

## ASSIGNMENT -6

a1) 10 protocols : TCP,HTTP,  
ARP,ICMP,TLSv1.2,NBNS,LOOP,SSDP,LLMNR,DNS,BROWSER

a2) http.request.method == "GET" || http.response.code == 200, just used the filter http.response.code==200 and time since request= 0.013117 sec.

a3) used the filter : http.host contains "google.com" [google.com](http://google.com) ip :  
172.31.100.14  
ip of the system : 172.31.108.101

Applications Places Wireshark Network Analyzer

Capturing from eno1 [Wireshark 1.10.3 (SVN Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
35	12.004891000	fe80::7cca:32b3:adcf:baaff02::1:3	224.0.0.252	LLMNR	84	Standard query 0xe7c7 A wpad
36	12.004910000	172.31.108.187	172.31.111.255	LLMNR	64	Standard query 0xe7c7 A wpad
37	12.205371000	172.31.108.187	172.31.111.255	NBNS	92	Name query NB WPAD<00>
38	12.708042000	172.31.108.85	172.31.108.82	ICMP	90	Echo (ping) request id=0x2a34, seq=1/256, ttl=63
39	12.954997000	172.31.108.187	172.31.111.255	NBNS	92	Name query NB WPAD<00>
40	13.704934000	172.31.108.187	172.31.111.255	NBNS	92	Name query NB WPAD<00>
41	14.002100000	Cisco_fe6c:98	Broadcast	Spanning-tree (for-bridgSTP	60	Conf. Root = 32768/0/00:1b:90:95:b0:7d Cost = 24 Port = 0x8018
42	14.200932000	Cisco_95:b0:00	Broadcast	ARP	60	Who has 172.31.108.38? Tell 172.31.108.1
43	15.999731000	Cisco_fe6c:98	Spanning-tree (for-bridgSTP	60	Conf. Root = 32768/0/00:1b:90:95:b0:7d Cost = 24 Port = 0x8018	
44	17.201078000	Cisco_95:b0:00	Broadcast	ARP	60	Who has 172.31.108.38? Tell 172.31.108.1
45	17.566833000	Cisco_fe6c:98	Cisco_fe6c:98	LOOP	60	Reply
46	17.999763000	Cisco_fe6c:98	Spanning-tree (for-bridgSTP	60	Conf. Root = 32768/0/00:1b:90:95:b0:7d Cost = 24 Port = 0x8018	
47	20.001865000	Cisco_fe6c:98	Spanning-tree (for-bridgSTP	60	Conf. Root = 32768/0/00:1b:90:95:b0:7d Cost = 24 Port = 0x8018	
48	21.770614000	172.31.108.101	172.31.100.14	TCP	112	[TCP segment of a reassembled PDU]
49	21.771096000	172.31.100.14	172.31.108.101	TCP	66	ndL-aas > 50620 [ACK] Seq=1 Ack=47 Win=172 Len=0 TSval=2827808486 TSecr=3589445
50	21.784123000	172.31.100.14	172.31.108.101	TCP	126	[TCP segment of a reassembled PDU]
51	21.784150000	172.31.100.14	172.31.108.101	TCP	66	ndL-aas > 50620 [FIN, ACK] Seq=61 Ack=47 Win=172 Len=0 TSval=2827808499 TSecr=35894
52	21.784244000	172.31.108.101	172.31.100.14	TCP	112	[TCP segment of a reassembled PDU]

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

- IEEE 802.3 Ethernet
- Logical-Link Control
- Spanning Tree Protocol

0000 01 80 c2 00 00 00 a4 0c c3 fe 6c 98 00 26 42 42 .....6B

0010 03 00 00 00 00 00 80 00 00 1b 90 95 b0 7d 00 00 .....)

0020 00 18 80 7d a4 0c c3 fe 6c 98 00 18 06 00 14 00 .....)

0030 02 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 .....)

eno1: <live capture in progress> Fil... Packets: 298 Displayed: 298 (100.0%) Profile: Default

