

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

??????????

??

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

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

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

??Hub ????

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 )?

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

Wireshark  
<http://blog.shaolin.tw/2008/03/wireshark.html>  
 ???UTF8???wireshark

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

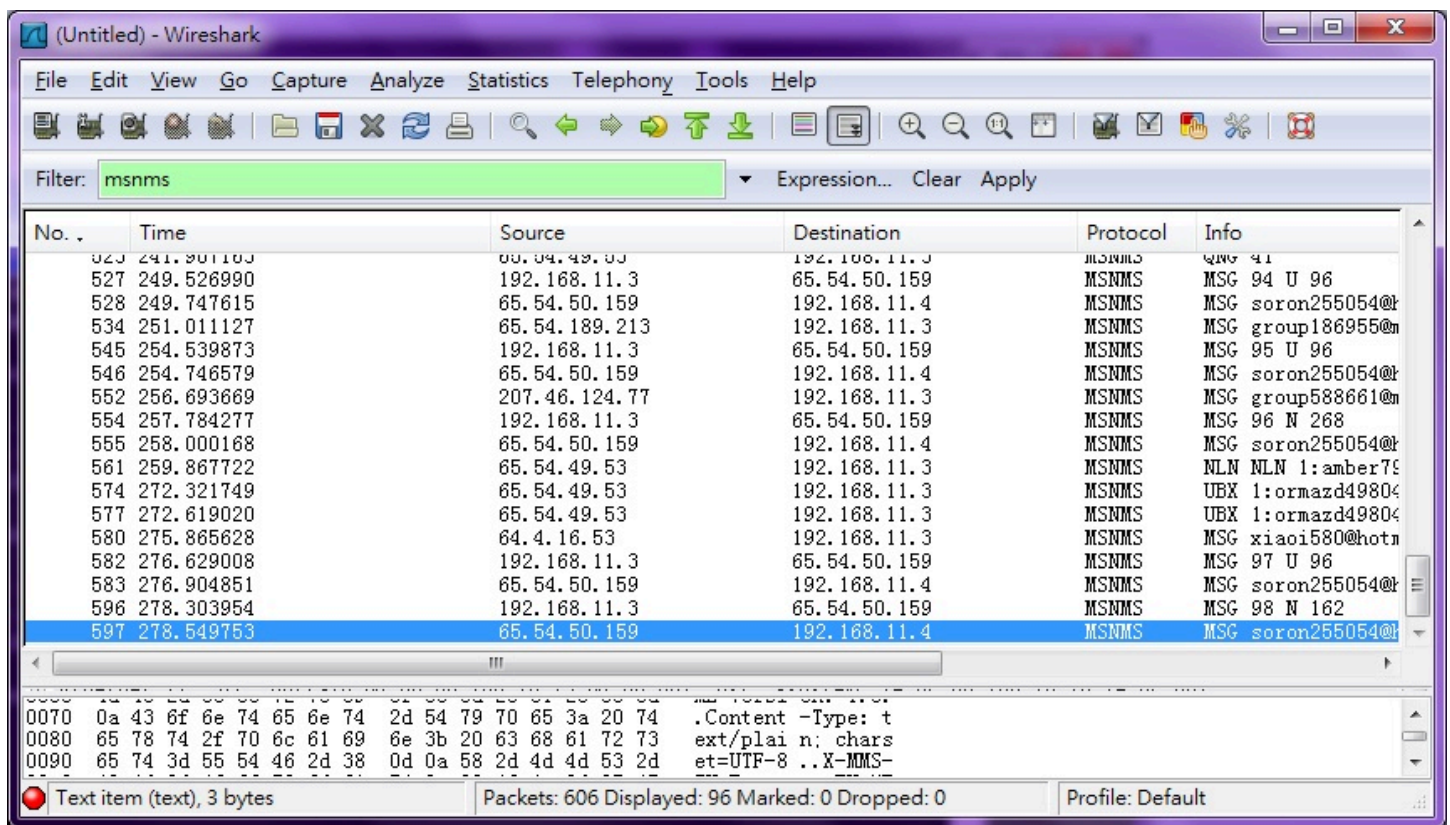
????????????????????????????????????

??????

