第二章

足跡

偵查

- 偵查是預備階段(preparatory phase)，攻擊者在進行攻擊之前，會儘可能的蒐集有關目標的資訊。

足跡

- 足跡是蒐集有關組織或目標所有資訊的過程，這些收集到的資訊可以在進行後續的入侵行動時使用。

足跡

- 「足跡」是攻擊發起前(Pre-attack Phase)三階段的其中之一，另外兩個是掃瞄(Scanning，第三章) 及列舉(Enumeration，第四章)。
- 一個攻擊者可能會花費 90% 以上的時間，去進行資料的蒐集，但是只用10% 的時間來進行攻擊。

資訊收集

- 資訊收集(Information Gathering)可以區分為七個邏輯步驟，而「足跡」包含了前兩個步驟，第三至第七個步驟則涵蓋了後面「掃瞄」及「列舉」兩個章節。

資訊收集的七步驟

資訊收集七步驟	攻擊發起前三階段
發掘初始資訊	「足跡」
找出網路的範圍	
探知活動中的機器	「掃瞄」及「列舉」
探索開啟的Port或存取點	
偵測作業系統	
揭露Port上的服務	
繪製網路地圖	

發掘初始資訊

- 發掘該組織的背景基本資料。
- 領域名稱或 URL 查詢：尋找與該組織相關的領域名稱與 URL。
- 位置：尋找該組織的地理位置，包含週邊道路位置。
- 接洽(Telephone /Mail)：該組織服務台或服務部門的電話或郵件帳號。

找出網路的範圍

- 使用工具，尋找該組織的 IP 範圍及遮罩...等資訊。

探知活動中的機器

- 使用工具，在該組織的 IP 範圍內，掃瞄是否有經常存活 (開機) 的電腦。

探索開啟的 Port 或存取點

- 使用工具，針對存活的機器，逐一掃瞄探索哪些 Port 已經開啟。

偵測作業系統

- 使用工具，偵測該主機使用哪種作業系統，以及這個作業系統做了哪些更新。

揭露 Port 上的服務

- 不同的 Port 上會有不同的服務，某些服務不見得是在原先預設的 Port 上，例如：HTTP 有可能出現在 Port 8080 上。

繪製網路地圖

- 將前述得到的資訊繪製成網路關連地圖。

被動資訊蒐集

- 「被動資訊蒐集」是去了解一個特定資訊系統目前的安全狀態，被動資訊收集的完成，乃是從網路上公開的資訊中，發現各種資訊細節的技術，此種方式不需要直接與組織中的伺服器接觸(偵查階段的被動偵查)。

