105學年(上)期中報告

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

- 目前概況
  - 預計成果
  - 本學期研究目標
  - 工作職位
  - 工作占比
  - 工作分配
  - 研究進度表
- 參考資料
- 附錄
  1. 有線抓包實作
  2. 無線抓包實作
  3. 釣魚抓包介紹

預計成果

- 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)

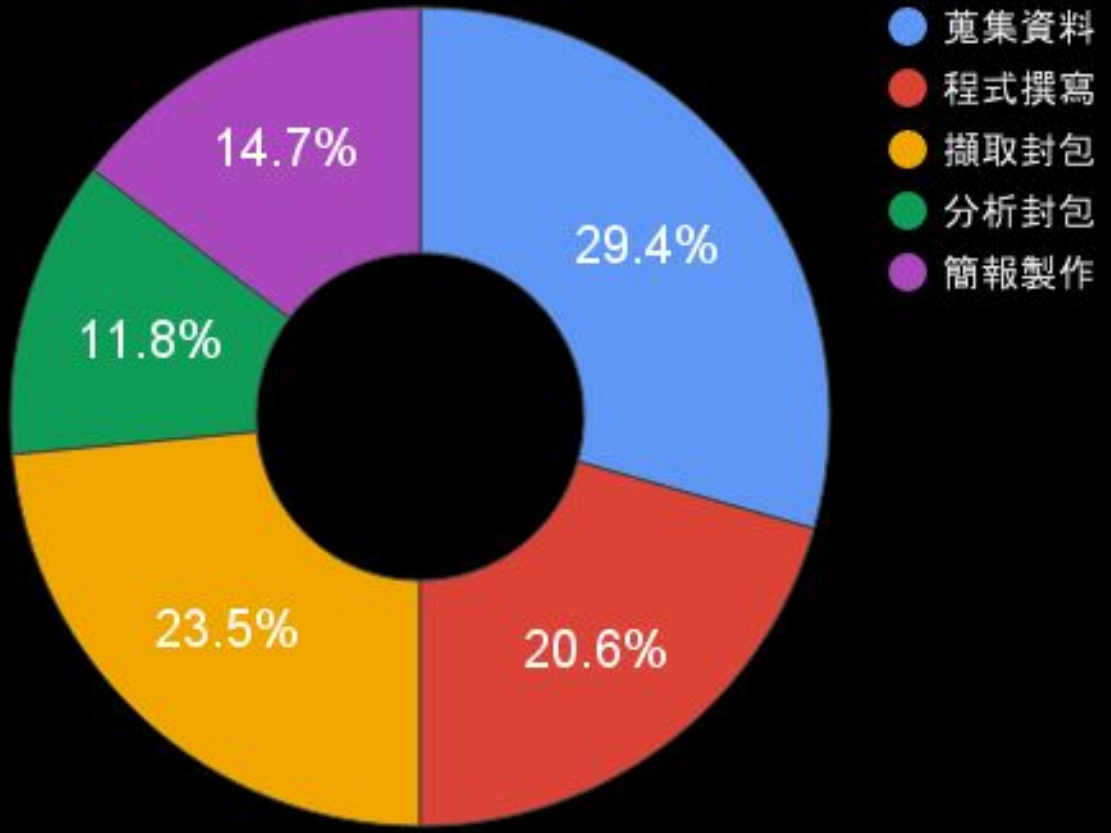
本學期研究目標

- ★ 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
  (ex:瀏覽器,遊戲,服務等)

工作職位

黃政哲	分析功能,程式編寫,軟體整合,無線攔截
陳俊瑋	分析介面,程式設計,有線抓包
蕭　徹	介面設計,簡報美工,文書處理
郭　瀟	報告講者,無線釣魚,收集資料
林坤皇	文字圖形化,宿網攔截,資料蒐集

工作時間占比

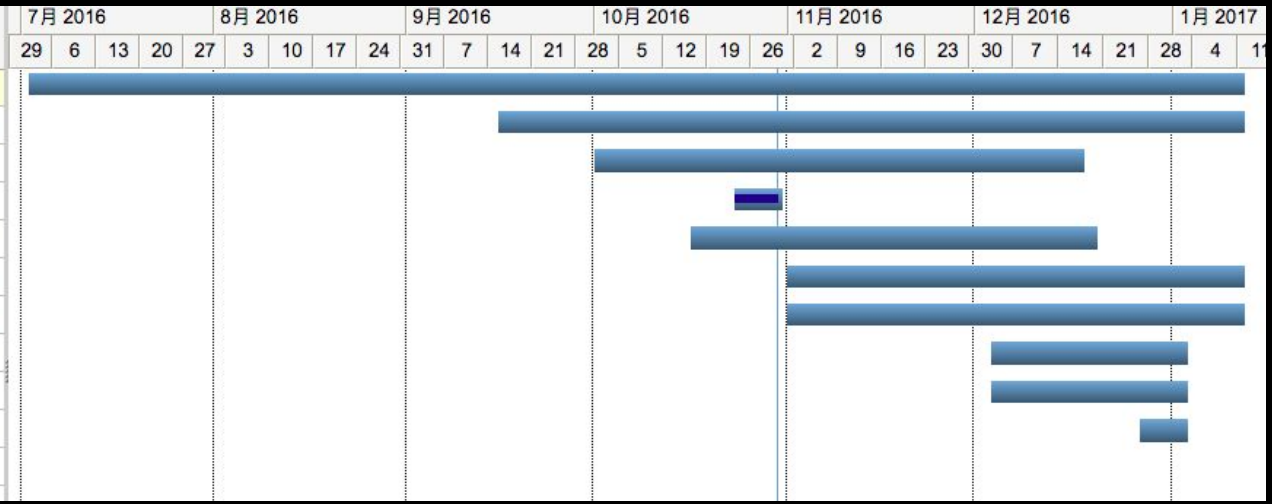


工作分配

(少)1 ~ 5(多)	黃政哲	陳俊瑋	蕭　徹	郭　瀟	林坤皇
蒐集資料研究	5	3	2	2	1
程式撰寫	4	5	2	2	1
擷取封包	4	4	3	2	2
分析封包	5	1	1	1	1
簡報	2	4	5	3	2

研究進度表

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

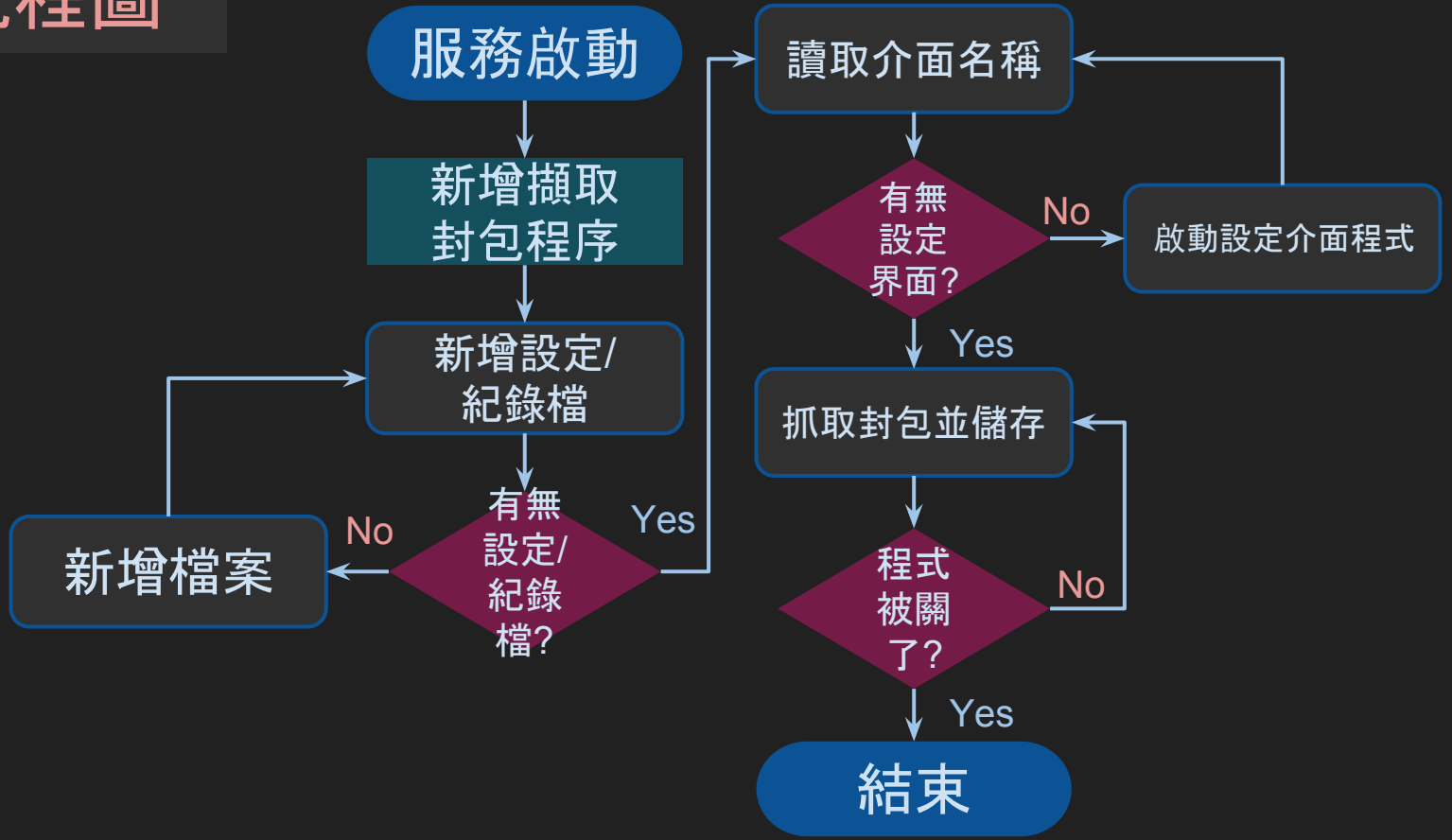


參考資料

- http://pubs.opengroup.org/onlinepubs/7908799/xsh/systime.h.html
- https://www.wireshark.org
- https://www.winpcap.org
- http://www.tcpdump.org
- http://baike.baidu.com
- http://www.pngmart.com/image/26446

