

# Lab Hours

- We need to allocate 3 hours in this week for hands-on lab hours (March 23<sup>rd</sup> 09:10-12:00).
- The instructor will set up the SIP server.
- Every student will bring a labtop or desktop PC and install a SIP UA (softphone). It will be even better if you have a WiFi-phone.
- 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](mailto:solomon@ipv6.club.tw)

# Exercise 1: SIP UA operations

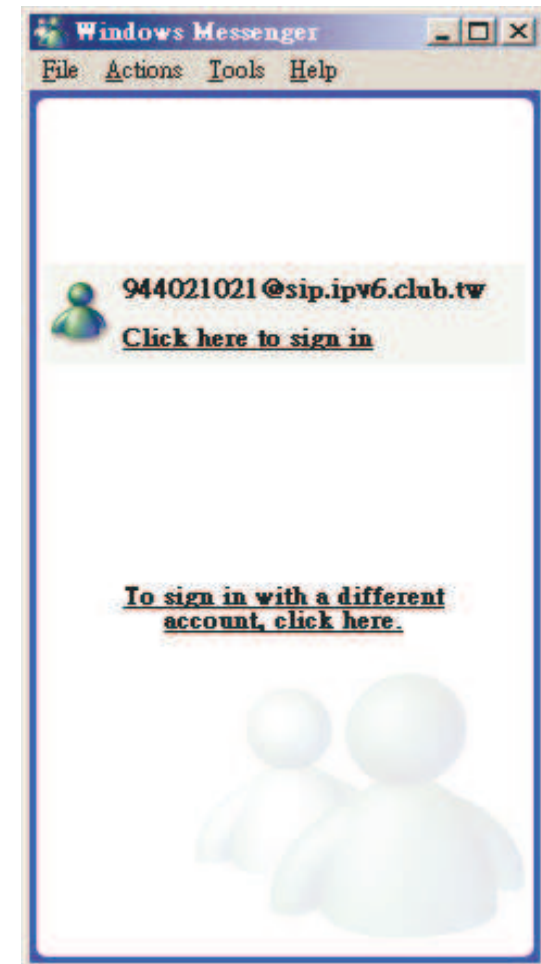
- Download & Install SIP UA
- Download & Install Ethereal
- Packet Analysis Using Ethereal
  - SIP signaling flow
  - RTP traffic
  - SIP headers
  - SDP Contents
  - Call Hold/Retrieve

# Windows-based SIP UA

- Microsoft Windows Messenger
- X-Lite

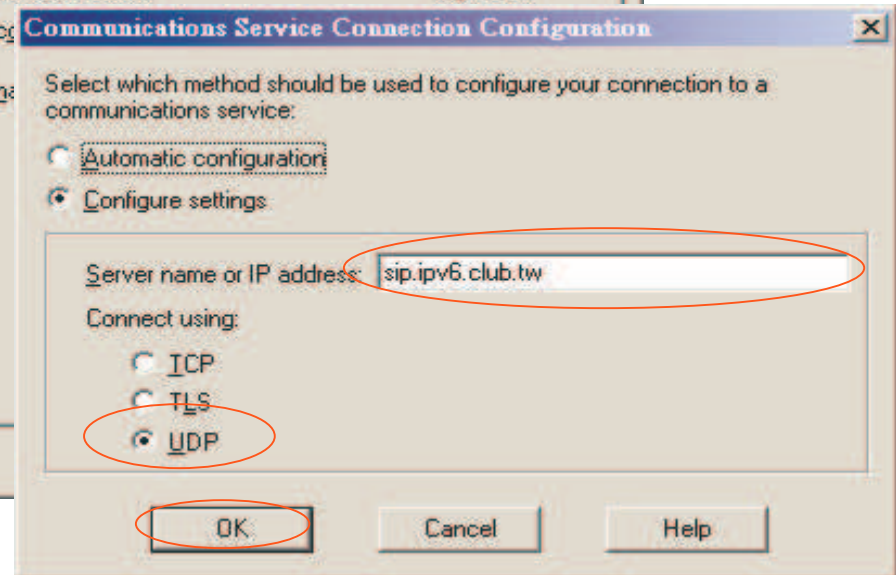
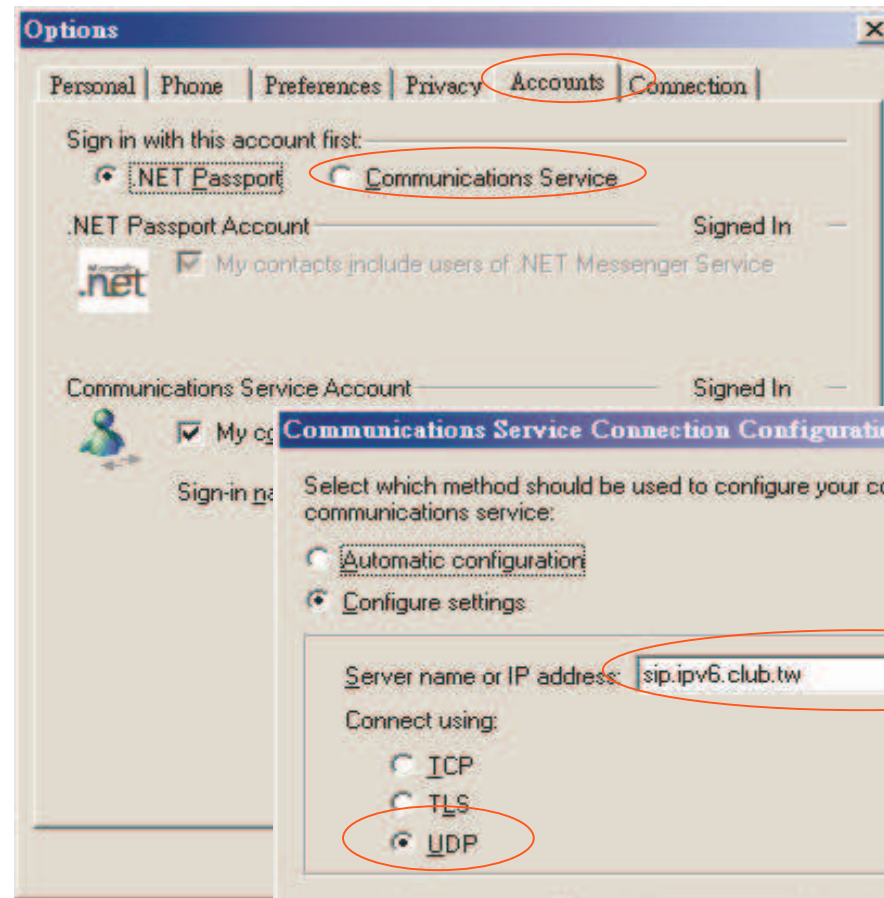
# SIP UA – Windows Messenger

- 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/winxpro/evaluate/insid01.msp>



