105學年(上)期末報告

網路流量分析研究

Research on Network Traffic Analysis

指導教授:柯志亨

組長:黃政哲(110310522)
組員:陳俊瑋(110310524) 郭　瀟(110310551)
蕭　徹(110310534)　林坤皇(110310548)

概　要

- 緒論
  - 研究背景動機
  - 預計成果
  - 本學期研究目標
  - 專案流程圖
- 期末進度報告
- 軟體介紹
  - 介面
  - DEMO / 實際操作
- 參考資料
- 附錄
  - 程式操作
  - 程式架構
  - 程式原理

緒論

研究背景

在這個資訊爆炸的時代，周圍時時刻刻充斥著無數的網路訊號；
無論是在有線還是無線，都有著巨量的資料正在傳輸。

這些網路訊息不被人們所看見，不被人們所聽見；
他們是由0與1組合而成的資訊，這些資訊和我們現代人類生活息息相關。

躲在我們的背後，在資訊世界裡，到底暗藏著哪些玄機？
值得我們一探究竟。

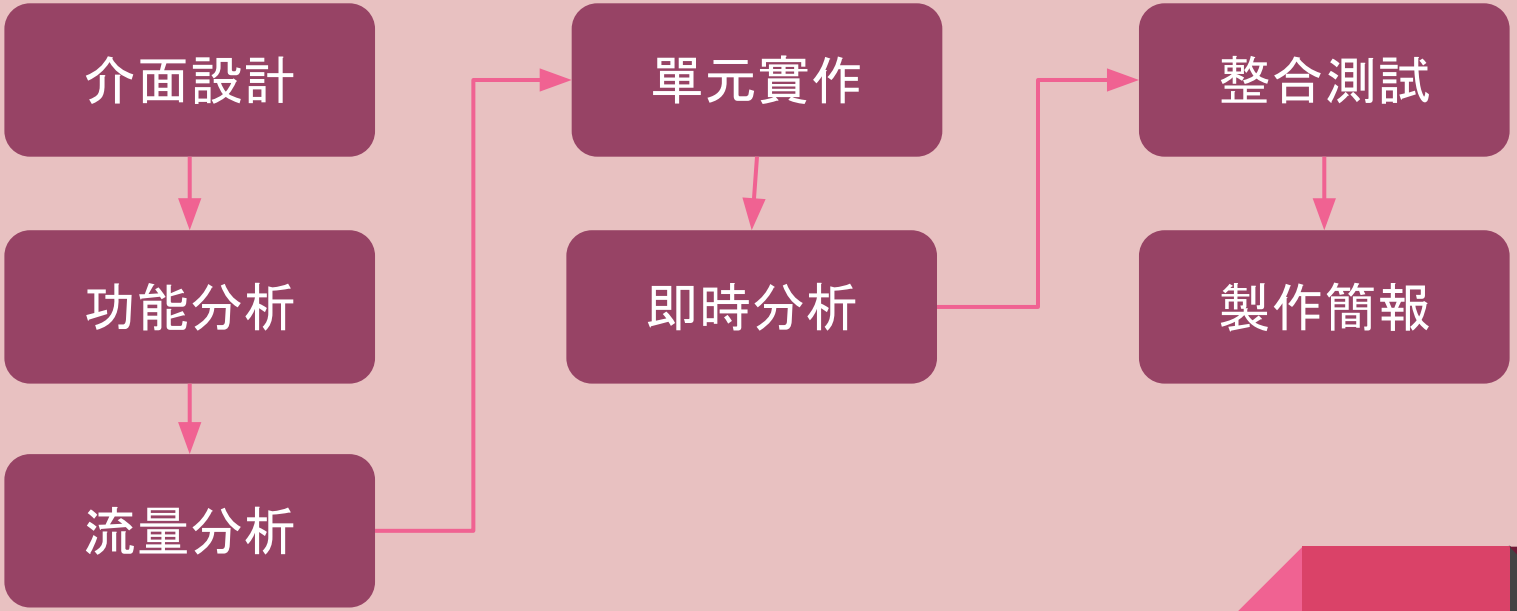
預期成果

- 製作出一個應用程式(或app) 
- 具有親民的UI界面
- 能夠抓取目前的流量並即時分析 
- 提供視覺化的統計數據
- 給予使用者適當的建議(ex提醒使用者異常的流量)