附錄1:有線抓包實作

流程圖


服務啟動
新增擷取
封包程序
新增設定/
紀錄檔
有無
設定/
紀錄
檔?
No
新增檔案
Yes
讀取介面名稱
有無
設定
界面?
No
啟動設定介面程式
Yes
抓取封包並儲存
程式
被關
了?
No
Yes
結束

軟體環境

程式名稱: Automatic Packet Miner(APM)

程式語言: C \ C++

程式環境: Windows

IDE ：Dev C++ \ Visual Studio

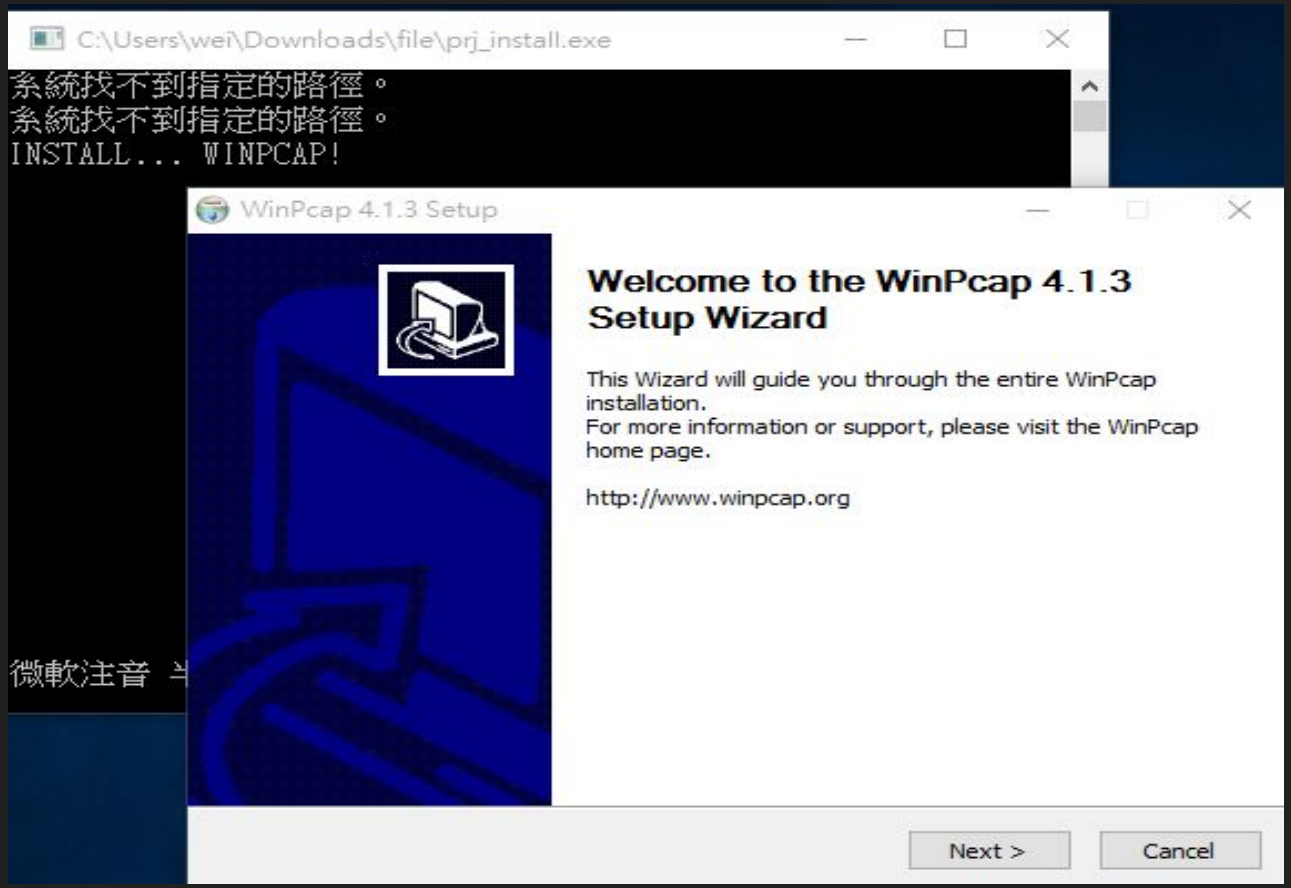
必裝程式: Winpcap

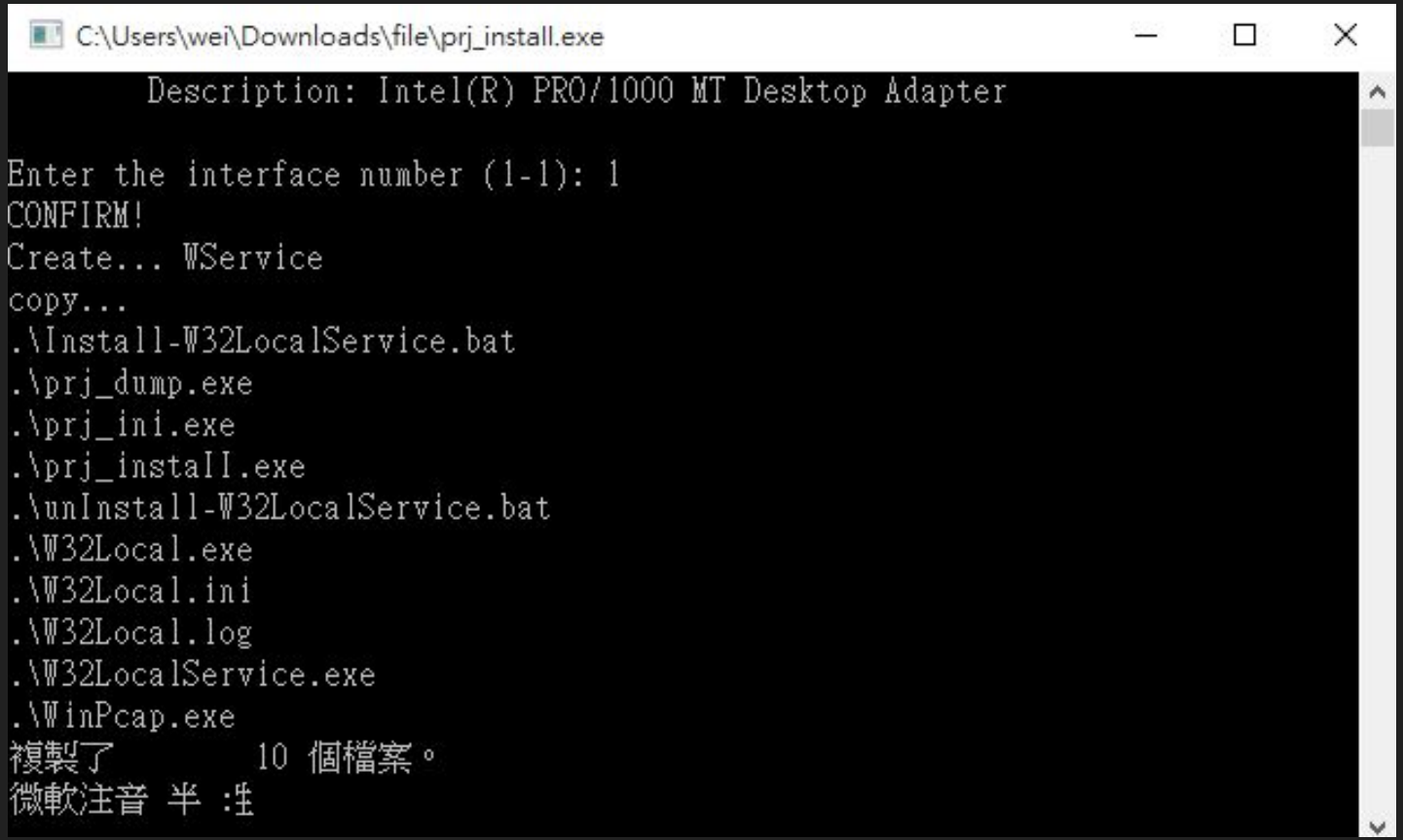
程式功能介紹

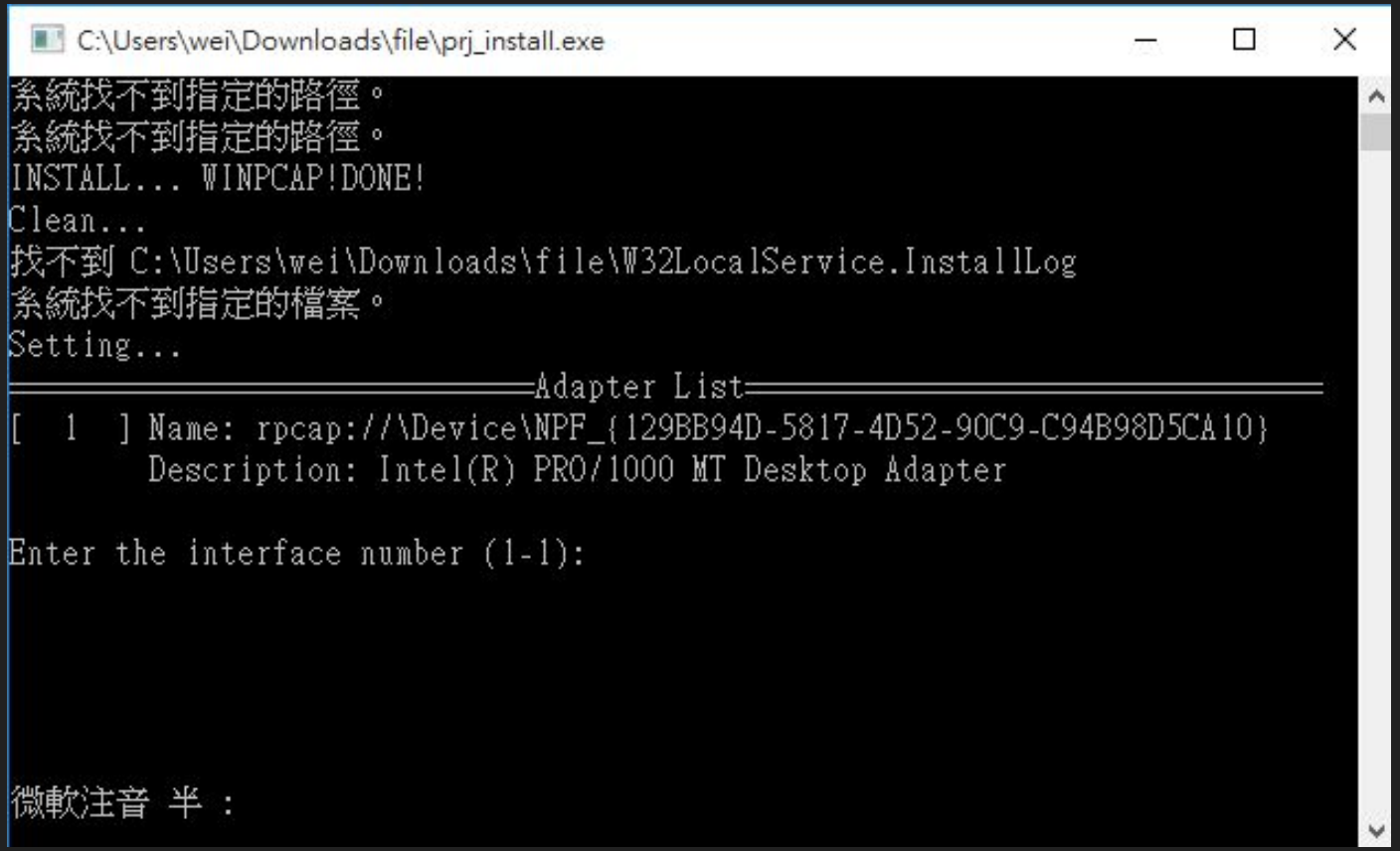
(目標功能)

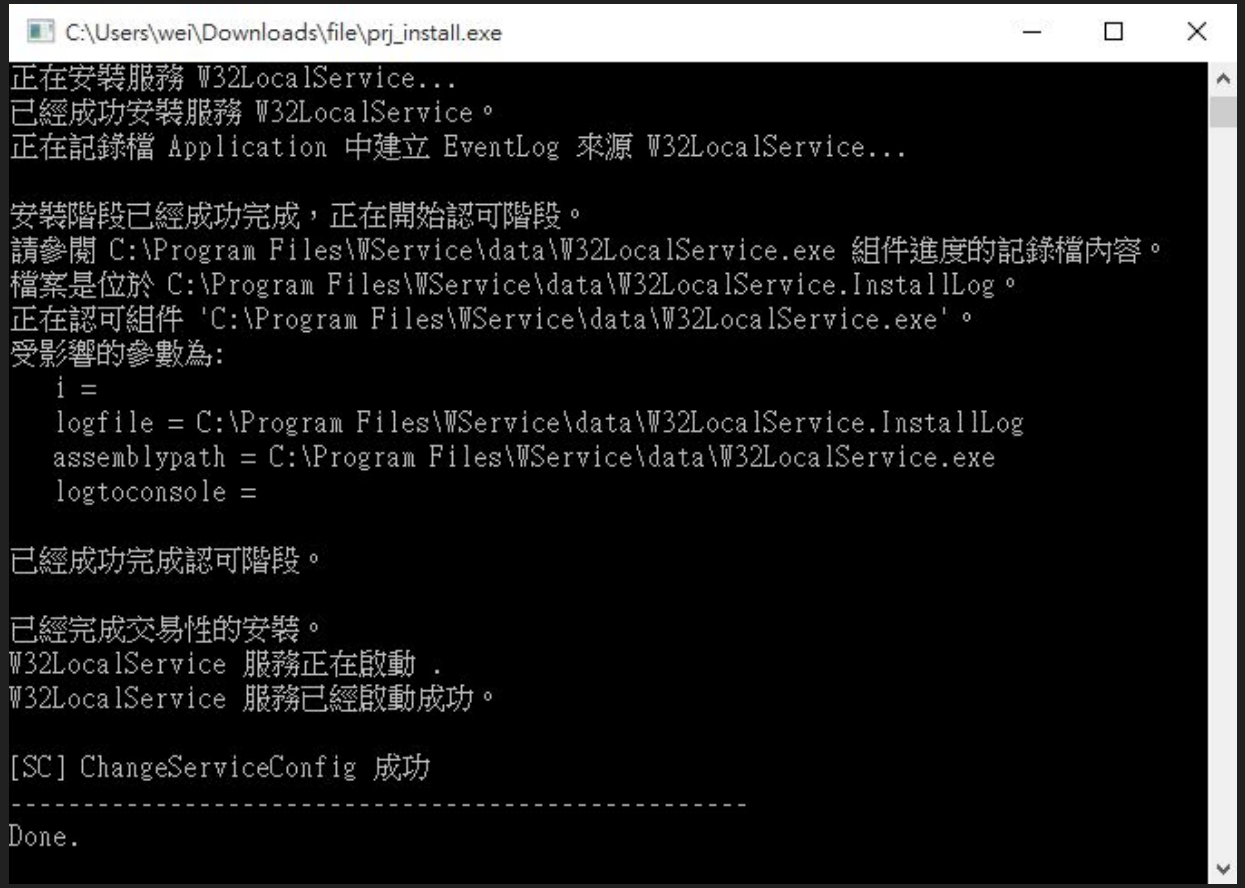
