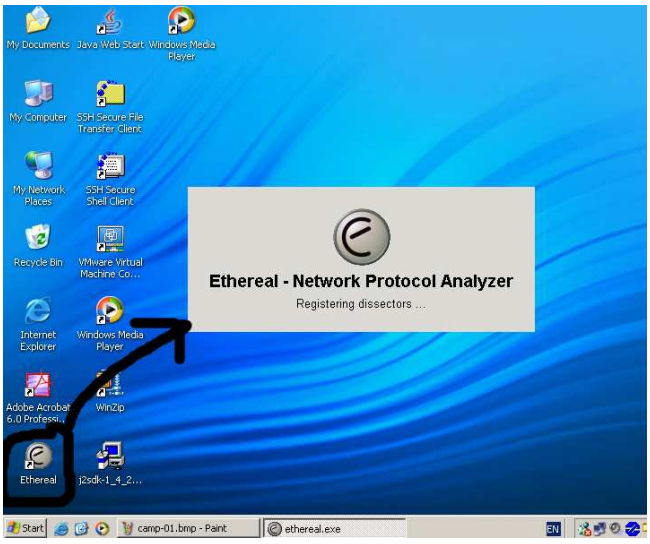
Information Engineering Workshop for School Visits: Packet Sniffering

Prepared by Adrian Sai-wah TAM
swtam9@ie.cuhk.edu.hk

Last modified: October 19, 2005

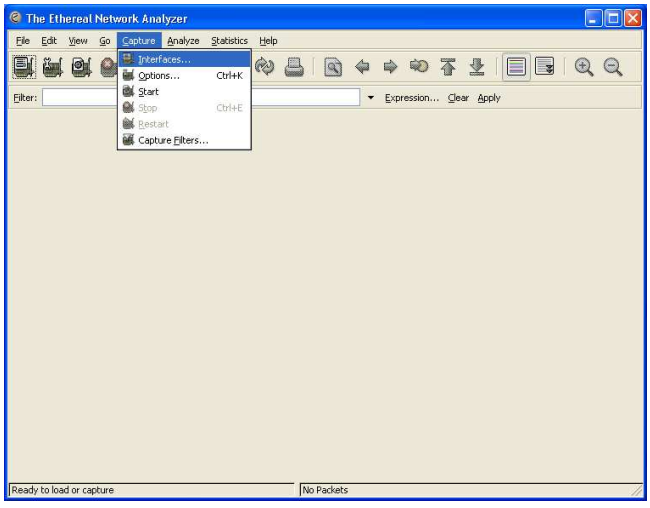
This workshop is to use Ethereal as a sniffering tool to sniffer the local network. The procedure and objectives are demonstrated and discussed step-by-step as follows:
這個workshop旨在LAN上使用Ethereal作為嗅探工具

1. Starting Ethereal As shown in the figure below. Click on the Ethereal icon on desktop and start Ethereal.
先在桌面上執行Ethereal

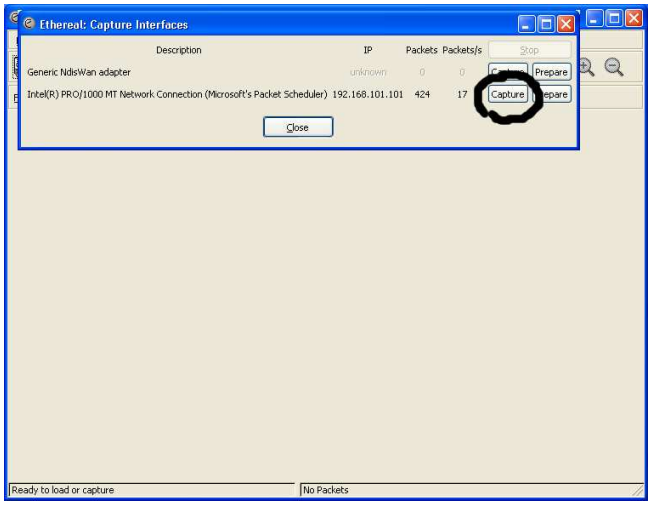


(1)

Afterwards, click on "Capture ▹ Interface" and you will get the dialog box as below. Which you can click "Capture" to start packet capture.
之後，在選單上選取「Capture ▹ Interface」。然後在彈出的視窗選取「Capture」以開始搜捕封包。