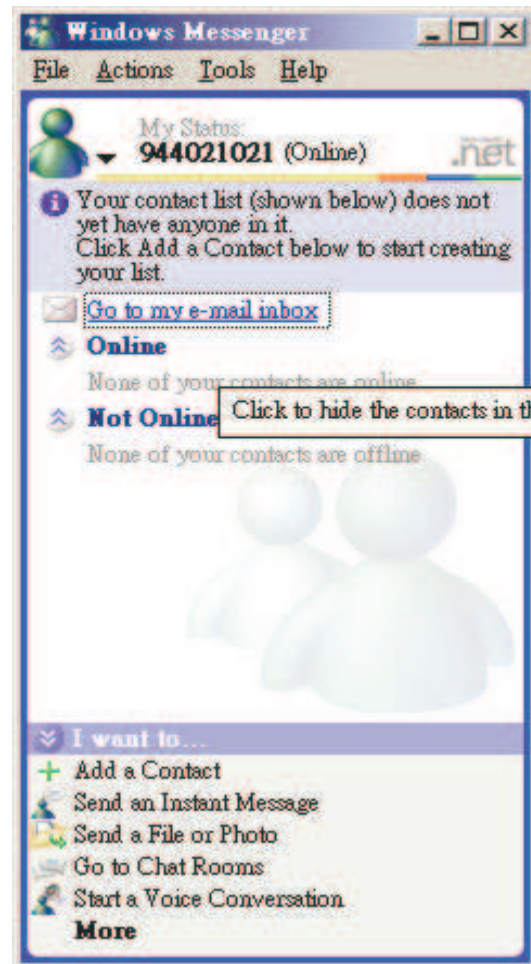


# Step 1: Configure



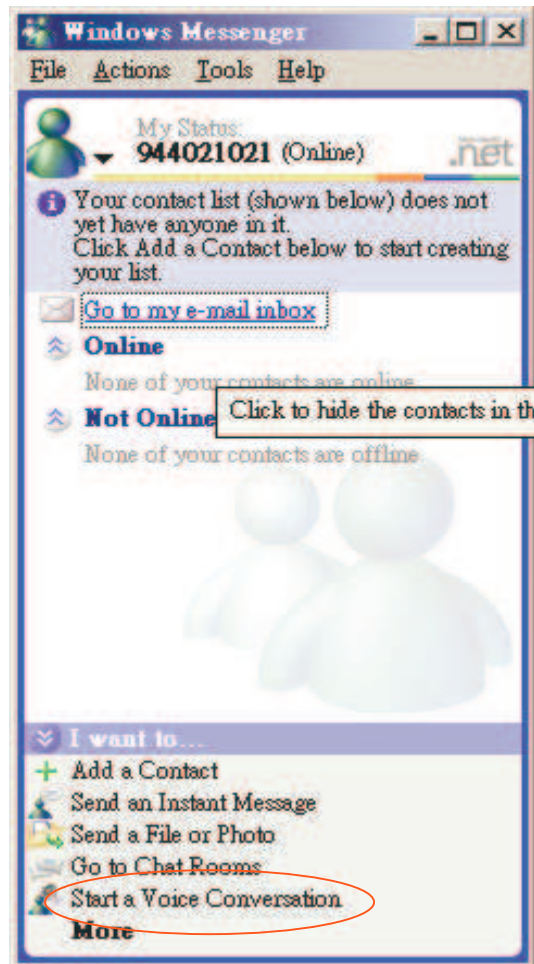


# Step 2: REGISTER





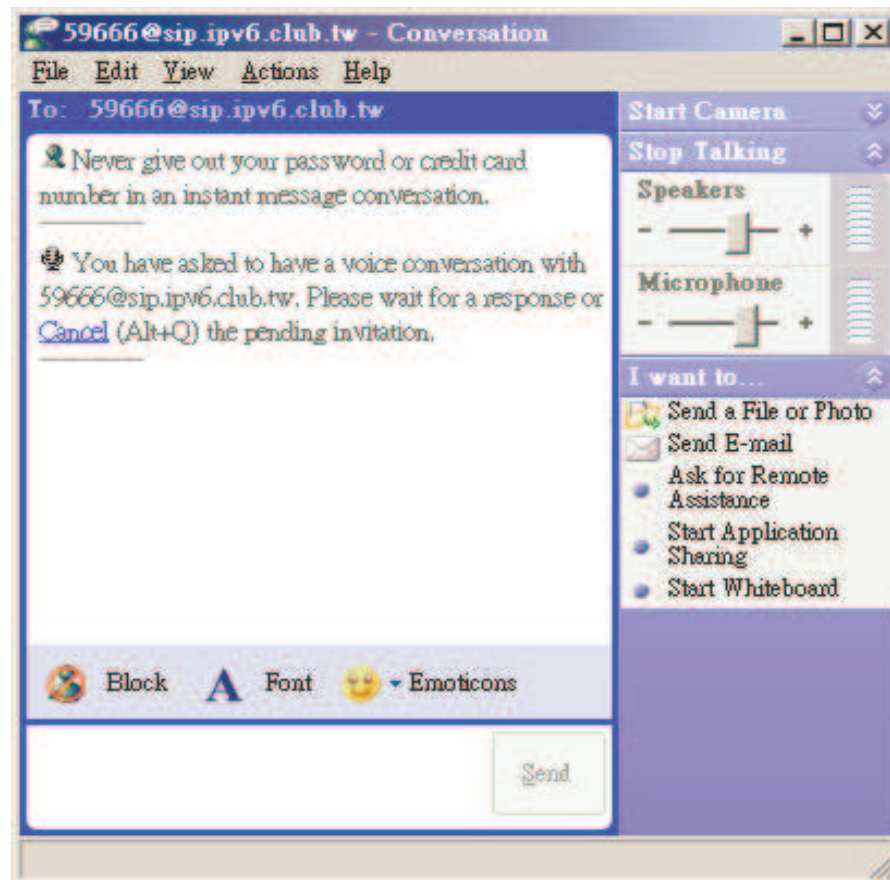
# Step 3: Make A Call





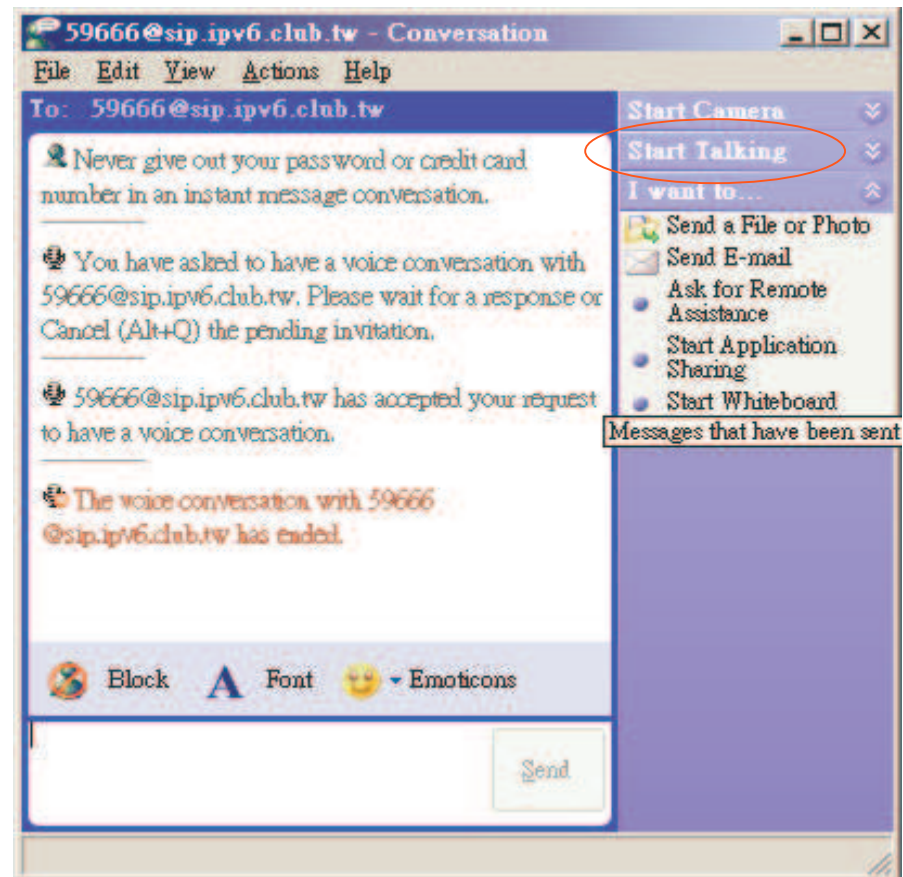


# Step 4: Ringing



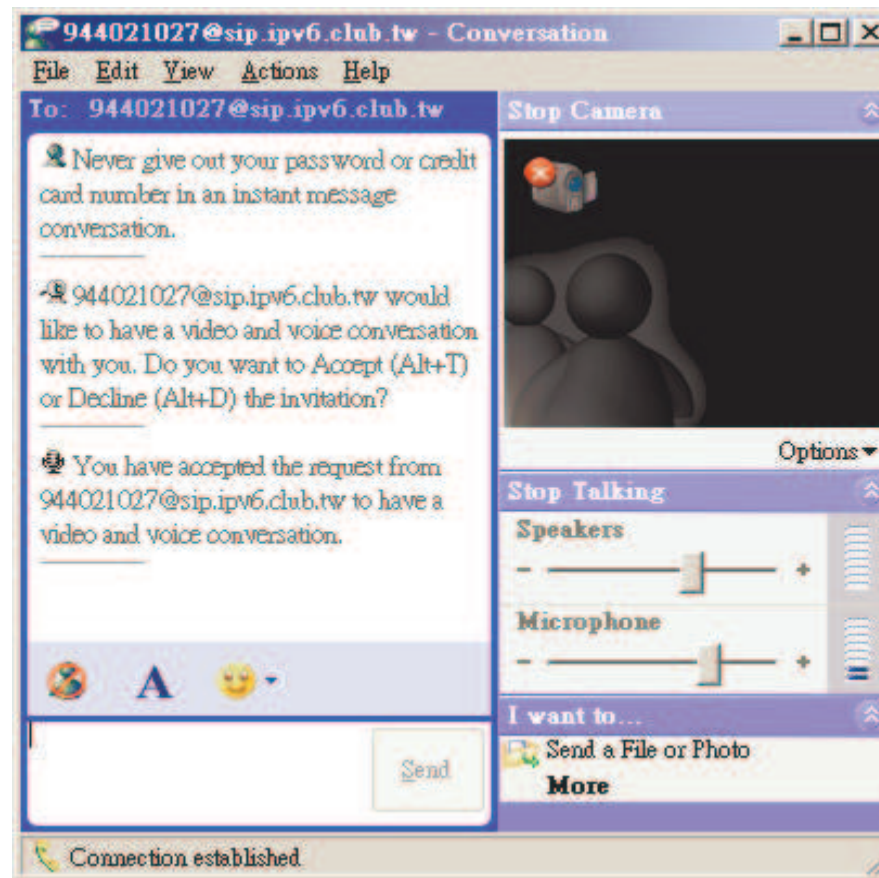


