??????????????????????

??????????????????????????????????????

??????????????????????????????

http://linux.vbird.org/adsl/031intranet_hubswitch.php

?????????Hub ??????mac address .?????port??????switch???????

??Hub??????????????????(??ARP???)?????????????

mirror port ????

?????????mirror port

???100M HUB ????100M HUB ?????? ,???????????

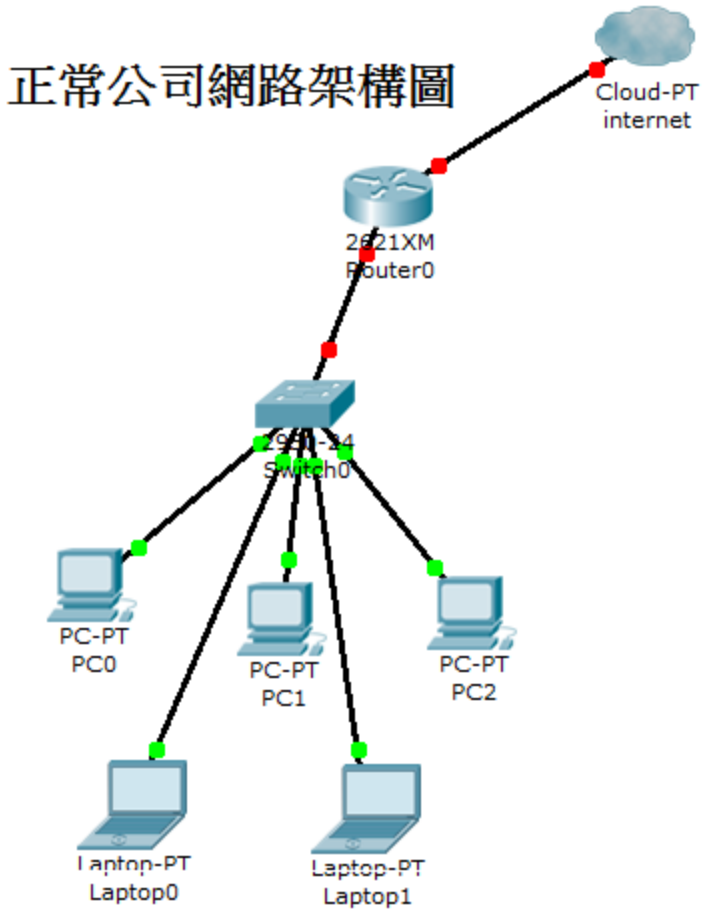
A Port ? Gateway
B Port ????
C Port ????Switch
A ?B ???? C ???..
a=10/2=5Mbps
b=10/2=5Mbps

?????100M HUB????????(??????????????100M ?HUB??Switch)?

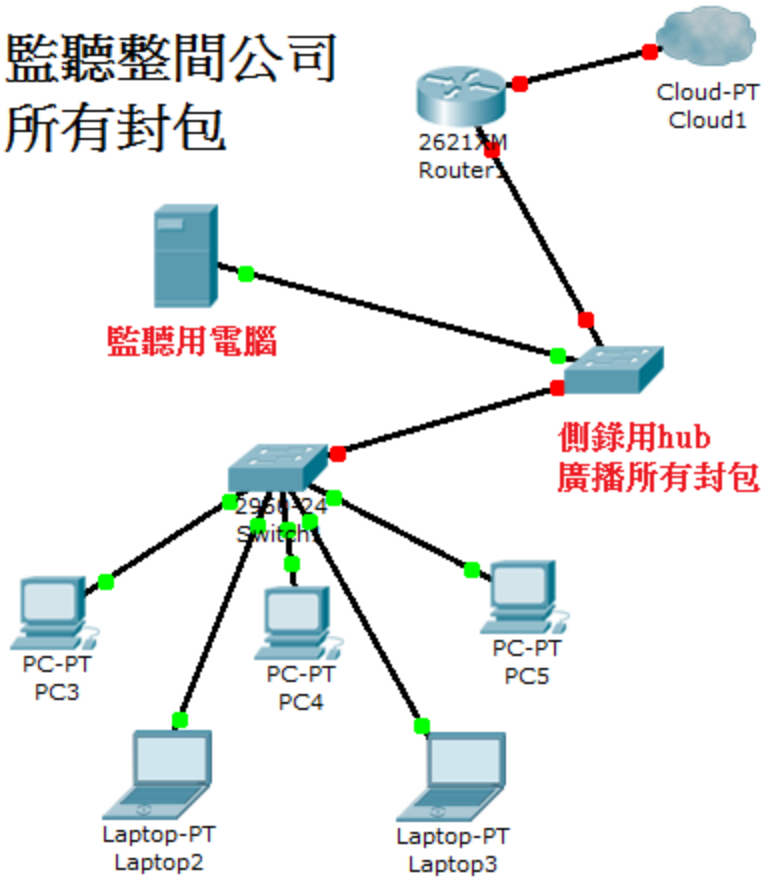
??????????????????????????????????????

???????

????????

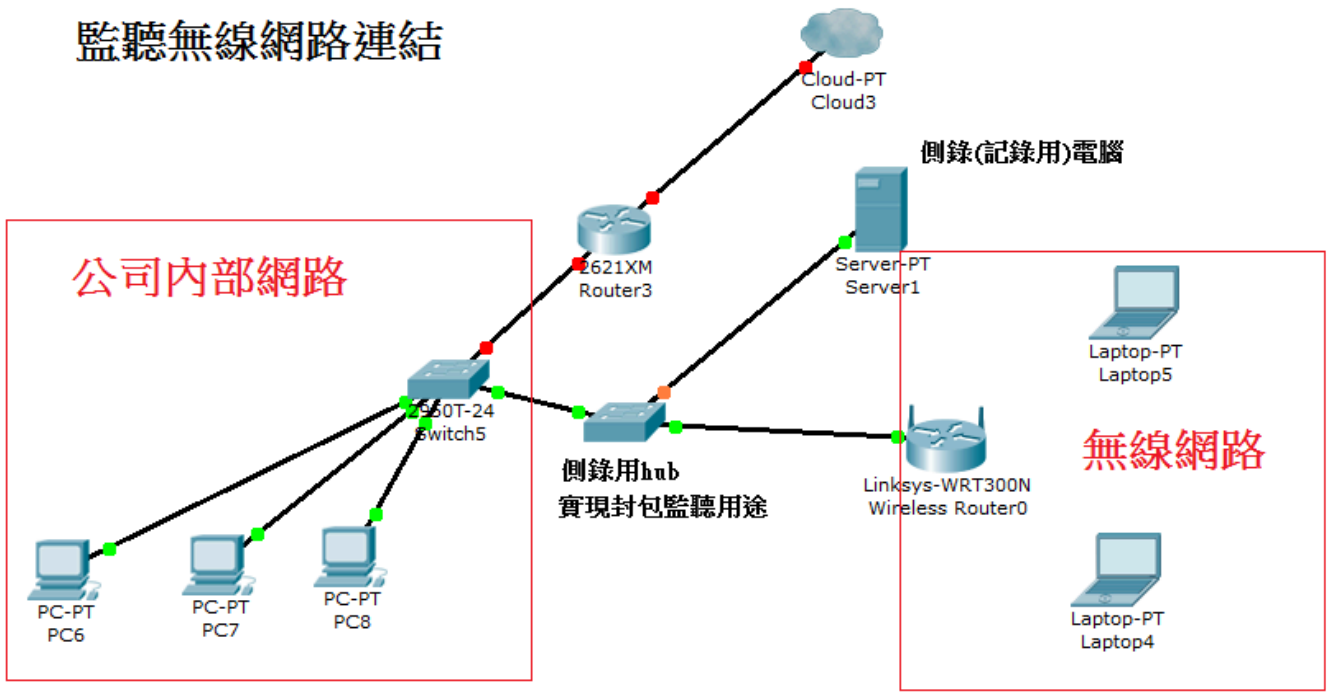

正常公司網路架構圖
Cloud-PT
internet
2621XM
Router0
Switch0
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
Laptop-PT
Laptop0
Laptop-PT
Laptop1

???????????