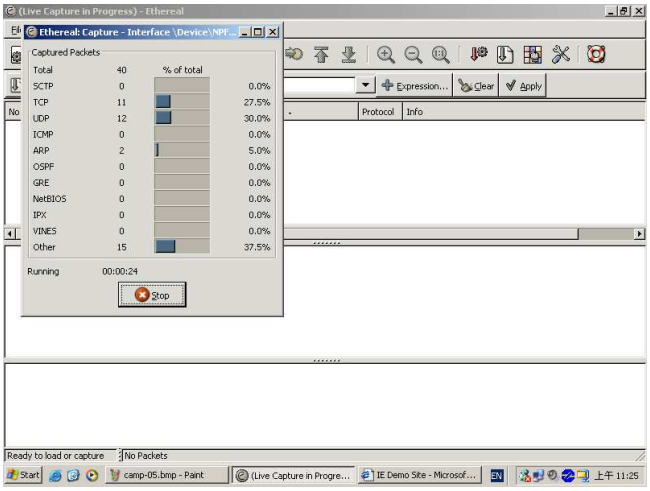


(2)



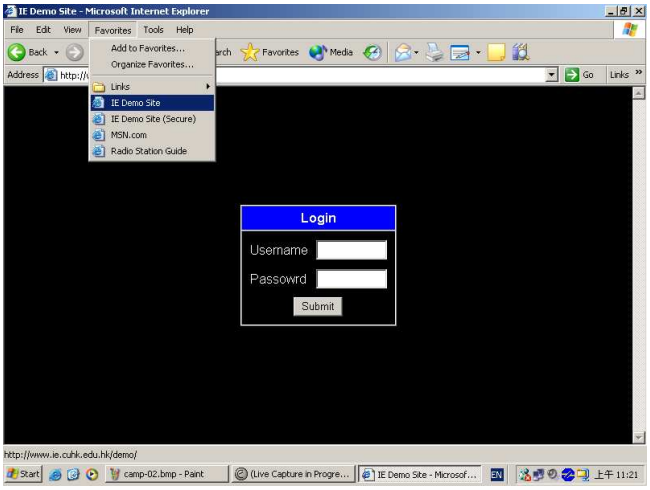
(3)

You can now click on “Close” in the previous dialog box named “Caputre Interfaces”. Below is the screen during capture:
之後就可以選取「Close」關閉「Capture Interfaces」視窗。搜捕封包時的畫面如下：



(4)

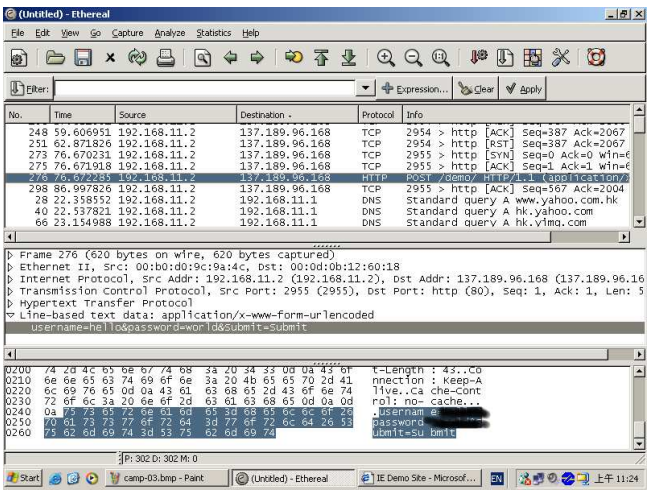
2. Login attempt using Browser Next, go to the desktop and start the Internet Explorer. In the “favorites”, there is already a bookmarked link called “IE Demo Site” as shown below, or you can type in `http://www.ie.cuhk.edu.hk/demo/`:
接著，啓動Internet Explorer。在favorites，選取「IE Demo Site」，或鍵入網址`http://www.ie.cuhk.edu.hk/demo/`：



(5)

You can type anything and click “Submit” to login. You should get a failed message as you do not know the password.
之後請嘗試隨便輸入login name和password以登入網頁，按下「Submit」後應看到Authentication failed的訊息。

