

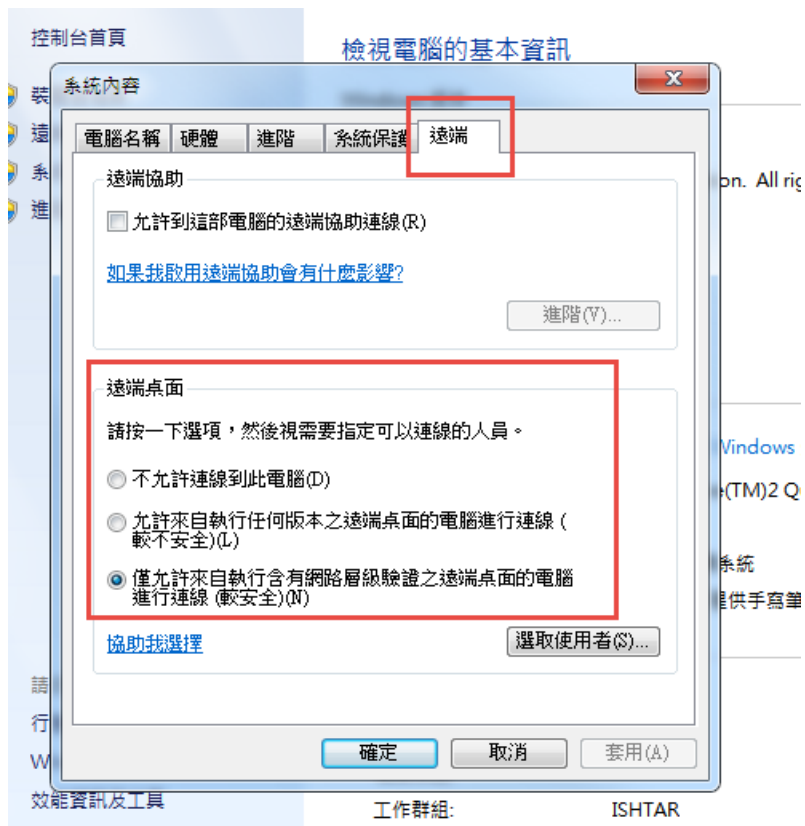
1. 先檢查有沒有開遠端桌面，開始->電腦上按右鍵->選內容



2. 打開內容後，點選進階系統設定



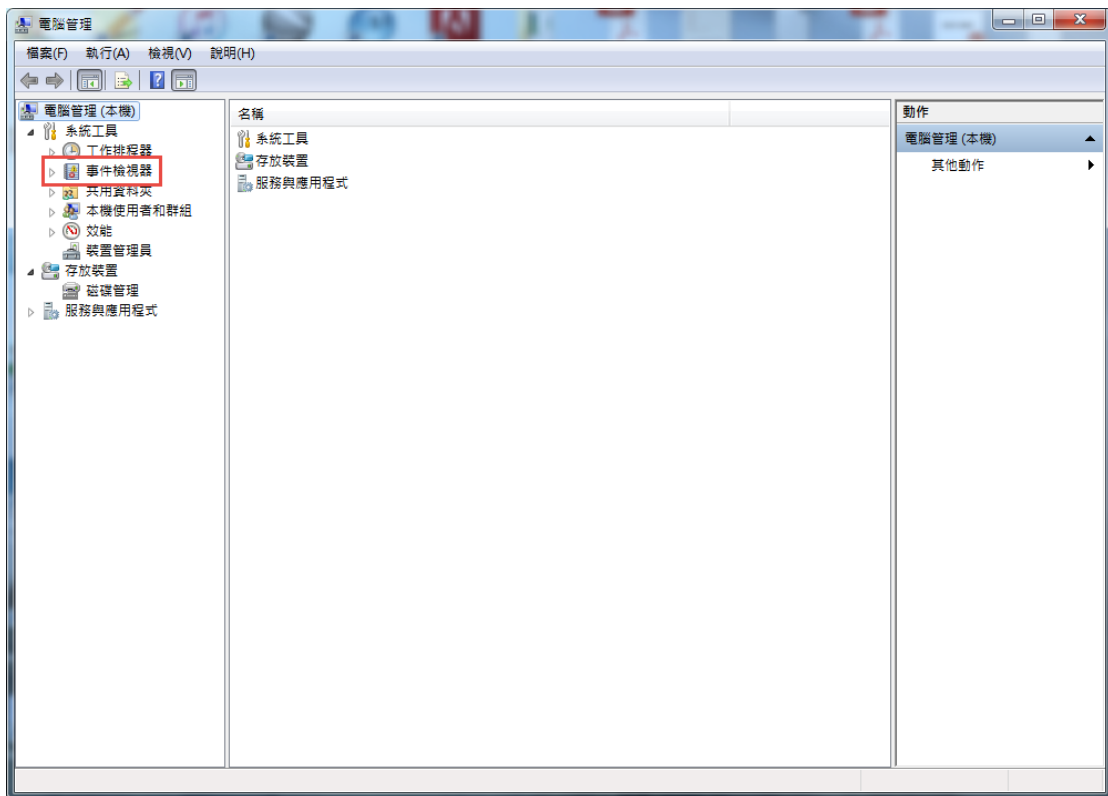
3. 點到「遠端」那個分頁，看一下遠端桌面如果是選下面兩項，就表示有開遠端桌面。