本學期研究目標

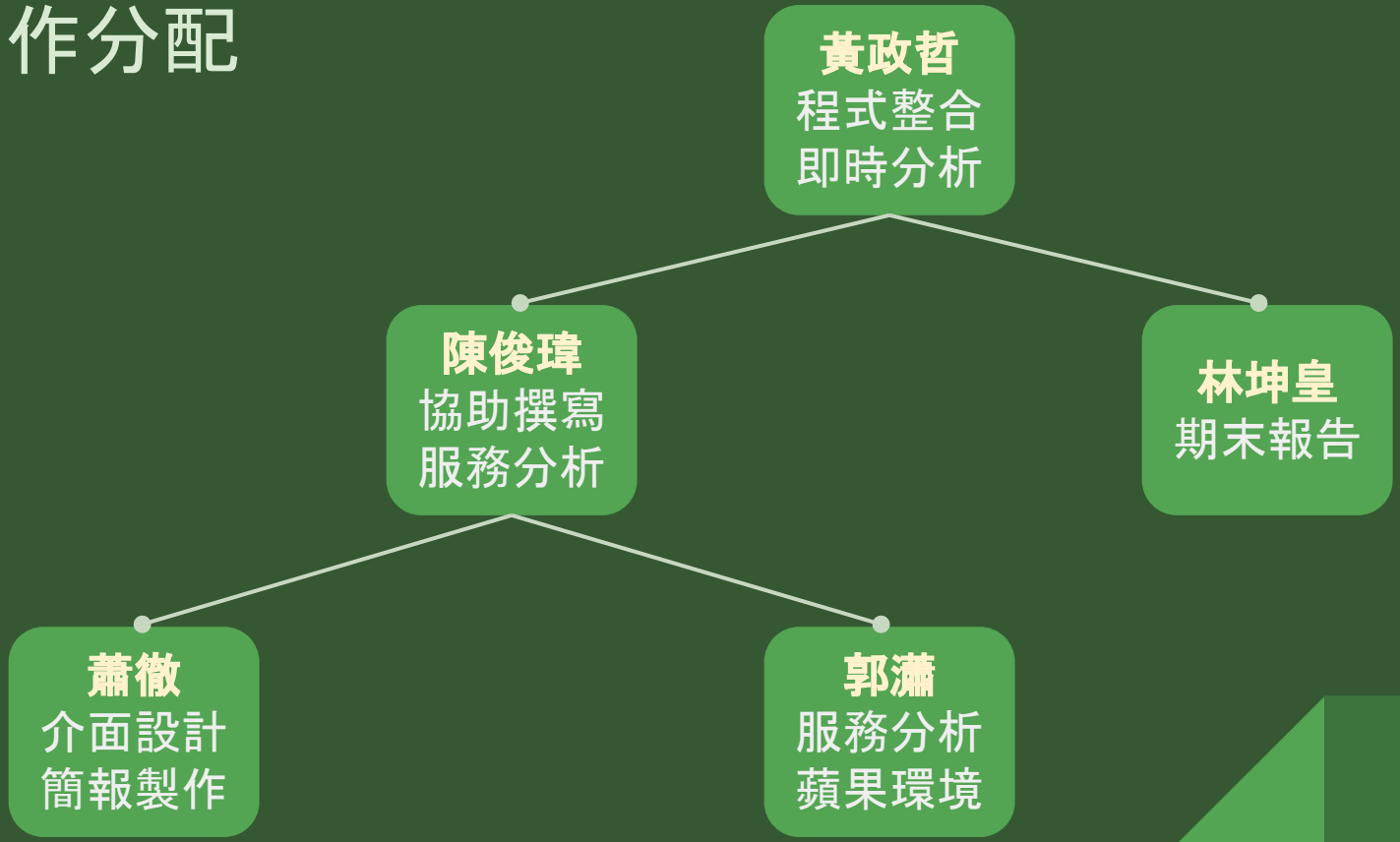
- 熟悉常見的通訊協定以及標頭格式 
- 初步攔截封包工具製作 
- 初步分析各裝置的流量數據 
- 初步分析流量中各種服務資料的數據