監聽整間公司
所有封包
Cloud-PT
Cloud1
2621XM
Router1
監聽用電腦
側錄用hub
廣播所有封包
2950-24
Switch1
PC-PT
PC3
PC-PT
PC4
PC-PT
PC5
Laptop-PT
Laptop2
Laptop-PT
Laptop3

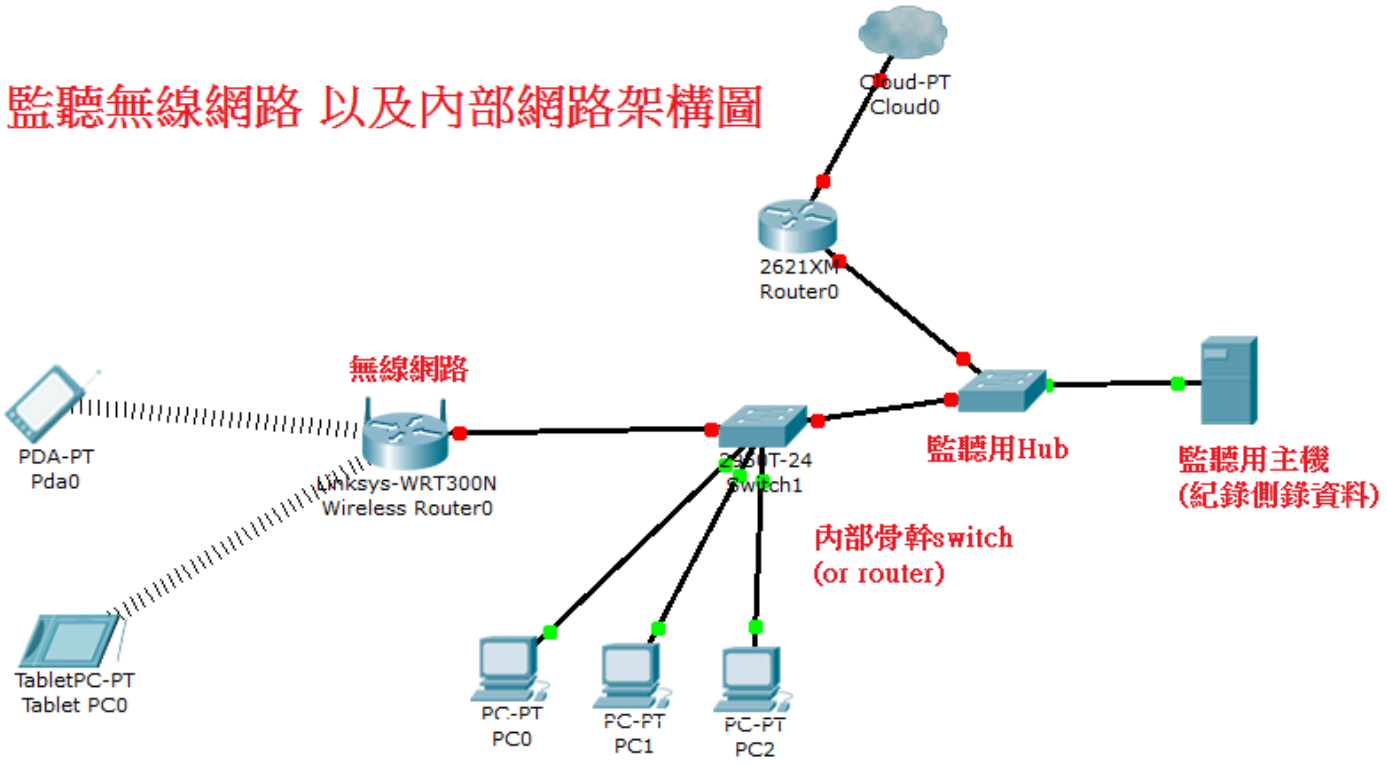
???????????Hub??????????????????

??????(???????)?????


監聽無線網路連結
Cloud-PT
Cloud3
側錄(記錄用)電腦
公司內部網路
2621XM
Router3
Server-PT
Server1
Laptop-PT
Laptop5
2950T-24
Switch5
側錄用hub
實現封包監聽用途
Linksys-WRT300N
Wireless Router0
無線網路
PC-PT
PC6
PC-PT
PC7
PC-PT
PC8
Laptop-PT
Laptop4

??????????????????(????????)???????????(????)???

????


監聽無線網路 以及內部網路架構圖
Cloud-PT
Cloud0
2621XM
Router0
無線網路
PDA-PT
Pda0
Linksys-WRT300N
Wireless Router0
2950T-24
Switch1
監聽用Hub
監聽用主機
(紀錄側錄資料)
內部骨幹switch
(or router)
TabletPC-PT
Tablet PC0
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2

??????????????????????????(????)??????(????)

????Wireshark
http://blog.shaolin.tw/2008/03/wireshark.html

????????????demo????????????????????????

CAIN
http://www.oxid.it/cain.html

Cain??????????????????VOIP???????

FreeHttpsniff
http://www.cleanersoft.com/sniffer/f...tp_sniffer.htm

??

MSN ??
http://formessengers.com/mdetect.htm
??????????MSN?????yahoo????Facebook web chat , ICQ ,AIM ?????????????

websitesniffer

??????Http sniff??????http??????? ??????? sources IP .

Winpcap
http://www.winpcap.org/

????????????????????????????????

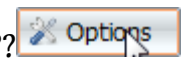
Wireshark
http://www.wireshark.org/

??UTF8????????????????????
Wireshark-utf8-1.2.2 ??????.

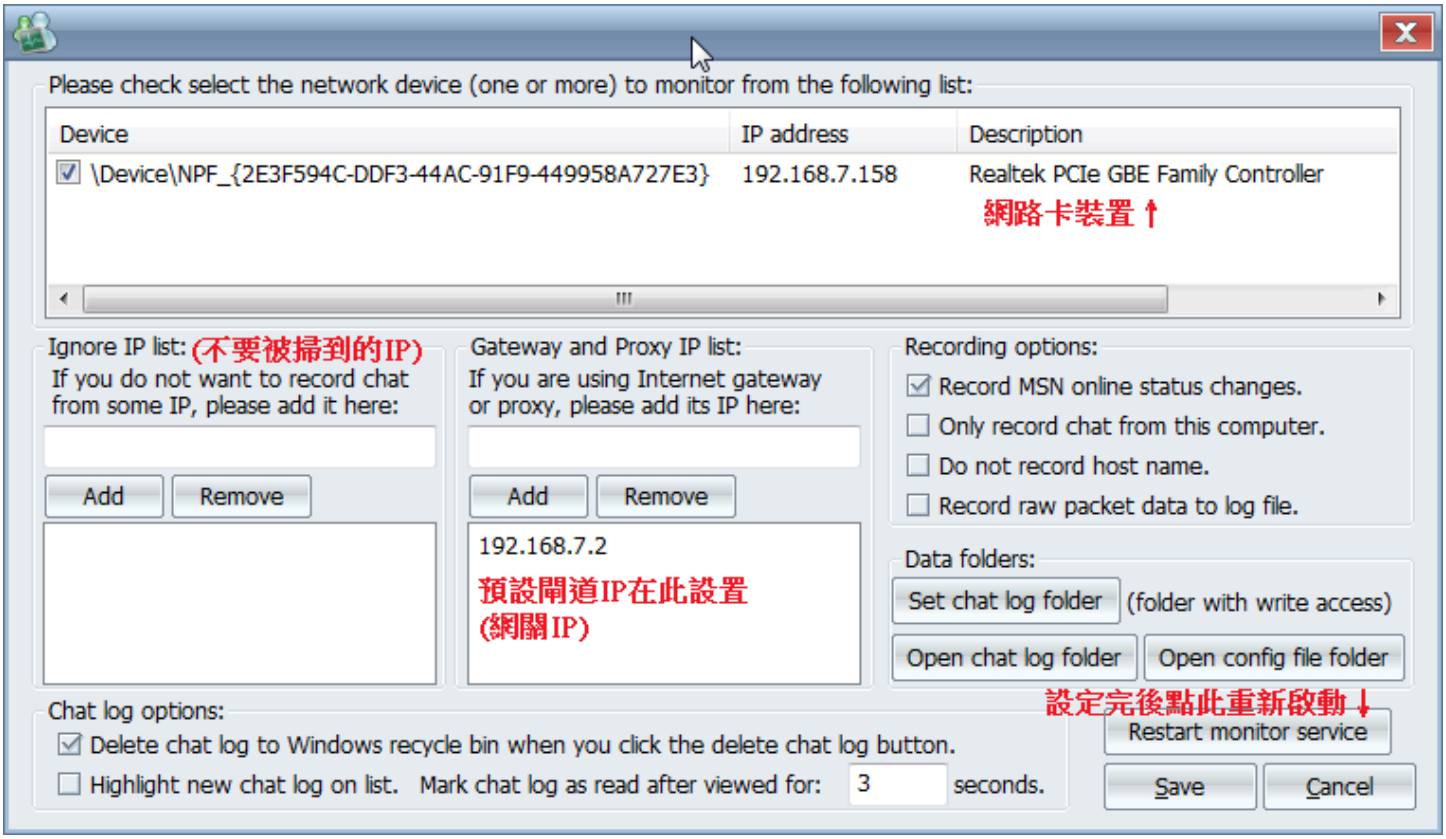
??????????????(??????????)

MSN????????

