21CY681– Internet Protocol lab

ASSIGNMENT -3

Name: B.Shebu

Register Number : CYS22005

Title: Analyzing HTTP requests and responses using wireshark

Date of Assignment provided: 20/10/2022

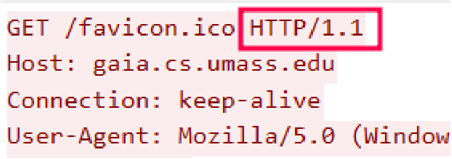
Aim: Exploring the Web application protocols using Protocol analysing tool called wireshark

PROCEDURE -

By looking at the information in the HTTP GET and response messages, answer the following questions.

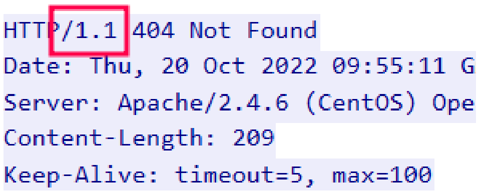
Q -> http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html

1. Is your browser running HTTP version 1.0 or 1.1? – **v1.1**



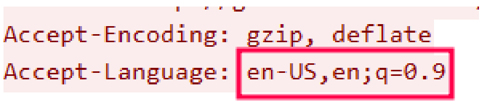
```
GET /favicon.ico HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
User-Agent: Mozilla/5.0 (Window
```

What version of HTTP is the server running? – **v1.1**



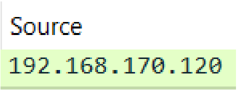
```
HTTP/1.1 404 Not Found
Date: Thu, 20 Oct 2022 09:55:11 G
Server: Apache/2.4.6 (CentOS) Ope
Content-Length: 209
Keep-Alive: timeout=5, max=100
```

2. What languages (if any) do your browser indicate that it can accept to the server? - **en-US,en**



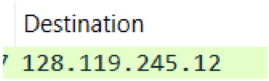
```
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

3. What is the IP address of your computer? - **192.168.170.120**



```
Source
192.168.170.120
```

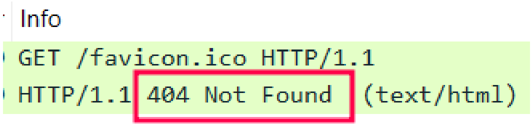
Of the gaia.cs.umass.edu server? - **128.119.245.12**



```
Destination
128.119.245.12
```

4. What is the status code returned from the server to your browser?

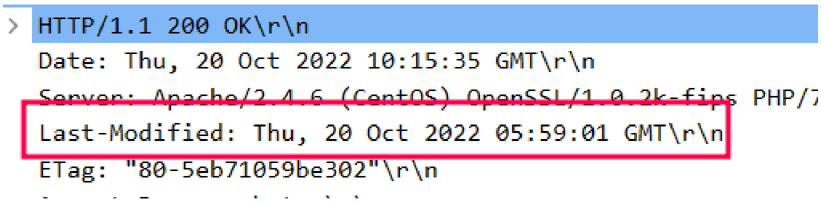
- **404 NOT FOUND**



```
Info
GET /favicon.ico HTTP/1.1
HTTP/1.1 404 Not Found (text/html)
```

5. When was the HTML file that you are retrieving last modified at the server?

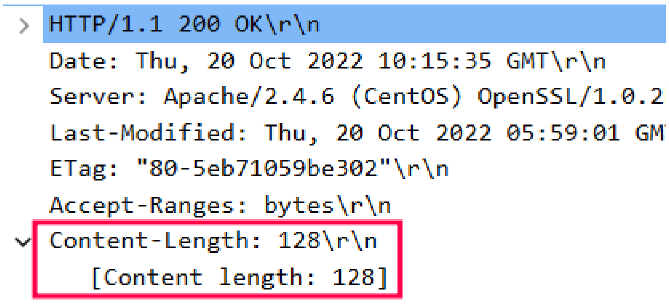
– **Thu, 20 Oct 2022 05:59:01 GMT**