- 組織及資訊網站對於攻擊者的這種資訊收集活動與方式，並不會提高其警覺。

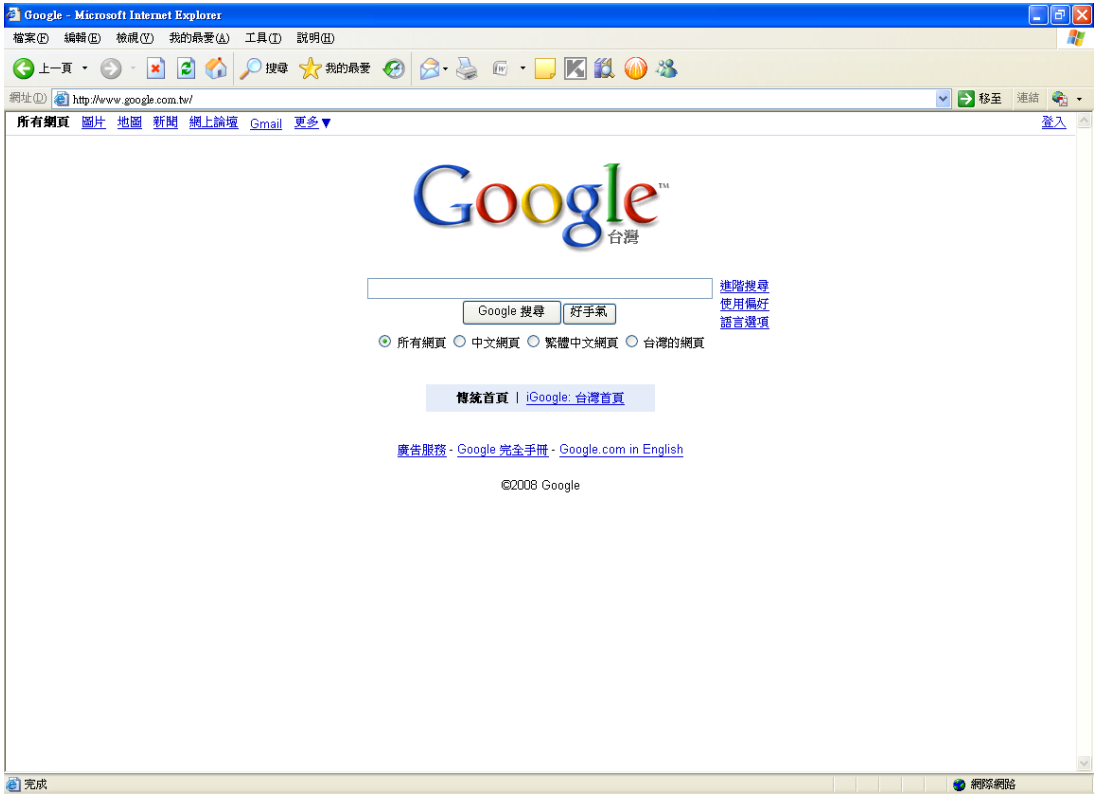
搜尋引擎

- 網路上有多個知名的搜尋引擎(例如：google)，這些搜尋引擎以蒐集網路上的資料為目的。

- 攻擊者可以利用這些公共的搜尋引擎，來搜尋組織內的 URL 資訊，搜尋引擎提供了豐富的資訊給「被動偵察」，只要輸入名稱或關鍵字就可以找到該組織的網址。

Google

- 只要輸入名稱或關鍵字，就可以找到該組織的網址、使用的作業系統、硬體設備、IP 位址、管理者的聯絡電話號碼及郵件帳號、該組織的資安政策…等。

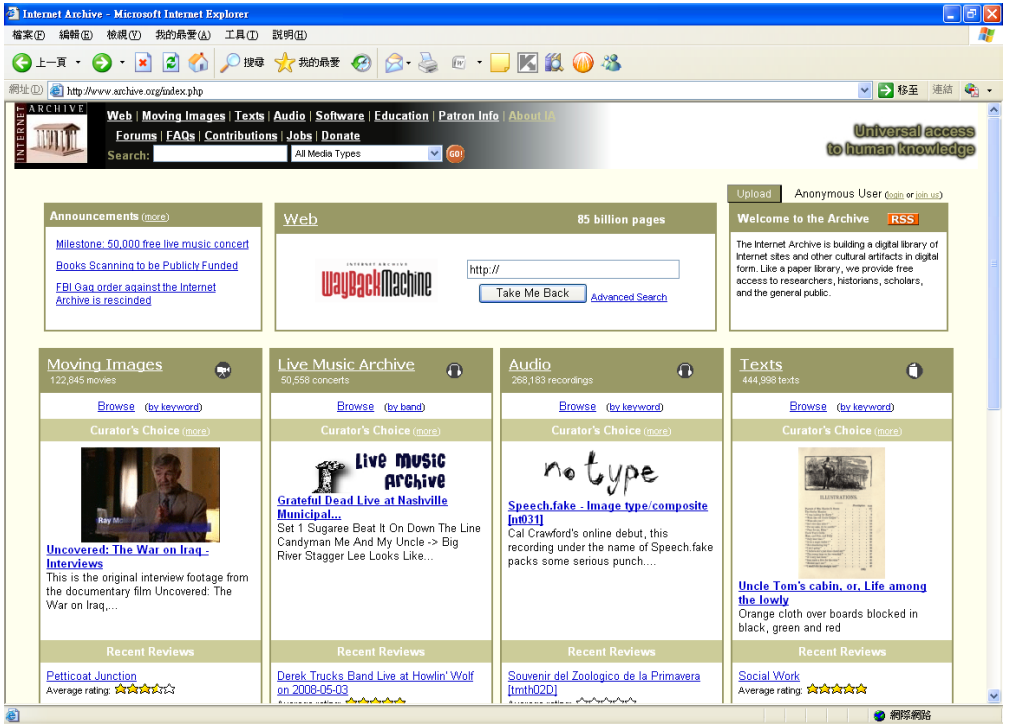


被動資訊蒐集的工具

- 搜尋部落格(blogs)或論壇(forums)。
- 用猜的方式用猜的方式 。
- 可以使用 DNS 工具尋找 URL 資訊 。

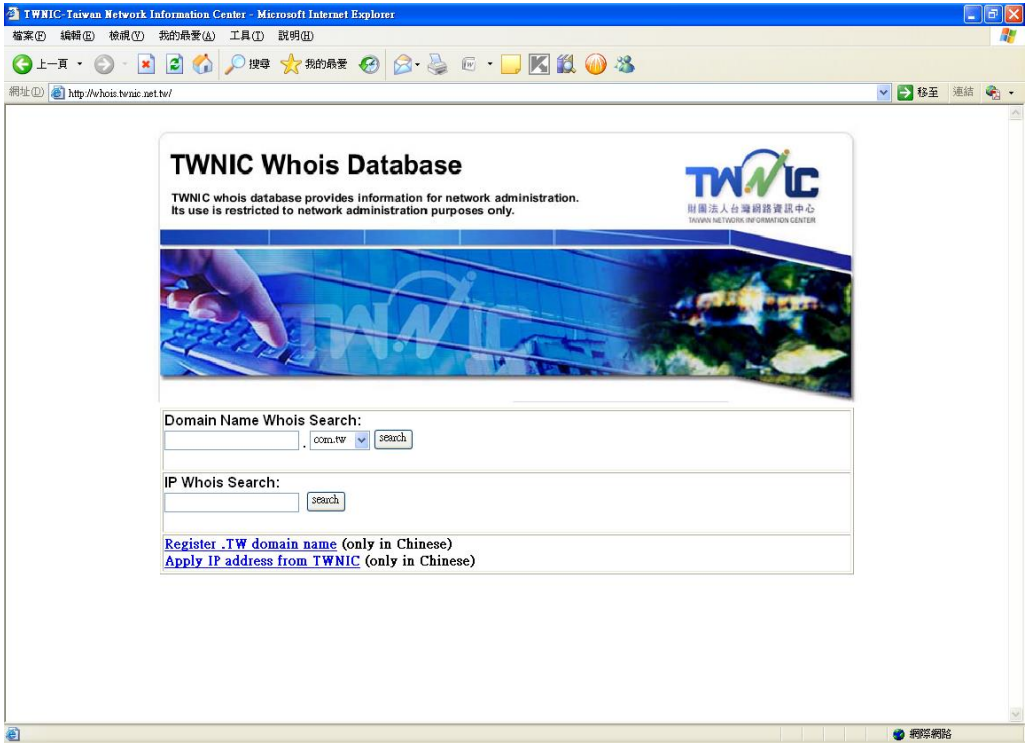