專案流程圖

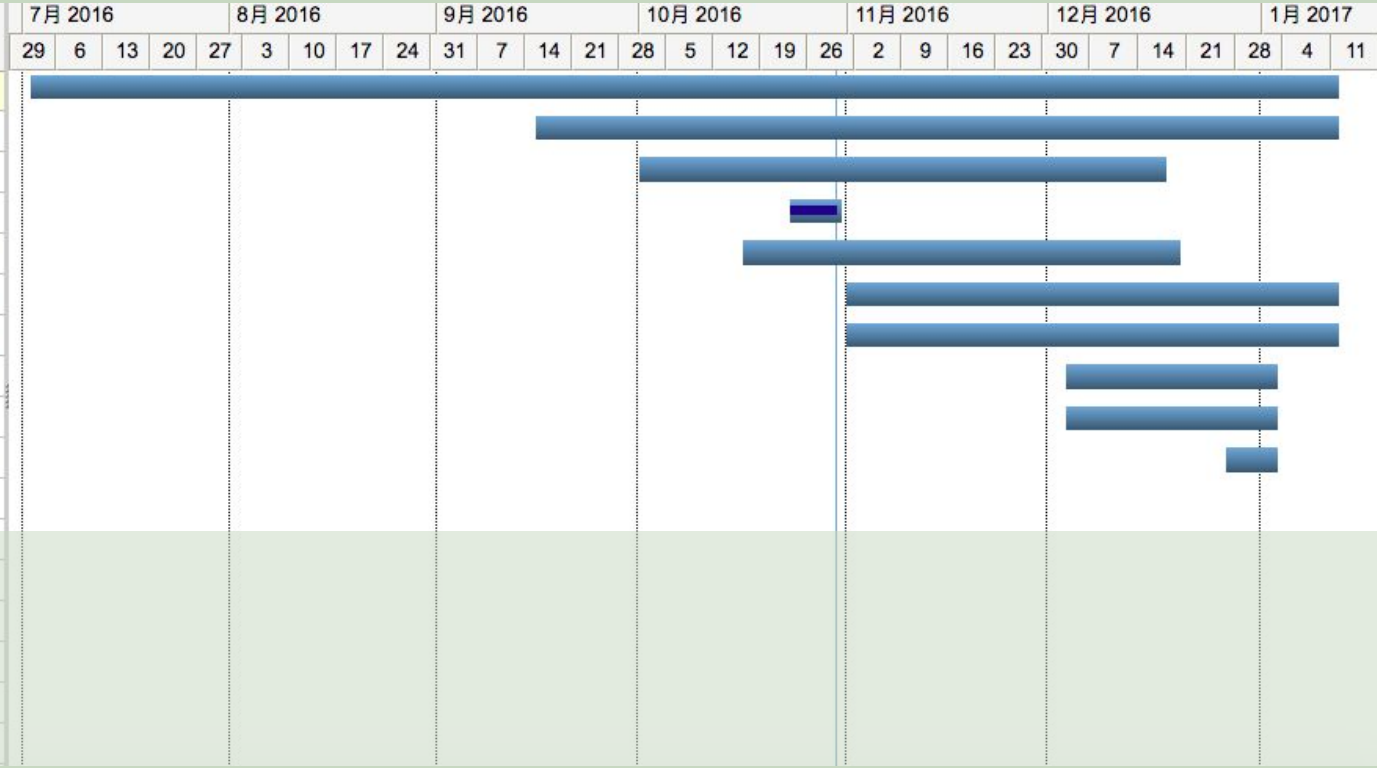


期末進度報告

工作分配



名称	工期	开始	结束
蒐集資料	136天?	07/01/2016	01/06/2017
攔截封包	85天	09/12/2016	01/06/2017
熟悉網路通訊協定	55天?	09/27/2016	12/12/2016
期中報告製作	6天	10/19/2016	10/26/2016
分析封包工具製作	46天?	10/12/2016	12/14/2016
設計UI	52天?	10/27/2016	01/06/2017
工具整合	52天?	10/27/2016	01/06/2017
視覺化工具製作	23天?	11/28/2016	12/28/2016
即時分析功能整合	23天?	11/28/2016	12/28/2016
期末報告製作	6天?	12/21/2016	12/28/2016



