**透明化代理**

1. **研究方法及架構**
2. 研究時需要電腦一台、vmware(client)、mitmproxy以及所要測試的瀏覽器(google chrome、IE)。
3. 本實作環境建立在Ubuntu 16.04，在linux系統下安裝mitmproxy。使用透明代理時，流量將重導向到網絡層的代理，無需任何客戶端配置。 這使得透明代理非常適合那些無法改變客戶端行為的情況。
4. 修改其頁面、自製CA並掛載在所要測試的瀏覽器。
5. 研究架構圖

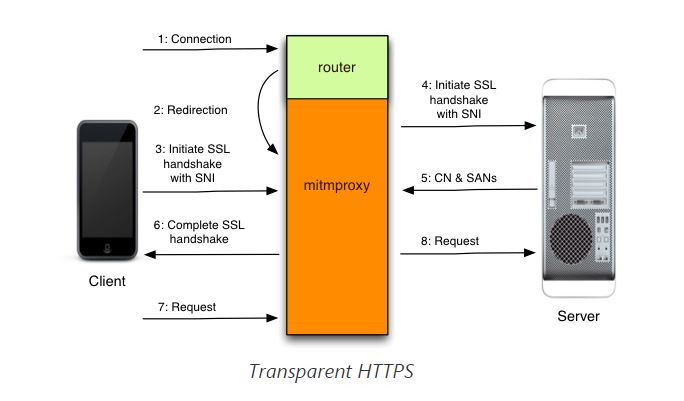


圖1.

1.客戶端連接到服務器。

2.路由器連接到mitmproxy。

3.客戶端認為它正在與遠程服務器通話，並啟動TLS連接。 它使用SNI來指示它所連接的主機名。

4.Mtmproxy連接到服務器，並使用客戶端指定的SNI主機名建立TLS連接。

5.服務器使用匹配的證書進行響應，該證書包含生成攔截證書所需的CN和SAN值。

6.可自產攔截證書，並繼續在步驟3中暫停客戶端TLS。

7.客戶端通過建立的TLS連接發送請求。

8.Mitmproxy通過步驟4中啟動的TLS連接將請求傳遞到服務器。

1. **實作環境**

**1.iptables設置**

要設置透明代理，我們需要兩個新組件。 第一種是重定向機制，它透明地將發往Internet上的服務器的TCP連接重新路由到偵聽代理服務器。 這通常採用與代理服務器相同的主機上的防火牆形式 - Linux上的[iptables](https://translate.googleusercontent.com/translate_c?depth=1&hl=zh-TW&prev=search&rurl=translate.google.com.tw&sl=en&sp=nmt4&u=http://www.netfilter.org/&xid=17259,15700022,15700043,15700124,15700149,15700168,15700186,15700191,15700201,15700208&usg=ALkJrhiF8WrNEPqqCS3Mkowx-8O8Ivy-zg)或OSX上的[pf](https://translate.googleusercontent.com/translate_c?depth=1&hl=zh-TW&prev=search&rurl=translate.google.com.tw&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/PF_(firewall)&xid=17259,15700022,15700043,15700124,15700149,15700168,15700186,15700191,15700201,15700208&usg=ALkJrhhC5bh75GEmvJtRX7_fEjfxwaV84g) 。 當代理收到重定向連接時，它會看到一個沒有主機規範的vanilla HTTP請求。 這是第二個新組件進入的位置 - 一個主機模塊，允許我們向重定向器查詢TCP連接的原始目標。

* 1. Enable IP forwarding

這可以確保您的計算機轉發數據包而不是拒絕它們。

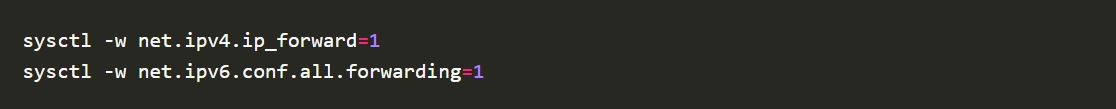


圖2.

* 1. Disable ICMP redirects

如果您的測試設備位於同一物理網絡上，則您的計算機不應通過跳過代理來通知設備可用的路由較短。

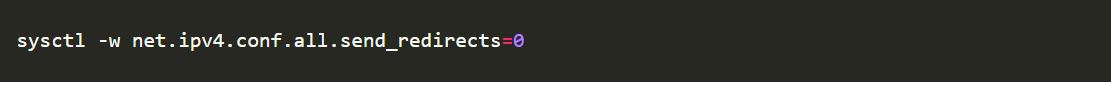


圖3.

