0416005 資工 08 張彧豪

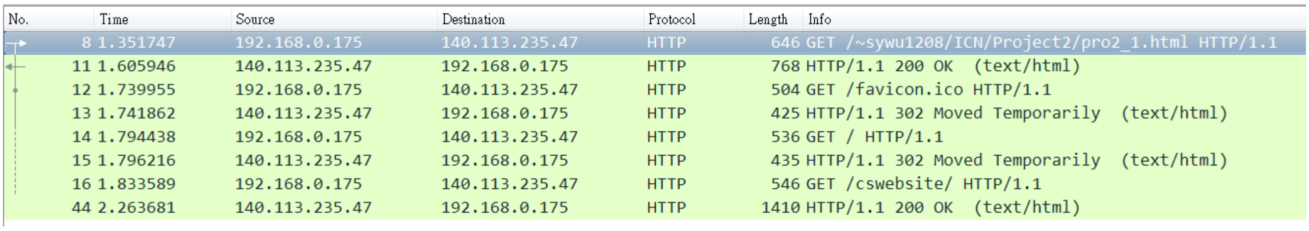
ICN Project 2 Report

- 實驗環境：

1. OS：Windows 7 Ultimate SP1
2. 網卡型號：Intel Ethernet Connection I217-V
3. 實驗用瀏覽器：Opera Developer 42.0.2392.0 無痕模式
4. IP：192.168.0.175

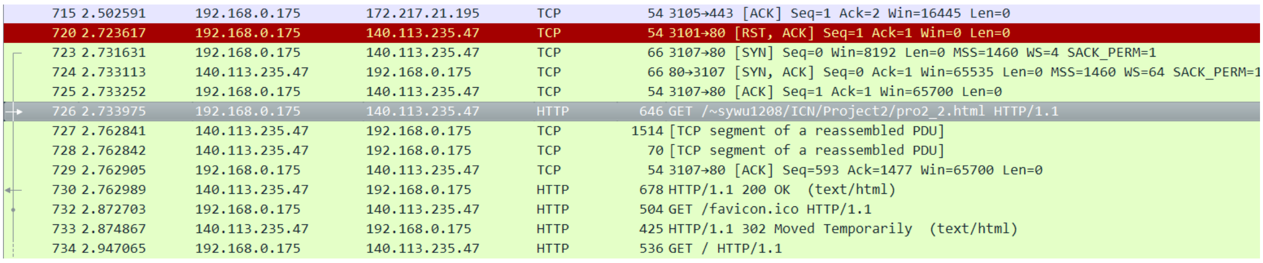
一、 實驗一問題回答

1. 當連上短內容網頁時，我的 browser 共發出了 1 個 HTTP GET request message。



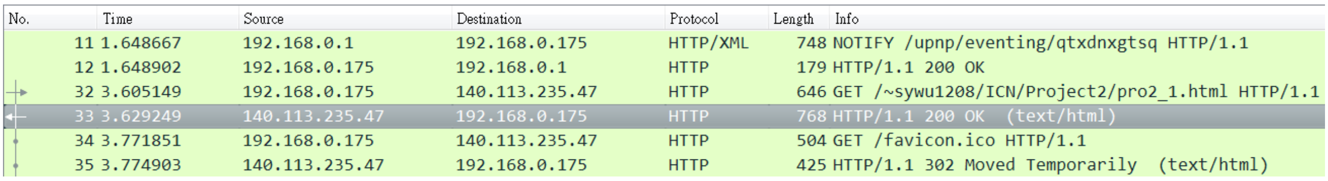
No.	Time	Source	Destination	Protocol	Length	Info
8	1.351747	192.168.0.175	140.113.235.47	HTTP	646	GET /~sywu1208/ICN/Project2/pro2_1.html HTTP/1.1
11	1.605946	140.113.235.47	192.168.0.175	HTTP	768	HTTP/1.1 200 OK (text/html)
12	1.739955	192.168.0.175	140.113.235.47	HTTP	504	GET /favicon.ico HTTP/1.1
13	1.741862	140.113.235.47	192.168.0.175	HTTP	425	HTTP/1.1 302 Moved Temporarily (text/html)
14	1.794438	192.168.0.175	140.113.235.47	HTTP	536	GET / HTTP/1.1
15	1.796216	140.113.235.47	192.168.0.175	HTTP	435	HTTP/1.1 302 Moved Temporarily (text/html)
16	1.833589	192.168.0.175	140.113.235.47	HTTP	546	GET /cswebsite/ HTTP/1.1
44	2.263681	140.113.235.47	192.168.0.175	HTTP	1410	HTTP/1.1 200 OK (text/html)

