**GATHERING INFORMATION THROUGH HARVESTER**

**Exp no:6**

Aim:

To demonstrate information gathering using theHarvester.

Procedure:

Step 1:Open Terminal in the kali Linux.

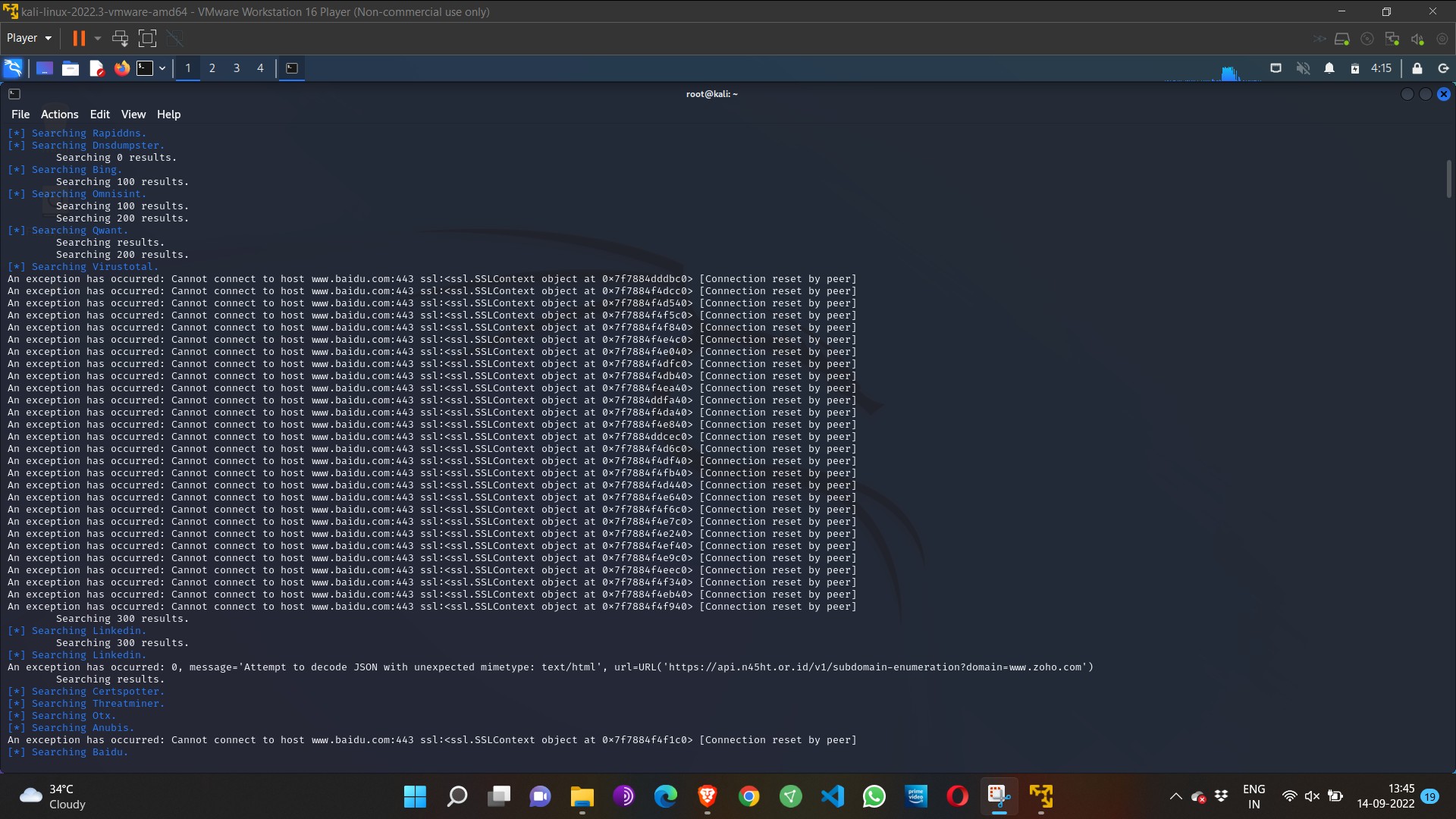
Step 2: Run the following command

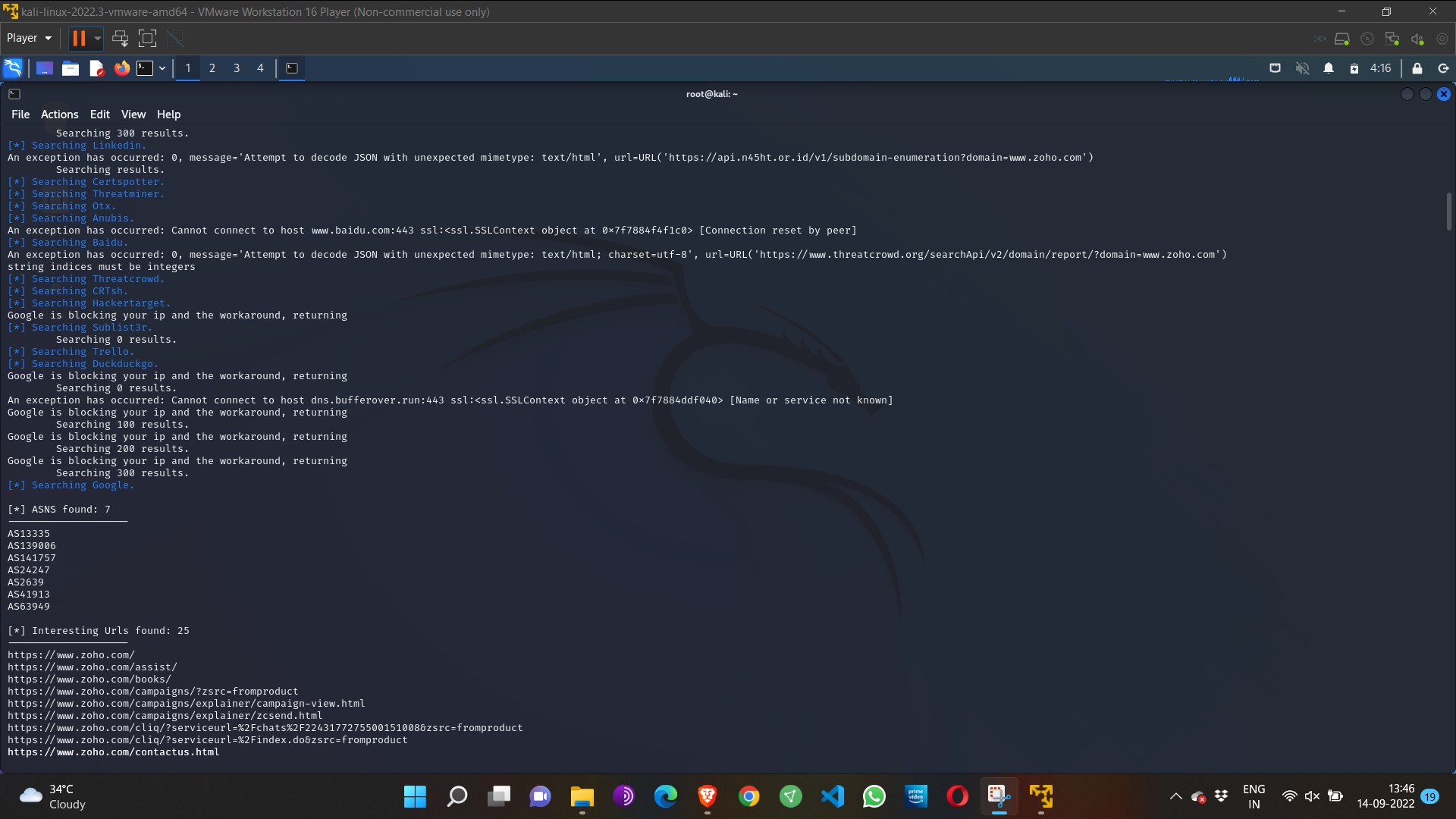
Command: theHarvester -d [www.zoho.com](http://www.zoho.com/) -l 300 -b all

