CS 315 : Computer Networks Lab
Assignment - 8
Wireshark Lab: NAT & SMTP

Ayush Mallick
CS22BT008

Part-1

1.1

Source IP address : *192.168.10.11*
Source port number : *53924*
Destination IP address : *138.76.29.8*
Destination port number : *80*

```
[Header checksum status: Unverified]
Source Address: 192.168.10.11
Destination Address: 138.76.29.8
Transmission Control Protocol, Src Port: 53924, Dst Port: 80, Seq: 1, Ack: 1, Len: 330
Source Port: 53924
Destination Port: 80
[Stream index: 0]
```

1.2

0.030672101

No.	Time	Source	Destination	Protocol	Length	Info
4	0.027362245	192.168.10.11	138.76.29.8	HTTP	396	GET / HTTP/1.1
6	0.030672101	138.76.29.8	192.168.10.11	HTTP	613	HTTP/1.1 200 OK (text/html)
8	0.231407421	192.168.10.11	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
10	0.233074462	138.76.29.8	192.168.10.11	HTTP	555	HTTP/1.1 404 Not Found (text/html)

1.3

Source IP address : *138.76.29.8*
Source port number : *80*
Destination IP address : *192.168.10.11*
Destination port number : *53924*

```
[Header checksum status: Unverified]
Source Address: 138.76.29.8
Destination Address: 192.168.10.11
Transmission Control Protocol, Src Port: 80, Dst Port: 53924, Seq: 1, Ack: 331, Len: 547
Source Port: 80
Destination Port: 53924
[Stream index: 0]
```

1.4

0.027356291

No.	Time	Source	Destination	Protocol	Length	Info
4	0.027356291	10.0.1.254	138.76.29.8	HTTP	396	GET / HTTP/1.1
6	0.030625966	138.76.29.8	10.0.1.254	HTTP	613	HTTP/1.1 200 OK (text/html)
8	0.231400190	10.0.1.254	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
10	0.233043313	138.76.29.8	10.0.1.254	HTTP	555	HTTP/1.1 404 Not Found (text/html)

1.5

Source IP address : *10.0.1.254*
Source port number : *53924*
Destination IP address : *138.76.29.8*
Destination port number : *80*

```
[Header checksum status: Unverified]
Source Address: 10.0.1.254
Destination Address: 138.76.29.8
Transmission Control Protocol, Src Port: 53924, Dst Port: 80, Seq: 1, Ack: 1, Len: 330
Source Port: 53924
Destination Port: 80
[Stream index: 0]
```

1.6

Source IP address field differs due to NAT translation.

1.7

No, none of the fields in the HTTP GET message are changed.

1.8

The *Time to Live*, *Header Checksum*, and *Source Address* fields are changed.

```
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0x64dc [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.10.11
Destination Address: 138.76.29.8
```

```
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 63
Protocol: TCP (6)
Header Checksum: 0x2492 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.0.1.254
Destination Address: 138.76.29.8
```

1.9

0.30625966

No.	Time	Source	Destination	Protocol	Length	Info
4	0.027356291	10.0.1.254	138.76.29.8	HTTP	396	GET / HTTP/1.1
6	0.030625966	138.76.29.8	10.0.1.254	HTTP	613	HTTP/1.1 200 OK (text/html)
8	0.231400190	10.0.1.254	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
10	0.233043313	138.76.29.8	10.0.1.254	HTTP	555	HTTP/1.1 404 Not Found (text/html)

1.10

Source IP address : *138.76.29.8*
Source port number : *80*
Destination IP address : *10.0.1.254*
Destination port number : *53924*

```
[Header checksum status: Unverified]
Source Address: 138.76.29.8
Destination Address: 10.0.1.254
Transmission Control Protocol, Src Port: 80, Dst Port: 53924, Seq: 1, Ack: 331, Len: 547
Source Port: 80
Destination Port: 53924
[Stream index: 0]
```

1.11

Source IP address : *138.76.29.8*
Source port number : *80*
Destination IP address : *192.168.10.11*
Destination port number : *53924*

```
[Header checksum status: Unverified]
Source Address: 138.76.29.8
Destination Address: 192.168.10.11
▾ Transmission Control Protocol, Src Port: 80, Dst Port: 53924, Seq: 1, Ack: 331, Len: 547
  Source Port: 80
  Destination Port: 53924
  [Stream index: 0]
```

Part-2

2.1

Client IP address : *10.10.1.4*
DNS resolver IP address : *10.10.1.1*

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.1.4	10.10.1.1	DNS	76	Standard query 0x7956 A mail.patriots.in
2	0.034025	10.10.1.1	10.10.1.4	DNS	142	Standard query response 0x7956 A mail.pat

2.2

Domain name : *mail.patriots.in*
IP address : *74.53.140.153*

```
▾ Domain Name System (response)
    Transaction ID: 0x7956
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 2
    Additional RRs: 0
  ▸ Queries
  ▾ Answers
    ▾ mail.patriots.in: type CNAME, class IN, cname patriots.in
        Name: mail.patriots.in
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 10827 (3 hours, 27 seconds)
        Data length: 2
        CNAME: patriots.in
    ▾ patriots.in: type A, class IN, addr 74.53.140.153
        Name: patriots.in
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 10828 (3 hours, 28 seconds)
        Data length: 4
        Address: 74.53.140.153
  ▸ Authoritative nameservers
    [Request In: 1]
    [Time: 0.034025000 seconds]
```

2.3

Source port number : *1470*
Destination port number : *25*

```
▾ Transmission Control Protocol, Src Port: 1470, Dst Port: 25, Seq: 1, Ack: 182, Len: 9
    Source Port: 1470
    Destination Port: 25
    [Stream index: 0]
```

