# Lab Hours

- We need to allocate 3 hours in this week for hands-on lab hours (November 10th  09:00-12:00).
- The instructor will set up the SIP server.
- Every student will bring a labtop or desktop PC and install a SIP UA (softphone).
- Packet analyzer will be utilized to capture and analyze the SIP messages.

# SIP UAs
# and
# SIP Message Analysis

Quincy Wu

National Chi Nan University

Email: solomon@ipv6.club.tw

# Exercise 1: SIP UA operations

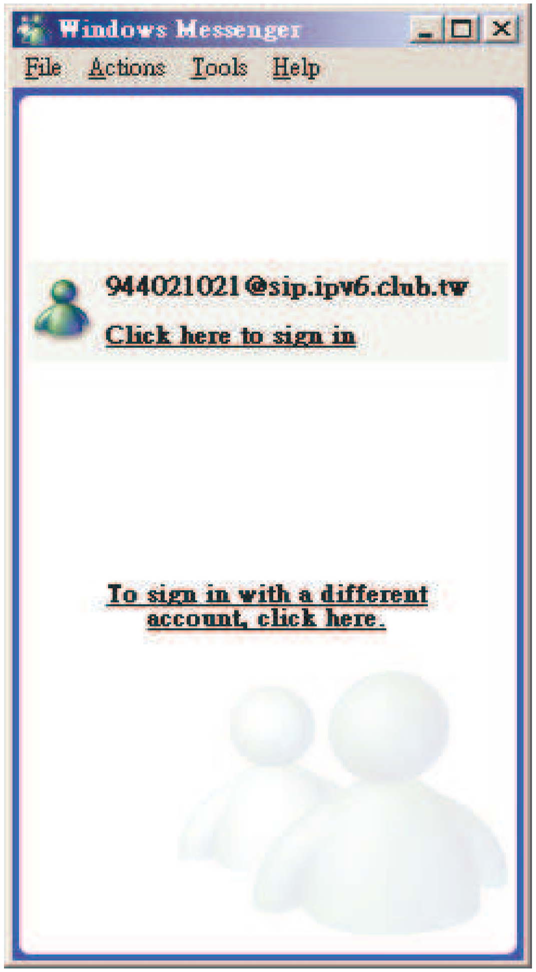
- Download & Install SIP UA
- Download & Install Ethereal
- Packet Analysis Using Ethereal
  - SIP signaling flow
  - RTP traffic
  - SIP headers
  - SDP Contents
  - Call Hold/Retrieve

# Windows-based SIP UA

- Microsoft Windows Messenger
- NBEN UA
- X-Lite

# SIP UA – Windows Messenger

- By default, Windows XP installs Windows Messenger Version 4.7
- There are two messengers from Microsoft
  - MSN Messenger 6.2, 7.0
  - Windows Messenger 4.7, 5.1
- Inside Windows Messenger - How it Communicates
  - http://www.microsoft.com/technet/prodtechnol/winxppro/evaluate/insid01.mspx

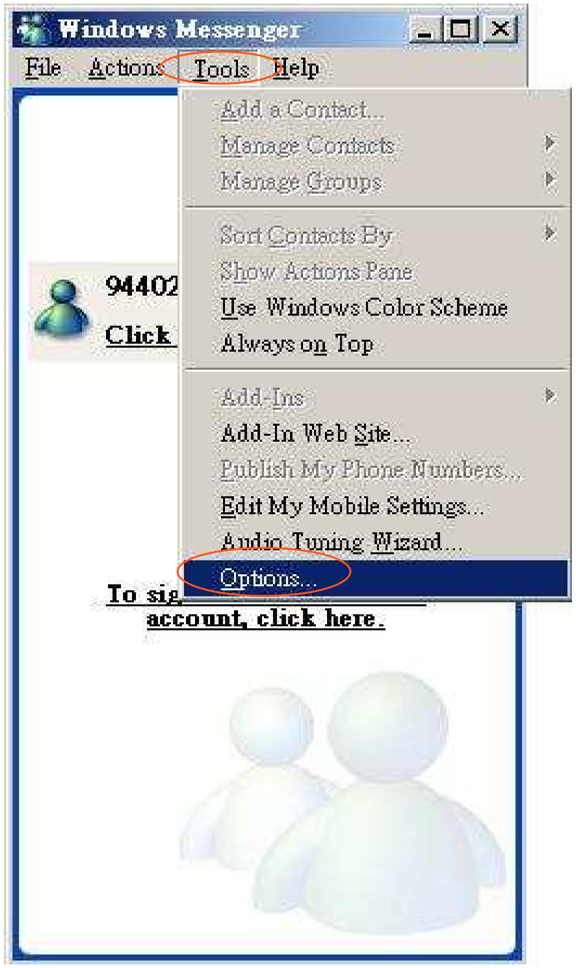


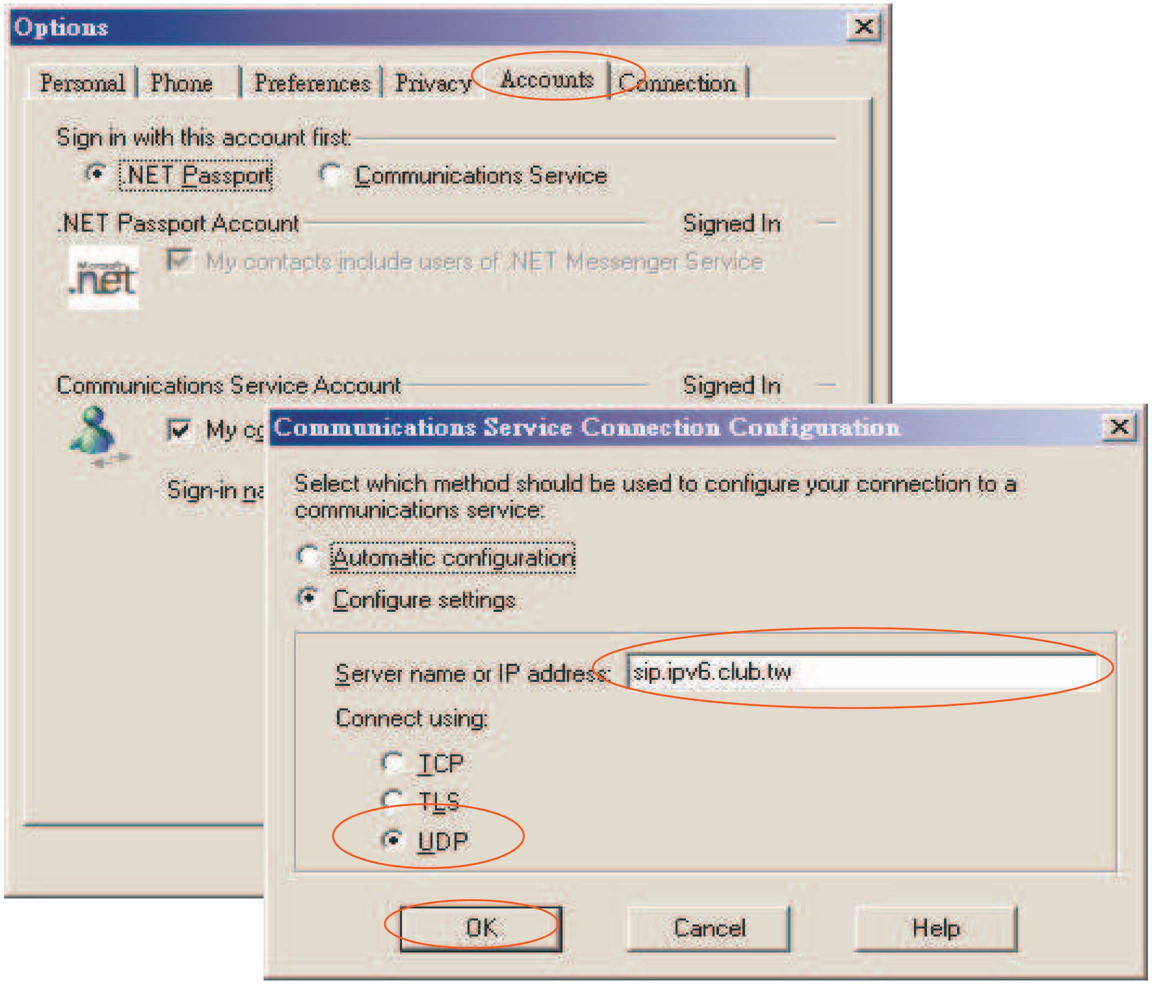
944021021@sip.ipv6.club.tw

Click here to sign in

To sign in with a different account, click here.

# Step 1: Configure





Sign in with this account first:
● .NET Passport ○ Communications Service

.NET Passport Account Signed In
☑ My contacts include users of .NET Messenger Service

Communications Service Account Signed In
☑ My co

Sign-in na

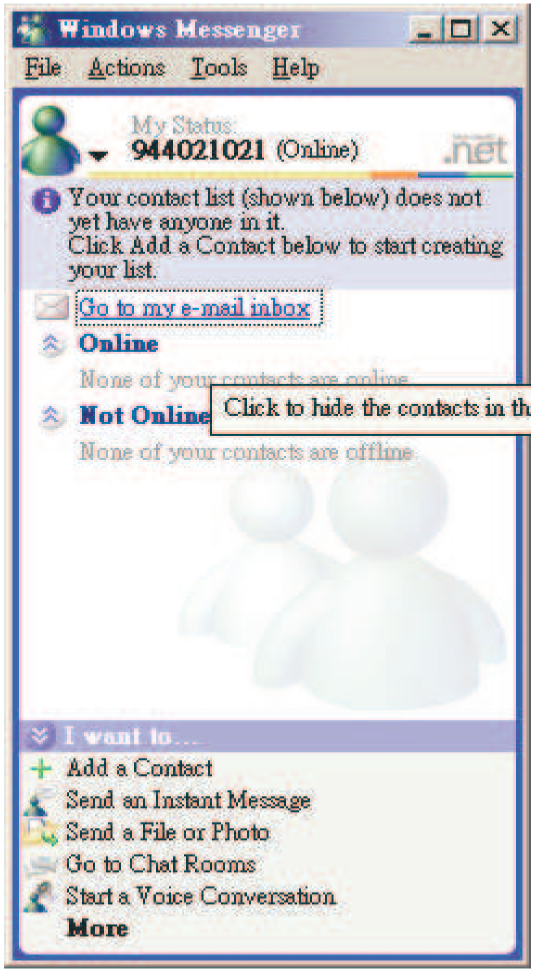
Select which method should be used to configure your connection to a communications service:

○ Automatic configuration
● Configure settings

Server name or IP address: sip.ipv6.club.tw

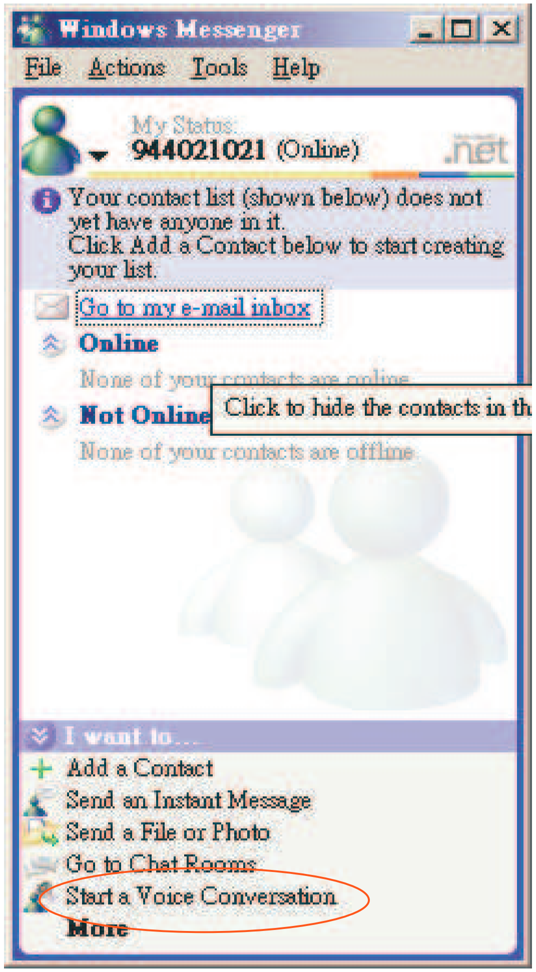
Connect using:
○ TCP
○ TLS
● UDP

# Step 2: REGISTER



Your contact list (shown below) does not yet have anyone in it.
Click Add a Contact below to start creating your list.

# Step 3: Make A Call



My Status: 944021021 (Online)

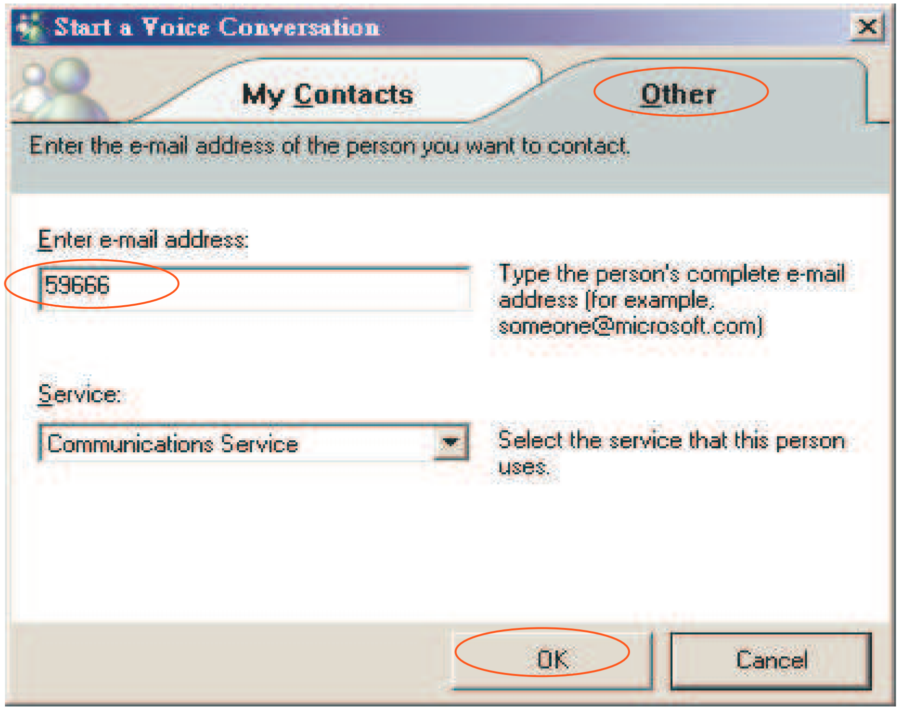
Your contact list (shown below) does not yet have anyone in it.
Click Add a Contact below to start creating your list.

Go to my e-mail inbox

None of your contacts are online

Click to hide the contacts in th

None of your contacts are offline



Enter the e-mail address of the person you want to contact.

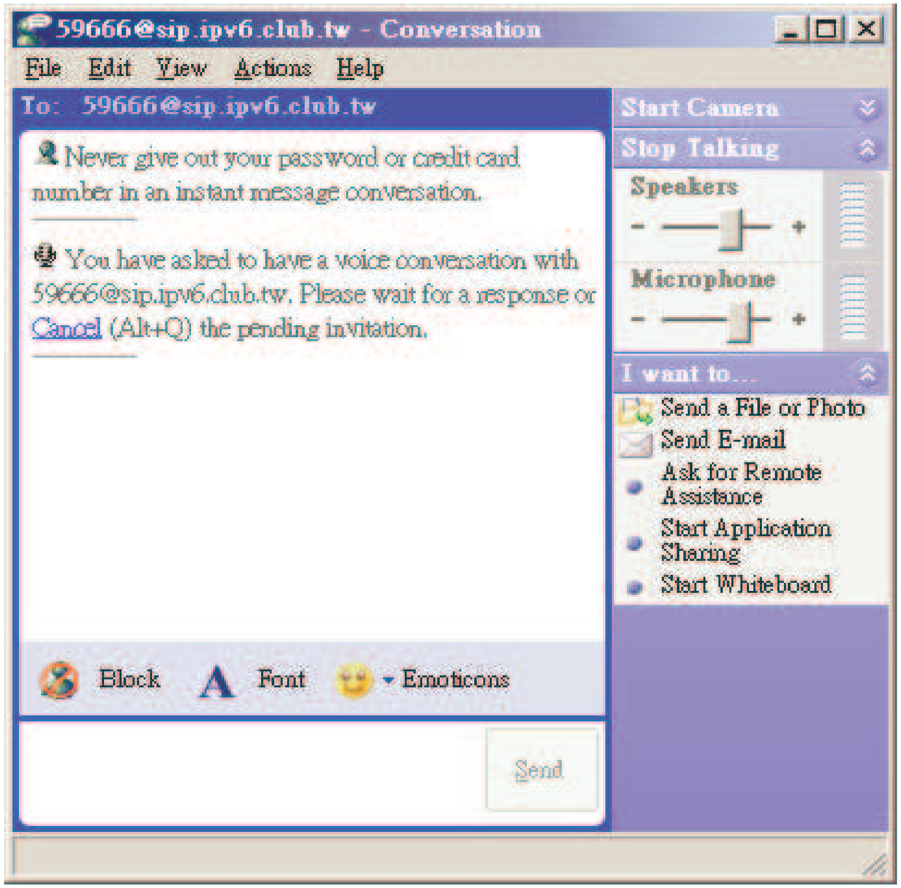
Enter e-mail address: 59666

Type the person's complete e-mail address (for example, someone@microsoft.com)

Service: Communications Service

Select the service that this person uses.

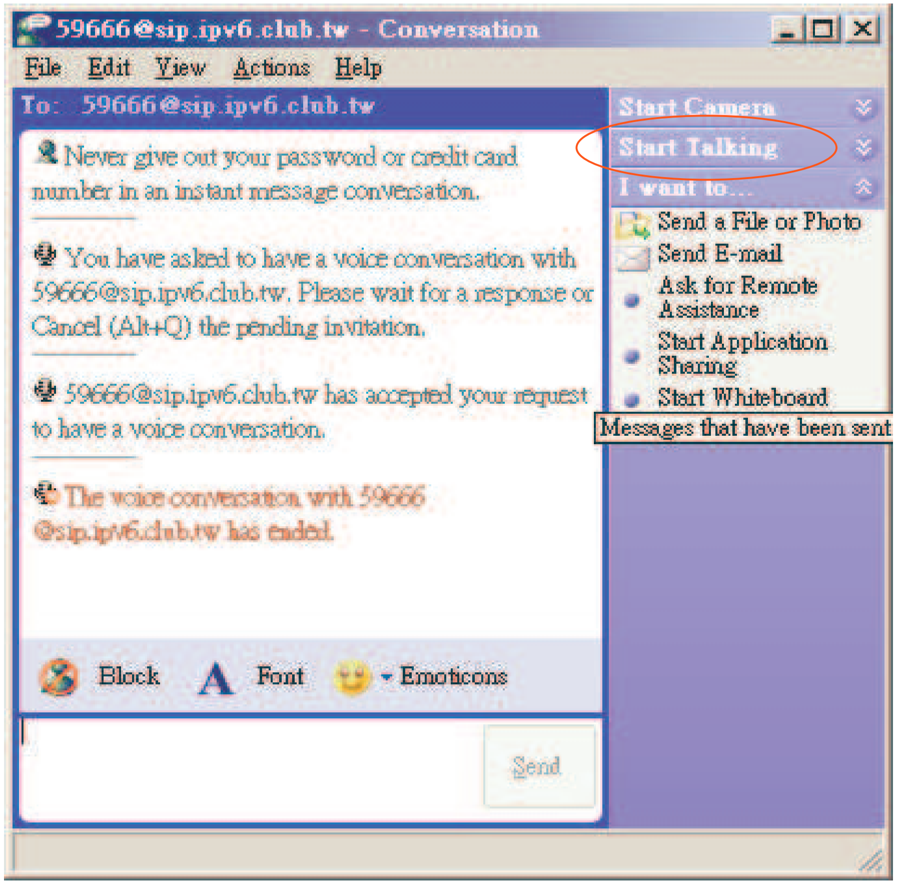
# Step 4: Ringing


59666@sip.ipv6.club.tw - Conversation
File Edit View Actions Help
To: 59666@sip.ipv6.club.tw
Start Camera
Stop Talking
Speakers
Microphone
I want to...
Send a File or Photo
Send E-mail
Ask for Remote Assistance
Start Application Sharing
Start Whiteboard
Block
Font
Emoticons
Send

Never give out your password or credit card number in an instant message conversation.

You have asked to have a voice conversation with 59666@sip.ipv6.club.tw. Please wait for a response or Cancel (Alt+Q) the pending invitation.

# Step 5: Conversation


59666@sip.ipv6.club.tw - Conversation
File Edit View Actions Help
To: 59666@sip.ipv6.club.tw
Start Camera
Start Talking
I want to...
Send a File or Photo
Send E-mail
Ask for Remote Assistance
Start Application Sharing
Start Whiteboard
Messages that have been sent
Block
Font
Emoticons
Send

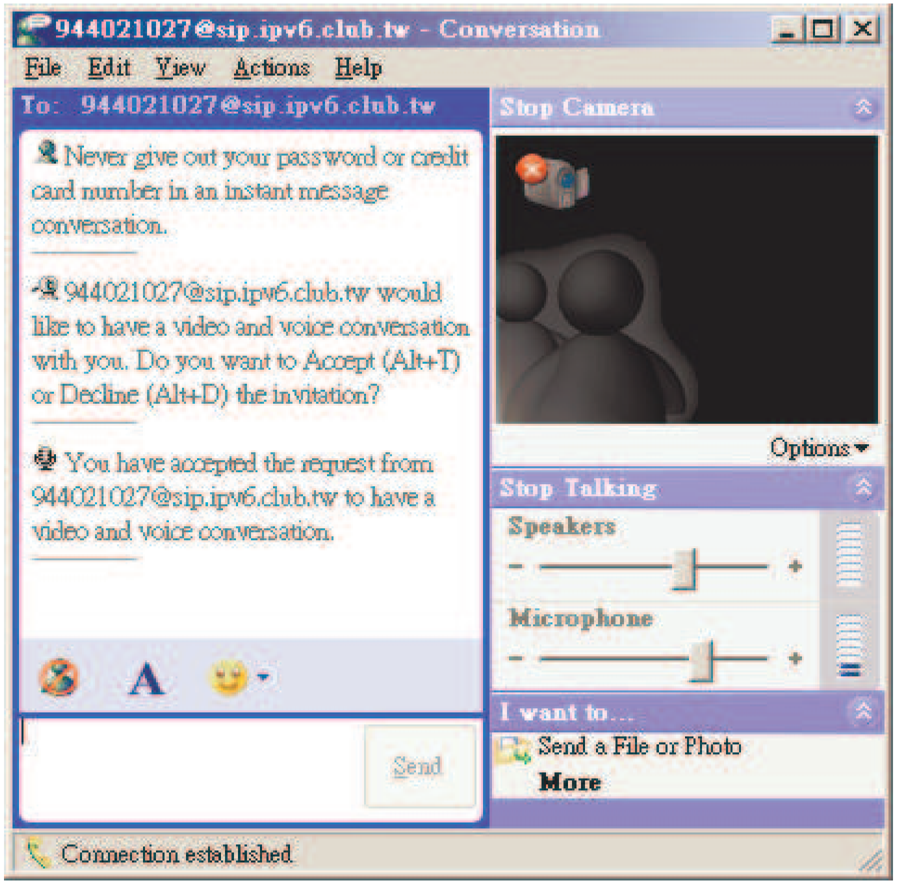
Never give out your password or credit card number in an instant message conversation.

You have asked to have a voice conversation with 59666@sip.ipv6.club.tw. Please wait for a response or Cancel (Alt+Q) the pending invitation.

59666@sip.ipv6.club.tw has accepted your request to have a voice conversation.

The voice conversation with 59666 @sip.ipv6.club.tw has ended.

# Step 6: Answer A Call


944021027@sip.ipv6.club.tw - Conversation
File Edit View Actions Help
To: 944021027@sip.ipv6.club.tw
Stop Camera
Options
Stop Talking
Speakers
Microphone
I want to...
Send a File or Photo
More
Send

Never give out your password or credit card number in an instant message conversation.

