

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

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

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

[http://linux.vbird.org/adsl/031intranet\\_hubswitch.php](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

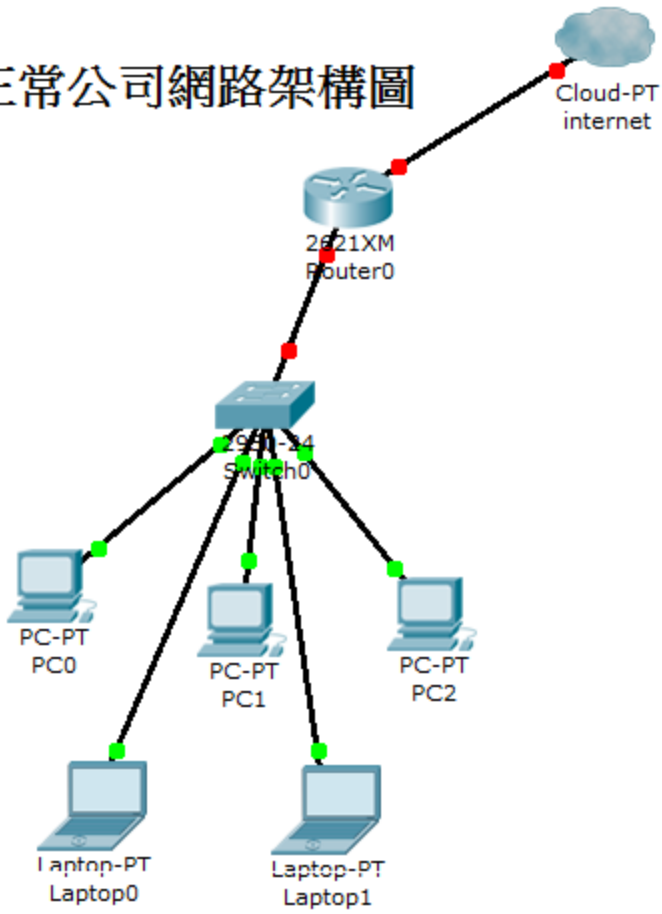
?????100M HUB????????(?????????????????100M ?HUB??Switch )?

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

????????

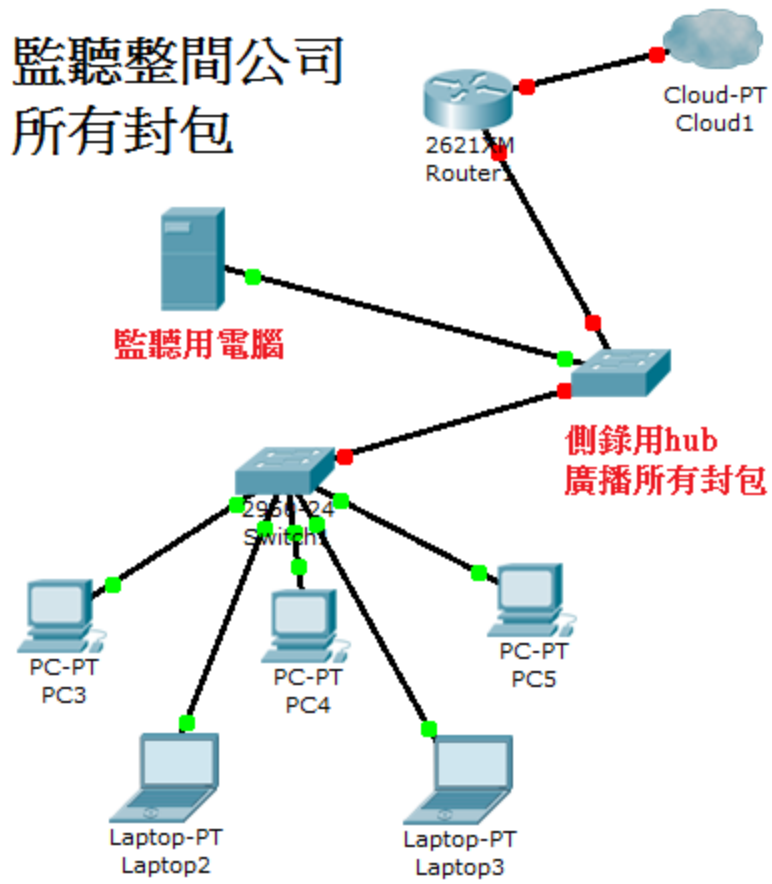
????????

# 正常公司網路架構圖



???????????

