



# 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

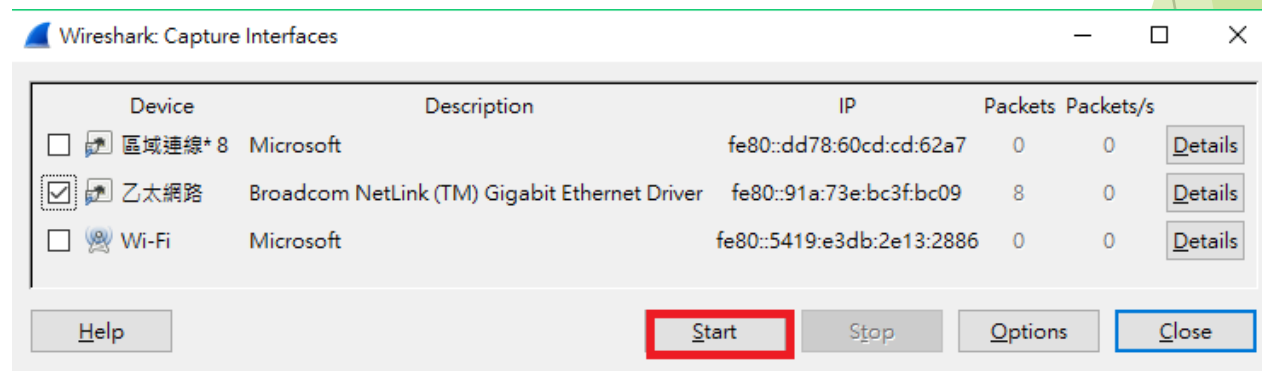
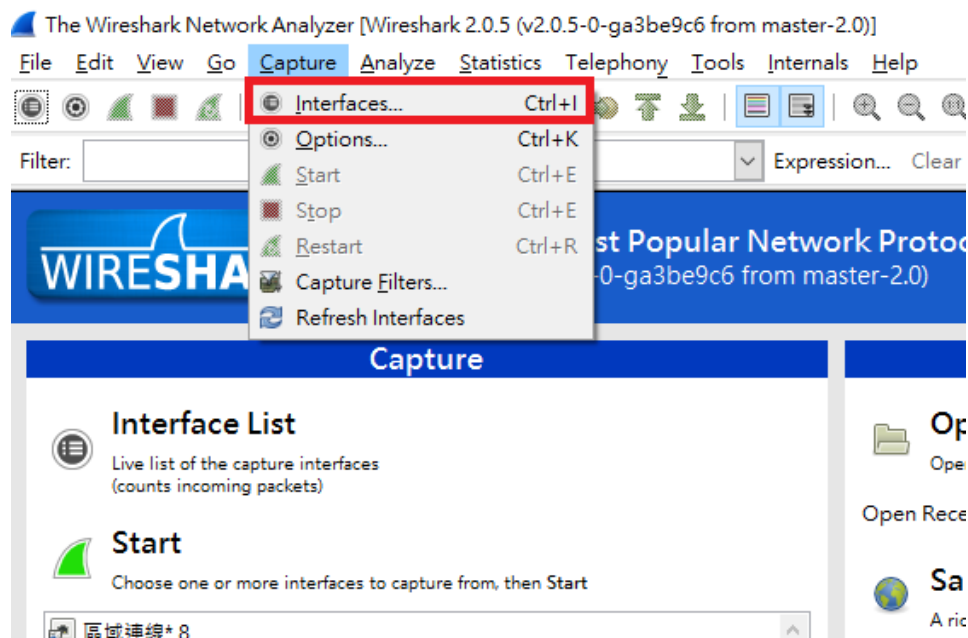
支援大部分的網路協定