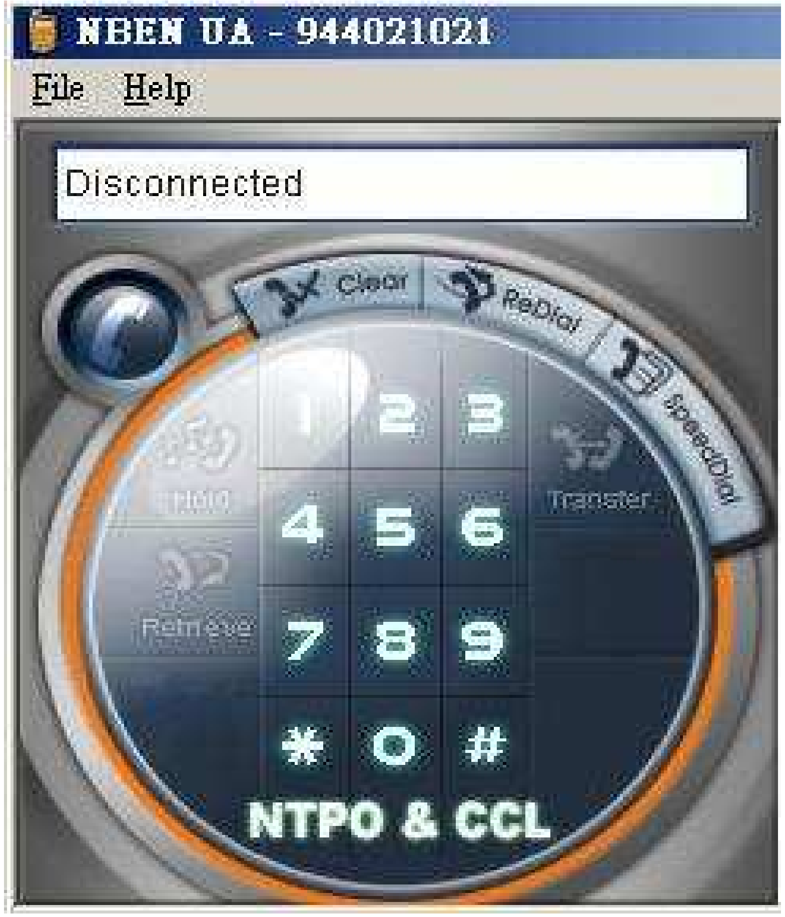
944021027@sip.ipv6.club.tw would like to have a video and voice conversation with you. Do you want to Accept (Alt+T) or Decline (Alt+D) the invitation?

You have accepted the request from 944021027@sip.ipv6.club.tw to have a video and voice conversation.

Connection established

# SIP UA – NBEN UA

- NBEN UA is a SIP User Agent which provides easy interface for IP telephony.
- This software was developed as a tool for VoIP tutorials in Taiwan.
- You can type the digits and make phone calls directly, without typing the complete SIP URI (sip:0944021021@sip.ipv6.club.tw:5060)
- It supports features like Hold/Retrieve, Redial, Speed Dial, Transfer.



NBEN UA - 944021021

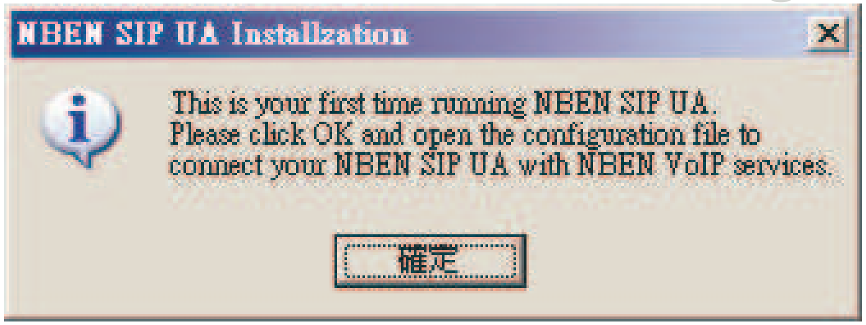
Disconnected

# Features

- NBEN UA runs on Windows 2000/XP/2003.
- Both signaling and media data are transported on UDP.
  - SIP: port 5060
  - RTP: port 9000
- Supported audio codec:
  - G.711 (64Kbps)
  - G.729 (8Kbps)
  - G.723.1 (6.3Kbps)

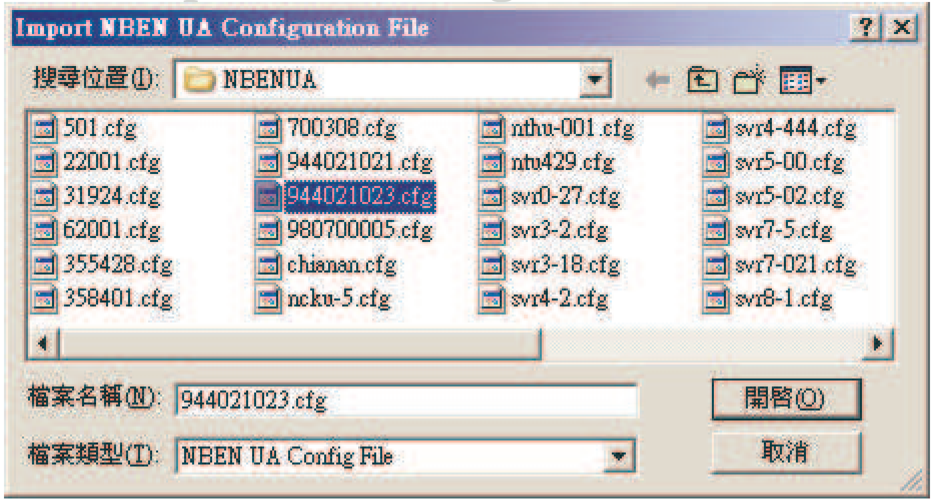
# Download NBEN SIP UA

- Download link & Installation guide can be found at http://voip.ipv6.club.tw/Download/
- Phone numbers are assigned in a separate configuration file.



NBEN SIP UA Installzation

This is your first time running NBEN SIP UA.
Please click OK and open the configuration file to connect your NBEN SIP UA with NBEN VoIP services.



Import NBEN UA Configuration File

搜尋位置(I): NBENUA

501.cfg
22001.cfg
31924.cfg
62001.cfg
355428.cfg
358401.cfg
700308.cfg
944021021.cfg
944021023.cfg
980700005.cfg
chianan.cfg
ncku-5.cfg
nthu-001.cfg
ntu429.cfg
svr0-27.cfg
svr3-2.cfg
svr3-18.cfg
svr4-2.cfg
svr4-444.cfg
svr5-00.cfg
svr5-02.cfg
svr7-5.cfg
svr7-021.cfg
svr8-1.cfg

檔案名稱(N): 944021023.cfg
檔案類型(T): NBEN UA Config File

- Try to call each other and see the signaling of SIP.
- Each SIP UA is required to possess a public IP address.
  - A patch is available to traverse NAT by utilizing STUN.

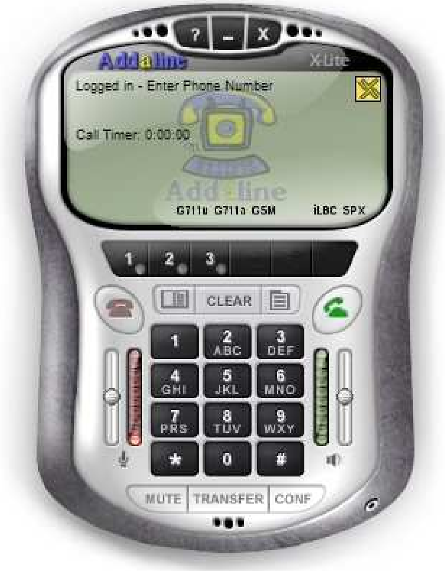
# SIP UA - X-Lite

- X-Lite - The Best Free Softphone
- A FREE premium SIP softphone with many PBX-like features.
- Open standards-based design (SIP) allows for maximum network interoperation and integration.
- Download from http://www.xten.com/

# Features

- Touch-tones [DTMF]
- 3 Lines, Multiple Proxies
- Line Hold
- Inbound Call 'Ignore'
- Inbound Call 'Go to Voicemail'
- Dial/ Redial/Hangup
- Caller ID [SIP ID]
- Call Timer
- Mute
- Microphone & Speakers Levels
- Microphone & Speakers Meters
- Recent Calls Dialed
- Recent Calls Received
- Speed Dial

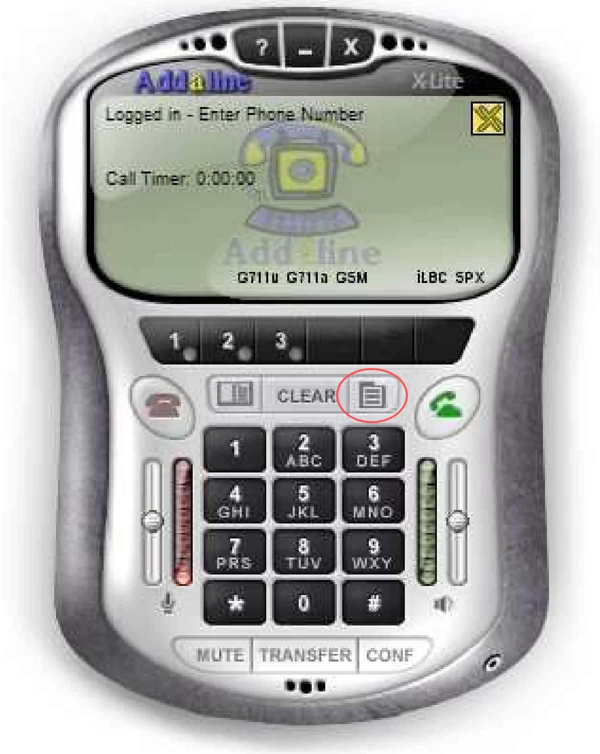
- G.711u+a/iLBC/GSM codecs
- NAT/Firewall support
- Specify NAT IP to be written in SIP messages
- Supports Windows 98SE/NT4/ME/2000/XP

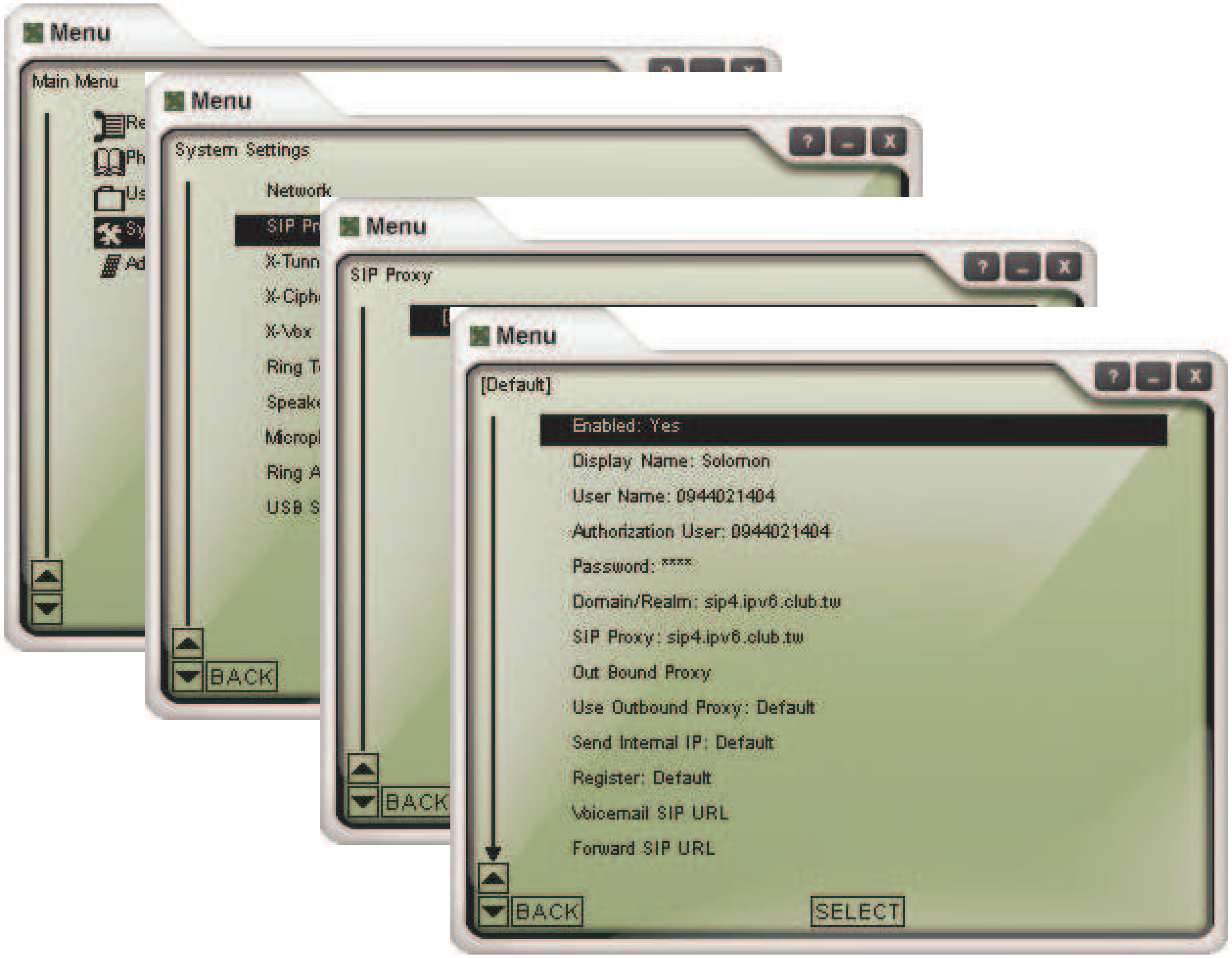


Logged in - Enter Phone Number

Call Timer: 0:00:00

# Step 1: Configuration



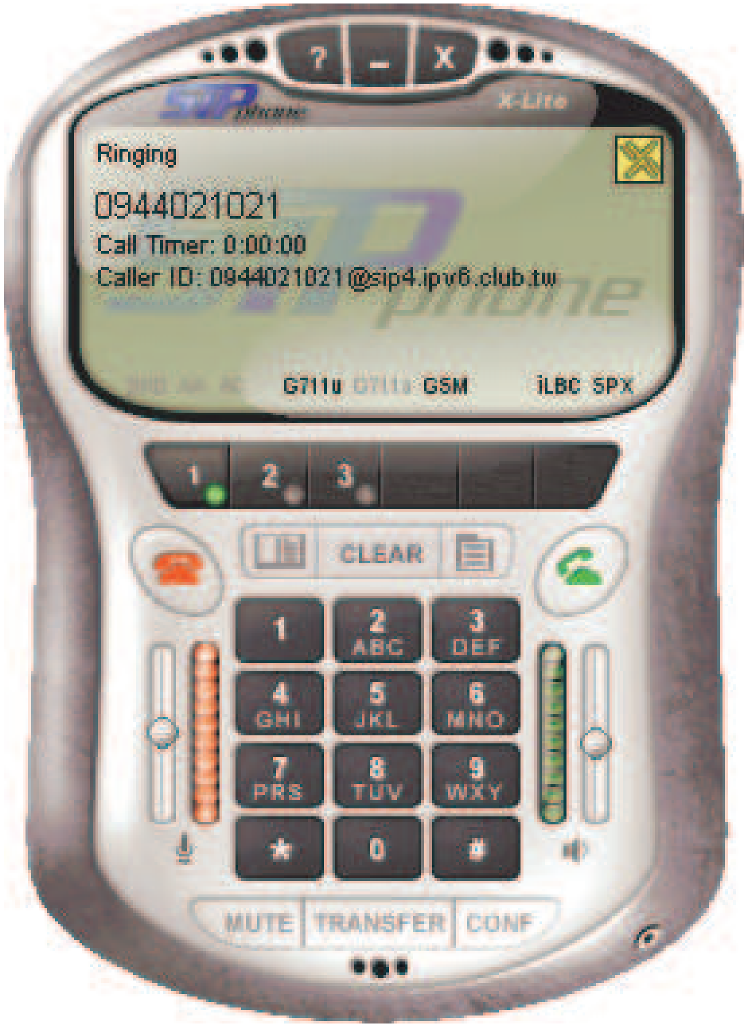


[Default]

Enabled: Yes
Display Name: Solomon
User Name: 0944021404
Authorization User: 0944021404
Password: ****
Domain/Realm: sip4.ipv6.club.tw
SIP Proxy: sip4.ipv6.club.tw
Out Bound Proxy
Use Outbound Proxy: Default
Send Internal IP: Default
Register: Default
Voicemail SIP URL
Forward SIP URL

# Step 2: Make/Receive Calls

- Automatically send a REGISTER request to registrar when the program starts up.
- Dial digits, and domain realm will be appended automatically.



Ringing

0944021021

Call Timer: 0:00:00

Caller ID: 0944021021@sip4.ipv6.club.tw

# Packets Capturing
# &
# Analyzing

# Ethereal – What Is It?

- Every network manager at some time or other needs a tool that can capture packets off the network and analyze them.
- In the past, such tools were either very expensive, proprietary, or both.
- With the advent of Ethereal, all that has changed.

- *"A rose by any other name would smell as sweet."*
  - William Shakespeare

# Features of Ethereal

- Available for UNIX and Windows.
- Capture and display packets from any interface on a UNIX system.
- Display packets captured under a number of other capture programs:
  - tcpdump
  - Network Associates Sniffer and Sniffer Pro
  - NetXray
  - Microsoft Network Monitor
- Filter packets on many criteria.
- Colorize packet display based on filters
- Allow people to add new protocols to Ethereal.

# Where to Get Ethereal

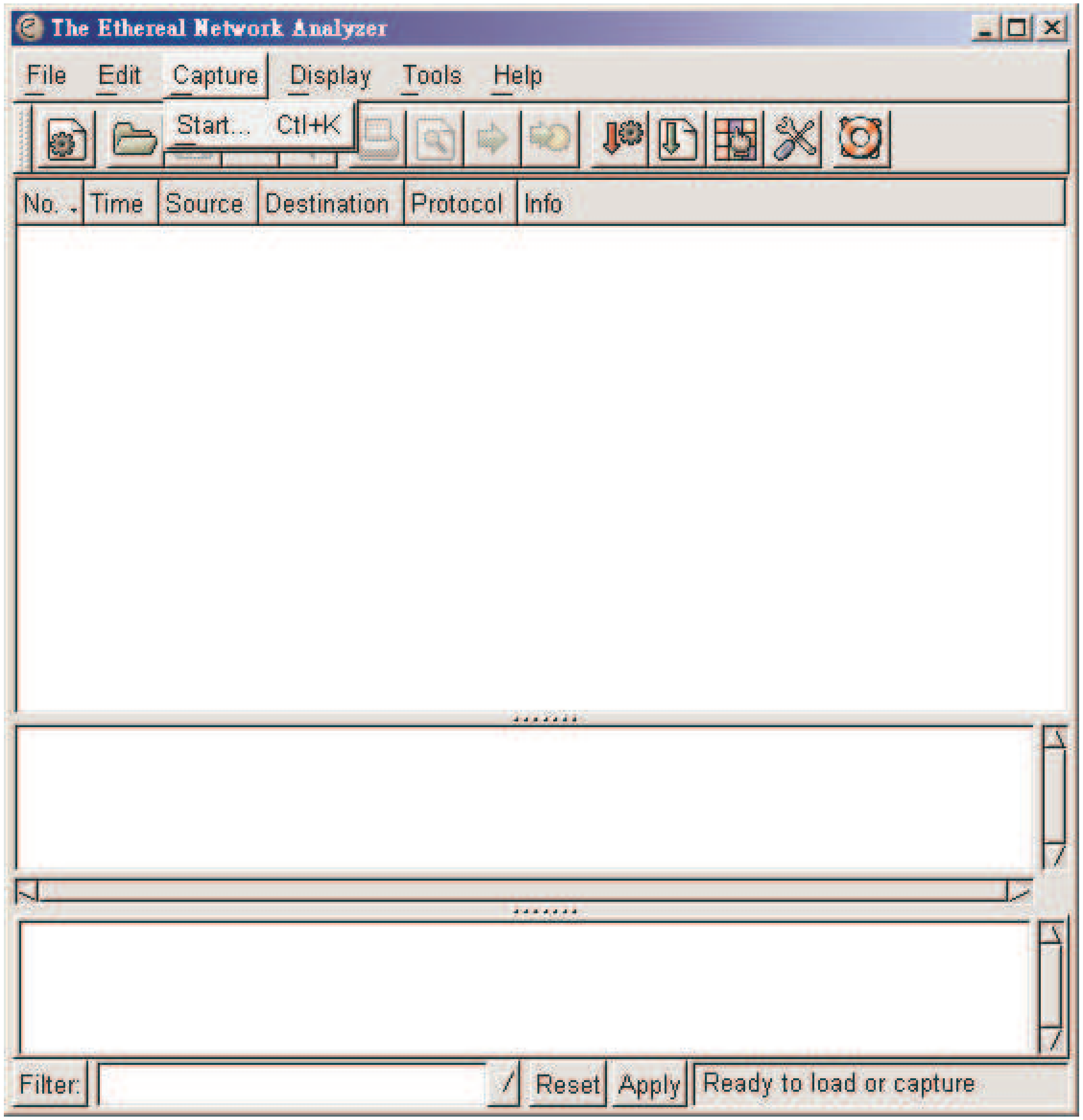
- Official site: http://www.ethereal.com/
- Local mirror: http://voip.ipv6.club.tw/Download/

# Install Ethereal under Windows

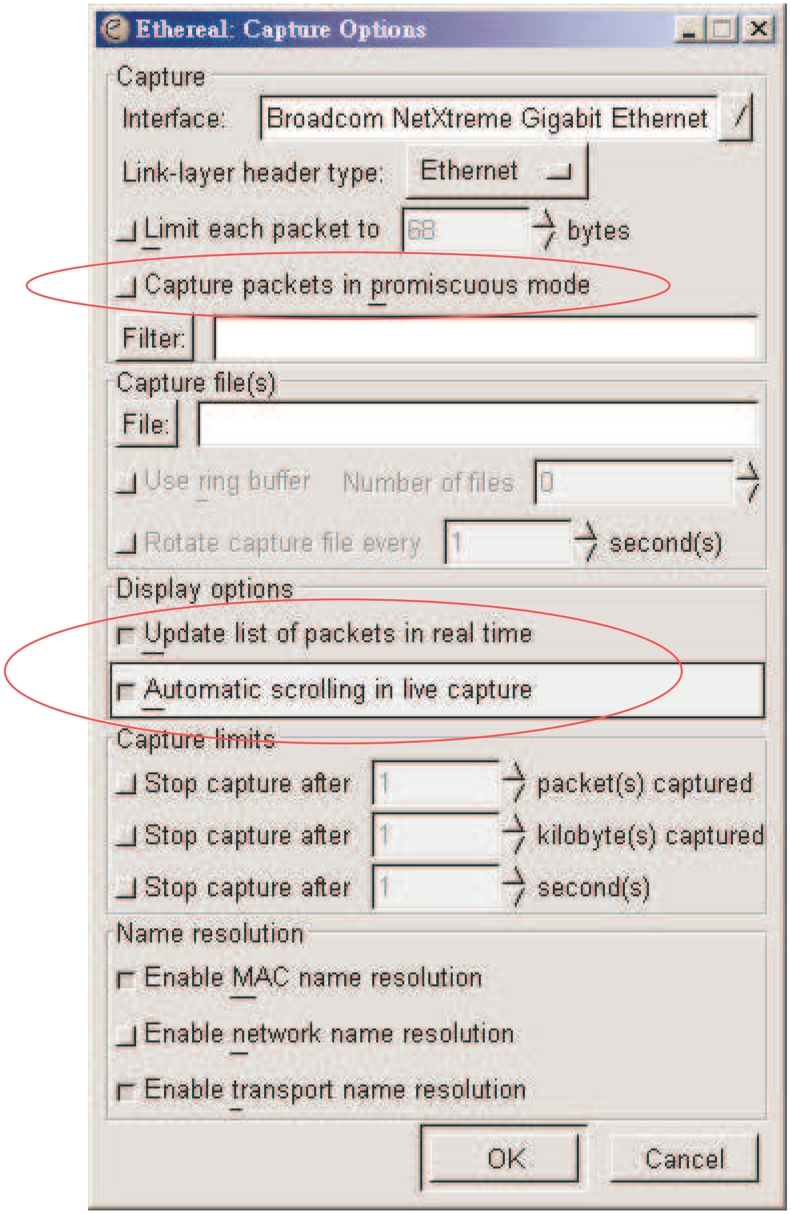
- Install WinPcap 3.1.
  - WinPcap is an architecture for packet capture and network analysis for the Win32 platforms.
  - It includes
    - ☞a kernel-level packet filter,
    - ☞a low-level dynamic link library (packet.dll), and
    - ☞a high-level and system-independent library (wpcap.dll, based on libpcap version 0.6.2)
- Install Ethereal 0.10.13.

