實驗一
網路協定觀察與分析
HTTP Protocol

計算機網路 Computer Network

實驗目的

- 了解網路協定(network protocol)在網路環境中所扮演的角色
- 透過實際觀察封包的組成及特定協定的運作，了解通訊協定層的意義和網路運作的機制。
- 熟悉網路封包分析軟體(wireshark)的操作

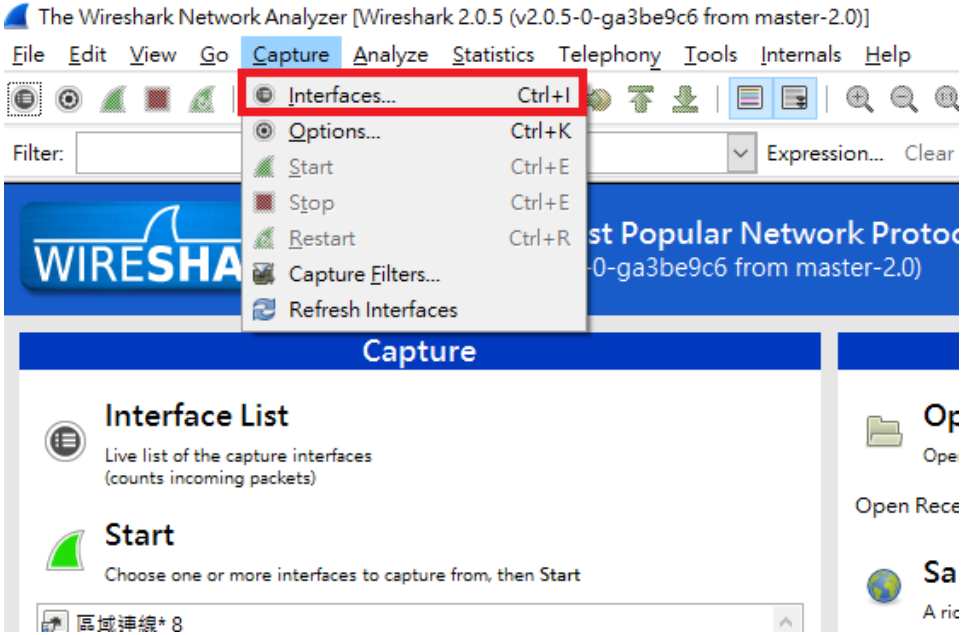
實驗步驟

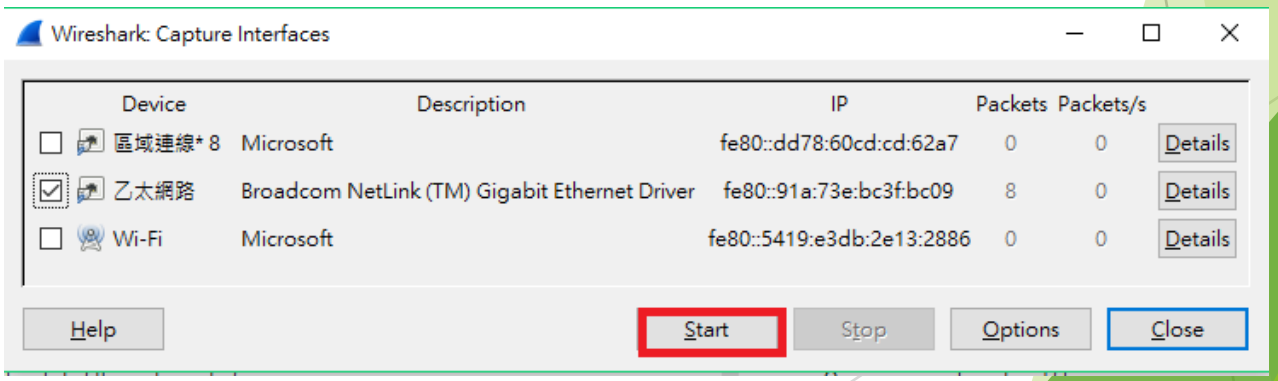
1. 下載安裝Wireshark並開啟
2. 瀏覽不同網頁，並逐步觀察HTTP封包分析內容
3. 回答相關問題