被安裝的電腦每次開機都會抓指定介面卡的資料，並儲存。

安裝過程

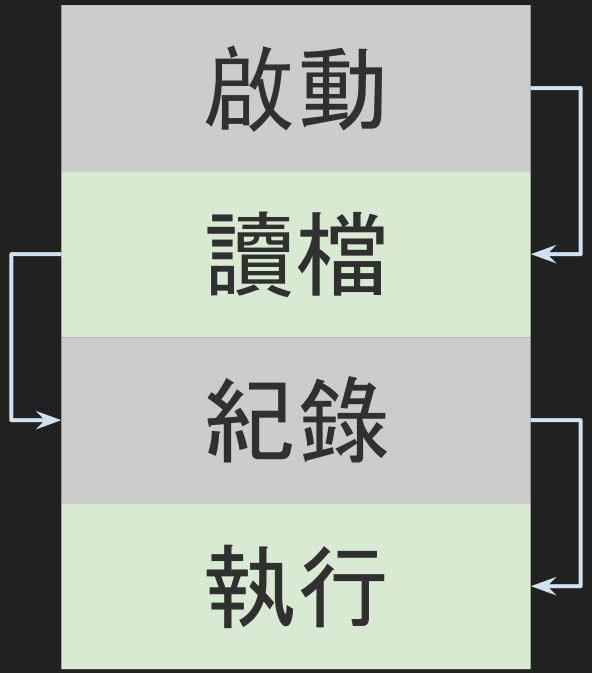

C:\Users\wei\Downloads\file\prj_install.exe
系統找不到指定的路徑。
系統找不到指定的路徑。
INSTALL... WINPCAP!
微軟注音
WinPcap 4.1.3 Setup
Welcome to the WinPcap 4.1.3 Setup Wizard
This Wizard will guide you through the entire WinPcap installation.
For more information or support, please visit the WinPcap home page.
http://www.winpcap.org
Next >
Cancel