* 1. 創建一個iptables規則集，將所需的流量重定向到mitmproxy。

根據您的設置，詳細信息會有所不同，但規則集應如下所示：

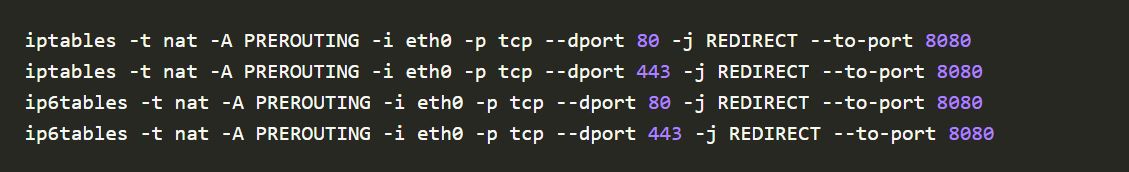


圖4.

* 1. Fire up mitmproxy.

--mode透明選項打開透明模式， - showhost參數告訴mitmproxy使用Host標頭的值進行URL顯示。



圖5.

**2.修改mitmproxy認證下載頁面**

希望能夠在認證CA的時候把網頁導入我們自己設置的頁面

並且下載自己所生產的CA證書。

2.1如在linux輸入指令mitmproxy開啟後，在任意瀏覽器上搜尋mitm.it會跑出相對應的證書安裝說明。如下mitmproxy初始設定:

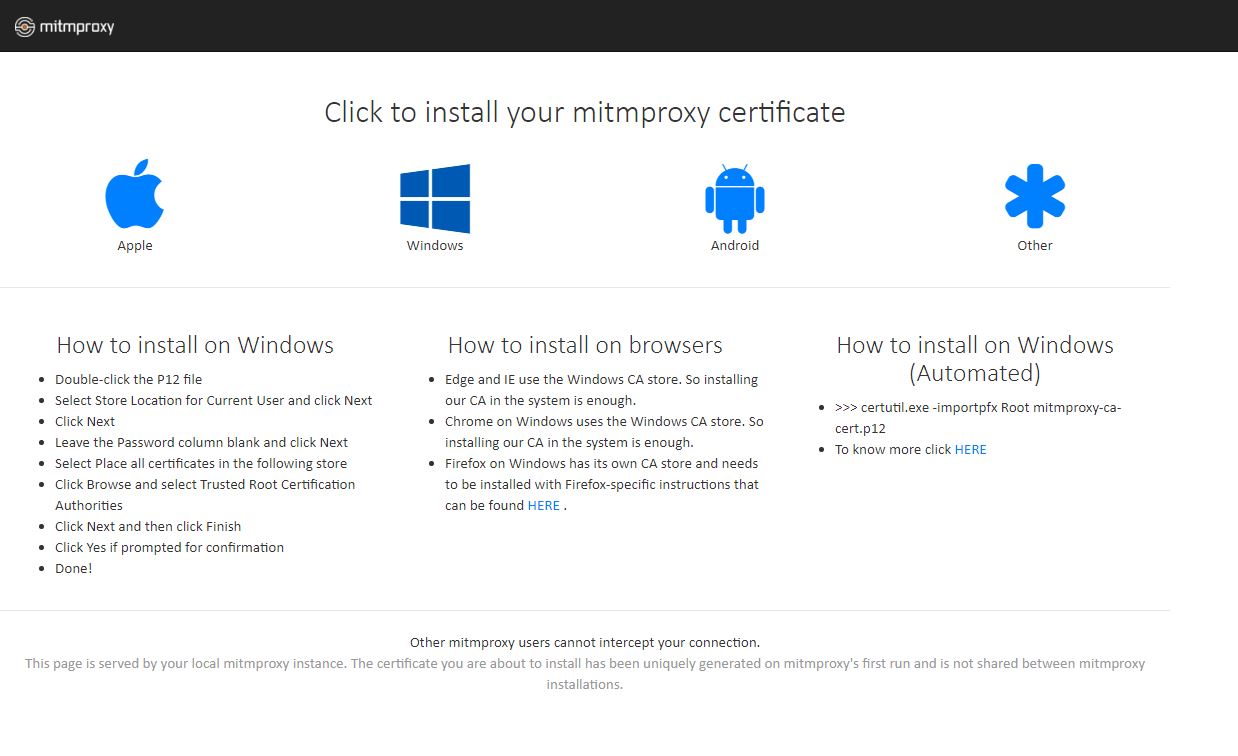


圖6.