研究進度表

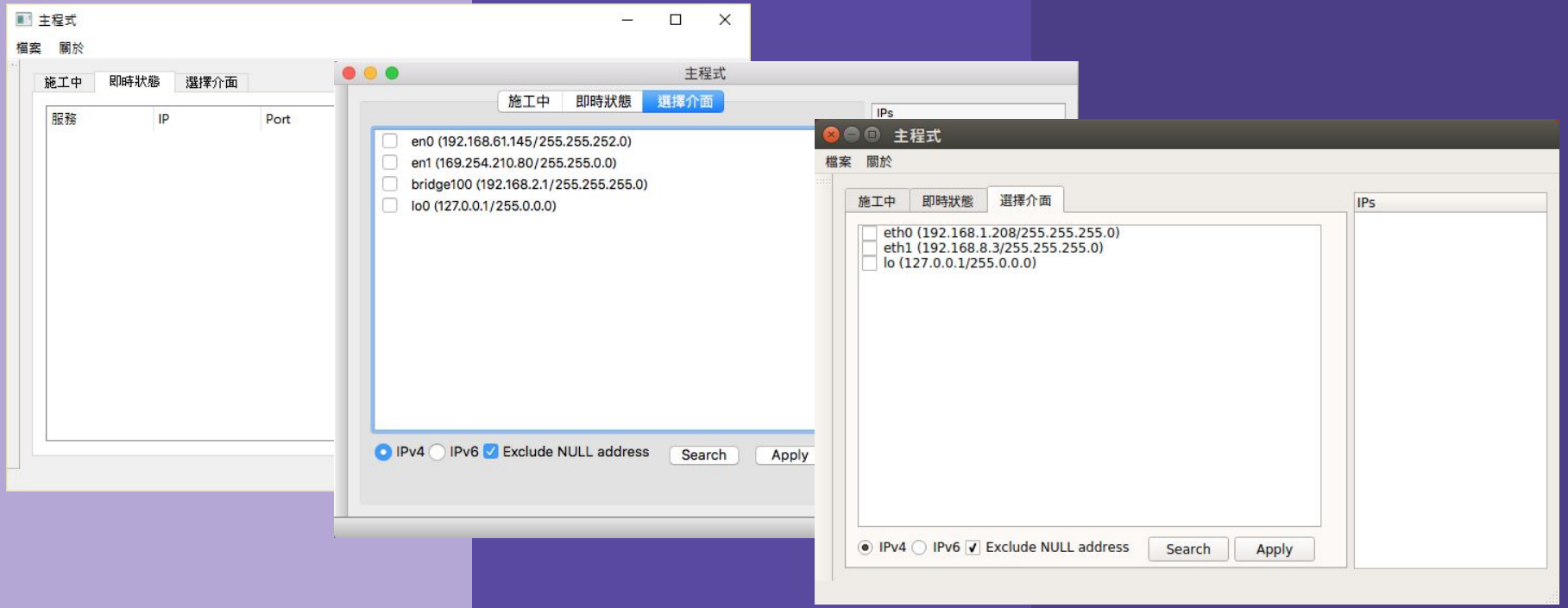
軟體介紹

Qt介紹 - 支援的大平台

Windows 10

Mac OS X

Ubuntu



程式功能

- 選擇監聽介面 
- 過濾服務流量 
- 即時更新功能 
- 可改變要過濾的服務 
- 跨平台 

情境分析

DEMO

實際操作

未來展望

未來我們希望結合嵌入式系統raspberry pi來延伸應用，如點名系統:利用學生手機的實體網路卡位置來判斷學生是否在場，或著是利用:在某展覽的各櫃位前放置裝置，搜集附近裝置的資訊停留時間，進而分析各展覽攤位的吸引程度。