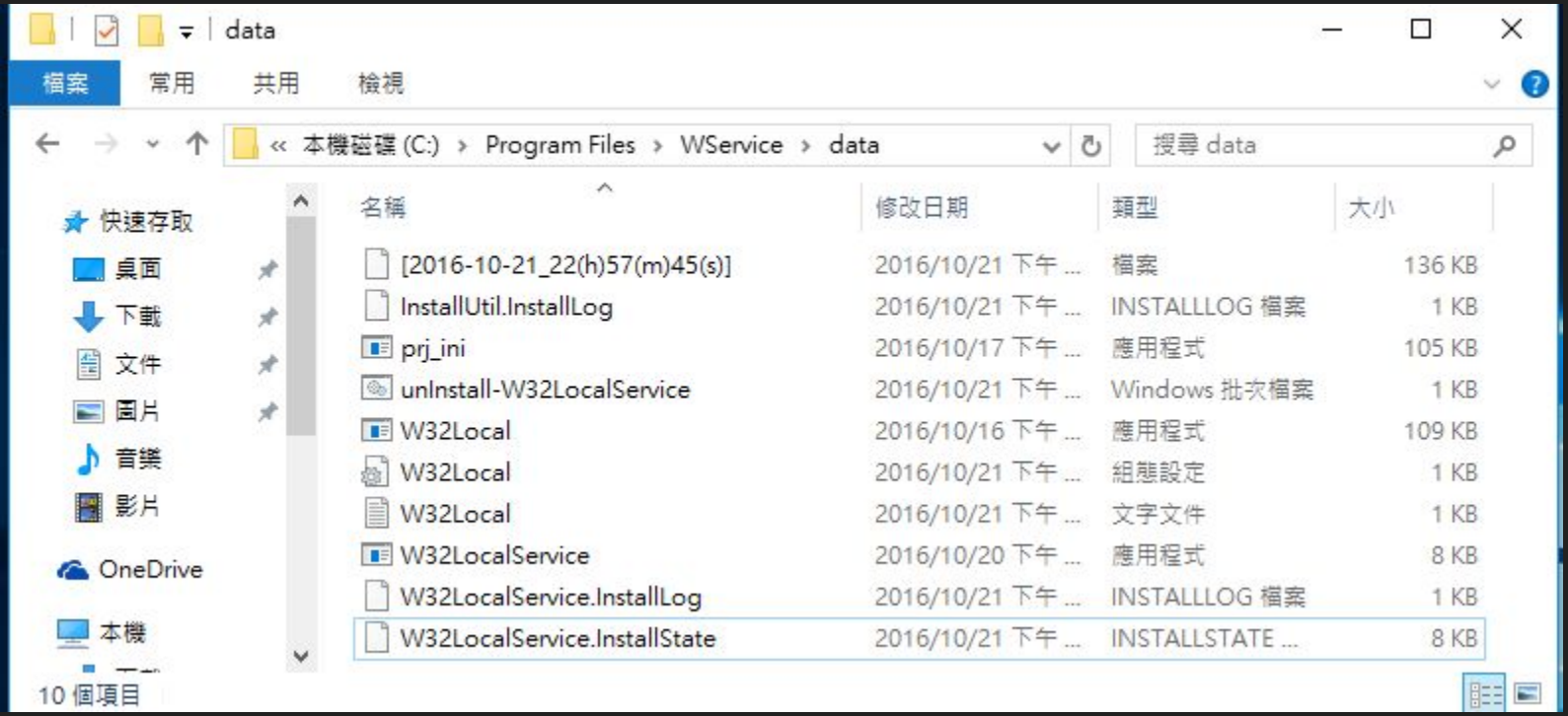

C:\Users\wei\Downloads\file\prj_install.exe
Description: Intel(R) PRO/1000 MT Desktop Adapter
Enter the interface number (1-1): 1
CONFIRM!
Create... WService
copy...
.\Install-W32LocalService.bat
.\prj_dump.exe
.\prj_ini.exe
.\prj_instaII.exe
.\unInstall-W32LocalService.bat
.\W32Local.exe
.\W32Local.ini
.\W32Local.log
.\W32LocalService.exe
.\WinPcap.exe
複製了 10 個檔案。
微軟注音 半 :生

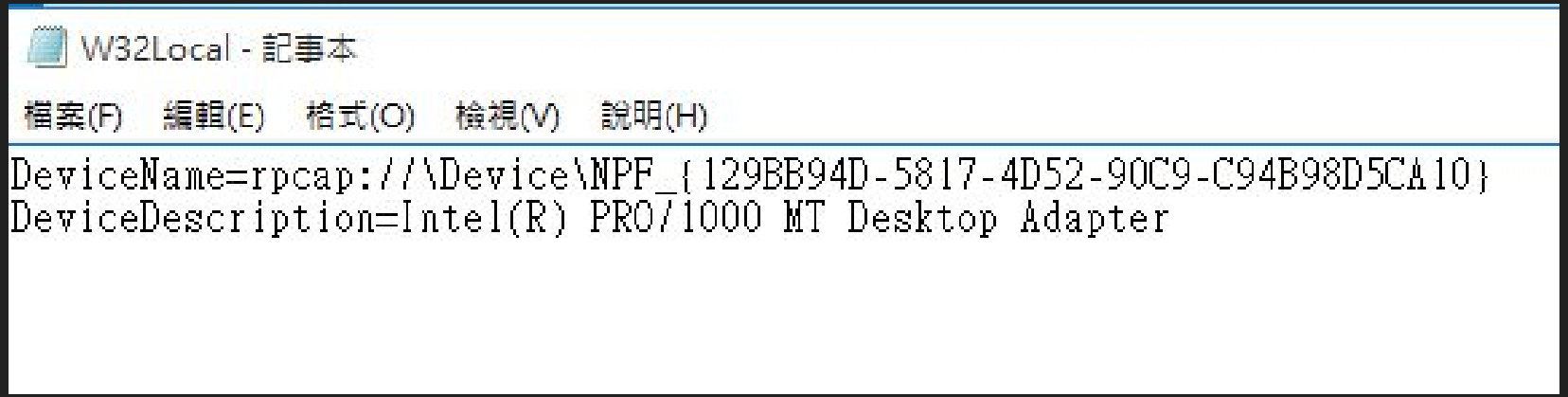

C:\Users\wei\Downloads\file\prj_install.exe
系統找不到指定的路徑。
系統找不到指定的路徑。
INSTALL... WINPCAP!DONE!
Clean...
找不到 C:\Users\wei\Downloads\file\W32LocalService.InstallLog
系統找不到指定的檔案。
Setting...
Adapter List
[1] Name: rpcap://\Device\NPF_{129BB94D-5817-4D52-90C9-C94B98D5CA10}
Description: Intel(R) PRO/1000 MT Desktop Adapter
Enter the interface number (1-1):
微軟注音 半 :

