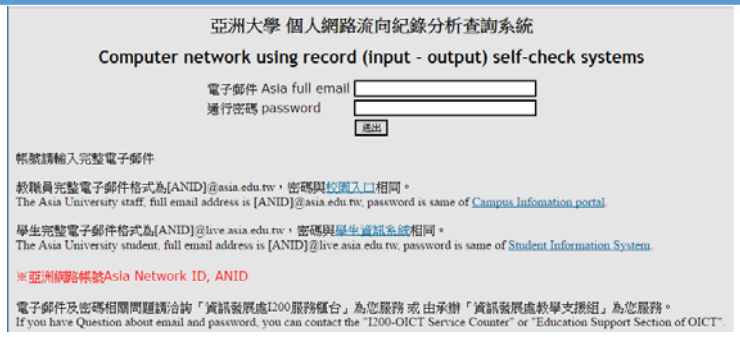
亞洲大學 個人網路流向紀錄分析查詢系統 使用說明
Computer network using record (input - output) self-check systems manual



109.02修訂

網址URL http://userlog.asia.edu.tw
系統目前開放校內查詢

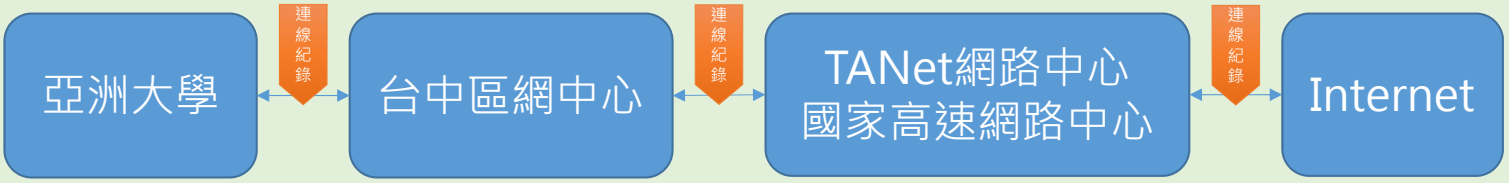
●在系統裡查詢到的資料，這些資料就是您的「網路連線紀錄」(有方向性，來源/目的)。

開始之前，先想想你要查詢什麼
[哪一天] 、[從什麼時間開始]、[要看多久的資料]、[從哪裡來]、[往哪裡去]

當你要查詢某一個時段的紀錄
先設定好查詢條件[日期] [開始時間] [延伸時間] [IP] ，再送出查詢。
要查詢一整天：開始日期的啟動時間 03 00 延伸24hr ，要查詢某時段：開始日期的啟動時間加延伸時間

查詢結果，預設是網頁(html)格式，可以複製到EXCEL，
也可以在查詢之前在[輸出]欄位選擇用[TEXT]存檔成純文字檔案。

「網路連線紀錄」：
通過學校與校外連接的路由器的網路紀錄，有使用過(經過)才會記錄產生連線紀錄，
與校外連線同樣的紀錄在[台中區網中心]及[TANet網路中心]或[國家高速網路中心]都有。



使用Internet只要經過任何一站都會留下足跡，學校只是通往Internet中的一站，也只有在你的電腦連線有經過學校與台中區網中心連線的設備時，才會有對外的使用足跡可以紀錄。
※校內大樓與機房間，也會有網路紀錄存在，查詢時也會出現在紀錄裡，不過並不會計算在使用流量中。

非常抱歉，網路的紀錄只能提供您看到歷史資料，只能知道
[連線開始與結束的時間]、[從外部進/從內部出]、[時段內的連線數量]、
[每一個連線使用的流量]及[每一個連線使用的封包數量]
沒有辦法知道您的電腦發生什麼事情。
[哪個程式設定不對]、[哪個程式在攻擊]、[哪個程式下載了多少東西]、[電腦有沒有中毒]、
[哪個網站開了會一直增加使用流量]、[電腦休眠後有沒有在下載東西].....等等等
這些都不會知道，**所有的東西都只在您的電腦裡，當您有發現異常的網路紀錄或流量產生，請檢查您電腦**。

在**「超過流量限制與異常清單」**中，阻斷原因為「網路行為異常」

IP封鎖資料區

帳號	IP	啟動封鎖時間	解除封鎖時間	原因	群組流量	總流量	限用量	異常原因
		2015-07-13 14:15	請與系統管理者聯絡	網路行為異常				session,