參考資料

http://www.tcpdump.org/pcap.html

https://www.qt.io/

Google圖片

Q & A

發問時間

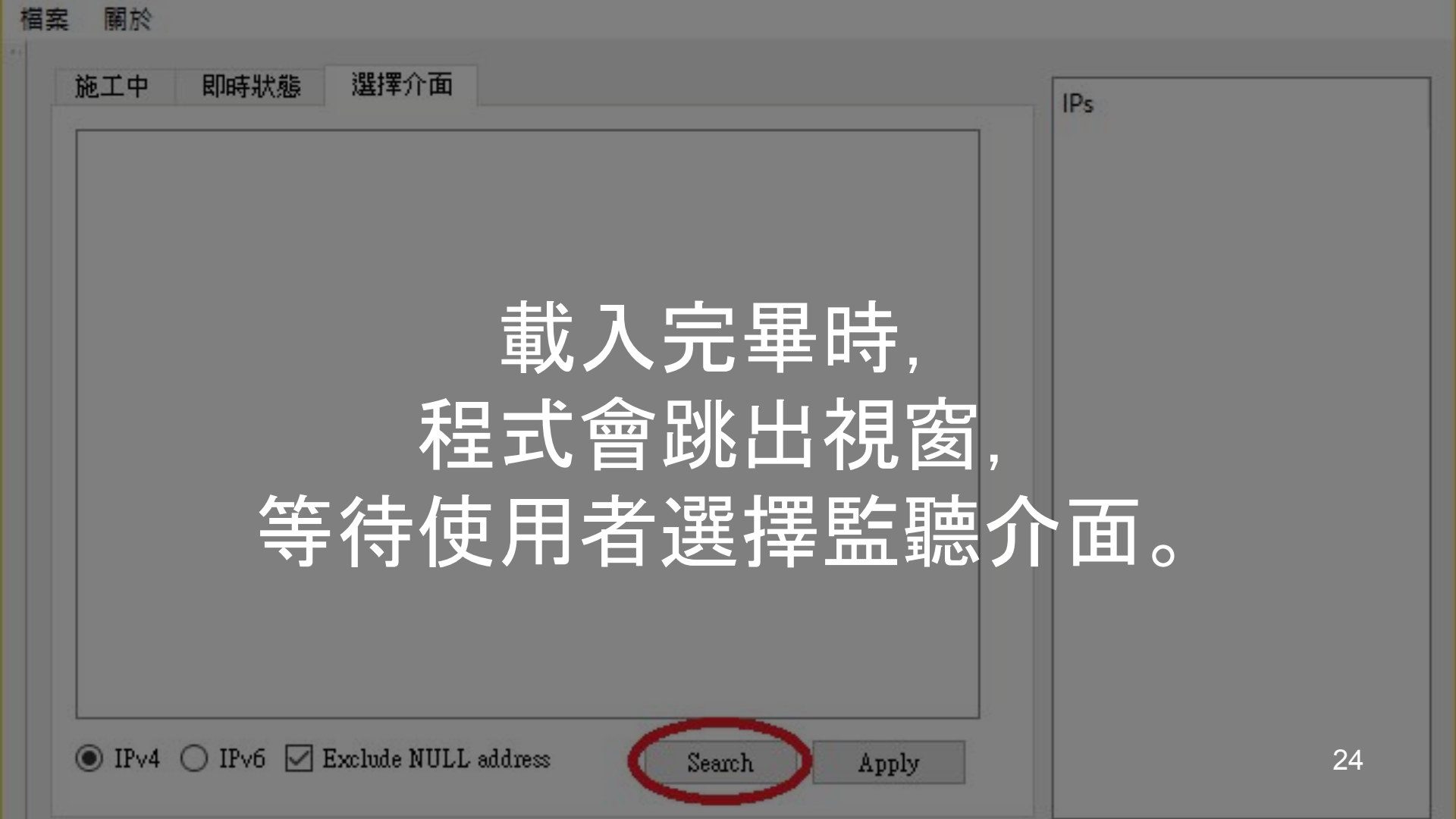