# Step 5: Conversation





# Step 6: Answer A Call



# SIP UA - X-Lite

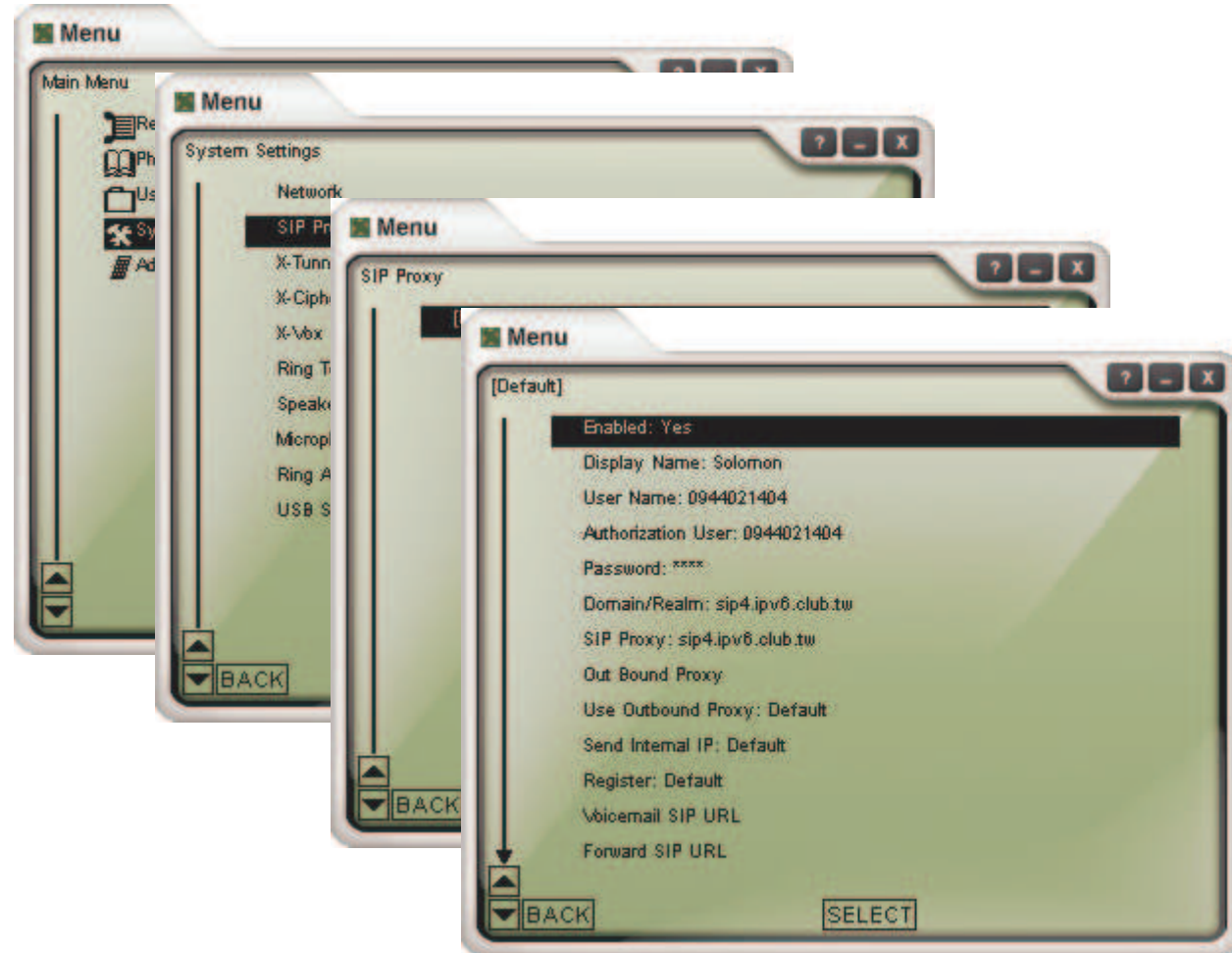
- X-Lite - The Best Free Softphone
- A FREE premium SIP softphone with many PBX-like features.
- Open standards-based design (SIP) allows for maximum network interoperation and integration.
- Download from <http://www.xten.com/>

