



Lab 1

Packet Analysis at Application layer by using Wireshark Software

Objective:

1. To introduce student with Wireshark software tool for packet analyzer.
2. To analyze protocol used in application layer such as *http*, *ftp*, and *dns*.

Preliminary Works: Student is needed to install Wireshark and learn how to capture and analyze packet using steps that were provided in “Wireshark Lab: Getting Started v6.0 Supplement to Computer Networking: A Top-Down Approach, 6th ed., J.F. Kurose and K.W. Ross.

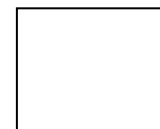
Name : _____

Section: _____

Name : _____

Section: _____

Date: _____



Checked By: _____

Mark

Lab #1: Use Wireshark to analyze captured file lab1.pcapng.

1a. Open the given file lab1.pcapng using Wireshark software. Filter packet connection to display only the *http* protocol transactions. Investigate *http* request made in frame number 90 at application layer. Consider the following HTTP GET message. Answer the following:

```
⊕ Frame 90: 760 bytes on wire (6080 bits), 760 bytes captured (6080 bits) on interface 0
⊕ Ethernet II, Src: QuantaCo_02:eb:19 (00:1e:68:02:eb:19), Dst: Cisco_d5:79:ff (00:14:6a:d5:79:ff)
⊕ Internet Protocol Version 4, Src: 10.60.80.213 (10.60.80.213), Dst: 161.139.21.50 (161.139.21.50)
⊕ Transmission Control Protocol, Src Port: nms-dpnss (2503), Dst Port: http (80), Seq: 1, Ack: 1, Len: 706
⊕ Hypertext Transfer Protocol
  * GET / HTTP/1.1\r\n
    Host: utmonline.utm.my\r\n
    User-Agent: Mozilla/5.0 (windows NT 5.1; rv:19.0) Gecko/20100101 Firefox/19.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    [truncated] Cookie: __utma=223080415.435223643.1321413706.1357014565.1357484172.13; __utmz=223080415.135
    Connection: keep-alive\r\n
    IF-Modified-Since: Tue, 05 Mar 2013 05:23:22 GMT\r\n
    If-None-Match: w/"c60f0-1464f-3f545e00"\r\n
    \r\n
    [Full request URI: http://utmonline.utm.my/]
  
```

- a. What is the URL, hostname, and filename requested?
- b. What version of HTTP is the browser running?
- c. Is the browser a Mozilla or an Internet Explorer?
- d. Is the browser requesting a non-persistent or a persistent connection? Justify.
- e. What is the IP address of the requesting computer?
- f. What type of transport protocol does this connection used?
- g. What port number does HTTP protocol communicate from client to server?

1b Consider the following HTTP reply message. The server reply is shown in frame number 185 as follows:

```

* Frame 185: 752 bytes on wire (6016 bits), 752 bytes captured (6016 bits) on interface 0
+ Ethernet II, Src: Cisco_d5:79:ff (00:14:6a:d5:79:ff), Dst: QuantaCo_02:eb:19 (00:1e:68:02:eb:19)
+ Internet Protocol Version 4, Src: 161.139.21.50 (161.139.21.50), Dst: 10.60.80.213 (10.60.80.213)
+ Transmission Control Protocol, Src Port: http (80), Dst Port: nms-dpns (2503), Seq: 82284, Ack: 707,
+ [62 Reassembled TCP Segments (82981 bytes): #92(275), #93(1380), #95(1380), #96(1380), #98(1380), #99
+ Hypertext Transfer Protocol
  + HTTP/1.1 200 OK\r\n
    Date: Tue, 05 Mar 2013 12:12:35 GMT\r\n
    Server: Apache\r\n
    Last-Modified: Tue, 05 Mar 2013 12:12:35 GMT\r\n
    ETag: w/"c60ff-14312-dd64b40"\r\n
    Accept-Ranges: bytes\r\n
  + Content-Length: 82706\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: keep-alive\r\n
    Content-Type: text/html\r\n
    \r\n
+ Line-based text data: text/html

```

Answer the following:

- a. Was the server able to find the document successfully or not?