報告到此結束　謝謝大家

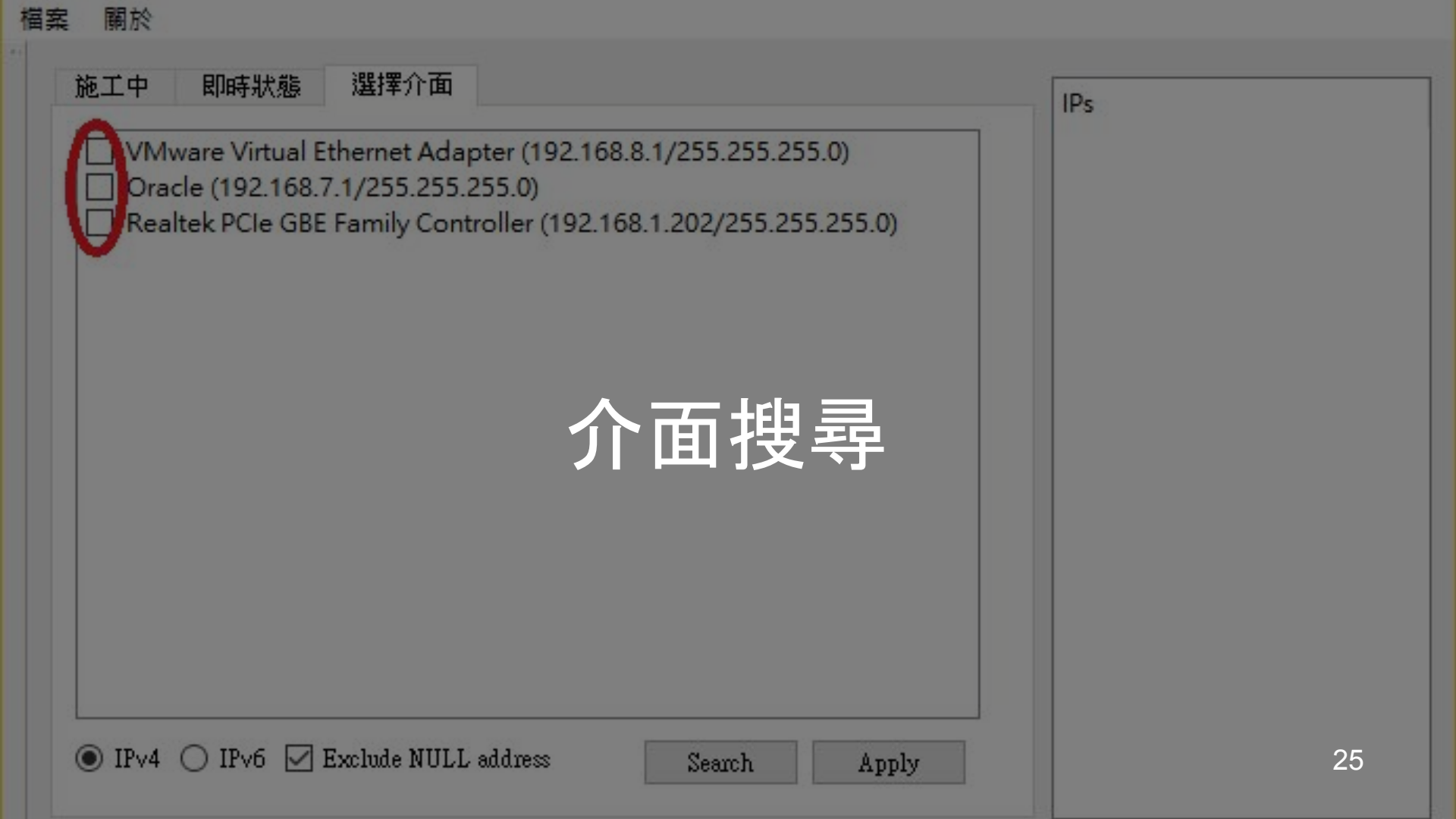
附錄

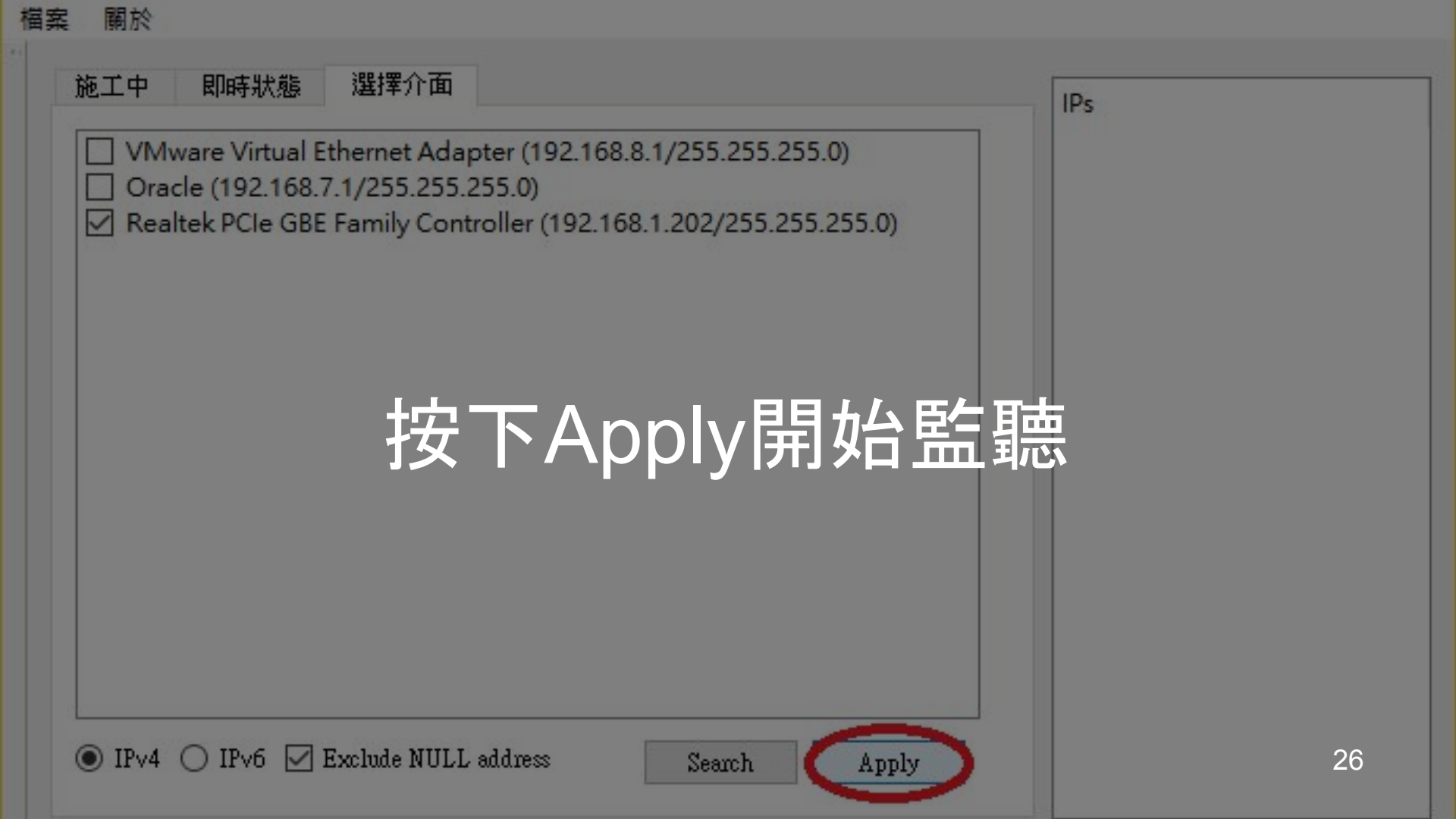
程式操作

