

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

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

電子郵件 Asia full email

通行密碼 password

帳號請輸入完整電子郵件
教職員完整電子郵件格式為[ANID]@asia.edu.tw，密碼與校園入口相同。
The Asia University staff, full email address is [ANID]@asia.edu.tw, password is same of [Campus Information portal](#).
學生完整電子郵件格式為[ANID]@live.asia.edu.tw，密碼與學生資訊系統相同。
The Asia University student, full email address is [ANID]@live.asia.edu.tw, password is same of [Student Information System](#).

※亞洲網路帳號Asia Network ID, ANID

電子郵件及密碼相關問題請洽詢「資訊發展處1200服務櫃台」為您服務 或由承辦「資訊發展處教學支援組」為您服務。
If you have Question about email and password, you can contact the "1200-OICT Service Counter" or "Education Support Section of OICT".

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。

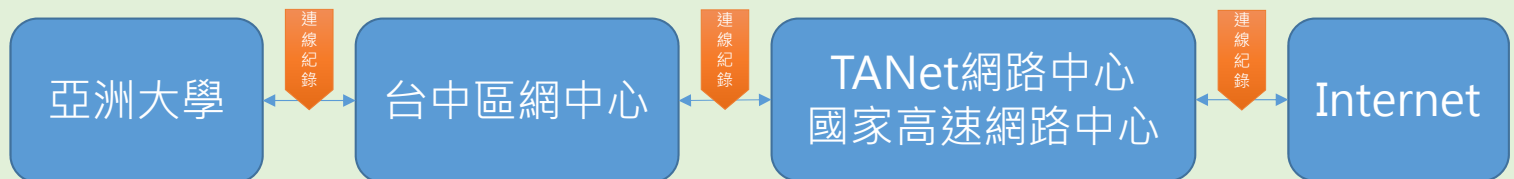
要查詢一整天：開始日期的啟動時間 03 00 延伸24hr，要查詢某時段：開始日期的啟動時間加延伸時間

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，才会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

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							
編號	IP	啟動封鎖時間	解除封鎖時間	原因	詳細流量	總流量	預用量
		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。

2017 ▾ 年 (Year) (01)

04 ▾ 月 (month)

28 ▾ 日 (Day)

開始時間 (The time from): (02)

14 ▾ 20 ▾

延伸 (extend): (03)

0 hr 20 min

您的 IP (Your IP): (04)

10.10.10.10 /

port

< size <

每頁 50 行 (06)

(rows per page)

輸出方式 (Output format) HTML ▾ (07)

確定 (Submit) 清除 (Reset)

IP-FLOW流向查詢									
960筆資料,共有20頁 請選擇第 1 ▾ 頁 下十頁 > 前往第 1 頁 確定									
順序	來源IP	來源服務Port	目的IP	目的服務Port	Protocol	packets	size	啟動時間	停止時間
1	如果您的IP	57,225	如果您的IP	443	6 (tcp)	14	1,773	04-28 14:19:50	04-28 14:19:56
2	出現在這欄位	57,226	出現在這欄位	443	6 (tcp)	6	985	04-28 14:19:56	04-28 14:19:56
3	表示連線是	57,228	表示連線是	443	6 (tcp)	6	846	04-28 14:20:02	04-28 14:20:02
4	從	3,128	從	57,196	6 (tcp)	26	13,170	04-28 14:18:29	04-28 14:20:02
5	您的電腦	57,227	您的電腦	443	6 (tcp)	14	1,912	04-28 14:19:56	04-28 14:20:02
6	網際網路	57,229	網際網路	443	6 (tcp)	14	1,773	04-28 14:20:02	04-28 14:20:08
7	連往	57,230	連往	443	6 (tcp)	6	846	04-28 14:20:08	04-28 14:20:08
8	您的電腦	57,242	您的電腦	443	6 (tcp)	6	846	04-28 14:20:14	04-28 14:20:14
9	網際網路	57,231	網際網路	443	6 (tcp)	14	1,773	04-28 14:20:08	04-28 14:20:14
10	連往	443	連往	54,125	6 (tcp)	124	12,112	04-28 13:48:21	04-28 14:20:20
11	您的電腦	80	您的電腦	57,249	6 (tcp)	5	1,308	04-28 14:20:20	04-28 14:20:20
12	網際網路	80	網際網路	57,248	6 (tcp)	5	1,308	04-28 14:20:20	04-28 14:20:20
13	網際網路	54,125	網際網路	443	6 (tcp)	134	10,960	04-28 13:48:21	04-28 14:20:21
14	網際網路	57,243	網際網路	443	6 (tcp)	14	1,773	04-28 14:20:14	04-28 14:20:20
15	網際網路	57,246	網際網路	443	6 (tcp)	6	846	04-28 14:20:20	04-28 14:20:20
16	網際網路	57,249	網際網路	80	6 (tcp)	5	367	04-28 14:20:20	04-28 14:20:20
17	網際網路	57,248	網際網路	80	6 (tcp)	5	366	04-28 14:20:20	04-28 14:20:20
18	網際網路	57,251	網際網路	443	6 (tcp)	6	846	04-28 14:20:26	04-28 14:20:26
19	網際網路	57,253	網際網路	443	6 (tcp)	6	846	04-28 14:20:26	04-28 14:20:26
20	網際網路	57,254	網際網路	443	6 (tcp)	6	846	04-28 14:20:26	04-28 14:20:26
21	網際網路	80	網際網路	57,250	6 (tcp)	6	2,099	04-28 14:20:20	04-28 14:20:26
22	網際網路	57,247	網際網路	443	6 (tcp)	14	1,773	04-28 14:20:20	04-28 14:20:26

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)。

IP-FLOW流向查詢									
5393筆資料,共有270頁 請選擇第 1 ▾ 頁 下十頁 > 前往第 1 頁 確定									
順序	來源IP	來源服務Port	目的IP	目的服務Port	Protocol	pkts	size	啟動時間	停止時間
1	10.34.	50,129	111.111.111.111	80	6 (tcp)	2	96	03-14 11:54:58	03-14 11:55:01
2	10.34.	50,023	111.111.111.111	80	6 (tcp)	2	104	03-14 11:54:58	03-14 11:55:01
3	10.56.	54,476	111.111.111.111	80	6 (tcp)	2	104	03-14 11:54:58	03-14 11:55:01

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

2017 ▾ 年 (Year)
04 ▾ 月 (month)
27 ▾ 日 (Day)
開始時間 (The time from):
23 ▾ 40 ▾
延伸 (extend):
0 hr 20 ▾ min
您的 IP (Your IP):
10.41.1.1 /
port
< size <
每頁 50 行 (rows/per page)
輸出方式 (Output format) HTML ▾
確定 (Submit) 清除 (Reset)

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

2020 ▾ 年 (Year)
02 ▾ 月 (month)
20 ▾ 日 (Day)
開始時間 (The time from):
03 ▾ 00 ▾
延伸 (extend):
8 <input type="text"/> hr 20 ▾ min
您的 IP (Your IP):
<input type="text" value="10.41.1.1"/> /
port <input type="text"/>
<input type="text" value="1000000"/> < size < <input type="text"/>
每頁 50 <input type="text"/> 行
(rows/per page)
輸出方式 (Output format) HTML ▾
<input type="button" value="確定 (Submit)"/> <input type="button" value="清除 (Reset)"/>

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