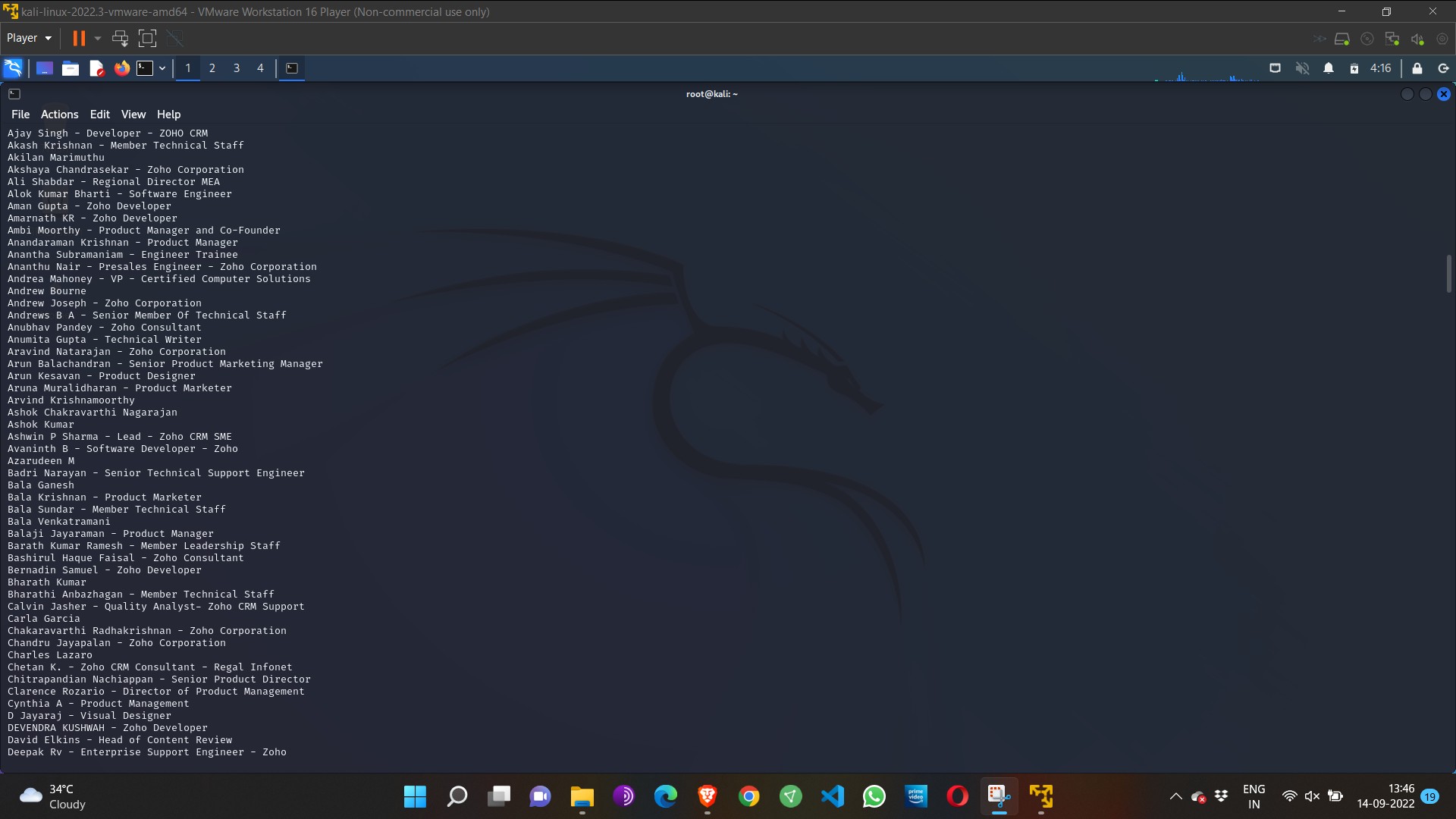
Step 4: run this command “the Harvester -d [www.zoho.com](http://www.zoho.com/) -l 300 -b all -f test” andhit enter to export the result as html file and xml file

Step 5: now close the terminal and navigate the home folder and search for test file.

****

****



Result:

Thus , information has been collected successfully through harvester.