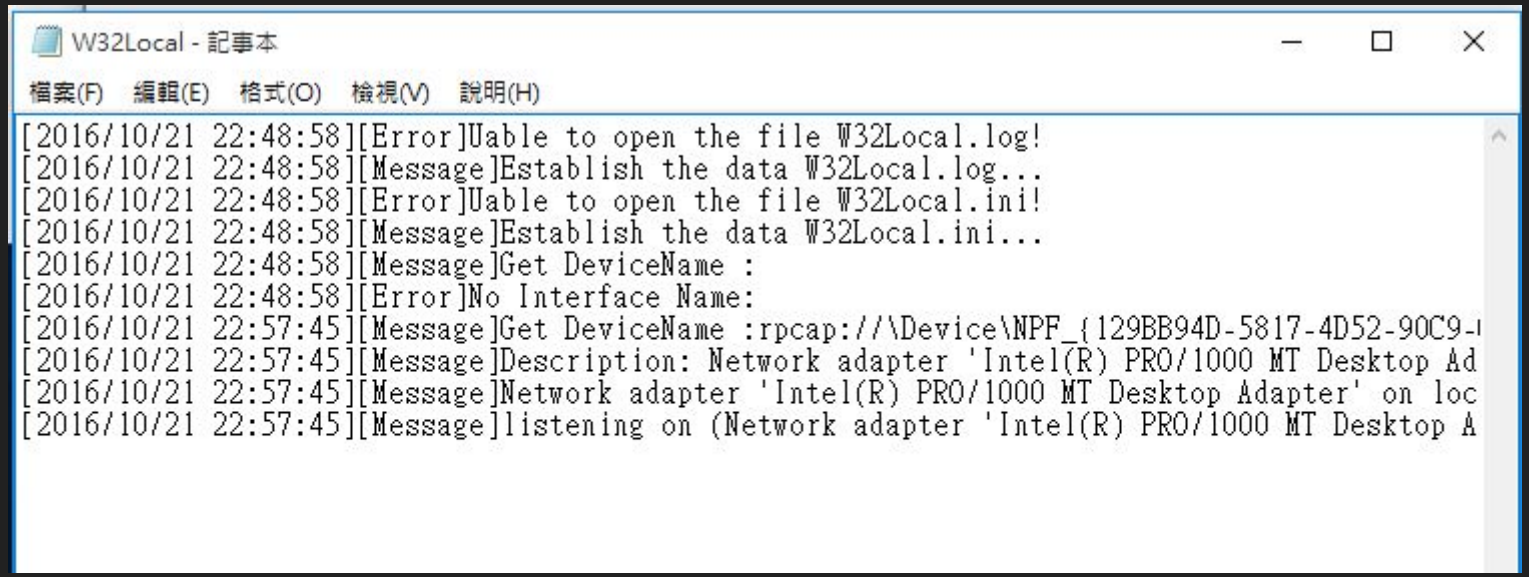

C:\Users\wei\Downloads\file\prj_install.exe
正在安裝服務 W32LocalService...
已經成功安裝服務 W32LocalService。
正在記錄檔 Application 中建立 EventLog 來源 W32LocalService...
安裝階段已經成功完成，正在開始認可階段。
請參閱 C:\Program Files\WService\data\W32LocalService.exe 組件進度的記錄檔內容。
檔案是位於 C:\Program Files\WService\data\W32LocalService.InstallLog。
正在認可組件 'C:\Program Files\WService\data\W32LocalService.exe'。
受影響的參數為:
i =
logfile = C:\Program Files\WService\data\W32LocalService.InstallLog
assemblypath = C:\Program Files\WService\data\W32LocalService.exe
logtoconsole =
已經成功完成認可階段。
已經完成交易性的安裝。
W32LocalService 服務正在啟動 .
W32LocalService 服務已經啟動成功。
[SC] ChangeServiceConfig 成功
Done.

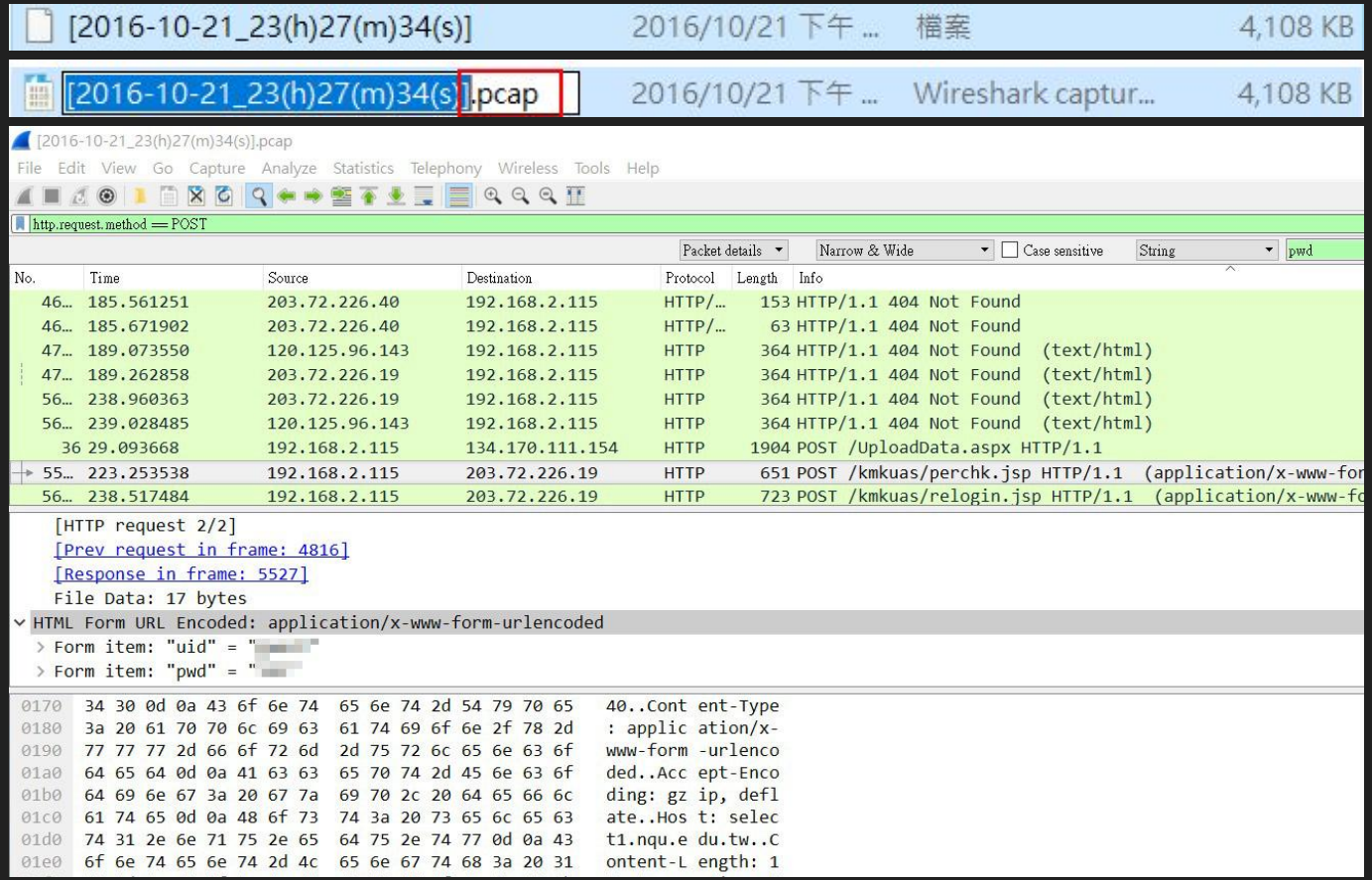
執行過程




data
檔案
常用
共用
檢視
« 本機磁碟 (C:) › Program Files › WService › data
搜尋 data
快速存取
桌面
下載
文件
圖片
音樂
影片
OneDrive
本機
名稱
修改日期
類型
大小
[2016-10-21_22(h)57(m)45(s)] 2016/10/21 下午 ... 檔案 136 KB
InstallUtil.InstallLog 2016/10/21 下午 ... INSTALLLOG 檔案 1 KB
prj_ini 2016/10/17 下午 ... 應用程式 105 KB
unInstall-W32LocalService 2016/10/21 下午 ... Windows 批次檔案 1 KB
W32Local 2016/10/16 下午 ... 應用程式 109 KB
W32Local 2016/10/21 下午 ... 組態設定 1 KB
W32Local 2016/10/21 下午 ... 文字文件 1 KB
W32LocalService 2016/10/20 下午 ... 應用程式 8 KB
W32LocalService.InstallLog 2016/10/21 下午 ... INSTALLLOG 檔案 1 KB
W32LocalService.InstallState 2016/10/21 下午 ... INSTALLSTATE ... 8 KB
10 個項目

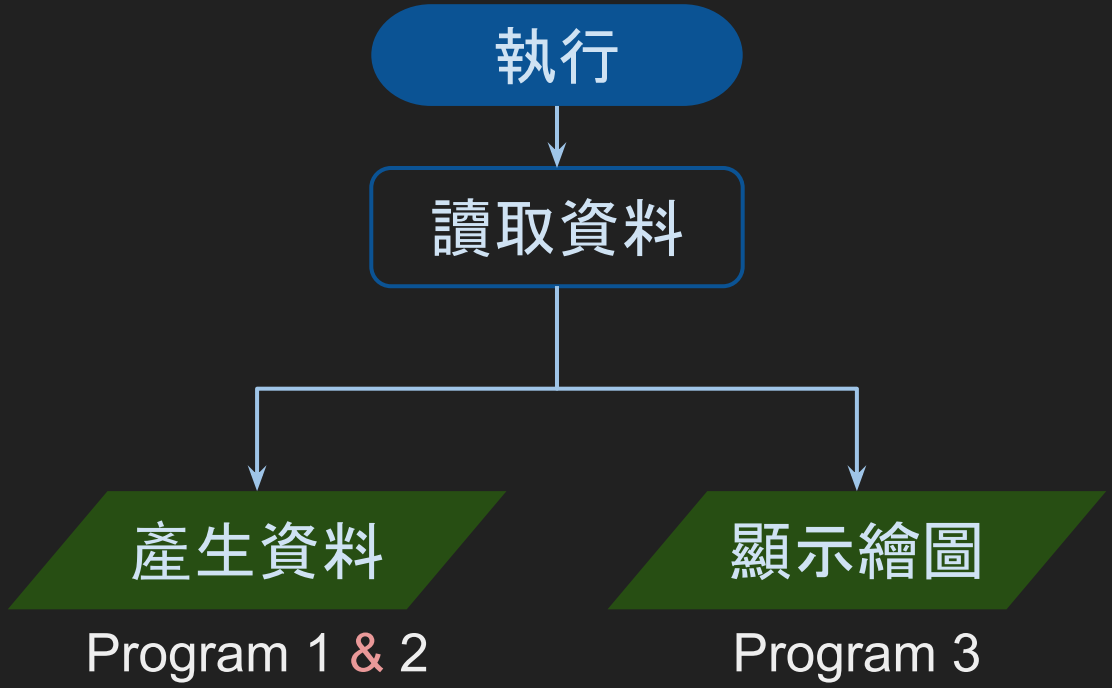

W32Local - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
DeviceName=rpcap://\Device\NPF_{129BB94D-5817-4D52-90C9-C94B98D5CA10}
DeviceDescription=Intel(R) PRO/1000 MT Desktop Adapter