2. 當連上短內容網頁時，我的 browser 共發出了 1 個 HTTP GET request message。



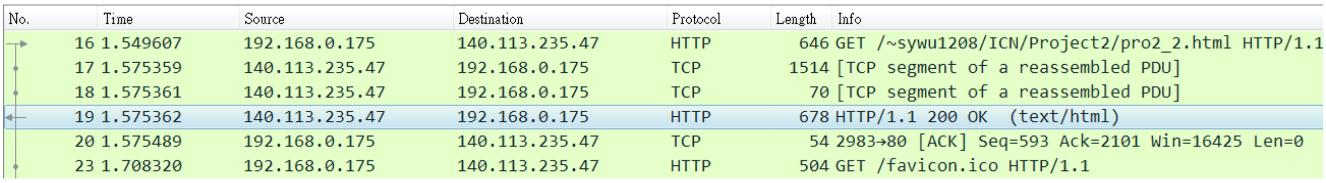
715	2.502591	192.168.0.175	172.217.21.195	TCP	54	3105→443 [ACK] Seq=1 Ack=2 Win=16445 Len=0
720	2.723617	192.168.0.175	140.113.235.47	TCP	54	3101→80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
723	2.731631	192.168.0.175	140.113.235.47	TCP	66	3107→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
724	2.733113	140.113.235.47	192.168.0.175	TCP	66	80→3107 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM=1
725	2.733252	192.168.0.175	140.113.235.47	TCP	54	3107→80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
726	2.733975	192.168.0.175	140.113.235.47	HTTP	646	GET /~sywu1208/ICN/Project2/pro2_2.html HTTP/1.1
727	2.762841	140.113.235.47	192.168.0.175	TCP	1514	[TCP segment of a reassembled PDU]
728	2.762842	140.113.235.47	192.168.0.175	TCP	70	[TCP segment of a reassembled PDU]
729	2.762905	192.168.0.175	140.113.235.47	TCP	54	3107→80 [ACK] Seq=593 Ack=1477 Win=65700 Len=0
730	2.762989	140.113.235.47	192.168.0.175	HTTP	678	HTTP/1.1 200 OK (text/html)
732	2.872703	192.168.0.175	140.113.235.47	HTTP	504	GET /favicon.ico HTTP/1.1
733	2.874867	140.113.235.47	192.168.0.175	HTTP	425	HTTP/1.1 302 Moved Temporarily (text/html)
734	2.947065	192.168.0.175	140.113.235.47	HTTP	536	GET / HTTP/1.1

3. 短網頁的 data-containing segment 是一個，No.33 即是該 TCP segment，雖然顯示是 HTTP 協議，但內部仍有 TCP segment。



No.	Time	Source	Destination	Protocol	Length	Info
11	1.648667	192.168.0.1	192.168.0.175	HTTP/XML	748	NOTIFY /upnp/eventing/qtxdnxgtsq HTTP/1.1
12	1.648902	192.168.0.175	192.168.0.1	HTTP	179	HTTP/1.1 200 OK
32	3.605149	192.168.0.175	140.113.235.47	HTTP	646	GET /~sywu1208/ICN/Project2/pro2_1.html HTTP/1.1
33	3.629249	140.113.235.47	192.168.0.175	HTTP	768	HTTP/1.1 200 OK (text/html)
34	3.771851	192.168.0.175	140.113.235.47	HTTP	504	GET /favicon.ico HTTP/1.1
35	3.774903	140.113.235.47	192.168.0.175	HTTP	425	HTTP/1.1 302 Moved Temporarily (text/html)