# 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



# Step 1: Configuration



## 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.



# 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/>

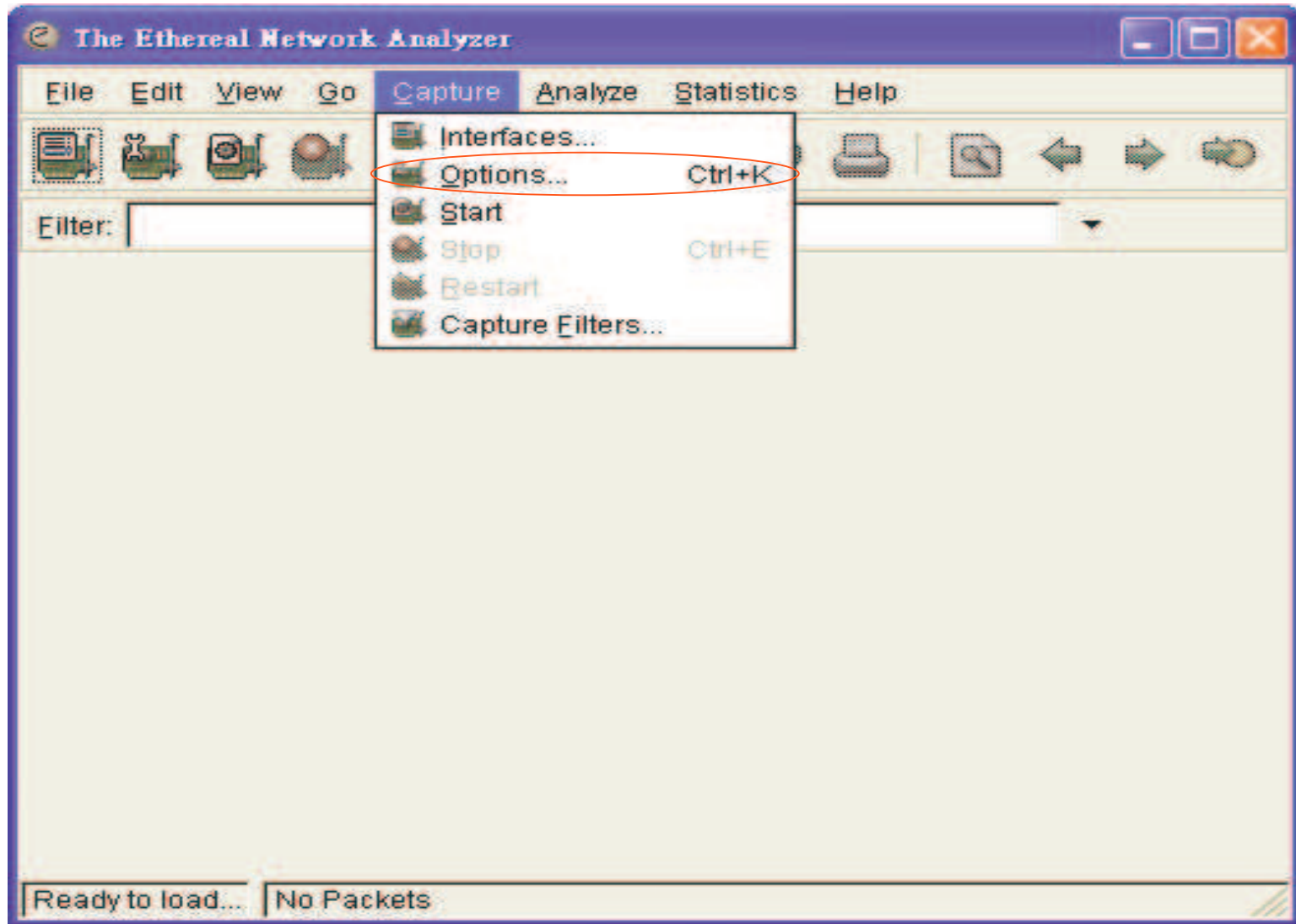
# Install Ethereal under Windows

## ■ Install WinPcap 3.1.

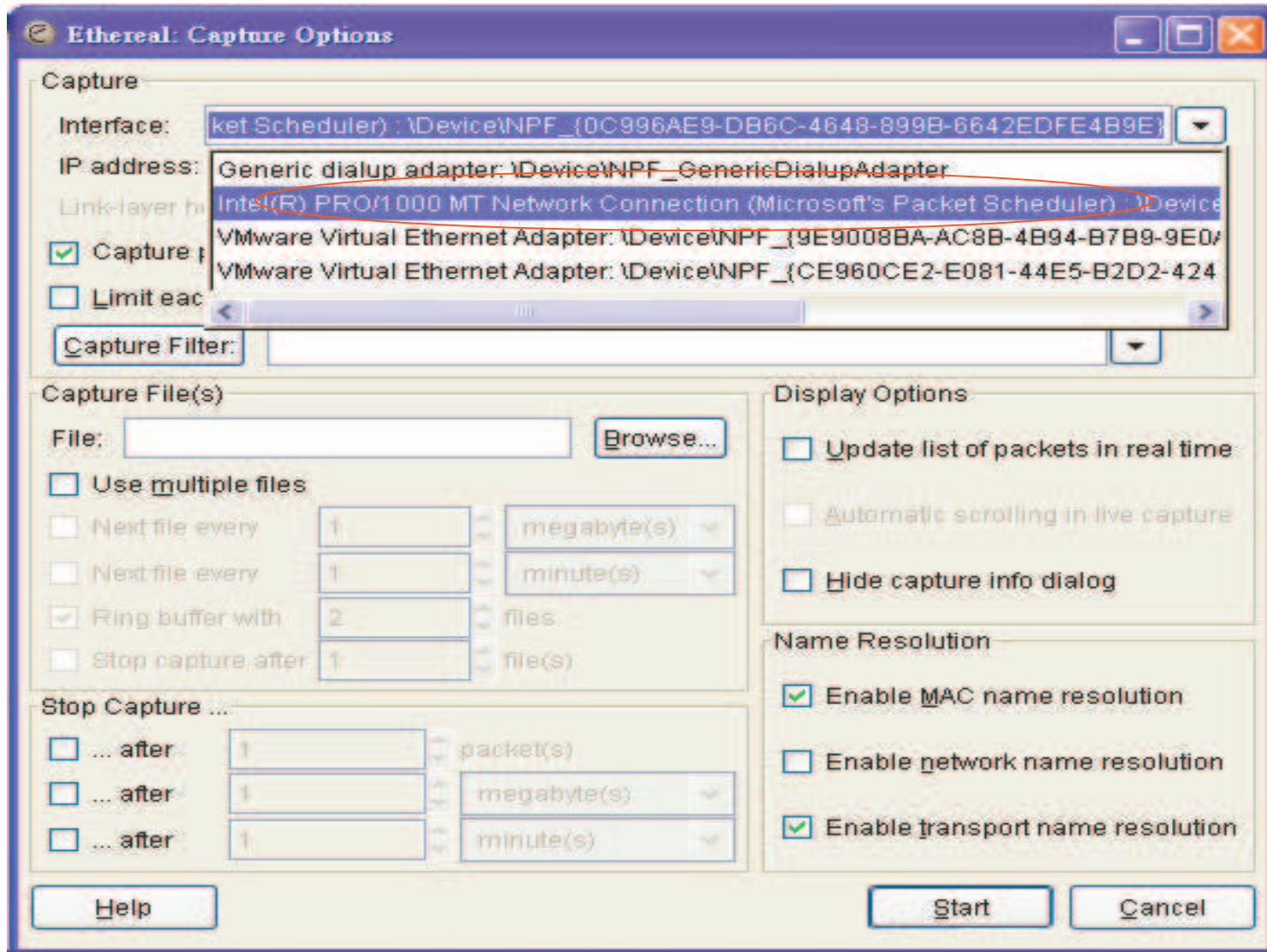
- WinPcap is an architecture for packet capture and network analysis for the Win32 platforms.
- It includes
  - ☞ a kernel-level packet filter,
  - ☞ a low-level dynamic link library (packet.dll), and
  - ☞ a high-level and system-independent library (wpcap.dll, based on libpcap version 0.6.2)