```
> HTTP/1.1 200 OK\r\n
  Date: Thu, 20 Oct 2022 10:15:35 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7
  Last-Modified: Thu, 20 Oct 2022 05:59:01 GMT\r\n
  ETag: "80-5eb71059be302"\r\n
```

6. How many bytes of content are being returned to your browser?

- **128 bytes**



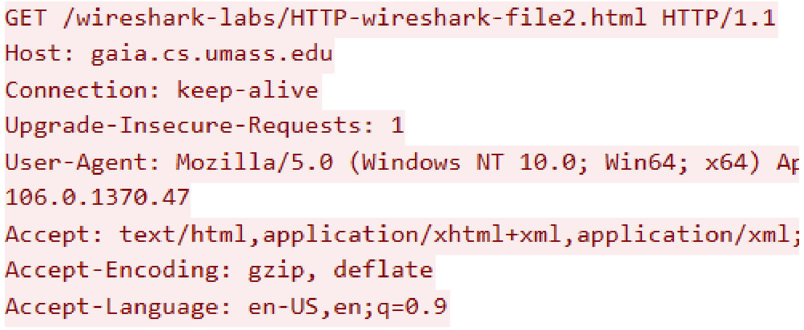
```
> HTTP/1.1 200 OK\r\n
  Date: Thu, 20 Oct 2022 10:15:35 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2
  Last-Modified: Thu, 20 Oct 2022 05:59:01 GM
  ETag: "80-5eb71059be302"\r\n
  Accept-Ranges: bytes\r\n
v Content-Length: 128\r\n
     [Content length: 128]
```

7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

ANS – **No , we don’t see any new headers .**

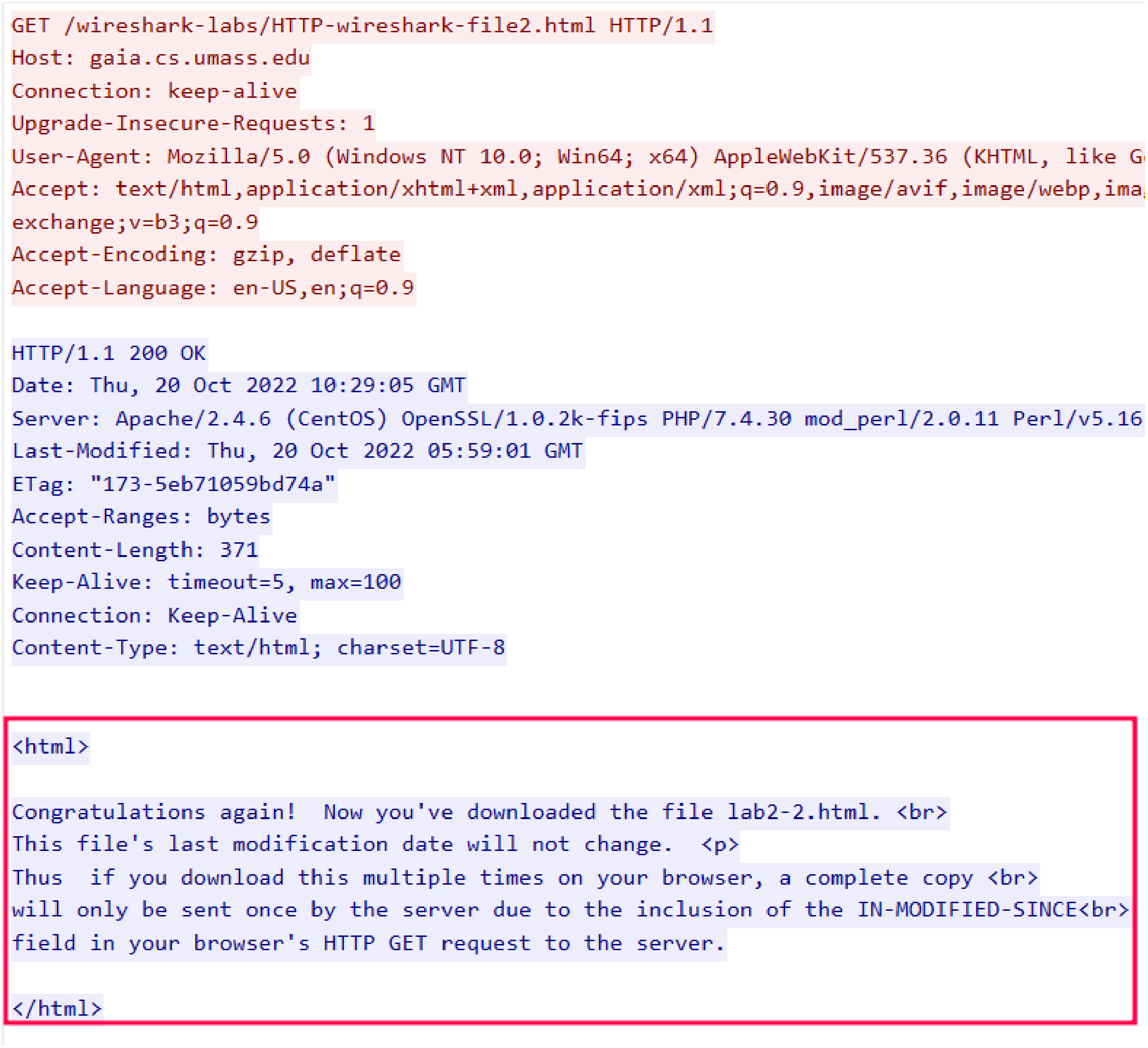
Q - > http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html

8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET? - No