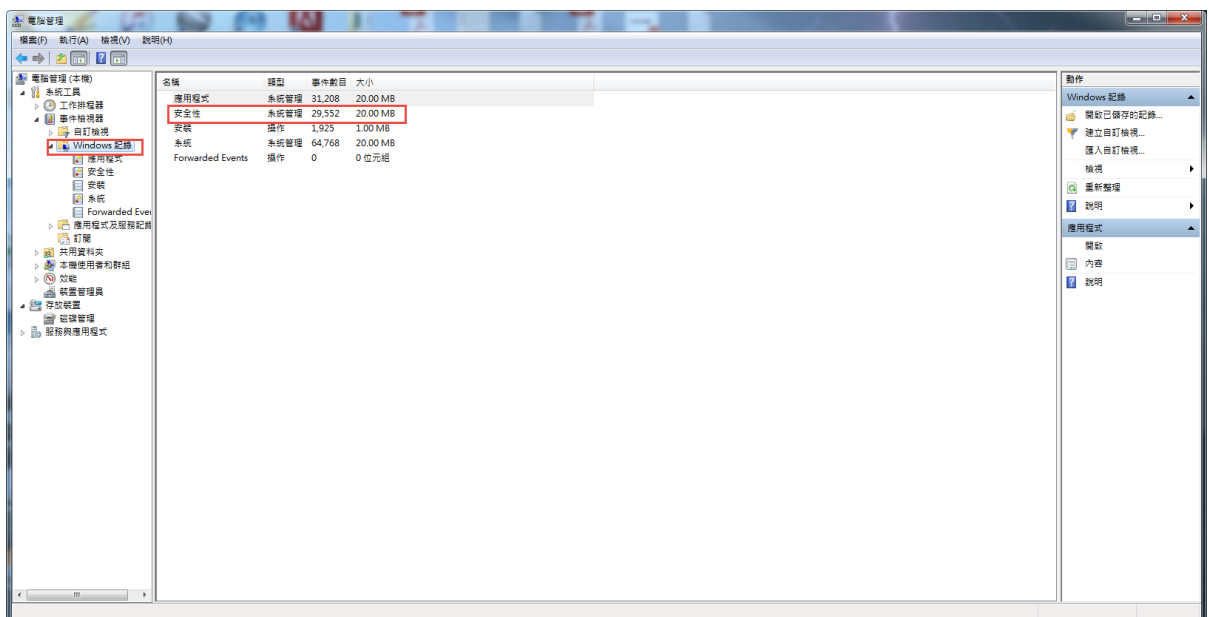
4. 如果有開遠端桌面，就請查一下系統事件紀錄。開始->電腦上按右鍵->選管理。