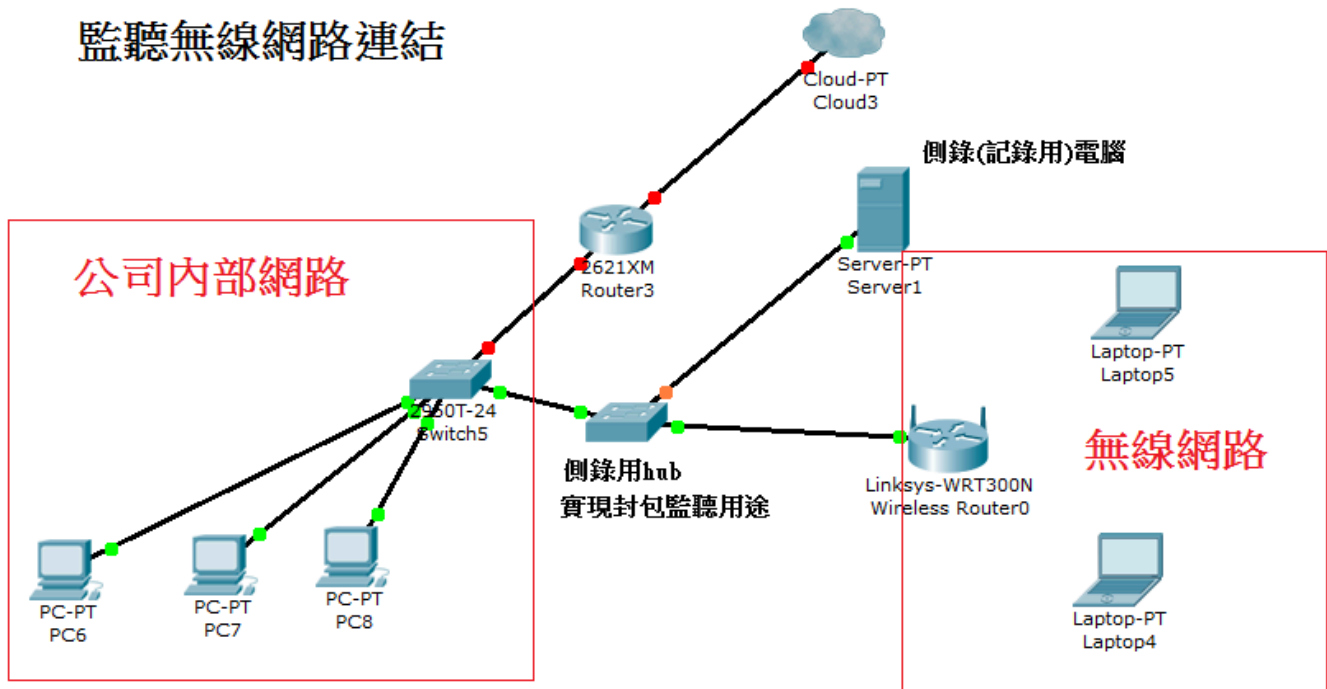
# 監聽整間公司 所有封包



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

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

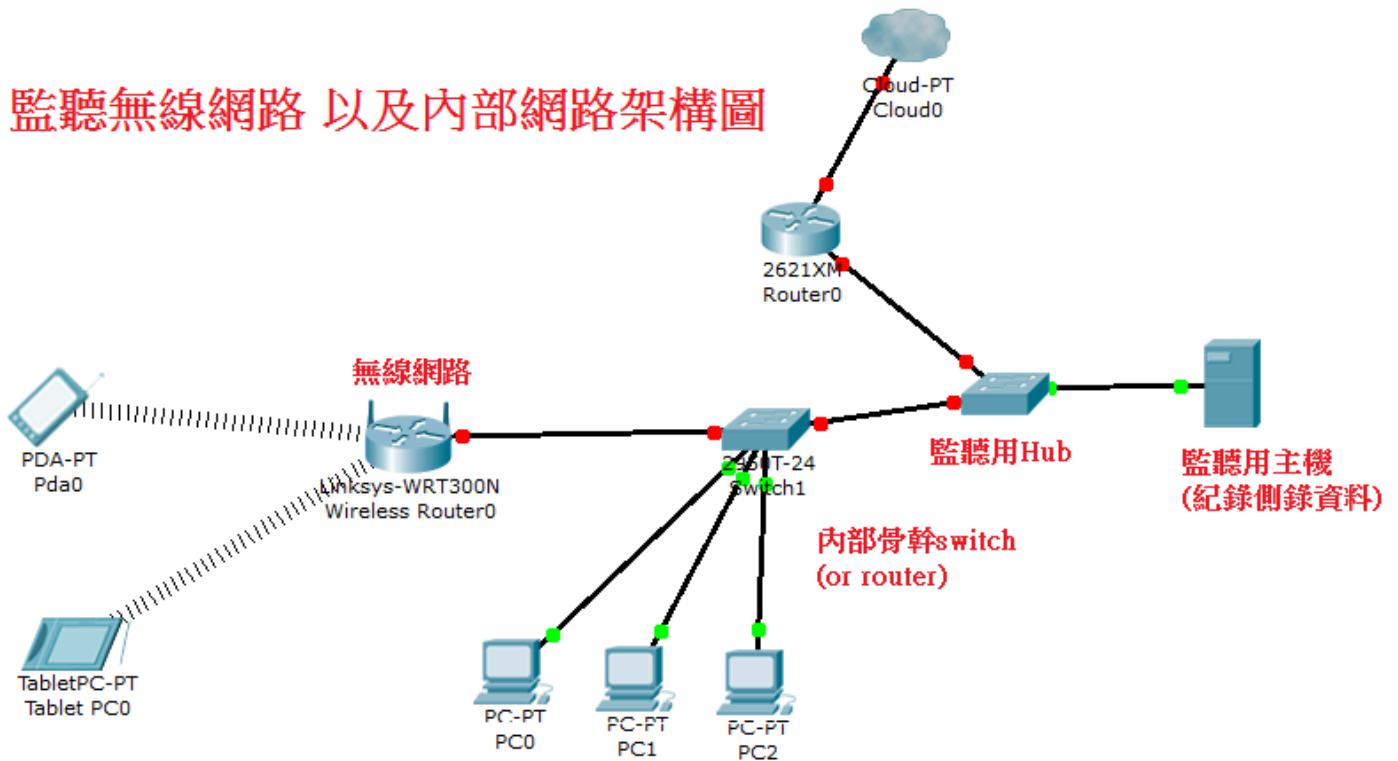
### 監聽無線網路連結



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

????