而長網頁的 data-containing segment 為三個，No.17、No.18、No.19 皆是 data containing segment。

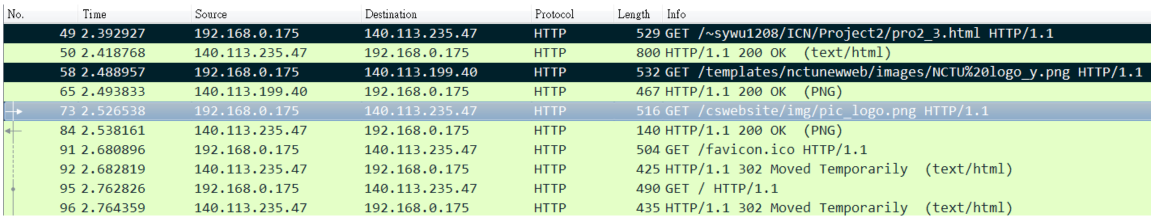


No.	Time	Source	Destination	Protocol	Length	Info
16	1.549607	192.168.0.175	140.113.235.47	HTTP	646	GET /~sywu1208/ICN/Project2/pro2_2.html HTTP/1.1
17	1.575359	140.113.235.47	192.168.0.175	TCP	1514	[TCP segment of a reassembled PDU]
18	1.575361	140.113.235.47	192.168.0.175	TCP	70	[TCP segment of a reassembled PDU]
19	1.575362	140.113.235.47	192.168.0.175	HTTP	678	HTTP/1.1 200 OK (text/html)
20	1.575489	192.168.0.175	140.113.235.47	TCP	54	2983→80 [ACK] Seq=593 Ack=2101 Win=16425 Len=0
23	1.708320	192.168.0.175	140.113.235.47	HTTP	504	GET /favicon.ico HTTP/1.1

4. 回應的 status code 為 200，phrase 為 OK。
5. 而第一張圖的 No.12 及第二張圖的 No.732 不算的原因是 icon 不在網頁的 html 裡，它是分頁欄最左方的那個 icon，故不算在 icon 內。