Yes, the destination port number matches with the standard port of SMTP in /etc/services.

```
cs101@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ grep smtp /etc/services
smtp            25/tcp          mail
submissions     465/tcp         ssmtp smtps urd # Submission over TLS [RFC8314]
```

2.4

SMTP commands sent by the client to the mail server :

EHLO
AUTH LOGIN
User
Pass
MAIL FROM
RCPT TO
DATA
QUIT

smtp.req

No.	Time	Source	Destination	Protocol	Length	Info
7	0.732749	10.10.1.4	74.53.140.153	SMTP	63	C: EHLO GP
10	1.076669	10.10.1.4	74.53.140.153	SMTP	66	C: AUTH LOGIN
12	1.419595	10.10.1.4	74.53.140.153	SMTP	84	C: User: Z3VycGFydGFwQHBhdHJpb3RzLmlu
14	1.762058	10.10.1.4	74.53.140.153	SMTP	72	C: Pass: cHVuamFiQDEyMw==
16	2.122354	10.10.1.4	74.53.140.153	SMTP	90	C: MAIL FROM: <gurpartap@patriots.in>
18	2.465190	10.10.1.4	74.53.140.153	SMTP	93	C: RCPT TO: <raj_deol2002in@yahoo.co.in>
20	2.828143	10.10.1.4	74.53.140.153	SMTP	60	C: DATA
54	7.271765	10.10.1.4	74.53.140.153	SMTP	60	C: QUIT

2.5

Service ready response code : *220*
Response code to EHLO : *250*
Response code to AUTH LOGIN : *334*
Response code to User : *334*
Response code to Pass : *235*
Response code to MAIL FROM : *250*
Response code to RCPT TO : *250*
Response code to DATA : *354*
Response code to QUIT : *221*

smtp.rsp

No.	Time	Source	Destination	Protocol	Length	Info
6	0.727603	74.53.140.153	10.10.1.4	SMTP	235	S: 220-xc90.websitewelcome.com ESMTP Exim 4.69 #1 Mon, 05
9	1.074123	74.53.140.153	10.10.1.4	SMTP	191	S: 250-xc90.websitewelcome.com Hello GP [122.162.143.157]
11	1.419021	74.53.140.153	10.10.1.4	SMTP	72	S: 334 VXNlcm5hbWU6
13	1.761484	74.53.140.153	10.10.1.4	SMTP	72	S: 334 UGFzc3dvcmQ6
15	2.121738	74.53.140.153	10.10.1.4	SMTP	84	S: 235 Authentication succeeded
17	2.464705	74.53.140.153	10.10.1.4	SMTP	62	S: 250 OK
19	2.827648	74.53.140.153	10.10.1.4	SMTP	68	S: 250 Accepted
21	3.169619	74.53.140.153	10.10.1.4	SMTP	110	S: 354 Enter message, ending with "." on a line by itself
52	4.756729	74.53.140.153	10.10.1.4	SMTP	82	S: 250 OK id=1Mugho-0003Dg-Un
56	7.613407	74.53.140.153	10.10.1.4	SMTP	102	S: 221 xc90.websitewelcome.com closing connection

2.6

From : *gurpartap@patriots.in*
To : *raj_deol2002in@yahoo.co.in*
Subject : *SMTP*
Date : *Mon, 5 Oct 2009 11:36:07 +0530*
Message ID : *000301ca4581$ef9e57f0$cedb07d0$@in*
MIME version : *1.0*

```
▾ Internet Message Format
  ▾ From: "Gurpartap Singh" <gurpartap@patriots.in>, 1 item
    ▾ Item: "Gurpartap Singh" <gurpartap@patriots.in>\r\n
        Display-Name: "Gurpartap Singh"
        Address: gurpartap@patriots.in
  ▾ To: <raj_deol2002in@yahoo.co.in>, 1 item
    ▾ Item: <raj_deol2002in@yahoo.co.in>\r\n
        Address: raj_deol2002in@yahoo.co.in
    Subject: SMTP
    Date: Mon, 5 Oct 2009 11:36:07 +0530
    Message-ID: <000301ca4581$ef9e57f0$cedb07d0$@in>
    MIME-Version: 1.0
```

2.7

Total data size : *15156 bytes*
Number of data fragments : *14*

```
▾ Simple Mail Transfer Protocol
    C: .
  ▾ [14 DATA fragments (15156 bytes): #22(1460), #23(14
      [Frame: 22, payload: 0-1459 (1460 bytes)]
      [Frame: 23, payload: 1460-2919 (1460 bytes)]
      [Frame: 24, payload: 2920-4379 (1460 bytes)]
      [Frame: 25, payload: 4380-5839 (1460 bytes)]
      [Frame: 26, payload: 5840-6347 (508 bytes)]
      [Frame: 28, payload: 6348-6855 (508 bytes)]
      [Frame: 29, payload: 6856-7363 (508 bytes)]
      [Frame: 30, payload: 7364-7871 (508 bytes)]
      [Frame: 38, payload: 7872-9323 (1452 bytes)]
      [Frame: 39, payload: 9324-10775 (1452 bytes)]
      [Frame: 41, payload: 10776-12227 (1452 bytes)]
      [Frame: 42, payload: 12228-13679 (1452 bytes)]
      [Frame: 44, payload: 13680-15131 (1452 bytes)]
      [Frame: 45, payload: 15132-15155 (24 bytes)]
      [DATA fragment count: 14]
      [Reassembled DATA length: 15156]
```