# Starting Ethereal

# Capturing packets with Ethereal



# The Capture Preferences dialog box



Ethereal: Capture Options

Capture

Interface: Broadcom NetXtreme Gigabit Ethernet

Link-layer header type: Ethernet

□ Limit each packet to 68 bytes

□ Capture packets in promiscuous mode

Filter:

Capture file(s)

File:

□ Use ring buffer Number of files 0

□ Rotate capture file every 1 second(s)

Display options

☑ Update list of packets in real time

☑ Automatic scrolling in live capture

Capture limits

□ Stop capture after 1 packet(s) captured

□ Stop capture after 1 kilobyte(s) captured

□ Stop capture after 1 second(s)

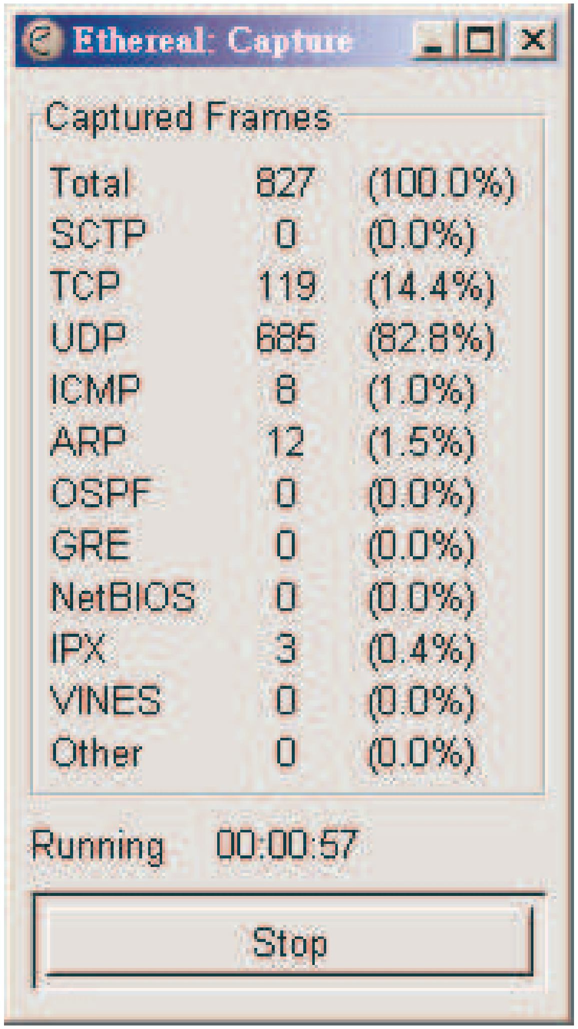
Name resolution

☑ Enable MAC name resolution

□ Enable network name resolution

☑ Enable transport name resolution

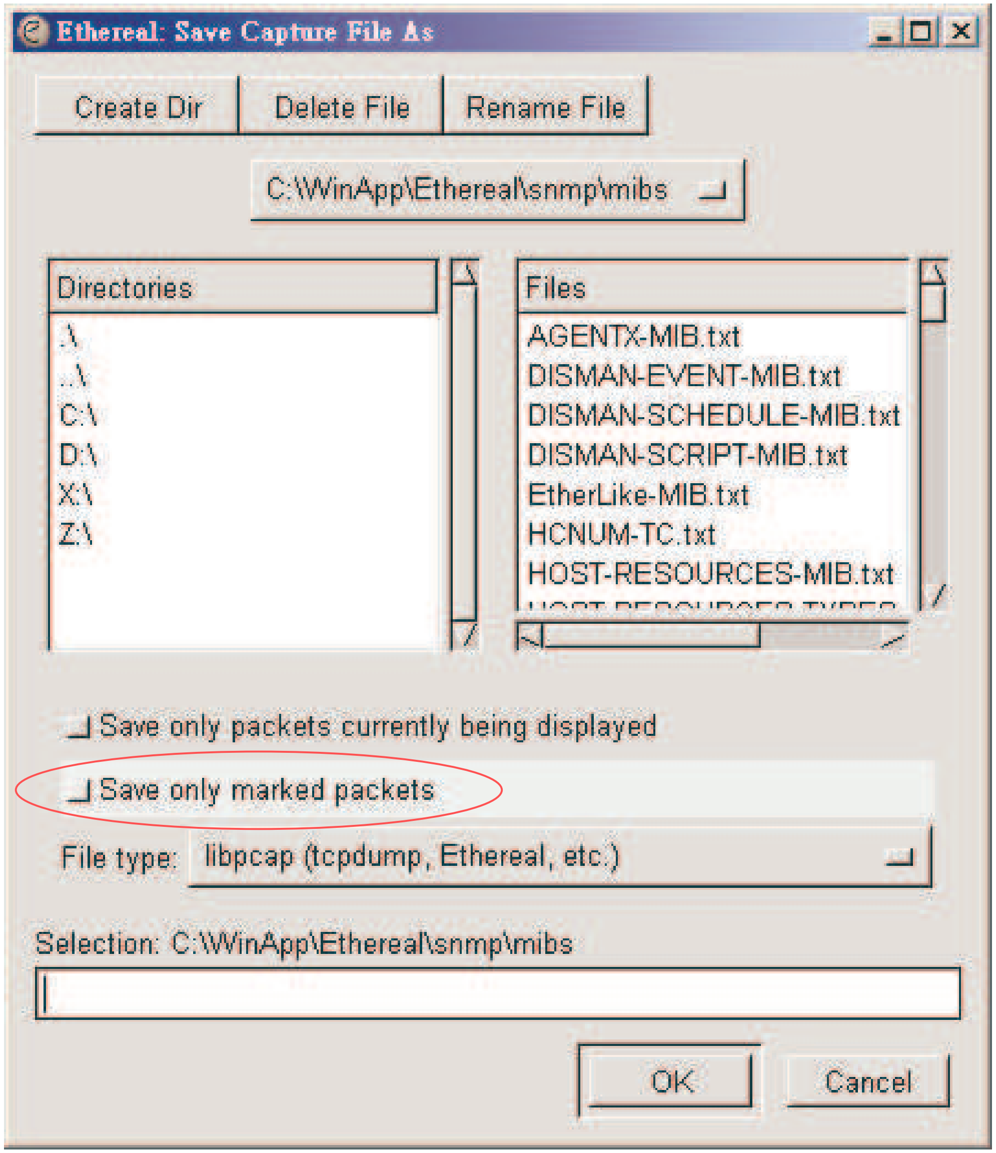
# Stop after you have collected enough packets



| | | |
|---|---|---|
| Total | 827 | (100.0%) |
| SCTP | 0 | (0.0%) |
| TCP | 119 | (14.4%) |
| UDP | 685 | (82.8%) |
| ICMP | 8 | (1.0%) |
| ARP | 12 | (1.5%) |
| OSPF | 0 | (0.0%) |
| GRE | 0 | (0.0%) |
| NetBIOS | 0 | (0.0%) |
| IPX | 3 | (0.4%) |
| VINES | 0 | (0.0%) |
| Other | 0 | (0.0%) |

Running 00:00:57

# File – Save As



C:\WinApp\Ethereal\snmp\mibs

| Directories | Files |
|---|---|
| .\ | AGENTX-MIB.txt |
| ..\ | DISMAN-EVENT-MIB.txt |
| C:\ | DISMAN-SCHEDULE-MIB.txt |
| D:\ | DISMAN-SCRIPT-MIB.txt |
| X:\ | EtherLike-MIB.txt |
| Z:\ | HCNUM-TC.txt |
| | HOST-RESOURCES-MIB.txt |

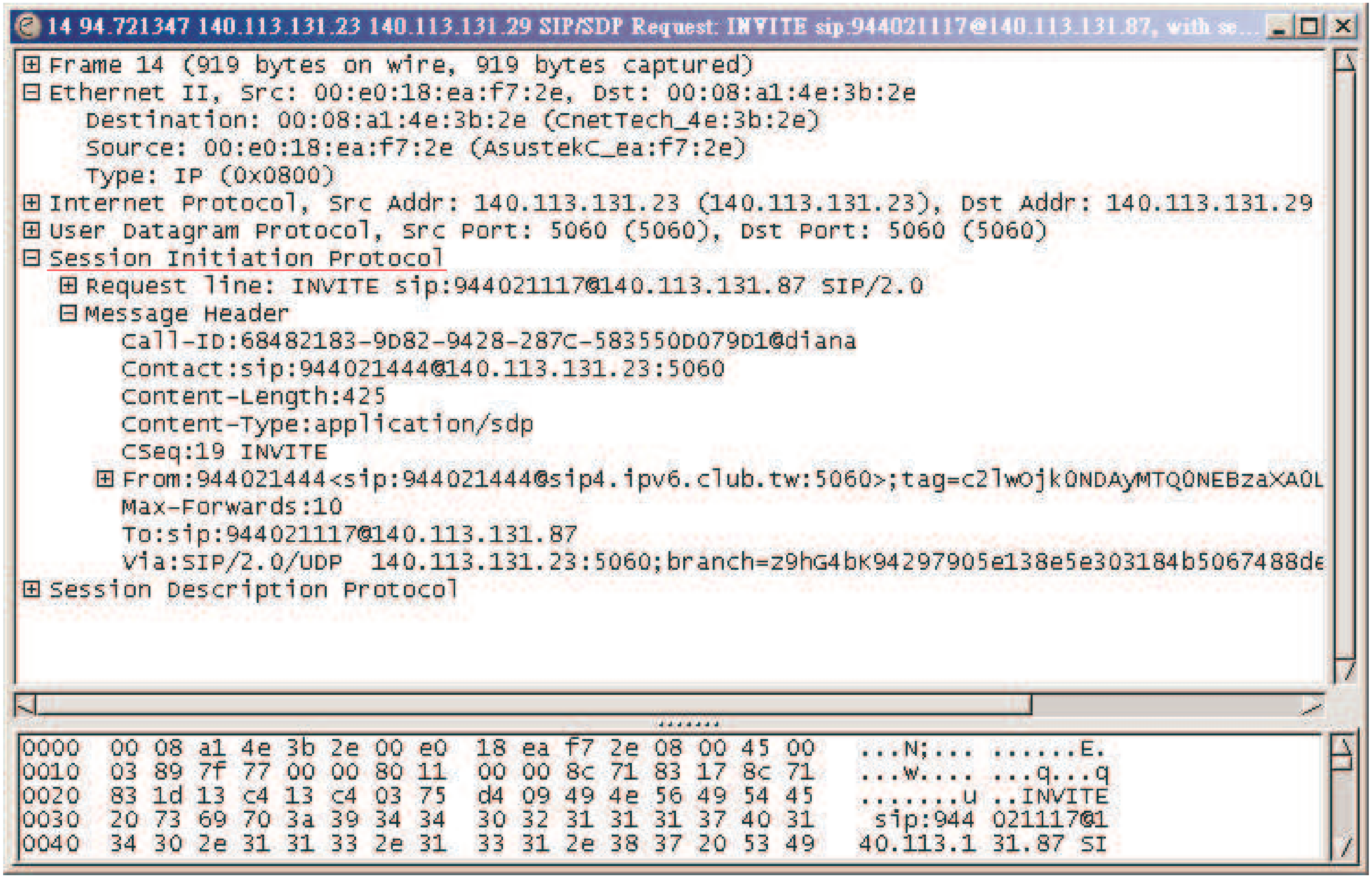
□ Save only packets currently being displayed

□ Save only marked packets

File type: libpcap (tcpdump, Ethereal, etc.)

Selection: C:\WinApp\Ethereal\snmp\mibs

# Show Packet in New Window



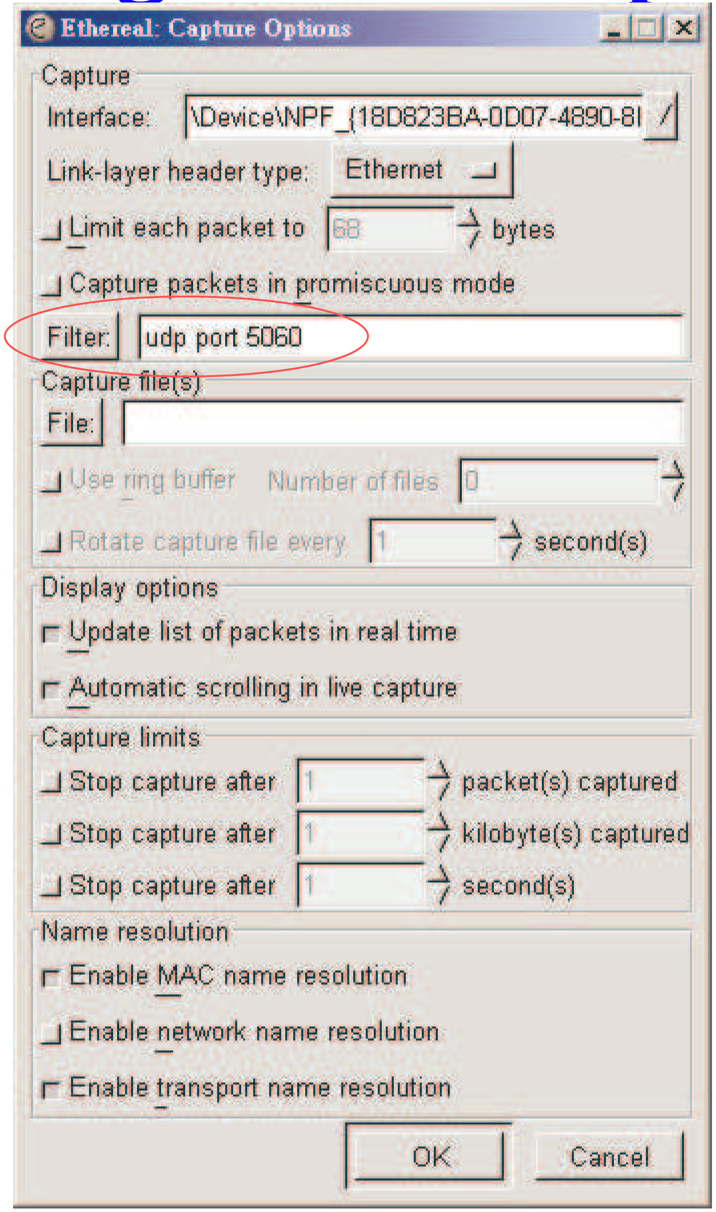
14 94.721347 140.113.131.23 140.113.131.29 SIP/SDP Request: INVITE sip:944021117@140.113.131.87, with se...

```
⊞ Frame 14 (919 bytes on wire, 919 bytes captured)
⊟ Ethernet II, Src: 00:e0:18:ea:f7:2e, Dst: 00:08:a1:4e:3b:2e
    Destination: 00:08:a1:4e:3b:2e (CnetTech_4e:3b:2e)
    Source: 00:e0:18:ea:f7:2e (AsustekC_ea:f7:2e)
    Type: IP (0x0800)
⊞ Internet Protocol, Src Addr: 140.113.131.23 (140.113.131.23), Dst Addr: 140.113.131.29
⊞ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
⊟ Session Initiation Protocol
    ⊞ Request line: INVITE sip:944021117@140.113.131.87 SIP/2.0
    ⊟ Message Header
        Call-ID:68482183-9D82-9428-287C-583550D079D1@diana
        Contact:sip:944021444@140.113.131.23:5060
        Content-Length:425
        Content-Type:application/sdp
        CSeq:19 INVITE
      ⊞ From:944021444<sip:944021444@sip4.ipv6.club.tw:5060>;tag=c2lwOjk0NDAyMTQ0NEBzaXA0L
        Max-Forwards:10
        To:sip:944021117@140.113.131.87
        Via:SIP/2.0/UDP  140.113.131.23:5060;branch=z9hG4bK94297905e138e5e303184b5067488de
⊞ Session Description Protocol
```

```
0000   00 08 a1 4e 3b 2e 00 e0  18 ea f7 2e 08 00 45 00   ...N;... ......E.
0010   03 89 7f 77 00 00 80 11  00 00 8c 71 83 17 8c 71   ...w.... ...q...q
0020   83 1d 13 c4 13 c4 03 75  d4 09 49 4e 56 49 54 45   .......u ..INVITE
0030   20 73 69 70 3a 39 34 34  30 32 31 31 31 37 40 31    sip:944 021117@1
0040   34 30 2e 31 31 33 2e 31  33 31 2e 38 37 20 53 49   40.113.1 31.87 SI
```

# Capture Filters

# Filtering While Capturing



Ethereal: Capture Options

Capture

Interface: \Device\NPF_{18D823BA-0D07-4890-8I

Link-layer header type: Ethernet

□ Limit each packet to 68 bytes

□ Capture packets in promiscuous mode

Filter: udp port 5060

Capture file(s)

File:

□ Use ring buffer Number of files 0

□ Rotate capture file every 1 second(s)

Display options

☑ Update list of packets in real time

☑ Automatic scrolling in live capture

Capture limits

□ Stop capture after 1 packet(s) captured

□ Stop capture after 1 kilobyte(s) captured

□ Stop capture after 1 second(s)

Name resolution

☑ Enable MAC name resolution

□ Enable network name resolution

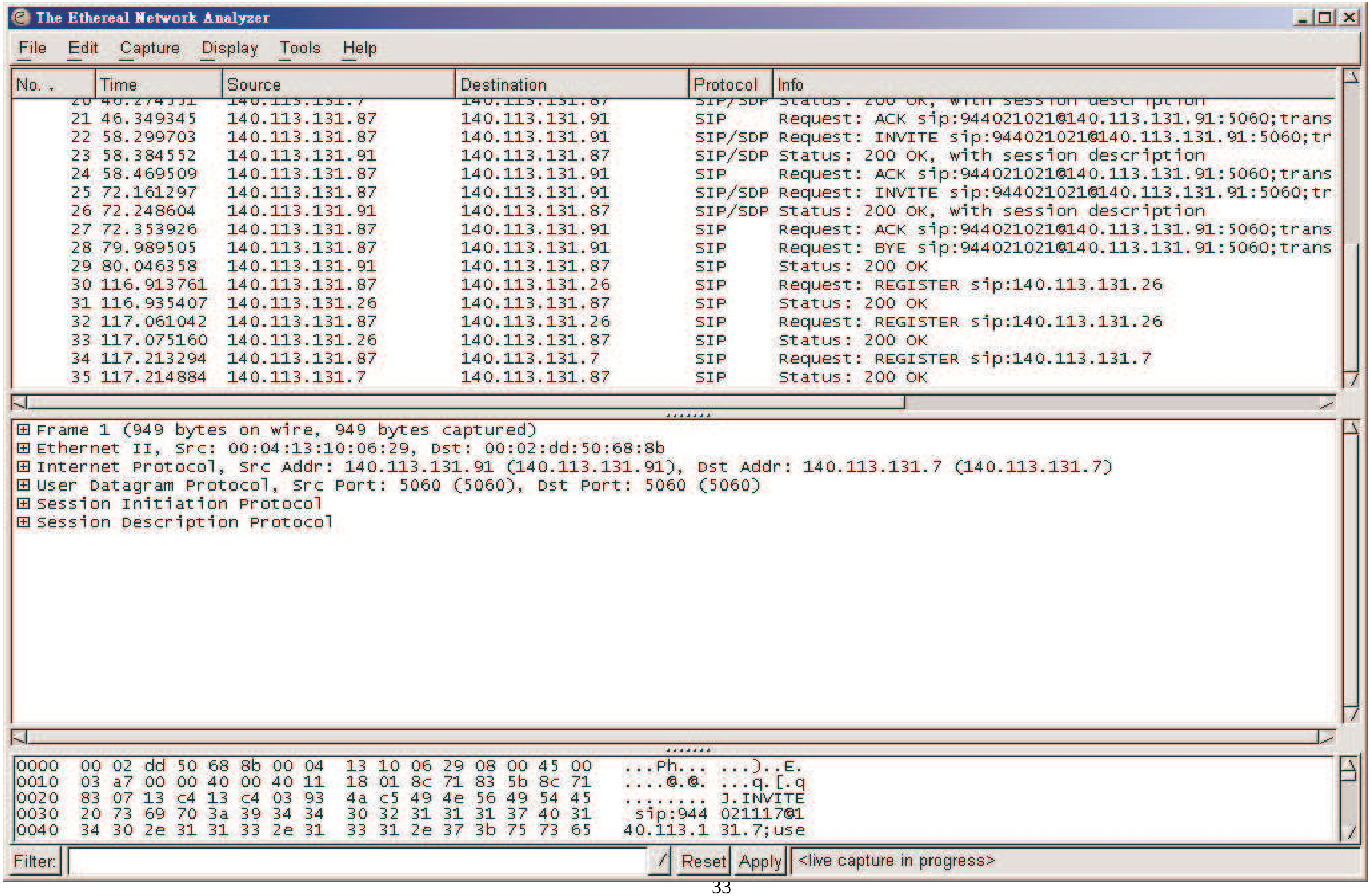
☑ Enable transport name resolution

# Syntax of the tcpdump capture filter language

- [not] **primitive** [and|or [not] **primitive** ...]
  - tcp port 23 and host 10.0.0.5
  - tcp port 23 and not host 10.0.0.5
- **tcpdump** filter language is explained in the man page.