被動資訊蒐集的工具 https//web.archive.org

- 記錄了許多 URL 的背景資料，包括該網站開始被記錄的時間及網頁更新的狀況。



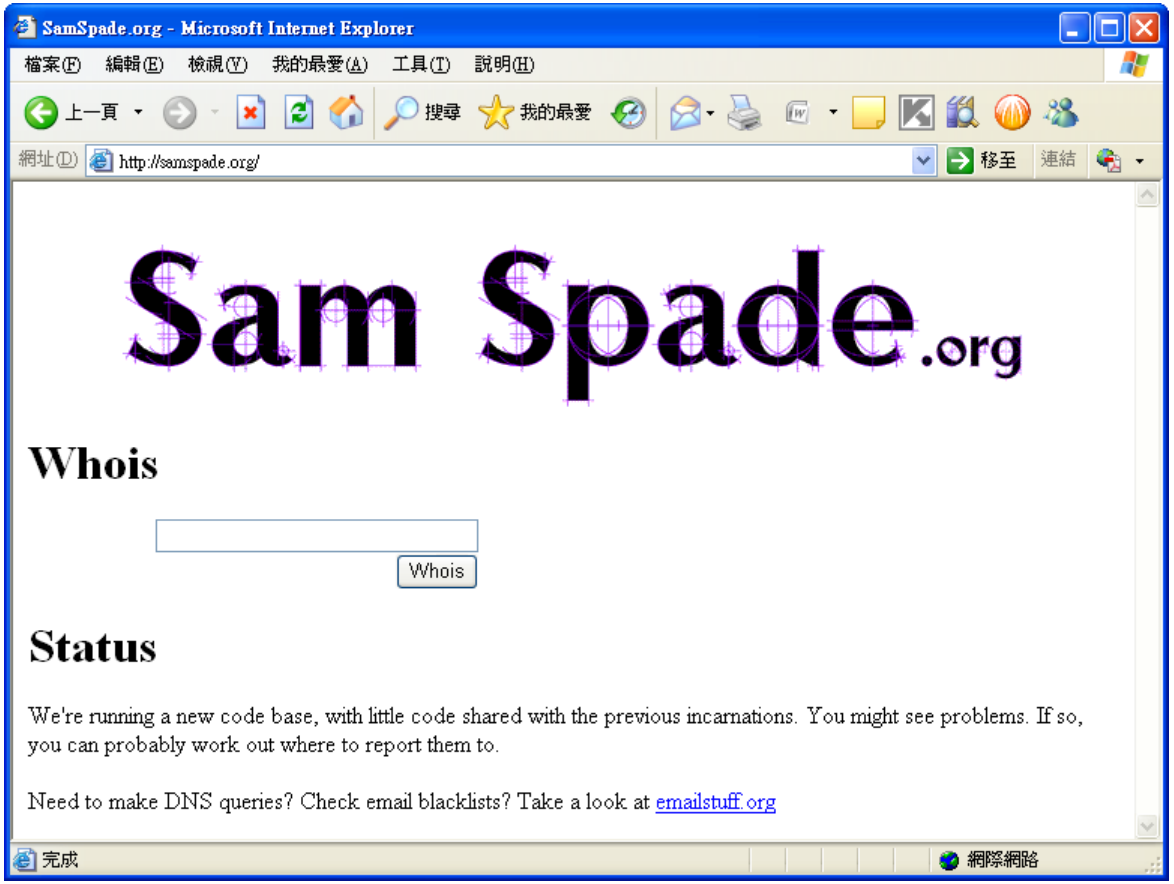
工具：http://whois.twnic.net.tw/

- Whois 可以查詢得到目標網站及接洽管理者的資訊。



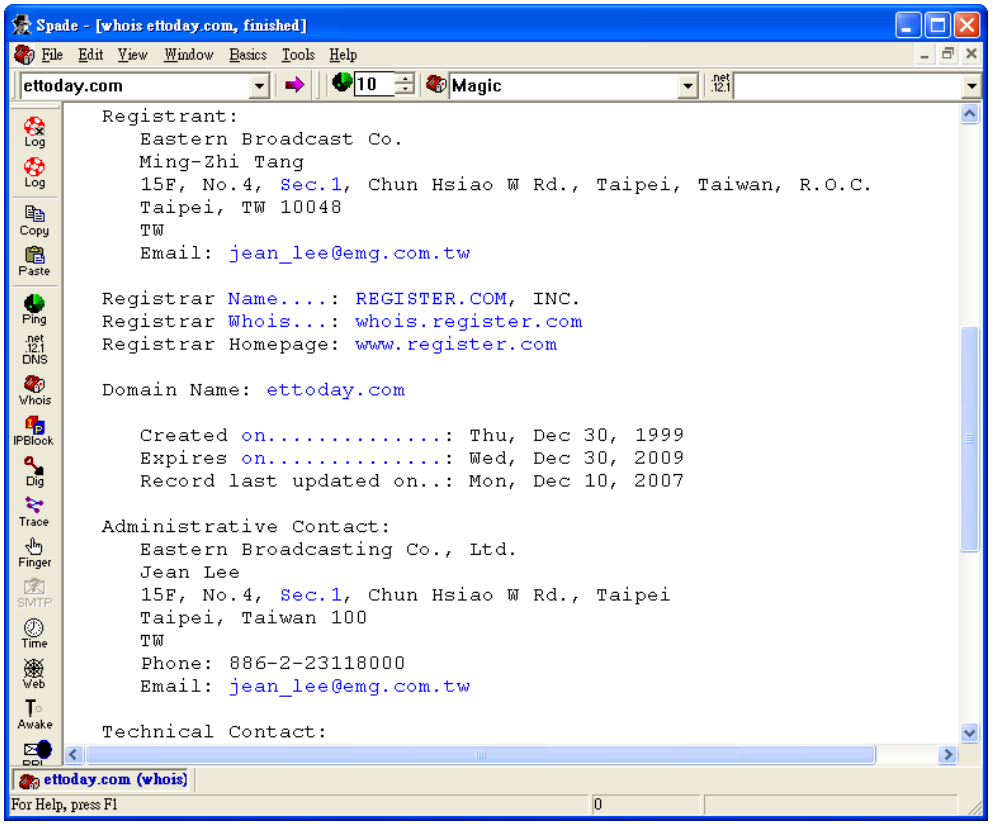
工具：http://www.who.is/ http://whois.domaintools.com/

工具：Sam Spade(網路版)



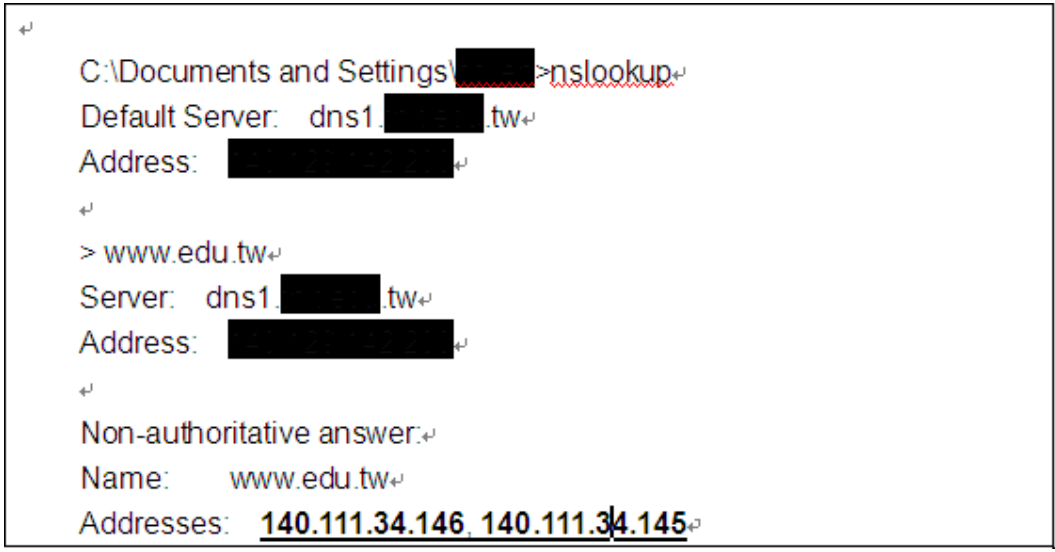
Sam Spade 程式版

- 可以使用包括 ping、nslookup、whois、dig、traceroute、finger、raw HTTP web browser、DNS zone transfer、SMTP relay check…等功能。