2.2 mitm.it原始網頁位置在mitmproxymaster\mitmproxy\addons\onboardingapp\templates

裡面含有index.html、layout.html。

2.2.1修改 index.html，把安裝步驟、敘述改成中文

Index內容為圖6，分為apple、windows、Android、other等四部分

並詳細說明其安裝方法及步驟。

把敘述改成較容易理解的中文字。如下圖:



圖7.

2.2.2 修改 layout.html

Layout內容為標題”網頁圖檔….等。

把標題改為HAN HAN，並把一些原始的圖檔移除掉。



圖8.

2.2.3 把下載下來的CA簽發者改為自己

修改檔案路徑在 \mitmproxy-master\mitmproxy\proxy

裡面的config.py。

把config.py裡面的 “CONF\_BASENAME = “ 改成自己想要的名字。

這樣在下載CA的時候會把CA的檔名改為自己的名字，且簽發者也會是自己的名字。

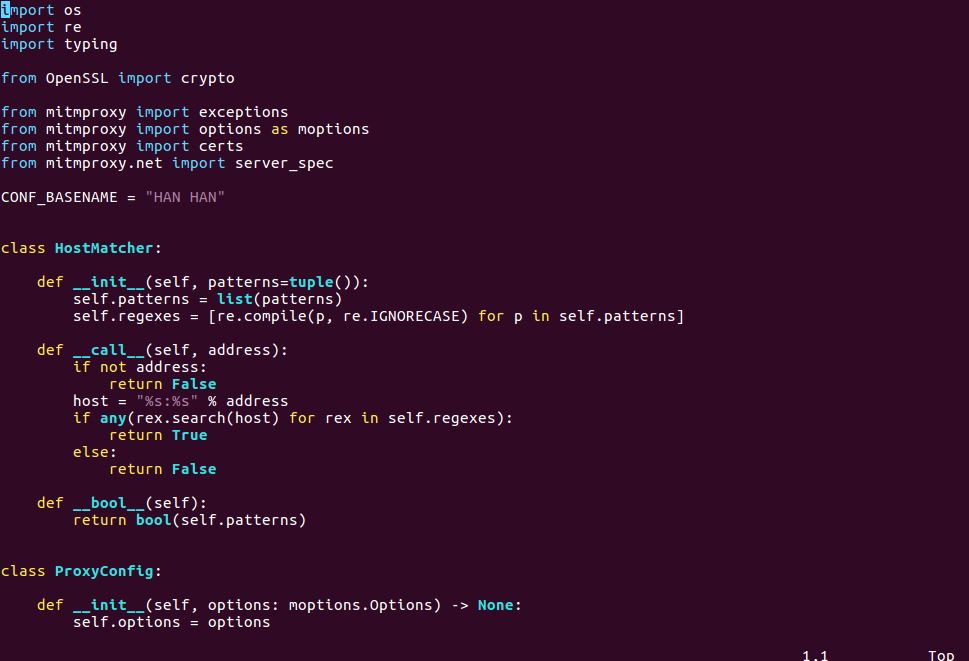
****

圖9.