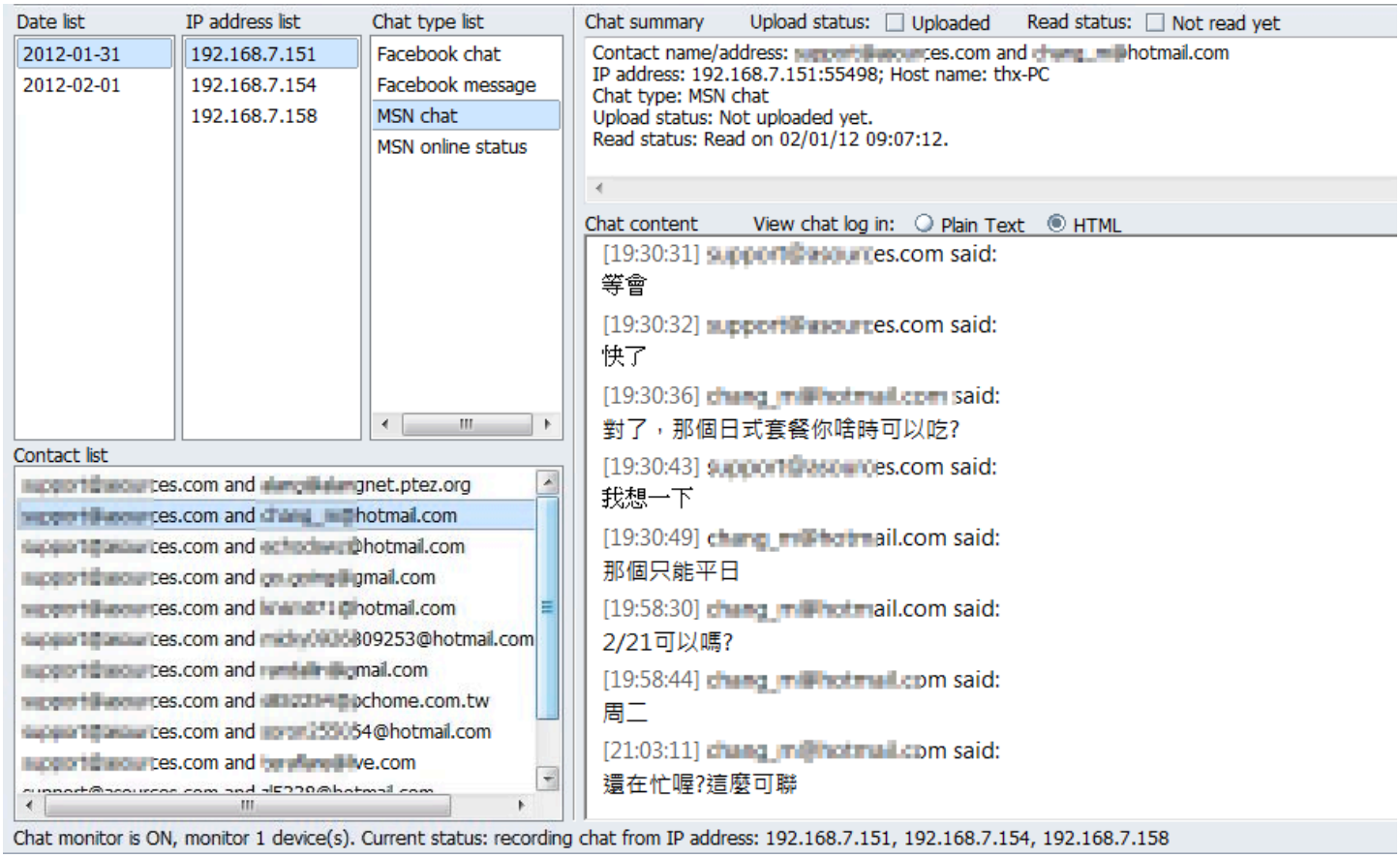
????winpcap

??????????????? 

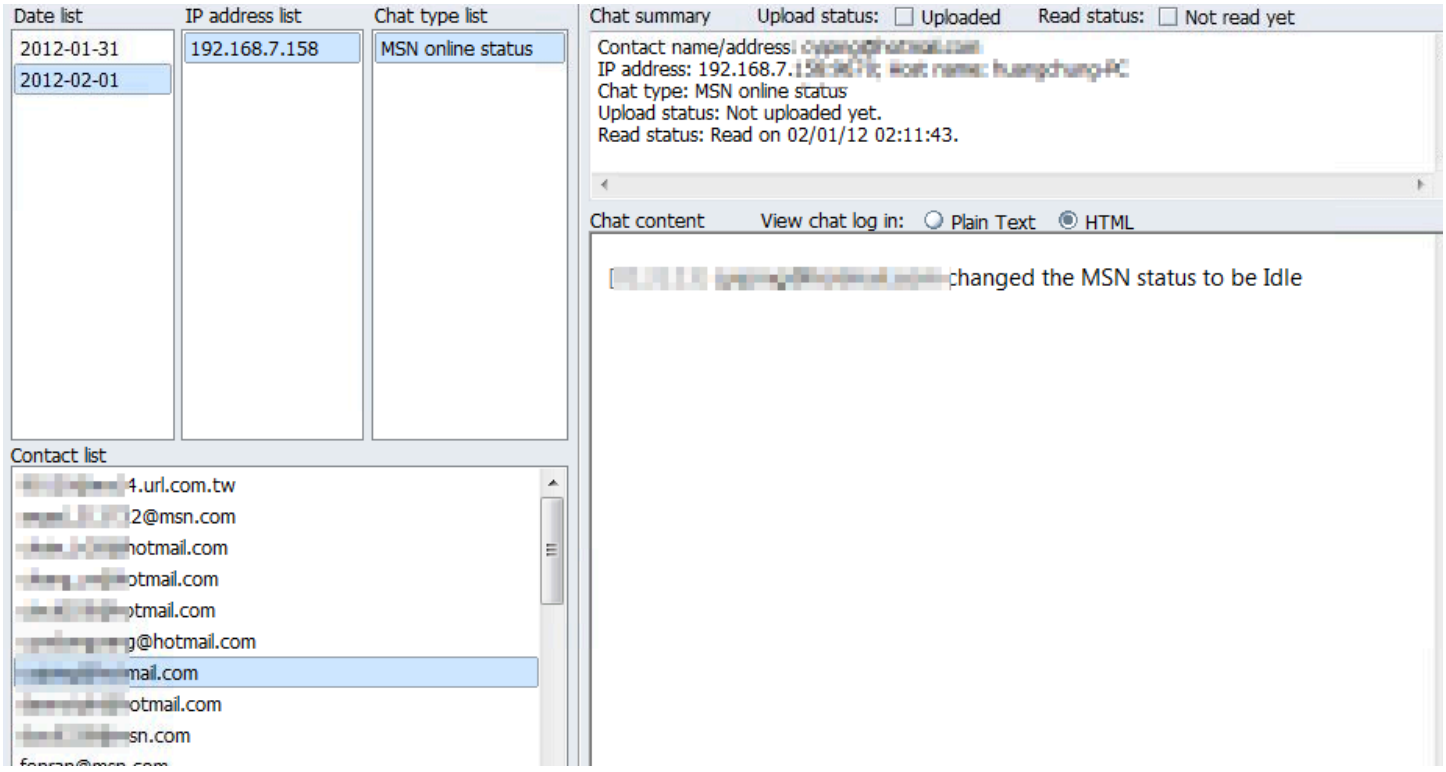
??????


Please check select the network device (one or more) to monitor from the following list:
Device
IP address
Description
\Device\NPF_{2E3F594C-DDF3-44AC-91F9-449958A727E3}
192.168.7.158
Realtek PCIe GBE Family Controller
網路卡裝置
Ignore IP list: (不要被掃到的IP)
If you do not want to record chat from some IP, please add it here:
Add
Remove
Gateway and Proxy IP list:
If you are using Internet gateway or proxy, please add its IP here:
Add
Remove
192.168.7.2
預設閘道IP在此設置
(網關IP)
Recording options:
Record MSN online status changes.
Only record chat from this computer.
Do not record host name.
Record raw packet data to log file.
Data folders:
Set chat log folder
(folder with write access)
Open chat log folder
Open config file folder
設定完後點此重新啟動
Chat log options:
Delete chat log to Windows recycle bin when you click the delete chat log button.
Highlight new chat log on list. Mark chat log as read after viewed for: 3 seconds.
Restart monitor service
Save
Cancel

Msn ????