在[異常原因]欄位都會有與「您的電腦發生的狀況」同樣類型的網路行為說明，
您可以依照相同類型狀況的處理方式檢查您的電腦問題。(就是電腦已經發生問題了，請儘速修復它。)
網路行為異常放著不管的話，嚴重時會阻塞那一樓層的對外網路，同一樓層其他使用對外網路的人就會覺得變很慢，所以會暫時阻斷那個IP的對外網路，到電腦問題排除為止。

亞洲大學 個人網路流向紀錄分析查詢系統 使用說明
Computer network using record (input - output) self-check systems manual

查詢條件欄位

(01) [年月日] 要查詢的那一天
(02) [開始時間] 從何時開始
(03) [延伸] 從開始時間多久，延伸越久越慢
(04) [您的IP] 請輸入您的IP (可登入網管系統查詢)
(05) [Size] 可以設定檔案大小滿足條件才顯示
如：大於1MB的才顯示
1000000 <size< [空白]
(06) [行數] 每一頁出現幾行紀錄
(07) [輸出方式]紀錄查詢後以HTML(網頁)呈現或TXT(純文字檔)存檔。
(08) [確定]開始查詢及[清除]查詢條件
(09) [登出系統] 使用完登出系統，請記得

查詢結果欄位

表格中的每一列(筆)資料表示一個連線(session)的紀錄。
正常情況下，打開一個網頁同時間不會超過50個連線(大部分都在7~20個連線，除非那個網頁很用力的推廣告給你)。

順序	來源IP	來源服務Port	目的IP	目的服務Port	Protocol	Pkts	size
順序	從哪來的	來源設備使用的網路連接埠	到哪裡去	目的設備使用的網路連接埠	使用的通訊協定 Ex. TCP, UDP, ICMP	使用的網路封包數量	傳輸檔案的大小 Byte，1KB=1024Byte, 1MB=1024KB, 1GB=1024MB