## ■ Install Ethereal 0.10.14.

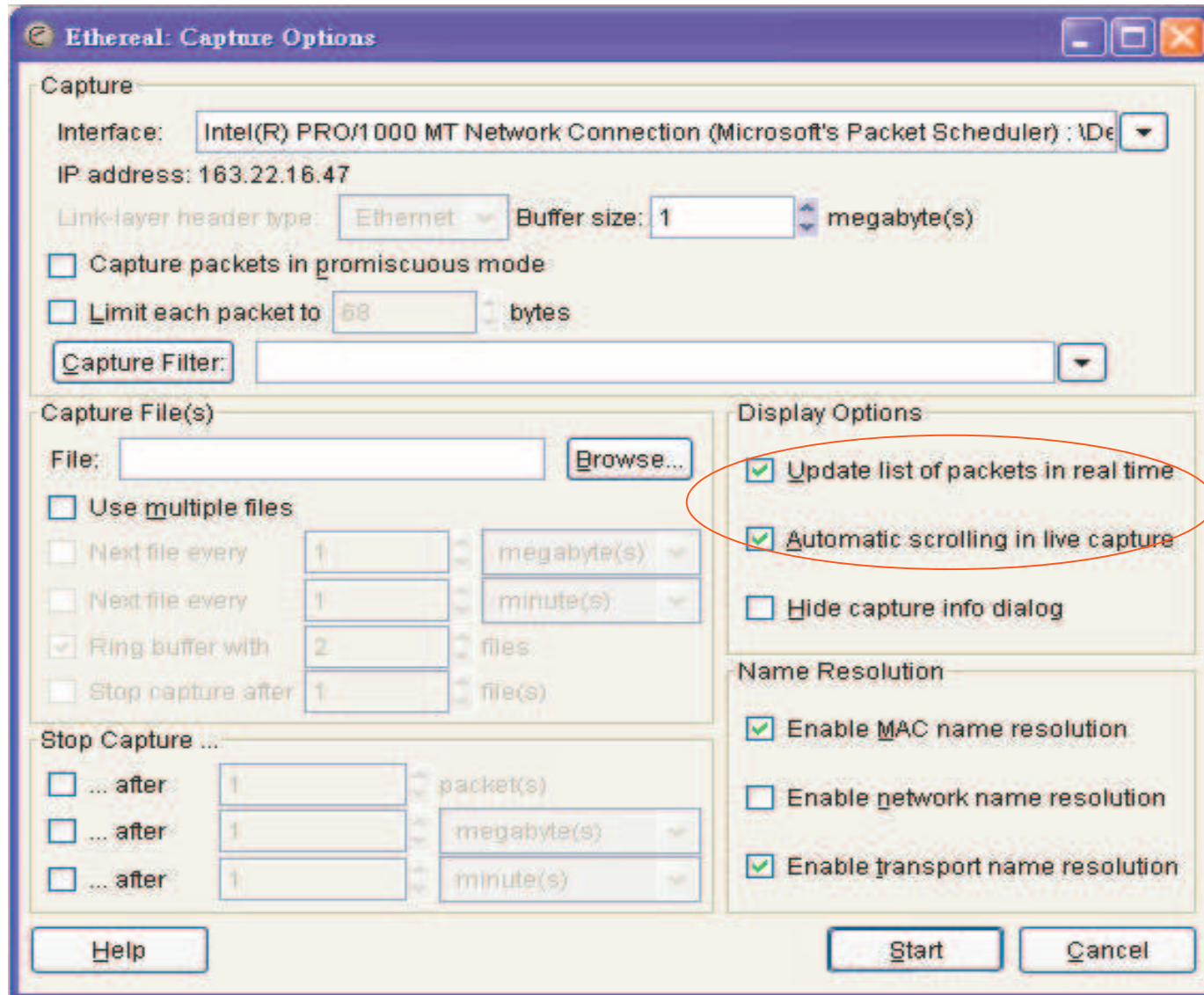
# Capturing packets with Ethereal



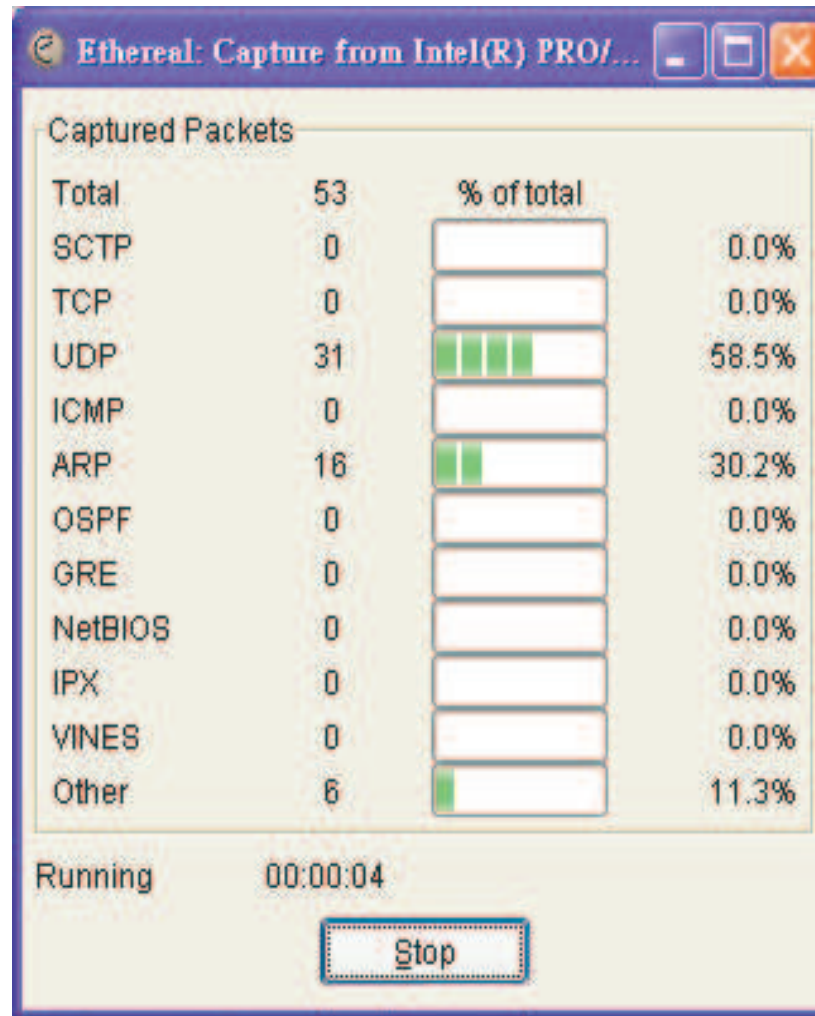
# Capturing packets with Ethereal



# The Capture Preferences dialog box



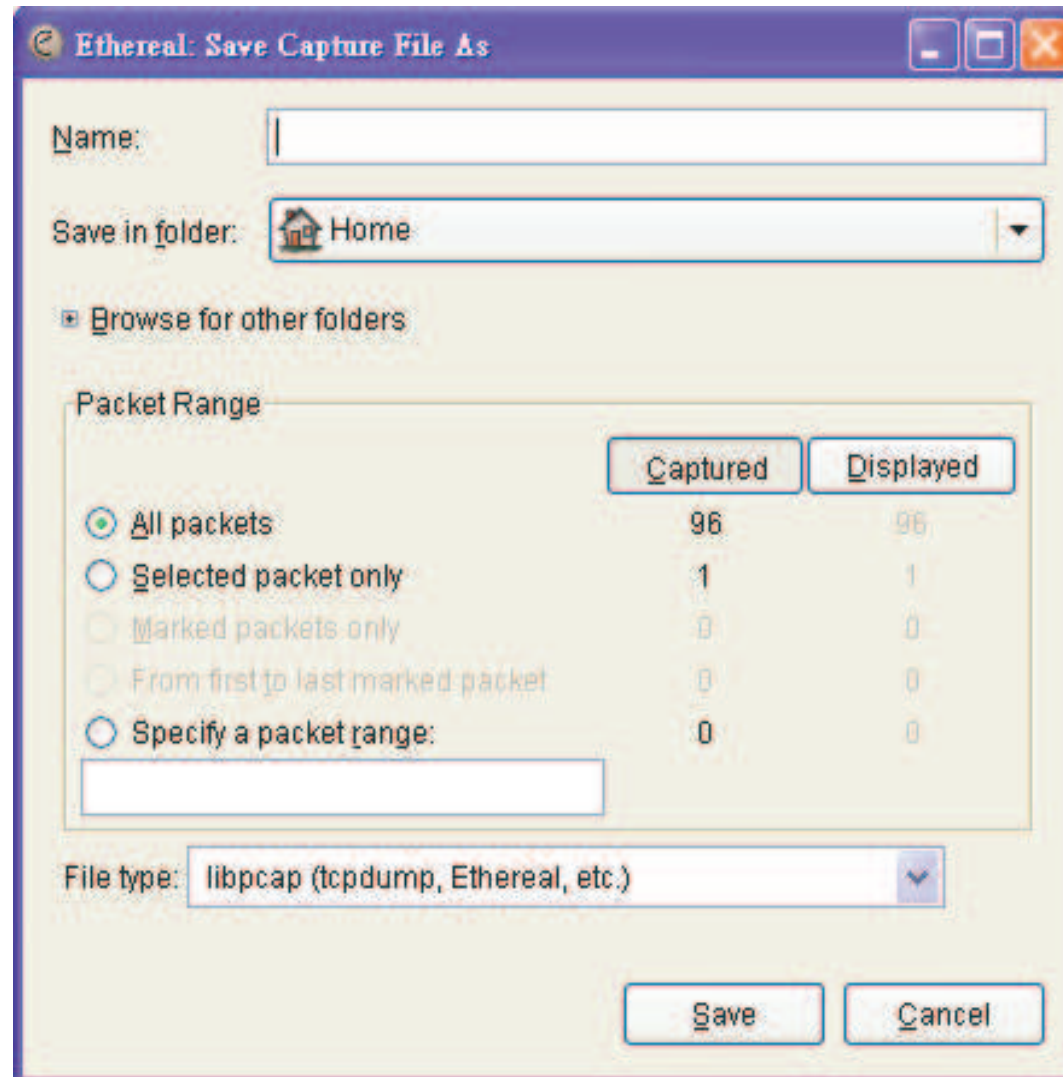
# Stop after you have collected enough packets







# File – Save As





# Show Packet in New Window

The screenshot shows the SIP - Ethereal interface. The packet list at the top shows several SIP-related packets. Packet 428 is selected, and its details are expanded in the main pane. The details include Ethernet II, Internet Protocol, User Datagram Protocol, and Session Initiation Protocol (SIP) headers and body.