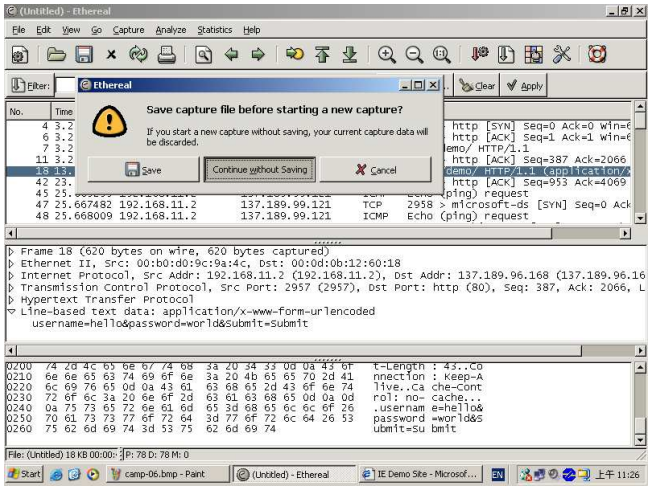
3. Examine plain HTTP Back to Ethereal and stop the capture. The packets captured during your login attempt is tabularized as rows, as follows:
之後，回到Ethereal，按「Stop」停止搜捕。之前找到的網路封包會以列表形式顯示，如下圖：



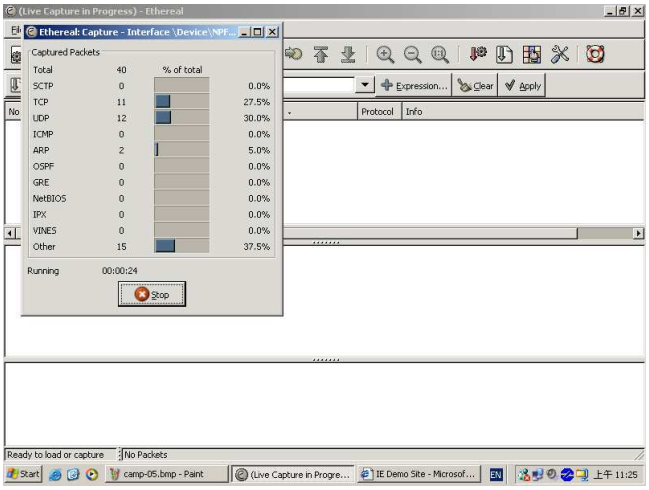
(6)

You can click on the table header to sort the packets. To find your HTTP packet, please try to *sort by destination*, and look for the destination IP 137.189.96.168. Among them, there is one in protocol `HTTP` and the "info" begins with `POST`. Clicking on the packet will show the detailed packet information in the middle frame. The bottom frame will show the packet in byte-by-byte format, which you can see your password and login name that you was typed to the browser.
你可以按下表格的標頭對封包進行排序。要找出你的HTTP封包，你可以按下Destination排序，然後找出IP為137.189.96.168 （剛才的網頁的伺服器地址）的封包。再找出protocol標示為`HTTP`而info欄位是`POST`開首的封包，用滑鼠按一下，那麼這個封包的詳細資料就會在視窗的中央部分顯示，而最底部就是以位元組形式(byte-by-byte)顯示的封包，你在那兒可以找到你自己輸入的login name和password。

4. Examine secure HTTP Firstly, clear all your captured packets and restart a new caputre section by selecting "Capture▹Start" in Ethereal's menu. It will prompt you to save the capture as shown below. Please choose "continue without saving" and you can start a new section again.
首先，在Ethereal的選單上選取「Capture▹Start」，再按下「continue without saving」。這樣你就會刪除你之前搜捕得來的封包資料，並開始新一次的搜捕工作。

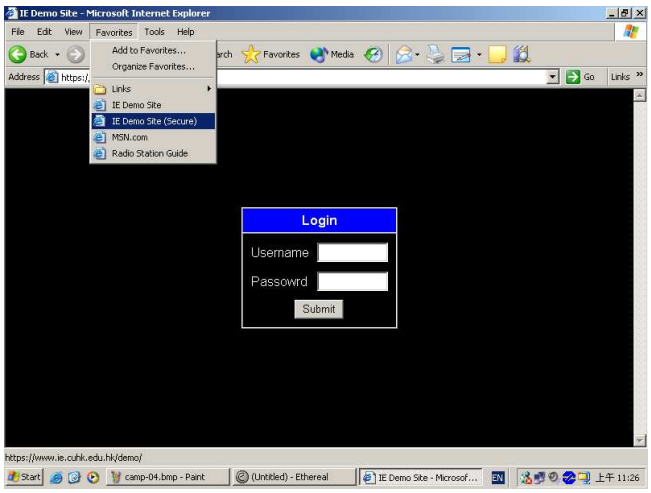


(7)