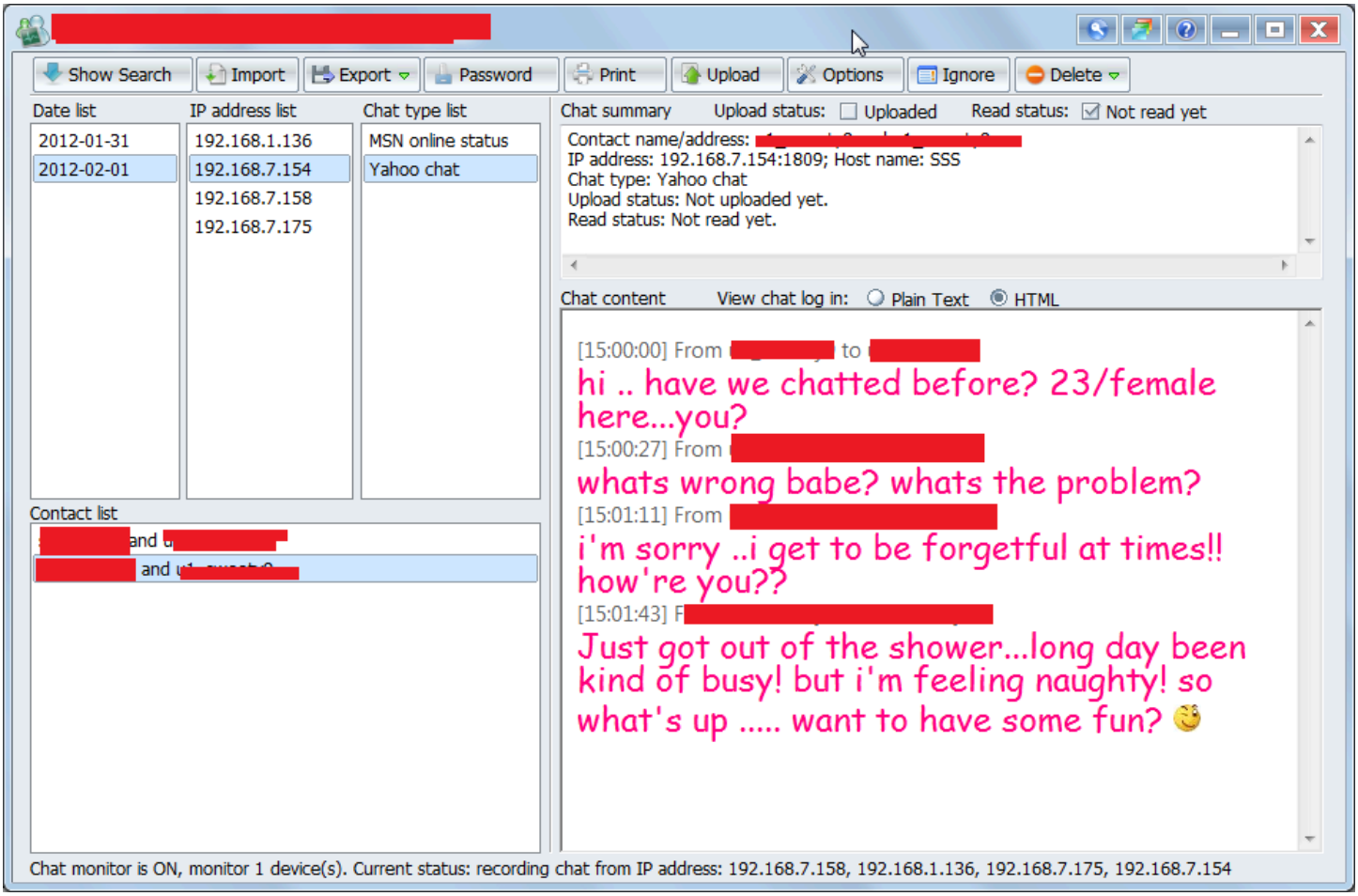

Date list
IP address list
Chat type list
2012-01-31
2012-02-01
192.168.7.151
192.168.7.154
192.168.7.158
Facebook chat
Facebook message
MSN chat
MSN online status
Chat summary
Upload status: Uploaded
Read status: Not read yet
Contact name/address: hotmail.com
IP address: 192.168.7.151:55498; Host name: thx-PC
Chat type: MSN chat
Upload status: Not uploaded yet.
Read status: Read on 02/01/12 09:07:12.
Chat content
View chat log in: Plain Text HTML
[19:30:31] es.com said:
等會
[19:30:32] es.com said:
快了
[19:30:36] said:
對了，那個日式套餐你啥時可以吃?
[19:30:43] es.com said:
我想一下
[19:30:49] ail.com said:
那個只能平日
[19:58:30] ail.com said:
2/21可以嗎?
[19:58:44] om said:
周二
[21:03:11] om said:
還在忙喔?這麼可聯
Contact list
Chat monitor is ON, monitor 1 device(s). Current status: recording chat from IP address: 192.168.7.151, 192.168.7.154, 192.168.7.158

MSN ????

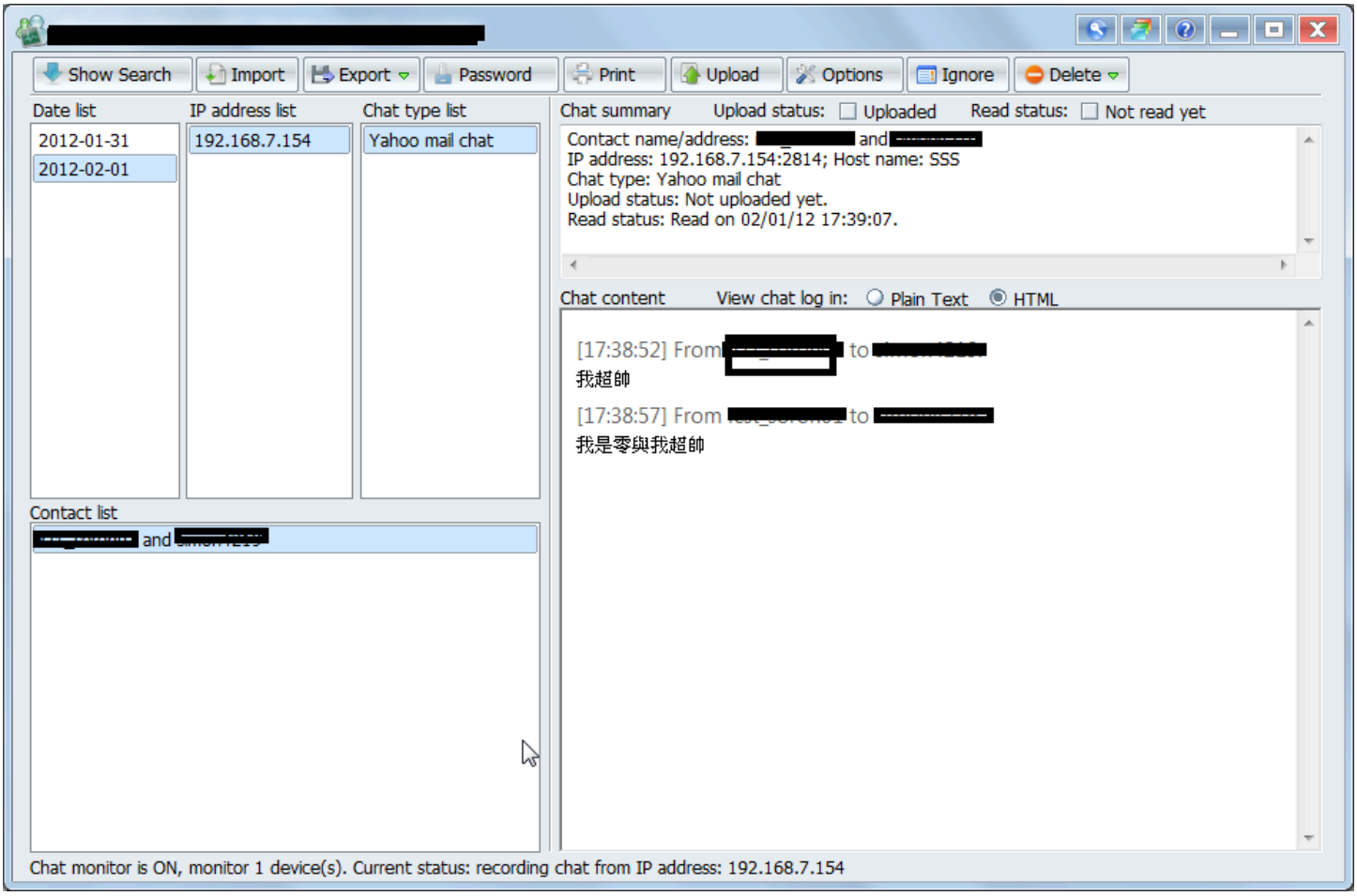

Date list
IP address list
Chat type list
2012-01-31
2012-02-01
192.168.7.158
MSN online status
Chat summary
Upload status: Uploaded
Read status: Not read yet
IP address: 192.168.7.
Chat type: MSN online status
Upload status: Not uploaded yet.
Read status: Read on 02/01/12 02:11:43.
Chat content
View chat log in: Plain Text HTML
changed the MSN status to be Idle
Contact list