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



# 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

Filter: http

No.	Time	Source	Destination	Protocol	Info
64	2006-10-24 22:09:50.894364	140.113.179.36	203.84.202.164	HTTP	GET / HTTP/1.1
65	2006-10-24 22:09:51.594531	140.113.179.36	203.84.202.164	HTTP	GET /i/tw/hp/spirit/spirit.css HTTP/1.1
66	2006-10-24 22:09:51.599228	203.84.202.164	140.113.179.36	HTTP	HTTP/1.1 304 Not Modified
67	2006-10-24 22:09:51.859365	140.113.179.36	203.84.202.164	HTTP	GET /i/tw/hp/spirit/head.js HTTP/1.1
68	2006-10-24 22:09:51.863677	203.84.202.164	140.113.179.36	HTTP	HTTP/1.1 304 Not Modified
69	2006-10-24 22:09:51.952470	140.113.179.36	203.84.202.164	HTTP	GET /i/tw/hp/spirit/w3.gif HTTP/1.1
70	2006-10-24 22:09:51.957638	203.84.202.164	140.113.179.36	HTTP	HTTP/1.0 200 OK (GIF89a)
71	2006-10-24 22:09:51.970280	140.113.179.36	203.84.202.164	HTTP	GET /i/tw/hp/nmh/1009_masthead.gif HTTP/1.1
72	2006-10-24 22:09:51.970697	140.113.179.36	203.84.202.164	HTTP	GET /i/tw/hp/spirit/mhbg.gif HTTP/1.1
73	2006-10-24 22:09:51.971050	140.113.179.36	203.84.202.164	HTTP	GET /i/tw/hp/spirit/mhbg_left.gif HTTP/1.1
74	2006-10-24 22:09:52.023416	140.113.179.36	203.84.202.164	HTTP	GET /i/tw/hp/spirit/mhbg_right.gif HTTP/1.1
75	2006-10-24 22:09:52.023700	140.113.179.36	203.84.202.164	HTTP	GET /i/tw/hp/spirit/20.gif HTTP/1.1
76	2006-10-24 22:09:52.023941	140.113.179.36	203.84.202.164	HTTP	GET /i/tw/hp/spirit/search_background.gif HTTP/1.1
77	2006-10-24 22:09:52.024686	140.113.179.36	203.84.202.164	HTTP	GET /i/tw/hp/spirit/bg_switch.gif HTTP/1.1
78	2006-10-24 22:09:52.026147	203.84.202.164	140.113.179.36	HTTP	HTTP/1.0 304 Not Modified
79	2006-10-24 22:09:52.032180	140.113.179.36	203.84.202.164	HTTP	GET /i/tw/hp/spirit/btrmore2.gif HTTP/1.1
80	2006-10-24 22:09:52.034571	140.113.179.36	203.84.202.164	HTTP	GET /i/tw/hp/spirit/tabonbg.gif HTTP/1.1
81	2006-10-24 22:09:52.037216	140.113.179.36	203.84.202.164	HTTP	GET /a/tw/wenhuang/expand_banner_101.gif HTTP/1.1
82	2006-10-24 22:09:52.038199	140.113.179.36	203.84.202.164	HTTP	GET /i/tw/hp/news/spirit/s_newsimg.jpg HTTP/1.1
83	2006-10-24 22:09:52.041921	203.84.202.164	140.113.179.36	HTTP	HTTP/1.0 304 Not Modified
84	2006-10-24 22:09:52.043853	203.84.202.164	140.113.179.36	HTTP	HTTP/1.0 304 Not Modified
85	2006-10-24 22:09:52.044473	203.84.202.164	140.113.179.36	HTTP	HTTP/1.0 200 OK (GIF89a)

Frame 64 (531 bytes on wire (531 bytes captured))

Ethernet II, Src: CnetTech\_35:a9:5f (00:08:a1:35:a9:5f), Dst: Cisco\_48:af:cb (00:0e:38:48:af:cb)

Internet Protocol, Src: 140.113.179.36 (140.113.179.36), Dst: 203.84.202.164 (203.84.202.164)

Transmission Control Protocol, Src Port: 1894 (1894), Dst Port: http (80), Seq: 1, Ack: 1, Len: 465

Hypertext Transfer Protocol

0040 e2 ed 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 ..GET / HTTP/1.1

0050 00 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 41 ..Accept: \*/\*..

0060 52 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 ..Accept-Language: zh-tw..

0070 7a 68 2d 74 77 0d 0a 41 63 63 65 70 74 2d 45 6e ..Accept-Encoding: gzip, deflate..

0080 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 ..Accept-Charset: utf-8..

0090 66 6c 61 74 65 0d 0a 55 73 65 72 2d 41 67 65 6e ..User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4324) ..

00a0 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 34 2e 30 20 28 ..Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4324) ..

00b0 63 6f 6d 70 61 74 69 62 6c 63 30 20 4d 53 49 45 ..Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4324) ..

00c0 20 3e 2e 30 30 20 57 69 6e 64 6f 77 73 20 4e 54 ..Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4324) ..

00d0 2a 2e 3a 2a 2e 3a 2e 3a 2a 2e 3a 2e 3a 2e 3a 2e ..Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4324) ..

Hypertext Transfer Protocol (http), 465 bytes

P: 4084 D: 478 M: 0

Capturing from 乙太網路 [Wireshark 2.0.5 (v2.0.5-0-ga3be9c6 from master-2.0)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear

No.	Time	Source	Destination	Protocol	Length
1	0.000000	54.192.233.52	192.168.1.100	TLSv1.2	1506
2	0.000088	192.168.1.100	54.192.233.52	TCP	54
3	0.003901	54.192.233.52	192.168.1.100	TLSv1.2	1506
4	0.005379	54.192.233.52	192.168.1.100	TLSv1.2	1506

## 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」。

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.