# Capturing SIP signaling

## (filter: udp port 5060)



The Ethereal Network Analyzer
File Edit Capture Display Tools Help

```
No. .  Time        Source           Destination      Protocol Info
    20 46.274331   140.113.131.7    140.113.131.87   SIP/SDP  Status: 200 OK, with session description
    21 46.349345   140.113.131.87   140.113.131.91   SIP      Request: ACK sip:944021021@140.113.131.91:5060;trans
    22 58.299703   140.113.131.87   140.113.131.91   SIP/SDP  Request: INVITE sip:944021021@140.113.131.91:5060;tr
    23 58.384552   140.113.131.91   140.113.131.87   SIP/SDP  Status: 200 OK, with session description
    24 58.469509   140.113.131.87   140.113.131.91   SIP      Request: ACK sip:944021021@140.113.131.91:5060;trans
    25 72.161297   140.113.131.87   140.113.131.91   SIP/SDP  Request: INVITE sip:944021021@140.113.131.91:5060;tr
    26 72.248604   140.113.131.91   140.113.131.87   SIP/SDP  Status: 200 OK, with session description
    27 72.353926   140.113.131.87   140.113.131.91   SIP      Request: ACK sip:944021021@140.113.131.91:5060;trans
    28 79.989505   140.113.131.87   140.113.131.91   SIP      Request: BYE sip:944021021@140.113.131.91:5060;trans
    29 80.046358   140.113.131.91   140.113.131.87   SIP      Status: 200 OK
    30 116.913761  140.113.131.87   140.113.131.26   SIP      Request: REGISTER sip:140.113.131.26
    31 116.935407  140.113.131.26   140.113.131.87   SIP      Status: 200 OK
    32 117.061042  140.113.131.87   140.113.131.26   SIP      Request: REGISTER sip:140.113.131.26
    33 117.075160  140.113.131.26   140.113.131.87   SIP      Status: 200 OK
    34 117.213294  140.113.131.87   140.113.131.7    SIP      Request: REGISTER sip:140.113.131.7
    35 117.214884  140.113.131.7    140.113.131.87   SIP      Status: 200 OK
```

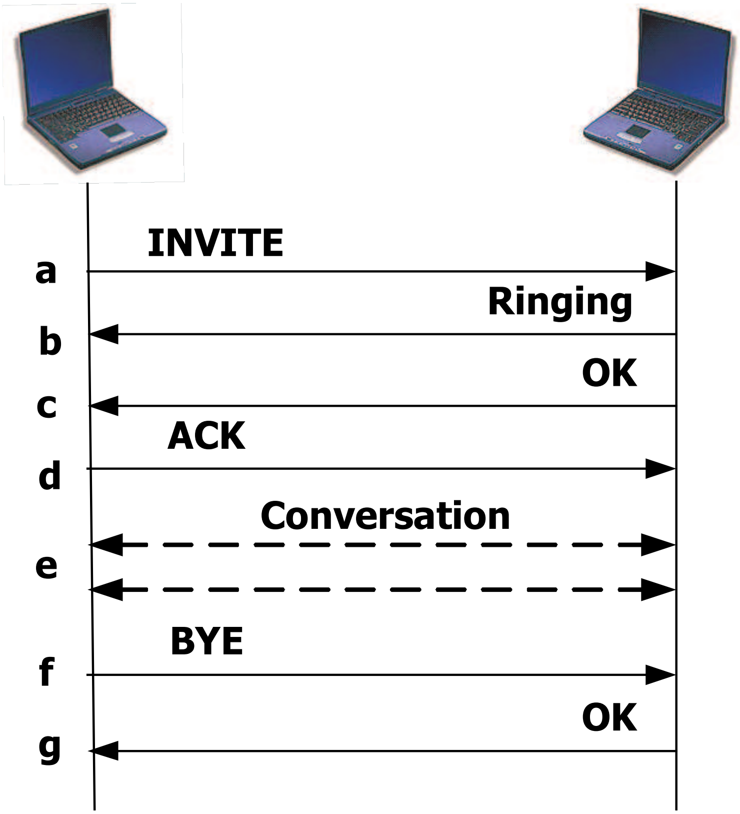
```
⊞ Frame 1 (949 bytes on wire, 949 bytes captured)
⊞ Ethernet II, Src: 00:04:13:10:06:29, Dst: 00:02:dd:50:68:8b
⊞ Internet Protocol, Src Addr: 140.113.131.91 (140.113.131.91), Dst Addr: 140.113.131.7 (140.113.131.7)
⊞ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
⊞ Session Initiation Protocol
⊞ Session Description Protocol
```

```
0000  00 02 dd 50 68 8b 00 04  13 10 06 29 08 00 45 00   ...Ph...  ...)..E.
0010  03 a7 00 00 40 00 40 11  18 01 8c 71 83 5b 8c 71   ....@.@.  ...q.[.q
0020  83 07 13 c4 13 c4 03 93  4a c5 49 4e 56 49 54 45   ........  J.INVITE
0030  20 73 69 70 3a 39 34 34  30 32 31 31 31 37 40 31    sip:944  021117@1
0040  34 30 2e 31 31 33 2e 31  33 31 2e 37 3b 75 73 65   40.113.1  31.7;use
```

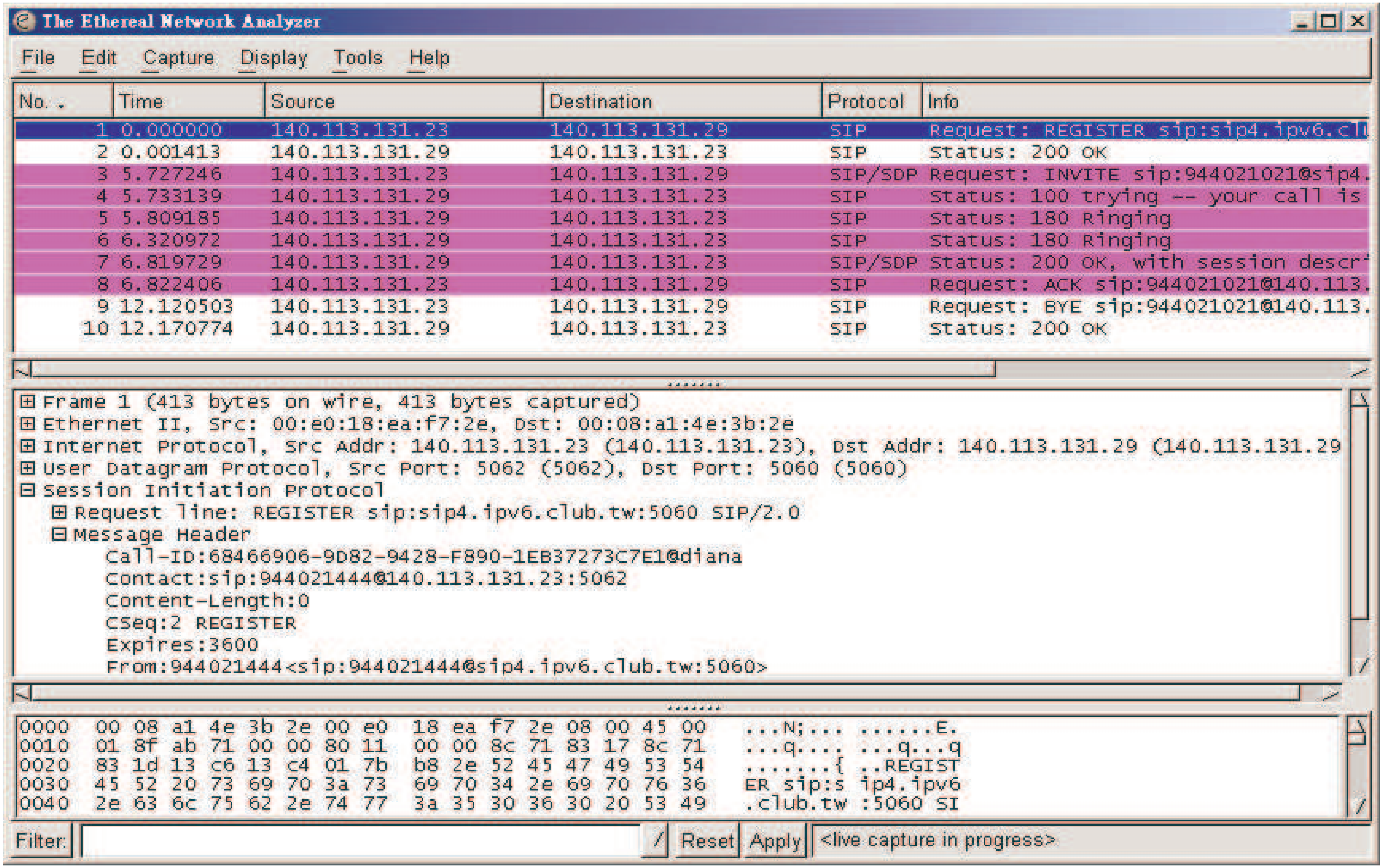
Filter: Reset Apply <live capture in progress>

# SIP Call Establishment

- It is simple, which contains a number of interim responses.



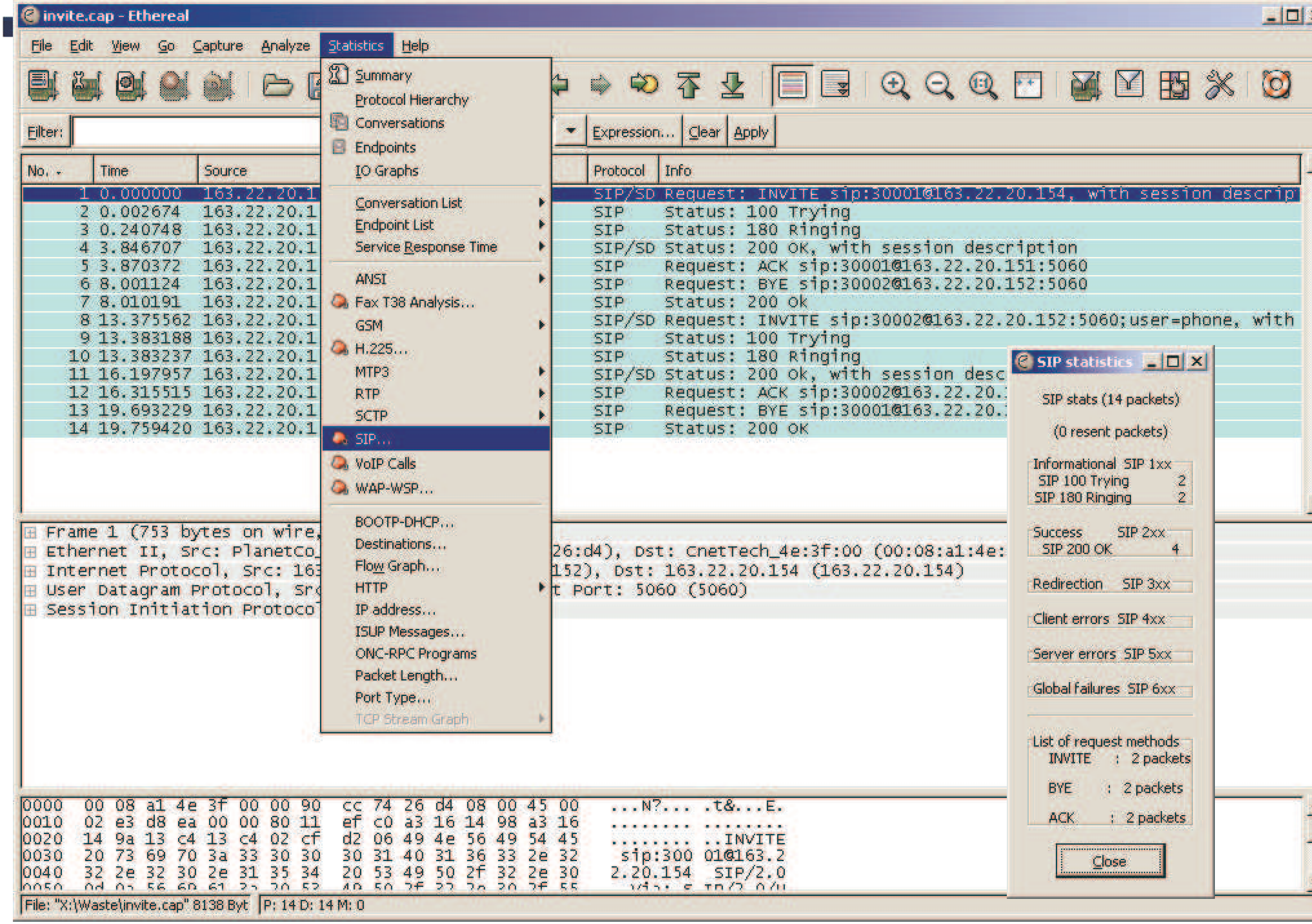
# Basic Call Flow


The Ethereal Network Analyzer
File Edit Capture Display Tools Help
Filter:
Reset
Apply
<live capture in progress>

```
No. .   Time        Source           Destination      Protocol  Info
     1  0.000000    140.113.131.23   140.113.131.29   SIP       Request: REGISTER sip:sip4.ipv6.cl
     2  0.001413    140.113.131.29   140.113.131.23   SIP       Status: 200 OK
     3  5.727246    140.113.131.23   140.113.131.29   SIP/SDP   Request: INVITE sip:944021021@sip4.
     4  5.733139    140.113.131.29   140.113.131.23   SIP       Status: 100 trying -- your call is
     5  5.809185    140.113.131.29   140.113.131.23   SIP       Status: 180 Ringing
     6  6.320972    140.113.131.29   140.113.131.23   SIP       Status: 180 Ringing
     7  6.819729    140.113.131.29   140.113.131.23   SIP/SDP   Status: 200 OK, with session descr
     8  6.822406    140.113.131.23   140.113.131.29   SIP       Request: ACK sip:944021021@140.113.
     9  12.120503   140.113.131.23   140.113.131.29   SIP       Request: BYE sip:944021021@140.113.
    10  12.170774   140.113.131.29   140.113.131.23   SIP       Status: 200 OK
```

```
⊞ Frame 1 (413 bytes on wire, 413 bytes captured)
⊞ Ethernet II, Src: 00:e0:18:ea:f7:2e, Dst: 00:08:a1:4e:3b:2e
⊞ Internet Protocol, Src Addr: 140.113.131.23 (140.113.131.23), Dst Addr: 140.113.131.29 (140.113.131.29
⊞ User Datagram Protocol, Src Port: 5062 (5062), Dst Port: 5060 (5060)
⊟ Session Initiation Protocol
    ⊞ Request line: REGISTER sip:sip4.ipv6.club.tw:5060 SIP/2.0
    ⊟ Message Header
          Call-ID:68466906-9D82-9428-F890-1EB37273C7E1@diana
          Contact:sip:944021444@140.113.131.23:5062
          Content-Length:0
          CSeq:2 REGISTER
          Expires:3600
          From:944021444<sip:944021444@sip4.ipv6.club.tw:5060>
```

```
0000  00 08 a1 4e 3b 2e 00 e0  18 ea f7 2e 08 00 45 00   ...N;... ......E.
0010  01 8f ab 71 00 00 80 11  00 00 8c 71 83 17 8c 71   ...q.... ...q...q
0020  83 1d 13 c6 13 c4 01 7b  b8 2e 52 45 47 49 53 54   .......{ ..REGIST
0030  45 52 20 73 69 70 3a 73  69 70 34 2e 69 70 76 36   ER sip:s ip4.ipv6
0040  2e 63 6c 75 62 2e 74 77  3a 35 30 36 30 20 53 49   .club.tw :5060 SI
```



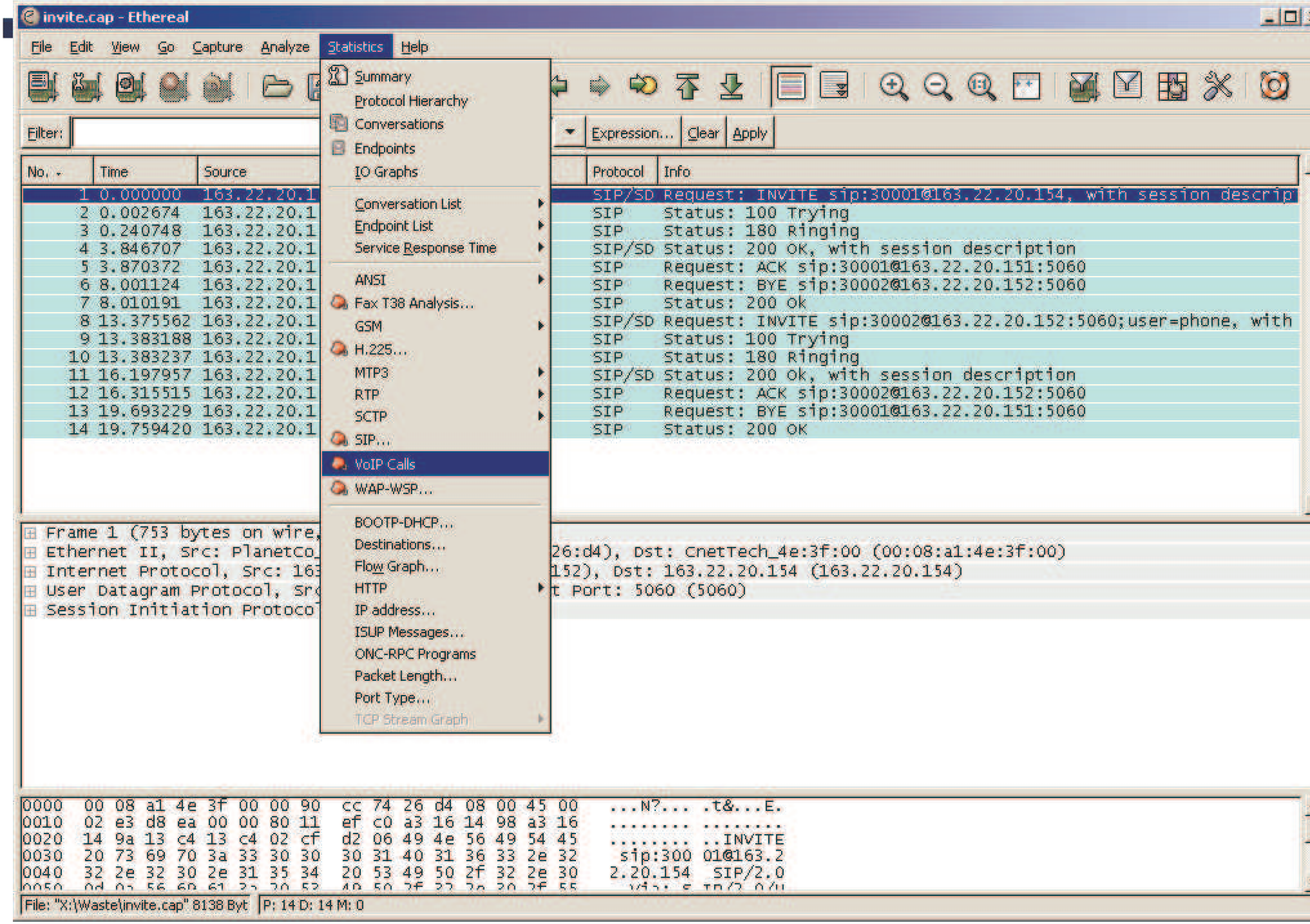
```
No. -   Time       Source                   Protocol  Info
  1 0.000000   163.22.20.1              SIP/SD Request: INVITE sip:30001@163.22.20.154, with session descrip
  2 0.002674   163.22.20.1              SIP    Status: 100 Trying
  3 0.240748   163.22.20.1              SIP    Status: 180 Ringing
  4 3.846707   163.22.20.1              SIP/SD Status: 200 OK, with session description
  5 3.870372   163.22.20.1              SIP    Request: ACK sip:30001@163.22.20.151:5060
  6 8.001124   163.22.20.1              SIP    Request: BYE sip:30002@163.22.20.152:5060
  7 8.010191   163.22.20.1              SIP    Status: 200 Ok
  8 13.375562  163.22.20.1              SIP/SD Request: INVITE sip:30002@163.22.20.152:5060;user=phone, with
  9 13.383188  163.22.20.1              SIP    Status: 100 Trying
 10 13.383237  163.22.20.1              SIP    Status: 180 Ringing
 11 16.197957  163.22.20.1              SIP/SD Status: 200 Ok, with session desc
 12 16.315515  163.22.20.1              SIP    Request: ACK sip:30002@163.22.20.
 13 19.693229  163.22.20.1              SIP    Request: BYE sip:30001@163.22.20.
 14 19.759420  163.22.20.1              SIP    Status: 200 OK
```

```
⊞ Frame 1 (753 bytes on wire,
⊞ Ethernet II, Src: PlanetCo_          26:d4), Dst: CnetTech_4e:3f:00 (00:08:a1:4e:
⊞ Internet Protocol, Src: 163          152), Dst: 163.22.20.154 (163.22.20.154)
⊞ User Datagram Protocol, Src          t Port: 5060 (5060)
⊞ Session Initiation Protoco
```

```
0000  00 08 a1 4e 3f 00 00 90  cc 74 26 d4 08 00 45 00   ...N?... .t&...E.
0010  02 e3 d8 ea 00 00 80 11  ef c0 a3 16 14 98 a3 16   ........ ........
0020  14 9a 13 c4 13 c4 02 cf  d2 06 49 4e 56 49 54 45   ........ ..INVITE
0030  20 73 69 70 3a 33 30 30  30 31 40 31 36 33 2e 32    sip:300 01@163.2
0040  32 2e 32 30 2e 31 35 34  20 53 49 50 2f 32 2e 30   2.20.154  SIP/2.0
```

```
File: "X:\Waste\invite.cap" 8138 Byt   P: 14 D: 14 M: 0
```

```
SIP stats (14 packets)

(0 resent packets)

Informational  SIP 1xx
 SIP 100 Trying        2
 SIP 180 Ringing       2

Success        SIP 2xx
 SIP 200 OK            4

Redirection    SIP 3xx

Client errors  SIP 4xx

Server errors  SIP 5xx

Global failures  SIP 6xx

List of request methods
   INVITE   :  2 packets

   BYE      :  2 packets

   ACK      :  2 packets
```

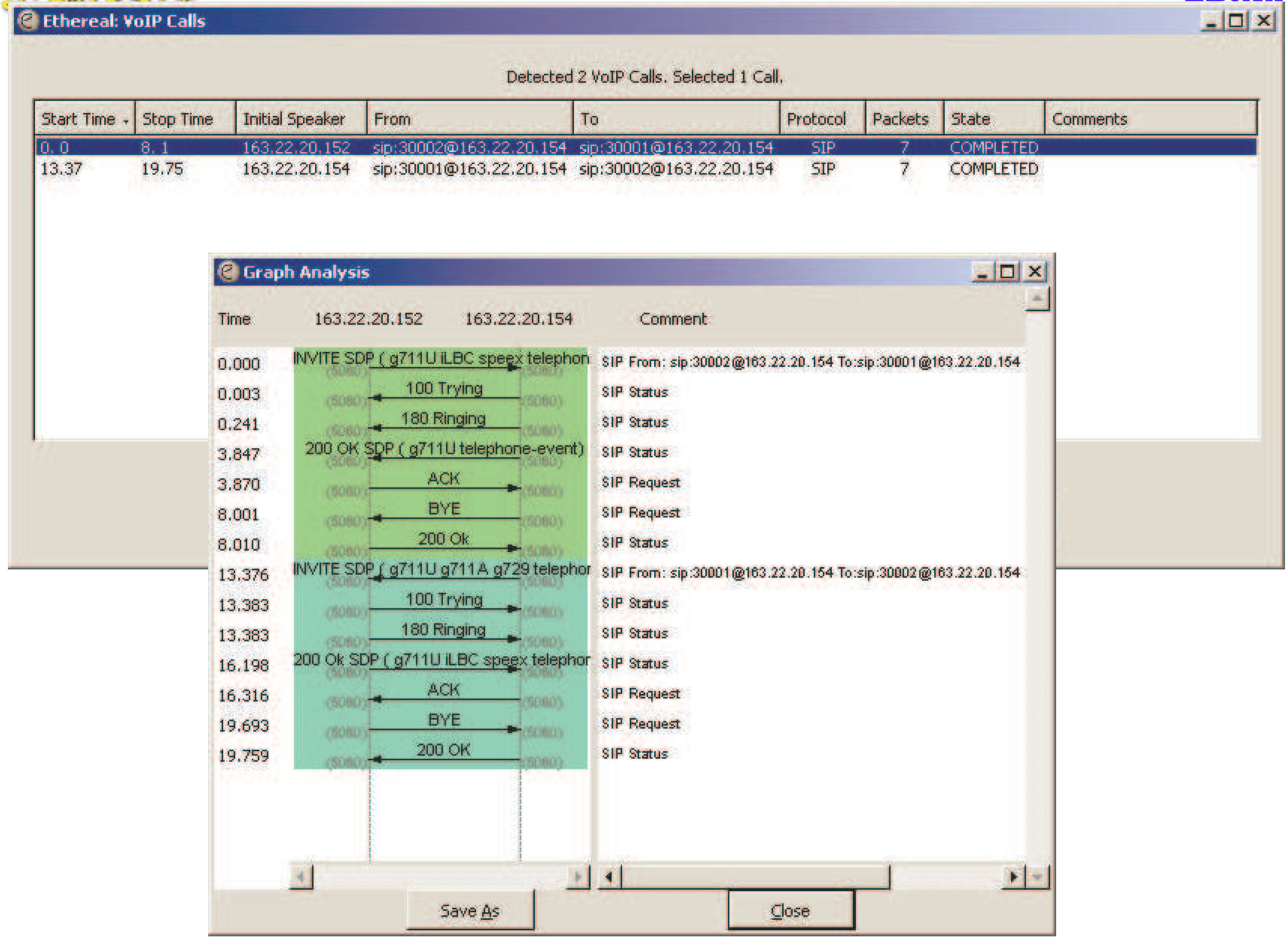


```
No. -   Time       Source                   Protocol Info
  1 0.000000  163.22.20.1            SIP/SD Request: INVITE sip:30001@163.22.20.154, with session descrip
  2 0.002674  163.22.20.1            SIP    Status: 100 Trying
  3 0.240748  163.22.20.1            SIP    Status: 180 Ringing
  4 3.846707  163.22.20.1            SIP/SD Status: 200 OK, with session description
  5 3.870372  163.22.20.1            SIP    Request: ACK sip:30001@163.22.20.151:5060
  6 8.001124  163.22.20.1            SIP    Request: BYE sip:30002@163.22.20.152:5060
  7 8.010191  163.22.20.1            SIP    Status: 200 Ok
  8 13.375562 163.22.20.1            SIP/SD Request: INVITE sip:30002@163.22.20.152:5060;user=phone, with
  9 13.383188 163.22.20.1            SIP    Status: 100 Trying
 10 13.383237 163.22.20.1            SIP    Status: 180 Ringing
 11 16.197957 163.22.20.1            SIP/SD Status: 200 Ok, with session description
 12 16.315515 163.22.20.1            SIP    Request: ACK sip:30002@163.22.20.152:5060
 13 19.693229 163.22.20.1            SIP    Request: BYE sip:30001@163.22.20.151:5060
 14 19.759420 163.22.20.1            SIP    Status: 200 OK
```

```
⊞ Frame 1 (753 bytes on wire,
⊞ Ethernet II, Src: PlanetCo_                26:d4), Dst: CnetTech_4e:3f:00 (00:08:a1:4e:3f:00)
⊞ Internet Protocol, Src: 16                 152), Dst: 163.22.20.154 (163.22.20.154)
⊞ User Datagram Protocol, Src                t Port: 5060 (5060)
⊞ Session Initiation Protoco
```

```
0000  00 08 a1 4e 3f 00 00 90  cc 74 26 d4 08 00 45 00   ...N?... .t&...E.
0010  02 e3 d8 ea 00 00 80 11  ef c0 a3 16 14 98 a3 16   ........ ........
0020  14 9a 13 c4 13 c4 02 cf  d2 06 49 4e 56 49 54 45   ........ ..INVITE
0030  20 73 69 70 3a 33 30 30  30 31 40 31 36 33 2e 32    sip:300 01@163.2
0040  32 2e 32 30 2e 31 35 34  20 53 49 50 2f 32 2e 30   2.20.154  SIP/2.0
```

