Have you once imaged that you go to the Starbucks ,order one coffee, pick a seat, open your laptop , choose the wi-fi ”Starbucks public” and open the browser connect to the Facebook or PTT , but meanwhile another guy sitting beside you are watching the same pages as yours in his screen? This may happen in real world! It’s package wiretapping, a method which listens the package sent in/out through your laptop. By create a fake wi-fi AP and analysis packages sent in and out, another guy may establish the same image which displays on your screen and know all the information (if the packages are not encrypted).

I would like to introduce the software Wireshark , a tool (a sniffer) listen the package through your computer. Wireshark is the world's foremost network protocol analyzer. It lets you capture and interactively browse the traffic running on a computer network. It is the de facto (and often de jure) standard across many industries and educational institutions.

The simplest procedure is just steps:

1. Download and install the software.
2. Open and start capturing.
3. Analysis the package you get.

Let me take connecting to ptt.cc using telnet for example : when I open PCMAN, connect to ptt.cc and type in my account “tim” and password 1234, the captured packages my like this:

```
0000   28 94 0f 61 be 43 10 bf   48 4d eb aa 08 00 45 00   (..a.C.. HM....E.
0010   00 29 4e f0 40 00 80 06   00 00 8c 70 12 d0 8c 70   .)N.@... ...p...p
0020   ac 01 06 91 00 17 93 37   d2 48 0a e2 89 a9 50 18   .......7 .H....P.
0030   40 29 d7 cd 00 00 74                               @)....t

0000   28 94 0f 61 be 43 10 bf   48 4d eb aa 08 00 45 00   (..a.C.. HM....E.
0010   00 29 4e f1 40 00 80 06   00 00 8c 70 12 d0 8c 70   .)N.@... ...p...p
0020   ac 01 06 91 00 17 93 37   d2 49 0a e2 89 aa 50 18   .......7 .I....P.
0030   40 28 d7 cd 00 00 69                               @(....i

0000   28 94 0f 61 be 43 10 bf   48 4d eb aa 08 00 45 00   (..a.C.. HM....E.
0010   00 29 4e f3 40 00 80 06   00 00 8c 70 12 d0 8c 70   .)N.@... ...p...p
0020   ac 01 06 91 00 17 93 37   d2 4a 0a e2 89 ab 50 18   .......7 .J....P.
```

```
0030   40 28 d7 cd 00 00 6d                                  @(....m

0000   28 94 0f 61 be 43 10 bf   48 4d eb aa 08 00 45 00    (..a.C.. HM....E.
0010   00 29 4f 03 40 00 80 06   00 00 8c 70 12 d0 8c 70    .)O.@... ...p...p
0020   ac 01 06 91 00 17 93 37   d2 52 0a e2 89 d4 50 18    .......7 .R....P.
0030   40 1e d7 cd 00 00 31                                  @.....1

0000   28 94 0f 61 be 43 10 bf   48 4d eb aa 08 00 45 00    (..a.C.. HM....E.
0010   00 29 4f 04 40 00 80 06   00 00 8c 70 12 d0 8c 70    .)O.@... ...p...p
0020   ac 01 06 91 00 17 93 37   d2 53 0a e2 89 d4 50 18    .......7 .S....P.
0030   40 1e d7 cd 00 00 32                                  @.....2

0000   28 94 0f 61 be 43 10 bf   48 4d eb aa 08 00 45 00    (..a.C.. HM....E.
0010   00 29 4f 05 40 00 80 06   00 00 8c 70 12 d0 8c 70    .)O.@... ...p...p
0020   ac 01 06 91 00 17 93 37   d2 54 0a e2 89 d4 50 18    .......7 .T....P.
0030   40 1e d7 cd 00 00 33                                  @.....3

0000   28 94 0f 61 be 43 10 bf   48 4d eb aa 08 00 45 00    (..a.C.. HM....E.
0010   00 29 4f 06 40 00 80 06   00 00 8c 70 12 d0 8c 70    .)O.@... ...p...p
0020   ac 01 06 91 00 17 93 37   d2 55 0a e2 89 d4 50 18    .......7 .U....P.
0030   40 1e d7 cd 00 00 34                                  @.....4
```

As you can see the red part is my account and password!!!this tells us the telnet protocol is an unsafe protocol because it's unencrypted the other can easily capture these information and further : reestablish the image displayed on your screen!!!It's important that don't connect to an unsafe wi-fi (ex: doesn't need password and free to use) when you're out.