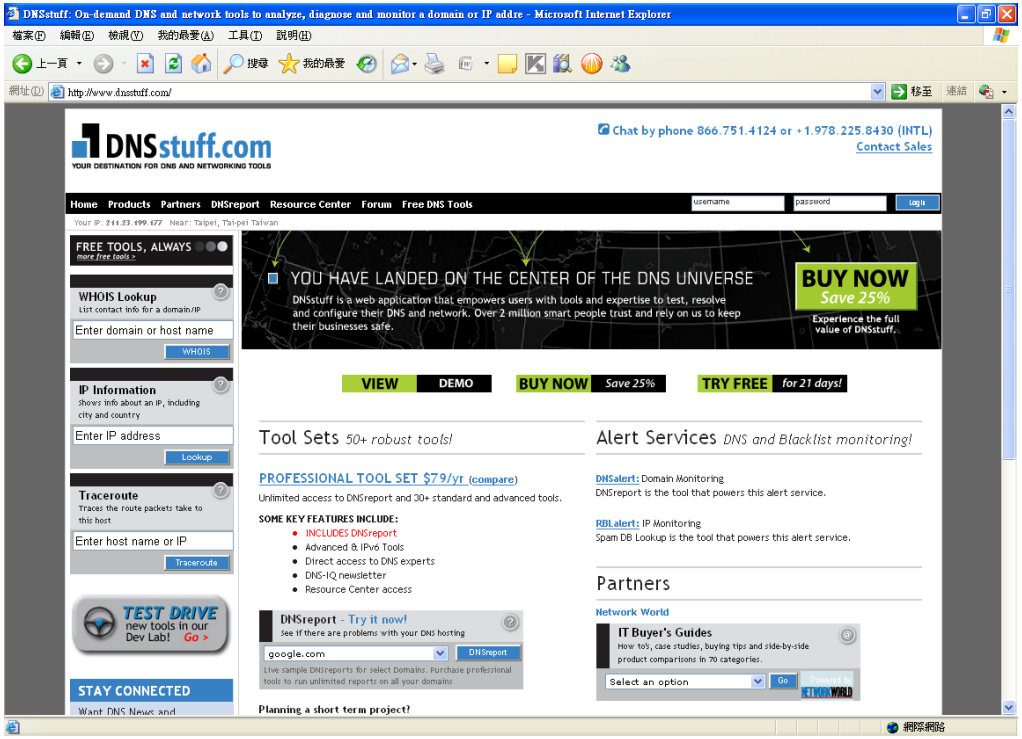
Nslookup

- 這個程式可以用來查詢網路領域名稱伺服器。也可以用來診斷DNS 的架構，如果知道DNS 的名稱，還可以幫助尋找額外的 IP 位址 。



www.dnsstuff.com

- 可以獲得 DNS 的訊息，包括 Mail server extensions 及 IP 位址。



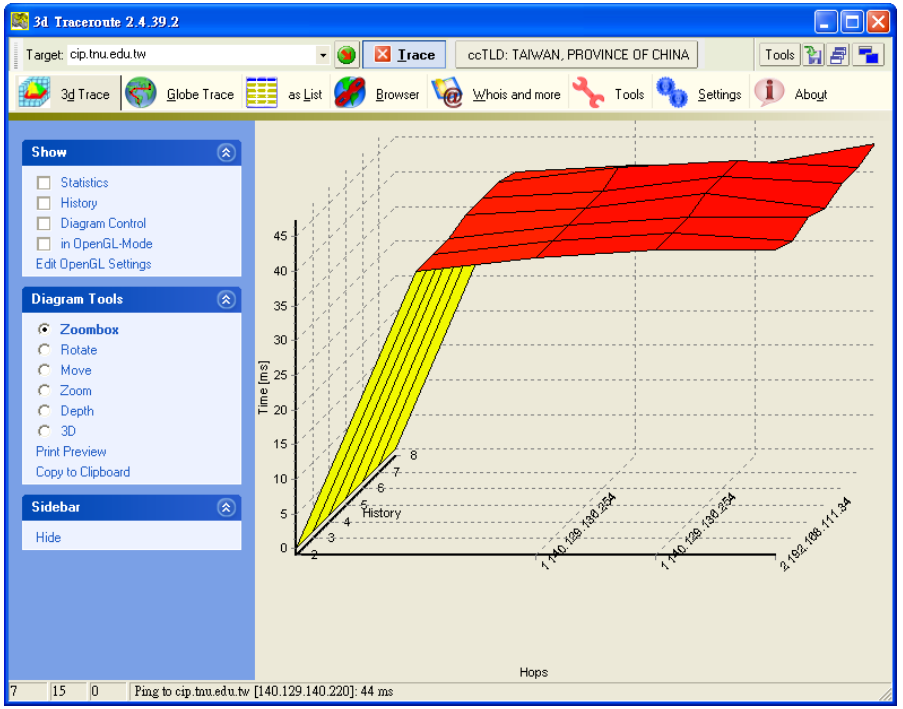
Traceroute

- Traceroute 可以找出主機的來源及路徑資訊，Traceroute 在許多作業系統上都有，是利用 ICMP 協定的特性來工作，這特性稱為 TTL (Time To Live)。Traceroute 會送出 ICMP 封包，並且每次送出不同 TTL (每次加 1)的 ICMP 封包。

- ICMP 封包每經過一個路由器就減1，當 TTL 到達 0 時，路由器會送回"TTL exceeded" 的訊息(ICMP)到原始發送訊息的設備上，於是路徑追蹤就完成了。