File: "X:\Waste\invite.cap" 8138 Byt  P: 14 D: 14 M: 0



Ethereal: VoIP Calls

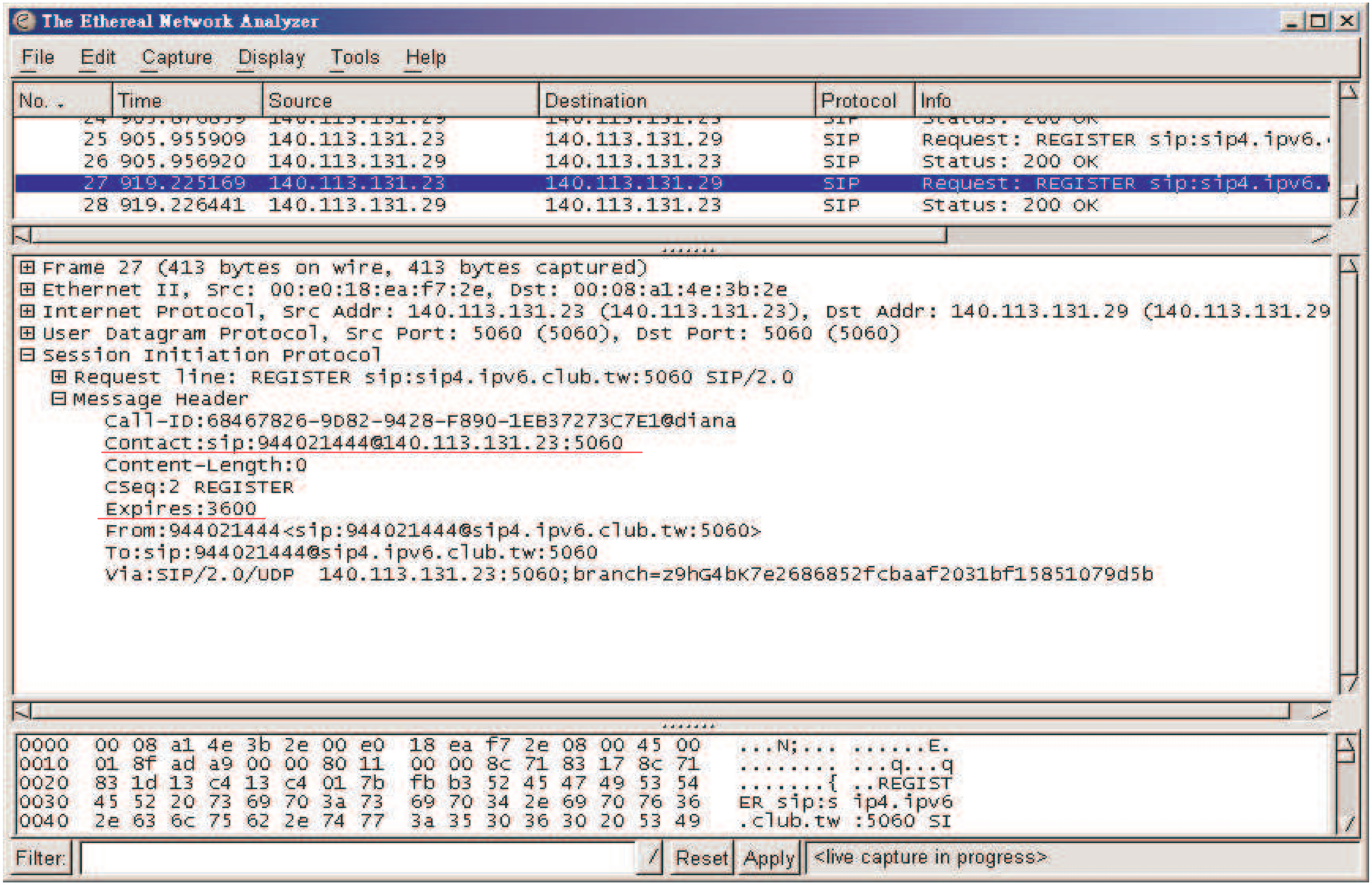
Detected 2 VoIP Calls. Selected 1 Call.

| Start Time | Stop Time | Initial Speaker | From | To | Protocol | Packets | State | Comments |
|---|---|---|---|---|---|---|---|---|
| 0. 0 | 8. 1 | 163.22.20.152 | sip:30002@163.22.20.154 | sip:30001@163.22.20.154 | SIP | 7 | COMPLETED | |
| 13.37 | 19.75 | 163.22.20.154 | sip:30001@163.22.20.154 | sip:30002@163.22.20.154 | SIP | 7 | COMPLETED | |

Graph Analysis

| Time | 163.22.20.152 — 163.22.20.154 | Comment |
|---|---|---|
| 0.000 | INVITE SDP ( g711U iLBC speex telephon → | SIP From: sip:30002@163.22.20.154 To:sip:30001@163.22.20.154 |
| 0.003 | ← 100 Trying | SIP Status |
| 0.241 | ← 180 Ringing | SIP Status |
| 3.847 | 200 OK SDP ( g711U telephone-event) | SIP Status |
| 3.870 | ACK → | SIP Request |
| 8.001 | ← BYE | SIP Request |
| 8.010 | 200 Ok → | SIP Status |
| 13.376 | ← INVITE SDP ( g711U g711A g729 telephor | SIP From: sip:30001@163.22.20.154 To:sip:30002@163.22.20.154 |
| 13.383 | 100 Trying → | SIP Status |
| 13.383 | 180 Ringing → | SIP Status |
| 16.198 | 200 Ok SDP ( g711U iLBC speex telephor → | SIP Status |
| 16.316 | ← ACK | SIP Request |
| 19.693 | BYE → | SIP Request |
| 19.759 | ← 200 OK | SIP Status |

# REGISTER

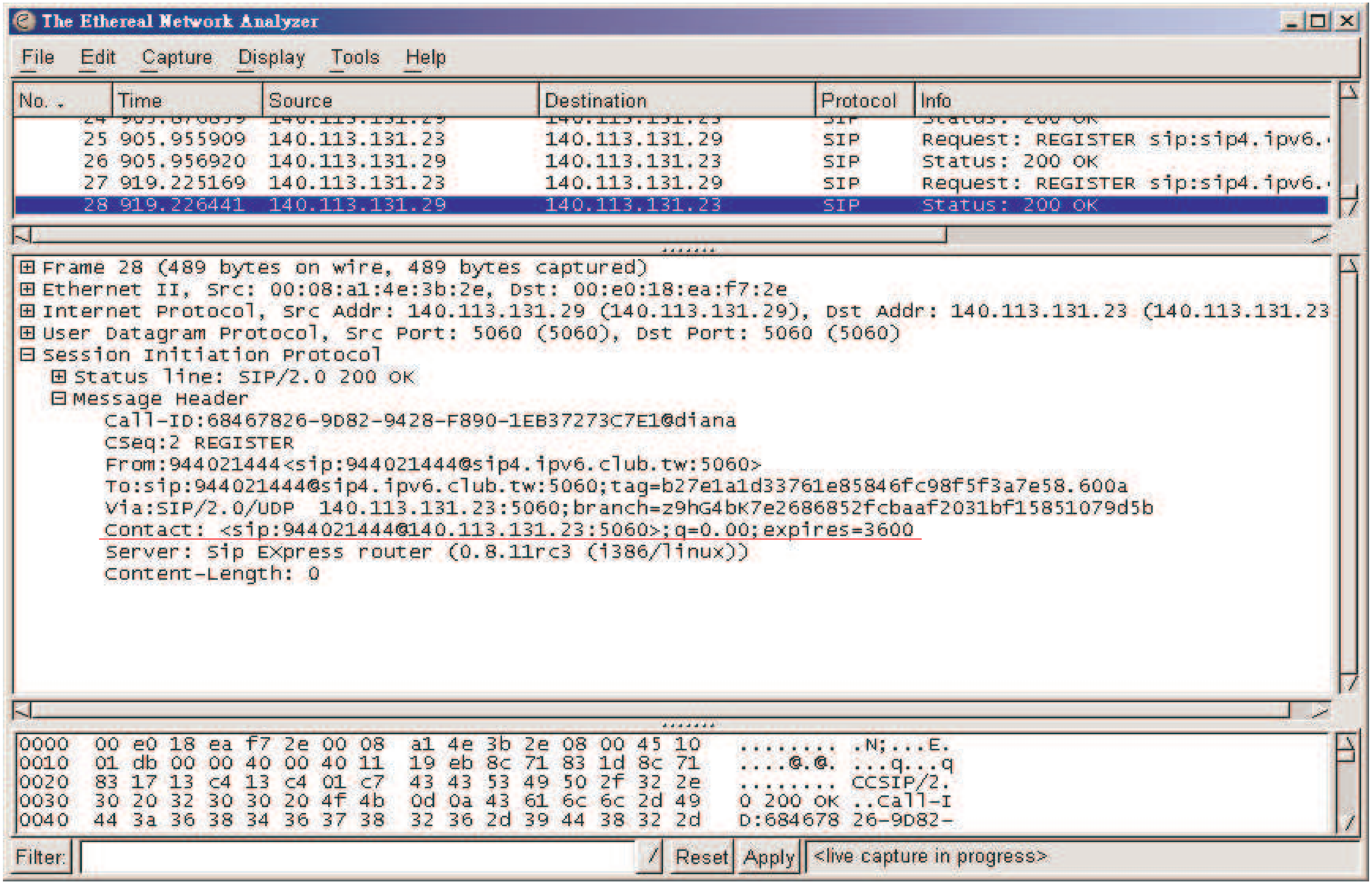

The Ethereal Network Analyzer
File Edit Capture Display Tools Help
Filter:
Reset
Apply
<live capture in progress>

```
No.  Time         Source           Destination      Protocol  Info
  25 905.955909   140.113.131.23   140.113.131.29   SIP       Request: REGISTER sip:sip4.ipv6.
  26 905.956920   140.113.131.29   140.113.131.23   SIP       Status: 200 OK
  27 919.225169   140.113.131.23   140.113.131.29   SIP       Request: REGISTER sip:sip4.ipv6.
  28 919.226441   140.113.131.29   140.113.131.23   SIP       Status: 200 OK
```

```
⊞ Frame 27 (413 bytes on wire, 413 bytes captured)
⊞ Ethernet II, Src: 00:e0:18:ea:f7:2e, Dst: 00:08:a1:4e:3b:2e
⊞ Internet Protocol, Src Addr: 140.113.131.23 (140.113.131.23), Dst Addr: 140.113.131.29 (140.113.131.29
⊞ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
⊟ Session Initiation Protocol
   ⊞ Request line: REGISTER sip:sip4.ipv6.club.tw:5060 SIP/2.0
   ⊟ Message Header
       Call-ID:68467826-9D82-9428-F890-1EB37273C7E1@diana
       Contact:sip:944021444@140.113.131.23:5060
       Content-Length:0
       CSeq:2 REGISTER
       Expires:3600
       From:944021444<sip:944021444@sip4.ipv6.club.tw:5060>
       To:sip:944021444@sip4.ipv6.club.tw:5060
       Via:SIP/2.0/UDP  140.113.131.23:5060;branch=z9hG4bK7e2686852fcbaaf2031bf15851079d5b
```

```
0000  00 08 a1 4e 3b 2e 00 e0  18 ea f7 2e 08 00 45 00   ...N;... ......E.
0010  01 8f ad a9 00 00 80 11  00 00 8c 71 83 17 8c 71   ........ ...q...q
0020  83 1d 13 c4 13 c4 01 7b  fb b3 52 45 47 49 53 54   .......{ ..REGIST
0030  45 52 20 73 69 70 3a 73  69 70 34 2e 69 70 76 36   ER sip:s ip4.ipv6
0040  2e 63 6c 75 62 2e 74 77  3a 35 30 36 30 20 53 49   .club.tw :5060 SI
```

# 200 OK

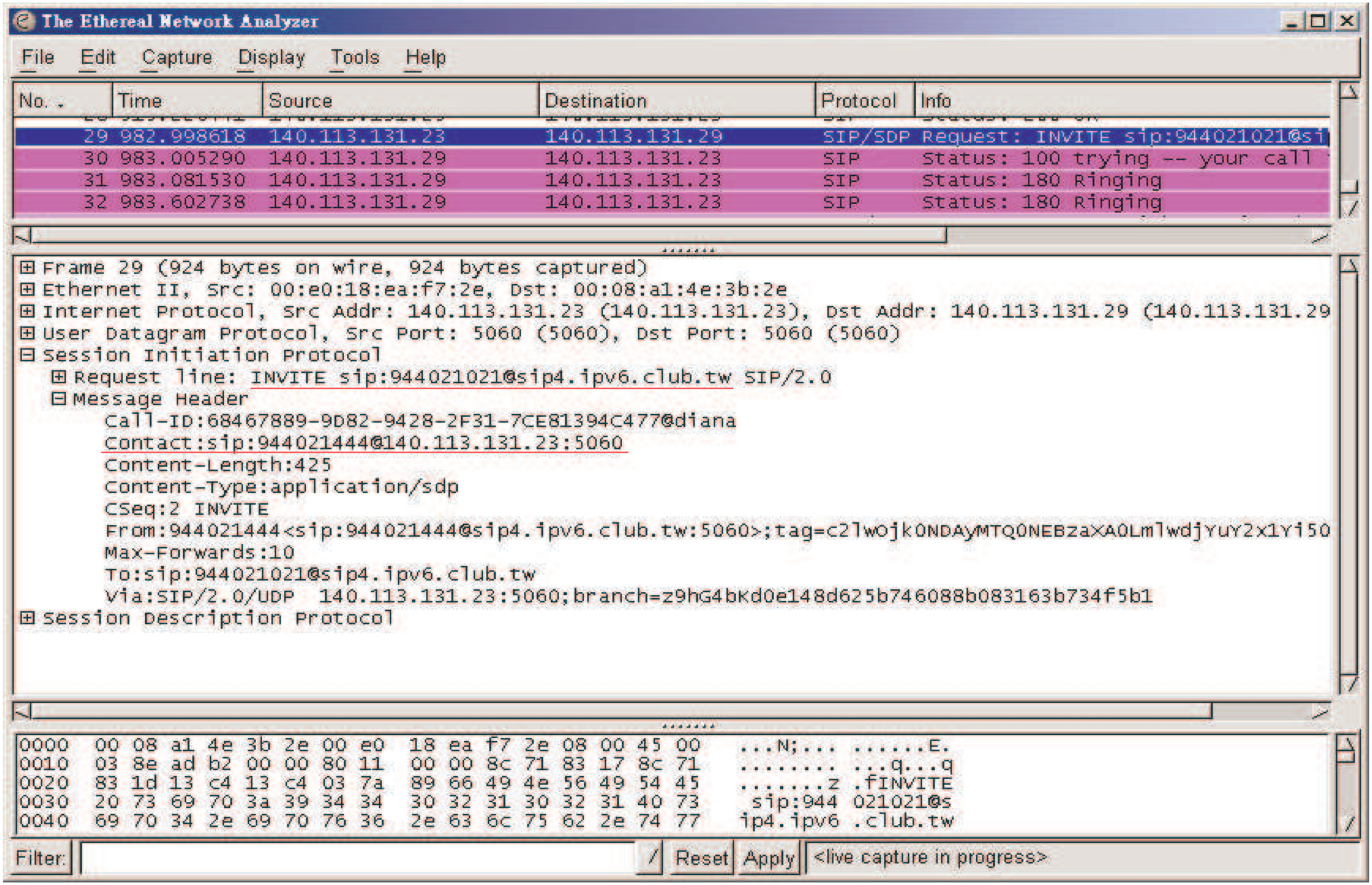

The Ethereal Network Analyzer
File Edit Capture Display Tools Help
Filter:
Reset
Apply
<live capture in progress>

```
No. .   Time         Source           Destination      Protocol  Info
  25 905.955909   140.113.131.23   140.113.131.29   SIP       Request: REGISTER sip:sip4.ipv6.
  26 905.956920   140.113.131.29   140.113.131.23   SIP       Status: 200 OK
  27 919.225169   140.113.131.23   140.113.131.29   SIP       Request: REGISTER sip:sip4.ipv6.
  28 919.226441   140.113.131.29   140.113.131.23   SIP       Status: 200 OK
```

```
⊞ Frame 28 (489 bytes on wire, 489 bytes captured)
⊞ Ethernet II, Src: 00:08:a1:4e:3b:2e, Dst: 00:e0:18:ea:f7:2e
⊞ Internet Protocol, Src Addr: 140.113.131.29 (140.113.131.29), Dst Addr: 140.113.131.23 (140.113.131.23
⊞ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
⊟ Session Initiation Protocol
    ⊞ Status line: SIP/2.0 200 OK
    ⊟ Message Header
          Call-ID:68467826-9D82-9428-F890-1EB37273C7E1@diana
          CSeq:2 REGISTER
          From:944021444<sip:944021444@sip4.ipv6.club.tw:5060>
          To:sip:944021444@sip4.ipv6.club.tw:5060;tag=b27e1a1d33761e85846fc98f5f3a7e58.600a
          Via:SIP/2.0/UDP  140.113.131.23:5060;branch=z9hG4bK7e2686852fcbaaf2031bf15851079d5b
          Contact: <sip:944021444@140.113.131.23:5060>;q=0.00;expires=3600
          Server: Sip Express router (0.8.11rc3 (i386/linux))
          Content-Length: 0
```

```
0000  00 e0 18 ea f7 2e 00 08  a1 4e 3b 2e 08 00 45 10   ........ .N;...E.
0010  01 db 00 00 40 00 40 11  19 eb 8c 71 83 1d 8c 71   ....@.@. ...q...q
0020  83 17 13 c4 13 c4 01 c7  43 43 53 49 50 2f 32 2e   ........ CCSIP/2.
0030  30 20 32 30 30 20 4f 4b  0d 0a 43 61 6c 6c 2d 49   0 200 OK ..Call-I
0040  44 3a 36 38 34 36 37 38  32 36 2d 39 44 38 32 2d   D:684678 26-9D82-
```

# INVITE

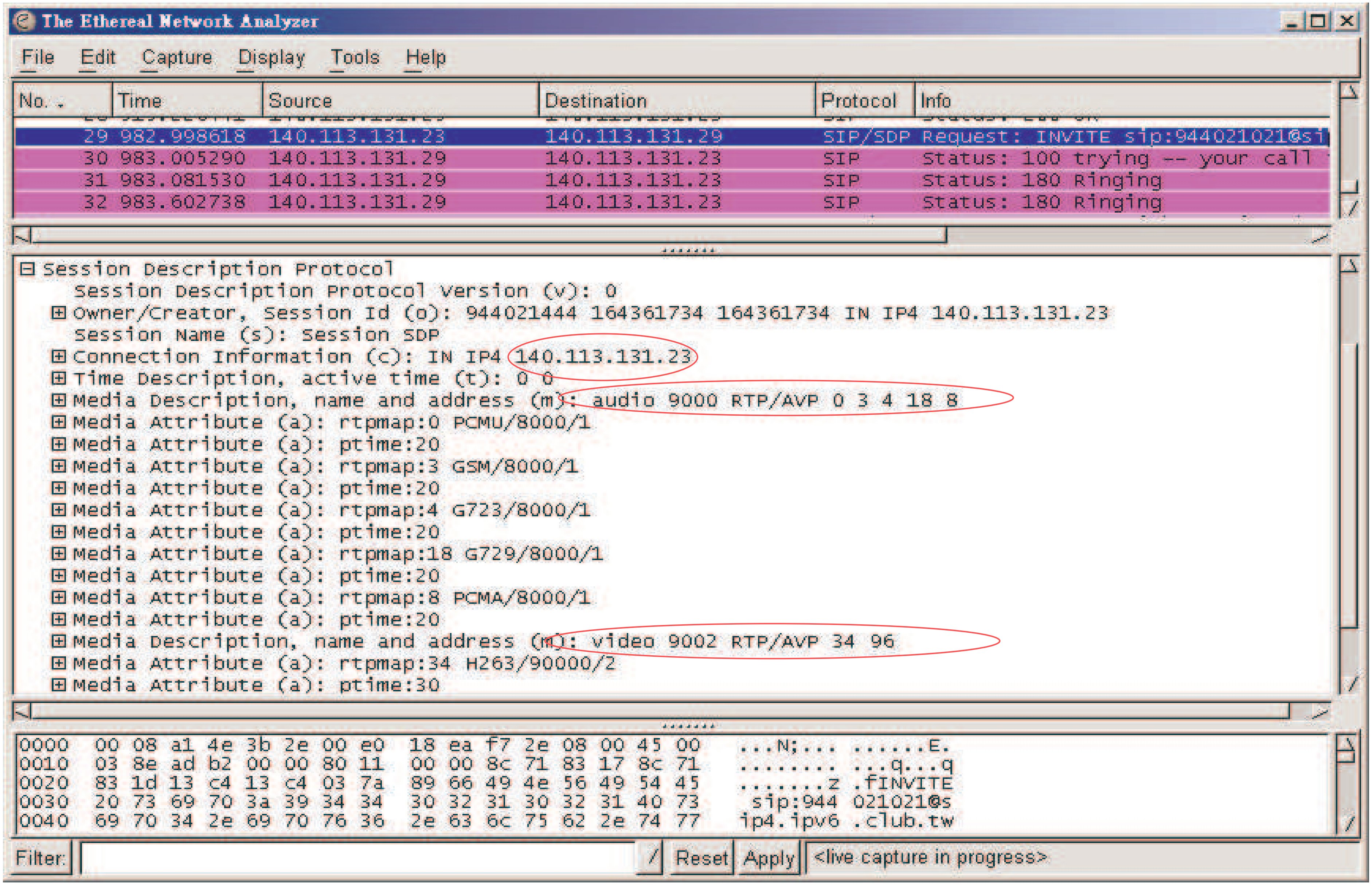


```
No. .  Time        Source           Destination      Protocol Info
    29 982.998618  140.113.131.23   140.113.131.29   SIP/SDP  Request: INVITE sip:944021021@si
    30 983.005290  140.113.131.29   140.113.131.23   SIP      Status: 100 trying -- your call
    31 983.081530  140.113.131.29   140.113.131.23   SIP      Status: 180 Ringing
    32 983.602738  140.113.131.29   140.113.131.23   SIP      Status: 180 Ringing
```

```
⊞ Frame 29 (924 bytes on wire, 924 bytes captured)
⊞ Ethernet II, Src: 00:e0:18:ea:f7:2e, Dst: 00:08:a1:4e:3b:2e
⊞ Internet Protocol, Src Addr: 140.113.131.23 (140.113.131.23), Dst Addr: 140.113.131.29 (140.113.131.29
⊞ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
⊟ Session Initiation Protocol
   ⊞ Request line: INVITE sip:944021021@sip4.ipv6.club.tw SIP/2.0
   ⊟ Message Header
        Call-ID:68467889-9D82-9428-2F31-7CE81394C477@diana
        Contact:sip:944021444@140.113.131.23:5060
        Content-Length:425
        Content-Type:application/sdp
        CSeq:2 INVITE
        From:944021444<sip:944021444@sip4.ipv6.club.tw:5060>;tag=c2lwOjk0NDAyMTQ0NEBzaXA0Lmlwdjyuy2x1Yi50
        Max-Forwards:10
        To:sip:944021021@sip4.ipv6.club.tw
        Via:SIP/2.0/UDP  140.113.131.23:5060;branch=z9hG4bKd0e148d625b746088b083163b734f5b1
⊞ Session Description Protocol
```

```
0000  00 08 a1 4e 3b 2e 00 e0  18 ea f7 2e 08 00 45 00   ...N;... ......E.
0010  03 8e ad b2 00 00 80 11  00 00 8c 71 83 17 8c 71   ........ ...q...q
0020  83 1d 13 c4 13 c4 03 7a  89 66 49 4e 56 49 54 45   .......z .fINVITE
0030  20 73 69 70 3a 39 34 34  30 32 31 30 32 31 40 73    sip:944 021021@s
0040  69 70 34 2e 69 70 76 36  2e 63 6c 75 62 2e 74 77   ip4.ipv6 .club.tw
```