### 監聽無線網路 以及內部網路架構圖



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

????Wireshark

<http://blog.shaolin.tw/2008/03/wireshark.html>

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

**CAIN**

<http://www.oxid.it/cain.html>

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

**FreeHttpsniiff**

[http://www.cleansoft.com/sniffer/f...tp\\_sniffer.htm](http://www.cleansoft.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 ??????.**

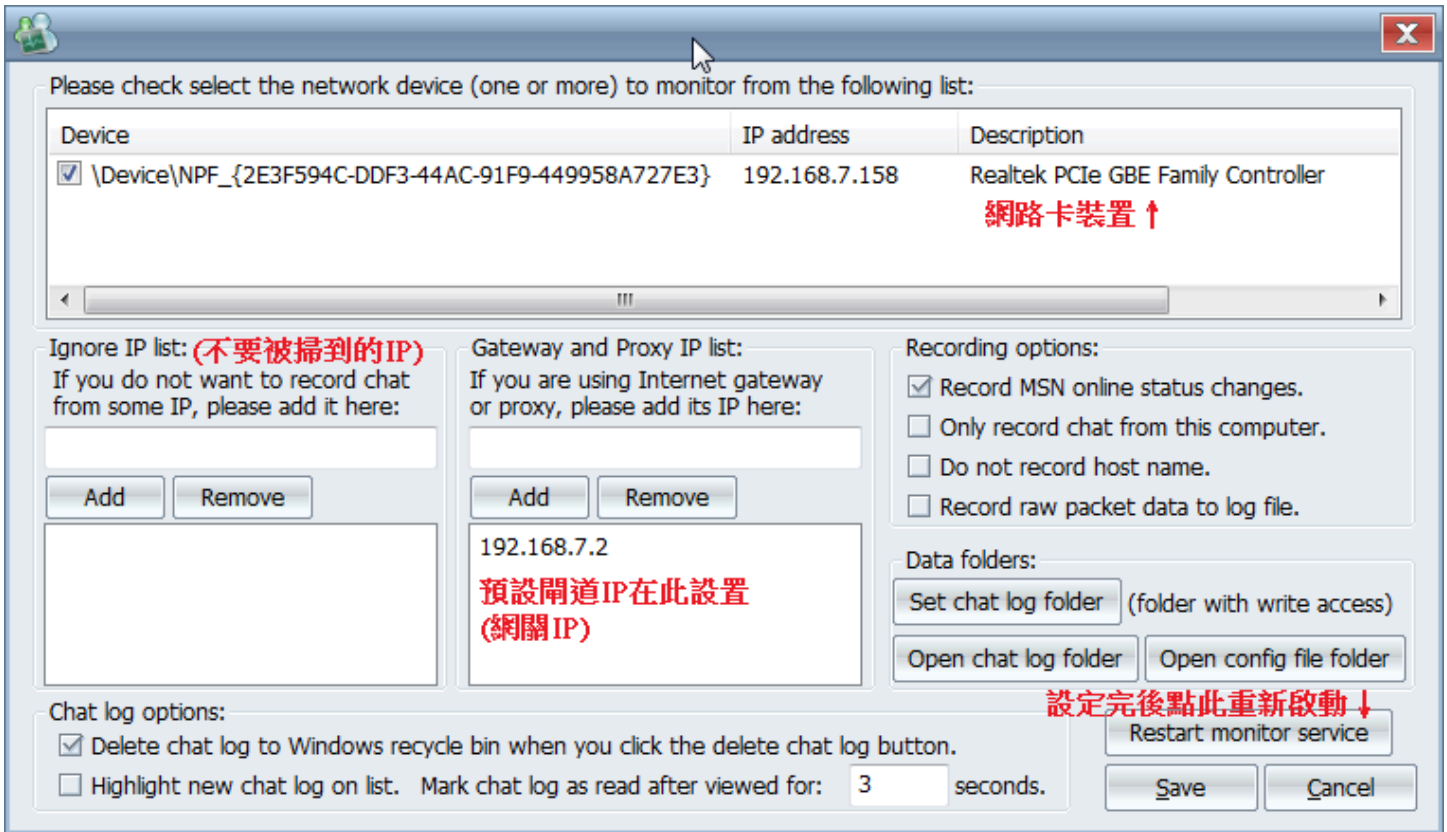
????????????????(?????????)

MSN????????

????winpcap

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

??????



Msn ????

Date list	IP address list	Chat type list	Chat summary
2012-01-31	192.168.7.151	Facebook chat	Upload status: <input type="checkbox"/> Uploaded    Read status: <input type="checkbox"/> Not read yet Contact name/address: support@resources.com and chang_mi@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.
2012-02-01	192.168.7.154	Facebook message	
	192.168.7.158	MSN chat	
		MSN online status	

Chat content
View chat log in: <input type="radio"/> Plain Text <input checked="" type="radio"/> HTML [19:30:31] support@resources.com said: 等會 [19:30:32] support@resources.com said: 快了 [19:30:36] chang_mi@hotmail.com said: 對了，那個日式套餐你啥時可以吃? [19:30:43] support@resources.com said: 我想一下 [19:30:49] chang_mi@hotmail.com said: 那個只能平日 [19:58:30] chang_mi@hotmail.com said: 2/21可以嗎? [19:58:44] chang_mi@hotmail.com said: 周二 [21:03:11] chang_mi@hotmail.com said: 還在忙哩?這麼可聯

Contact list
support@resources.com and sheng@shengnet.ptez.org support@resources.com and chang_mi@hotmail.com support@resources.com and schodew@hotmail.com support@resources.com and go.going@gmail.com support@resources.com and kiana071@hotmail.com support@resources.com and michy000809253@hotmail.com support@resources.com and hmdell@gmail.com support@resources.com and 880034@pchome.com.tw support@resources.com and ipron250054@hotmail.com support@resources.com and tyafire@live.com support@resources.com and al5228@hotmail.com

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	Chat summary
2012-01-31	192.168.7.158	MSN online status	Upload status: <input type="checkbox"/> Uploaded    Read status: <input type="checkbox"/> Not read yet Contact name/address: cypanq@hotmail.com IP address: 192.168.7.158:3676; Host name: huangchung-PC Chat type: MSN online status Upload status: Not uploaded yet. Read status: Read on 02/01/12 02:11:43.
2012-02-01			

Chat content
View chat log in: <input type="radio"/> Plain Text <input checked="" type="radio"/> HTML [02:11:43] cypanq@hotmail.com changed the MSN status to be Idle

Contact list
4.url.com.tw 2@msn.com hotmail.com hotmail.com hotmail.com hotmail.com hotmail.com hotmail.com hotmail.com msn.com msn.com

## MSN Web Chat

yahoo ???