Applications Places Wireshark Network Analyzer

Capturing from eno1 [Wireshark 1.10.3 (SVN Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
187	75.537540000	172.31.108.101	172.31.100.14	TCP	66	50622 > ndL-aas [ACK] Seq=3033 Ack=2026 Win=20736 Len=0 TSval=3643212 TSecr=2827862
188	75.537696000	172.31.108.101	172.31.100.14	TLSv1.2	112	Application Data
189	75.538203000	172.31.100.14	172.31.108.101	TCP	66	ndL-aas > 50622 [ACK] Seq=2026 Ack=3079 Win=20608 Len=0 TSval=2827862244 TSecr=3645
190	76.006974000	Cisco_fe6c:98	Spanning-tree (for-bridgSTP	60	Conf. Root = 32768/0/00:1b:90:95:b0:7d Cost = 24 Port = 0x8018	
191	77.594678000	Cisco_fe6c:98	LOOP	60	Reply	
192	78.006895000	Cisco_fe6c:98	Spanning-tree (for-bridgSTP	60	Conf. Root = 32768/0/00:1b:90:95:b0:7d Cost = 24 Port = 0x8018	
193	79.235244000	fe80::7cca:32b3:adcf:baaff02::1:3	224.0.0.252	LLMNR	84	Standard query 0x6138 A wpad
194	79.235287000	172.31.108.187	224.0.0.252	LLMNR	64	Standard query 0x6138 A wpad
195	79.335175000	fe80::7cca:32b3:adcf:baaff02::1:3	224.0.0.252	LLMNR	84	Standard query 0x6138 A wpad
196	79.335205000	172.31.108.187	224.0.0.252	LLMNR	64	Standard query 0x6138 A wpad
197	79.535631000	172.31.108.187	172.31.111.255	NBNS	92	Name query NB WPAD<00>
198	80.061207000	Cisco_fe6c:98	Spanning-tree (for-bridgSTP	60	Conf. Root = 32768/0/00:1b:90:95:b0:7d Cost = 24 Port = 0x8018	
199	80.285289000	172.31.108.187	172.31.111.255	NBNS	92	Name query NB WPAD<00>
200	80.998958000	172.31.110.2	239.255.255.250	SSDP	299	NOTIFY * HTTP/1.1
201	80.999807000	172.31.110.2	239.255.255.250	SSDP	307	NOTIFY * HTTP/1.1
202	81.000314000	172.31.110.2	239.255.255.250	SSDP	351	NOTIFY * HTTP/1.1
203	81.000851000	172.31.110.2	239.255.255.250	SSDP	365	NOTIFY * HTTP/1.1
204	81.001394000	172.31.110.2	239.255.255.250	SSDP	363	NOTIFY * HTTP/1.1
205	81.035388000	172.31.108.187	172.31.111.255	NBNS	92	Name query NB WPAD<00>

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

- IEEE 802.3 Ethernet
- Logical-Link Control
- Spanning Tree Protocol

0000 01 80 c2 00 00 00 a4 0c c3 fe 6c 98 00 26 42 42 .....6B

0010 03 00 00 00 00 00 80 00 00 1b 90 95 b0 7d 00 00 .....)

0020 00 18 80 7d a4 0c c3 fe 6c 98 00 18 06 00 14 00 .....)

0030 02 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 .....)

eno1: <live capture in progress> Fil... Packets: 472 Displayed: 472 (100.0%) Profile: Default

Applications Places Wireshark Network Analyzer Fri 09:43 User

Capturing from eno1 [Wireshark 1.10.3 (SVN Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http.host contains "google.com" Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
169	75.044674000	172.31.108.101	172.31.100.14	HTTP	322	CONNECT mail.google.com:443 HTTP/1.1
548	241.599210000	172.31.108.101	172.31.100.14	HTTP	322	CONNECT play.google.com:443 HTTP/1.1
1129	329.152463000	172.31.108.101	172.31.100.14	HTTP	330	CONNECT clients6.google.com:443 HTTP/1.1
1155	329.300815000	172.31.108.101	172.31.100.14	HTTP	330	CONNECT clients6.google.com:443 HTTP/1.1
1185	329.784647000	172.31.108.101	172.31.100.14	HTTP	330	CONNECT clients4.google.com:443 HTTP/1.1
1883	433.403198000	172.31.108.101	172.31.100.14	HTTP	322	CONNECT play.google.com:443 HTTP/1.1
1942	448.781458000	172.31.108.101	172.31.100.14	HTTP	330	CONNECT clients6.google.com:443 HTTP/1.1
1963	448.901660000	172.31.108.101	172.31.100.14	HTTP	330	CONNECT clients6.google.com:443 HTTP/1.1
2197	549.053986000	172.31.108.101	172.31.100.14	HTTP	322	CONNECT plus.google.com:443 HTTP/1.1
2284	573.302708000	172.31.108.101	172.31.100.14	HTTP	322	CONNECT play.google.com:443 HTTP/1.1
2301	573.346478000	172.31.108.101	172.31.100.14	HTTP	330	CONNECT clients6.google.com:443 HTTP/1.1
2306	573.347332000	172.31.108.101	172.31.100.14	HTTP	330	CONNECT clients6.google.com:443 HTTP/1.1
2363	573.746759000	172.31.108.101	172.31.100.14	HTTP	322	CONNECT apis.google.com:443 HTTP/1.1
2525	581.356928000	172.31.108.101	172.31.100.14	HTTP	330	CONNECT clients4.google.com:443 HTTP/1.1
2925	675.633440000	172.31.108.101	172.31.100.14	HTTP	322	CONNECT mail.google.com:443 HTTP/1.1
3006	699.867855000	172.31.108.101	172.31.100.14	HTTP	322	CONNECT plus.google.com:443 HTTP/1.1
3077	726.084298000	172.31.108.101	172.31.100.14	HTTP	330	CONNECT clients6.google.com:443 HTTP/1.1
3135	727.084942000	172.31.108.101	172.31.100.14	HTTP	322	CONNECT apis.google.com:443 HTTP/1.1
3371	733.420198000	172.31.108.101	172.31.100.14	HTTP	322	CONNECT play.google.com:443 HTTP/1.1