MSN Web Chat

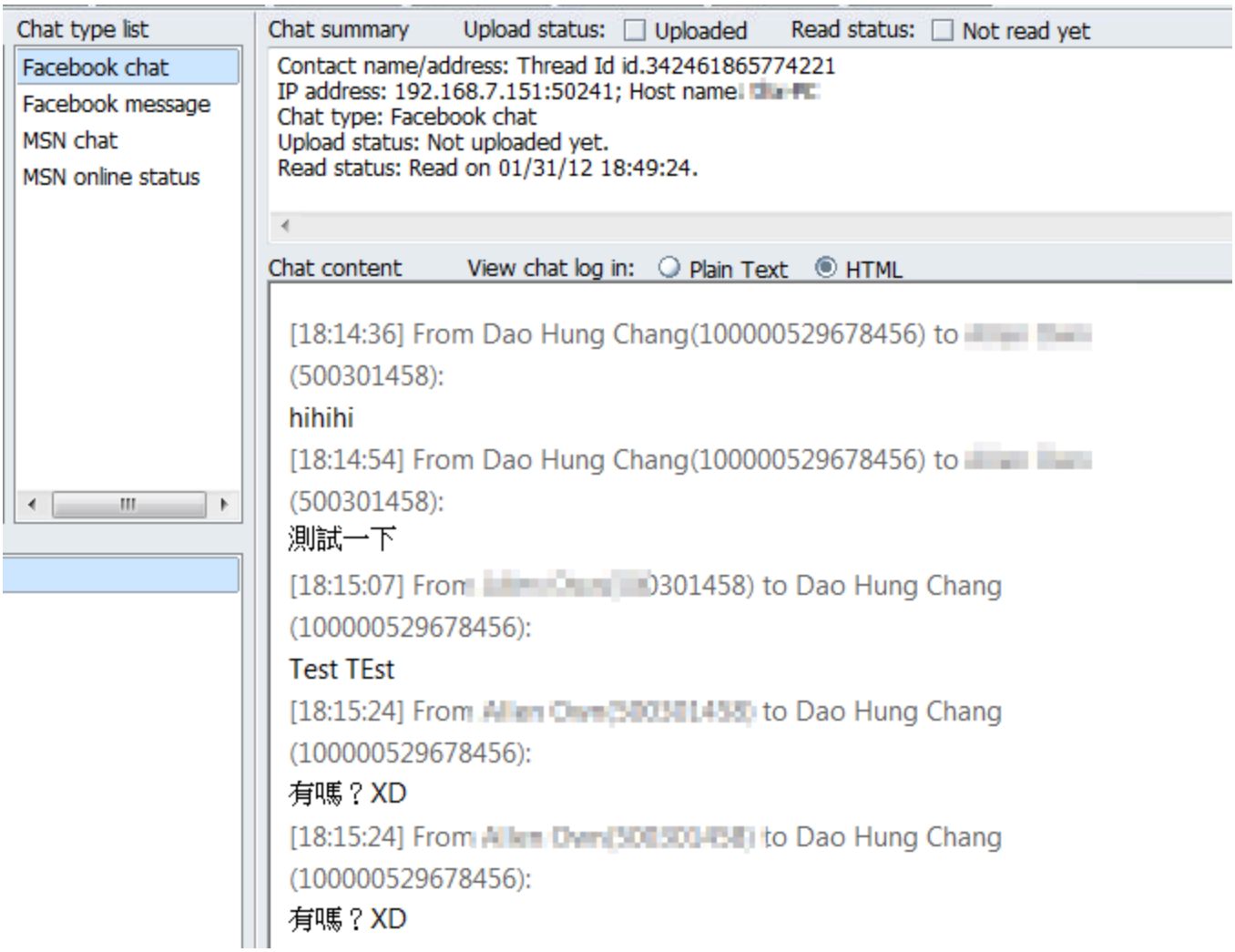
yahoo ???



Yahoo????

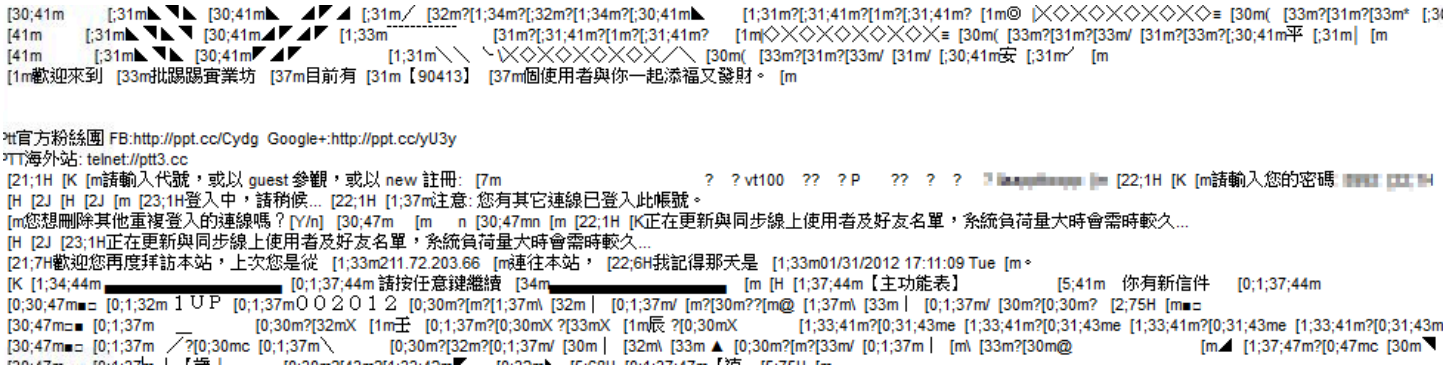


Facebook chat ????



http://www.oxid.it/cain.html ?????????????

Telnet ??



FTP ??

Timestamp	FTP server	Client	Username	Password
31/01/2012 - 18:46:00		192.168.7.154		

???????

server	Client	Username	Password	URL	UserField	PassField	AuthTyp
5.31.156	192.168.7.158	1263612021....	5	com.tw/v4/news.php	id=	p=	Basic (F
5.31.155	192.168.7.158	1263612021....	5	g.doubleclick.net/pagead/ads?client=c...	id=	p=	Basic (F
5.31.138	192.168.7.158	407485253	/v4/index.php	com.tw/v4/index.php	id=	p=	Basic (F
5.31.138	192.168.7.158	1951136101	/v4/login.php	com.tw/v4/login.php	id=	p=	Basic (F
2.203.61	192.168.7.158			com.tw/v4/login.php	username=	password=	Basic (F
5.31.138	192.168.7.158	1916785736	/v4/index.php	com.tw/v4/index.php	id=	p=	Basic (F

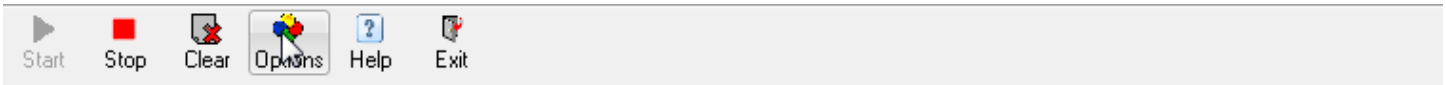
74.125.31.156	192.168.7.158	2739871951	5		http://googleads.g.doubleclic
74.125.31.156	192.168.7.158	2596134854	5		http://googleads.g.doubleclic
123.204.250.1...	192.168.7.158	thx			http://digiland.tw/login.php
74.125.31.156	192.168.7.158	3998330345	5		http://digiland.tw/index.php
74.125.31.156	192.168.7.158	2739871951	5		http://digiland.tw/index.php

web ????

??????????Free HTTP Sniffer

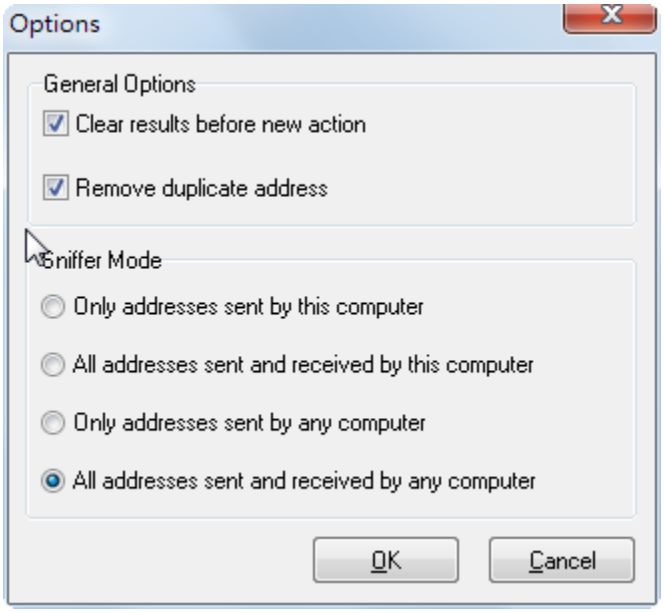
???????????????