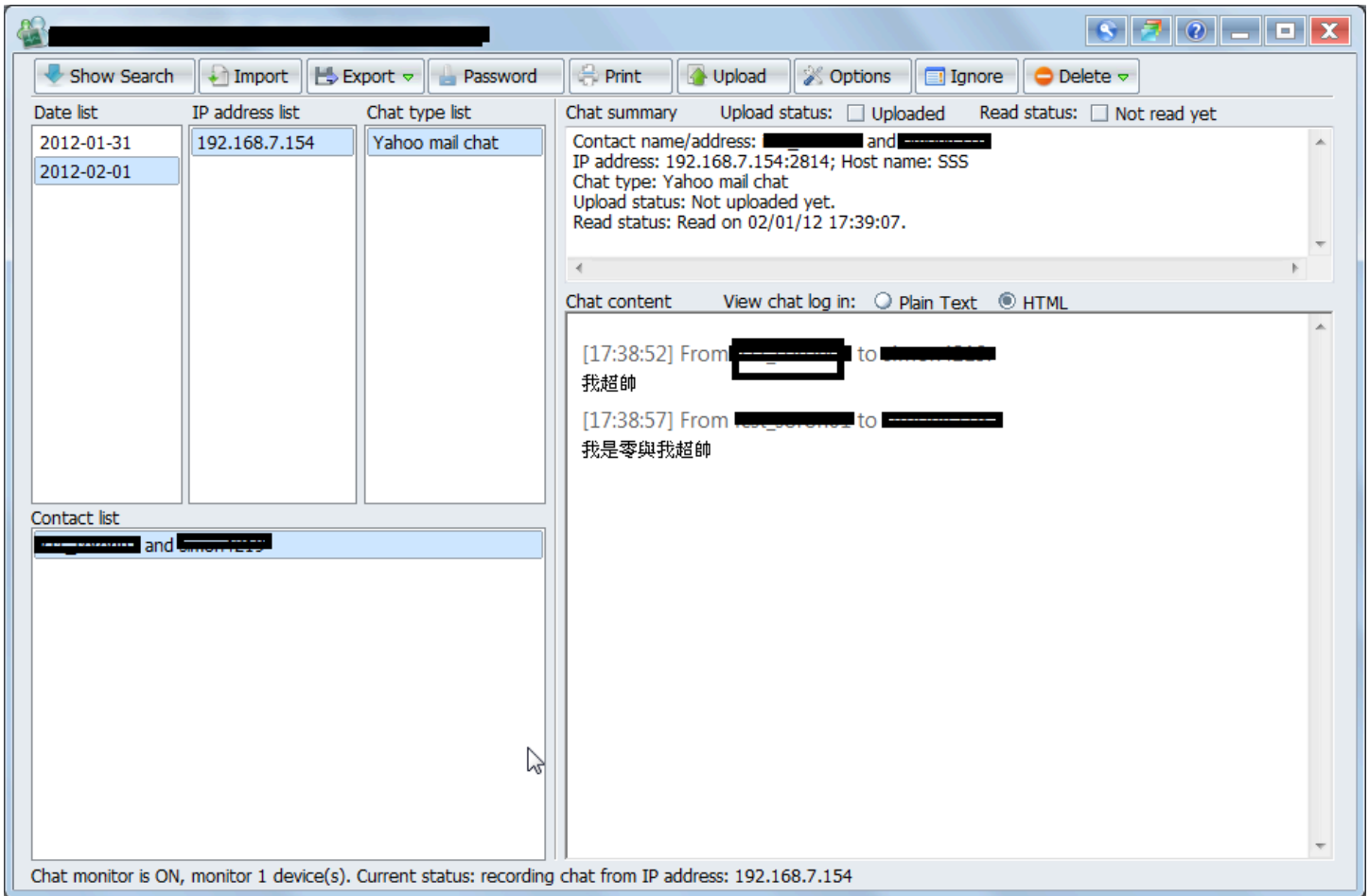
The screenshot displays a web-based chat monitoring interface. The window title is redacted. The interface includes a toolbar with buttons for Show Search, Import, Export, Password, Print, Upload, Options, Ignore, and Delete. Below the toolbar are three columns: Date list, IP address list, and Chat type list. The Date list shows 2012-01-31 and 2012-02-01. The IP address list shows 192.168.1.136, 192.168.7.154, 192.168.7.158, and 192.168.7.175. The Chat type list shows MSN online status and Yahoo chat. Below these columns is a Contact list with redacted names. The main area is divided into Chat summary and Chat content. The Chat summary shows Contact name/address (redacted), IP address: 192.168.7.154:1809; Host name: SSS, Chat type: Yahoo chat, Upload status: Not uploaded yet, and Read status: Not read yet. The Chat content shows a chat log in HTML format with the following messages:

[15:00:00] From [redacted] to [redacted]  
 hi .. have we chatted before? 23/female here...you?  
 [15:00:27] From [redacted]  
 whats wrong babe? whats the problem?  
 [15:01:11] From [redacted]  
 i'm sorry ..i get to be forgetful at times!! how're you??  
 [15:01:43] F [redacted]  
 Just got out of the shower...long day been kind of busy! but i'm feeling naughty! so what's up ..... want to have some fun? 😊

At the bottom, a status bar indicates: Chat monitor is ON, monitor 1 device(s). Current status: recording chat from IP address: 192.168.7.158, 192.168.1.136, 192.168.7.175, 192.168.7.154

Yahoo????