Wireshark also helps you to understand what the package is telling.Take the telnet package

```
0000   28 94 0f 61 be 43 10 bf   48 4d eb aa 08 00 45 00    (..a.C.. HM....E.
0010   00 2b 50 a9 40 00 80 06   00 00 8c 70 12 d0 8c 70    .+P.@... ...p...p
0020   ac 01 06 91 00 17 93 37   d2 79 0a e2 a8 a2 50 18    .......7 .y....P.
0030   40 29 d7 cf 00 00 1b 4f   42                         @).....O B
```

For example:

You can read like this:

Destination: Cisco_61:be:43 (28:94:0f:61:be:43)

Source: AsustekC_4d:eb:aa (10:bf:48:4d:eb:aa)

Type: IP (0x0800)

And below are Internet Protocol Version 4, Src: 140.112.18.208 (140.112.18.208), Dst: 140.112.172.1 (140.112.172.1)

45 =>Version: 4, Header length: 20 bytes

00=>Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))

00 2b=>Total Length: 43

50 a9=>Identification: 0x50a9 (20649)

40=Flags: 0x02 (Don't Fragment)

……

00 00 is checksum…etc

06 91 00 17 93 37 d2 79 0a e2 a8 a2 50 18 40 29 d7 cf 00 00:

Transmission Control Protocol, Src Port: sd-elmd (1681), Dst Port: telnet (23), Seq: 1, Ack: 1, Len: 3

And the rest 1b 4f 42 represents data

We can count the size of each part since it hex-based and every 2 slot is 1 byte.

Destination	6bytes
Source	6bytes
Type	2bytes
Internet Protocol Version	20bytes
Transmission Control Protocol	20bytes

And data takes the rest.

Futhermore, since you know what a unencrypted package look like, you can create a fake one and send it!

Take the web game http://www.roomi.com.tw/web/index.php for example:

It's a small web game generating money to decorate your imaginary character and room.

Play one round scored 111 and we can found a critical HTTP 1.1 package like this:

```
GET
/obj/swf/minigame/php/index.php?type=honeybee&PA=save&score=111
HTTP/1.1Host: http://www.roomi.com.tw/User-Agent:
Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-TW; rv:1.8.1.11) Gecko/20071127
Firefox/2.0.0.11Accept:
text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0
.5Accept-Language:
zh-tw,en-us;q=0.7,en;q=0.3Accept-Encoding: gzip,deflateAccept-Charset:
Big5,utf-8;q=0.7,*;q=0.7Keep-Alive: 300Connection: keep-aliveCookie:
```

PHPSESSID=0c8a8ebd9ffd07114acb6a866417c99b;