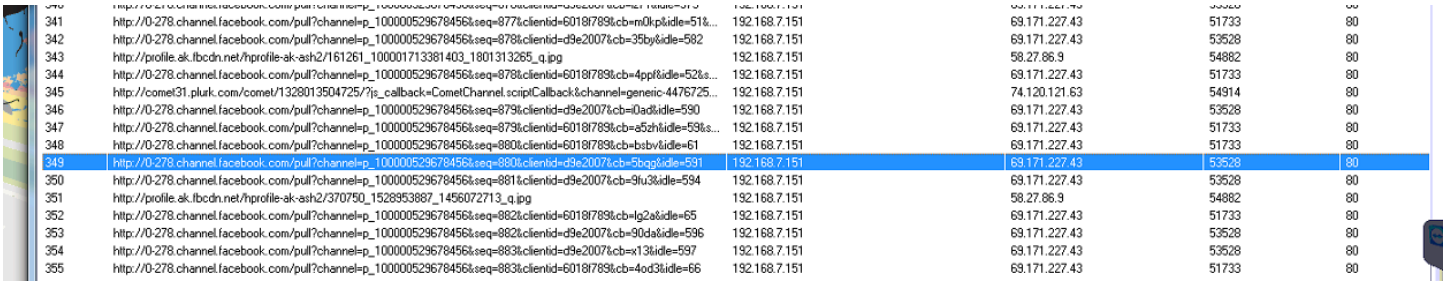
???????????????



??????Options

????????????(All addresses sent and received by any computer)





341	http://0-278.channel.facebook.com/pull?channel=p_100000529678456&seq=877&clientid=6018f789&cb=m0kp&idle=51&...	192.168.7.151	69.171.227.43	51733	80
342	http://0-278.channel.facebook.com/pull?channel=p_100000529678456&seq=878&clientid=d9e2007&cb=35by&idle=582	192.168.7.151	69.171.227.43	53528	80
343	http://profile.ak.fbcdn.net/hprofile-ak-ash2/161261_100001713381403_1801313265_q.jpg	192.168.7.151	58.27.86.9	54882	80
344	http://0-278.channel.facebook.com/pull?channel=p_100000529678456&seq=878&clientid=6018f789&cb=4ppf&idle=52&s...	192.168.7.151	69.171.227.43	51733	80
345	http://comet31.plurk.com/comet/1328013504725/?js_callback=CometChannel.scriptCallback&channel=generic-4476725...	192.168.7.151	74.120.121.63	54914	80
346	http://0-278.channel.facebook.com/pull?channel=p_100000529678456&seq=879&clientid=d9e2007&cb=i0ad&idle=590	192.168.7.151	69.171.227.43	53528	80
347	http://0-278.channel.facebook.com/pull?channel=p_100000529678456&seq=879&clientid=6018f789&cb=a5zh&idle=59&s...	192.168.7.151	69.171.227.43	51733	80
348	http://0-278.channel.facebook.com/pull?channel=p_100000529678456&seq=880&clientid=6018f789&cb=bsbv&idle=61	192.168.7.151	69.171.227.43	51733	80
349	http://0-278.channel.facebook.com/pull?channel=p_100000529678456&seq=880&clientid=d9e2007&cb=5bqg&idle=591	192.168.7.151	69.171.227.43	53528	80
350	http://0-278.channel.facebook.com/pull?channel=p_100000529678456&seq=881&clientid=d9e2007&cb=9fu3&idle=594	192.168.7.151	69.171.227.43	53528	80
351	http://profile.ak.fbcdn.net/hprofile-ak-ash2/370750_1528953887_1456072713_q.jpg	192.168.7.151	58.27.86.9	54882	80
352	http://0-278.channel.facebook.com/pull?channel=p_100000529678456&seq=882&clientid=6018f789&cb=lg2a&idle=65	192.168.7.151	69.171.227.43	51733	80
353	http://0-278.channel.facebook.com/pull?channel=p_100000529678456&seq=882&clientid=d9e2007&cb=90da&idle=596	192.168.7.151	69.171.227.43	53528	80
354	http://0-278.channel.facebook.com/pull?channel=p_100000529678456&seq=883&clientid=d9e2007&cb=x13t&idle=597	192.168.7.151	69.171.227.43	53528	80
355	http://0-278.channel.facebook.com/pull?channel=p_100000529678456&seq=883&clientid=6018f789&cb=4od3&idle=66	192.168.7.151	69.171.227.43	51733	80

?????+?????? ?????????? ??????? ???? ?????

???? Voip ????

??????????
http://www.ublink.org/index.php/2010...rtmonitor.html
http://www.mobile01.com/topicdetail....&t=1503696&r=9
http://januslin.blog.ithome.com.tw/post/1861/134092
2820 ???? ?????????