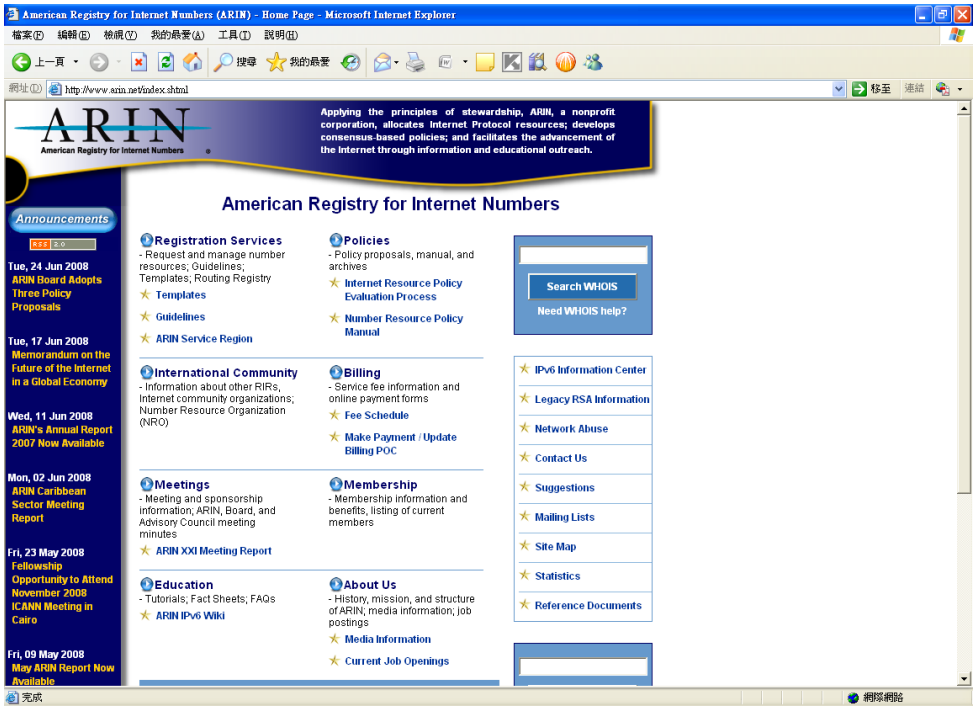
3D Traceroute

- 很好用的節點追蹤工具，能夠將追蹤的結果以 3D 立體圖表繪製，讓你一眼就能看見網路上那一個結點效能不好或者是出了問題。



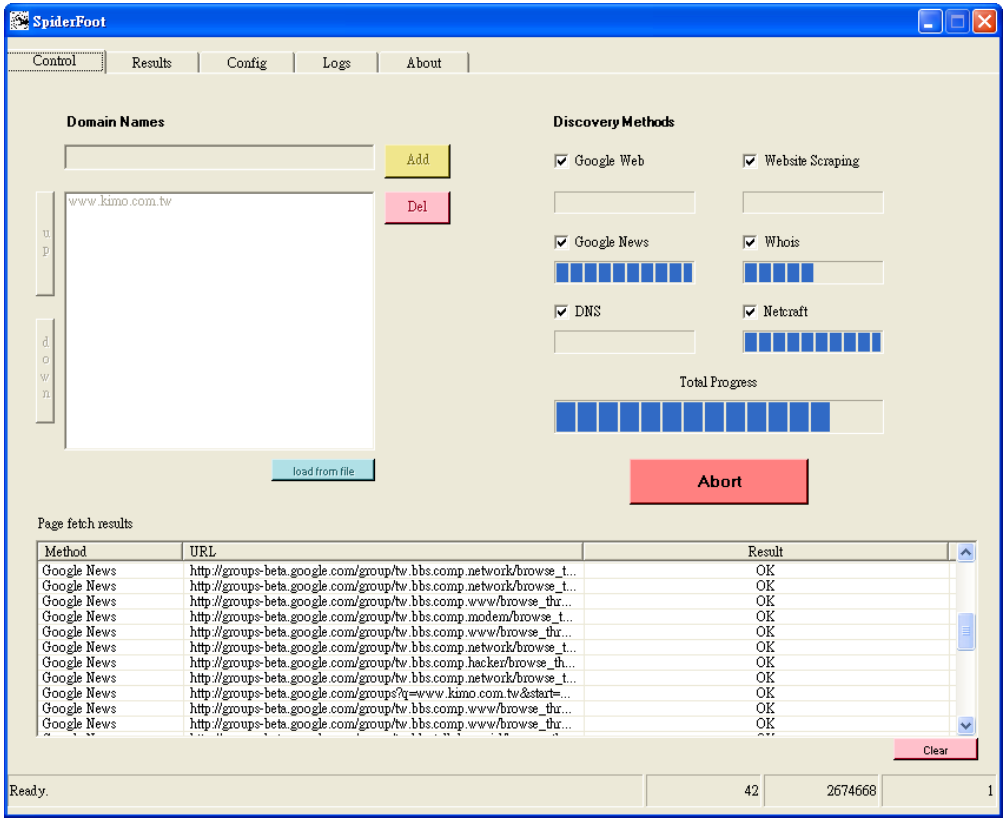
ARIN ：http://www.arin.net

- ARIN 是美洲互聯網號碼註冊管理機構，是一個非營利的機構。



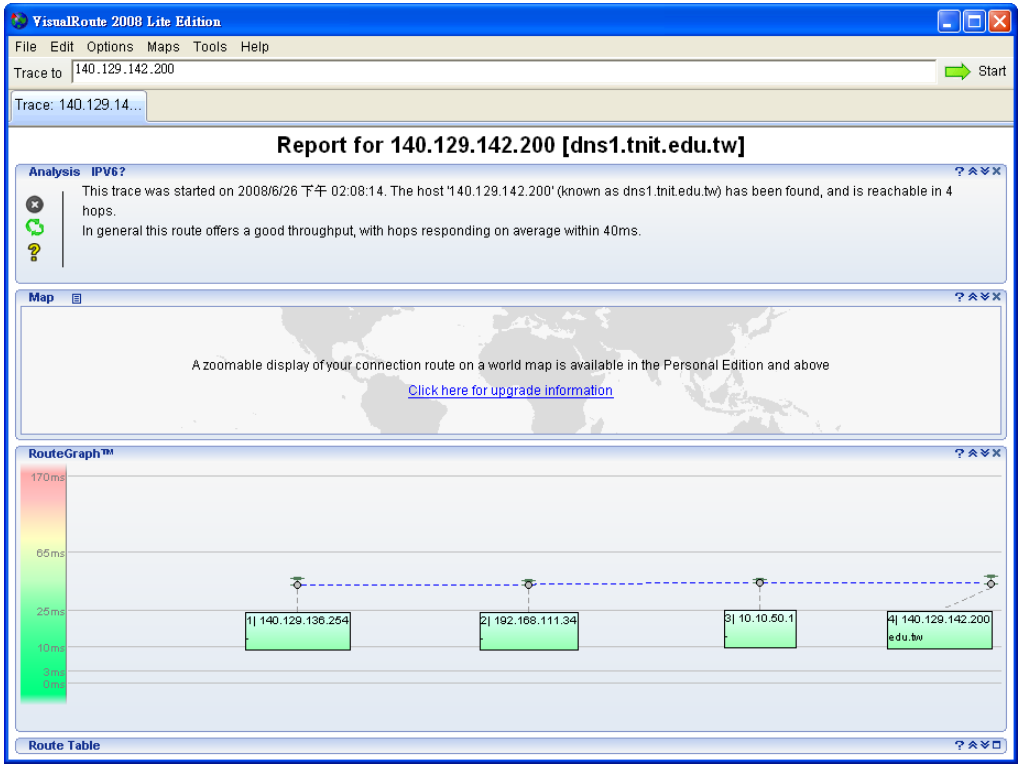
Spiderfoot

- 是一個免費的「足跡」工具程式，能在Google、,Netcraft、,Whois及 DNS 中，將目標網站的相關訊息綜合，包括：：次領域，網頁伺服器的版本，使用者，郵件位址，網路區塊.....等。



