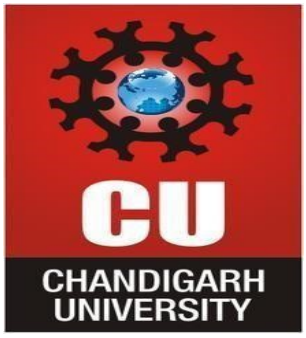
CHANDIGARH UNIVERSITY
UNIVERSITY INSTITUTE OF ENGINEERING

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING



Submitted To:	Arvind Gautam
Submitted by:	Rajiv Paul
UID	20BCS1812
Section/Group:	702(A)
Subject Name:	Project Based Learning in Java Lab
Subject Code:	20CSP-321
Branch:	BE-CSE
Semester:	5th

LAB INDEX

NAME: SUBJECTNAME: Competitive Coding Lab Date:
UID: SUBJECTCODE:20CSP-314
SECTION: 702(A)

Sr. No	Program	Date	Evaluation				Sign
			LW (12)	VV (8)	FW (10)	Total (30)	
1.	To Identify http packets on monitoring tool i.e Wireshark						
2.							
3.							
4.							
5.							
6.							
7.							
8.							
9.							
10.							

Worksheet-1

Web and Mobile Security (CSP-338)

Aim: Open any website on computer system and identify http packet on monitoring tool like Wireshark.

Objective: To analyse http traffic.

Software/Hardware Requirements:

Kali Linux, Wireshark Packet Sniffer

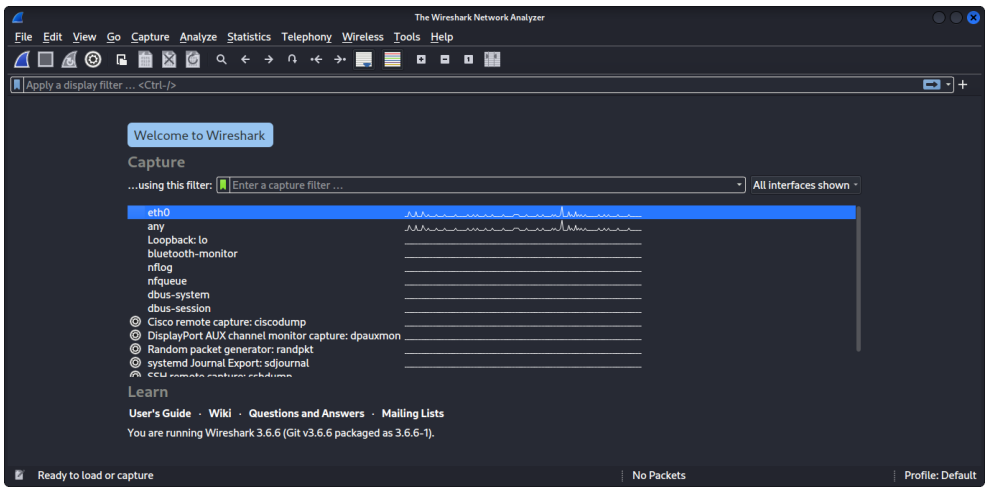
PC(Macbook Air)

Steps/Method/Coding:

1. Started Kali Linux on UTM(Virtual Machine).
2. Opened Terminal in kali Linux.
3. In the terminal we typed “Wireshark” command and hit enter.
4. Wireshark started and shows the type of internet connections are in use.
5. Then we click on the Wireshark capture options.
6. In the Wireshark capture option we select eth0 and click start.
7. After starting capturing packets of the traffic, we go to any of browser and visit the url http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html
8. After loading the above url it shows some message like “Congratulation, You’ve downloaded the file”
9. Then we stop capturing packets.
10. Then we search for http protocols which has got captured while capturing packets.
11. We save the captured traffic file with an extension (.pcap)