# SDP in INVITE

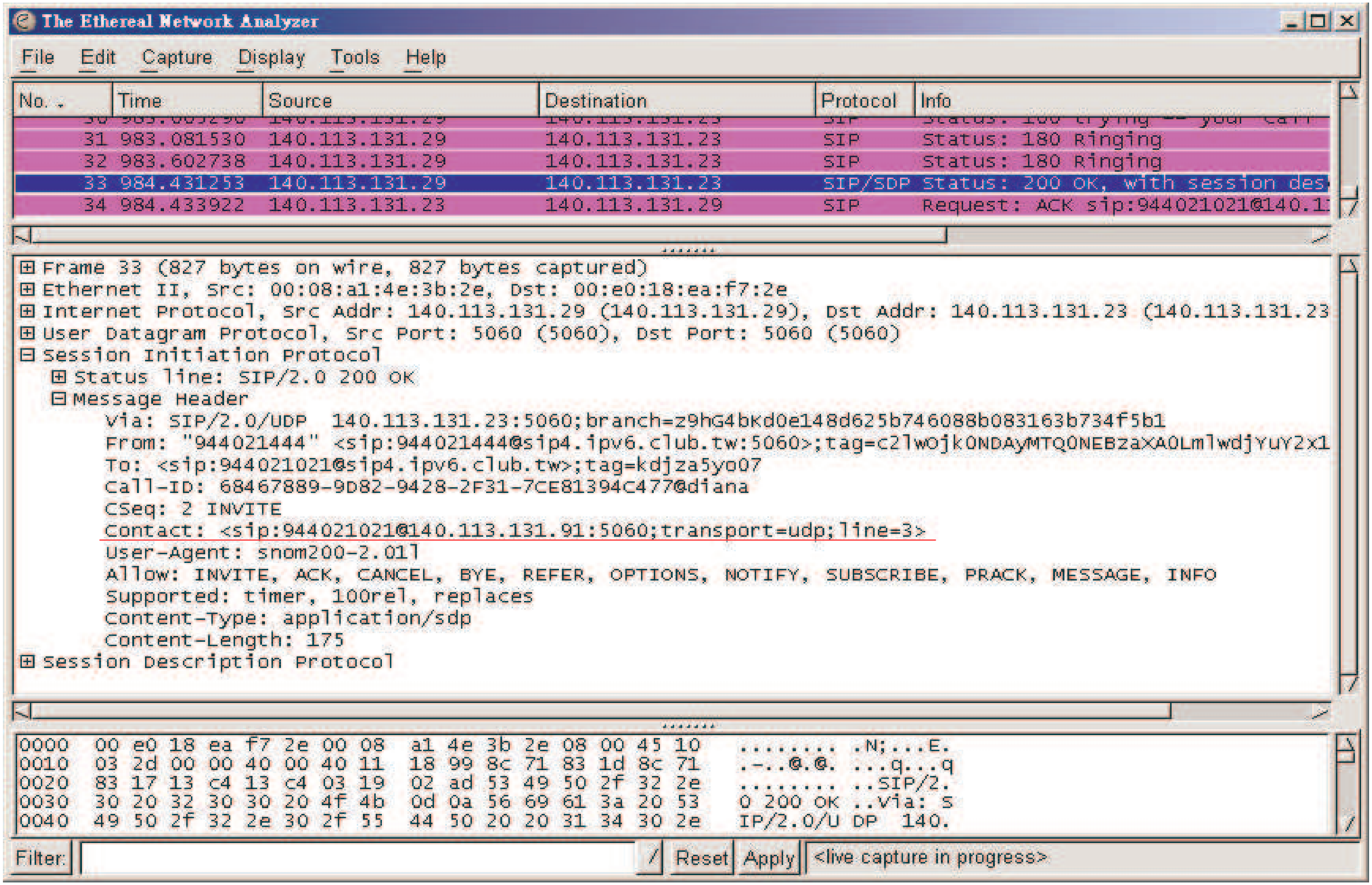

The Ethereal Network Analyzer
File Edit Capture Display Tools Help
Filter:
Reset
Apply
<live capture in progress>

```
No.   Time        Source            Destination       Protocol Info
  29 982.998618  140.113.131.23    140.113.131.29    SIP/SDP  Request: INVITE sip:944021021@si
  30 983.005290  140.113.131.29    140.113.131.23    SIP      Status: 100 trying -- your call
  31 983.081530  140.113.131.29    140.113.131.23    SIP      Status: 180 Ringing
  32 983.602738  140.113.131.29    140.113.131.23    SIP      Status: 180 Ringing
```

```
⊟ Session Description Protocol
    Session Description Protocol Version (v): 0
  ⊞ Owner/Creator, Session Id (o): 944021444 164361734 164361734 IN IP4 140.113.131.23
    Session Name (s): Session SDP
  ⊞ Connection Information (c): IN IP4 140.113.131.23
  ⊞ Time Description, active time (t): 0 0
  ⊞ Media Description, name and address (m): audio 9000 RTP/AVP 0 3 4 18 8
  ⊞ Media Attribute (a): rtpmap:0 PCMU/8000/1
  ⊞ Media Attribute (a): ptime:20
  ⊞ Media Attribute (a): rtpmap:3 GSM/8000/1
  ⊞ Media Attribute (a): ptime:20
  ⊞ Media Attribute (a): rtpmap:4 G723/8000/1
  ⊞ Media Attribute (a): ptime:20
  ⊞ Media Attribute (a): rtpmap:18 G729/8000/1
  ⊞ Media Attribute (a): ptime:20
  ⊞ Media Attribute (a): rtpmap:8 PCMA/8000/1
  ⊞ Media Attribute (a): ptime:20
  ⊞ Media Description, name and address (m): video 9002 RTP/AVP 34 96
  ⊞ Media Attribute (a): rtpmap:34 H263/90000/2
  ⊞ Media Attribute (a): ptime:30
```

```
0000  00 08 a1 4e 3b 2e 00 e0  18 ea f7 2e 08 00 45 00   ...N;... ......E.
0010  03 8e ad b2 00 00 80 11  00 00 8c 71 83 17 8c 71   ........ ...q...q
0020  83 1d 13 c4 13 c4 03 7a  89 66 49 4e 56 49 54 45   .......z .fINVITE
0030  20 73 69 70 3a 39 34 34  30 32 31 30 32 31 40 73    sip:944 021021@s
0040  69 70 34 2e 69 70 76 36  2e 63 6c 75 62 2e 74 77   ip4.ipv6 .club.tw
```

# 200 OK



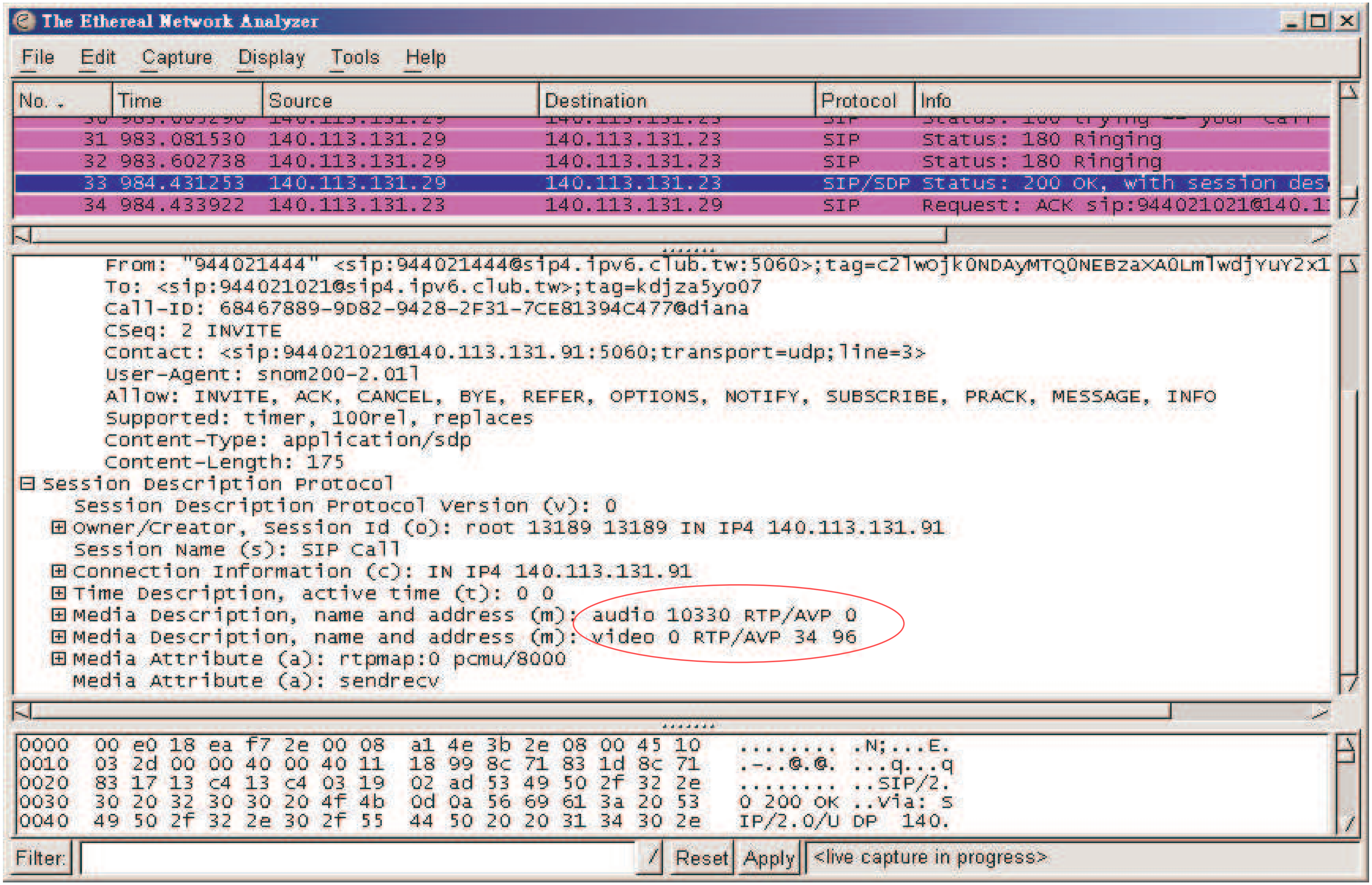
The Ethereal Network Analyzer
File Edit Capture Display Tools Help

```
No. .   Time         Source            Destination       Protocol Info
     31 983.081530   140.113.131.29    140.113.131.23    SIP      Status: 180 Ringing
     32 983.602738   140.113.131.29    140.113.131.23    SIP      Status: 180 Ringing
     33 984.431253   140.113.131.29    140.113.131.23    SIP/SDP  Status: 200 OK, with session des
     34 984.433922   140.113.131.23    140.113.131.29    SIP      Request: ACK sip:944021021@140.11
```

```
⊞ Frame 33 (827 bytes on wire, 827 bytes captured)
⊞ Ethernet II, Src: 00:08:a1:4e:3b:2e, Dst: 00:e0:18:ea:f7:2e
⊞ Internet Protocol, Src Addr: 140.113.131.29 (140.113.131.29), Dst Addr: 140.113.131.23 (140.113.131.23
⊞ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
⊟ Session Initiation Protocol
   ⊞ Status line: SIP/2.0 200 OK
   ⊟ Message Header
       Via: SIP/2.0/UDP  140.113.131.23:5060;branch=z9hG4bKd0e148d625b746088b083163b734f5b1
       From: "944021444" <sip:944021444@sip4.ipv6.club.tw:5060>;tag=c2lwOjk0NDAyMTQ0NEBzaXA0LmlwdjYuY2x1
       To: <sip:944021021@sip4.ipv6.club.tw>;tag=kdjza5yo07
       Call-ID: 68467889-9D82-9428-2F31-7CE81394C477@diana
       CSeq: 2 INVITE
       Contact: <sip:944021021@140.113.131.91:5060;transport=udp;line=3>
       User-Agent: snom200-2.01l
       Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, NOTIFY, SUBSCRIBE, PRACK, MESSAGE, INFO
       Supported: timer, 100rel, replaces
       Content-Type: application/sdp
       Content-Length: 175
⊞ Session Description Protocol
```

```
0000  00 e0 18 ea f7 2e 00 08  a1 4e 3b 2e 08 00 45 10   ........ .N;...E.
0010  03 2d 00 00 40 00 40 11  18 99 8c 71 83 1d 8c 71   .-..@.@. ...q...q
0020  83 17 13 c4 13 c4 03 19  02 ad 53 49 50 2f 32 2e   ........ ..SIP/2.
0030  30 20 32 30 30 20 4f 4b  0d 0a 56 69 61 3a 20 53   0 200 OK ..Via: S
0040  49 50 2f 32 2e 30 2f 55  44 50 20 20 31 34 30 2e   IP/2.0/U DP  140.
```

# SDP in 200 OK

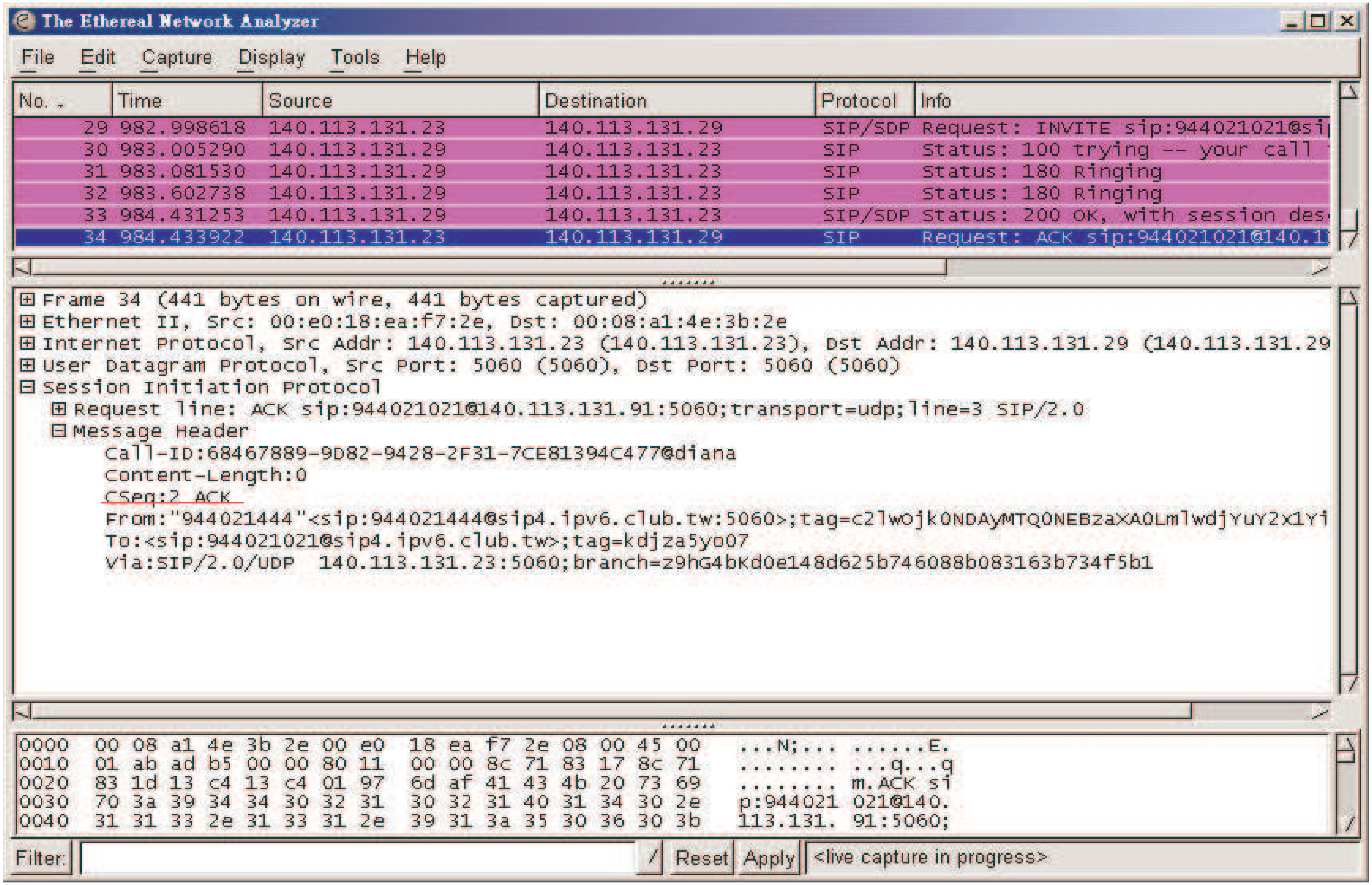

The Ethereal Network Analyzer
File Edit Capture Display Tools Help
Filter:
Reset
Apply
<live capture in progress>

```
No. .  Time        Source           Destination      Protocol Info
    30 983.005290  140.113.131.29   140.113.131.23   SIP      Status: 100 Trying -- your call
    31 983.081530  140.113.131.29   140.113.131.23   SIP      Status: 180 Ringing
    32 983.602738  140.113.131.29   140.113.131.23   SIP      Status: 180 Ringing
    33 984.431253  140.113.131.29   140.113.131.23   SIP/SDP  Status: 200 OK, with session des
    34 984.433922  140.113.131.23   140.113.131.29   SIP      Request: ACK sip:944021021@140.11
```

```
        From: "944021444" <sip:944021444@sip4.ipv6.club.tw:5060>;tag=c2lwOjk0NDAyMTQ0NEBzaXA0LmlwdjYuY2x1
        To: <sip:944021021@sip4.ipv6.club.tw>;tag=kdjza5yo07
        Call-ID: 68467889-9D82-9428-2F31-7CE81394C477@diana
        CSeq: 2 INVITE
        Contact: <sip:944021021@140.113.131.91:5060;transport=udp;line=3>
        User-Agent: snom200-2.01l
        Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, NOTIFY, SUBSCRIBE, PRACK, MESSAGE, INFO
        Supported: timer, 100rel, replaces
        Content-Type: application/sdp
        Content-Length: 175
⊟ Session Description Protocol
      Session Description Protocol Version (v): 0
    ⊞ Owner/Creator, Session Id (o): root 13189 13189 IN IP4 140.113.131.91
      Session Name (s): SIP Call
    ⊞ Connection Information (c): IN IP4 140.113.131.91
    ⊞ Time Description, active time (t): 0 0
    ⊞ Media Description, name and address (m): audio 10330 RTP/AVP 0
    ⊞ Media Description, name and address (m): video 0 RTP/AVP 34 96
    ⊞ Media Attribute (a): rtpmap:0 pcmu/8000
      Media Attribute (a): sendrecv
```

```
0000  00 e0 18 ea f7 2e 00 08  a1 4e 3b 2e 08 00 45 10   ........ .N;...E.
0010  03 2d 00 00 40 00 40 11  18 99 8c 71 83 1d 8c 71   .-..@.@. ...q...q
0020  83 17 13 c4 13 c4 03 19  02 ad 53 49 50 2f 32 2e   ........ ..SIP/2.
0030  30 20 32 30 30 20 4f 4b  0d 0a 56 69 61 3a 20 53   0 200 OK ..Via: S
0040  49 50 2f 32 2e 30 2f 55  44 50 20 20 31 34 30 2e   IP/2.0/U DP  140.
```

# ACK



```
No. .  Time        Source           Destination      Protocol Info
    29 982.998618  140.113.131.23   140.113.131.29   SIP/SDP  Request: INVITE sip:944021021@si
    30 983.005290  140.113.131.29   140.113.131.23   SIP      Status: 100 trying -- your call
    31 983.081530  140.113.131.29   140.113.131.23   SIP      Status: 180 Ringing
    32 983.602738  140.113.131.29   140.113.131.23   SIP      Status: 180 Ringing
    33 984.431253  140.113.131.29   140.113.131.23   SIP/SDP  Status: 200 OK, with session des
    34 984.433922  140.113.131.23   140.113.131.29   SIP      Request: ACK sip:944021021@140.1
```

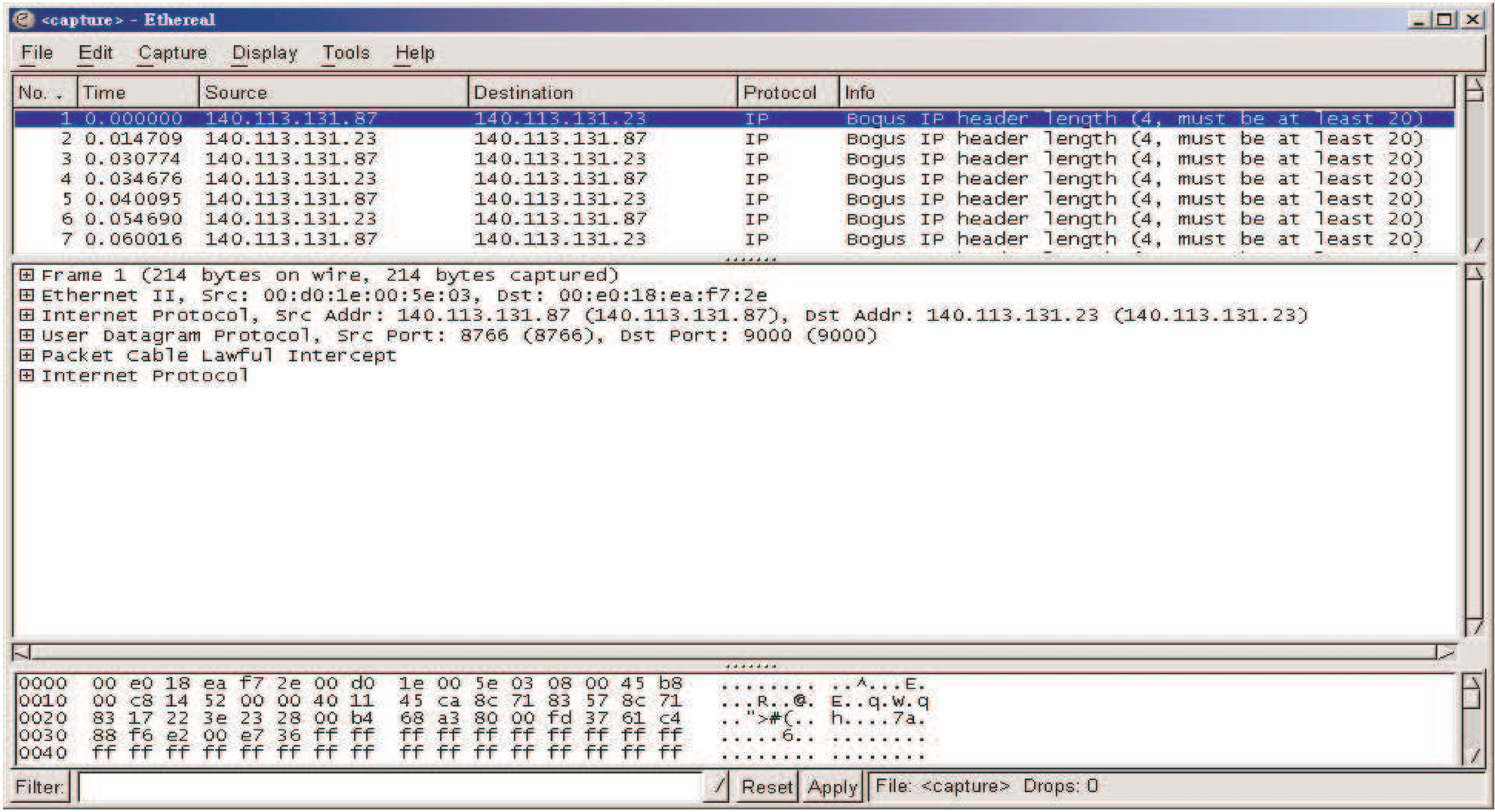
```
⊞ Frame 34 (441 bytes on wire, 441 bytes captured)
⊞ Ethernet II, Src: 00:e0:18:ea:f7:2e, Dst: 00:08:a1:4e:3b:2e
⊞ Internet Protocol, Src Addr: 140.113.131.23 (140.113.131.23), Dst Addr: 140.113.131.29 (140.113.131.29
⊞ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
⊟ Session Initiation Protocol
   ⊞ Request line: ACK sip:944021021@140.113.131.91:5060;transport=udp;line=3 SIP/2.0
   ⊟ Message Header
        Call-ID:68467889-9D82-9428-2F31-7CE81394C477@diana
        Content-Length:0
        CSeq:2 ACK
        From:"944021444"<sip:944021444@sip4.ipv6.club.tw:5060>;tag=c2lwOjkONDAyMTQONEBzaXAOLmlwdjYuY2x1Yi
        To:<sip:944021021@sip4.ipv6.club.tw>;tag=kdjza5yo07
        Via:SIP/2.0/UDP  140.113.131.23:5060;branch=z9hG4bKd0e148d625b746088b083163b734f5b1
```

```
0000  00 08 a1 4e 3b 2e 00 e0  18 ea f7 2e 08 00 45 00   ...N;... ......E.
0010  01 ab ad b5 00 00 80 11  00 00 8c 71 83 17 8c 71   ........ ...q...q
0020  83 1d 13 c4 13 c4 01 97  6d af 41 43 4b 20 73 69   ........ m.ACK si
0030  70 3a 39 34 34 30 32 31  30 32 31 40 31 34 30 2e   p:944021 021@140.
0040  31 31 33 2e 31 33 31 2e  39 31 3a 35 30 36 30 3b   113.131. 91:5060;
```

