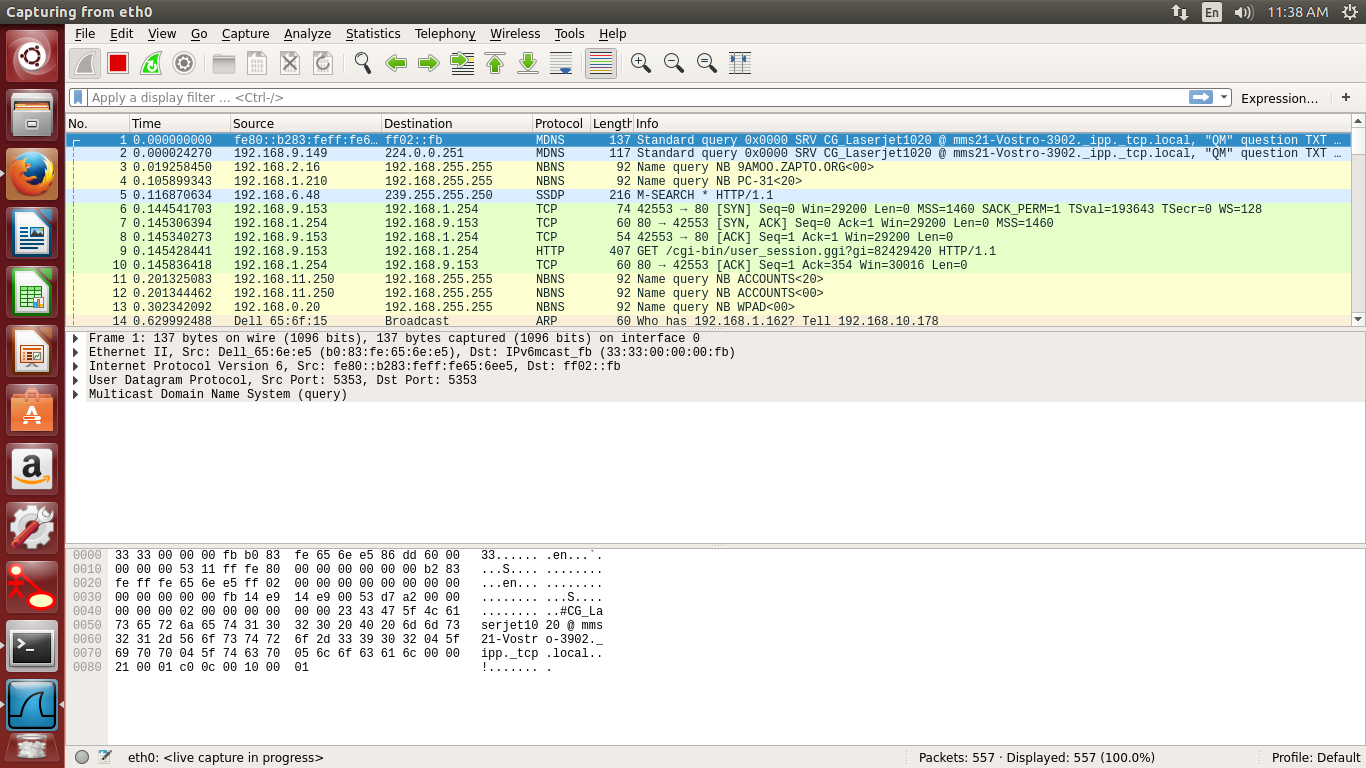
Step 1:



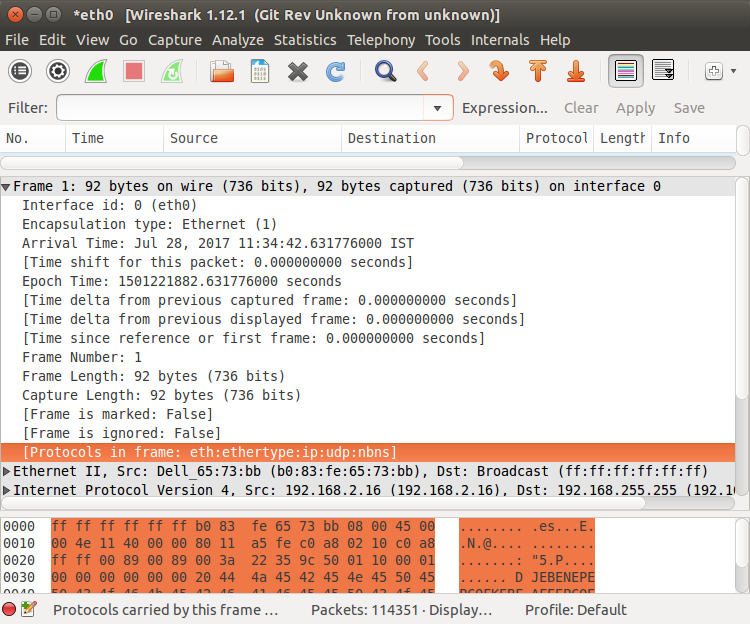
Step 2 :



