UNIVERSITI TEKNOLOGI MALAYSIA

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 : _____

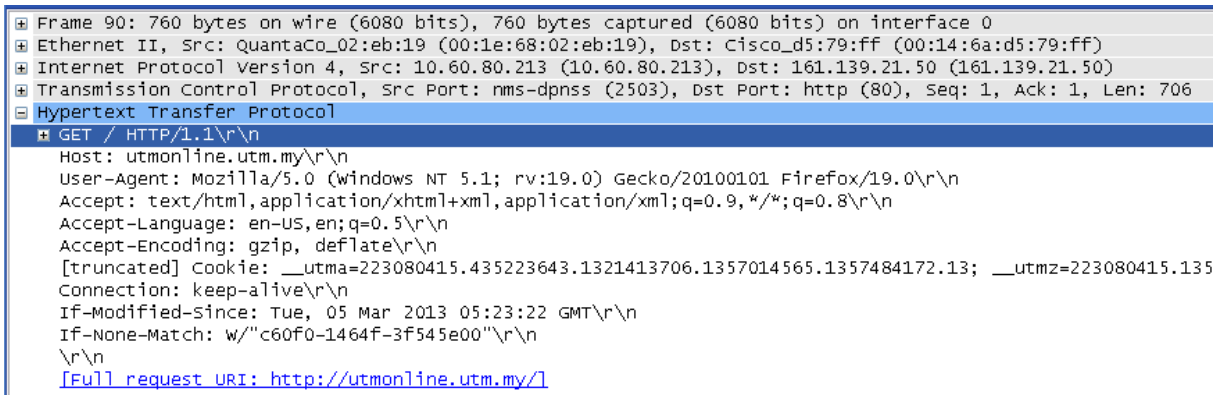
Section: _____

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:



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?

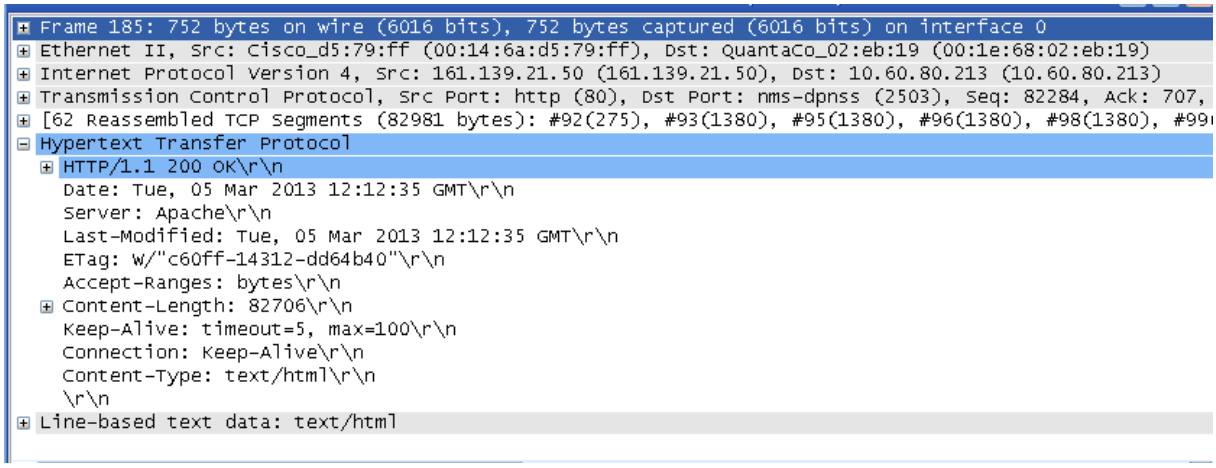
d. Is the browser requesting a non-persistent or a persistent connection? Justify.

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:



Answer the following:

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

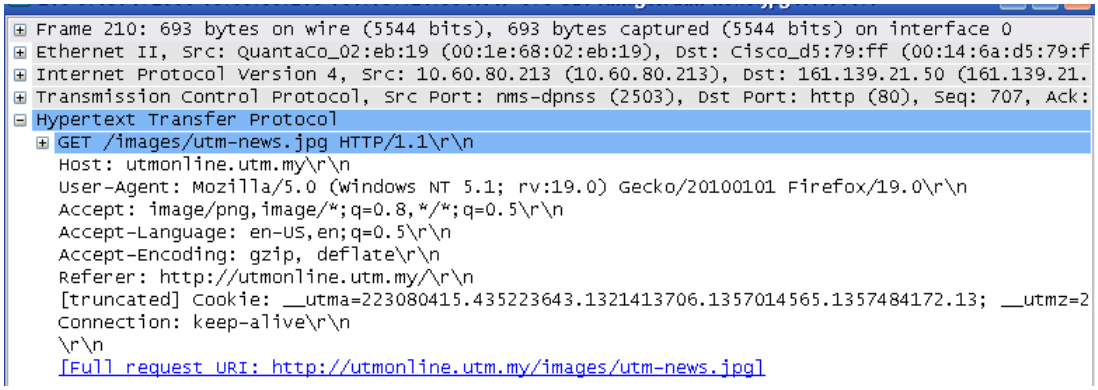
b. At what time was the document reply provided?

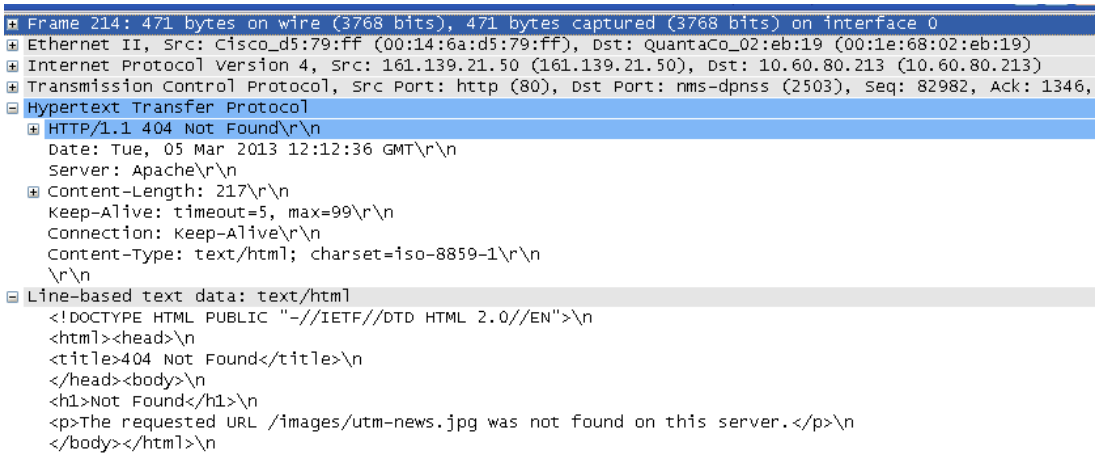
c. When was the document last modified?

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:.





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?