<live capture in progress>

# Capturing the packets of Media Data

# RTP Traffic (udp port 9000)



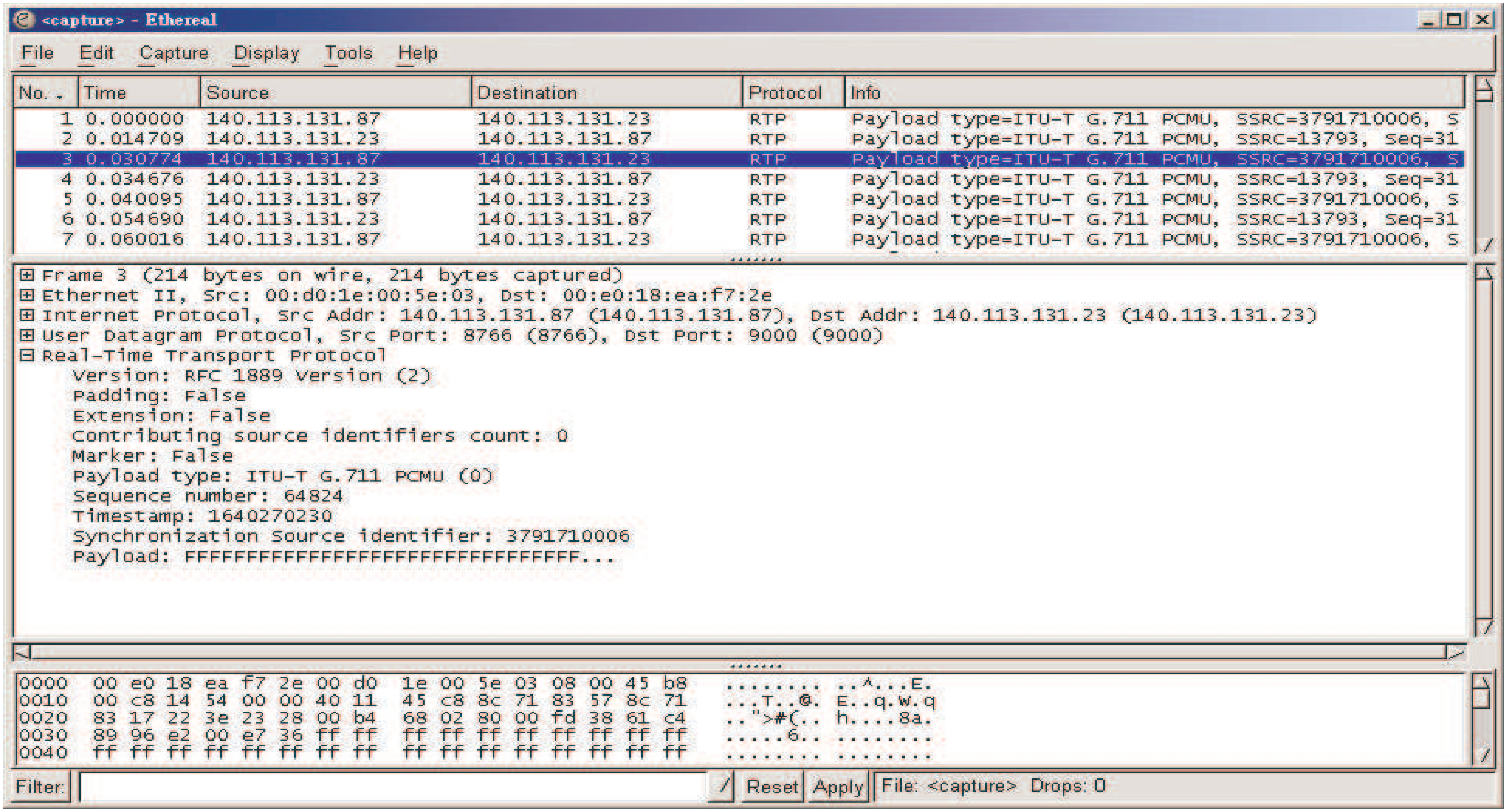
```
No. . Time      Source          Destination     Protocol Info
    1 0.000000  140.113.131.87  140.113.131.23  IP       Bogus IP header length (4, must be at least 20)
    2 0.014709  140.113.131.23  140.113.131.87  IP       Bogus IP header length (4, must be at least 20)
    3 0.030774  140.113.131.87  140.113.131.23  IP       Bogus IP header length (4, must be at least 20)
    4 0.034676  140.113.131.23  140.113.131.87  IP       Bogus IP header length (4, must be at least 20)
    5 0.040095  140.113.131.87  140.113.131.23  IP       Bogus IP header length (4, must be at least 20)
    6 0.054690  140.113.131.23  140.113.131.87  IP       Bogus IP header length (4, must be at least 20)
    7 0.060016  140.113.131.87  140.113.131.23  IP       Bogus IP header length (4, must be at least 20)
```

```
⊞ Frame 1 (214 bytes on wire, 214 bytes captured)
⊞ Ethernet II, Src: 00:d0:1e:00:5e:03, Dst: 00:e0:18:ea:f7:2e
⊞ Internet Protocol, Src Addr: 140.113.131.87 (140.113.131.87), Dst Addr: 140.113.131.23 (140.113.131.23)
⊞ User Datagram Protocol, Src Port: 8766 (8766), Dst Port: 9000 (9000)
⊞ Packet Cable Lawful Intercept
⊞ Internet Protocol
```

```
0000  00 e0 18 ea f7 2e 00 d0  1e 00 5e 03 08 00 45 b8   ........ ..^...E.
0010  00 c8 14 52 00 00 40 11  45 ca 8c 71 83 57 8c 71   ...R..@. E..q.W.q
0020  83 17 22 3e 23 28 00 b4  68 a3 80 00 fd 37 61 c4   ..">#(.. h....7a.
0030  88 f6 e2 00 e7 36 ff ff  ff ff ff ff ff ff ff ff   .....6.. ........
0040  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff   ........ ........
```

- What’s wrong?

# Tools – Decode As RTP

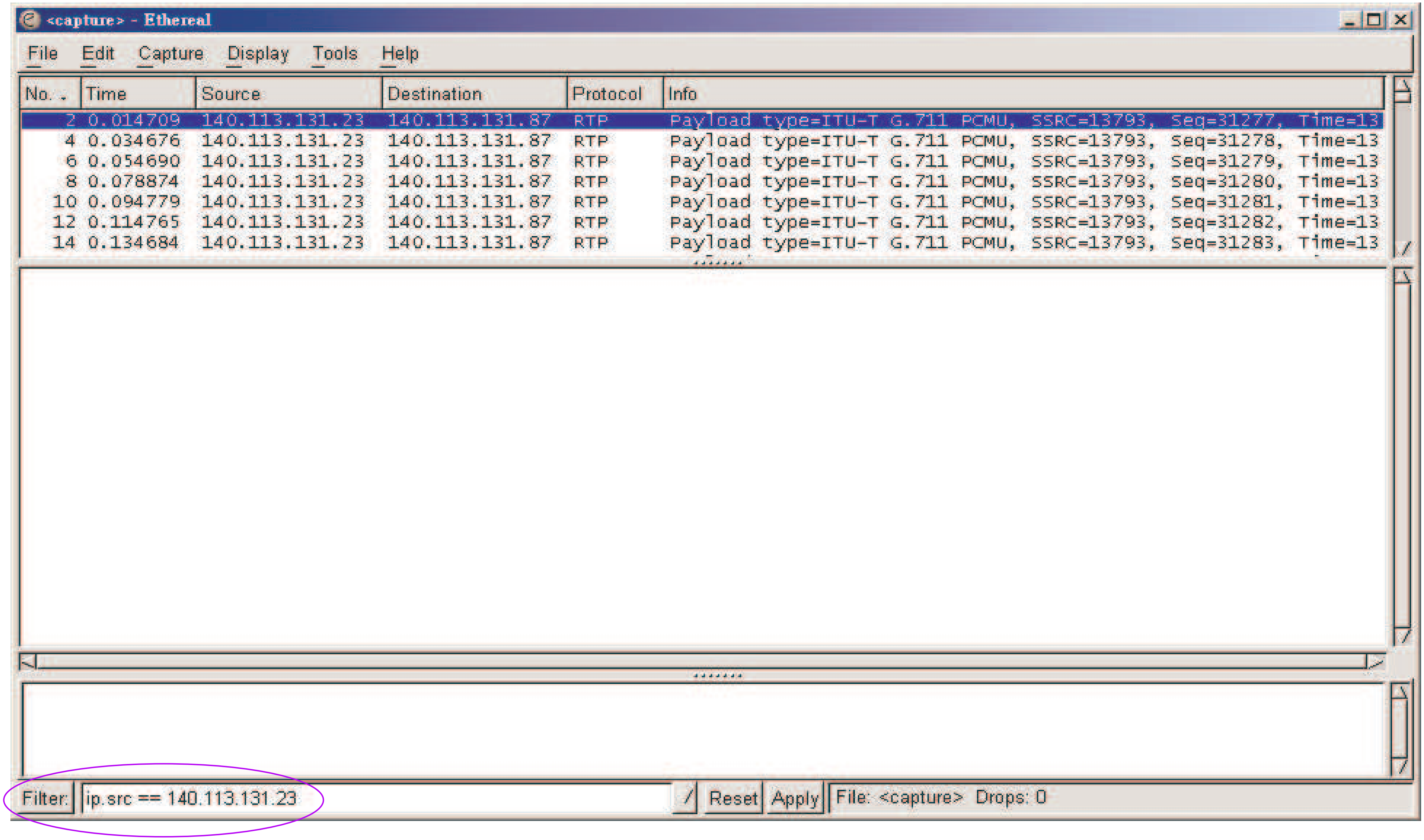


```
No. .  Time      Source           Destination      Protocol  Info
    1 0.000000  140.113.131.87   140.113.131.23   RTP       Payload type=ITU-T G.711 PCMU, SSRC=3791710006, S
    2 0.014709  140.113.131.23   140.113.131.87   RTP       Payload type=ITU-T G.711 PCMU, SSRC=13793, Seq=31
    3 0.030774  140.113.131.87   140.113.131.23   RTP       Payload type=ITU-T G.711 PCMU, SSRC=3791710006, S
    4 0.034676  140.113.131.23   140.113.131.87   RTP       Payload type=ITU-T G.711 PCMU, SSRC=13793, Seq=31
    5 0.040095  140.113.131.87   140.113.131.23   RTP       Payload type=ITU-T G.711 PCMU, SSRC=3791710006, S
    6 0.054690  140.113.131.23   140.113.131.87   RTP       Payload type=ITU-T G.711 PCMU, SSRC=13793, Seq=31
    7 0.060016  140.113.131.87   140.113.131.23   RTP       Payload type=ITU-T G.711 PCMU, SSRC=3791710006, S
```

```
⊞ Frame 3 (214 bytes on wire, 214 bytes captured)
⊞ Ethernet II, Src: 00:d0:1e:00:5e:03, Dst: 00:e0:18:ea:f7:2e
⊞ Internet Protocol, Src Addr: 140.113.131.87 (140.113.131.87), Dst Addr: 140.113.131.23 (140.113.131.23)
⊞ User Datagram Protocol, Src Port: 8766 (8766), Dst Port: 9000 (9000)
⊟ Real-Time Transport Protocol
    Version: RFC 1889 Version (2)
    Padding: False
    Extension: False
    Contributing source identifiers count: 0
    Marker: False
    Payload type: ITU-T G.711 PCMU (0)
    Sequence number: 64824
    Timestamp: 1640270230
    Synchronization Source identifier: 3791710006
    Payload: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF...
```

```
0000  00 e0 18 ea f7 2e 00 d0  1e 00 5e 03 08 00 45 b8   ........ ..^...E.
0010  00 c8 14 54 00 00 40 11  45 c8 8c 71 83 57 8c 71   ...T..@. E..q.W.q
0020  83 17 22 3e 23 28 00 b4  68 02 80 00 fd 38 61 c4   ..">#(.. h....8a.
0030  89 96 e2 00 e7 36 ff ff  ff ff ff ff ff ff ff ff   .....6.. ........
0040  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff   ........ ........
```

# Display Filter

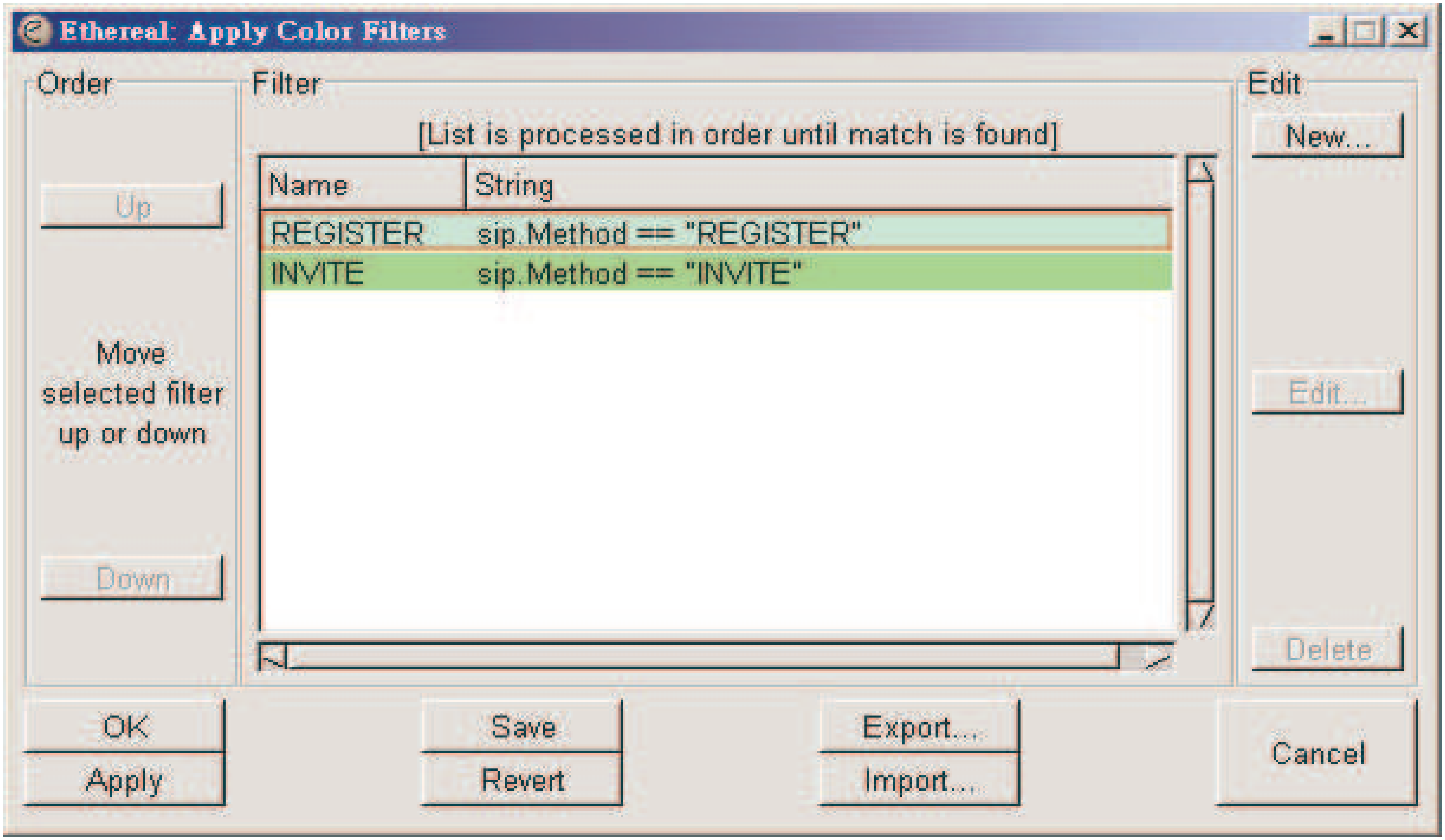


```
No. .  Time      Source          Destination     Protocol  Info
  2 0.014709  140.113.131.23  140.113.131.87  RTP       Payload type=ITU-T G.711 PCMU, SSRC=13793, Seq=31277, Time=13
  4 0.034676  140.113.131.23  140.113.131.87  RTP       Payload type=ITU-T G.711 PCMU, SSRC=13793, Seq=31278, Time=13
  6 0.054690  140.113.131.23  140.113.131.87  RTP       Payload type=ITU-T G.711 PCMU, SSRC=13793, Seq=31279, Time=13
  8 0.078874  140.113.131.23  140.113.131.87  RTP       Payload type=ITU-T G.711 PCMU, SSRC=13793, Seq=31280, Time=13
 10 0.094779  140.113.131.23  140.113.131.87  RTP       Payload type=ITU-T G.711 PCMU, SSRC=13793, Seq=31281, Time=13
 12 0.114765  140.113.131.23  140.113.131.87  RTP       Payload type=ITU-T G.711 PCMU, SSRC=13793, Seq=31282, Time=13
 14 0.134684  140.113.131.23  140.113.131.87  RTP       Payload type=ITU-T G.711 PCMU, SSRC=13793, Seq=31283, Time=13
```

Filter: ip.src == 140.113.131.23

File: <capture>  Drops: 0

# Display – Colorize Display

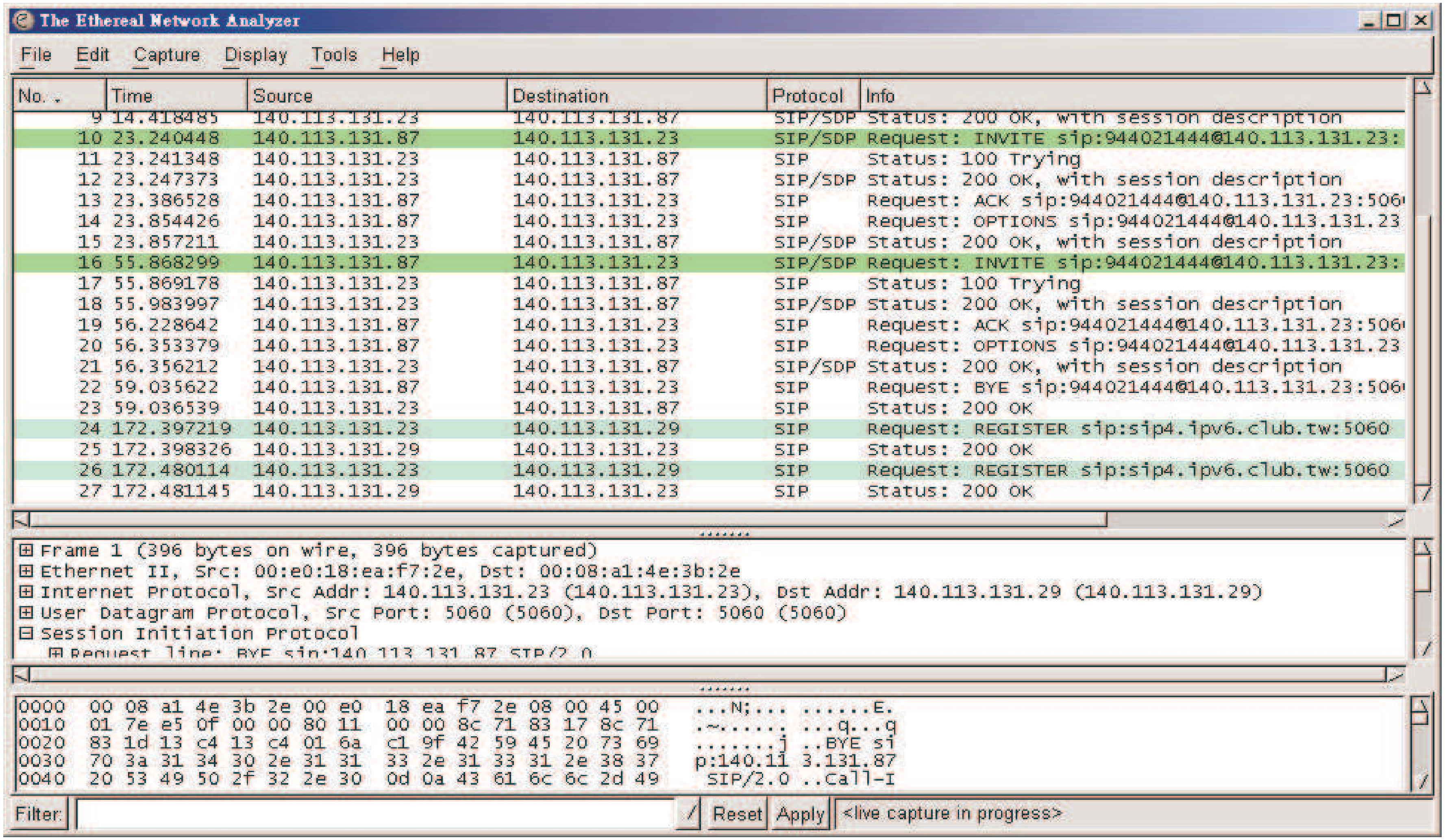

Ethereal: Apply Color Filters

[List is processed in order until match is found]

| Name | String |
|---|---|
| REGISTER | sip.Method == "REGISTER" |
| INVITE | sip.Method == "INVITE" |