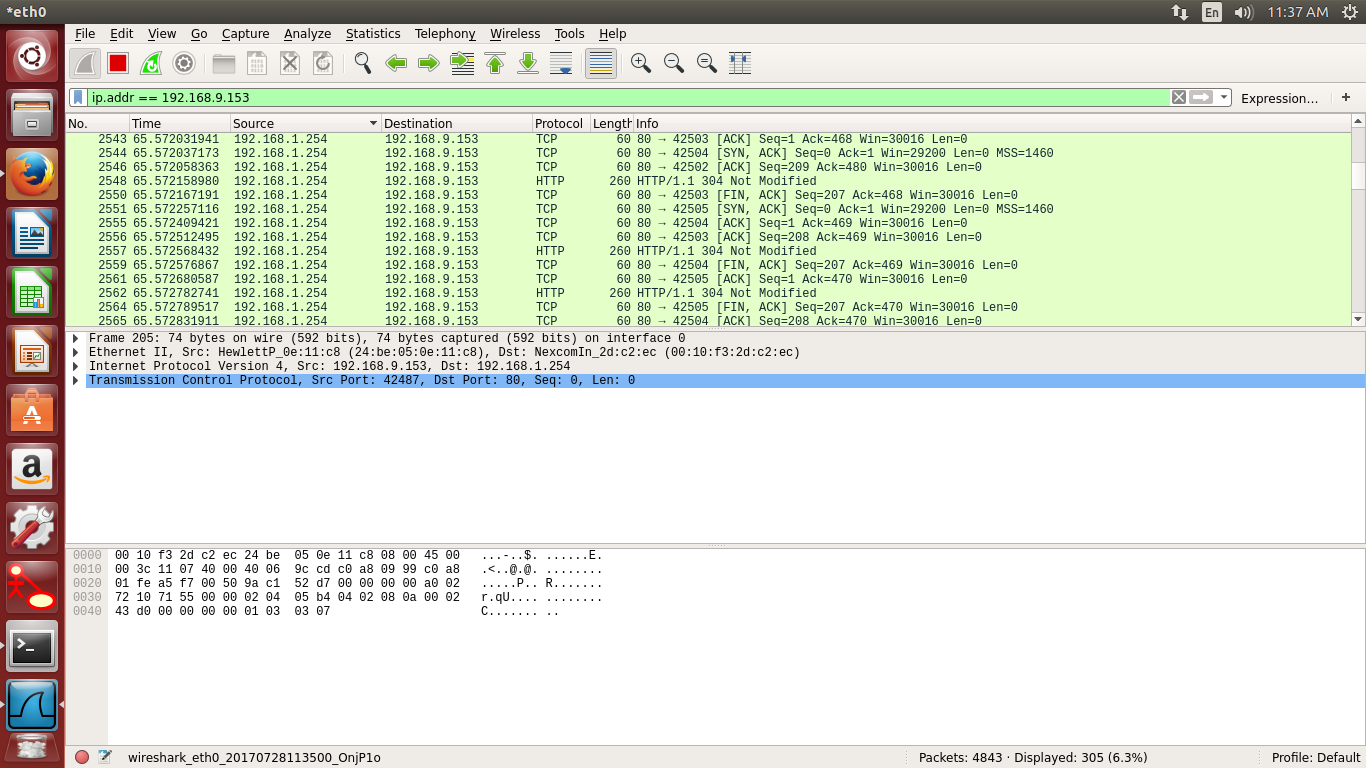
Step 3 :