No.	Time	Source	Destination	Protocol	Info
337	40.123905	140.113.131.29	163.22.16.47	SIP	Status: 488 Not Acceptable Media
338	40.125402	163.22.16.47	140.113.131.29	SIP	Request: ACK sip:4762@140.113.131.29
428	50.289461	163.22.16.47	140.113.131.29	SIP/SD	Request: INVITE sip:4763@140.113.131.29, with ses
429	50.298905	140.113.131.29	163.22.16.47	SIP	Status: 100 Trying

Expanded details for packet 428:

- Frame 428 (765 bytes on wire (765 bytes captured))
- Ethernet II, Src: AsustekC\_27:91:42 (00:11:d8:27:91:42), Dst: 10.10.16.254 (00:03:31:e4:2c:00)
  - Destination: 10.10.16.254 (00:03:31:e4:2c:00)
  - Source: AsustekC\_27:91:42 (00:11:d8:27:91:42)
  - Type: IP (0x0800)
- Internet Protocol, Src: 163.22.16.47 (163.22.16.47), Dst: 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:4763@140.113.131.29 SIP/2.0
  - Message Header
    - Via: SIP/2.0/UDP 163.22.16.47:5060;rport;branch=z9hG4bKd91DABC902764FA1ACBB69326D979962
    - From: Ying-shun <sip:22300@140.113.131.29>;tag=331578138
    - To: <sip:4763@140.113.131.29>
    - Contact: <sip:22300@163.22.16.47:5060>
    - Call-ID: 4EED06A4-F19C-4CBF-ADE6-6F502CB5F6B4@163.22.16.47
    - CSeq: 59546 INVITE
    - Max-Forwards: 70
    - Content-Type: application/sdp
    - User-Agent: X-Lite release 1105x
    - Content-Length: 279
  - Message body

Hex dump and ASCII view at the bottom of the packet details pane:

```

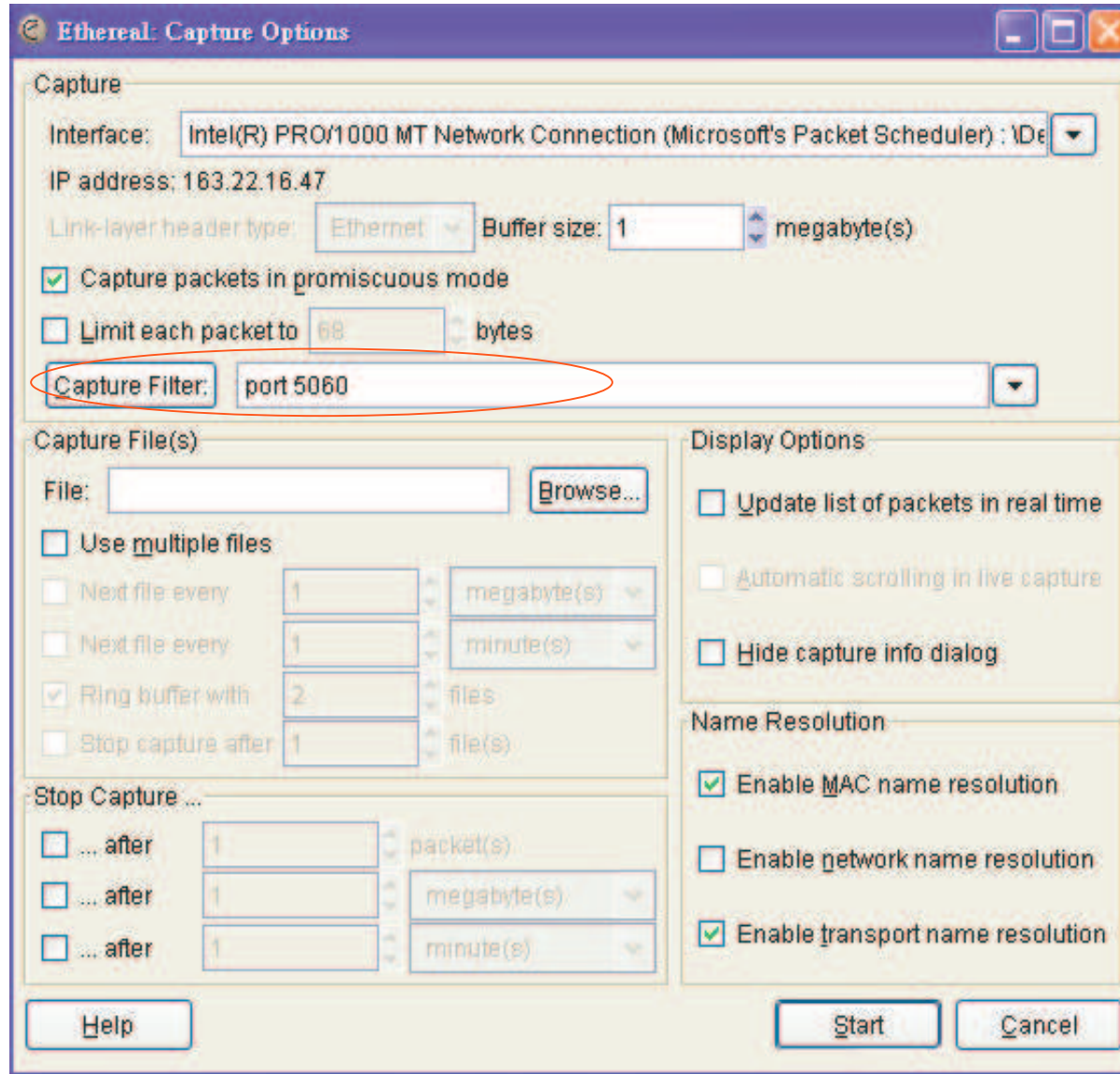
0180 46 6f 72 77 61 72 64 73 3a 20 37 30 0d 0a 43 6f 34 0 INVITE: Max-
0190 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c  Forward: 70..Co
01a0 69 63 61 74 69 6f 6e 2f 73 64 70 0d 0a 55 73 65  Content-Type: appl
01b0 72 2d 41 67 65 6e 74 3a 20 58 2d 4c 69 74 65 20  ication/sdp..Use
01c0 72 65 6c 65 61 73 65 20 31 31 30 35 78 0d 0a 43  User-Agent: X-Lite
    
```

Source Hardware Address (...): P: 534 D: 16 M: 0

# Capture Filters



# Filtering While Capturing



# 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)

2 - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter:  Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	163.22.16.47	140.113.131.29	UDP	Source port: 5060 Destination port: 5060
2	10.008613	163.22.16.47	140.113.131.29	UDP	Source port: 5060 Destination port: 5060
3	20.016384	163.22.16.47	140.113.131.29	UDP	Source port: 5060 Destination port: 5060
4	30.023816	163.22.16.47	140.113.131.29	UDP	Source port: 5060 Destination port: 5060
5	40.249024	163.22.16.47	140.113.131.29	SIP/SD	Request: INVITE sip:22200@140.113.131.29,
6	40.271682	140.113.131.29	163.22.16.47	SIP	Status: 100 Trying

Frame 5 (768 bytes on wire, 768 bytes captured)