VULNERABILITY ANALYSIS

Exp No: 7

Aim:

To perform vulnerability Analysis using CGI Scanning with Nikto

Procedure:

Step 1: open a terminal window and type nikto –H and press enter

Step 2: Type nikto –h <website> Tuning x and press enter

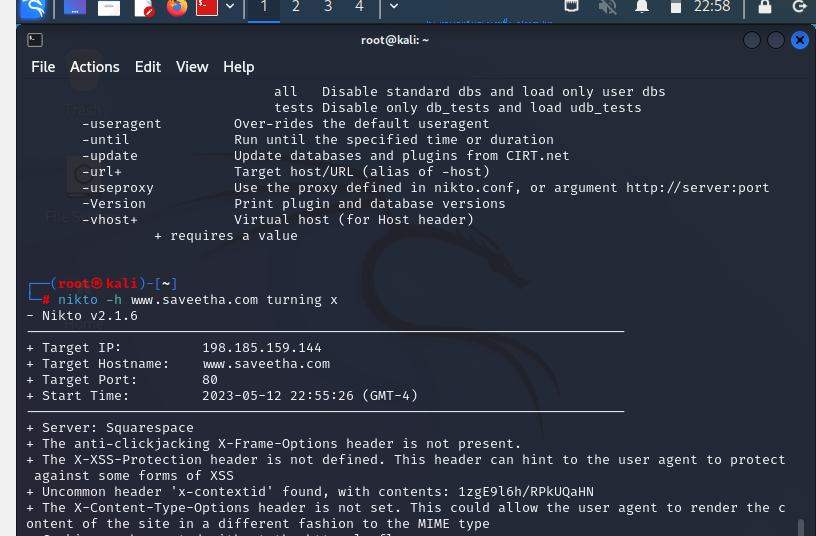
Step 3: Nikto starts web server scanning with all tuning options enabled.

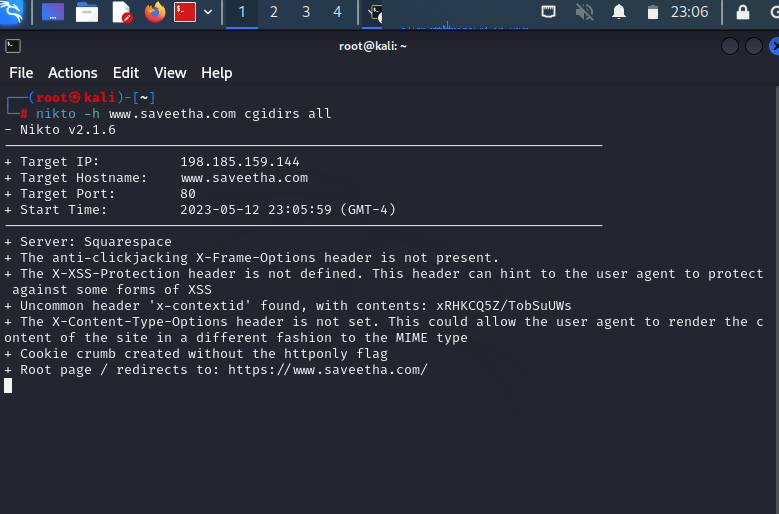
Step4: In the terminal window type “nikto –h <website>-Cgidirs all “and hit enter

Step 5. Nikto will scan the webserver as it looks vulnerable CGI directories. It

scans the webserver and list out the directories

Output:





Result:

Thus, we have completed the vulnerability analysis using nikto.

BASIC COMMANDS IN LINUX

Exp No:8

Aim:

To run the basic commands of Linux in kali Linux.

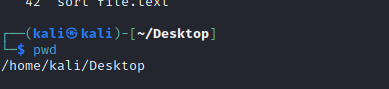
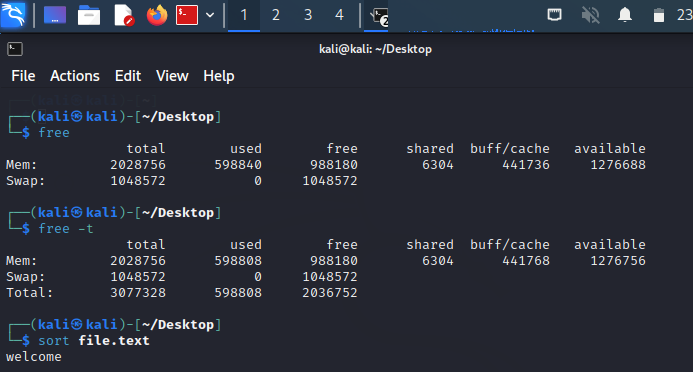
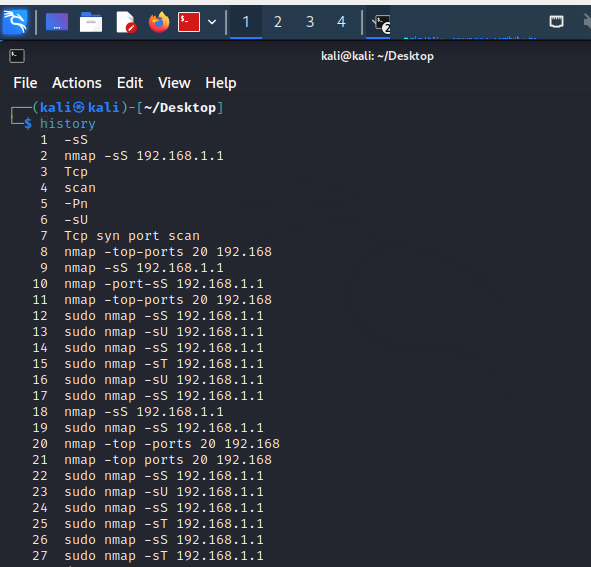
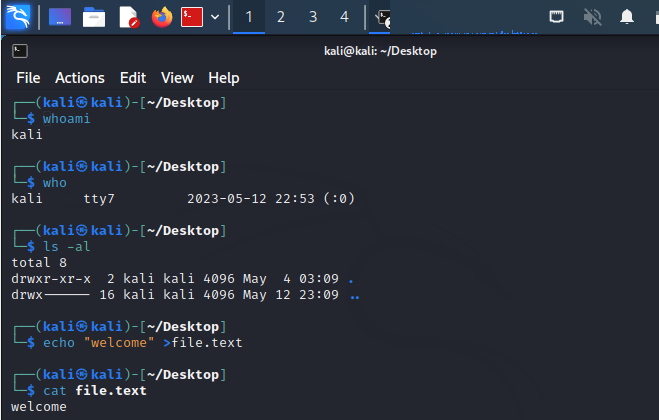
Procedure:

Step 1: Open the kali desktop

Step 2: Run the following basic commands

|  |  |
| --- | --- |
| date | free |
| whoami | free -t |
| who | pwd |
| ls -all | sort |
| history | cat |

Output:



Result:

Hence, we have run the basic commands of Linux successfully.