1. **實驗驗證**
2. 確認80 port的流量是否導入 8080 port

linux輸入指令mitmproxy開啟後

在對mitmprixy 輸入指令O，就可以觀察流量是否有導入8080 port。

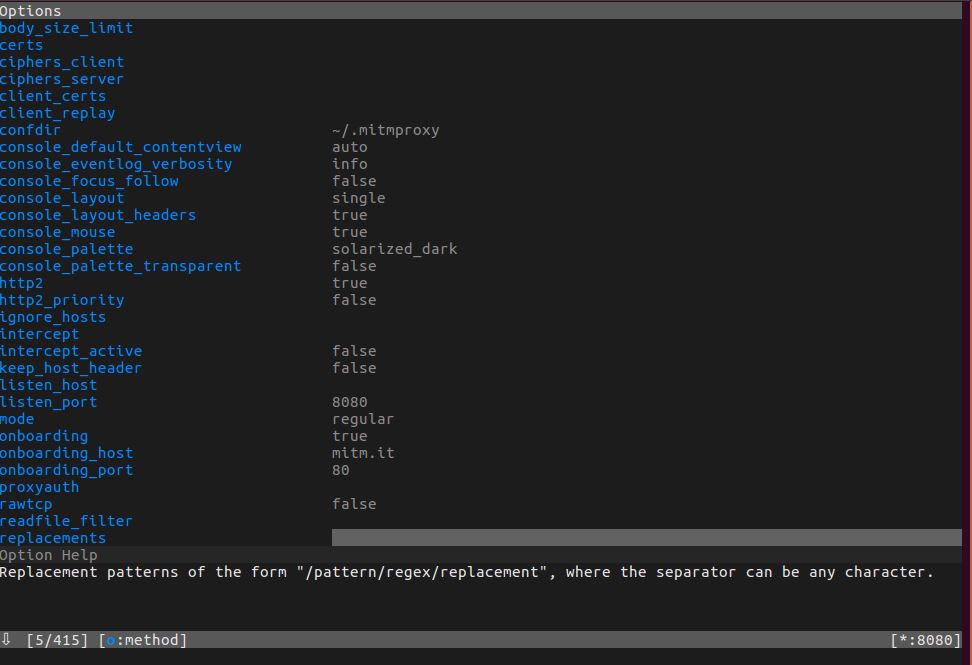
****

圖10.

