Christopher Bazyani

Practical Cyber Security

Unit 4

Packet Sniffing – HTTP

**Open the HTTP Trace**

Opening the http pcap file supplied

Text

Description automatically generated

**Inspect the Trace**

Filtering the HTTP requests and responses using the http filter

Text

Description automatically generated

First GET in the trace and expanding its HTTP block. This will be 802 GET /img/MIT\_logo.gif HTTP/1.1 as shown. Observing that the HTTP header follows the TCP and IP headers, as HTTP is an application protocol that is transported using TCP/IP.

Graphical user interface, text, application

Description automatically generated

Host, User-Agent, Accept, Accept-Encoding, Accept-Charset, Accept-Language, Cookies, and Cache-Control are listed in the hypertext transfer protocol of the HTTP block

Text, application

Description automatically generated

Selecting packet 4 which is the response that corresponds to the first GET in the trace and expanding its HTTP block



Sever, last modified, expiration, data and Etag are listed below according to the HTTP block

Text, letter

Description automatically generated

**Content Caching**

Third line in the sample trace i.e. 892 GET /img/MIT\_logo.gif HTTP 1.1



Expanding the block

Graphical user interface, text, application

Description automatically generated

The header that will let the server work out whether it needs to send fresh content is called the If-Modified-Since following by the date when expanding the cookie in the hypertext transfer protocol block

Text, letter

Description automatically generated

**Complex Pages**

Click on number 34 which is 750 GET / HTTP/1.1



Summarize the GETs for this page by bringing up a HTTP Load Distribution panel

Graphical user interface

Description automatically generated

This is the load distribution page

**Graphical user interface, application, table

Description automatically generated**

Bringing up an HTTP Packet Counter panel

**Graphical user interface, text, application

Description automatically generated**