**PACKET ANALYZER TOOL**

**EX NO: 5**

**Aim:**

To Analyse the network packet transmission using packet analyser tool (Wireshark).

**Procedure:**

1. Capture the packets (TCP / UDP / HTTP)
2. Filter those packets
3. Inspect those packets

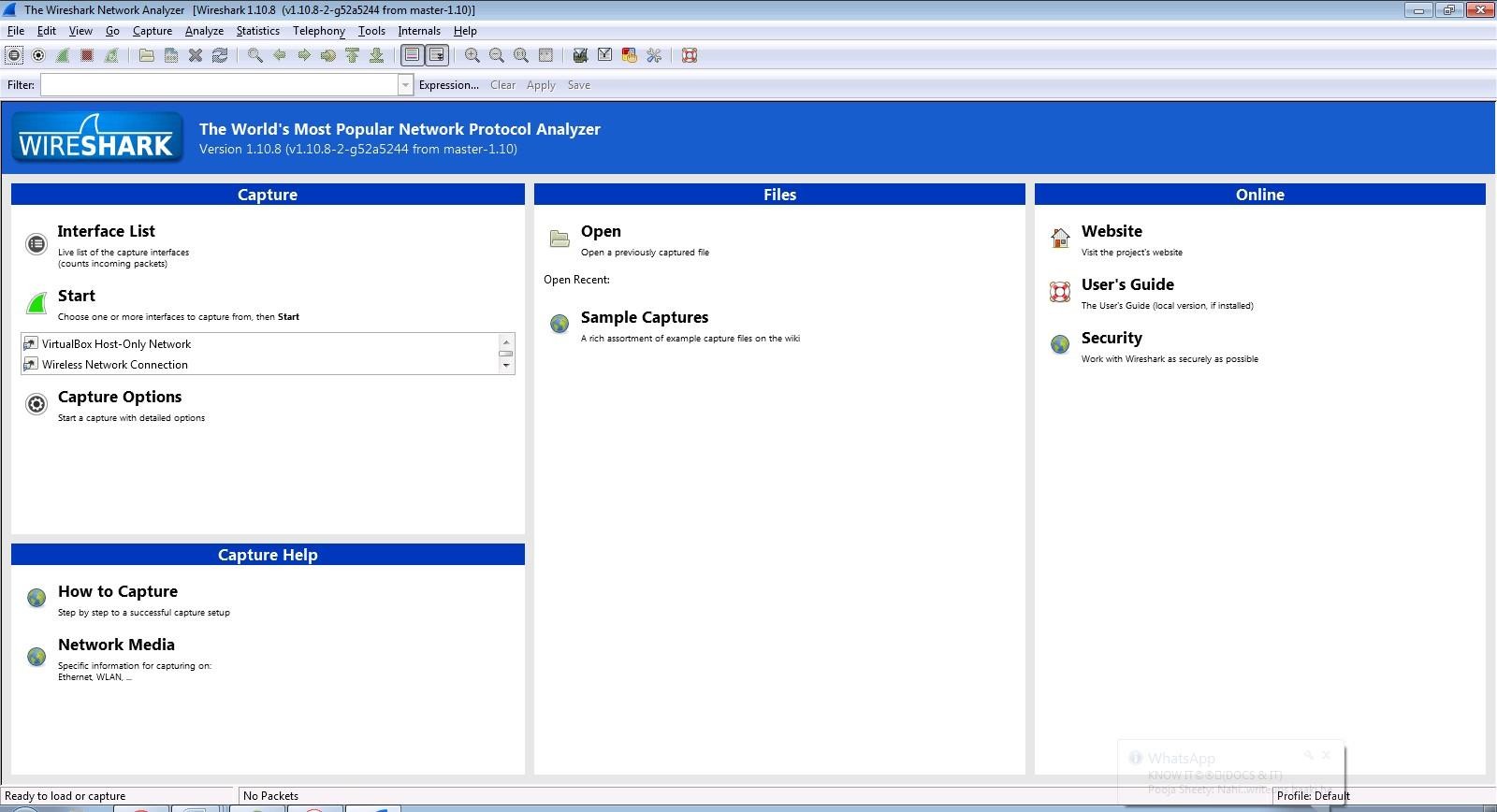
Step 1: Install and open Wireshark.

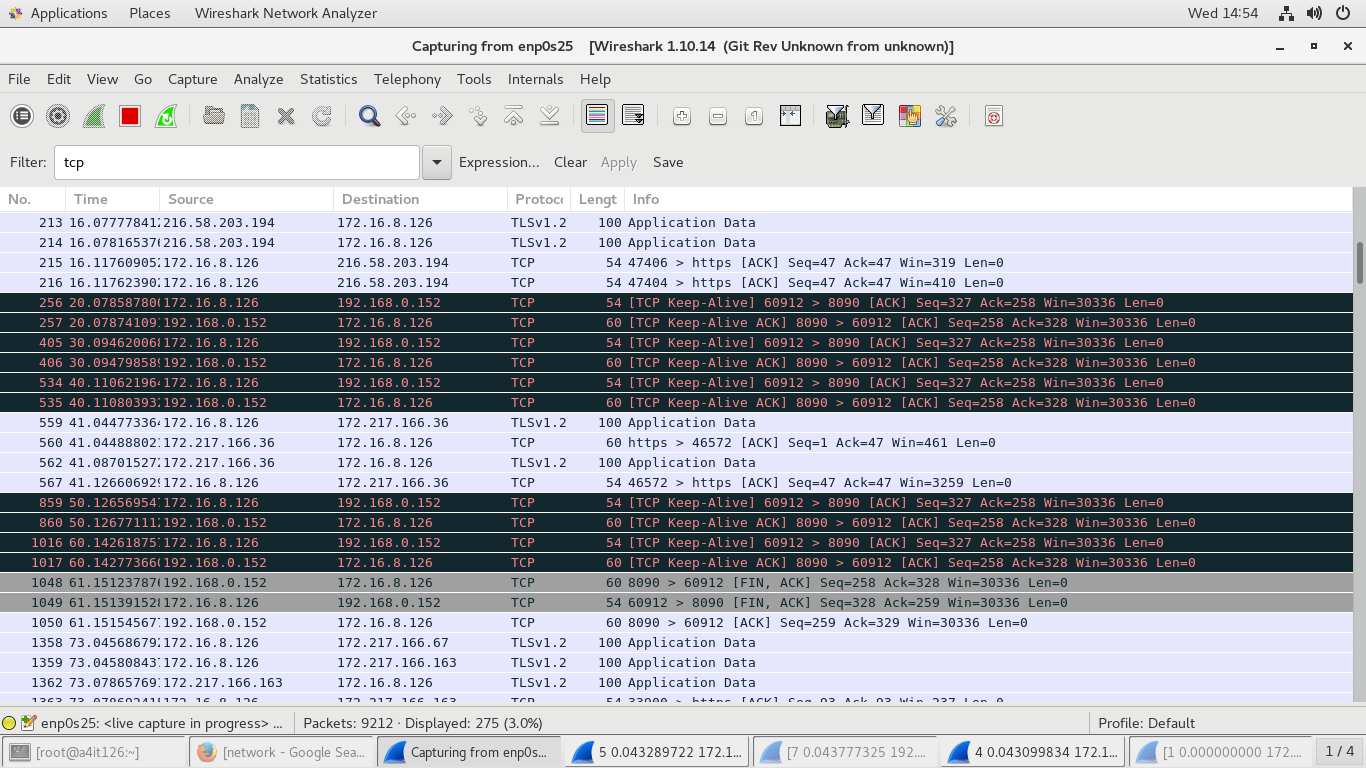
Step 2: To capture TCP / UDP /HTTP Packet.