1. 在linux輸入指令mitmproxy後，在任意瀏覽器上輸入任何關鍵字

會顯示你的連線不是私人連線

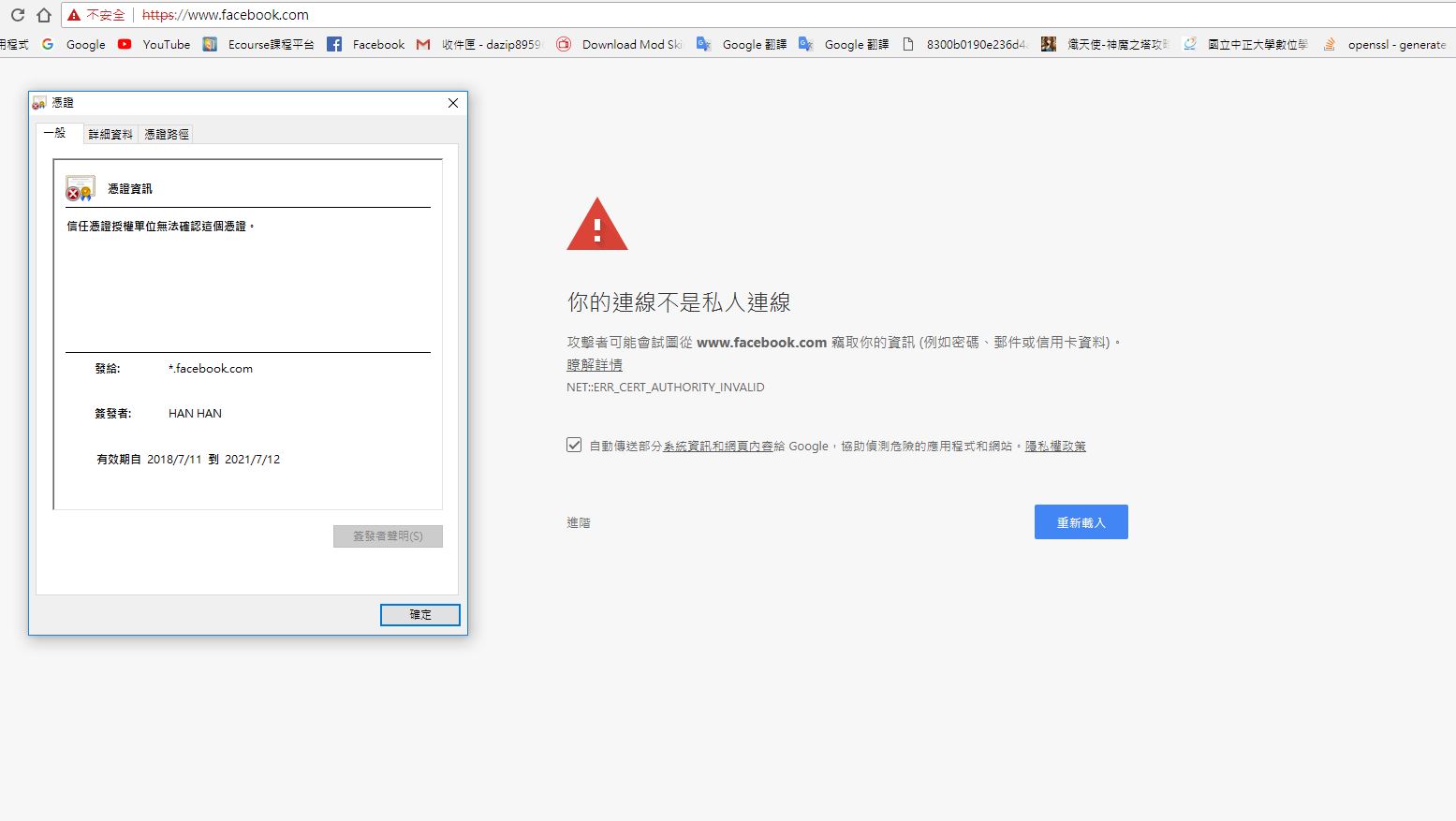


圖9.