Facebook chat ????



???????

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

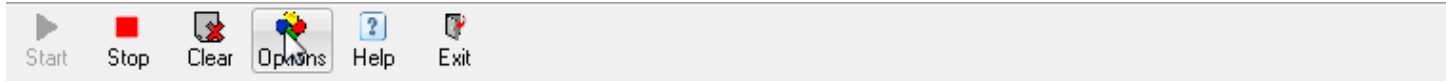
7	74.125.31.156	192.168.7.158	2739871951	5	http://googleads.g.doublecli
7	74.125.31.156	192.168.7.158	2596134854	5	http://googleads.g.doublecli
2	123.204.250.1...	192.168.7.158	thx	http://digiland.tw/login.php	
1	74.125.31.156	192.168.7.158	3998330343	5	http://digiland.tw/index.php
1	74.125.31.156	192.168.7.158	2739871951	5	http://digiland.tw/index.php

web ????

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

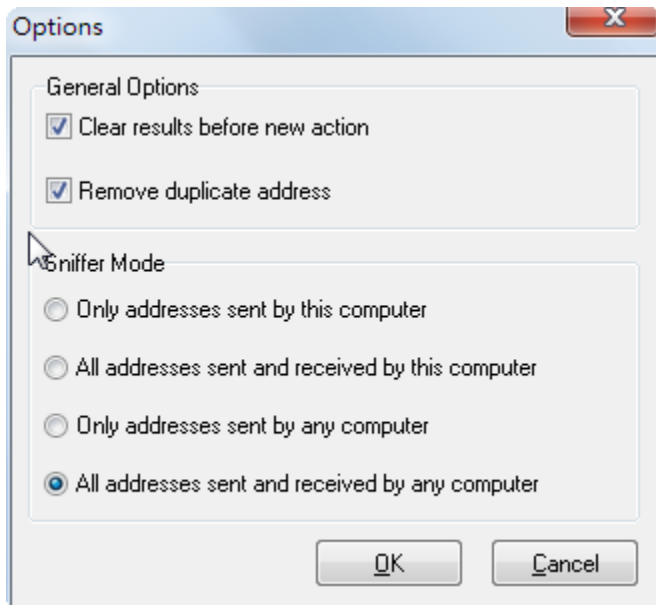
????????????????

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



??????Options

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



341	http://0-278.channel.facebook.com/pull?channel=p_100000529678456&seq=877&clientid=60181789&cb=m0k&pid=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=35b&id=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=60181789&cb=4ppf&id=52&...	192.168.7.151	69.171.227.43	51733	80
345	http://comet31.plurk.com/comet/1328013504725/?js_callback=CometChannel.scripCallback&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=0ad&id=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=60181789&cb=a5zh&id=596&...	192.168.7.151	69.171.227.43	51733	80
348	http://0-278.channel.facebook.com/pull?channel=p_100000529678456&seq=880&clientid=60181789&cb=bobv&id=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&id=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&id=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=60181789&cb=lg2&id=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=90ds&id=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=x13&id=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=60181789&cb=4od3&id=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