```
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Ap
106.0.1370.47
Accept: text/html,application/xhtml+xml,application/xml;
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

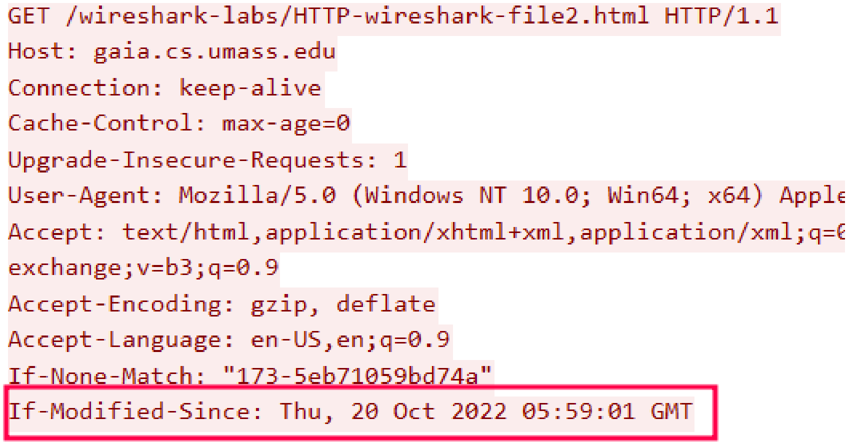
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell? - **Yes the server returned the contents of the HTML file**



```
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like G
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
Date: Thu, 20 Oct 2022 10:29:05 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16
Last-Modified: Thu, 20 Oct 2022 05:59:01 GMT
ETag: "173-5eb71059bd74a"
Accept-Ranges: bytes
Content-Length: 371
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html>

Congratulations again!  Now you've downloaded the file lab2-2.html. <br>
This file's last modification date will not change.  <p>
Thus  if you download this multiple times on your browser, a complete copy <br>
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>
field in your browser's HTTP GET request to the server.

</html>
```

10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET?

ANS – **YES we can see the IF-MODIFIED-SINCE header in the GET request.**

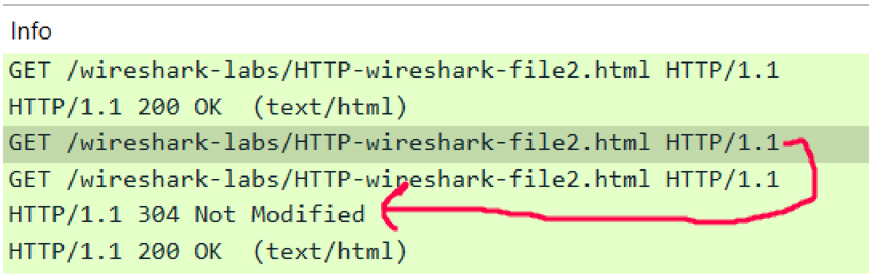


```
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Apple
Accept: text/html,application/xhtml+xml,application/xml;q=0
exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
If-None-Match: "173-5eb71059bd74a"
If-Modified-Since: Thu, 20 Oct 2022 05:59:01 GMT
```

What information follows the “IF-MODIFIEDSINCE:” header? - **Thu, 20 Oct 2022 05:59:01 GMT**

11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET?