2.2 簽發者為自己

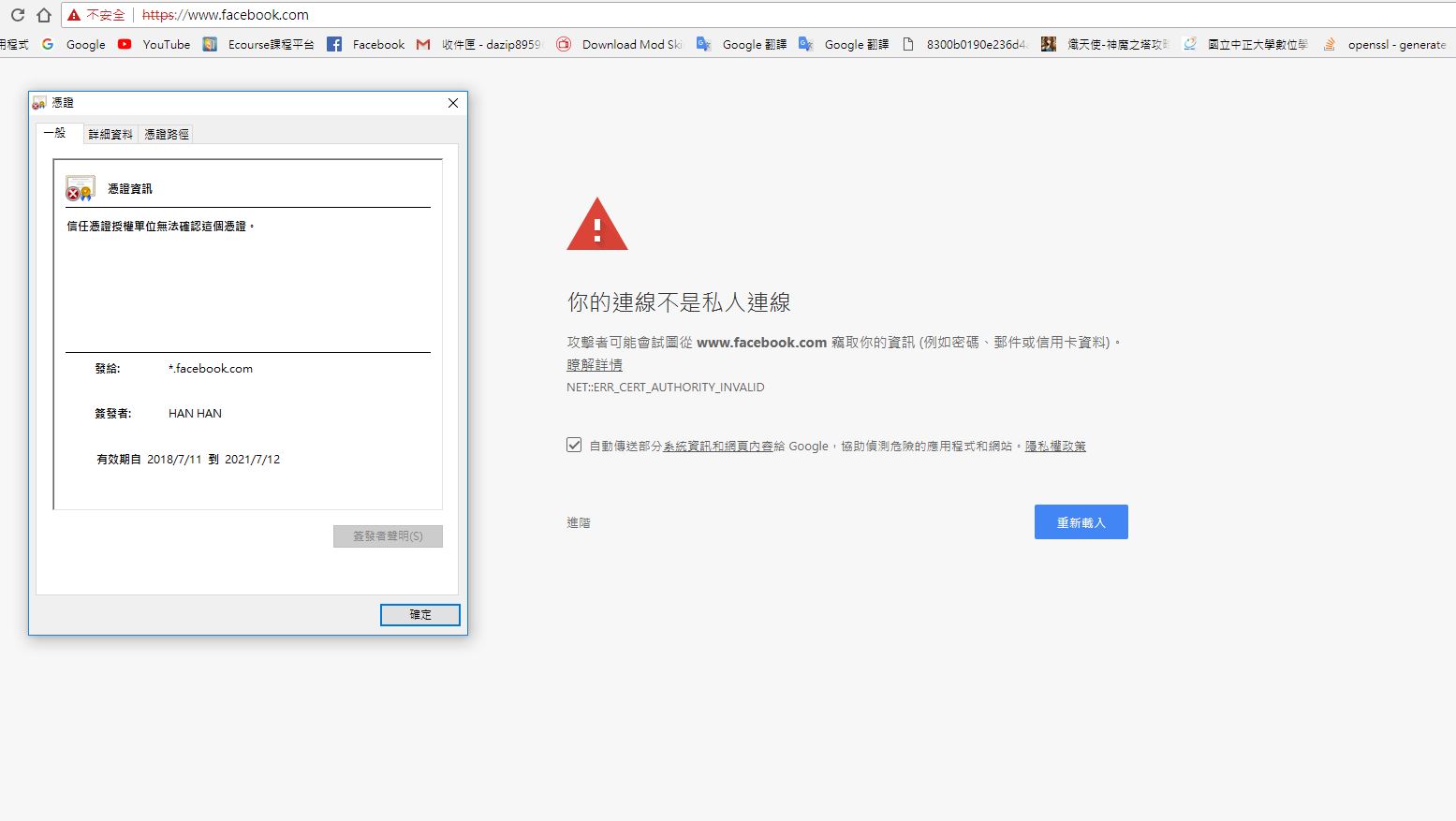
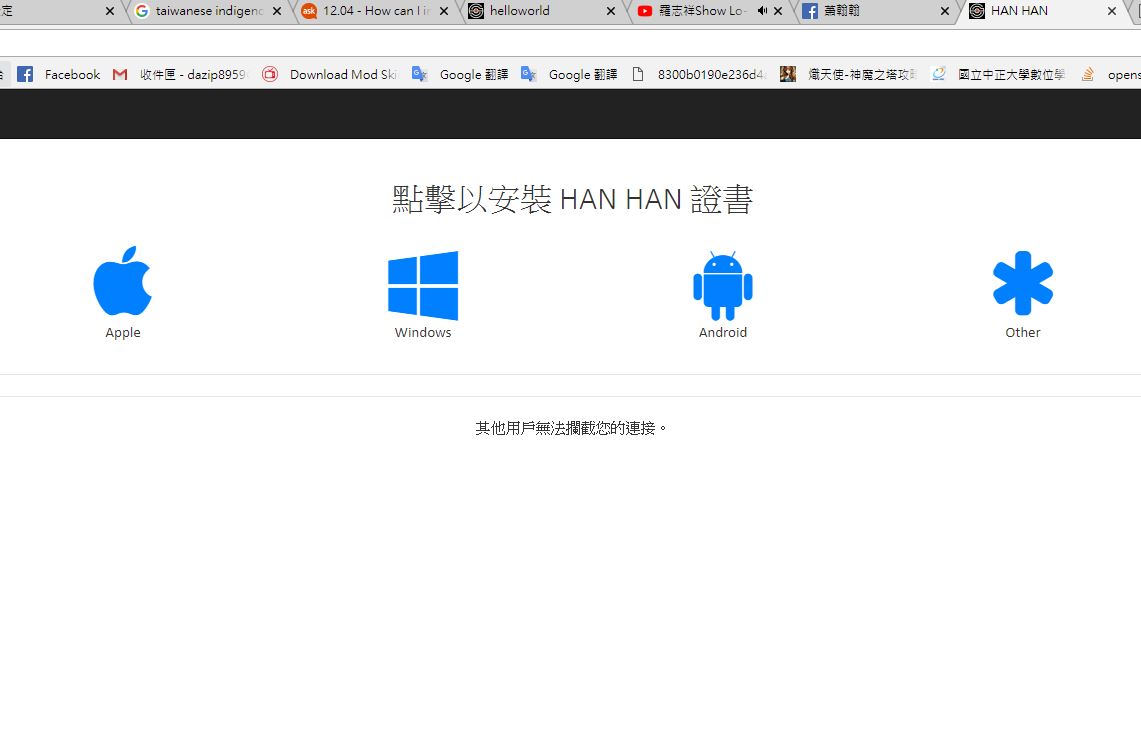


圖10.

1. 在任意瀏覽器上輸入 “mitm,it”，會跑出剛剛修改完成的網頁

圖9.

3.2 點擊想要的裝置(例:apple、windows、android、other)

會跑出中文的安裝方法及步驟



圖10.

3.3 分別點擊四個icon，跑出個別對應的四個CA

HAN HAN -ca.pem

HAN HAN -ca-cert.pem

HAN HAN -ca-cert.p12

HAN HAN -ca-cert.pem

名字都是剛剛所修改的。



圖11.