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

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

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





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
17	5.008635	192.168.11.4	65.54.48.116	MSNMS	MSG hacker255054@hotmail.com . 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 i° iaz*ã° 59

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

- Ethernet II, Src: Microsoft\_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
  - MIME-Version: 1.0\r\n
  - Content-Type: text/plain; charset=UTF-8\r\n
  - X-MMS-IM-Format: FN=KE6X96XB0XE7KB4XB0XE6X96X8EWE9KADW94; EF=: C0=0; CS=1; PF=0\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=KE6X 96XB0XE7  
 00a0 2f 20 31 2e 30 0d 0a 43 6f 6e 74 65 6e 74 2d 54

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

Filter: msnms

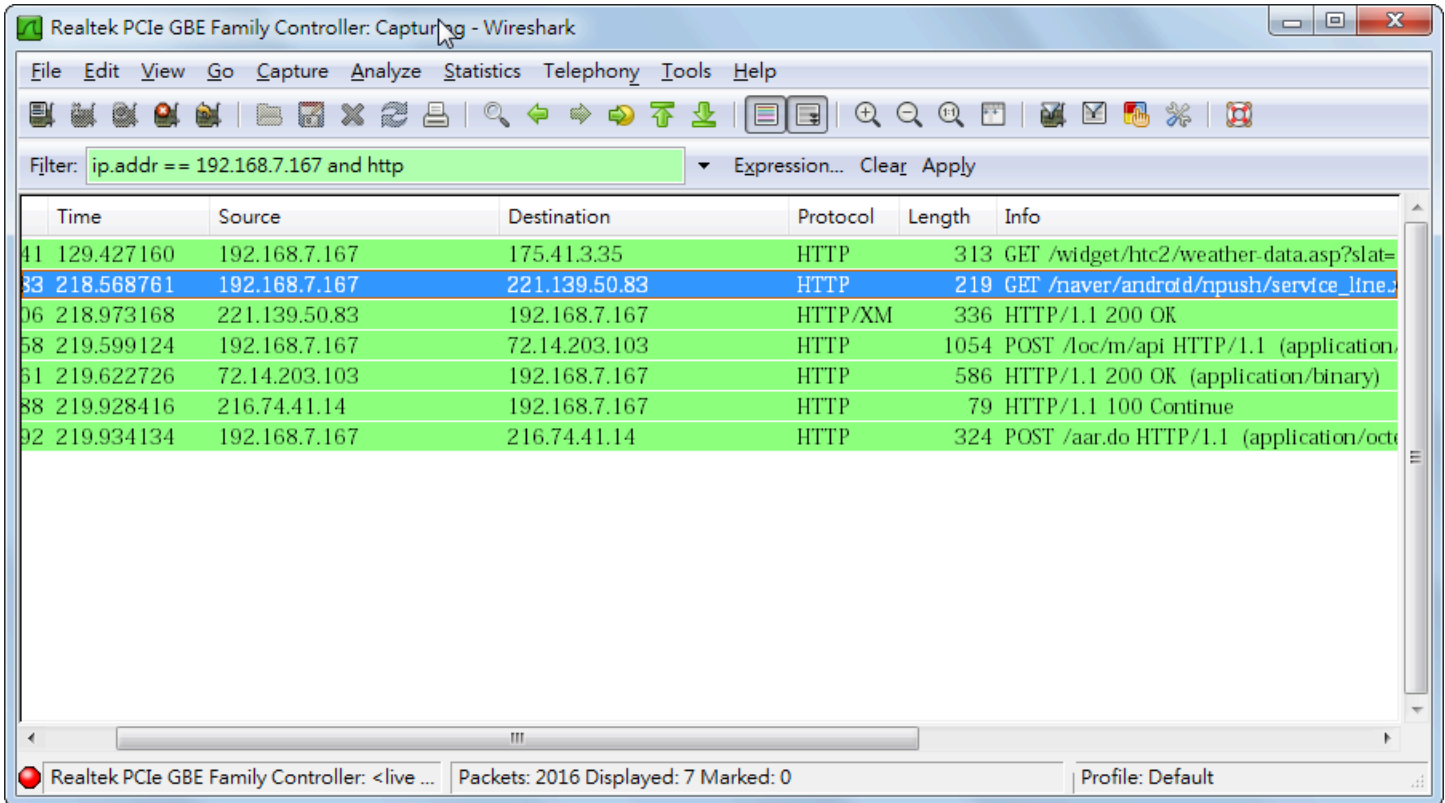
No.	Time	Source	Destination	Protocol	Info
523	241.901103	65.54.48.116	192.168.11.3	MSNMS	MSG 91
527	249.526990	192.168.11.3	65.54.50.159	MSNMS	MSG 94 U 96
528	249.747615	65.54.50.159	192.168.11.4	MSNMS	MSG soron255054@t
534	251.011127	65.54.189.213	192.168.11.3	MSNMS	MSG group186955@n
545	254.539873	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@n
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:amber7f
574	272.321749	65.54.49.53	192.168.11.3	MSNMS	UBX 1:ormazd4980f
577	272.619020	65.54.49.53	192.168.11.3	MSNMS	UBX 1:ormazd4980f
580	275.865628	64.4.16.53	192.168.11.3	MSNMS	MSG xiaoi580@hotn
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