W32Local - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
[2016/10/21 22:48:58][Error]Uable to open the file W32Local.log!
[2016/10/21 22:48:58][Message]Establish the data W32Local.log...
[2016/10/21 22:48:58][Error]Uable to open the file W32Local.ini!
[2016/10/21 22:48:58][Message]Establish the data W32Local.ini...
[2016/10/21 22:48:58][Message]Get DeviceName :
[2016/10/21 22:48:58][Error]No Interface Name:
[2016/10/21 22:57:45][Message]Get DeviceName :rpcap://\Device\NPF_{129BB94D-5817-4D52-90C9-
[2016/10/21 22:57:45][Message]Description: Network adapter 'Intel(R) PRO/1000 MT Desktop Ad
[2016/10/21 22:57:45][Message]Network adapter 'Intel(R) PRO/1000 MT Desktop Adapter' on loc
[2016/10/21 22:57:45][Message]listening on (Network adapter 'Intel(R) PRO/1000 MT Desktop A


[2016-10-21_23(h)27(m)34(s)] 2016/10/21 下午 ... 檔案 4,108 KB
[2016-10-21_23(h)27(m)34(s)].pcap 2016/10/21 下午 ... Wireshark captur... 4,108 KB
[2016-10-21_23(h)27(m)34(s)].pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request.method == POST
Packet details Narrow & Wide Case sensitive String pwd
No. Time Source Destination Protocol Length Info
46... 185.561251 203.72.226.40 192.168.2.115 HTTP/... 153 HTTP/1.1 404 Not Found
46... 185.671902 203.72.226.40 192.168.2.115 HTTP/... 63 HTTP/1.1 404 Not Found
47... 189.073550 120.125.96.143 192.168.2.115 HTTP 364 HTTP/1.1 404 Not Found (text/html)
47... 189.262858 203.72.226.19 192.168.2.115 HTTP 364 HTTP/1.1 404 Not Found (text/html)
56... 238.960363 203.72.226.19 192.168.2.115 HTTP 364 HTTP/1.1 404 Not Found (text/html)
56... 239.028485 120.125.96.143 192.168.2.115 HTTP 364 HTTP/1.1 404 Not Found (text/html)
36 29.093668 192.168.2.115 134.170.111.154 HTTP 1904 POST /UploadData.aspx HTTP/1.1
55... 223.253538 192.168.2.115 203.72.226.19 HTTP 651 POST /kmkuas/perchk.jsp HTTP/1.1 (application/x-www-for
56... 238.517484 192.168.2.115 203.72.226.19 HTTP 723 POST /kmkuas/relogin.jsp HTTP/1.1 (application/x-www-fo
[HTTP request 2/2]
[Prev request in frame: 4816]
[Response in frame: 5527]
File Data: 17 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "uid" = "
Form item: "pwd" = "
0170 34 30 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 40..Cont ent-Type
0180 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 2d : applic ation/x-
0190 77 77 77 2d 66 6f 72 6d 2d 75 72 6c 65 6e 63 6f www-form -urlenco
01a0 64 65 64 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f ded..Acc ept-Enco
01b0 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c ding: gz ip, defl
01c0 61 74 65 0d 0a 48 6f 73 74 3a 20 73 65 6c 65 63 ate..Hos t: selec
01d0 74 31 2e 6e 71 75 2e 65 64 75 2e 74 77 0d 0a 43 t1.nqu.e du.tw..C
01e0 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 31 ontent-L ength: 1

附錄2:無線抓包實作

流程圖



封包攔截工具

無線介面卡: Broadcom Wireless 43142 (2.4GHz Only, 筆記型電腦內建)

作業系統: Ubuntu Desktop (x64)

驅動程式: 6.30.223.271 - BRCM Linux Hybrid Wireless Driver

使用軟體: Wireshark

攔截時間

- 每週課堂上課
- 就寢到起床

攔截地點

圖資大樓
I102教室

學生一宿

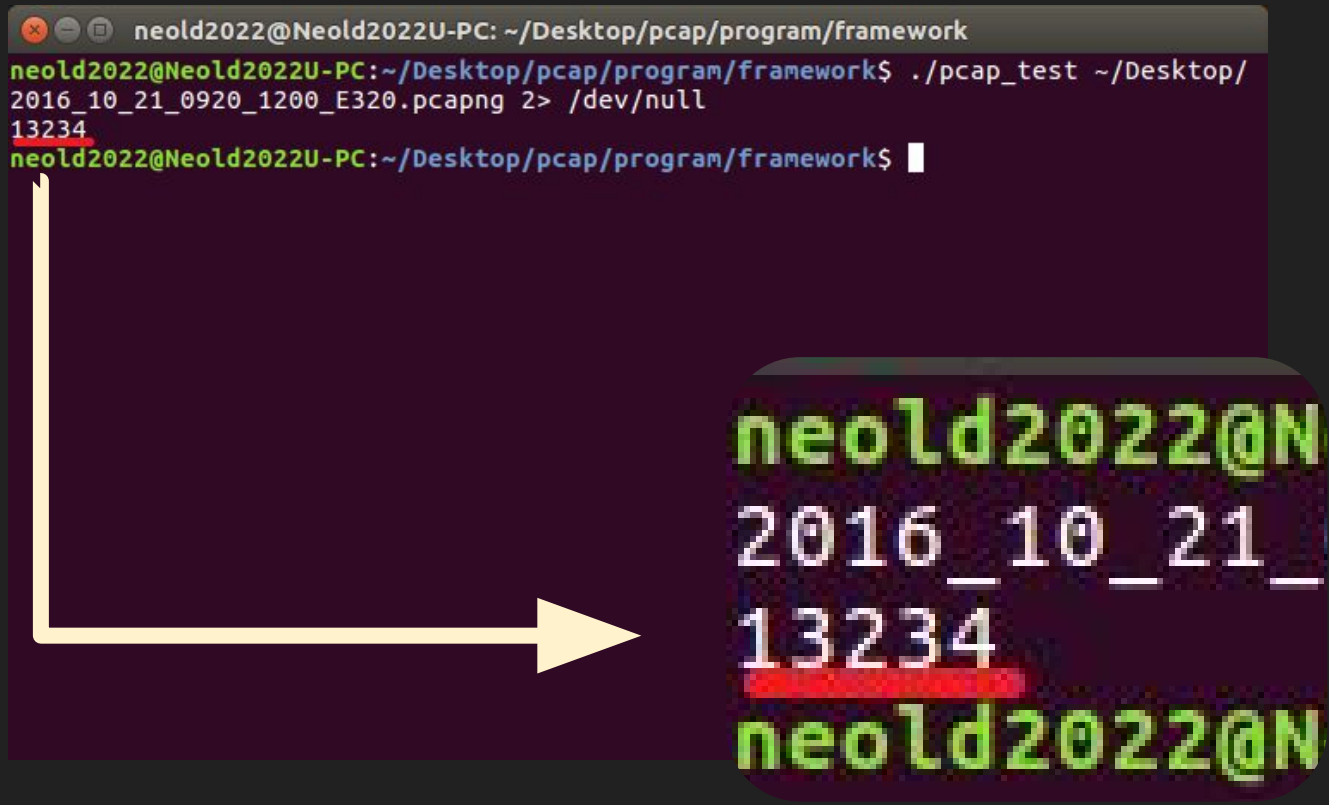
理工大樓
E320教室
E321教室
E322教室

綜合大樓
企管系 R328教室
觀光系 R232教室 (僅攔截兩次)
綜合一樓 R123教室 (僅攔截一次)

截至10/21號為止，已蒐集大約**21.4GB**的封包資料

初步封包分析程式

nConnections	計算在一批已經被攔截的封包中，TCP連線的數量
wlMediumUtilization	計算無線介質(空氣)的使用狀況
wlMU-Visualizer	將上一個工具的輸出視覺化



- nConnections

計算原理

利用一組 *來源<IP, Port>* 與 *目的<IP, Port>* 來表示出一條連線

(來源目的對調不影響)

例:

192.168.1.2:54321	===>	31.13.87.36:443	(facebook.com)
31.13.87.36:443	===>	192.168.1.2:54321	
192.168.1.4:49612	===>	192.30.253.113:22	(github.com)
192.30.253.113:22	===>	192.168.1.4:49612	