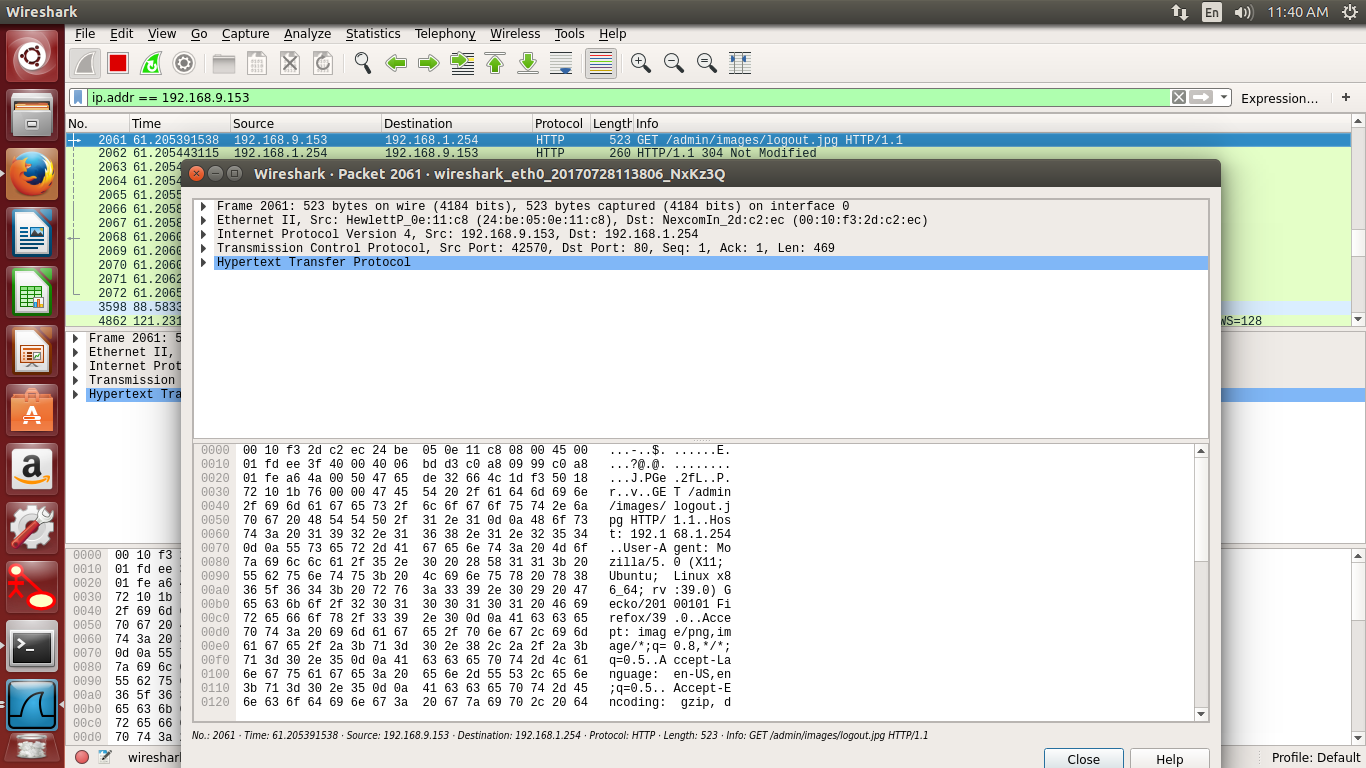
**Click the stop capture button when you want to stop capturing tarffic**



**Filtering packets**



**Inspecting Packets**



**tcpdump**

**Theory :**

tcpdump is a common packet analyzer that runs under the command line. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. Distributed under the BSD license, tcpdump is free software.

Tcpdump works on most Unix-like operating systems: Linux, Solaris, BSD, OS X, HP-UX, Android and AIX among others. In those systems, tcpdump uses the libpcap library to capture packets. The port of tcpdump for Windows is called WinDump; it uses WinPcap, the Windows port of libpcap.