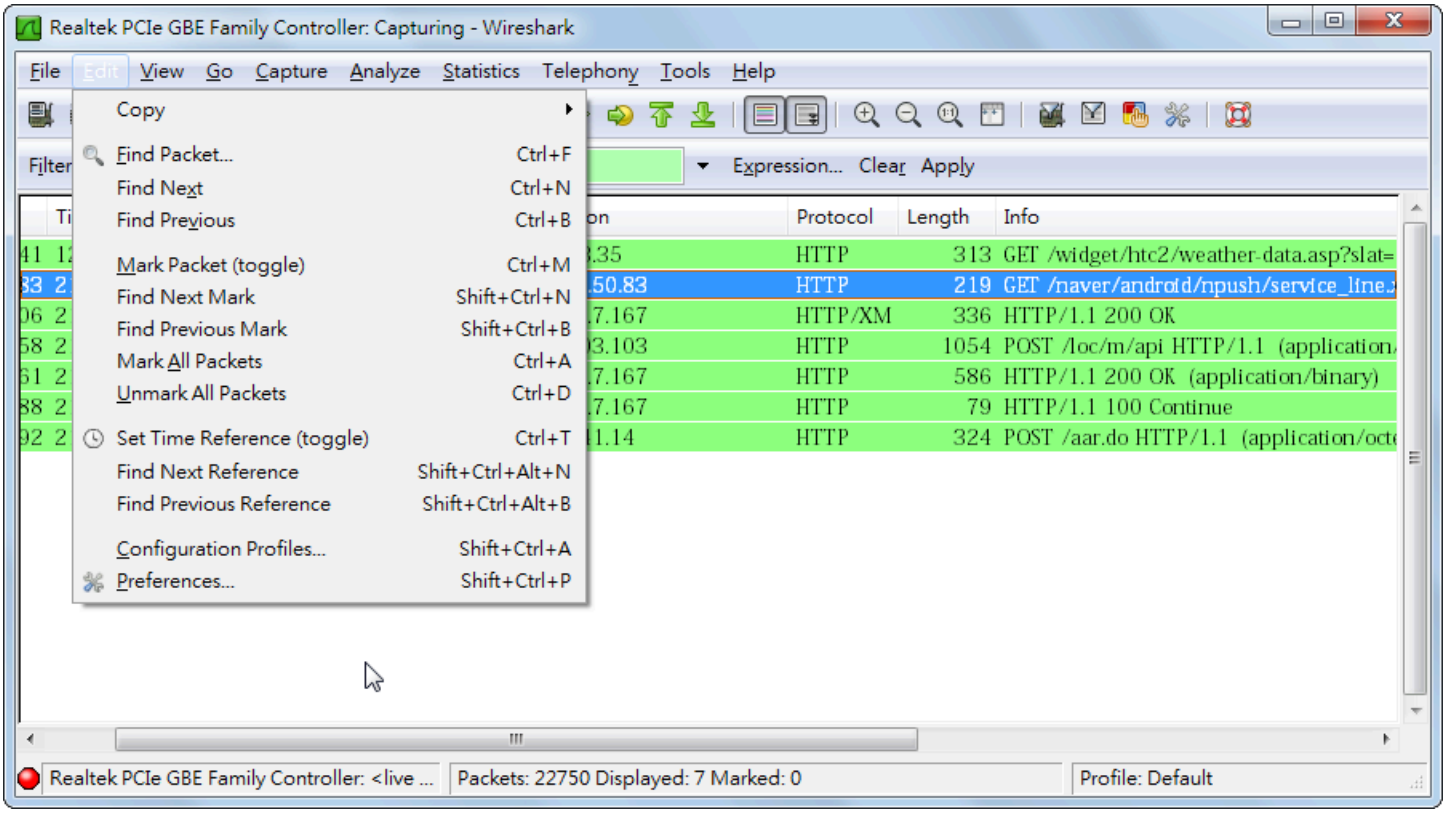
==========

???? wireshark
????UTF8???wireshark

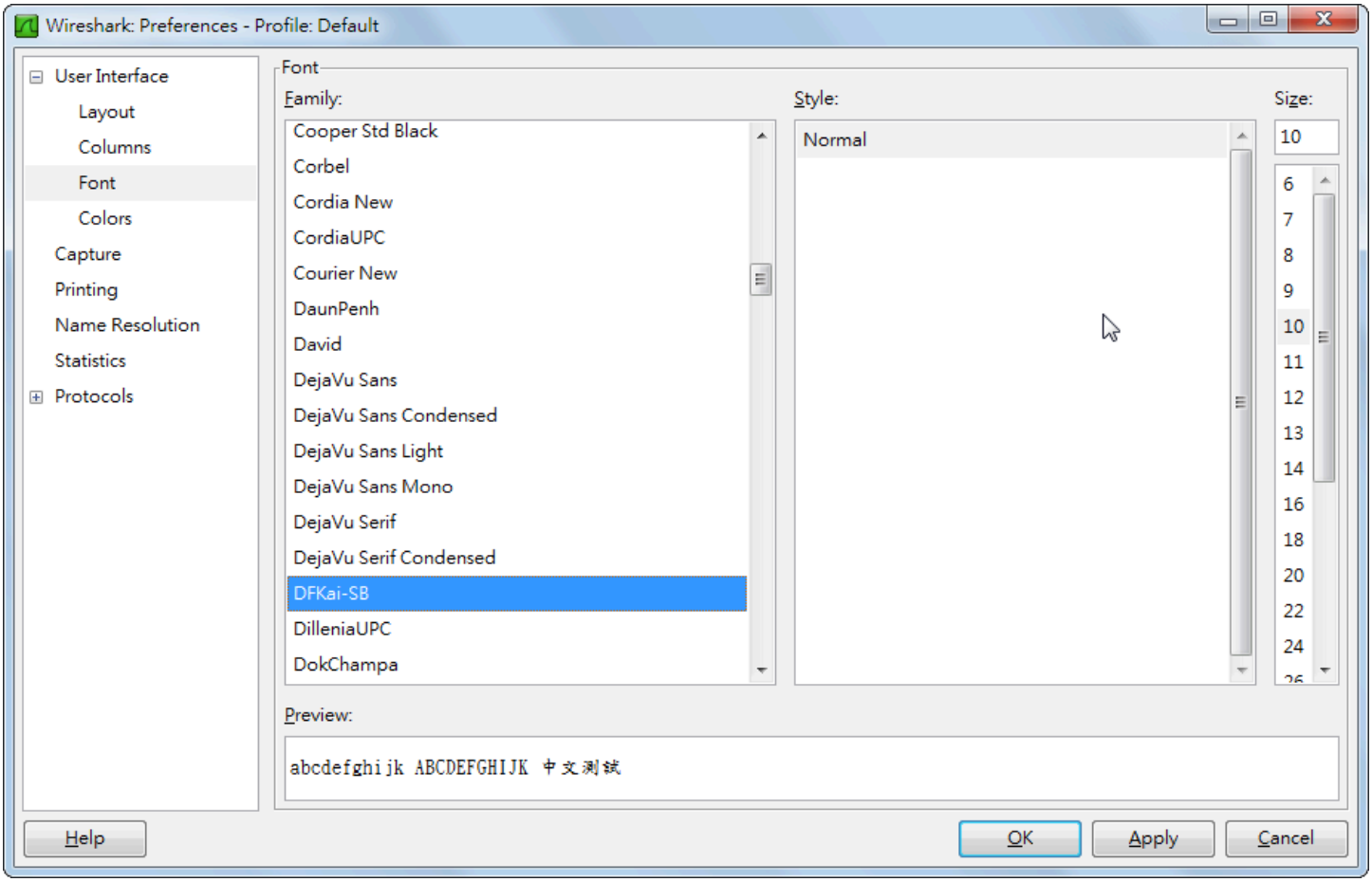
??? Wireshark???? utf8 ,?????????????
??????????????????????????????

??????

??????????????????(???shift+ctrl+p)

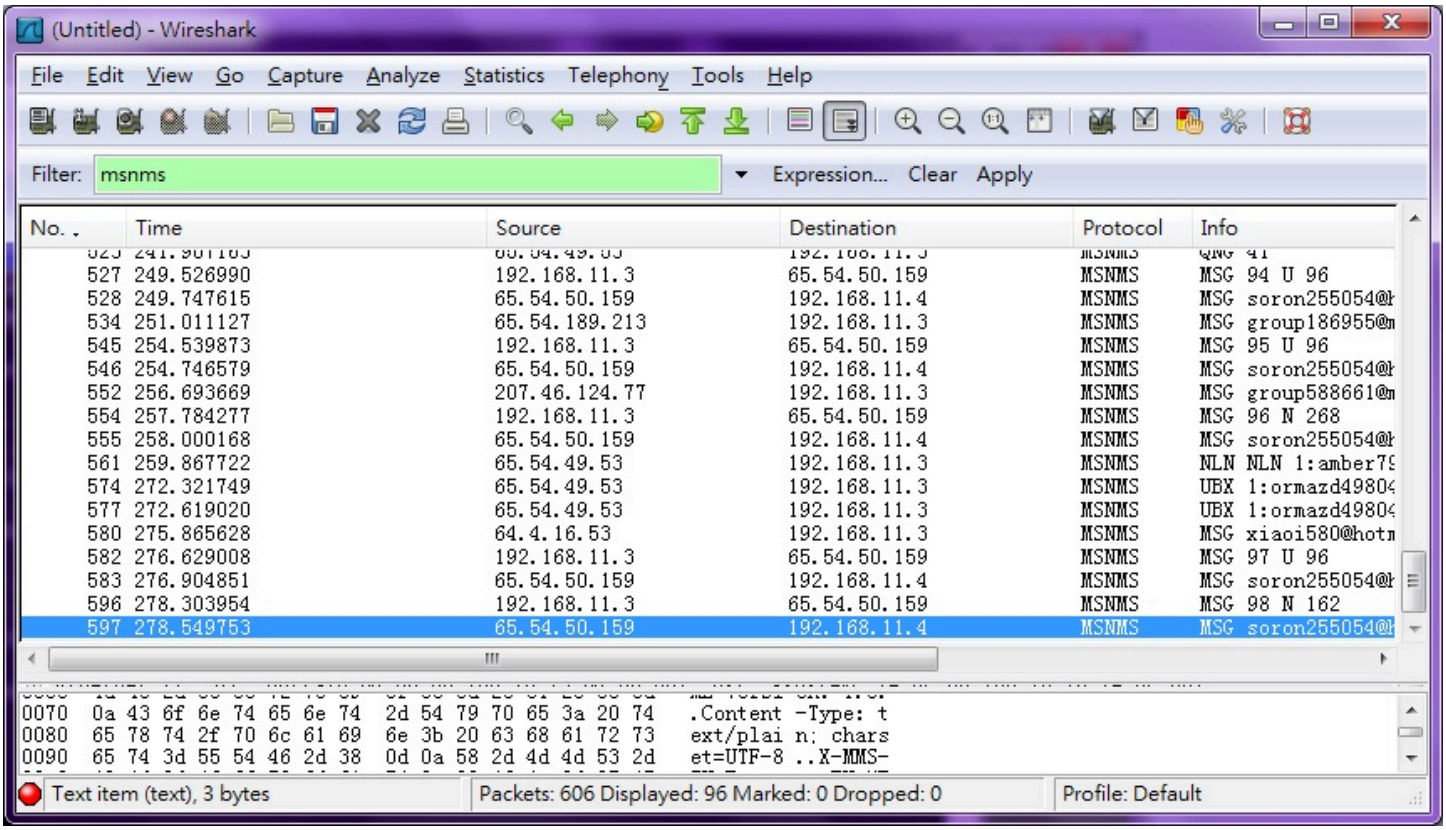

Realtek PCIe GBE Family Controller: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Copy
Find Packet... Ctrl+F
Find Next Ctrl+N
Find Previous Ctrl+B
Mark Packet (toggle) Ctrl+M
Find Next Mark Shift+Ctrl+N
Find Previous Mark Shift+Ctrl+B
Mark All Packets Ctrl+A
Unmark All Packets Ctrl+D
Set Time Reference (toggle) Ctrl+T
Find Next Reference Shift+Ctrl+Alt+N
Find Previous Reference Shift+Ctrl+Alt+B
Configuration Profiles... Shift+Ctrl+A
Preferences... Shift+Ctrl+P
Filter
Expression... Clear Apply
Protocol Length Info
HTTP 313 GET /widget/htc2/weather-data.asp?slat=
HTTP 219 GET /naver/android/npush/service_line.
HTTP/XM 336 HTTP/1.1 200 OK
HTTP 1054 POST /loc/m/api HTTP/1.1 (application
HTTP 586 HTTP/1.1 200 OK (application/binary)
HTTP 79 HTTP/1.1 100 Continue
HTTP 324 POST /aar.do HTTP/1.1 (application/octe
Realtek PCIe GBE Family Controller: <live ...
Packets: 22750 Displayed: 7 Marked: 0
Profile: Default