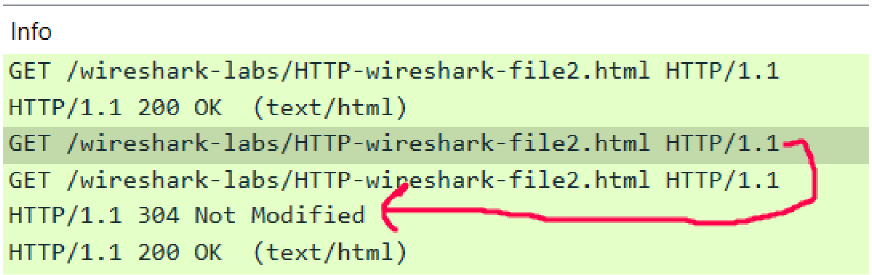
ANS – **Status_Code = 304 , Phrase is NOT MODIFIED**



```
Info
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
HTTP/1.1 200 OK  (text/html)
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
HTTP/1.1 304 Not Modified
HTTP/1.1 200 OK  (text/html)
```

Did the server explicitly return the file’s contents? Explain.

ANS – **No , the server didn’t return any contents because the contents of the file which was retrieved for the first time was not modified. So it displays 304 not modified.**

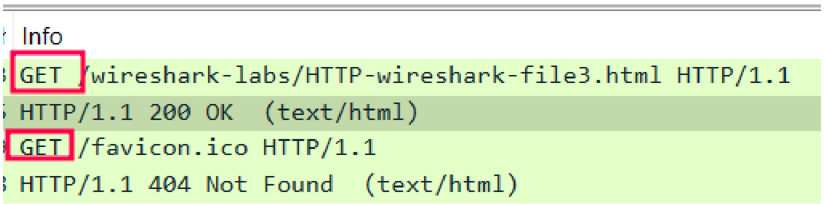


```
Info
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
HTTP/1.1 200 OK  (text/html)
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
HTTP/1.1 304 Not Modified
HTTP/1.1 200 OK  (text/html)
```

Q - > http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html

12. How many HTTP GET request messages did your browser send?

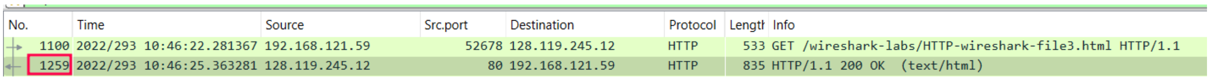
- **2 Get requests**



```
Info
GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
HTTP/1.1 200 OK  (text/html)
GET /favicon.ico HTTP/1.1
HTTP/1.1 404 Not Found  (text/html)
```

Which packet number in the trace contains the GET message for the Bill or Rights? – **First packet**

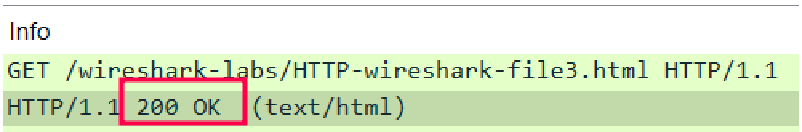
13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request? - **1259**



No.	Time	Source	Src.port	Destination	Protocol	Lengtl	Info
1100	2022/293 10:46:22.281367	192.168.121.59	52678	128.119.245.12	HTTP	533	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
1259	2022/293 10:46:25.363281	128.119.245.12	80	192.168.121.59	HTTP	835	HTTP/1.1 200 OK (text/html)

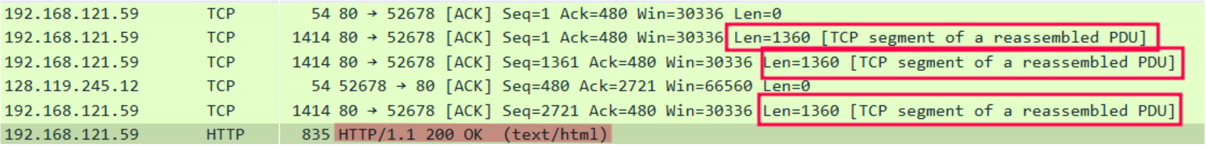
14. What is the status code and phrase in the response?