啟動時間	停止時間
這個連線開始的時間	這個連線結束的時間

流量統計

每日03:00至隔日03:00，[size]欄位的加總(需扣除校內連線)。
※連線SESSION要在「停止時間」後才會有網路記錄產生，那時才有紀錄能夠計算流量。

簡單的例子-固定時間段的連線紀錄

我的電腦IP是10.41.1.1

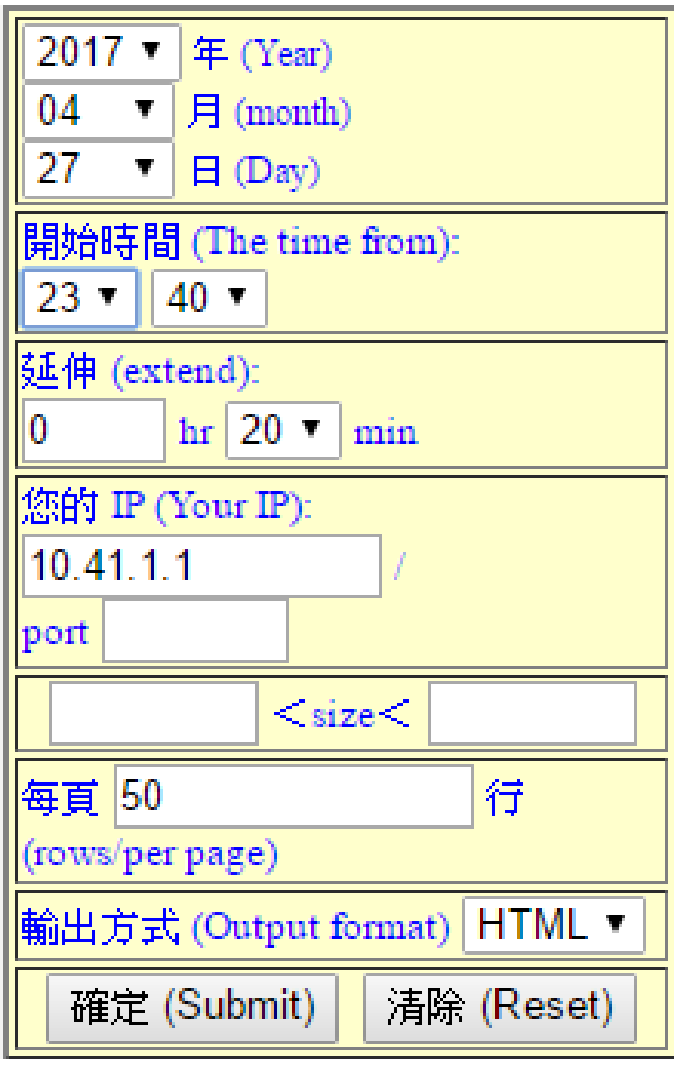
我的電腦在2017-04-27的23:55

因為[網路行為異常 Attacker] session 而被阻斷

2017-04-27 23:55	2017-04-29 00:00	網路行為異常 Attacker				session,

我應該查詢的是被阻斷5分鐘前，我的電腦產生了多少的網路連線。

紀錄的內容也許可以提供線索，來檢查我的電腦是哪一個應用程式或病毒在作怪



我的條件設定應該是

2017年　04月　27日

開始時間　23:40以後

延伸　20分鐘 (到00:00)

我的IP是10.41.1.1

所有服務port都列出(空白)

所有大小都列出

每一頁列出50行

在網頁顯示

簡單的例子-固定時間段的連線紀錄

我的電腦IP是10.41.1.1

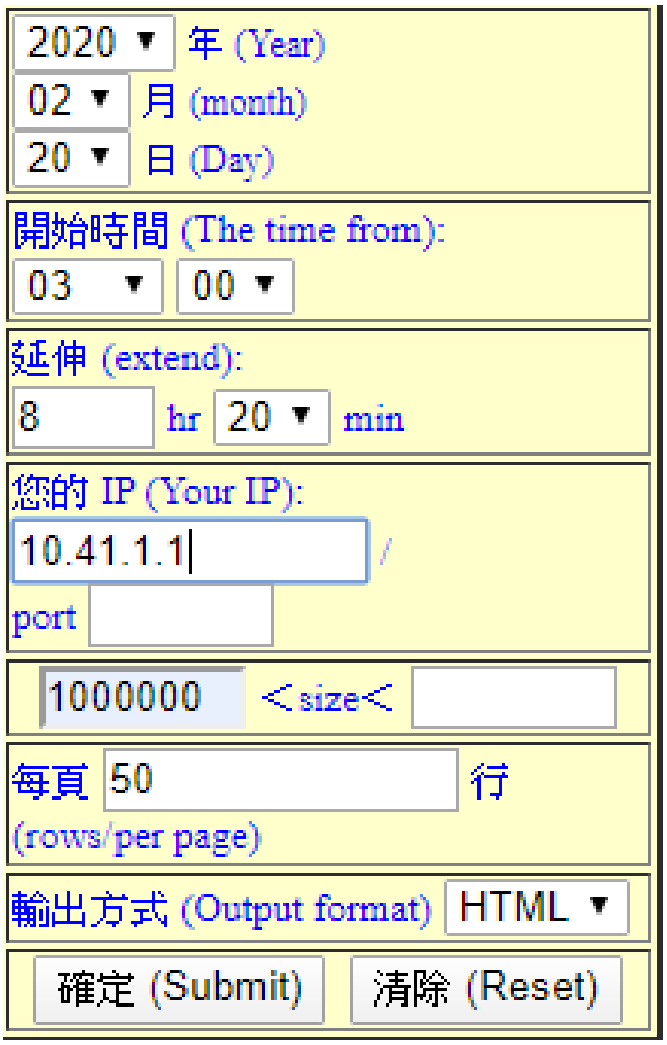
我的電腦在2017-04-27的23:55

因為[網路行為異常 Attacker] session 而被阻斷

2020-02-20 11:10	2020-02-21 03:00	使用超過每日流量上限 over traffic		7427 MB	0 MB

我應該查詢的是從當日的AM03:00到 被阻斷的時間(AM11:10)，有多少流量從校外到我的電腦。

紀錄的內容也許可以提供線索，來檢查我的電腦是從哪裡下載檔案



我的條件設定應該是

2020年　02月　20日

開始時間　AM03:00

延伸　8小時20分鐘 (到11:20)

我的IP是10.41.1.1

所有服務port都列出(空白)

列出大於1MB的紀錄

每一頁列出50行

在網頁顯示