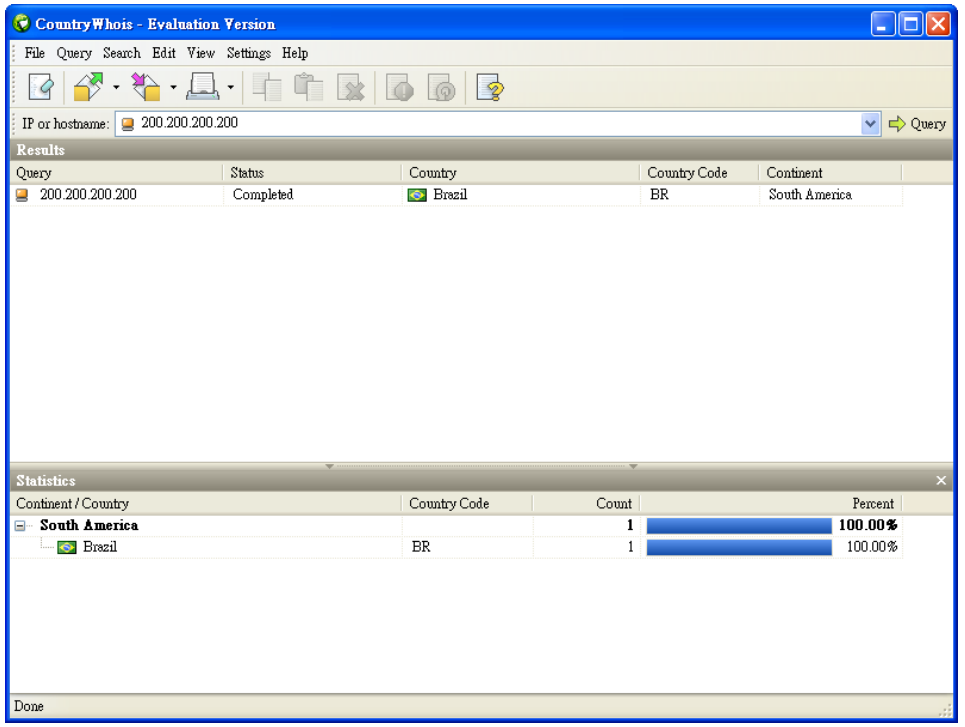
VisualRoute Lite

- 可以監測網路上某個輸入的網站要經過多少個節點，及其連線速度的分析工具軟體，以世界地圖的方式來顯示每一連結的路徑的情況，讓使用者知道當無法連上某些IP網站時，發生問題的點是在哪裡。



SmartWhois

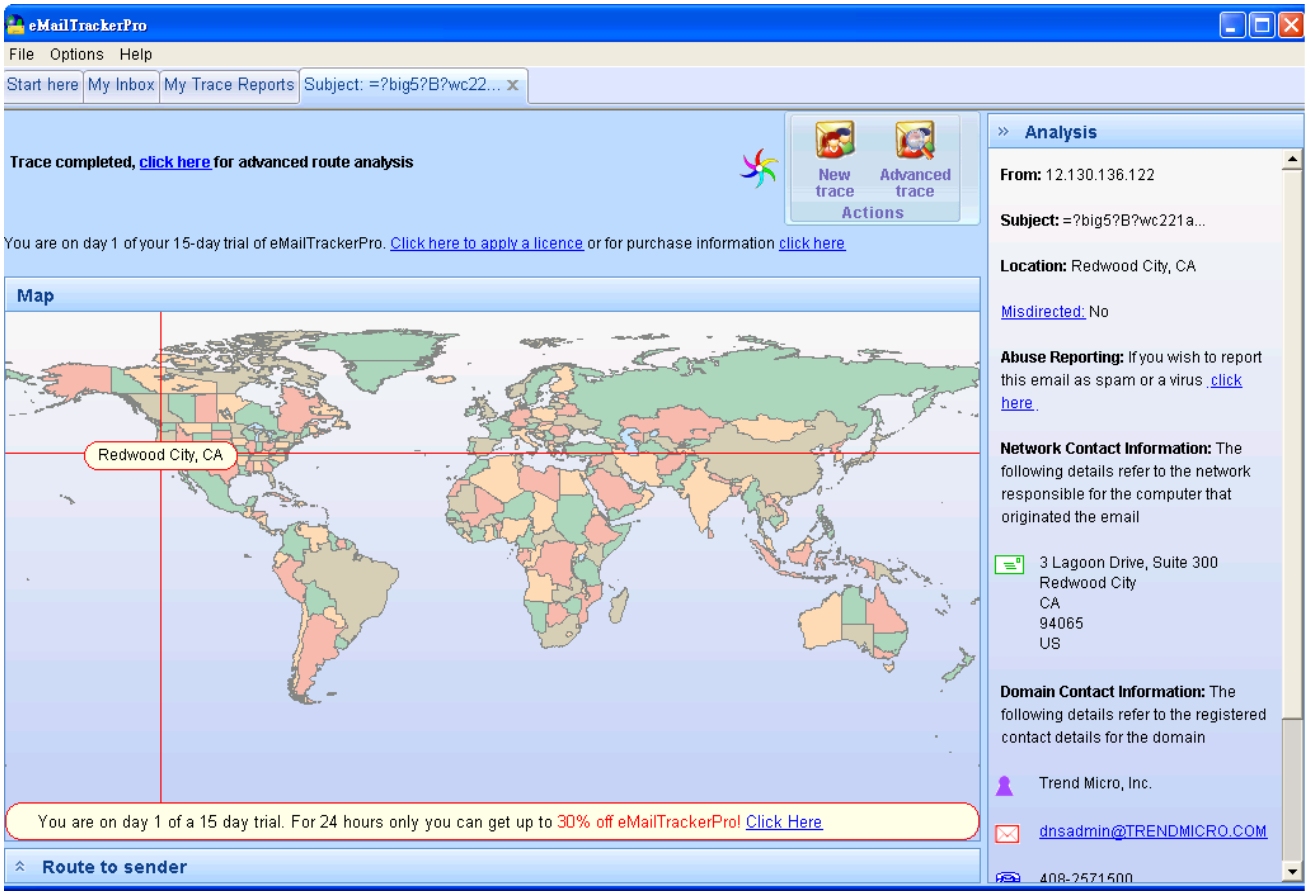
- 此軟體可以尋找出所有有關 IP 位址、主機名稱、領域、包含國家、州郡、市、網路提供者、管理者、及技術支援的資訊。