IP網段　　服務名稱 底色(RGB) 文字顏色(RGB)

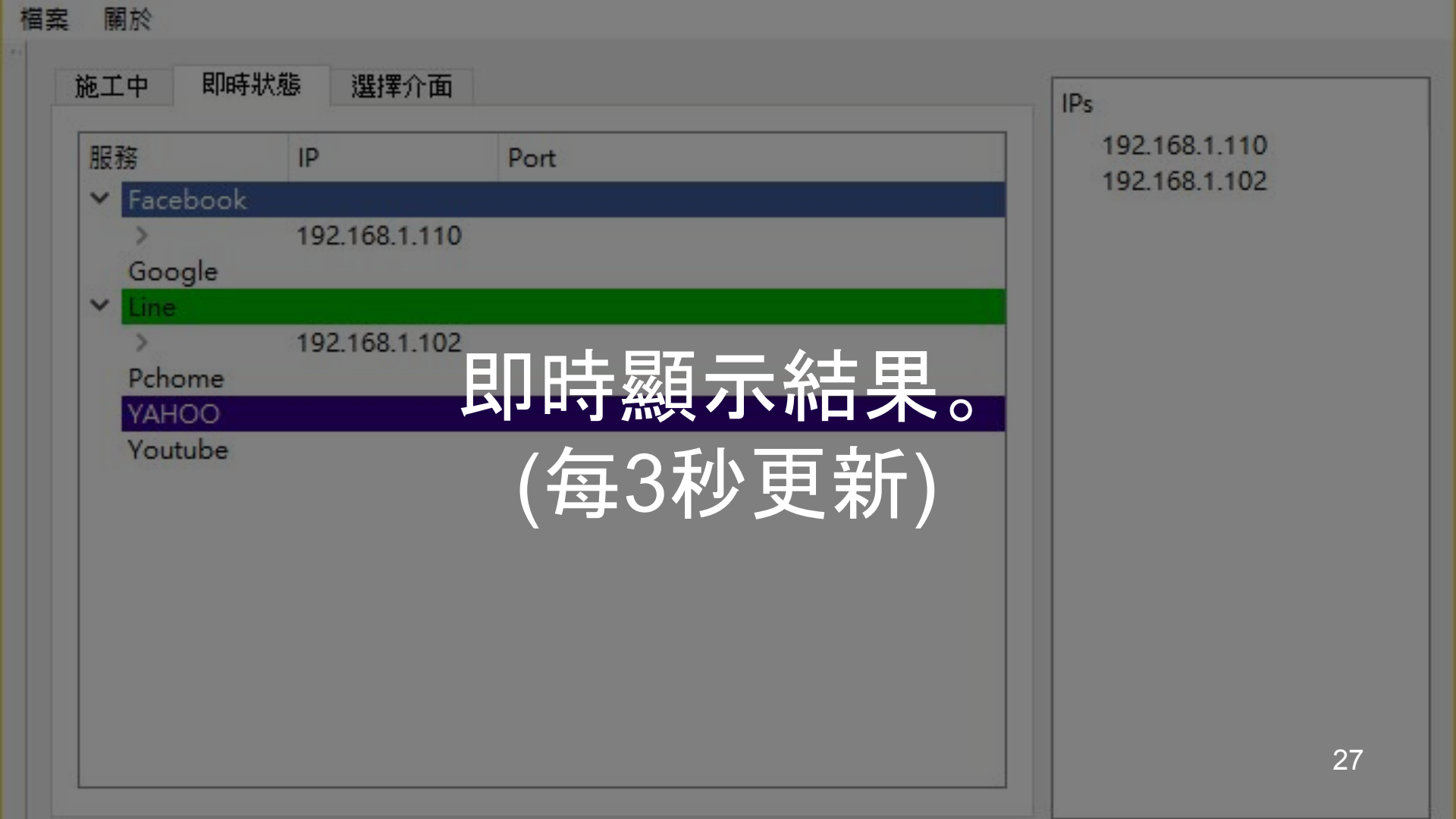
程式剛執行時，會讀取相同目錄底下的config.ini檔案。
這個檔案告訴程式要怎麼辨識服務的流量。