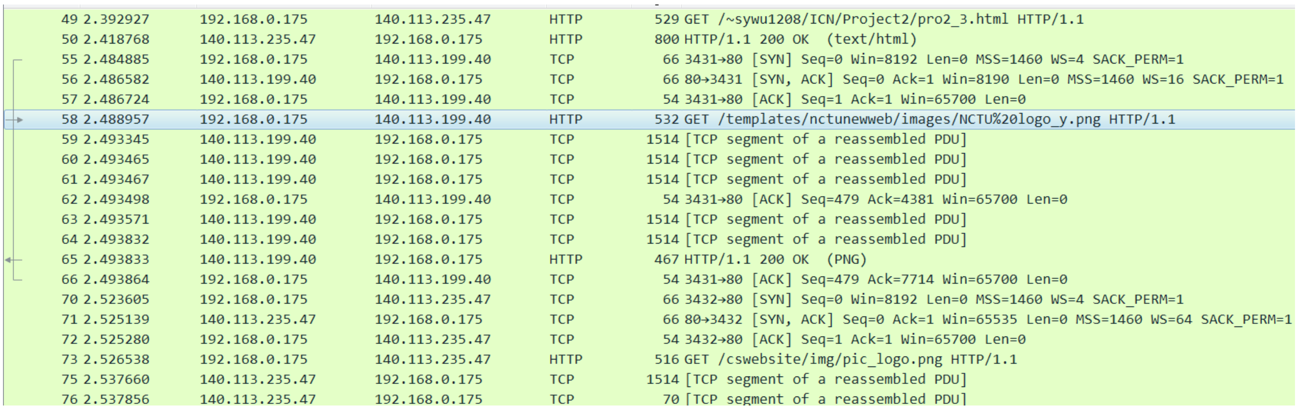
二、 實驗二問題回答：

1. 我的瀏覽器一共送出三個 HTTP GET request message。
   I. 第一個 request 送往的網址是：
   http://people.cs.nctu.edu.tw/~sywu1208/ICN/Project2/pro2_3.html
   II. 第二個 request 送往的網址是：
   http://www.nctu.edu.tw/templates/nctunewweb/images/NCTU%20logo_y.png
   III. 第三個 request 送往的網址是：
   http://www.cs.nctu.edu.tw/cswebsite/img/pic_logo.png
   截圖如下頁所示：



```
No.     Time        Source           Destination      Protocol  Length  Info
   49 2.392927    192.168.0.175    140.113.235.47   HTTP       529 GET /~sywu1208/ICN/Project2/pro2_3.html HTTP/1.1
   50 2.418768    140.113.235.47   192.168.0.175    HTTP       800 HTTP/1.1 200 OK  (text/html)
   58 2.488957    192.168.0.175    140.113.199.40   HTTP       532 GET /templates/nctunewweb/images/NCTU%20logo_y.png HTTP/1.1
   65 2.493833    140.113.199.40   192.168.0.175    HTTP       467 HTTP/1.1 200 OK  (PNG)
   73 2.526538    192.168.0.175    140.113.235.47   HTTP       516 GET /cswebsite/img/pic_logo.png HTTP/1.1
   84 2.538161    140.113.235.47   192.168.0.175    HTTP       140 HTTP/1.1 200 OK  (PNG)
   91 2.680896    192.168.0.175    140.113.235.47   HTTP       504 GET /favicon.ico HTTP/1.1
   92 2.682819    140.113.235.47   192.168.0.175    HTTP       425 HTTP/1.1 302 Moved Temporarily  (text/html)
   95 2.762826    192.168.0.175    140.113.235.47   HTTP       490 GET / HTTP/1.1
   96 2.764359    140.113.235.47   192.168.0.175    HTTP       435 HTTP/1.1 302 Moved Temporarily  (text/html)
```

2. 我的瀏覽器是平行下載的，因為根據 wireshark 所擷取的 HTTP 及 TCP 封包順序所得出的結論。
   wireshark 截圖：

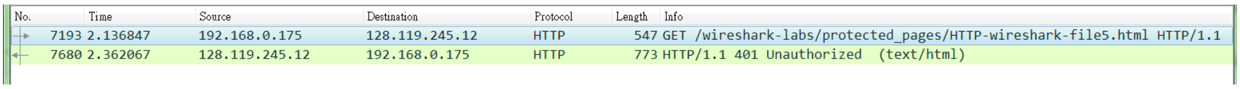


```
   49 2.392927    192.168.0.175    140.113.235.47   HTTP       529 GET /~sywu1208/ICN/Project2/pro2_3.html HTTP/1.1
   50 2.418768    140.113.235.47   192.168.0.175    HTTP       800 HTTP/1.1 200 OK  (text/html)
   55 2.484885    192.168.0.175    140.113.199.40   TCP         66 3431→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
   56 2.486582    140.113.199.40   192.168.0.175    TCP         66 80→3431 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1460 WS=16 SACK_PERM=1
   57 2.486724    192.168.0.175    140.113.199.40   TCP         54 3431→80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
   58 2.488957    192.168.0.175    140.113.199.40   HTTP       532 GET /templates/nctunewweb/images/NCTU%20logo_y.png HTTP/1.1
   59 2.493345    140.113.199.40   192.168.0.175    TCP       1514 [TCP segment of a reassembled PDU]
   60 2.493465    140.113.199.40   192.168.0.175    TCP       1514 [TCP segment of a reassembled PDU]
   61 2.493467    140.113.199.40   192.168.0.175    TCP       1514 [TCP segment of a reassembled PDU]
   62 2.493498    192.168.0.175    140.113.199.40   TCP         54 3431→80 [ACK] Seq=479 Ack=4381 Win=65700 Len=0
   63 2.493571    140.113.199.40   192.168.0.175    TCP       1514 [TCP segment of a reassembled PDU]
   64 2.493832    140.113.199.40   192.168.0.175    TCP       1514 [TCP segment of a reassembled PDU]
   65 2.493833    140.113.199.40   192.168.0.175    HTTP       467 HTTP/1.1 200 OK  (PNG)
   66 2.493864    192.168.0.175    140.113.199.40   TCP         54 3431→80 [ACK] Seq=479 Ack=7714 Win=65700 Len=0
   70 2.523605    192.168.0.175    140.113.235.47   TCP         66 3432→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
   71 2.525139    140.113.235.47   192.168.0.175    TCP         66 80→3432 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM=1
   72 2.525280    192.168.0.175    140.113.235.47   TCP         54 3432→80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
   73 2.526538    192.168.0.175    140.113.235.47   HTTP       516 GET /cswebsite/img/pic_logo.png HTTP/1.1
   75 2.537660    140.113.235.47   192.168.0.175    TCP       1514 [TCP segment of a reassembled PDU]
   76 2.537856    140.113.235.47   192.168.0.175    TCP         70 [TCP segment of a reassembled PDU]
```