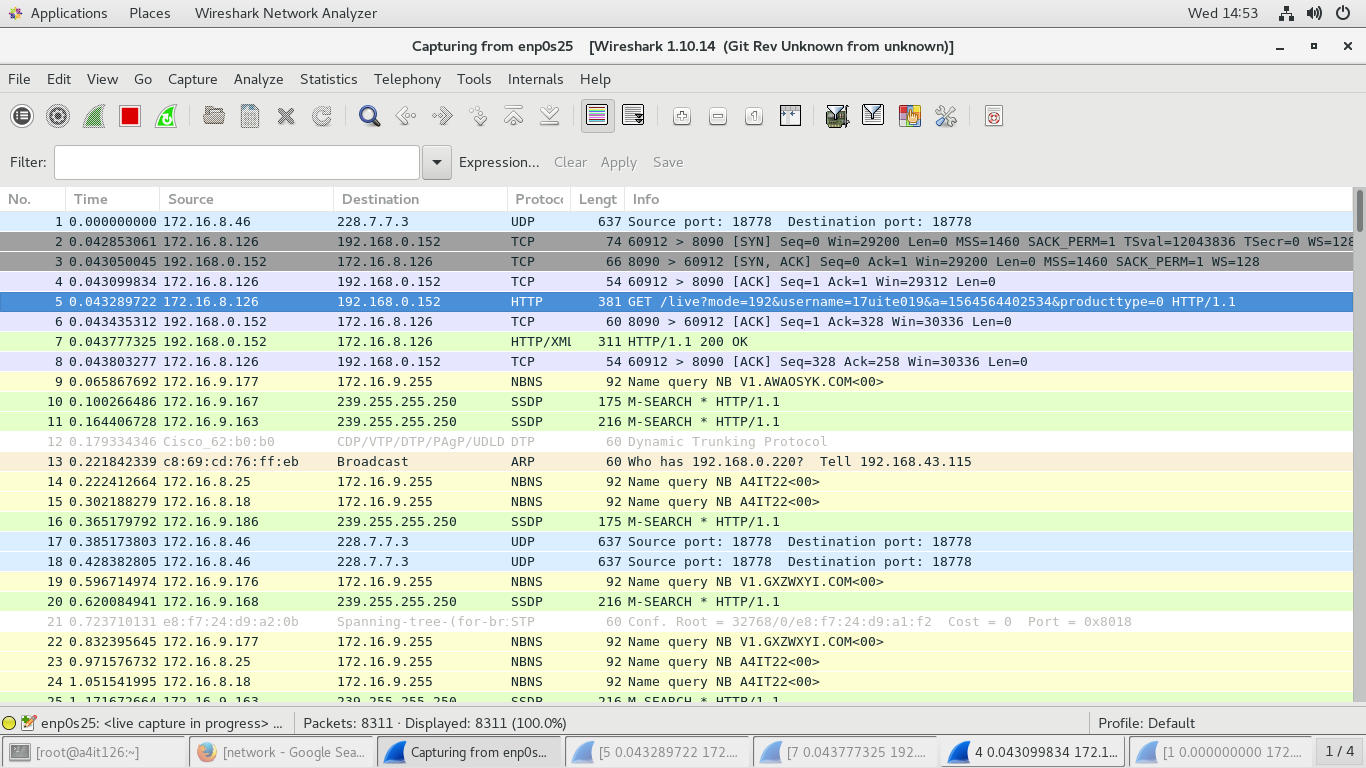
Step 3: to Filter TCP / UDP /HTTP Packet.