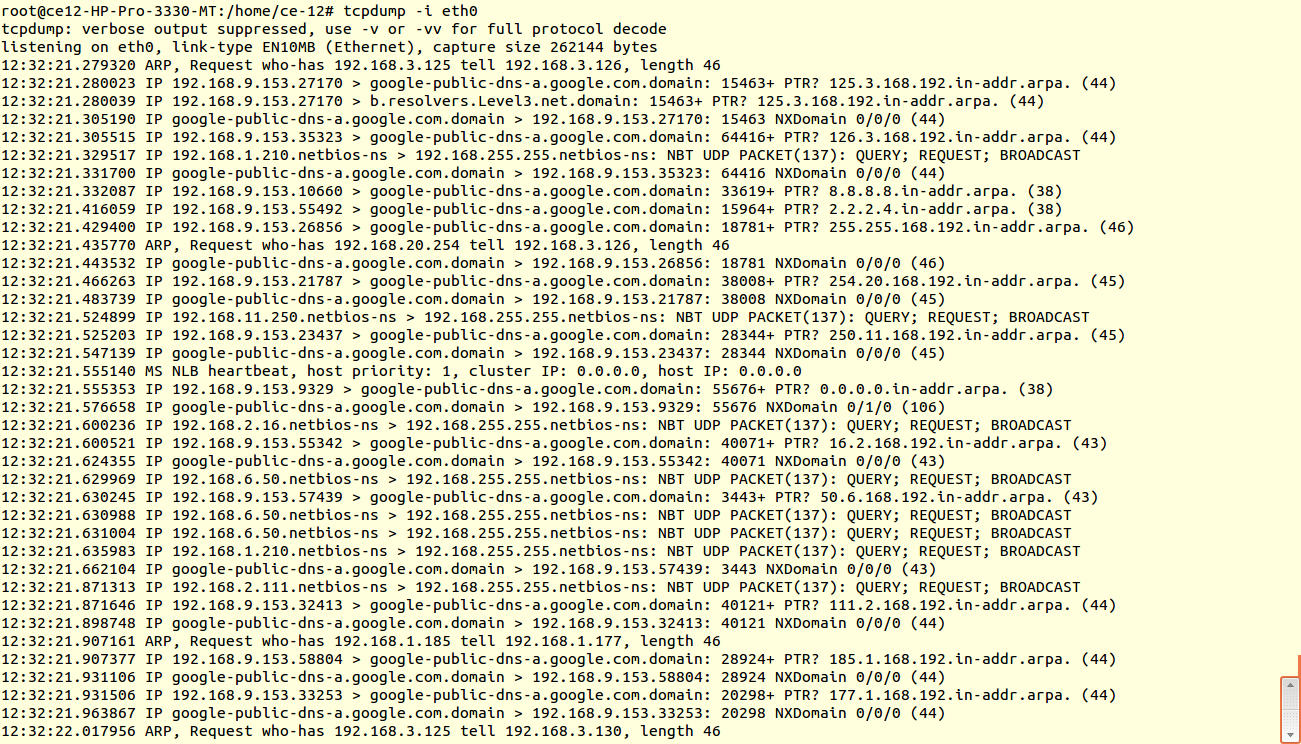
**Tcpdump commands:**

1. **Capture Packets from Specific Interface**

The command screen will scroll up until you interrupt and when we execute tcpdump command it will capture from all the interfaces, however with -i switch only capture from desire interface.