- Ethernet II, Src: 163.22.16.47 (00:11:d8:27:91:42), Dst: 10.10.16.254 (00:03:31:e4:2c:00)
- Internet Protocol, Src: 163.22.16.47 (163.22.16.47), Dst: 140.113.131.29 (140.113.131.29)
- User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
- Session Initiation Protocol

```

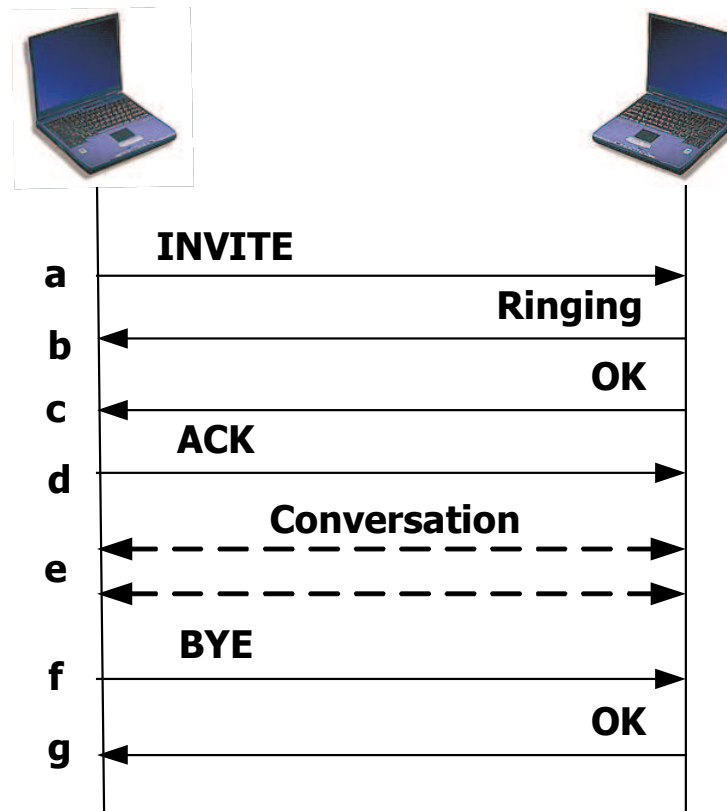
0000  00 03 31 e4 2c 00 00 11 d8 27 91 42 08 00 45 00  ..1.,... .'.B..E.
0010  02 f2 cc 3b 00 00 80 11 a8 eb a3 16 10 2f 8c 71  ...;.... ..../.q
0020  83 1d 13 c4 13 c4 02 de 56 54 49 4e 56 49 54 45  .....VTINVITE
0030  20 73 69 70 3a 32 32 32 30 30 40 31 34 30 2e 31  'sip:222 00@140.1
0040  31 33 2e 31 33 31 2e 32 39 20 53 49 50 2f 32 2e  13.131.2 9 SIP/2.
0050  30 0d 0a 56 69 61 3a 20 53 49 50 2f 32 2e 30 2f  0..via: SIP/2.0/
0060  55 44 50 20 31 36 33 2e 32 32 2e 31 36 2e 34 37  UDP 163. 22.16.47
0070  3a 35 30 36 30 3b 72 70 6f 72 74 3b 62 72 61 6e  :5060;rp ort;bran
    
```

File: "C:\Documents and Settings\smartderrick\桌面\2" 4886 Bytes 00:02:31 | P: 23 D: 23 M: 0



# SIP Call Establishment

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



# Basic Call Flow

2 - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
5	40.249024	163.22.16.47	140.113.131.29	SIP/SDP	Request: INVITE sip:22200@140
6	40.271682	140.113.131.29	163.22.16.47	SIP	Status: 100 Trying
8	40.311320	140.113.131.29	163.22.16.47	SIP	Status: 180 Ringing
9	43.881080	140.113.131.29	163.22.16.47	SIP/SDP	Status: 200 Ok, with session
10	43.888606	163.22.16.47	140.113.131.29	SIP	Request: ACK sip:22200@163.22
19	124.071551	163.22.16.47	140.113.131.29	SIP	Request: BYE sip:22200@163.22
20	124.115540	140.113.131.29	163.22.16.47	SIP	Status: 200 ok

Frame 5 (768 bytes on wire, 768 bytes captured)

- Ethernet II, Src: 163.22.16.47 (00:11:d8:27:91:42), Dst: 10.10.16.254 (00:03:31:e4:2c:00)
- Internet Protocol, Src: 163.22.16.47 (163.22.16.47), Dst: 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:22200@140.113.131.29 SIP/2.0
  - Message Header
    - Via: SIP/2.0/UDP 163.22.16.47:5060;rport;branch=z9hg4bk01E2A21AE64944ACBBB0274FFCEA9BB3
    - From: Ying-shun <sip:22300@140.113.131.29>;tag=3719953134
    - To: <sip:22200@140.113.131.29>
    - Contact: <sip:22300@163.22.16.47:5060>
    - Call-ID: 4D646BA9-B7A7-4BE6-B13E-C603C2BC7CC9@163.22.16.47
    - CSeq: 62356 INVITE

```

0000  00 03 31 e4 2c 00 00 11 d8 27 91 42 08 00 45 00  ..1.,... .'.B..E.
0010  02 f2 cc 3b 00 00 80 11 a8 eb a3 16 10 2f 8c 71  ....;.... ...../.q
0020  83 1d 13 c4 13 c4 02 de 56 54 49 4e 56 49 54 45  ..... VTINVITE
0030  20 73 69 70 3a 32 32 32 30 30 40 31 34 30 2e 31  sip:222 00@140.1
0040  31 33 2e 31 33 31 2e 32 39 20 53 49 50 2f 32 2e  13.131.2 9 SIP/2.
0050  30 0d 0a 56 69 61 3a 20 53 49 50 2f 32 2e 30 2f  0..Via: SIP/2.0/
0060  55 44 50 20 31 36 33 2e 32 32 2e 31 36 2e 34 37  UDP 163. 22.16.47
0070  3a 35 30 36 30 3b 72 70 6f 72 74 3b 62 72 61 6e  :5060;rp ort;bran
    
```

File: "C:\Documents and Settings\smartderrick\桌面\2" 4886 Bytes 0... | P: 23 D: 7 M: 1



The screenshot shows the Wireshark interface with a packet capture of SIP traffic. A 'SIP statistics' dialog box is open, providing a summary of the captured SIP packets.

**SIP statistics dialog box content:**

- SIP stats (18 packets)
- (0 resent packets)
- Informational SIP 1xx:
  - SIP 100 Trying: 3
  - SIP 180 Ringing: 2
- Success SIP 2xx:
  - SIP 200 OK: 4
- Redirection SIP 3xx: 0
- Client errors SIP 4xx:
  - SIP 480 Temporarily Unavailable: 1
- Server errors SIP 5xx: 0
- Global failures SIP 6xx: 0
- List of request methods:
  - INVITE: 3 packets
  - BYE: 2 packets
  - ACK: 3 packets

The background interface shows a packet list with 4 packets, a packet details pane for a SIP 'Request-Line: ACK sip:222000' packet, and a packet bytes pane showing the raw data.



Filter: |

No. -	Time	Source
1	0.000000	163.22.16.47
2	10.008613	163.22.16.47
3	20.016384	163.22.16.47
4	30.023816	163.22.16.47
5	40.249024	163.22.16.47
6	40.271682	140.113.131.29
7	40.277535	163.22.16.47
8	40.311320	140.113.131.29
9	43.881080	140.113.131.29
10	43.888606	163.22.16.47
11	50.511697	163.22.16.47
12	60.519324	163.22.16.47
13	70.527012	163.22.16.47

+ Frame 10 (470 bytes on wire, captured on interface eth0)
   
 + Ethernet II, Src: AsustekC\_27:00:02:00:00:00, Dst: Cisco\_e4:2c:00:00:03:31
   
 + Internet Protocol, Src: 163.22.16.47, Dst: 140.113.131.29
   
 + User Datagram Protocol, Src Port: 5060, Dst Port: 5060
   
 - Session Initiation Protocol
 

- Request-Line: ACK sip:22200@163.22.16.47
- Method: ACK
- [Resent Packet: False]
- Message Header
  - Via: SIP/2.0/UDP 163.22.16.47
  - From: ying-shun <sip:22300@140.113.131.29>
  - To: <sip:22200@140.113.131.29>
  - Contact: <sip:22300@163.22.16.47>
  - Route: <sip:140.113.131.29>
  - Call-ID: 4D646BA9-B7A7-4B8A-8000-000000000000
  - CSeq: 62356 ACK
  - Max-Forwards: 70
  - Content-Length: 0

- Summary
- Protocol Hierarchy
- Conversations
- Endpoints
- IO Graphs
- Conversation List
- Endpoint List
- Service Response Time
- ANSI
- Fax T38 Analysis...
- GSM
- H.225...
- MTP3
- RTP
- SCTP
- SIP...
- VoIP Calls
- WAP-WSP...
- BOOTP-DHCP...
- Destinations...
- Flow Graph...
- HTTP
- IP address...
- ISUP Messages...
- ONC-RPC Programs
- Packet Length...
- Port Type...
- TOP Stream Graph



pression... Clear Apply

Protocol	Info
UDP	Source port: 5060 Destination port: 5060
UDP	Source port: 5060 Destination port: 5060
UDP	Source port: 5060 Destination port: 5060
UDP	Source port: 5060 Destination port: 5060
SIP/SD	Request: INVITE sip:22200@140.113.131.29, with session description
SIP	Status: 100 Trying
UDP	Source port: 5060 Destination port: 5060
SIP	Status: 180 Ringing
SIP/SD	Status: 200 Ok, with session description
SIP	Request: ACK sip:22200@163.22.16.32:5060
UDP	Source port: 5060 Destination port: 5060
UDP	Source port: 5060 Destination port: 5060
UDP	Source port: 5060 Destination port: 5060