Wireshark 簡介
為Open source 網路封包分析軟體
支援大部分的網路協定
目的：
檢測網路問題，檢查資訊安全相關問題，為通訊協定除錯，學習網路協定的相關知識

安裝

1.請至https://www.wireshark.org/下載
2.安裝過程中，若無WinPcap請務必安裝，有則確認是否為最新版本


The Wireshark Network Analyzer [Wireshark 2.0.5 (v2.0.5-0-ga3be9c6 from master-2.0)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Interfaces... Ctrl+I
Options... Ctrl+K
Start Ctrl+E
Stop Ctrl+E
Restart Ctrl+R
Capture Filters...
Refresh Interfaces
Filter:
Expression... Clear
Capture
Interface List
Live list of the capture interfaces
(counts incoming packets)
Start
Choose one or more interfaces to capture from, then Start
區域連線* 8
Open Rece


Wireshark: Capture Interfaces
Device
Description
IP
Packets
Packets/s
區域連線* 8
Microsoft
fe80::dd78:60cd:cd:62a7
0
0
Details
乙太網路
Broadcom NetLink (TM) Gigabit Ethernet Driver
fe80::91a:73e:bc3f:bc09
8
0
Details
Wi-Fi
Microsoft
fe80::5419:e3db:2e13:2886
0
0
Details
Help
Start
Stop
Options
Close

一、基礎HTTP GET/response互動

步驟：

1.啟動瀏覽器

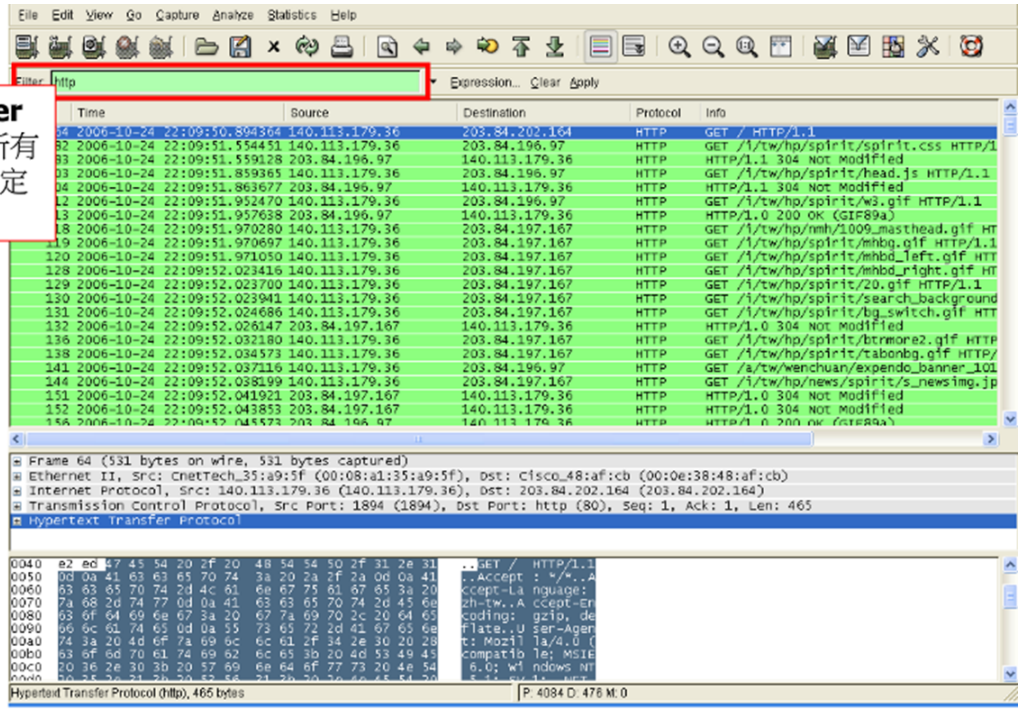
2.啟動wireshark，但先不要開始擷取封包，請在Filter欄位輸入「http」，使清單只顯示和http協定有關的封包，在按start開始擷取封包。