**Command:** **tcpdump -i eth0**

**Output:**

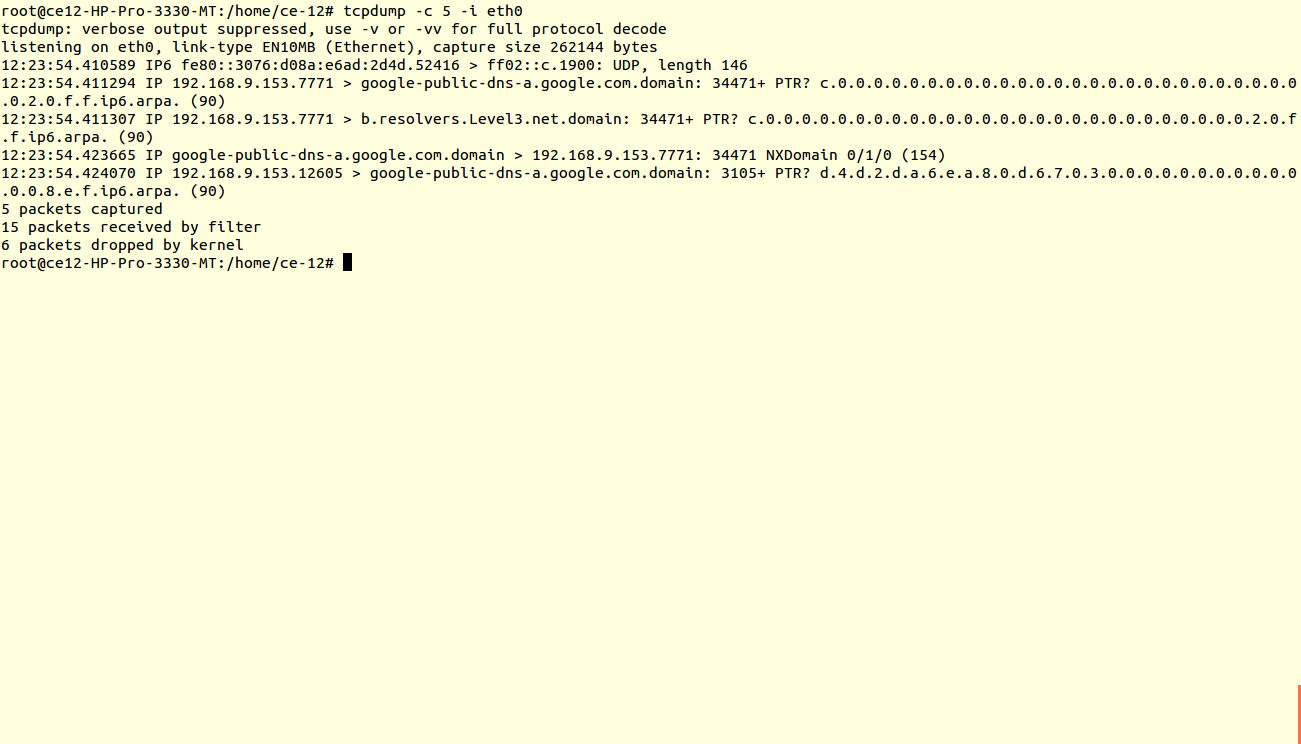


1. **Capture Only N Number of Packets**

When you run tcpdump command it will capture all the packets for specified interface, until you Hit cancel button. But using -c option, you can capture specified number of packets. The below example will only capture 6 packets.