- b. At what time was the document reply provided?

- c. When was the document last modified?

- d. How many bytes are there in the document being returned?

- e. Did the server agree to a persistent connection? Explain your answer.

1c. Consider the following HTTP GET message: Investigate *http* request made in frame number 210 at application layer and the server reply is shown in frame number 214 respectively as follows:

```
Frame 210: 693 bytes on wire (5544 bits), 693 bytes captured (5544 bits) on interface 0
Ethernet II, Src: QuantaCo_02:eb:19 (00:1e:68:02:eb:19), Dst: Cisco_d5:79:ff (00:14:6a:d5:79:ff)
Internet Protocol Version 4, Src: 10.60.80.213 (10.60.80.213), Dst: 161.139.21.50 (161.139.21.50)
Transmission Control Protocol, Src Port: nms-dpnss (2503), Dst Port: http (80), Seq: 707, Ack: 82982
Hypertext Transfer Protocol
GET /images/utm-news.jpg HTTP/1.1\r\n
Host: utmonline.utm.my\r\n
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:19.0) Gecko/20100101 Firefox/19.0\r\n
Accept: image/png, image/*; q=0.8, */*; q=0.5\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Referer: http://utmonline.utm.my/\r\n
[truncated] Cookie: __utma=223080415.435223643.1321413706.1357014565.1357484172.13; __utmz=2
Connection: keep-alive\r\n
\r\n
[Full request URI: http://utmonline.utm.my/images/utm-news.jpg]
```

```
Frame 214: 471 bytes on wire (3768 bits), 471 bytes captured (3768 bits) on interface 0
Ethernet II, Src: Cisco_d5:79:ff (00:14:6a:d5:79:ff), Dst: QuantaCo_02:eb:19 (00:1e:68:02:eb:19)
Internet Protocol Version 4, Src: 161.139.21.50 (161.139.21.50), Dst: 10.60.80.213 (10.60.80.213)
Transmission Control Protocol, Src Port: http (80), Dst Port: nms-dpnss (2503), Seq: 82982, Ack: 1346,
Hypertext Transfer Protocol
HTTP/1.1 404 Not Found\r\n
Date: Tue, 05 Mar 2013 12:12:36 GMT\r\n
Server: Apache\r\n
Content-Length: 217\r\n
Keep-Alive: timeout=5, max=99\r\n
Connection: keep-alive\r\n
Content-Type: text/html; charset=iso-8859-1\r\n
\r\n
Line-based text data: text/html
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
<html><head>\n
<title>404 Not Found</title>\n
</head><body>\n
<h1>Not Found</h1>\n
<p>The requested URL /images/utm-news.jpg was not found on this server.</p>\n
</body></html>\n
```

Answer the following:

- a. What is the URL, hostname, and filename requested?
- b. Was the server able to find the document successfully or not? Explain your answer.
- c. If the status code reply is 304, what does it mean? Explain your answer.

2. Filter packet connection to display only the *ftp* protocol. Investigate *ftp* transaction from frame number 4268 onward. Answer the following:

- a. List source and destination address for this ftp transaction?
- b. What transport protocol and port number does ftp used?
- c. Does ftp provide secure transaction? Explain.
- d. In the file content, can we trace the user ID and password used for ftp transaction? What is user ID and password used?
- e. From the tracing, list four commands that have been used in ftp transaction.

3. Filter packet connection to display only the *DNS* protocol transactions. Investigate *DNS* packet flows at frame number 191 and 192. Answer the following:

- a. What is the purpose of *DNS* application used for?
- b. List client and proxy address of these *DNS* transaction.

- c. What transport protocol and port number does *DNS* used?
- d. What is the query of client to proxy *DNS*?
- e. What is the response of client's query in (d) from proxy *DNS*?
- f. Briefly discuss why answer for client's query given in (e) by proxy *DNS* is more than one IP address?