檔案
關於
施工中
即時狀態
選擇介面
IPs
載入完畢時,
程式會跳出視窗,
等待使用者選擇監聽介面。
IPv4
IPv6
Exclude NULL address
Search
Apply

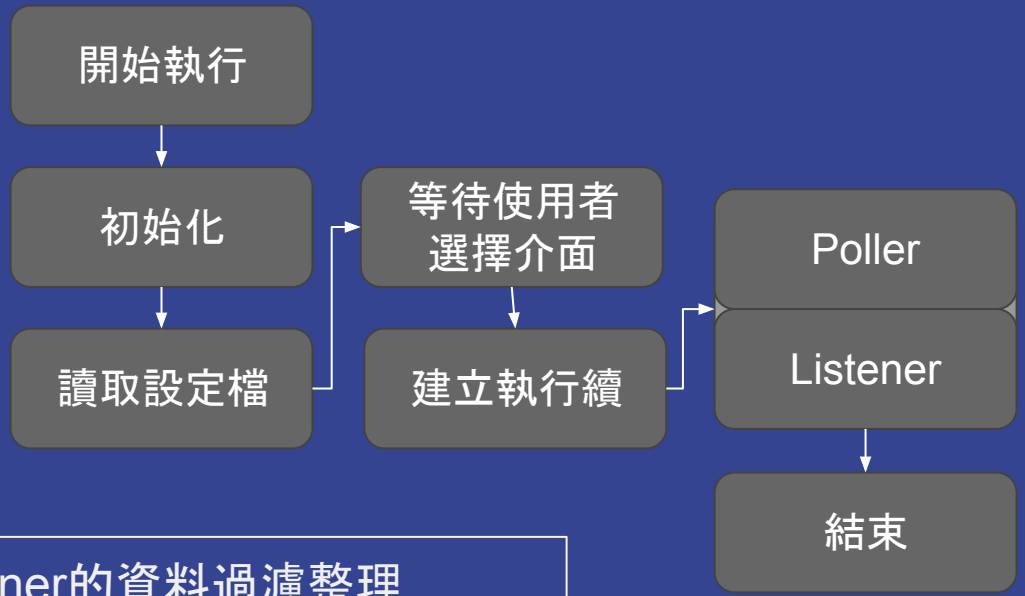

檔案
關於
施工中
即時狀態
選擇介面
VMware Virtual Ethernet Adapter (192.168.8.1/255.255.255.0)
Oracle (192.168.7.1/255.255.255.0)
Realtek PCIe GBE Family Controller (192.168.1.202/255.255.255.0)
IPs
介面搜尋
IPv4
IPv6
Exclude NULL address
Search
Apply



按下Apply開始監聽


檔案
關於
施工中
即時狀態
選擇介面
服務
IP
Port
Facebook
192.168.1.110
Google
Line
192.168.1.102
Pchome
YAHOO
Youtube
即時顯示結果。
(每3秒更新)
IPs
192.168.1.110
192.168.1.102

程式架構



Poller每隔固定時間會將所有Listener的資料過濾整理
並把結果顯示在UI上。

Listener專門在某一個固定的介面上呼叫Blocking Calls,
監聽封包。

程式原理

服務判斷根據:

1. 第3層通訊協定(IP)
2. 來源位置網段
3. 第4層通訊協定(TCP)
4. 來源埠號