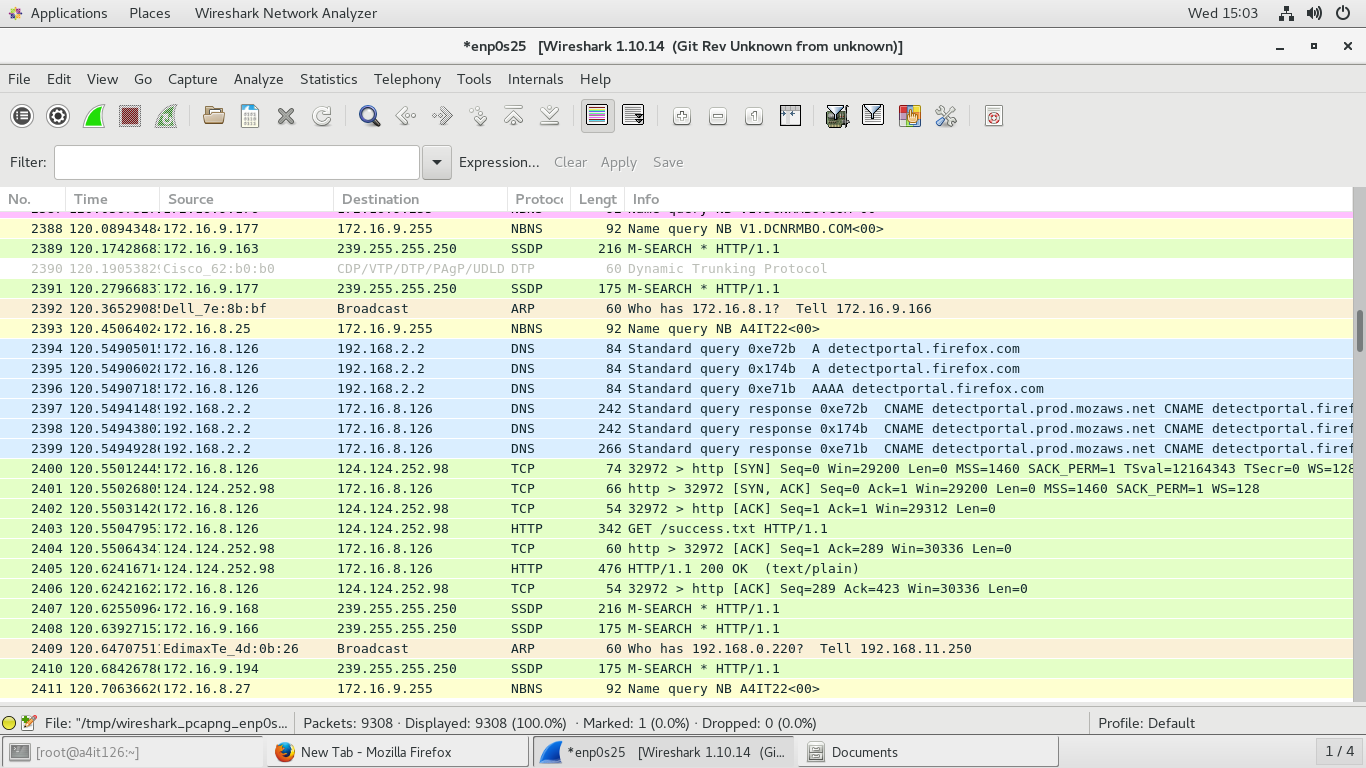
Step4: to inspect the TCP / UDP /HTTP Packet.