(8)

Go to the browser and do the same procedure again but type in the address `https://www.ie.cuhk.edu.hk/demo/`. You can login with any username and password as before to generate the "authentication failed" page.
回到瀏覽器去，重覆之前用隨意的login name和password登入的步驟，但這次請在網址列上輸入：`https://www.ie.cuhk.edu.hk/demo/`，同樣地，你都應得到「authentication failed」的訊息。

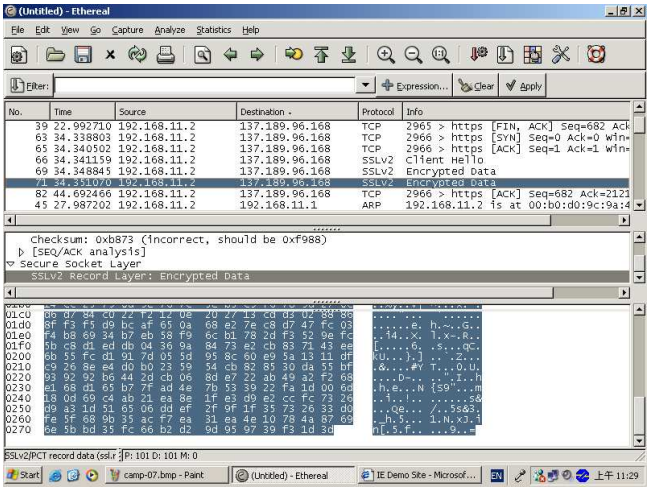


(9)

Next, go back to Ethereal and stop the capture. Check if you can get the login name and password you just typed! (Answer: No, you can't)
之後，回到Ethereal並停止搜捕封包，看看可否再找到你輸入的login name和password。（應該是看不到的）

You can only see those "encrypted" data which you cannot read the content. This effect is the difference between the `https://` (secured HTTP) in this example and `http://` (clear text HTTP) in the last example. Below is the capture of

the secured HTTP session:
你只會見到已加密的封包內容而非真正內容，這就是這步驟中的`https://`（已加密HTTP）和上一步中`http://`（明文HTTP）的分別。下圖是經過加密處理的封包內容：

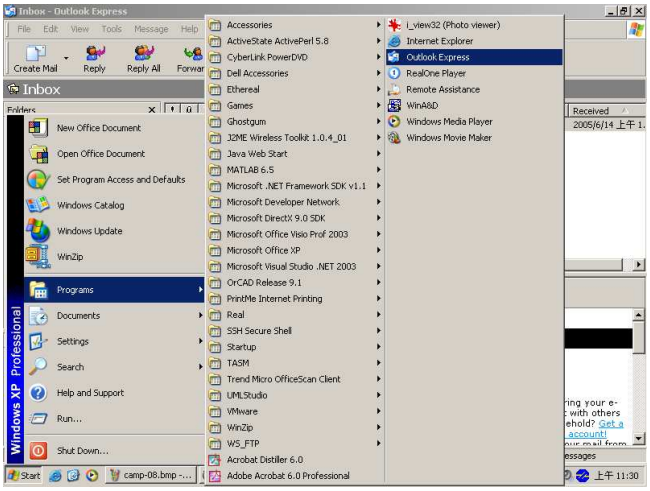


(10)

5. Obtaining Password by Sniffering You cannot login to the previous pages because you do not have the password. But the computers are configured with the Outlook Express correctly to send and receive emails. Of course you cannot recover the email password from Outlook Express directly. However, the following is to capture the password by sniffering the email session.
因為你不知道真正的login name和password，所以你不能成功登入之前的網頁。但你現在所使用的電腦內的Outlook Express就設定了一組可以用來收發電郵的login name和password。雖然你不能直接取得這些存儲了的資料，但是你可以透過搜捕封包的方法取得這些資料。