Frame 169: 322 bytes on wire (2576 bits), 322 bytes captured (2576 bits) on interface 0

Interface id: 0

Encapsulation type: Ethernet (1)

Arrival Time: Feb 12, 2016 09:18:33.274645000 IST

Time shift: for this packet: 0.000000000 seconds

0000 00 1b 90 95 b0 00 a0 48 1c 76 e8 ba 08 00 45 00 .....H.v....E..

0010 01 34 c4 d2 40 00 40 06 c4 3f ac 1f 6c 65 ac 1f ..4L@.@..?..le..

0020 64 0e c5 be 0c 38 c8 5f d9 8f c3 68 68 5d 80 18 d...8\_...hh)..

0030 00 73 29 d9 00 00 01 01 08 0a 00 37 95 5f a8 8d ..s).....?;...q

0040 be f7 43 4f 4e 4e 45 43 54 20 6d 61 69 6c 2e 67 ..CONNECT mail.g

eno1: alive capture in progress? Fil... Packets: 9675 - Displayed: 48 (0.5%)

Profile: Default

1 / 4

Applications Places Wireshark Network Analyzer Fri 09:29 User

Capturing from eno1 [Wireshark 1.10.3 (SVN Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http.response.code == 200 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
171	75.057842000	172.31.100.14	172.31.108.101	HTTP	105	HTTP/1.0 200 Connection established
550	241.612075000	172.31.100.14	172.31.108.101	HTTP	105	HTTP/1.0 200 Connection established
575	246.106225000	172.31.100.14	172.31.108.91	HTTP	105	HTTP/1.0 200 Connection established
639	272.569934000	172.31.100.14	172.31.108.87	HTTP	105	HTTP/1.0 200 Connection established
1131	329.165846000	172.31.100.14	172.31.108.101	HTTP	105	HTTP/1.0 200 Connection established
1157	329.313602000	172.31.100.14	172.31.108.101	HTTP	105	HTTP/1.0 200 Connection established
1192	329.798021000	172.31.100.14	172.31.108.101	HTTP	105	HTTP/1.0 200 Connection established
1885	433.416319000	172.31.100.14	172.31.108.101	HTTP	105	HTTP/1.0 200 Connection established
1944	448.794647000	172.31.100.14	172.31.108.101	HTTP	105	HTTP/1.0 200 Connection established
1965	448.915481000	172.31.100.14	172.31.108.101	HTTP	105	HTTP/1.0 200 Connection established
2199	549.067103000	172.31.100.14	172.31.108.101	HTTP	105	HTTP/1.0 200 Connection established
2288	573.315596000	172.31.100.14	172.31.108.101	HTTP	105	HTTP/1.0 200 Connection established
2309	573.371726000	172.31.100.14	172.31.108.101	HTTP	105	HTTP/1.0 200 Connection established
2311	573.371771000	172.31.100.14	172.31.108.101	HTTP	105	HTTP/1.0 200 Connection established
2365	573.759744000	172.31.100.14	172.31.108.101	HTTP	105	HTTP/1.0 200 Connection established
2408	574.213714000	172.31.100.14	172.31.108.101	HTTP	105	HTTP/1.0 200 Connection established
2527	581.370023000	172.31.100.14	172.31.108.101	HTTP	105	HTTP/1.0 200 Connection established
2927	675.646182000	172.31.100.14	172.31.108.101	HTTP	105	HTTP/1.0 200 Connection established
3006	699.867855000	172.31.100.14	172.31.108.101	HTTP	105	HTTP/1.0 200 Connection established

Frame 2199: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface 0

Interface id: 0

Encapsulation type: Ethernet (1)

Arrival Time: Feb 12, 2016 09:18:33.274645000 IST

Time shift: for this packet: 0.000000000 seconds

0000 00 7a 97 1e 00 00 01 01 08 0a a8 94 fa 50 00 3e ..2.....P.>

0010 d0 f8 48 54 54 50 2f 31 2e 30 20 32 30 30 20 43 ..HTTP/1.0 200 C

0020 6f 6e 6e 65 63 74 69 6f 6e 20 65 73 74 61 62 6c onnectio n establ

0030 69 73 68 65 64 0d 0a 0d 00 ..ished...