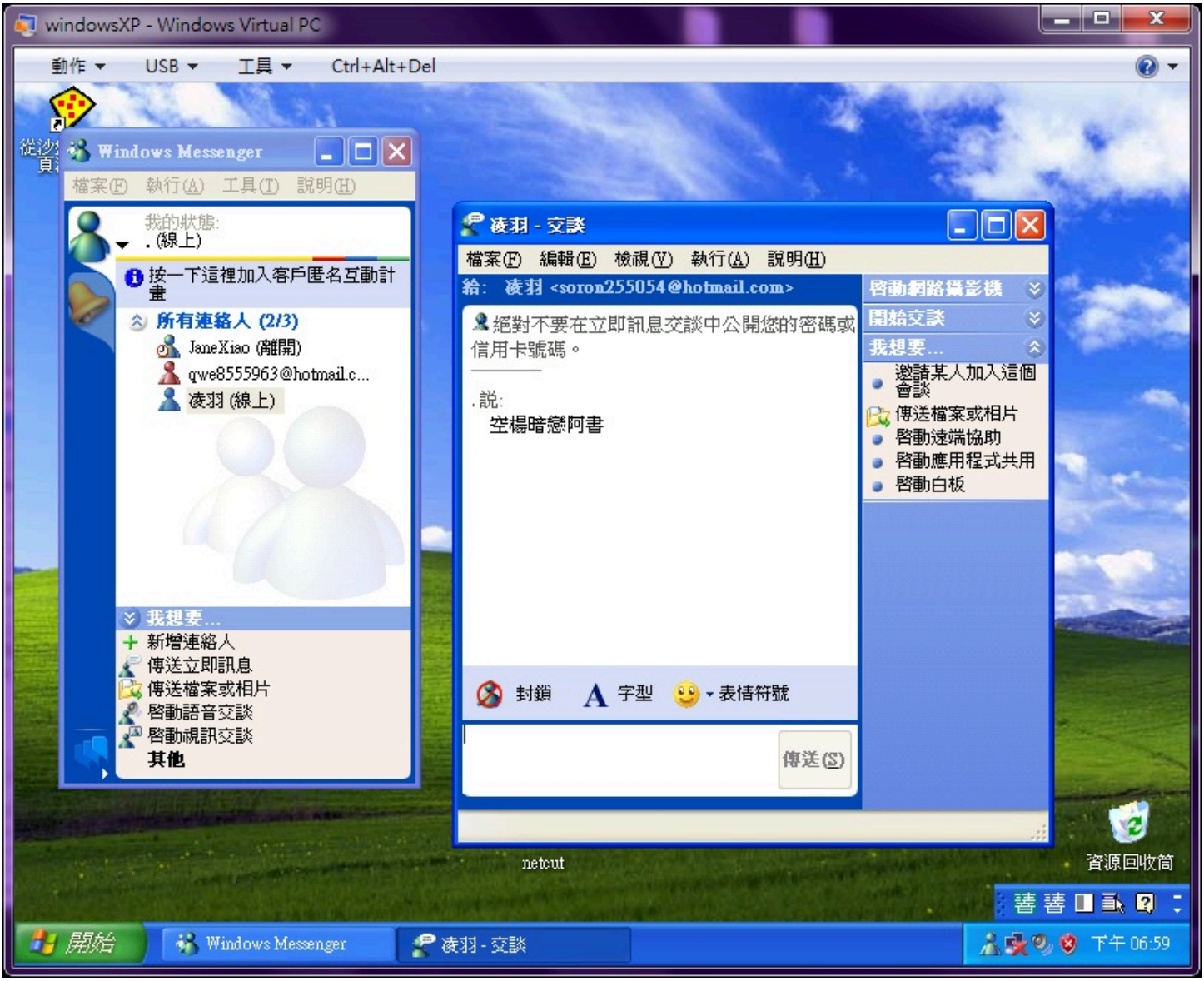
?????

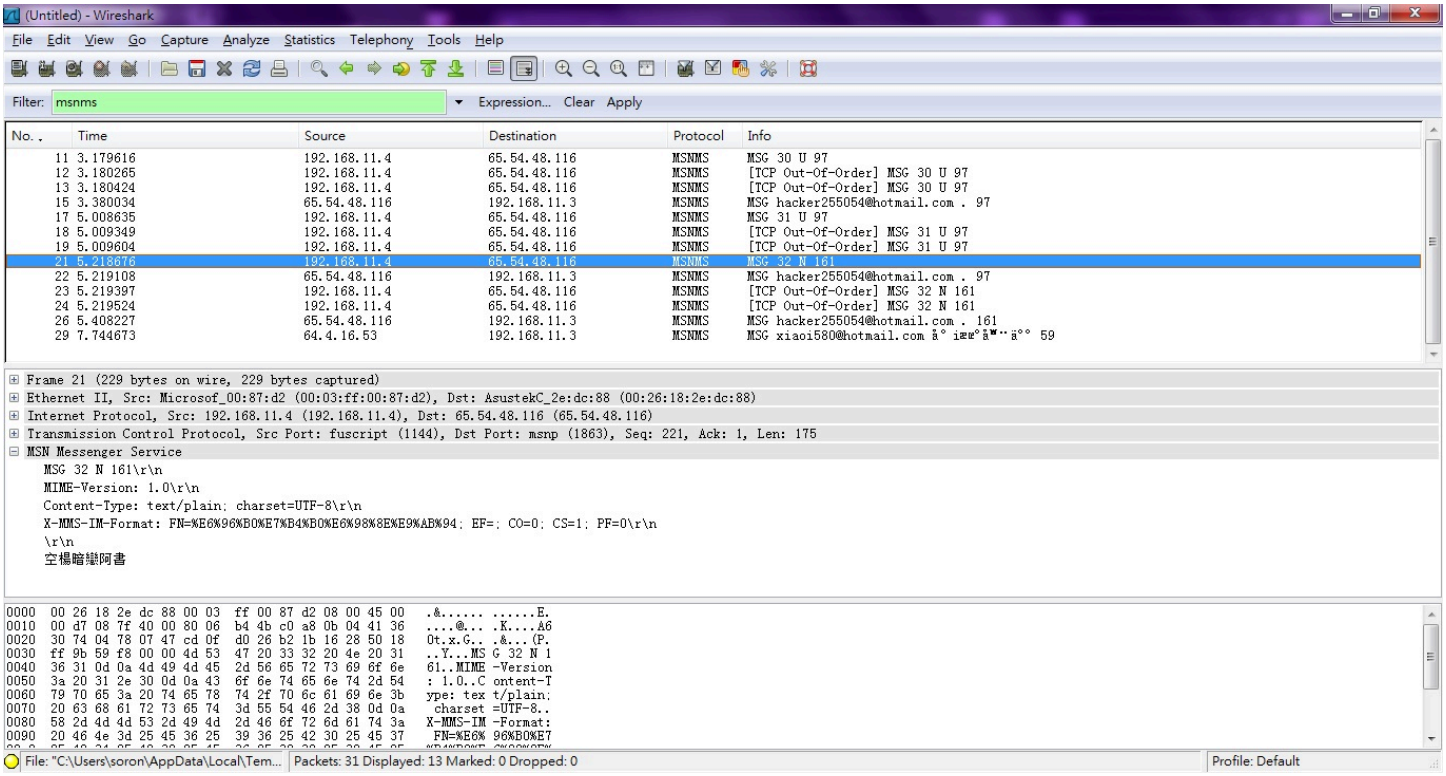

Wireshark: Preferences - Profile: Default
User Interface
Layout
Columns
Font
Colors
Capture
Printing
Name Resolution
Statistics
Protocols
Font
Family:
Style:
Size:
Cooper Std Black
Corbel
Cordia New
CordiaUPC
Courier New
DaunPenh
David
DejaVu Sans
DejaVu Sans Condensed
DejaVu Sans Light
DejaVu Sans Mono
DejaVu Serif
DejaVu Serif Condensed
DFKai-SB
DilleniaUPC
DokChampa
Normal
10
Preview:
abcdefghijk ABCDEFGHIJK 中文測試
Help
OK
Apply
Cancel

??????IP????????

ip.addr == 192.168.x.x and msnms




windowsXP - Windows Virtual PC
動作
USB
工具
Ctrl+Alt+Del
Windows Messenger
檔案(F) 執行(A) 工具(T) 說明(H)
我的狀態:
(線上)
按一下這裡加入客戶匿名互動計畫
所有連絡人 (2/3)
JaneXiao (離開)
qwe8555963@hotmail.c...
凌羽 (線上)
我想要...
新增連絡人
傳送立即訊息
傳送檔案或相片
啓動語音交談
啓動視訊交談
其他
凌羽 - 交談
檔案(F) 編輯(E) 檢視(V) 執行(A) 說明(H)
給: 凌羽 <soron255054@hotmail.com>
絕對不要在立即訊息交談中公開您的密碼或信用卡號碼。
說:
空楊暗戀阿書
封鎖
字型
表情符號
傳送(S)
啓動網路攝影機
開始交談
我想要...
邀請某人加入這個會談
傳送檔案或相片
啓動遠端協助
啓動應用程式共用
啓動白板
netcut
資源回收筒
開始
Windows Messenger
凌羽 - 交談
下午 06:59



???????http??

???? ip.addr == 192.168.x.x and http