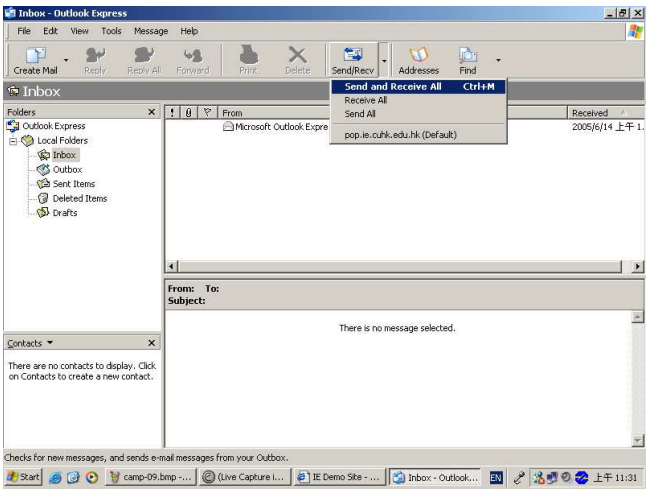
Firstly, start a new caputre in the Ethereal as the previous step. As shown in figures 7 and 8.
首先，如上一步驟中的圖7和圖8般，讓Ethereal重新開始封包的搜捕工作。

Then open Outlook Express as follows:
之後，如下圖般的啓動Outlook Express：



(11)

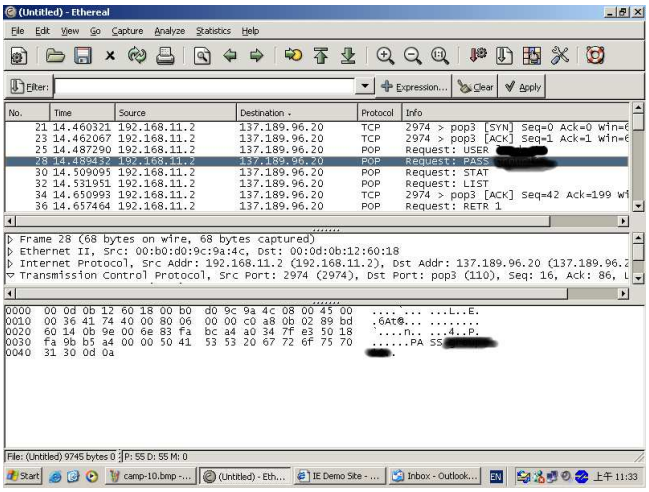
Then you can click on “send and receive” as shown below. This is to ask your Outlook Express to communication to the email server. By leting the Outlook Express to contact the email server, the program will send the password out, which you can capture it by Ethereal.
之後如下圖般按下「send and receive」，這樣Outlook Express就會和電郵伺服器聯接以收發電郵，這過程中Outlook Express會把login name和password傳送出去，而你也就可以使用Ethereal取得這些資料。



(12)

After your Outlook Express finish send and receive email, you can go back to Ethereal and stop the capture. Look for the destination IP 137.189.96.20, and see if you can get the correct login name and password. The correct packets should be in protocol `POP` and the info should begin with "`Request: USER`" (for login name) or "`Request: PASS`" (for password). The sample screen capture is shown below:

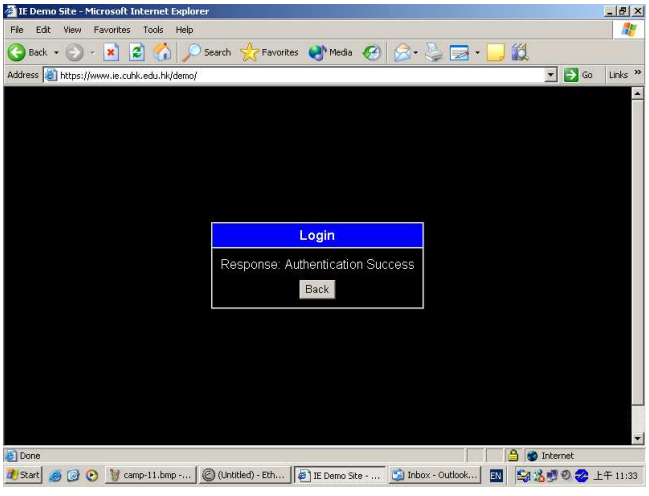
若Outlook Express完成收發電郵後，你就可以回到Ethereal並停止搜捕封包。在封包列表中，找出目標地址是137.189.96.20（電郵伺服器地址）的封包，並看看是否能夠從中找到login name和password。有關的封包應是protocol為`POP`及info以「`Request: USER`」（使用者名稱）或「`Request: PASS`」（密碼）開首的。畫面如下圖：



(13)

After you get the correct name and password, you can go back to the browser and login. If your answer is correct, you should see the following screen:

如果你已從Ethereal中找到login name和password，你就可以回到之前的那個網頁去，並用你找出來的login name和password登入。如果你找到的資料無誤，你應會見到如下圖的畫面：



(14)