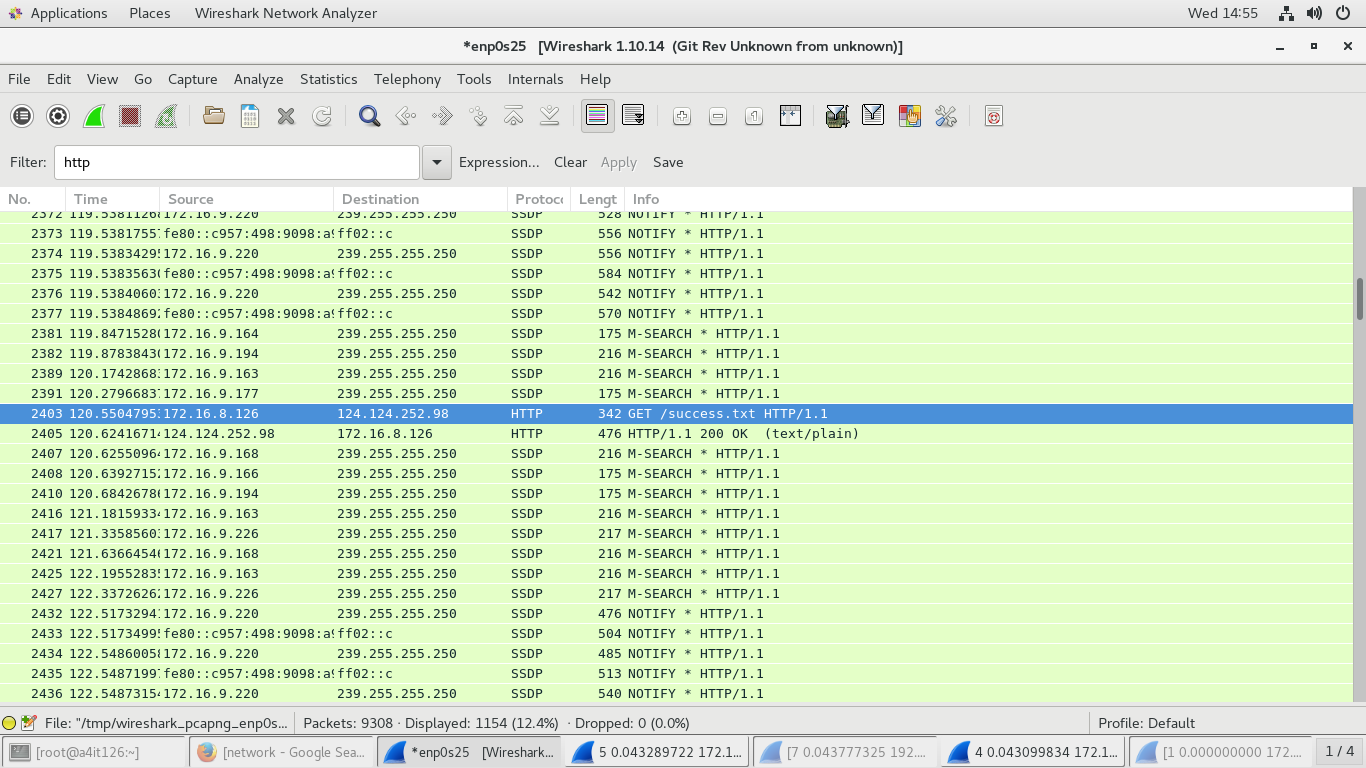
**Output:**

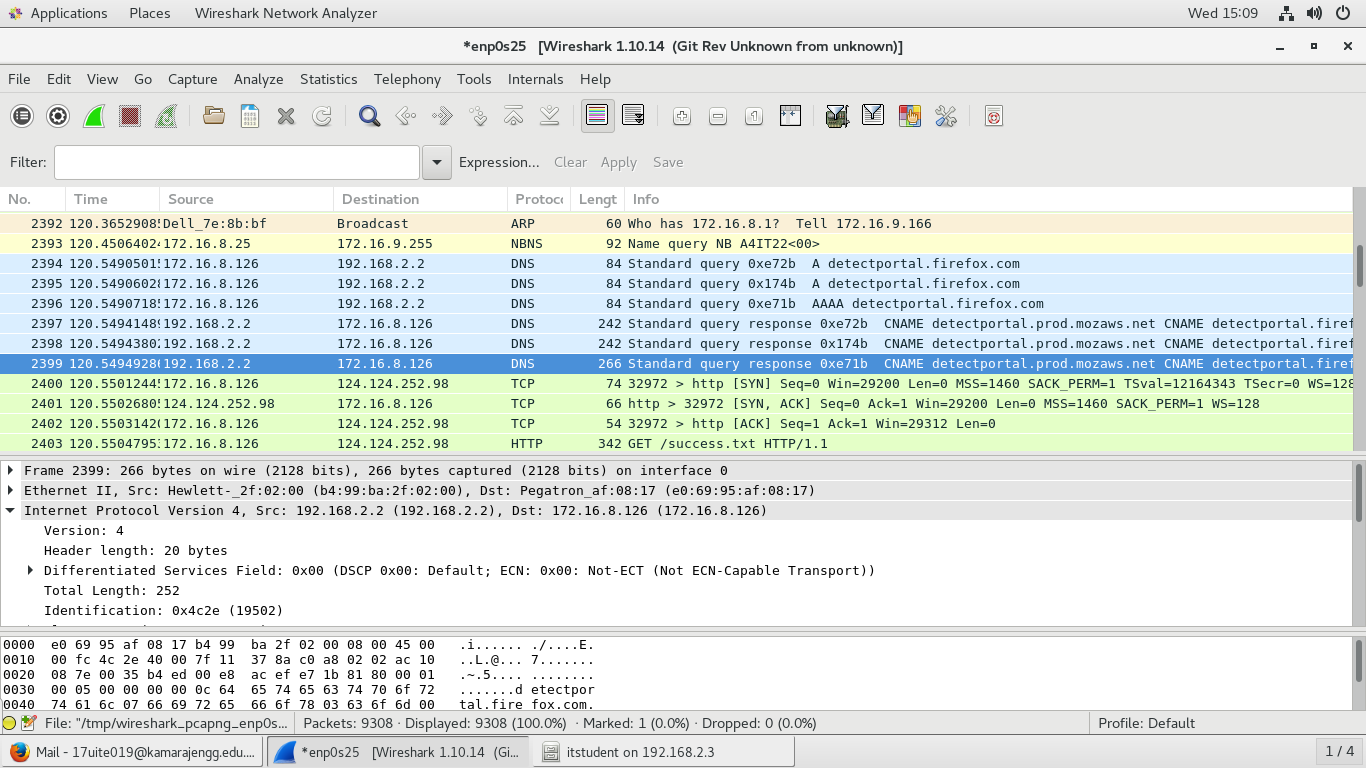
****

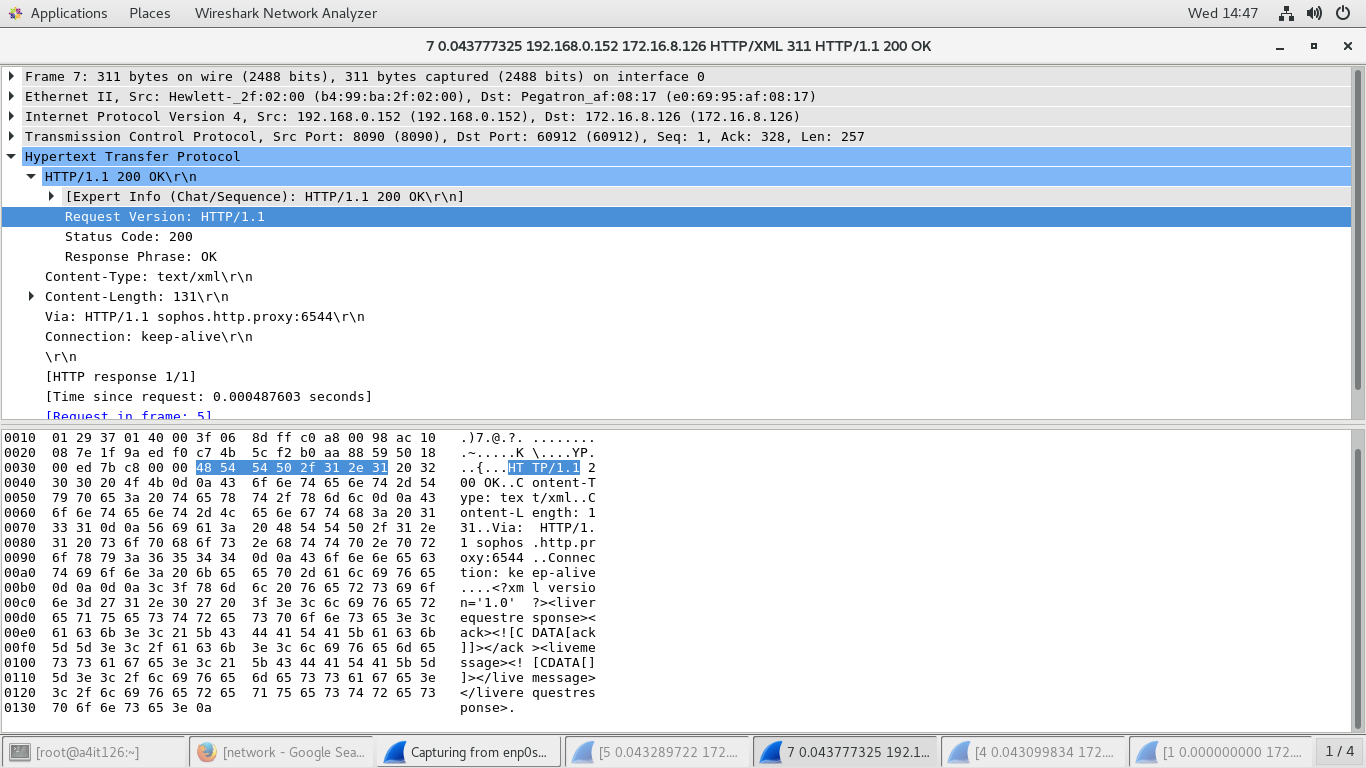


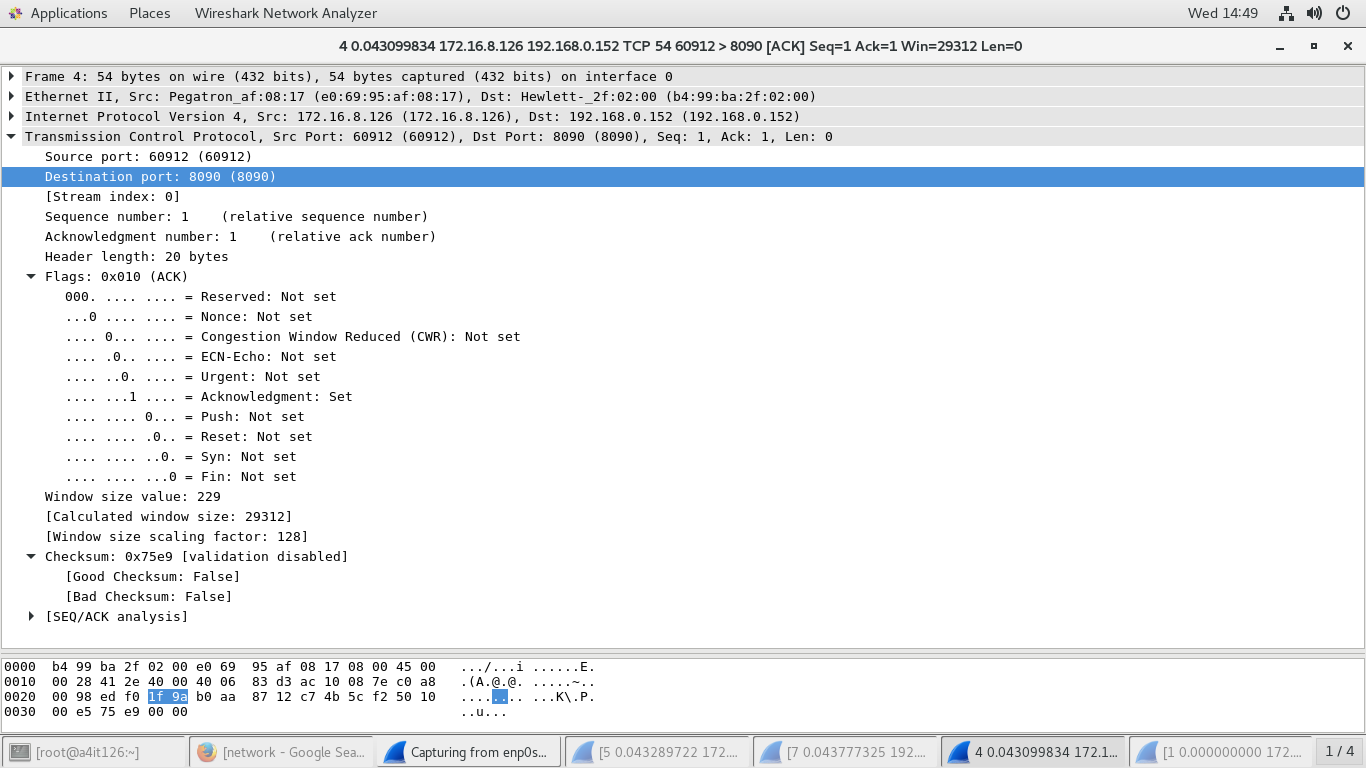