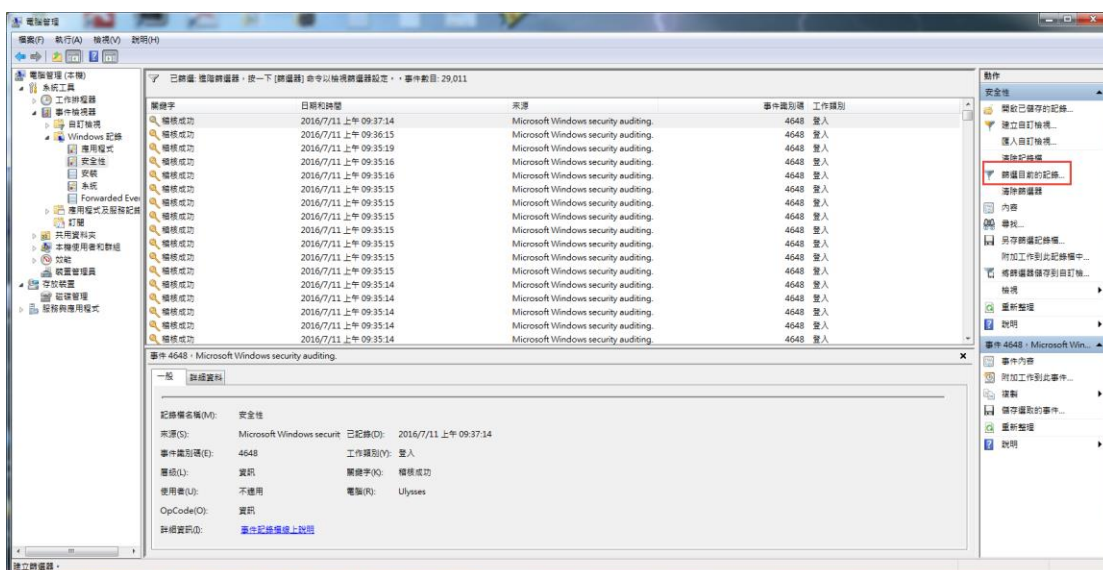
5. 點開電腦管理裡的事件檢視器



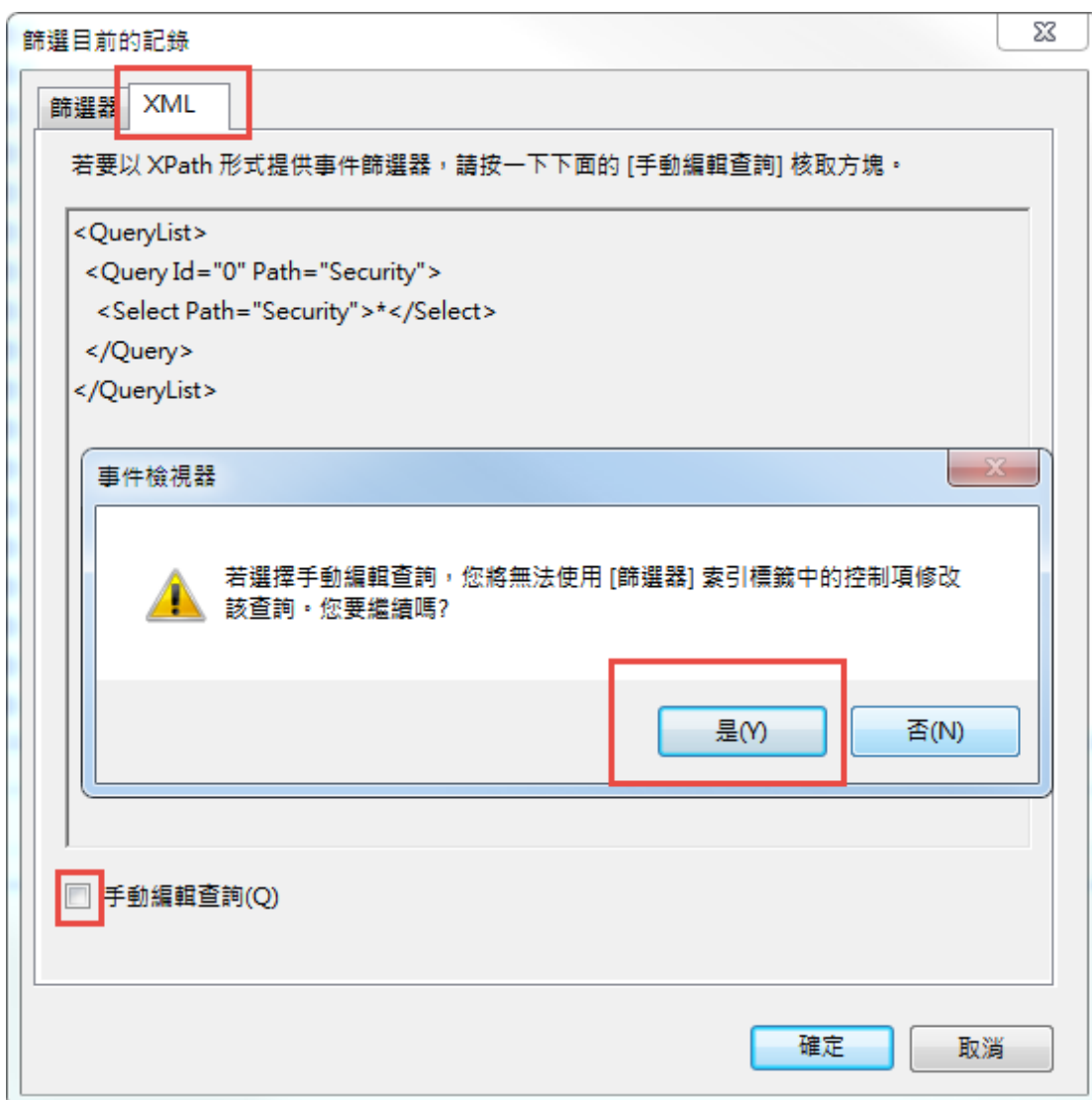
6. 依序點選 Windows 紀錄，安全性點兩下



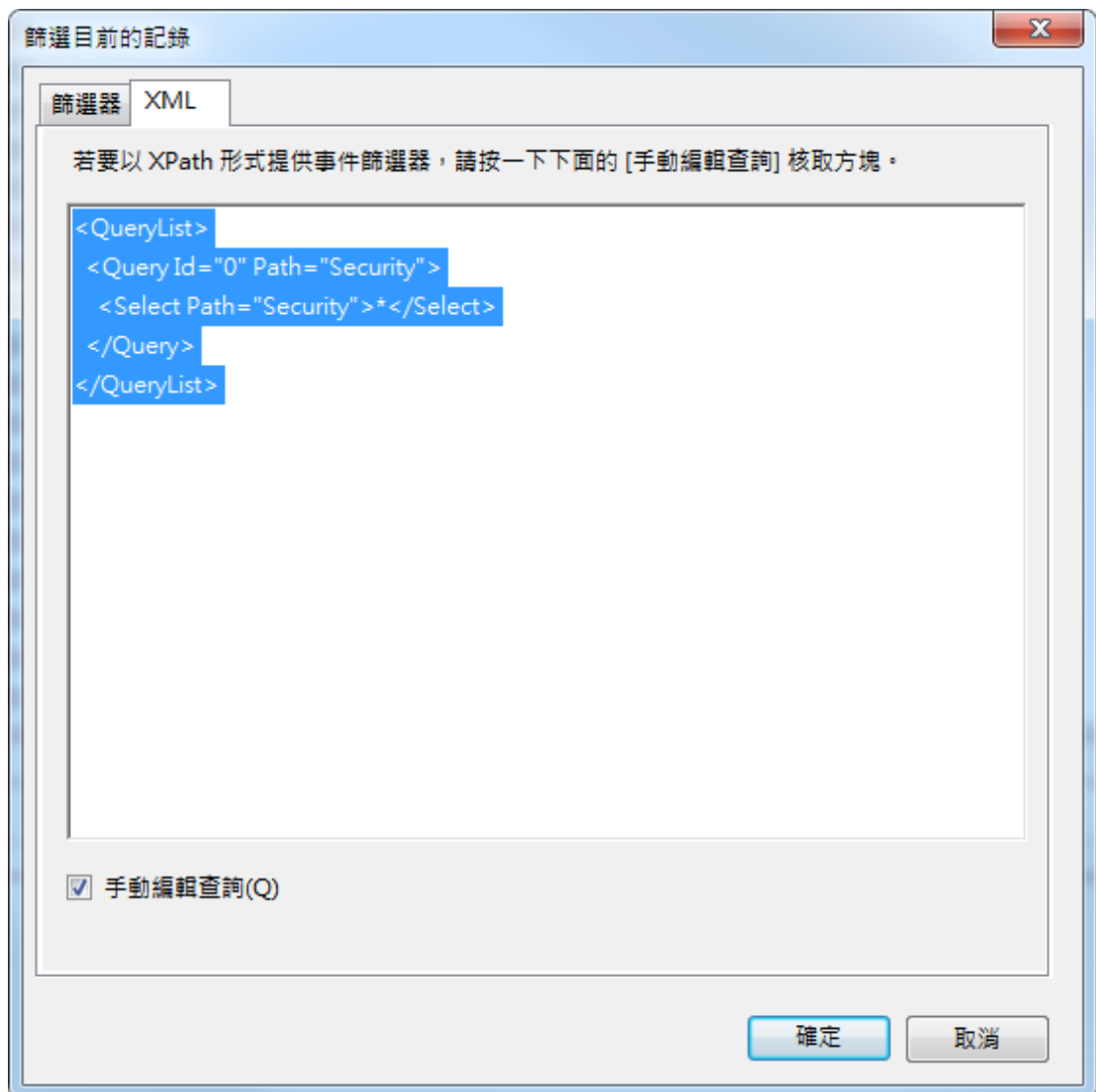
7. 點右邊的篩選目前的紀錄



8. 在篩選目前的紀錄視窗裡，選 XML 分頁，勾選手動編輯查詢，出現的詢問視窗，選是

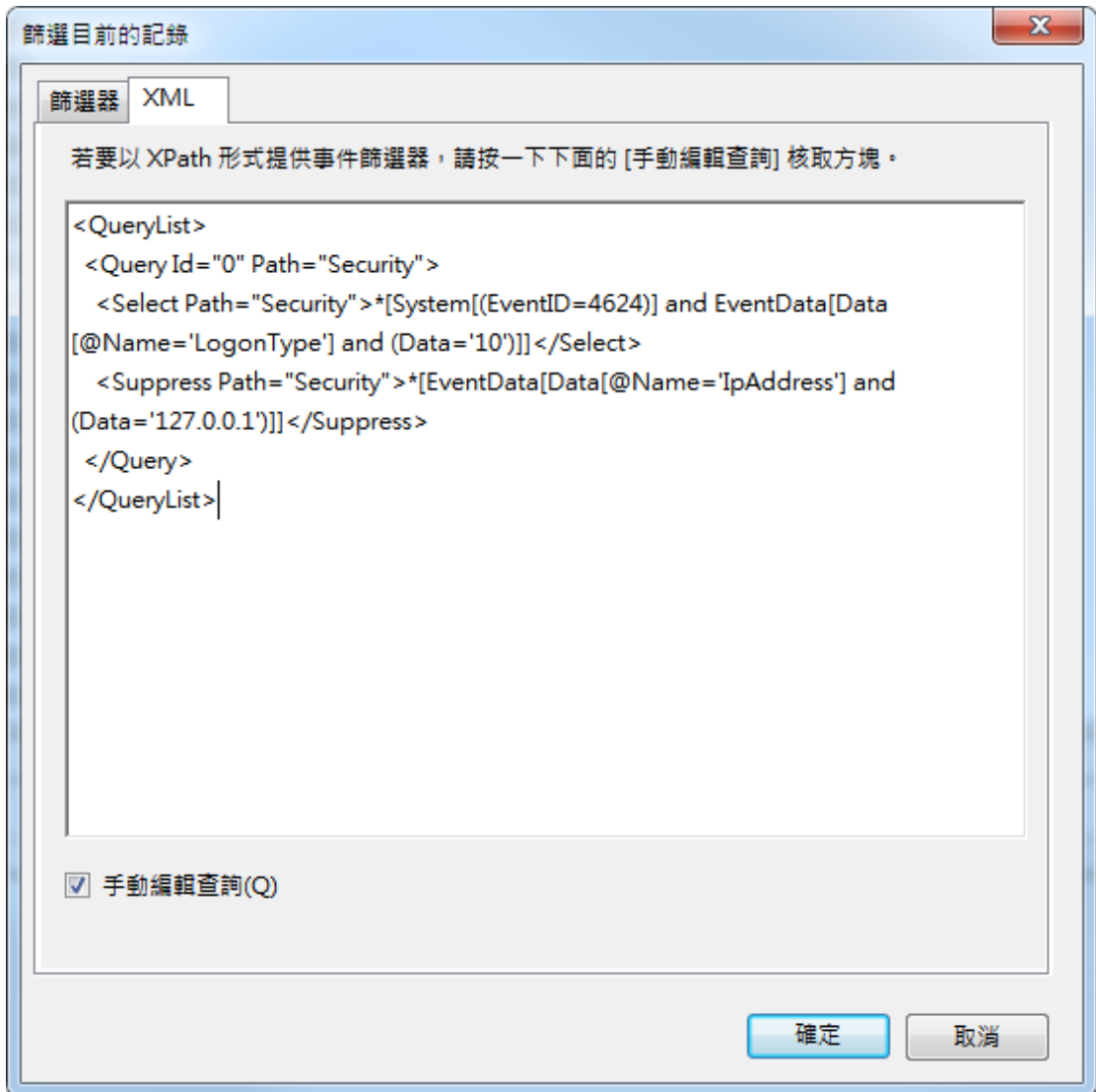


9. 把編輯窗裡的 XML 全選，按 Delete 鍵刪除