- nConnections

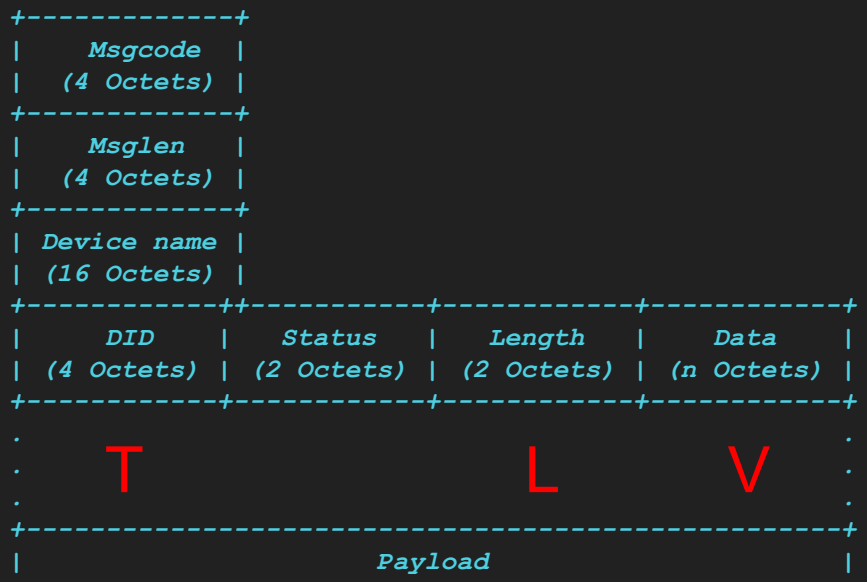
訊框開始傳輸的時間點

0.132199072	0.132399072
0.134413464	0.134661464
0.204627113	0.204844113
0.229243221	0.229449221
0.234647782	0.234847782
0.236902538	0.237150538
1.692518333	1.692735333
1.667952715	1.668158715
1.662551036	1.662751036
1.660191128	1.660439128
1.590123764	1.590340764
1.560142582	1.560342582
1.557802665	1.558050665
1.497544409	1.497572409
1.487721049	1.487938049
1.457746541	1.457946541
1.455379197	1.455627197
1.385316655	1.385533655
1.355342983	1.355542983
1.352997490	1.353245490
1.325371550	1.325615550
1.295862180	1.296051180
1.252972476	1.253172476
1.250613551	1.250861551

訊框結束傳輸的時間點

▲ wlMediumUtilization

PRISM標頭格式



- wlMediumUtilization

取得傳輸速率

訊框長度

DID代表欄位:

0x0000A041

0x000A0044

傳輸速度

DID代表欄位:

0x00008041

0x00080044

- wlMediumUtilization

取得封包到達時間

```
const u_char *pcap_next(pcap_t *p, struct pcap_pkthdr *h);
     //我們使用這個函數來取得封包的內容


//訊框的metadata
struct pcap_pkthdr {
     struct timeval tv;   //完整接收到訊框的時間，也就是訊框剛傳輸完成的那一瞬間
     bpf_u_int32          caplen;
     bpf_u_int32          len;
};

struct timeval {
     time_t               tv_sec     //接收到訊框時的秒數
     suseconds_t          tv_usec    //奈秒
};
```

- wlMediumUtilization

計算方式

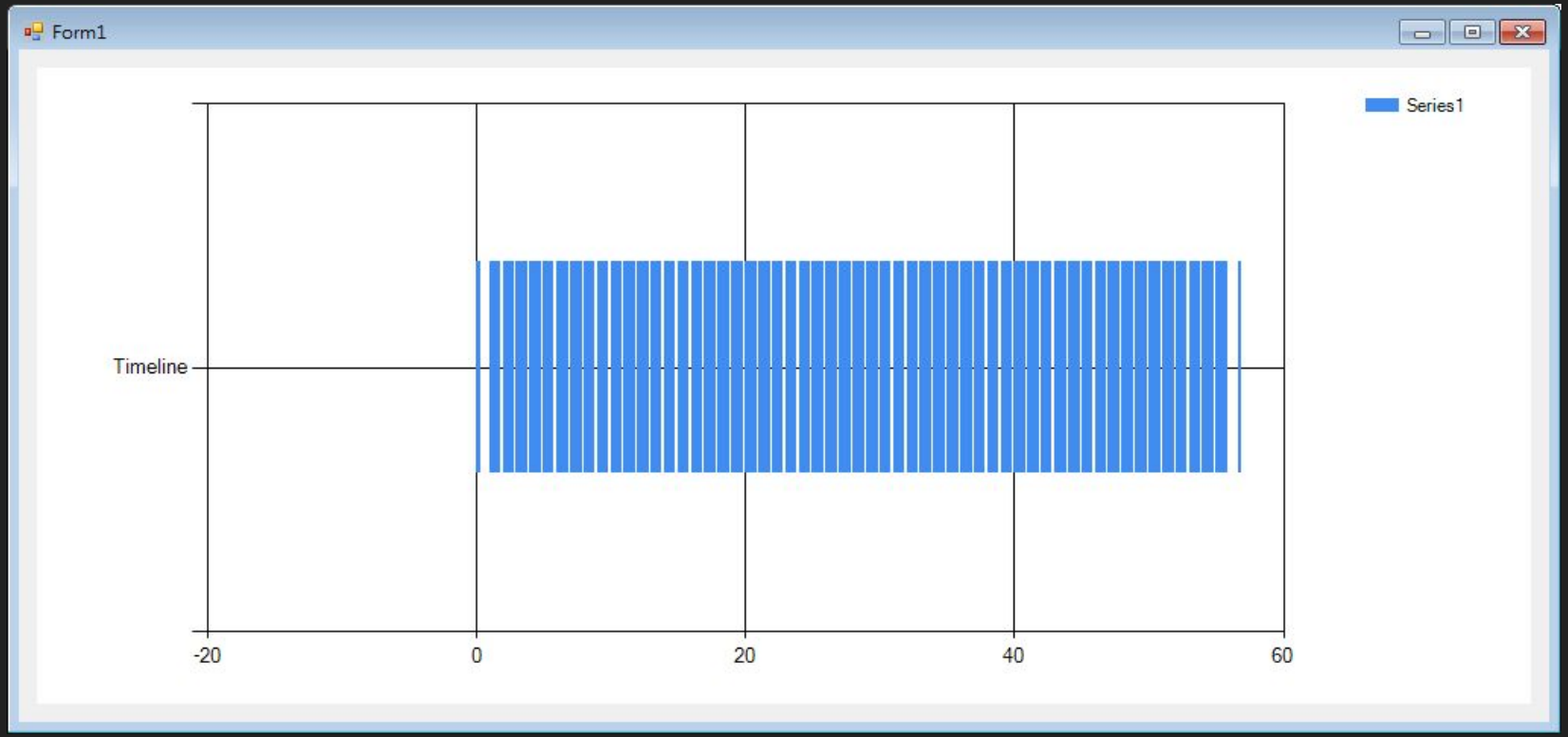
訊框剛開始被傳輸的時間點

= 訊框到達時間 - (傳輸長度 / 傳輸速率)