No.58 才打出 HTTP Request 要求第一張圖片，但 No.55 已經開始去建第一張圖片的 TCP 連線了，且 No.70 開始建下一張圖片的 TCP 連線，但 No.73 才打出 HTTP Request，由上述現象可判斷應該是平行下載。至於為何兩次的 TCP 連線建立有延遲應該可判斷是因為 CPU 執行時間所導致。

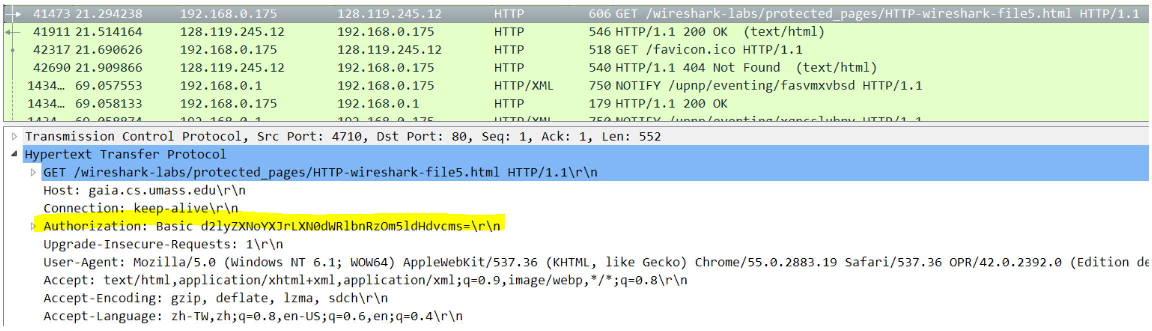
三、 實驗三問題回答：

1. 第一次的發出的 HTTP GET message 得到的回應為 status code 為 401，phrase 為 Unauthorized。



```
No.   Time        Source          Destination     Protocol  Length  Info
7193 2.136847     192.168.0.175   128.119.245.12  HTTP      547 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
7680 2.362067     128.119.245.12  192.168.0.175   HTTP      773 HTTP/1.1 401 Unauthorized  (text/html)
```

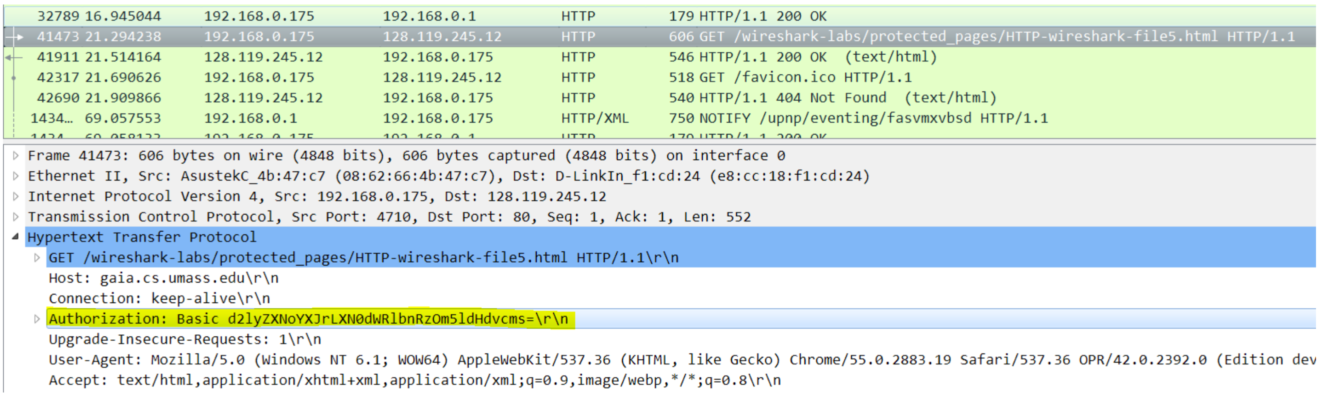
2. 在第二次發出的 HTTP GET message 中我發現到一個叫做 Authorization 的新 filed。



```
41473 21.294238   192.168.0.175   128.119.245.12  HTTP      606 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
41911 21.514164   128.119.245.12  192.168.0.175   HTTP      546 HTTP/1.1 200 OK  (text/html)
42317 21.690626   192.168.0.175   128.119.245.12  HTTP      518 GET /favicon.ico HTTP/1.1
42690 21.909866   128.119.245.12  192.168.0.175   HTTP      540 HTTP/1.1 404 Not Found  (text/html)
1434… 69.057553   192.168.0.1     192.168.0.175   HTTP/XML  750 NOTIFY /upnp/eventing/fasvmxvbsd HTTP/1.1
1434… 69.058133   192.168.0.175   192.168.0.1     HTTP      179 HTTP/1.1 200 OK

▷ Transmission Control Protocol, Src Port: 4710, Dst Port: 80, Seq: 1, Ack: 1, Len: 552
◢ Hypertext Transfer Protocol
  ▷ GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
  ▷ Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.19 Safari/537.36 OPR/42.0.2392.0 (Edition de
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate, lzma, sdch\r\n
    Accept-Language: zh-TW,zh;q=0.8,en-US;q=0.6,en;q=0.4\r\n
```