Text item (text), 2 bytes

Packets: 3276 - Displayed: 22 (0.7%)

Profile: Default

1 / 4

//hide text using stegananography

```
import java.io.*;
import java.awt.image.BufferedImage;
import java.io.ByteArrayOutputStream;
import java.io.File;
import java.io.IOException;
import javax.imageio.ImageIO;
import java.util.Scanner;
import java.nio.charset.StandardCharsets;
import java.io.UnsupportedEncodingException;

public class Steganography {
    public static void main(String args[])throws IOException {
        /* Convert Input Image to Byte */
        BufferedImage originalImage = ImageIO.read(new
File("/home/user/Desktop/image.jpg"));
        ByteArrayOutputStream baos = new
ByteArrayOutputStream();
        ImageIO.write( originalImage, "jpg", baos );
        baos.flush();
        byte[] imageInByte = baos.toByteArray();
        baos.close();
        Scanner sc=new Scanner(System.in);
        System.out.println("Enter Your Secret Message : ");
        String str=sc.next();

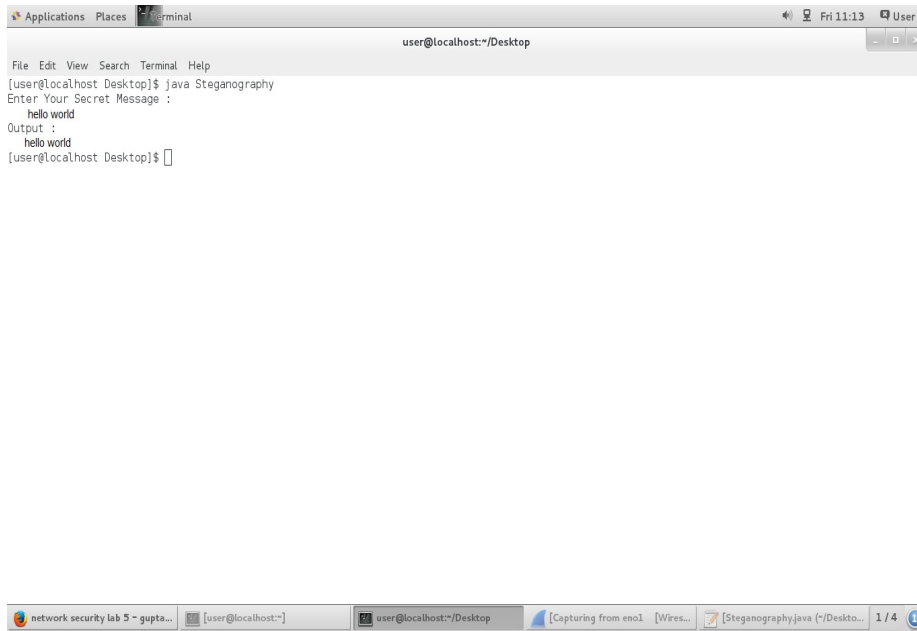
        byte[] b = str.getBytes();
        for(int i=0; i<b.length; i++) {
            imageInByte[i+100]=b[i];
        }
        /* Convert Steg Bytes to Image */
        BufferedImage img = ImageIO.read(new
ByteArrayInputStream(imageInByte));
        File f = new File("output.jpg");
        ImageIO.write(img, "JPEG", f);

        /* Convert Input Image to byte */
        BufferedImage originalImage2 = ImageIO.read(new
File("/home/user/Desktop/image2.jpg"));
        ByteArrayOutputStream baos2 = new
ByteArrayOutputStream();
        ImageIO.write( originalImage2, "jpg", baos2);
        baos2.flush();
        byte[] imageInByte2 = baos2.toByteArray();
        baos2.close();

        byte b2[]=new byte[b.length];
        for(int i=0; i<b.length; i++) {
            b2[i]=imageInByte2[i+100];
        }
        String s=new String(b);
```

```
        System.out.println("Output : \n "+s);  
    }  
}
```

## OUTPUT:



The screenshot shows a terminal window titled "Terminal" with the user "User" at "Fri 11:13". The terminal content is as follows:

```
user@localhost:~/Desktop  
File Edit View Search Terminal Help  
[user@localhost Desktop]$ java Steganography  
Enter Your Secret Message :  
hello world  
Output :  
hello world  
[user@localhost Desktop]$
```

The terminal window is part of a desktop environment. The taskbar at the bottom shows several open applications: "network security lab 5 - gupta...", "[user@localhost:~]", "user@localhost:~/Desktop", "[Capturing from eno1 [Wires...]", and "[Steganography.java (~/Desko... 1 / 4]".