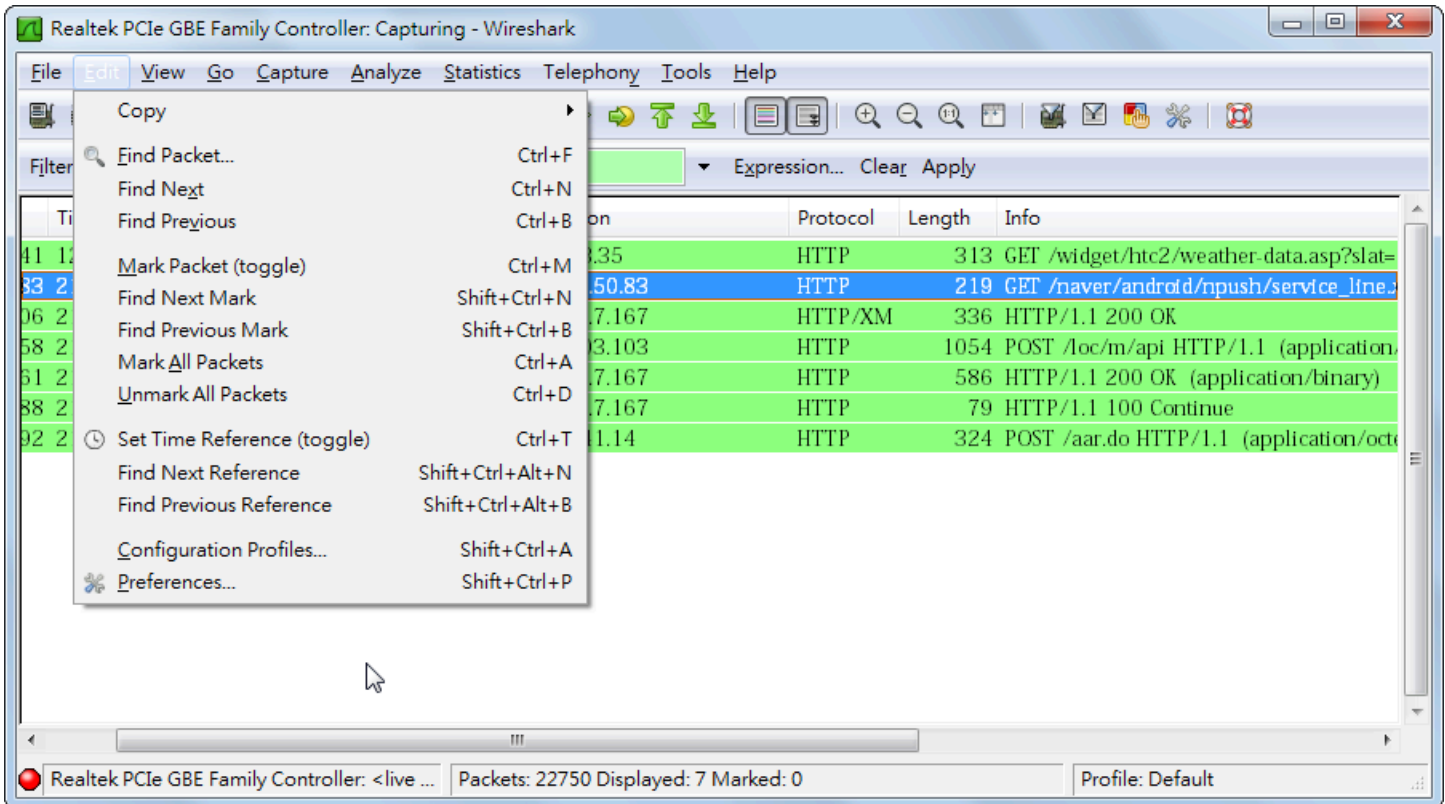
????UTF8???wireshark

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

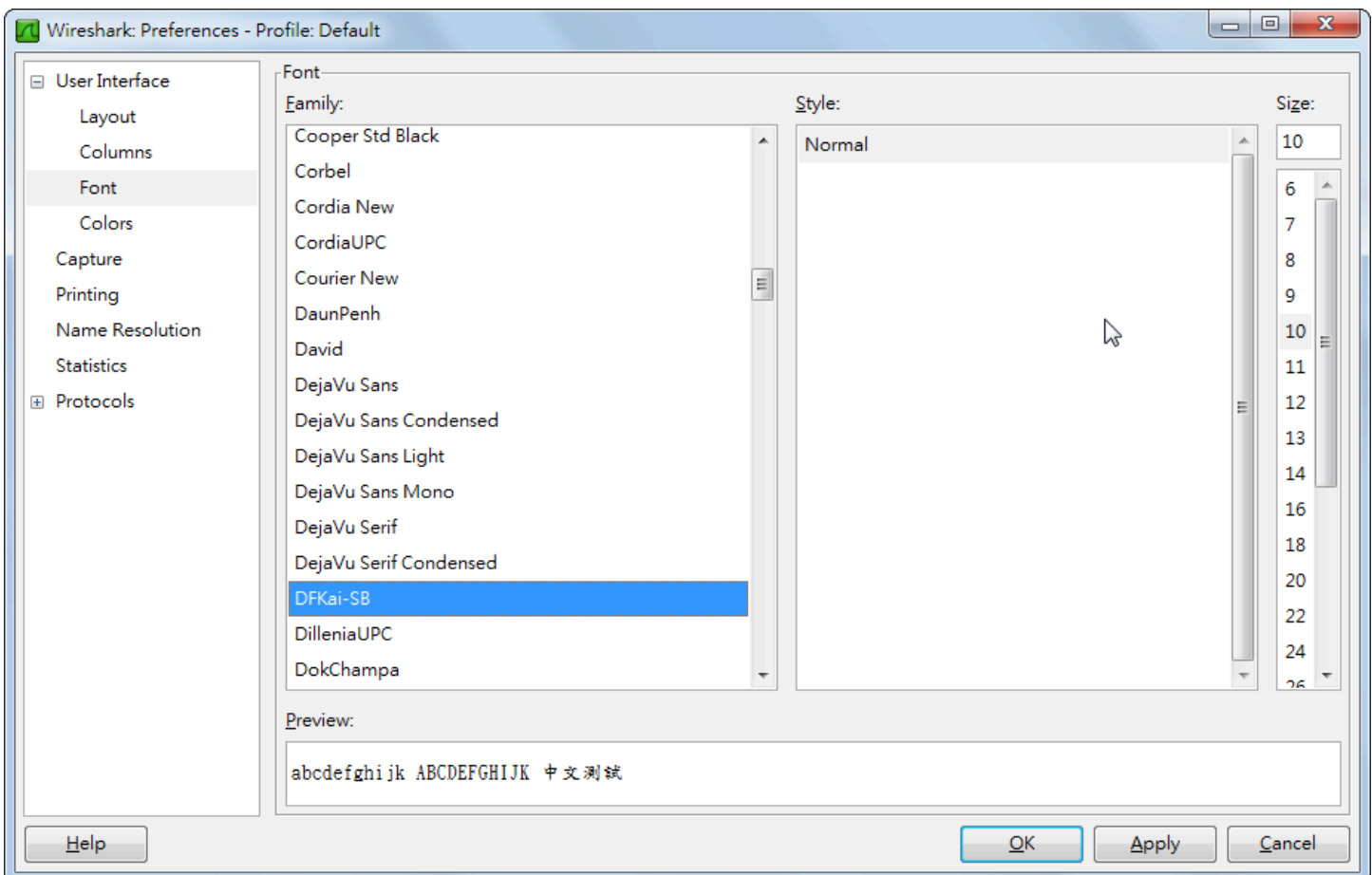
????????????????????????????????????

??????

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



?????