**Command: tcpdump -c 5 -i eth0**

**OutPut:**

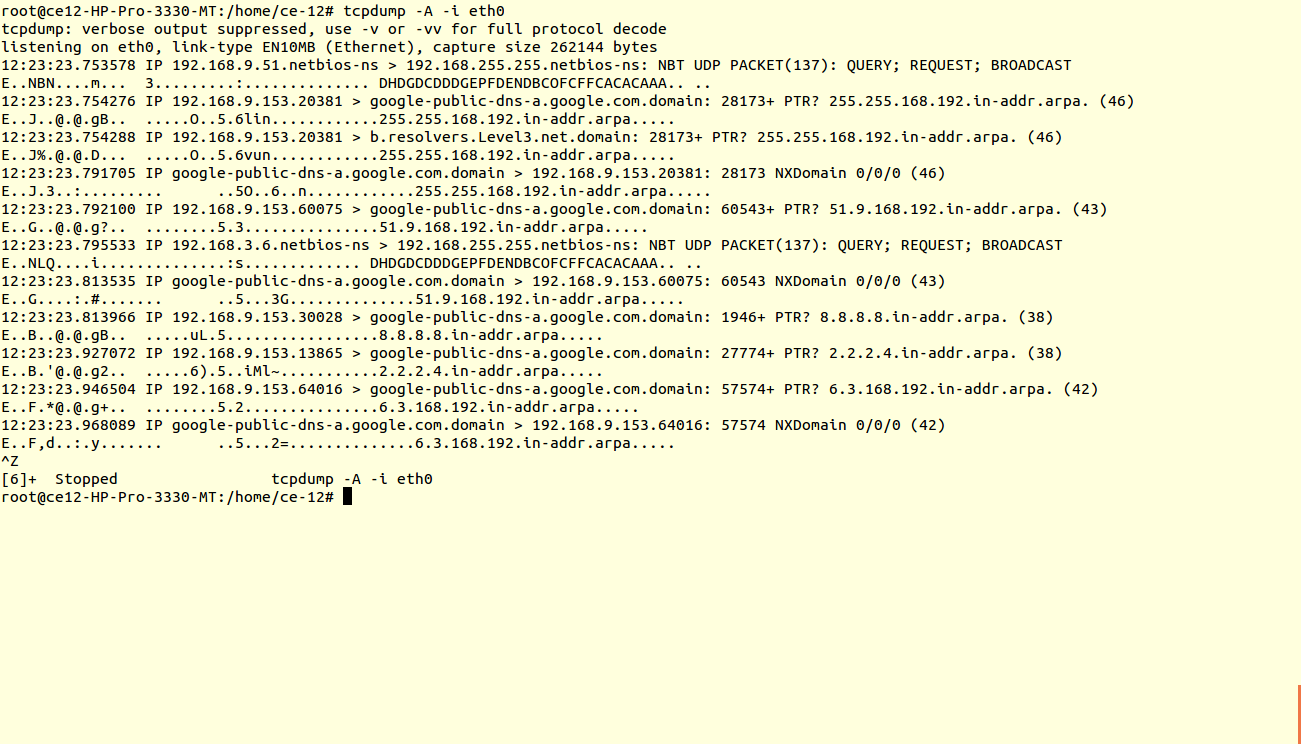


1. **Print Captured Packets in ASCII**

The below tcpdump command with option -A displays the package in ASCII format. It is a character-encoding scheme format.

**Command: tcpdump -A -i eth0**

**Output:**



1. **Display Available Interfaces**

To list number of available interfaces on the system, run the following command with -D option.

**Command: tcpdump -D**

**Output:**

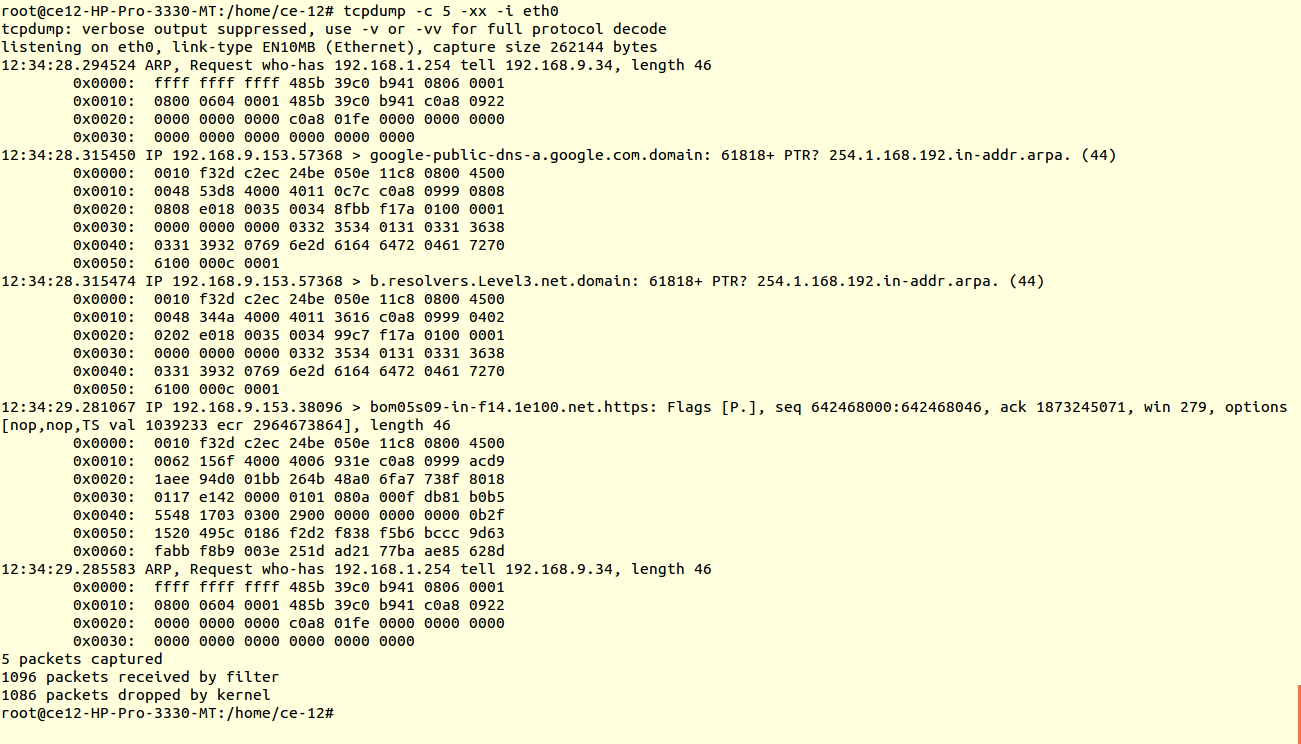


1. **Display Captured Packets in HEX and ASCII**

The following command with option -XX capture the data of each packet, including its link level header in HEX and ASCII format.

**Commands: tcpdump -c 5 -XX -i eth0**

**OutPut:**



**Conclusion:** Thus, we have studied and implemented Wireshark and tcpdump for network analysis.