ANS – **Status-Code = 200 , Phrase = OK**



```
Info
GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
HTTP/1.1 200 OK  (text/html)
```

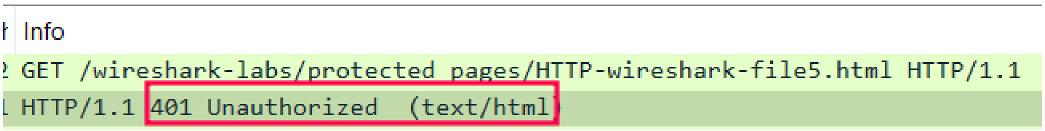
15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights? – **3 packets**



```
192.168.121.59        TCP       54 80 → 52678 [ACK] Seq=1 Ack=480 Win=30336 Len=0
192.168.121.59        TCP     1414 80 → 52678 [ACK] Seq=1 Ack=480 Win=30336 Len=1360 [TCP segment of a reassembled PDU]
192.168.121.59        TCP     1414 80 → 52678 [ACK] Seq=1361 Ack=480 Win=30336 Len=1360 [TCP segment of a reassembled PDU]
128.119.245.12        TCP       54 52678 → 80 [ACK] Seq=480 Ack=2721 Win=66560 Len=0
192.168.121.59        TCP     1414 80 → 52678 [ACK] Seq=2721 Ack=480 Win=30336 Len=1360 [TCP segment of a reassembled PDU]
192.168.121.59        HTTP     835 HTTP/1.1 200 OK  (text/html)
```

Q – HTTP Authentication Schmes (userland.com)
[http://frontier.userland.com/stories/storyReader$2159]

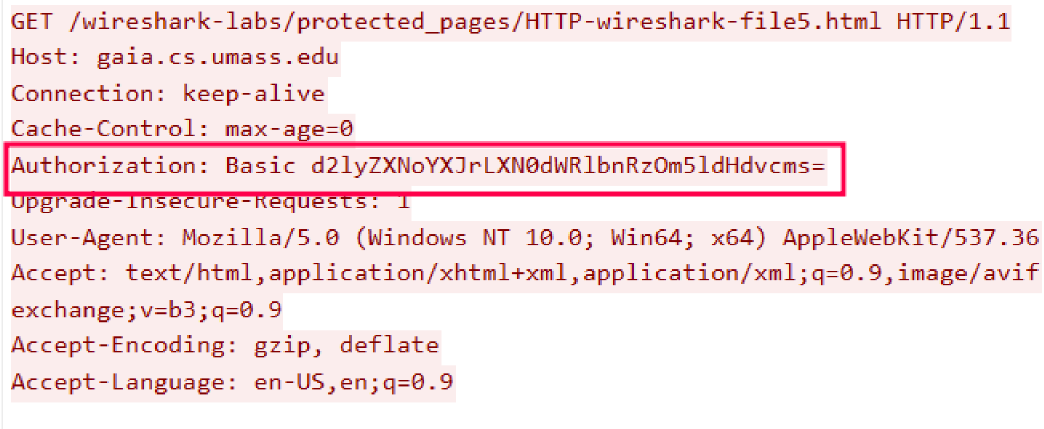
16. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser? – **401 UNAUTHORIZED**



```
Info
GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
HTTP/1.1 401 Unauthorized  (text/html)
```

17. When your browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

ANS – **AUTHORIZATION header with base64 encoded form of username and password.**



```
GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
Cache-Control: max-age=0
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

RESULT –

Thus the experiment to explore the Web application protocols using Protocol analysing tool called wireshark have been done practically .