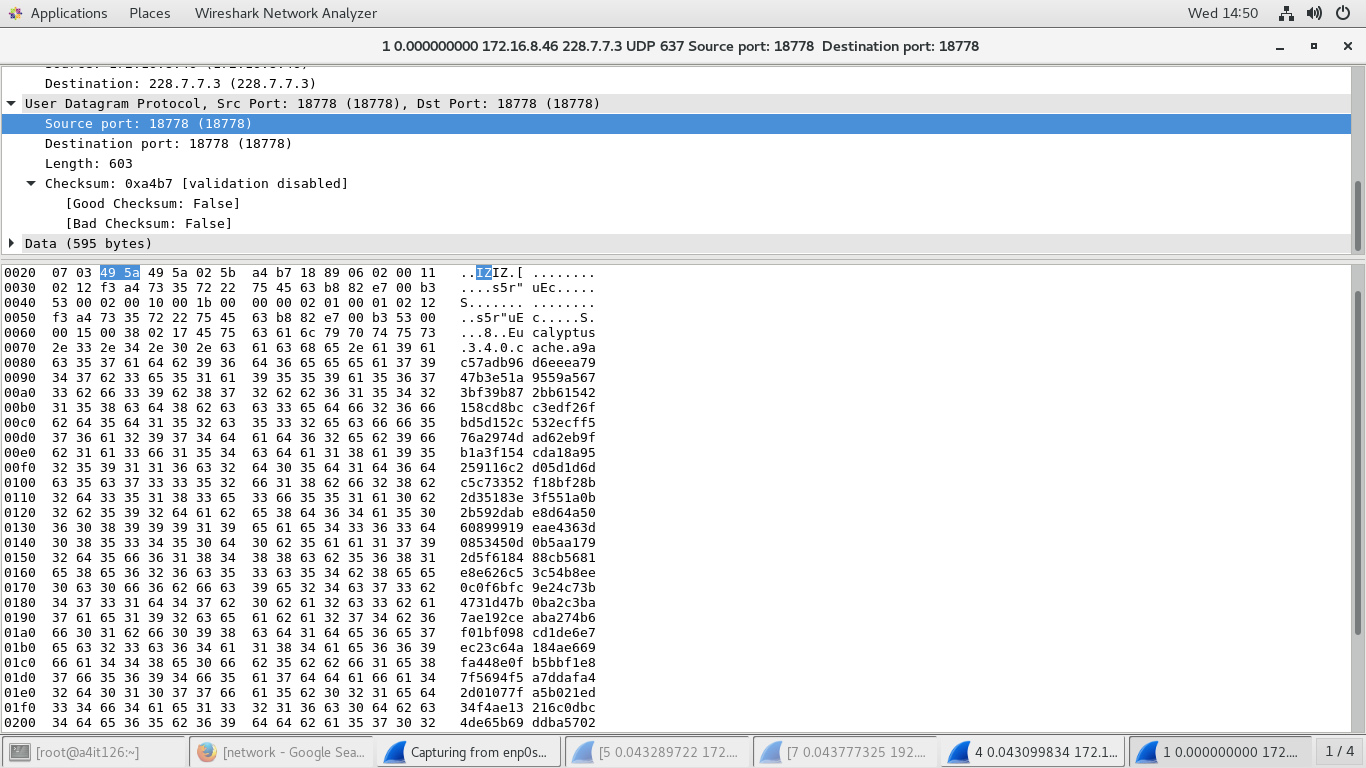












**Result:**

Thus, the network traffic packets were captured and inspected using the packet sniffer.