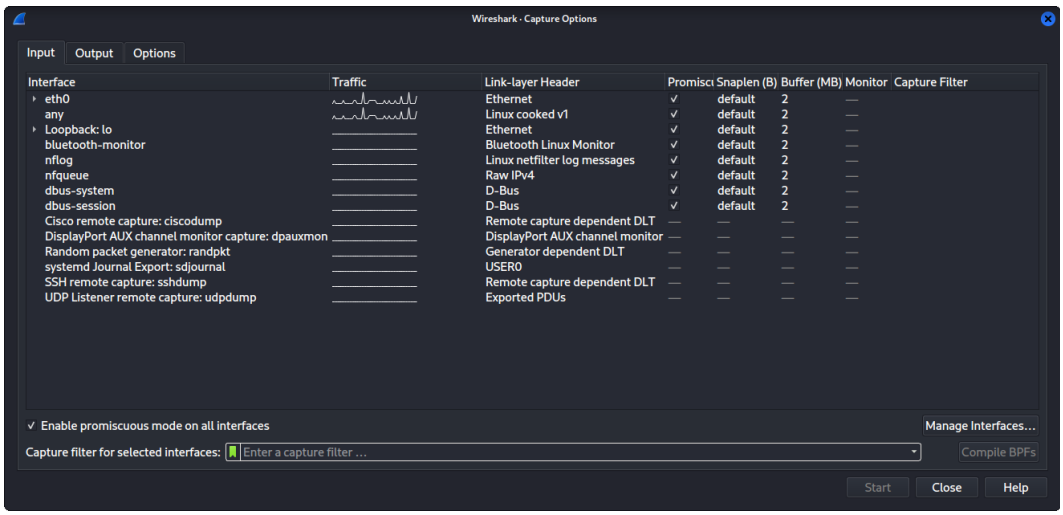
Output screenshot:

1.



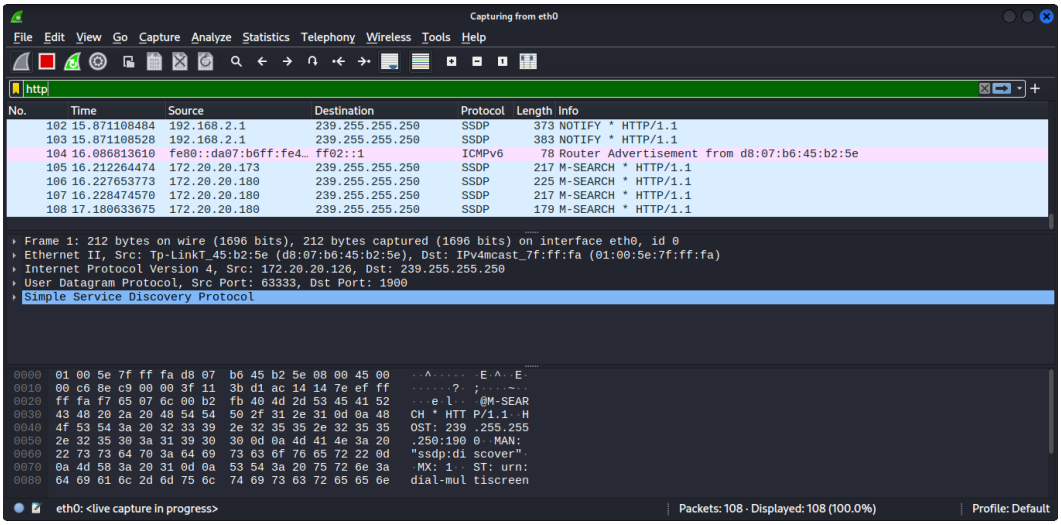
Starting Page of Wireshark

2.



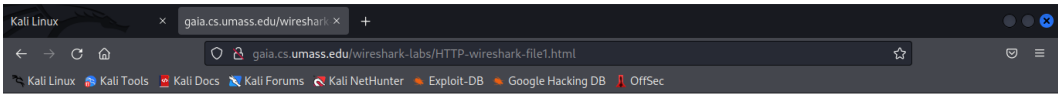
Capture Options

3.



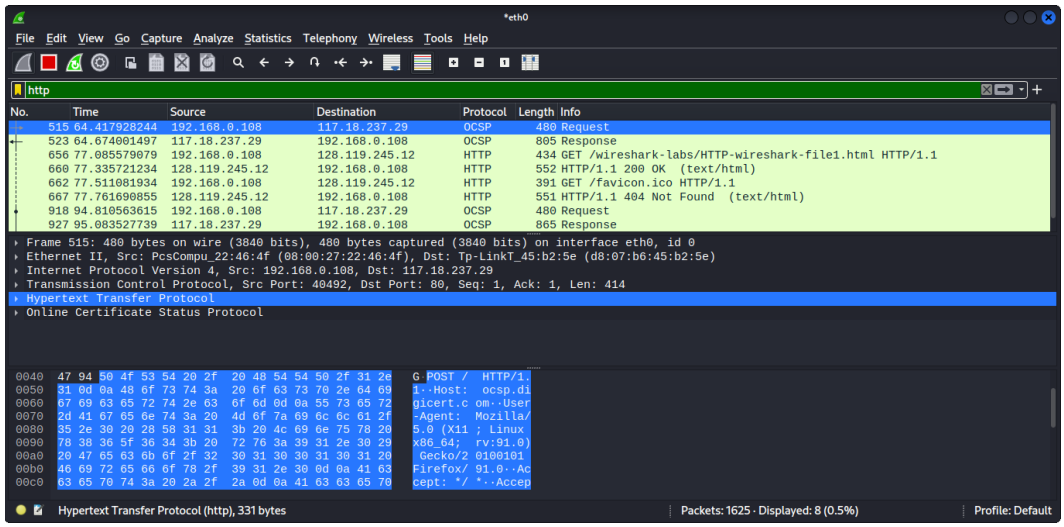
Capturing Traffic Packets

4.