10. 再用 ctrl-v 把下面這段 XML 貼上

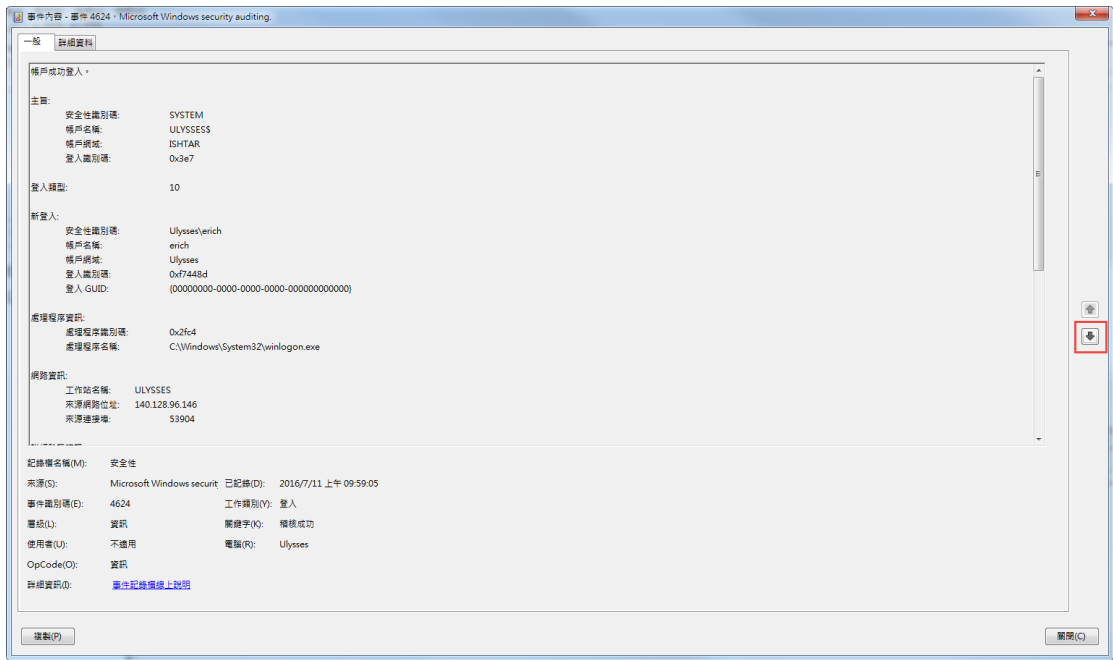
```
<QueryList>
  <Query Id="0" Path="Security">
    <Select Path="Security">*[System[(EventID=4624)] and
EventData[Data[@Name='LogonType'] and (Data='10')]]</Select>
    <Suppress Path="Security">*[EventData[Data[@Name='IpAddress'] and
(Data='127.0.0.1')]]</Suppress>
  </Query>
</QueryList>
```



11. 按下確定後，就可以看到遠端登入的紀錄了

圖示字	日期和時間	來源	事件類別碼	工作類別
	2016/7/11 上午 09:59:05	Microsoft Wi...	4624	登入
	2016/7/11 上午 09:59:05	Microsoft Wi...	4624	登入
	2016/6/22 下午 02:20:11	Microsoft Wi...	4624	登入

12. 點兩下第一條，或找到此次事件發生的時間點附近的紀錄點兩下。打開檢視視窗。並盡量拉大直到可以看到來源網路位址。右方有上下按鍵可以切換紀錄。



13. 請比對是否有出現異常的 IP

如何查 IP

<https://www.whois365.com/tw/>

全球 WHOIS 查詢 [關於 全球 WHOIS 查詢](#) [gTLD & ccTLD 列表](#) [工具](#) [English](#) [简体中文](#)

"開始免費做自己的網站"
3分鐘打造您的專業網站。用SimpleSite免費且容易！到 [singlesite.com/免費做網頁](https://singlesite.com/)

請輸入網域名稱或 IP 位址 [說明](#)

IP 位址：106.113.222.41
IP 位置：中國 

IANA WHOIS 主機：whois.iana.org
% IANA WHOIS server