3. 在封包的確可以找到帳號跟密碼，如下圖所示：



```
32789 16.945044   192.168.0.175   192.168.0.1     HTTP      179 HTTP/1.1 200 OK
41473 21.294238   192.168.0.175   128.119.245.12  HTTP      606 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
41911 21.514164   128.119.245.12  192.168.0.175   HTTP      546 HTTP/1.1 200 OK  (text/html)
42317 21.690626   192.168.0.175   128.119.245.12  HTTP      518 GET /favicon.ico HTTP/1.1
42690 21.909866   128.119.245.12  192.168.0.175   HTTP      540 HTTP/1.1 404 Not Found  (text/html)
1434… 69.057553   192.168.0.1     192.168.0.175   HTTP/XML  750 NOTIFY /upnp/eventing/fasvmxvbsd HTTP/1.1

▷ Frame 41473: 606 bytes on wire (4848 bits), 606 bytes captured (4848 bits) on interface 0
▷ Ethernet II, Src: AsustekC_4b:47:c7 (08:62:66:4b:47:c7), Dst: D-LinkIn_f1:cd:24 (e8:cc:18:f1:cd:24)
▷ Internet Protocol Version 4, Src: 192.168.0.175, Dst: 128.119.245.12
▷ Transmission Control Protocol, Src Port: 4710, Dst Port: 80, Seq: 1, Ack: 1, Len: 552
◢ Hypertext Transfer Protocol
  ▷ GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
  ▷ Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.19 Safari/537.36 OPR/42.0.2392.0 (Edition dev
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
```

Authorization 即是認證標頭檔，它被放在 HTTP 的標頭檔內。它產生的方式是將我打入的帳號與密碼中間加一個冒號後以 Base64 的編碼方法進行編碼後放入認證標頭檔，並在其編碼結果放入 " Basic " 這一個字串，表示其認證方法為 Basic(基本認證)，空格分隔帳號密碼與認證方法。

加密過的帳號密碼：d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=

四、 心得

這次的作業是我做到現在覺得最難的作業，每一題都蠻有挑戰性的，尤其是第一題，真的困惱我很久，為什麼會去 get 那個 icon 以及 data-containing TCP segment 的數量。其次應該是第二題的分析是否為同步下載，這要仔細觀察，不過這也讓我看到瀏覽器其實是平行下載這些物件。第三題應該算是最簡單的，找出兩次 request 中不同的 HTTP filed 再將其解碼即可得到原本打入的帳號密碼，但是我覺得第三題蠻有趣的，可以了解 HTTP 是怎麼做到基本認證的。這次的作業雖然難，但是也學到了不少有關於 HTTP 跟 TCP 封包的分析方法。