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

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

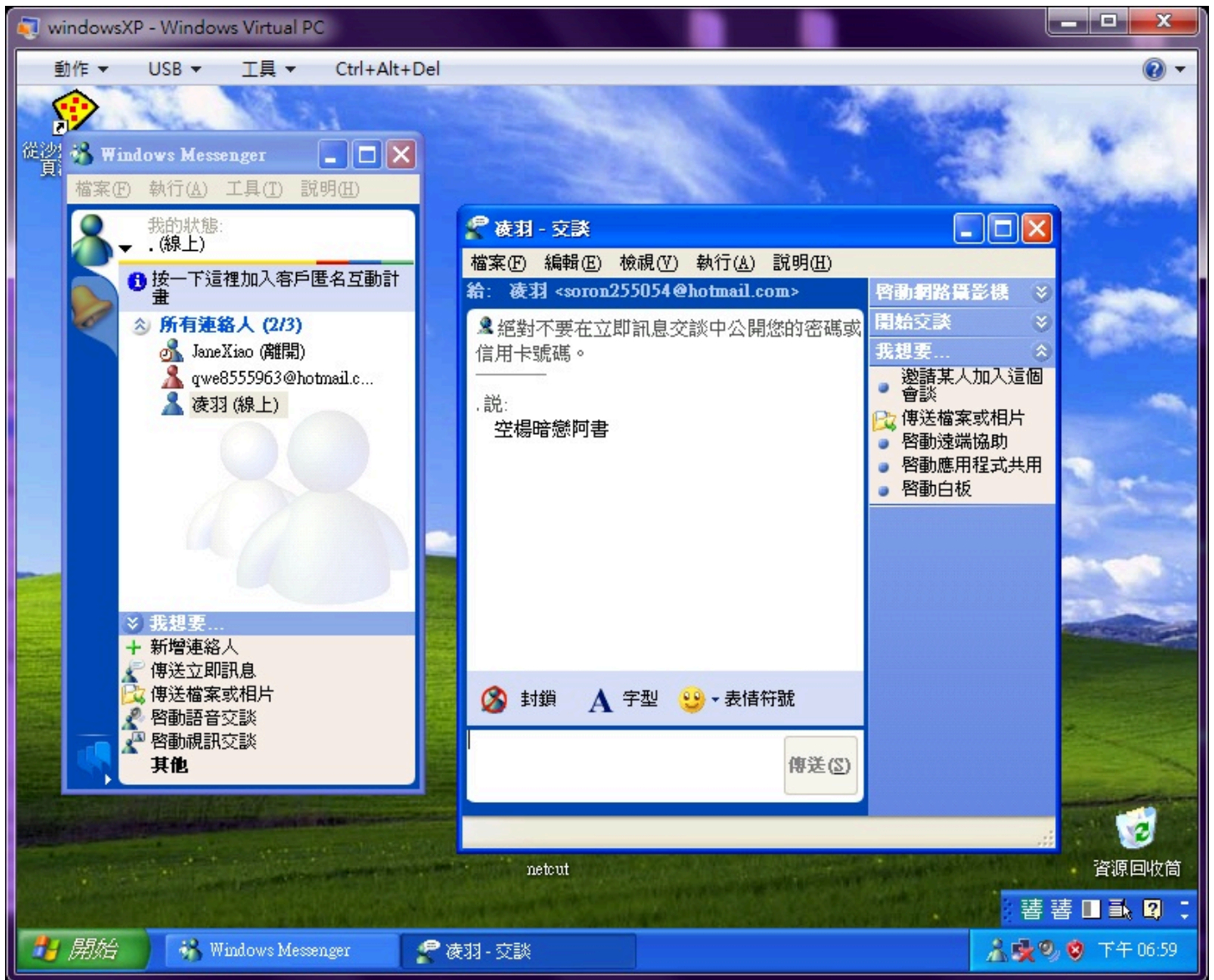
The image shows a Wireshark capture window titled "(Untitled) - Wireshark". The filter bar contains "msnms". The packet list pane shows a list of 96 packets, all of which are MSNMS. The selected packet (No. 597) is highlighted in blue. The packet details pane shows the following structure:

```

0070  0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74  .Content-Type: t
0080  65 78 74 2f 70 6c 61 69 6e 3b 20 63 68 61 72 73  ext/plai n; chars
0090  65 74 3d 55 54 46 2d 38 0d 0a 58 2d 4d 4d 53 2d  et=UTF-8 ..X-MMS-
  
```

The status bar at the bottom indicates: Text item (text), 3 bytes; Packets: 606 Displayed: 96 Marked: 0 Dropped: 0; Profile: Default.

No.	Time	Source	Destination	Protocol	Info
523	241.901103	65.54.49.53	192.168.11.3	MSNMS	MSG 91 U 96
527	249.526990	192.168.11.3	65.54.50.159	MSNMS	MSG 94 U 96
528	249.747615	65.54.50.159	192.168.11.4	MSNMS	MSG soron255054@t
534	251.011127	65.54.189.213	192.168.11.3	MSNMS	MSG group186955@m
545	254.539873	192.168.11.3	65.54.50.159	MSNMS	MSG 95 U 96
546	254.746579	65.54.50.159	192.168.11.4	MSNMS	MSG soron255054@t
552	256.693669	207.46.124.77	192.168.11.3	MSNMS	MSG group588661@m
554	257.784277	192.168.11.3	65.54.50.159	MSNMS	MSG 96 N 268
555	258.000168	65.54.50.159	192.168.11.4	MSNMS	MSG soron255054@t
561	259.867722	65.54.49.53	192.168.11.3	MSNMS	NLN NLN 1:amber75
574	272.321749	65.54.49.53	192.168.11.3	MSNMS	UBX 1:ormazd49804
577	272.619020	65.54.49.53	192.168.11.3	MSNMS	UBX 1:ormazd49804
580	275.865628	64.4.16.53	192.168.11.3	MSNMS	MSG xiaoi580@hotm
582	276.629008	192.168.11.3	65.54.50.159	MSNMS	MSG 97 U 96
583	276.904851	65.54.50.159	192.168.11.4	MSNMS	MSG soron255054@t
596	278.303954	192.168.11.3	65.54.50.159	MSNMS	MSG 98 N 162
597	278.549753	65.54.50.159	192.168.11.4	MSNMS	MSG soron255054@t