__utma=122646152.2093039428.1205467293.1205467293.1205467293.1;

__utmb=122646152; __utmc=122646152;

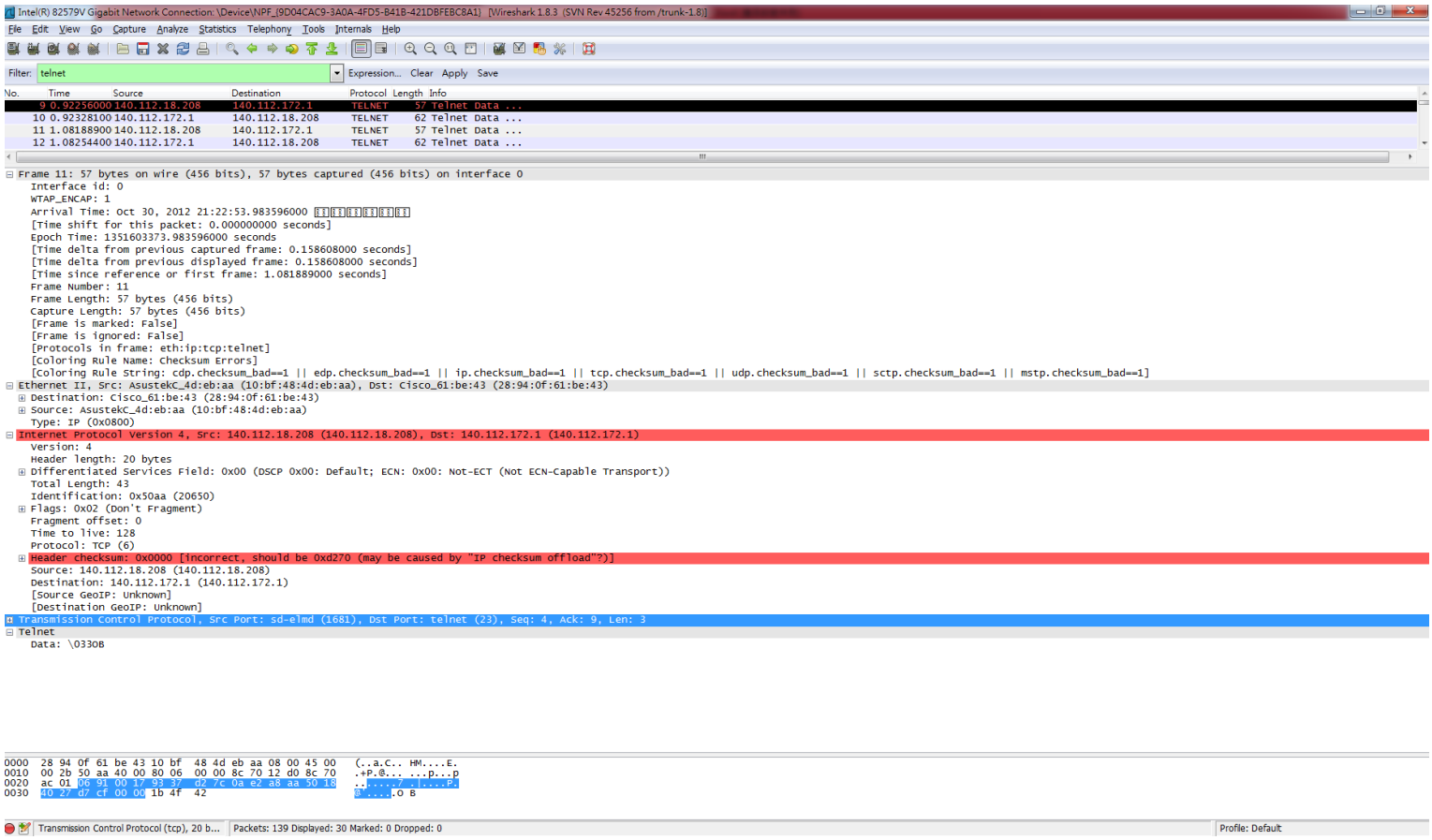
__utmz=122646152.1205467293.1.1.utmccn=(organic)utmcsr=googleutmctr=roomiutmcmd=organic

We can edit the score and use someway sent it then maybe you can become a millionare in the game!

WireShark is really a useful tool to help us verify what we learn at class. I think it build a connection between theory and reality.

Knowing this, next time when I go outside and need an wifi maybe I would choose SSH instead of TELNET portocol!!!!

WireShark interface



Reference: http://blog.shaolin.tw/2008/03/wireshark.html

http://en.wikipedia.org/wiki/Telnet