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-

Text item (text), 3 bytes | Packets: 606 Displayed: 96 Marked: 0 Dropped: 0 Profile: Default

???????http??

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



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

### CAIN

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

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

### FreeHttpsniiff

[http://www.cleansersoft.com/sniffer/f...tp\\_sniffer.htm](http://www.cleansersoft.com/sniffer/f...tp_sniffer.htm)

??

### MSN ??

????????????MSN?????yahoo?????Facebook web chat , ??????????????

### websitesniffer

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

### Winpcap

<http://www.winpcap.org/>







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

Date list	IP address list	Chat type list
2012-01-31	192.168.1.136	MSN online status
2012-02-01	192.168.7.154	Yahoo chat
	192.168.7.158	
	192.168.7.175	

Contact list

- [redacted] and [redacted]
- [redacted] and [redacted]

Chat summary

Upload status:  Uploaded    Read status:  Not read yet

Contact name/address: [redacted]  
IP address: 192.168.7.154:1809; Host name: SSS  
Chat type: Yahoo chat  
Upload status: Not uploaded yet.  
Read status: Not read yet.

Chat content    View chat log in:  Plain Text     HTML

[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? 😊

Yahoo????



The screenshot shows a software interface for monitoring network traffic. At the top, there is a menu bar with icons for Show Search, Import, Export, Password, Print, Upload, Options, Ignore, and Delete. Below the menu bar are three columns: 'Date list' with entries for 2012-01-31 and 2012-02-01; 'IP address list' with the entry 192.168.7.154; and 'Chat type list' with the entry 'Yahoo mail chat'. To the right of these columns is a 'Chat summary' section containing the following text: 'Contact name/address: [redacted] and [redacted]', 'IP address: 192.168.7.154:2814; Host name: SSS', 'Chat type: Yahoo mail chat', 'Upload status: Not uploaded yet.', and 'Read status: Read on 02/01/12 17:39:07.'. Below the summary is a 'Chat content' section with a radio button menu for 'View chat log in: Plain Text' and 'HTML'. The chat content shows two messages: '[17:38:52] From [redacted] to [redacted]' with the text '我超帥', and '[17:38:57] From [redacted] to [redacted]' with the text '我是零與我超帥'. At the bottom left, a 'Contact list' shows a single entry: '[redacted] and [redacted]'. A status bar at the bottom of the window reads: 'Chat monitor is ON, monitor 1 device(s). Current status: recording chat from IP address: 192.168.7.154'.

Facebook chat ????

Chat type list

- Facebook chat
- Facebook message
- MSN chat
- MSN online status

Chat summary    Upload status:  Uploaded    Read status:  Not read yet

Contact name/address: Thread Id id.342461865774221  
 IP address: 192.168.7.151:50241; Host name: [REDACTED]  
 Chat type: Facebook chat  
 Upload status: Not uploaded yet.  
 Read status: Read on 01/31/12 18:49:24.

Chat content    View chat log in:  Plain Text     HTML

[18:14:36] From Dao Hung Chang(100000529678456) to [REDACTED] (500301458):  
 hihhi

[18:14:54] From Dao Hung Chang(100000529678456) to [REDACTED] (500301458):  
 測試一下

[18:15:07] From [REDACTED] (500301458) to Dao Hung Chang (100000529678456):  
 Test TEst

[18:15:24] From Allen Chen(500301458) to Dao Hung Chang (100000529678456):  
 有嗎? XD

[18:15:24] From Allen Chen(500301458) to Dao Hung Chang (100000529678456):  
 有嗎? XD

Facebook ?????

ICQ ????

AOL????

AIM ????

Ebubby

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

Telnet ??



[???? 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 ???? ??????????