eMailTrackerPro

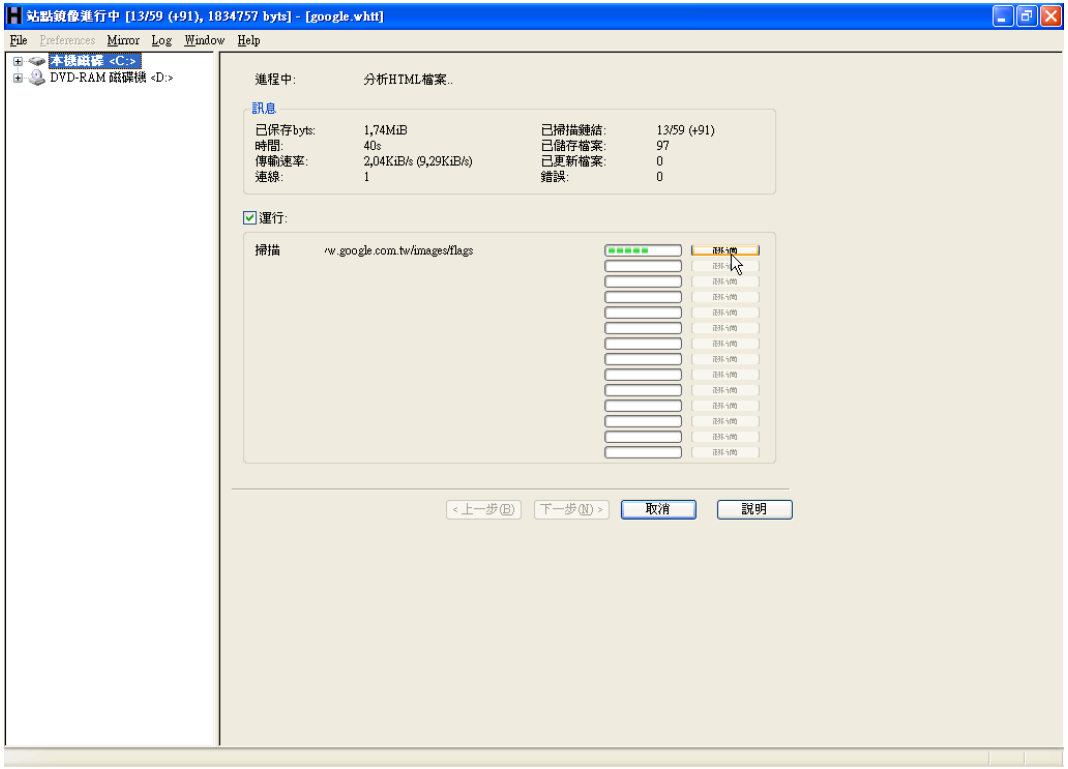
- 是郵件分析工具，能自動的分析郵件的表頭資訊(包括發信的 IP 位址)及並將結果以圖形來表示出發出的所在地位置。
- 右圖是用 Outlook Express 所看到的表頭資訊。

eMailTrackerPro



HTTrack Web Site Copier

- 這個軟體是多國語言版(可選Big5)，是一套相當容易使用的網站映射軟體(也就是俗稱的砍站軟體)，使用上相當方便，而且是免費的。

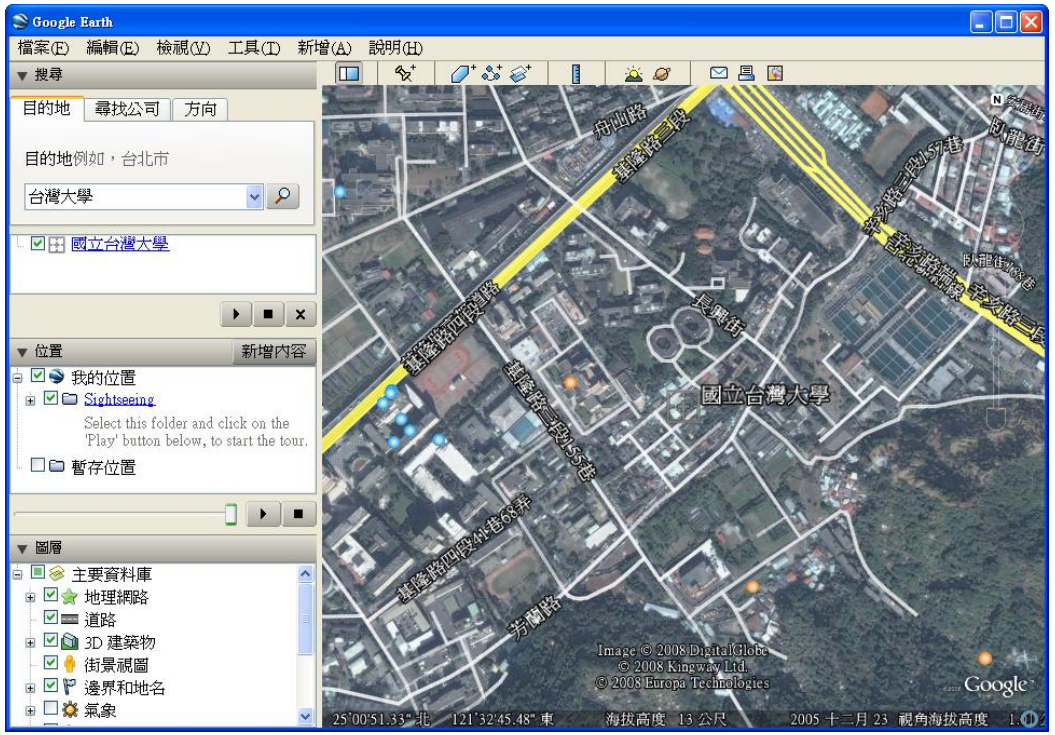


釣魚過程

- 先 Mirror 該網站，例如目標是 www.citibank.com。(利用HTTrack Web Site Copier 等工具程式砍站)
- 註冊一個假的領域名稱，名稱看起來非常接近真的網址。例如：註冊一個 www.citybank.com 網址。
- 將砍站下來的假網頁放在上述網址的伺服器內。
- 送出釣魚信件(phishing e-mail)到被害者的信箱，騙該用戶上這個假網站輸入帳號密碼。

