二、研究計畫內容(以10頁為限):

(一)摘要

本計畫將透過anaconda所提供的編譯器spyder來開發，利用python所寫出的scapy網路封包分析函式來挖掘和監測封包，配合Nprobe來偵測網路流量，利用netflow v9的流量分析資料表格標準得到封包數據，找到有問題的封包或是不正常的數據流量，並將資料進行分類，將需要的資料儲存在SQLite資料庫中，使用Scikit-learn實作機器學習，進行使用者上網行為分析，並以圖表方式呈現，能記錄下上網情形，且達到即時發現和防範網路上的不安全因素的效果。

(二)研究動機與研究問題

近年python語言越來越受到歡迎，除了簡潔的語法與程式碼可讀性外，提供了非常多的套件可以使用，而在網路分析方面，不管是netflow的python版本還是scapy函式都非常強大且實用，所以才有了使用python擷取封包實作使用者上網行為分析的想法。

因應大數據潮流與網路安全管理日漸重要，因而有此計畫，透過封包分析，讓公司管理者清楚了解員工的網路使用情形，得知何者或何事佔用了頻寬，或是能夠了解公司網路的尖峰使用時間，做為頻寬分配或使用者限制的參考標準，能讓管理者更方便管理和做後續應用。

個人使用方面，能夠了解自己的上網習慣，將常使用的網站名稱或是IP鍵入資料庫內容，進行上網行為分析，當有與以往不同且不正常的上網行為發生時能及時發現，並找出問題，讓對網路沒有深入了解者也能大略知道網路的使用情形。

最簡單的分析方式就是建立port number的分析，如做出https,DNS,http幾種服務的比例圖，如果https比例最多，代表網路流量以網頁服務為主，此種方式能做粗略的上網行為分析。如果要做再更深入一點的紀錄，便是將造訪的網站和造訪次數鍵入資料庫內，將類似於http協定的網站，這種安全性較低的網站記下，讓人可以點擊查詢。有太多太多的資料及方式能進行網路管理，但是這也造成網路資料繁多且複雜，讓一般人難以了解自己流量到底被甚麼占用，即使電腦被攻擊或入侵也不知道。

本研究基於以上動機，希望設計一個能幫助不管是管理者還是使用者都能使用的程式，如果有一程式能將較為重要資料如流量、特殊封包種類等，先分類規劃好放入資料庫內，結合用戶流量分析和web訪問分析的方式，以圖表方式呈現，那這樣能讓網路管理者更方便進行網路管理，清楚得知使用者平時的上網行為，那將會方便許多，使用者也不會對自己網路情形一無所知。

(三)文獻回顧與探討

(六)參考文獻

[1]<http://support.huawei.com/hedex/pages/EDOC1000089429DZE1112R/03/EDOC1000089429DZE1112R/03/resources/vsm_cfg/analyze/vsm_cfg_analyze_0500.html>

[2] <http://www.cc.ntu.edu.tw/chinese/epaper/0044/20180320_4407.html>

[3]