訊框剛被結束傳輸的時間點

= 訊框到達時間

▲ wlMediumUtilization



- wIMU-Visualizer

附錄3:釣魚抓包介紹

組成部分

USB內置驅動程序

wifi分享器

優點

Anywhere,

只要有電腦的地方

就可以用Wi-Fi收集數據

理工大樓

宿舍

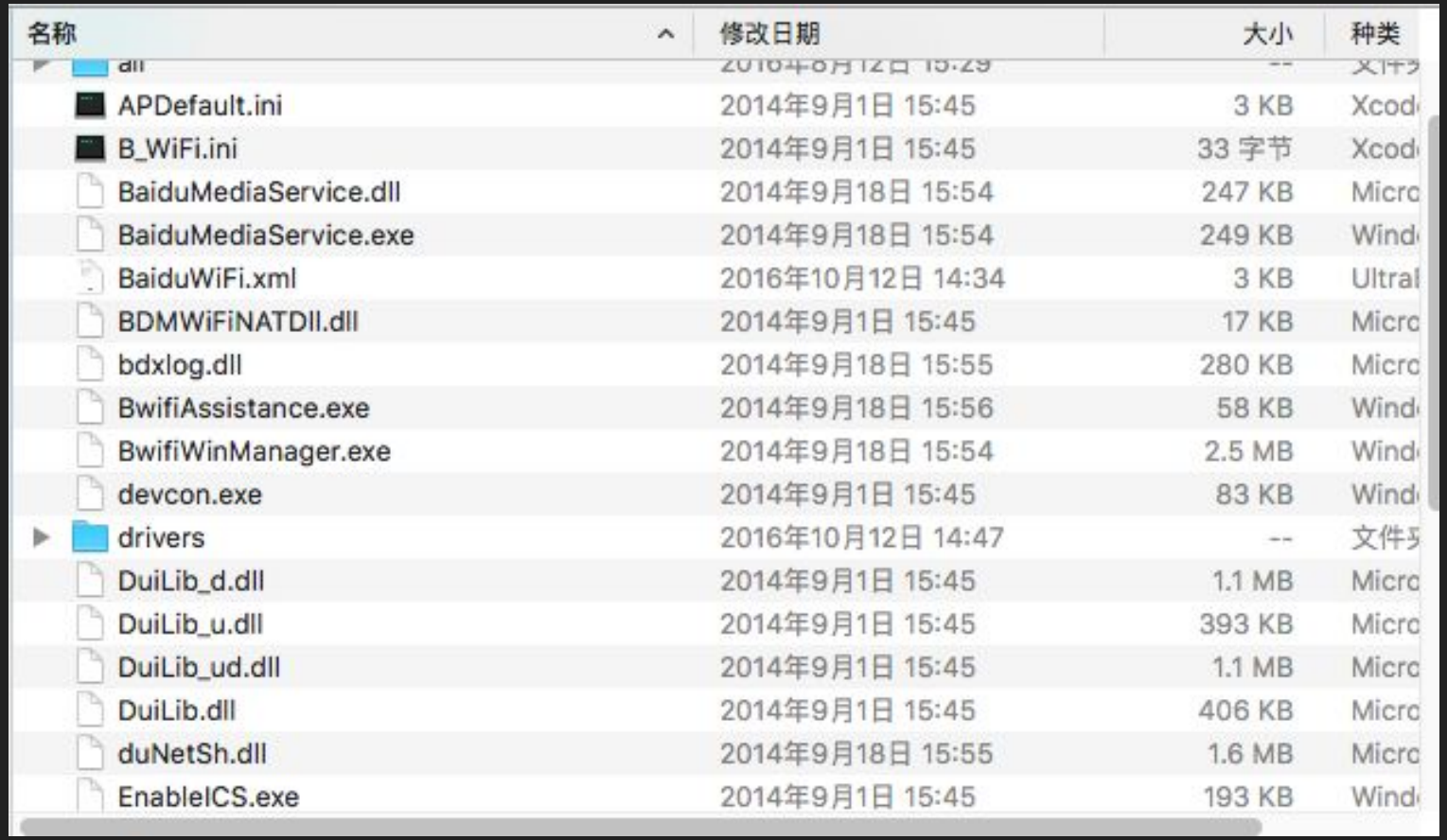
綜合大樓

圖資中心

基本規格

传输速率	11b：1/2/5.5/11Mbps
	11g：6/9/12/18/24/36/48/54Mbps
	11n：最高可达150Mbps
遵循协议标准	IEEE 802.11n；IEEE 802.11g；IEEE 802.11b
发射功率	18 dBm（最大值）
支持加密方式	WPA-PSK/WPA2-PSK
天线	内置PIFA天线
使用环境	工作温度：0℃~40℃
	存储温度：-20℃~70℃
	工作湿度：10% ~ 90% RH 无凝结
	存储湿度：5% ~ 90% RH 无凝结

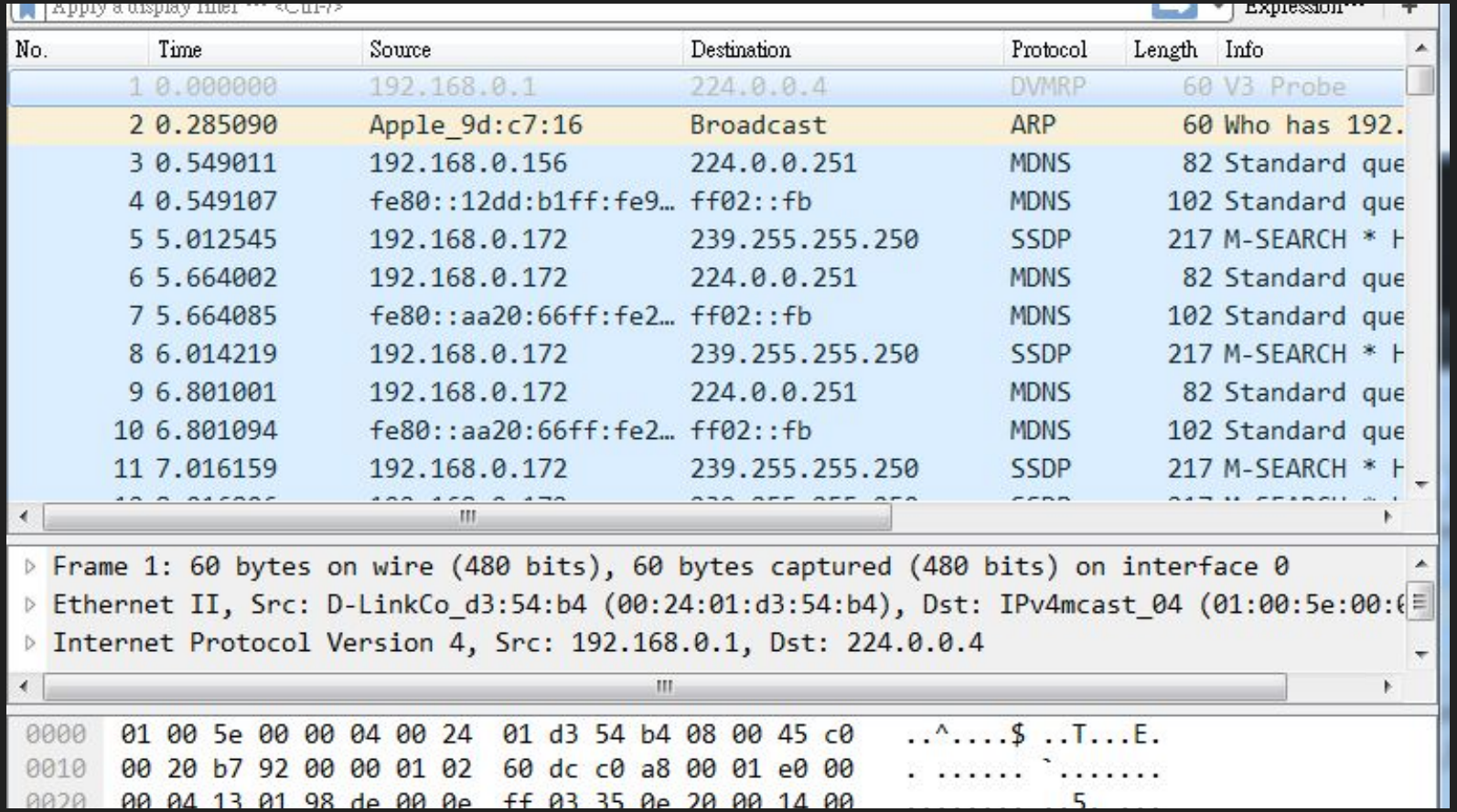
基本特征	USB 2.0接口
	支持20MHz/40MHz频宽
	自动侦测网络及变换传输速率
	1T1R天线模式
	支持2.4G频段
	支持Multiple BSSID
	支持QoS-WMM, WMM-PS
	支持集中控制模式(Infrastructure)和对等模式(Ad-hoc)
	低功耗及电源管理
	支持系统：XP/Vista 32/64, Win7 32/64,Win8 32/64



名称	修改日期	大小	种类
all	2016年8月12日 15:29	--	文件夹
APDefault.ini	2014年9月1日 15:45	3 KB	Xcod
B_WiFi.ini	2014年9月1日 15:45	33 字节	Xcod
BaiduMediaService.dll	2014年9月18日 15:54	247 KB	Micro
BaiduMediaService.exe	2014年9月18日 15:54	249 KB	Wind
BaiduWiFi.xml	2016年10月12日 14:34	3 KB	Ultral
BDMWiFiNATDll.dll	2014年9月1日 15:45	17 KB	Micro
bdxlog.dll	2014年9月18日 15:55	280 KB	Micro
BwifiAssistance.exe	2014年9月18日 15:56	58 KB	Wind
BwifiWinManager.exe	2014年9月18日 15:54	2.5 MB	Wind
devcon.exe	2014年9月1日 15:45	83 KB	Wind
drivers	2016年10月12日 14:47	--	文件夹
DuiLib_d.dll	2014年9月1日 15:45	1.1 MB	Micro
DuiLib_u.dll	2014年9月1日 15:45	393 KB	Micro
DuiLib_ud.dll	2014年9月1日 15:45	1.1 MB	Micro
DuiLib.dll	2014年9月1日 15:45	406 KB	Micro
duNetSh.dll	2014年9月18日 15:55	1.6 MB	Micro
EnableICS.exe	2014年9月1日 15:45	193 KB	Wind


小度WiFi
反馈意见
无线网络创建成功
可以使用手机连接了。
网络名称：Baidu3905
网络密码：12345678
修改
确定
手机怎么连接无线网络？


Welcome to the Wireshark 2.2.1 (32-bit) Setup Wizard
This wizard will guide you through the installation of Wireshark.
Before starting the installation, make sure Wireshark is not running.
Click 'Next' to continue.
Next >
Cancel


Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.0.1 224.0.0.4 DVMRP 60 V3 Probe
2 0.285090 Apple_9d:c7:16 Broadcast ARP 60 Who has 192.
3 0.549011 192.168.0.156 224.0.0.251 MDNS 82 Standard que
4 0.549107 fe80::12dd:b1ff:fe9… ff02::fb MDNS 102 Standard que
5 5.012545 192.168.0.172 239.255.255.250 SSDP 217 M-SEARCH * H
6 5.664002 192.168.0.172 224.0.0.251 MDNS 82 Standard que
7 5.664085 fe80::aa20:66ff:fe2… ff02::fb MDNS 102 Standard que
8 6.014219 192.168.0.172 239.255.255.250 SSDP 217 M-SEARCH * H
9 6.801001 192.168.0.172 224.0.0.251 MDNS 82 Standard que
10 6.801094 fe80::aa20:66ff:fe2… ff02::fb MDNS 102 Standard que
11 7.016159 192.168.0.172 239.255.255.250 SSDP 217 M-SEARCH * H
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: D-LinkCo_d3:54:b4 (00:24:01:d3:54:b4), Dst: IPv4mcast_04 (01:00:5e:00:
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 224.0.0.4
0000 01 00 5e 00 00 04 00 24 01 d3 54 b4 08 00 45 c0 ..^....$ ..T...E.
0010 00 20 b7 92 00 00 01 02 60 dc c0 a8 00 01 e0 00 . ..... `.....
0020 00 04 13 01 98 de 00 0e ff 03 35 0e 20 00 14 00 ....5. ...