Filter: msnms

No.	Time	Source	Destination	Protocol	Info
11	3.179616	192.168.11.4	65.54.48.116	MSNMS	MSG 30 U 97
12	3.180265	192.168.11.4	65.54.48.116	MSNMS	[TCP Out-Of-Order] MSG 30 U 97
13	3.180424	192.168.11.4	65.54.48.116	MSNMS	[TCP Out-Of-Order] MSG 30 U 97
15	3.380034	65.54.48.116	192.168.11.3	MSNMS	MSG hacker255054@hotmail.com . 97
17	5.008635	192.168.11.4	65.54.48.116	MSNMS	MSG 31 U 97
18	5.009349	192.168.11.4	65.54.48.116	MSNMS	[TCP Out-Of-Order] MSG 31 U 97
19	5.009804	192.168.11.4	65.54.48.116	MSNMS	[TCP Out-Of-Order] MSG 31 U 97
21	5.218876	192.168.11.4	65.54.48.116	MSNMS	MSG 32 N 161
22	5.219108	65.54.48.116	192.168.11.3	MSNMS	MSG hacker255054@hotmail.com . 97
23	5.219397	192.168.11.4	65.54.48.116	MSNMS	[TCP Out-Of-Order] MSG 32 N 161
24	5.219524	192.168.11.4	65.54.48.116	MSNMS	[TCP Out-Of-Order] MSG 32 N 161
26	5.408227	65.54.48.116	192.168.11.3	MSNMS	MSG hacker255054@hotmail.com . 161
29	7.744673	64.4.16.53	192.168.11.3	MSNMS	MSG xiaoi580@hotmail.com 空楊暗戀阿書

Frame 21 (229 bytes on wire, 229 bytes captured)

- Ethernet II, Src: Microsoft\_00:07:d2 (00:03:ff:00:87:d2), Dst: AsustekC\_2e:dc:88 (00:26:18:2e:dc:88)
- Internet Protocol, Src: 192.168.11.4 (192.168.11.4), Dst: 65.54.48.116 (65.54.48.116)
- Transmission Control Protocol, Src Port: fuscrypt (1144), Dst Port: msnp (1863), Seq: 221, Ack: 1, Len: 175
- MSN Messenger Service
  - MSG 32 N 161\r\n\r\n
  - MIME-Version: 1.0\r\n\r\n
  - Content-Type: text/plain; charset=UTF-8\r\n\r\n
  - X-MMS-IM-Format: FN=%E6%96%B0%E7%BB%96%E6%96%B0%E6%96%B0%E6%96%B0%E6%96%B0%E6%96%B0; EF=: C0=0; CS=1; PF=0\r\n\r\n\r\n
  - 空楊暗戀阿書

0000 00 26 18 2e dc 88 00 03 ff 00 87 d2 08 00 45 00 .&.....E.  
 0010 00 d7 08 7f 40 00 80 06 b4 4b c0 a8 0b 04 41 36 ....@...K...A6  
 0020 30 74 04 78 07 47 cd 0f d0 26 b2 1b 16 28 50 18 0t.x.G...&...P.  
 0030 ff 9b 59 f8 00 00 4d 53 47 20 33 32 20 4e 20 31 ..Y...MS G 32 N 1  
 0040 36 31 0d 0a 4d 49 4d 45 2d 56 65 72 73 69 6f 6e 6l..MIME -Version  
 0050 3a 20 31 2e 30 0d 0a 43 6f 6e 74 65 6e 74 2d 54 : 1.0..Content-T  
 0060 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 3b yper: tex t/plain:  
 0070 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 0d 0a charset =UTF-8..  
 0080 58 2d 4d 4d 53 2d 49 4d 2d 46 6f 72 6d 61 74 3a X-MMS-IM -Format:  
 0090 20 46 4e 3d 25 45 36 25 39 36 25 42 30 25 45 37 FN=%E6% 96%B0%E7  
 00a0 2f 3a 20 74 65 78 74 2f 70 6c 61 69 6e 3b 61 69 6e 3b

File: "C:\Users\oron\AppData\Local\Temp... | Packets: 31 Displayed: 13 Marked: 0 Dropped: 0 Profile: Default

??????http??

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

Filter: ip.addr == 192.168.7.167 and http

Time	Source	Destination	Protocol	Length	Info
41	129.427160	192.168.7.167	HTTP	313	GET /widget/htc2/weather-data.asp?slat=
33	218.568761	192.168.7.167	HTTP	219	GET /naver/android/npush/service_lfne...
06	218.973168	221.139.50.83	HTTP/XML	336	HTTP/1.1 200 OK
58	219.599124	192.168.7.167	HTTP	1054	POST /loc/m/api HTTP/1.1 (application/...
61	219.622726	72.14.203.103	HTTP	586	HTTP/1.1 200 OK (application/binary)
88	219.928416	216.74.41.14	HTTP	79	HTTP/1.1 100 Continue
92	219.934134	192.168.7.167	HTTP	324	POST /aar.do HTTP/1.1 (application/octe...

Realtek PCIe GBE Family Controller: <live ... | Packets: 2016 Displayed: 7 Marked: 0 Profile: Default