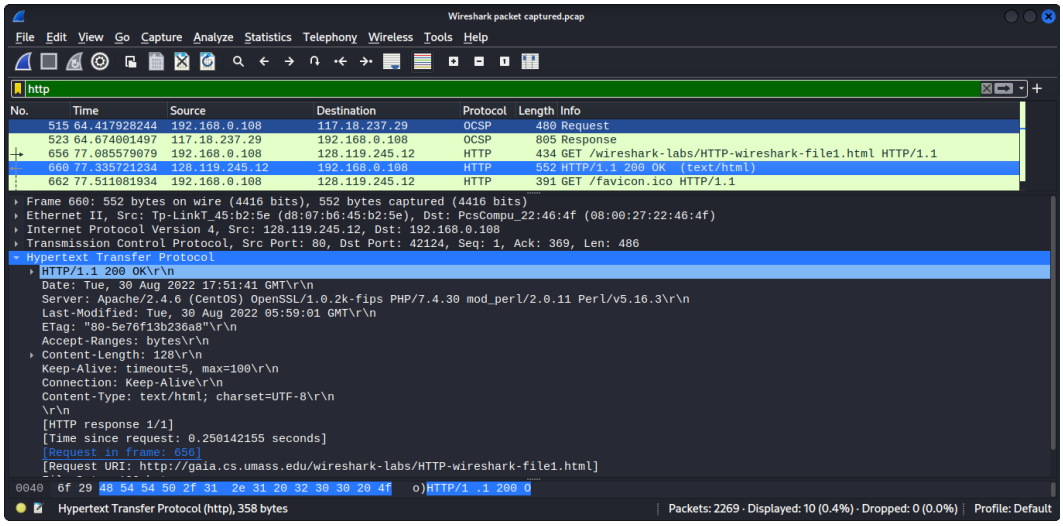
URL http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html page.

5.



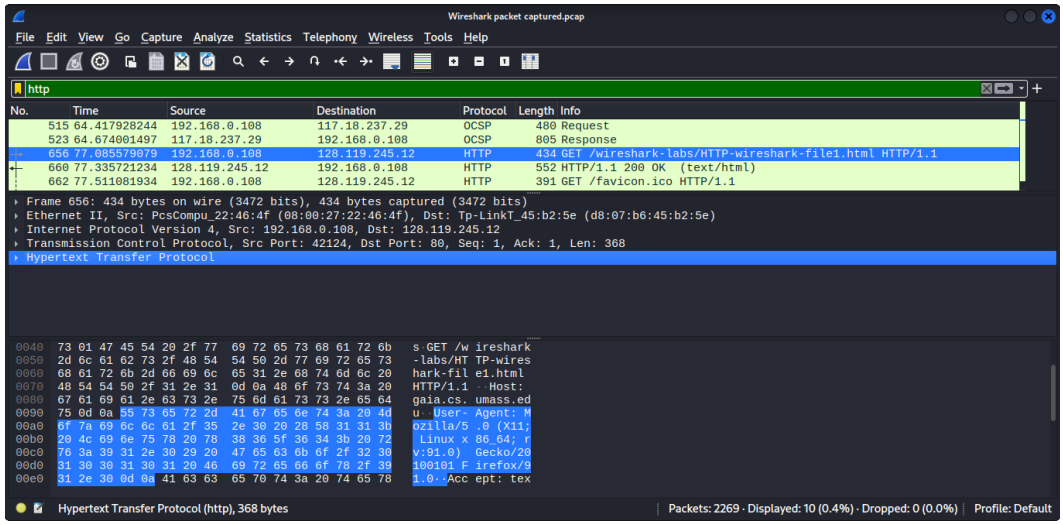
After stopping capture and filtering http packets in the traffic

6.



Details of request made by client and response packets

7.



Captured url i.e http trafficking

Learning Outcomes:

1. I learnt how to use Wireshark.
2. Learnt how to perform packet tracing.
3. Learnt how to perform packet snipping.
4. Learnt how to get details of a specific protocol got captured while capturing packets.
5. Learnt how http(unsecured) website can cause data/information leakage.