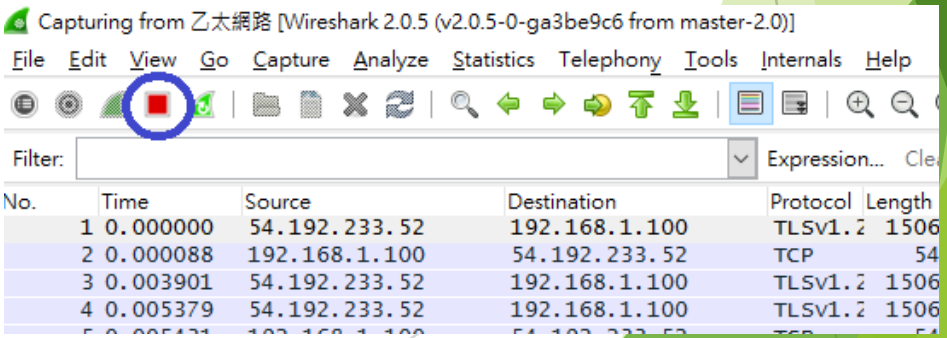
3.請在瀏覽器輸入以下網址

http://www.cs.nccu.edu.tw/~jang/welcome.html

4.停止擷取封包，觀察其分析內容

使用**filter**來篩選所有**HTTP**協定的封包





問題：

1.請問瀏覽器的HTTP版本為何？伺服器的HTTP版本為何？(1.0或1.1?) 請用圖片說明，如何找出

2.請問你的瀏覽器可以辨識何種語言？請用圖片說明如何找出。

3.請問伺服器的IP位址為何？

回傳至瀏覽器的內容大小為何？

4.請問從伺服器回傳的status code為何？

請用圖片說明如何找出

(Hint：從Hypertext Transfer Protocol找)

HTTP Messages -- Status Codes

- 1XX : Informational
- 2XX : Success
- 3XX : Redirection (further actions needed)
- 4XX : Client error
- 5XX : Server error

Examples.
100 : Continue
201 : Created
302 : Multiple choices
403 : Forbidden
504 : Gateway time-out

二、HTTP條件式 GET/response互動

1.啟動瀏覽器，確認瀏覽器的快取已清空。

2.啟動Wireshark，開始擷取封包。

3.在瀏覽器中輸入以下網址：

http://www.cs.nccu.edu.tw/~jang/teaching.html

4.再次輸入同一網址或按重新整理

5.停止擷取封包，並在filter輸入「http」。

問題：

1.檢查第一個從瀏覽器至伺服器HTTP GET指令的內容，是否看到HTTP GET裡有IF-MODIFIED-SINCE？

2.檢查第二個從瀏覽器至伺服器HTTP GET指令的內容，是否看到HTTP GET裡有IF-MODIFIED-SINCE?如果有，IF-MODIFIED-SINCE
標頭有哪些資訊？

二、HTTP授權

1.啟動瀏覽器，確認瀏覽器的快取已清空。

2.啟動Wireshark，開始擷取封包。

3.在瀏覽器中輸入以下網址：

https://i.nccu.edu.tw/Login.aspx?ReturnUrl=%2fdefault.aspx

在登入頁面輸入帳號、密碼

4.停止擷取封包，並在filter輸入「http」。


愛 政 大
iNCCU
校 園 個 人 化 入 口
政大首頁
English
帳號/學號
@nccu.edu.tw
密碼
記住我的帳號密碼
登入
建立帳戶
無法登入?

問題

1.請觀察瀏覽器一開始傳送HTTP GET訊息後，得到的伺服器回應是甚麼？

2.登入帳號、密碼後，即第二次傳送HTTP GET訊息是為何時？

3.此時的HTTP GET訊息和1.有何不同？請以文字說明

作業

請使用DOC檔繳交作業

必須說明：

1. 封面(班級、學號、姓名)
   檔名範例:Hw1_105XXXXXX_陳君虹
2. 請回答上述投影片的9個問題，將找到的答案截圖貼上，並作註解說明。
3. 實驗心得

請將問題、答案和圖片標示清楚，以便助教批改。

若有問題請e-mail 給助教.