Move selected filter up or down

# Emphasize the packets you are interested in

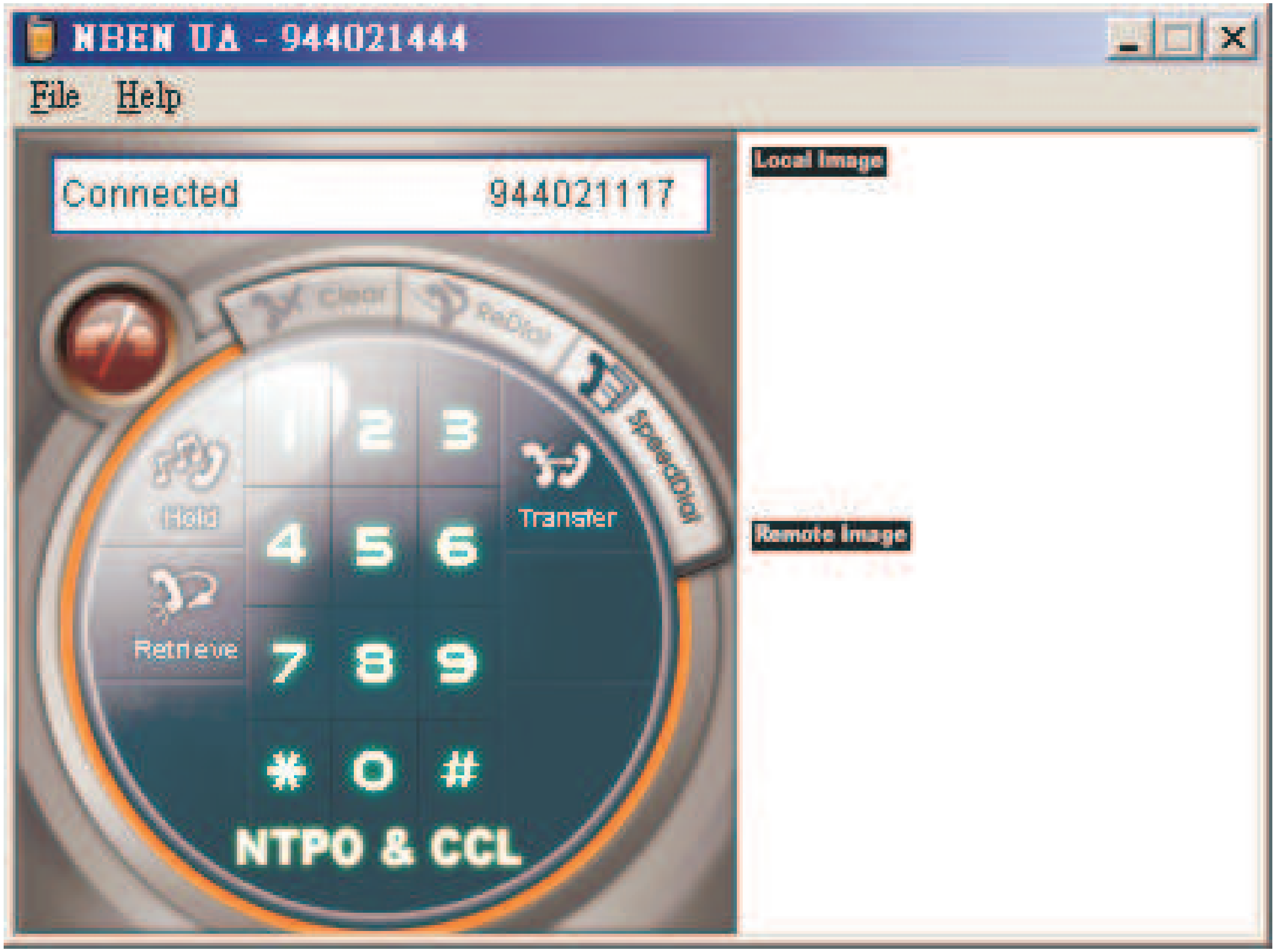

The Ethereal Network Analyzer
File Edit Capture Display Tools Help
Filter:
Reset
Apply
<live capture in progress>

```
No. .  Time        Source          Destination     Protocol Info
    9 14.418485   140.113.131.23  140.113.131.87  SIP/SDP  Status: 200 OK, with session description
   10 23.240448   140.113.131.87  140.113.131.23  SIP/SDP  Request: INVITE sip:944021444@140.113.131.23:
   11 23.241348   140.113.131.23  140.113.131.87  SIP      Status: 100 Trying
   12 23.247373   140.113.131.23  140.113.131.87  SIP/SDP  Status: 200 OK, with session description
   13 23.386528   140.113.131.87  140.113.131.23  SIP      Request: ACK sip:944021444@140.113.131.23:506
   14 23.854426   140.113.131.87  140.113.131.23  SIP      Request: OPTIONS sip:944021444@140.113.131.23
   15 23.857211   140.113.131.23  140.113.131.87  SIP/SDP  Status: 200 OK, with session description
   16 55.868299   140.113.131.87  140.113.131.23  SIP/SDP  Request: INVITE sip:944021444@140.113.131.23:
   17 55.869178   140.113.131.23  140.113.131.87  SIP      Status: 100 Trying
   18 55.983997   140.113.131.23  140.113.131.87  SIP/SDP  Status: 200 OK, with session description
   19 56.228642   140.113.131.87  140.113.131.23  SIP      Request: ACK sip:944021444@140.113.131.23:506
   20 56.353379   140.113.131.87  140.113.131.23  SIP      Request: OPTIONS sip:944021444@140.113.131.23
   21 56.356212   140.113.131.23  140.113.131.87  SIP/SDP  Status: 200 OK, with session description
   22 59.035622   140.113.131.87  140.113.131.23  SIP      Request: BYE sip:944021444@140.113.131.23:506
   23 59.036539   140.113.131.23  140.113.131.87  SIP      Status: 200 OK
   24 172.397219  140.113.131.23  140.113.131.29  SIP      Request: REGISTER sip:sip4.ipv6.club.tw:5060
   25 172.398326  140.113.131.29  140.113.131.23  SIP      Status: 200 OK
   26 172.480114  140.113.131.23  140.113.131.29  SIP      Request: REGISTER sip:sip4.ipv6.club.tw:5060
   27 172.481145  140.113.131.29  140.113.131.23  SIP      Status: 200 OK
```

```
⊞ Frame 1 (396 bytes on wire, 396 bytes captured)
⊞ Ethernet II, Src: 00:e0:18:ea:f7:2e, Dst: 00:08:a1:4e:3b:2e
⊞ Internet Protocol, Src Addr: 140.113.131.23 (140.113.131.23), Dst Addr: 140.113.131.29 (140.113.131.29)
⊞ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
⊟ Session Initiation Protocol
   ⊞ Request line: BYE sip:140.113.131.87 SIP/2.0
```

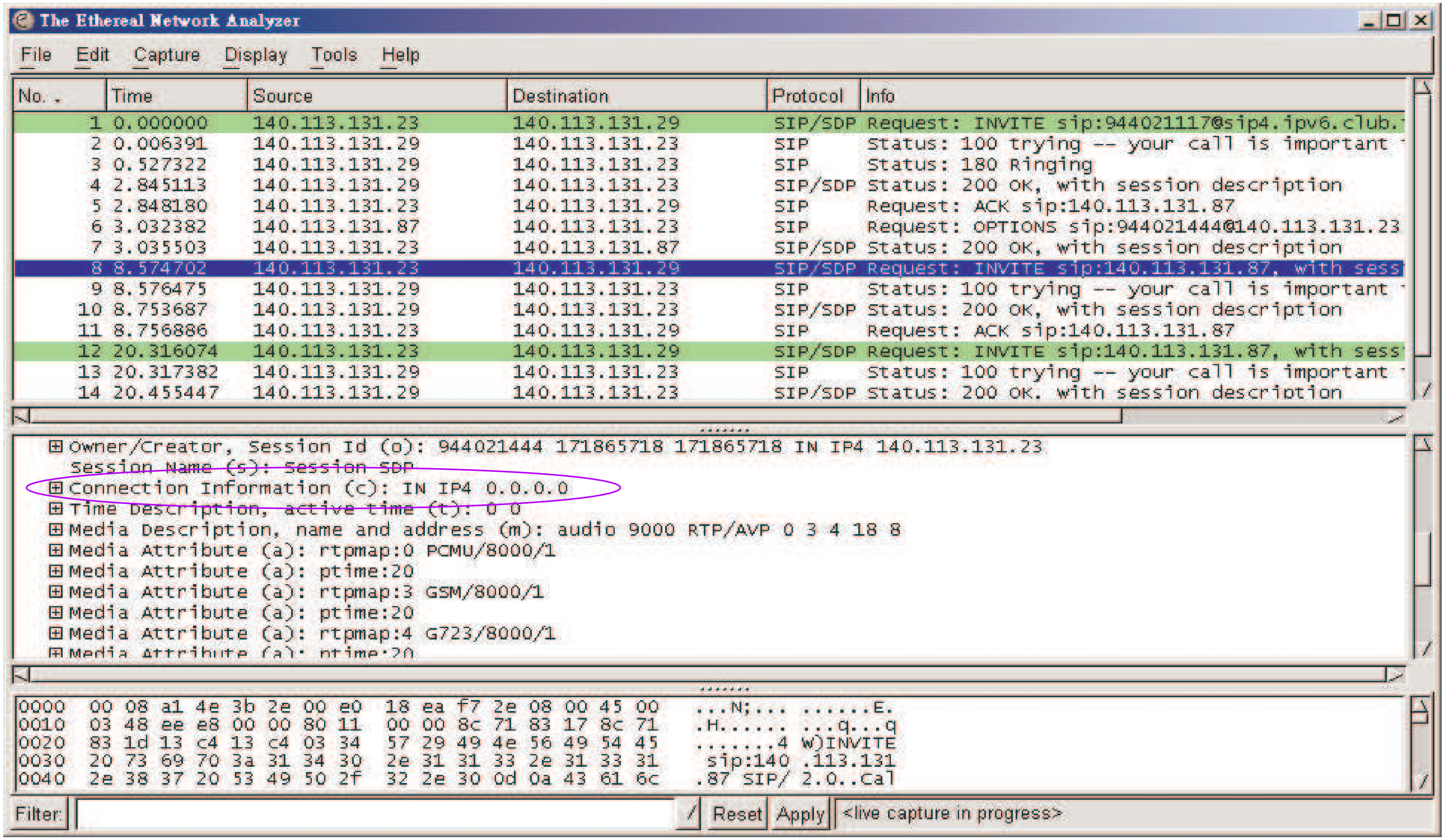
```
0000  00 08 a1 4e 3b 2e 00 e0  18 ea f7 2e 08 00 45 00   ...N;... ......E.
0010  01 7e e5 0f 00 00 80 11  00 00 8c 71 83 17 8c 71   .~...... ...q...q
0020  83 1d 13 c4 13 c4 01 6a  c1 9f 42 59 45 20 73 69   .......j ..BYE si
0030  70 3a 31 34 30 2e 31 31  33 2e 31 33 31 2e 38 37   p:140.11 3.131.87
0040  20 53 49 50 2f 32 2e 30  0d 0a 43 61 6c 6c 2d 49    SIP/2.0 ..Call-I
```

# Hold/Unhold of NBEN UA



Connected 944021117

# Hold



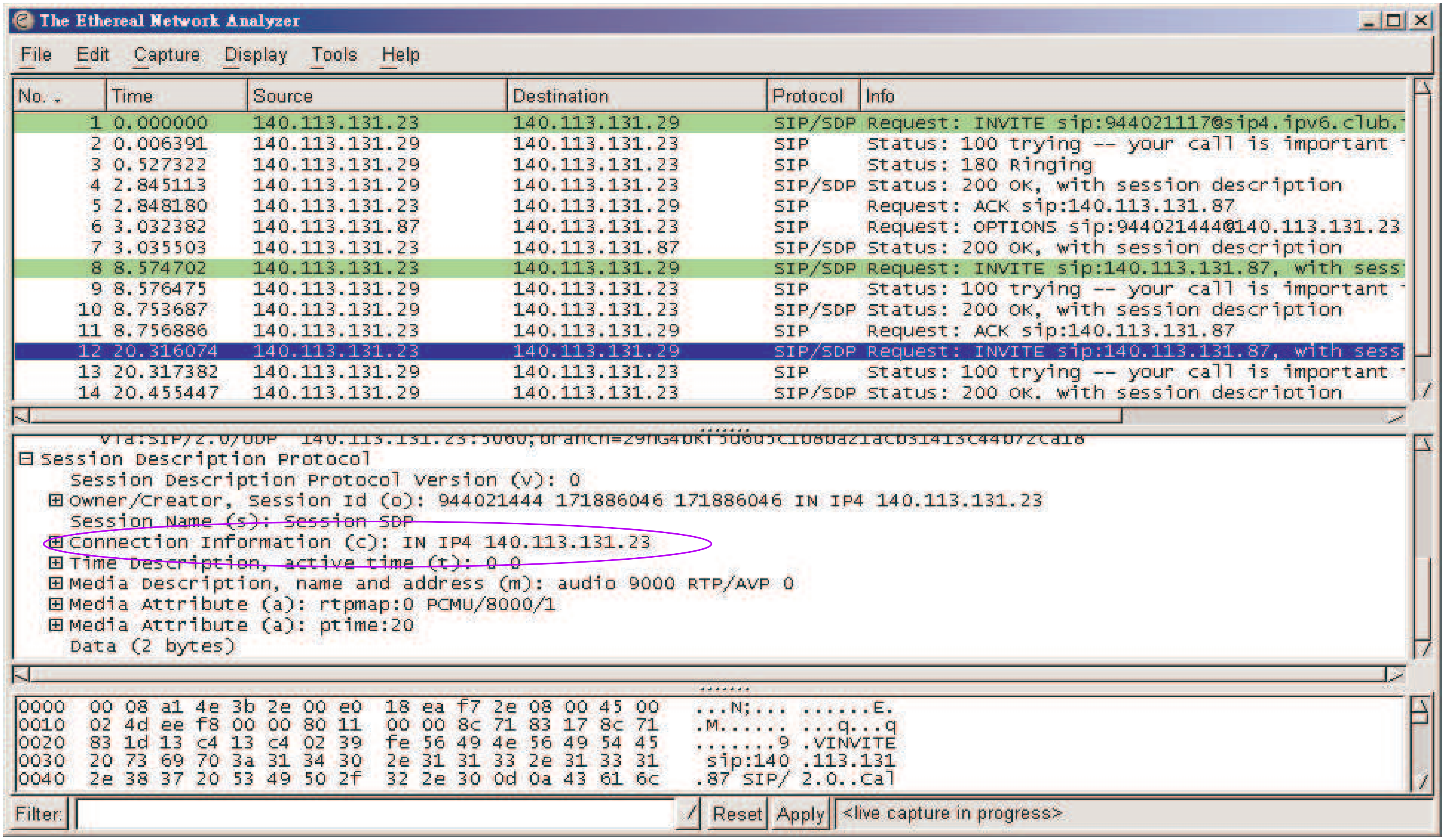
```
No. .  Time       Source          Destination     Protocol Info
     1 0.000000   140.113.131.23  140.113.131.29  SIP/SDP  Request: INVITE sip:944021117@sip4.ipv6.club.
     2 0.006391   140.113.131.29  140.113.131.23  SIP      Status: 100 trying -- your call is important
     3 0.527322   140.113.131.29  140.113.131.23  SIP      Status: 180 Ringing
     4 2.845113   140.113.131.29  140.113.131.23  SIP/SDP  Status: 200 OK, with session description
     5 2.848180   140.113.131.23  140.113.131.29  SIP      Request: ACK sip:140.113.131.87
     6 3.032382   140.113.131.87  140.113.131.23  SIP      Request: OPTIONS sip:944021444@140.113.131.23
     7 3.035503   140.113.131.23  140.113.131.87  SIP/SDP  Status: 200 OK, with session description
     8 8.574702   140.113.131.23  140.113.131.29  SIP/SDP  Request: INVITE sip:140.113.131.87, with sess
     9 8.576475   140.113.131.29  140.113.131.23  SIP      Status: 100 trying -- your call is important
    10 8.753687   140.113.131.29  140.113.131.23  SIP/SDP  Status: 200 OK, with session description
    11 8.756886   140.113.131.23  140.113.131.29  SIP      Request: ACK sip:140.113.131.87
    12 20.316074  140.113.131.23  140.113.131.29  SIP/SDP  Request: INVITE sip:140.113.131.87, with sess
    13 20.317382  140.113.131.29  140.113.131.23  SIP      Status: 100 trying -- your call is important
    14 20.455447  140.113.131.29  140.113.131.23  SIP/SDP  Status: 200 OK. with session description
```

```
  ⊞ Owner/Creator, Session Id (o): 944021444 171865718 171865718 IN IP4 140.113.131.23
    Session Name (s): Session SDP
  ⊞ Connection Information (c): IN IP4 0.0.0.0
  ⊞ Time Description, active time (t): 0 0
  ⊞ Media Description, name and address (m): audio 9000 RTP/AVP 0 3 4 18 8
  ⊞ Media Attribute (a): rtpmap:0 PCMU/8000/1
  ⊞ Media Attribute (a): ptime:20
  ⊞ Media Attribute (a): rtpmap:3 GSM/8000/1
  ⊞ Media Attribute (a): ptime:20
  ⊞ Media Attribute (a): rtpmap:4 G723/8000/1
  ⊞ Media Attribute (a): ptime:20
```

```
0000  00 08 a1 4e 3b 2e 00 e0  18 ea f7 2e 08 00 45 00   ...N;... ......E.
0010  03 48 ee e8 00 00 80 11  00 00 8c 71 83 17 8c 71   .H...... ...q...q
0020  83 1d 13 c4 13 c4 03 34  57 29 49 4e 56 49 54 45   .......4 W)INVITE
0030  20 73 69 70 3a 31 34 30  2e 31 31 33 2e 31 33 31    sip:140 .113.131
0040  2e 38 37 20 53 49 50 2f  32 2e 30 0d 0a 43 61 6c   .87 SIP/ 2.0..Cal
```

<live capture in progress>

# Retrieve



```
No. .  Time       Source           Destination      Protocol Info
     1 0.000000   140.113.131.23   140.113.131.29   SIP/SDP  Request: INVITE sip:944021117@sip4.ipv6.club.
     2 0.006391   140.113.131.29   140.113.131.23   SIP      Status: 100 trying -- your call is important
     3 0.527322   140.113.131.29   140.113.131.23   SIP      Status: 180 Ringing
     4 2.845113   140.113.131.29   140.113.131.23   SIP/SDP  Status: 200 OK, with session description
     5 2.848180   140.113.131.23   140.113.131.29   SIP      Request: ACK sip:140.113.131.87
     6 3.032382   140.113.131.87   140.113.131.23   SIP      Request: OPTIONS sip:944021444@140.113.131.23
     7 3.035503   140.113.131.23   140.113.131.87   SIP/SDP  Status: 200 OK, with session description
     8 8.574702   140.113.131.23   140.113.131.29   SIP/SDP  Request: INVITE sip:140.113.131.87, with sess
     9 8.576475   140.113.131.29   140.113.131.23   SIP      Status: 100 trying -- your call is important
    10 8.753687   140.113.131.29   140.113.131.23   SIP/SDP  Status: 200 OK, with session description
    11 8.756886   140.113.131.23   140.113.131.29   SIP      Request: ACK sip:140.113.131.87
    12 20.316074  140.113.131.23   140.113.131.29   SIP/SDP  Request: INVITE sip:140.113.131.87, with sess
    13 20.317382  140.113.131.29   140.113.131.23   SIP      Status: 100 trying -- your call is important
    14 20.455447  140.113.131.29   140.113.131.23   SIP/SDP  Status: 200 OK, with session description
```

```
      Via: SIP/2.0/UDP  140.113.131.23:5060;branch=z9hG4bKf5d6d5c1b8ba21acb31413c44b72ca18
⊟ Session Description Protocol
     Session Description Protocol Version (v): 0
   ⊞ Owner/Creator, Session Id (o): 944021444 171886046 171886046 IN IP4 140.113.131.23
     Session Name (s): Session SDP
   ⊞ Connection Information (c): IN IP4 140.113.131.23
   ⊞ Time Description, active time (t): 0 0
   ⊞ Media Description, name and address (m): audio 9000 RTP/AVP 0
   ⊞ Media Attribute (a): rtpmap:0 PCMU/8000/1
   ⊞ Media Attribute (a): ptime:20
     Data (2 bytes)
```

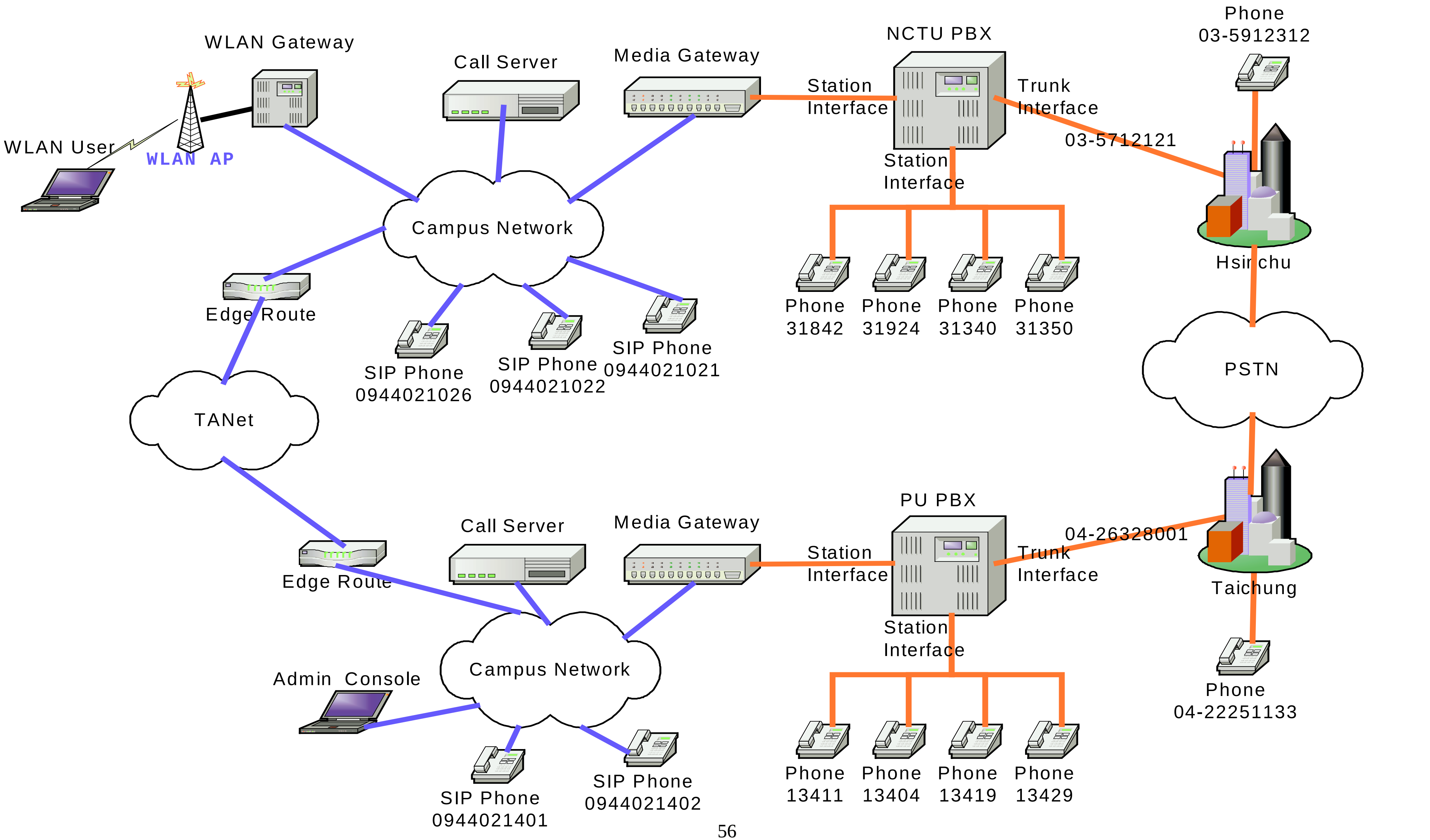
```
0000  00 08 a1 4e 3b 2e 00 e0  18 ea f7 2e 08 00 45 00   ...N;... ......E.
0010  02 4d ee f8 00 00 80 11  00 00 8c 71 83 17 8c 71   .M...... ...q...q
0020  83 1d 13 c4 13 c4 02 39  fe 56 49 4e 56 49 54 45   .......9 .VINVITE
0030  20 73 69 70 3a 31 34 30  2e 31 31 33 2e 31 33 31    sip:140 .113.131
0040  2e 38 37 20 53 49 50 2f  32 2e 30 0d 0a 43 61 6c   .87 SIP/ 2.0..Cal
```

<live capture in progress>

# Summary

- We demonstrate the functions of Windows Messenger and NBEN UA, which are two SIP User Agents with friendly user interface.
- We demonstrate the functions of Ethereal, which is a powerful tool for packets capturing & analyzing:
  - Capture Filters
  - Colorized Packets
- Practice using this tool to capture SIP signaling in the following call flows
  - REGISTER – 200 OK
  - INVITE – 200 OK - ACK
  - BYE – 200 OK
  - Hold/Retrieve

# NTP VoIP Platform


WLAN Gateway
WLAN User
WLAN AP
Call Server
Media Gateway
NCTU PBX
Station Interface
Trunk Interface
Station Interface
Phone 03-5912312
03-5712121
Campus Network
Edge Route
TANet
SIP Phone 0944021026
SIP Phone 0944021022
SIP Phone 0944021021
Phone 31842
Phone 31924
Phone 31340
Phone 31350
Hsinchu
PSTN
Edge Route
Call Server
Media Gateway
PU PBX
Station Interface
Trunk Interface
04-26328001
Station Interface
Taichung
Admin Console
Campus Network
SIP Phone 0944021401
SIP Phone 0944021402
Phone 13411
Phone 13404
Phone 13419
Phone 13429
Phone 04-22251133