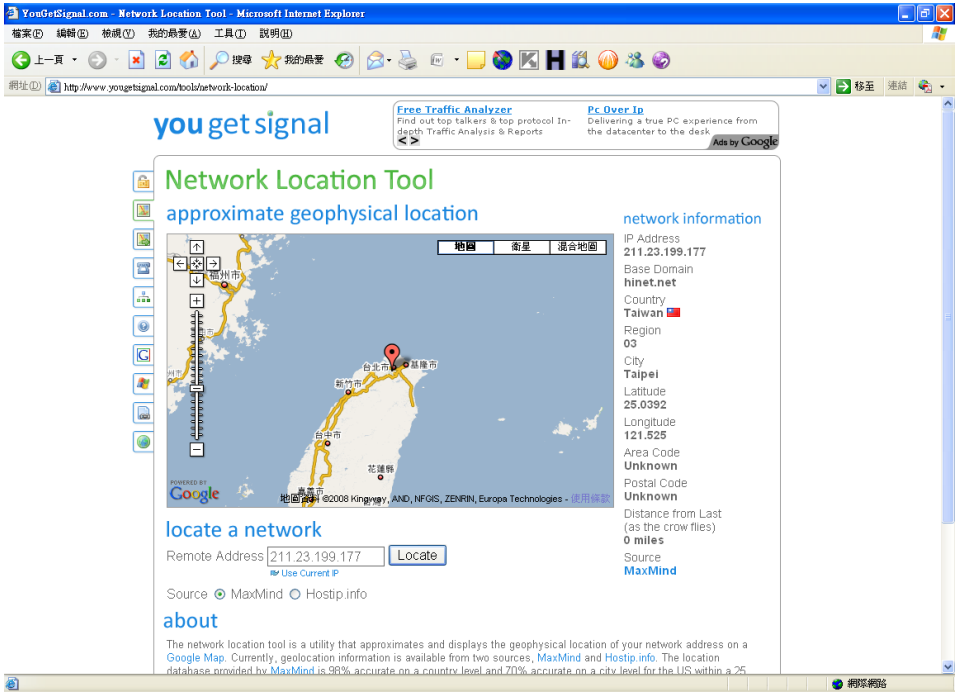
GoogleEarth

- Google 地球能如同飛在地球上空一樣，可以觀看地球的任何地方，可以觀看衛星圖像、地圖、地形圖、3D 建築物甚至到星際中探索星系。

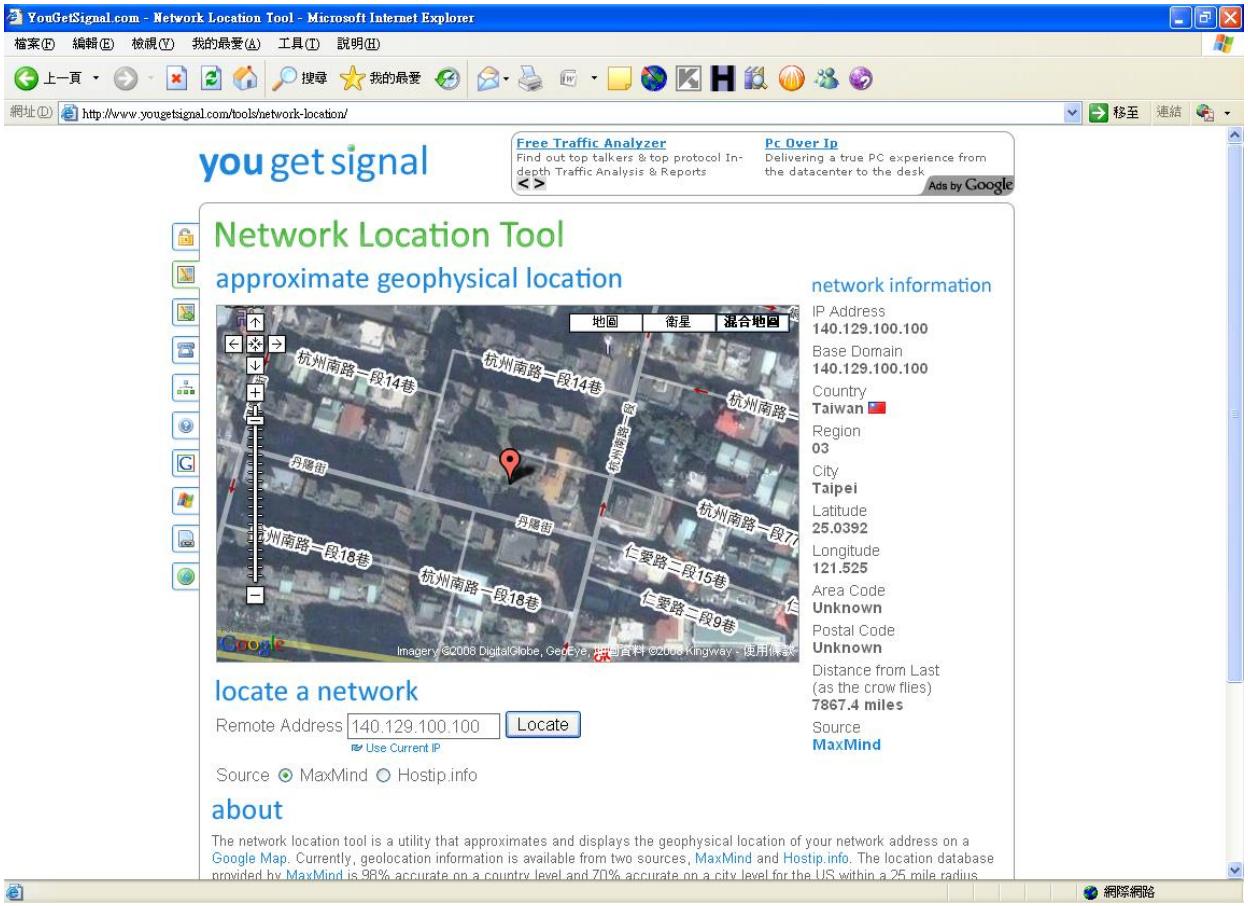


YouGetSignal.com

- 可以查出某個IP的使用位置，並可以利用Google Maps來顯示該地址的地圖。



YouGetSignal.com



「足跡」的主要執行步驟

- 尋找公司內部使用及對外公開的 URL。
- 執行 whois 尋找個人的細節資訊。
- 取得 DNS 及 IP 等相關的資訊。
- 鏡射(Mirror)整個網站及尋找人名（英文）。
- 抽取網頁的重點。
- 使用 Google 搜尋公司的內部的各種新聞及資訊。
- 搜尋僱員的個人資訊。
- 使用工具追蹤伺服器的實體位置。
- 了解公司架構細節。
- 追蹤郵件資訊。

練習

- 利用Google搜尋引擎，尋找10個「台灣大學」的不同URL網址（不能利用網頁連結尋找，只能在google中尋找）。上面實驗中輸入的關鍵字，也可以換成自己單位或組織的名稱。

練習

- 利用www.archive.org 觀察台灣最早架設的網站，在過去十餘年間的改變。
- 台灣最早架設的網站是www.tnjc.edu.tw（1996開始被紀錄），後改名為www.tnit.edu.tw（2001），最近網址又改為www.tnu.edu.tw（2007）。點選畫面中的連結，即可以看到台灣最早的網頁長什麼樣。以及這十餘年間網頁技術的變化。（若有亂碼，瀏覽器字形要選成繁體）
- 請記錄該網址使用的作業系統及網站架站軟體在十餘年間的變化。

練習

- 奇摩網站有兩個網址，分別是tw.yahoo.com及www.kimo.com.tw，選用適當的Whois網站，查詢此網站的註冊住址、Administrative Contact及Technical Contact…等相關資訊。

練習

- 先安裝好eMailTrackerPro（有試用期限），再找一封垃圾郵件（最好是英文的信件），複製這封垃圾郵件的表頭資訊，並使用eMailTrackerPro來檢查這封垃圾郵件，看看是從哪一個國家或地方寄送出來。

練習

- 利用GoogleEarth搜尋以下項目的空照圖，並且看看是否夠清楚：
- （1）自家住宅
- （2）工作或學校的地點

練習

- 利用YouGetSignal.com搜尋以下IP的地理位置圖：

（1）自家的IP

（2）工作或學校使用的電腦IP

（3）202.43.195.13