, Dst: Cisco\_e4:2c:00 (00:03:31:e4:2c:00)
   
 t: 140.113.131.29 (140.113.131.29)
   
 : 5060 (5060)

G4bk4850d57119584c75948760d0421c8bfa
   
 953134
   
 2.16.47

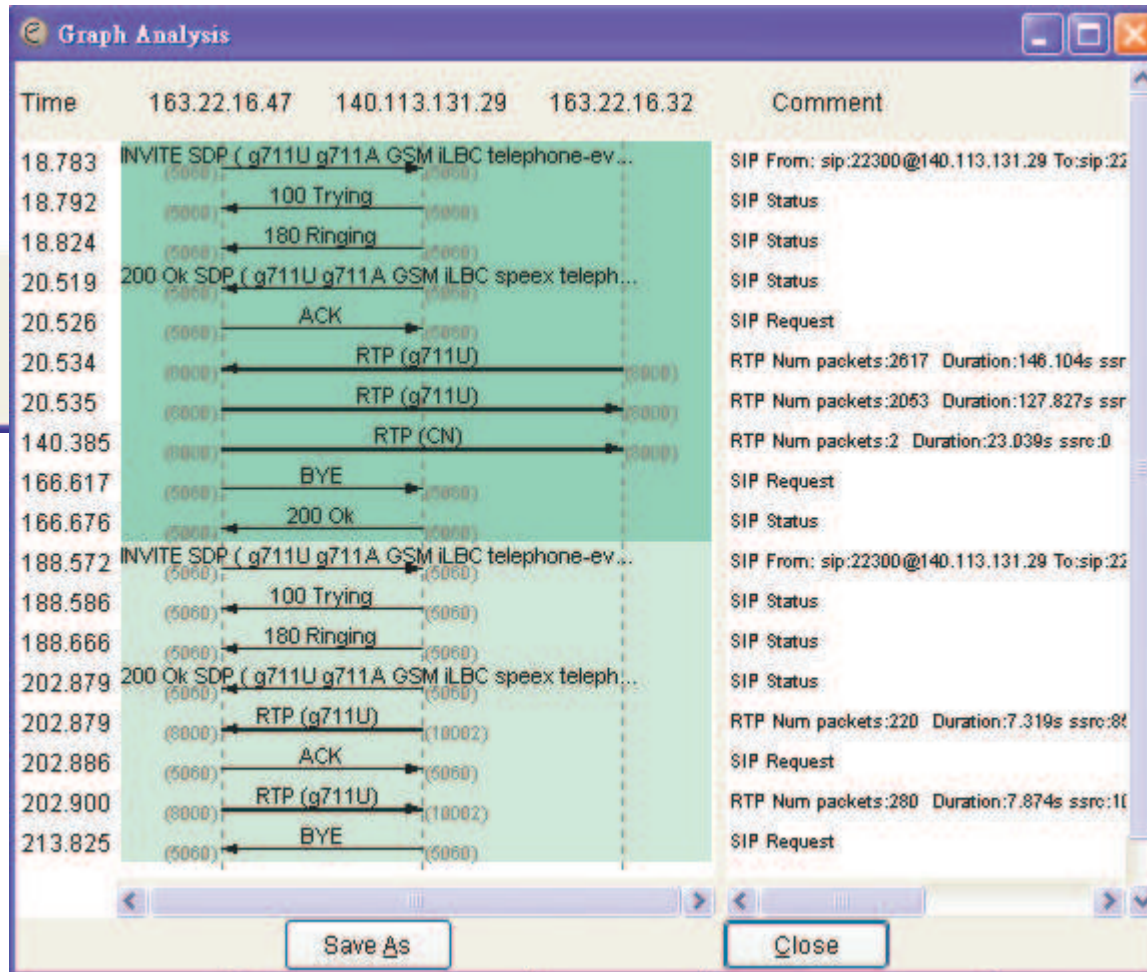
```

0000 00 03 31 e4 2c 00 00 11 d8 27 91 42 08 00 45 00  ..1.,... .'.B..E.
0010 01 c8 cc 3d 00 00 80 11 aa 13 a3 16 10 2f 8c 71  ...=.... ..../.q
0020 83 1d 13 c4 13 c4 01 b4 13 7e 41 43 4b 20 73 69  .....;~ACK s;
0030 70 3a 32 32 32 30 30 40 31 36 33 2e 32 32 2e 31  p:22200@ 163.22.1
0040 36 2e 33 32 3a 35 30 36 30 20 53 49 50 2f 32 2e  6.32:506 0 SIP/2.
0050 30 0d 0a 56 69 61 3a 20 53 49 50 2f 32 2e 30 2f  0..Via: SIP/2.0/
  
```

Ethereal: VoIP Calls

Detected 3 VoIP Calls. Selected 2 Calls.

Start Time	Stop Time	Initial Speaker	From	To	Protocol	Packets	State	Comments
9.47	9.51	163.22.16.47	sip:22300@140.113.13	sip:22400@140.113.13	SIP	4	REJECTEC	
18.78	166.67	163.22.16.47	sip:22300@140.113.13	sip:22200@140.113.13	SIP	7	COMPLETE	
188.57	213.82	163.22.16.47	sip:22300@140.113.13	sip:22400@140.113.13	SIP	7	COMPLETE	



# REGISTER

(Untitled) - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
121	1.908554	140.113.131.29	163.22.16.47	SIP	Status: 200 OK (0 bindings)
505	7.346143	163.22.16.47	140.113.131.29	SIP	Request: REGISTER sip:140.113.131.29
512	7.399067	140.113.131.29	163.22.16.47	SIP	Status: 200 OK (1 bindings)
704	14.595007	163.22.16.47	140.113.131.29	SIP	Request: REGISTER sip:140.113.131.29
705	14.647330	140.113.131.29	163.22.16.47	SIP	Status: 200 OK (0 bindings)
792	18.859500	163.22.16.47	140.113.131.29	SIP	Request: REGISTER sip:140.113.131.29

Frame 505 (488 bytes on wire, 488 bytes captured)

- Ethernet II, Src: 163.22.16.47 (00:11:d8:27:91:42), Dst: 10.10.16.254 (00:03:31:e4:2c:00)
- Internet Protocol, Src: 163.22.16.47 (163.22.16.47), Dst: 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:140.113.131.29 SIP/2.0
    - Method: REGISTER
    - [Resent Packet: False]
  - Message Header
    - Via: SIP/2.0/UDP 163.22.16.47:5060;rport;branch=z9hg4bk3134c5efb6144af5be4e8f732b91e6ce
    - From: Ying-shun <sip:22300@140.113.131.29>;tag=271102178
    - To: Ying-shun <sip:22300@140.113.131.29>
    - Contact: "Ying-shun" <sip:22300@163.22.16.47:5060>
    - Call-ID: 0ED86700464F41E9A9D8474C6C64E31E@140.113.131.29
    - CSeq: 24730 REGISTER
    - Expires: 1800
    - Max-Forwards: 70
    - User-Agent: X-Lite release 1105x
    - Content-Length: 0

0040 33 31 2e 32 39 20 53 49 50 2f 32 2e 30 0d 0a 56 31.29 SI P/2.0..M

0050 69 61 3a 20 53 49 50 2f 32 2e 30 2f 55 44 50 20 ia: SIP/ 2.0/UDP

0060 31 36 33 2e 32 32 2e 31 36 2e 34 37 3a 35 30 36 163.22.1 6.47:506

0070 30 3b 72 70 6f 72 74 3b 62 72 61 6e 63 68 3d 7a 0;rport; branch=z

0080 39 68 47 34 62 4b 33 31 33 34 43 35 45 46 42 36 9hg4bk31 34c5efb6

0090 31 34 34 41 46 35 42 45 34 45 38 46 37 33 32 42 144af5be 4e8f732b

Message Header in SIP message (sip.msg\_hdr), 409 bytes P: 980 D: 8 M: 0 Drops: 0

# 200 OK

Filter:  Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
121	1.908554	140.113.131.29	163.22.16.47	SIP	Status: 200 OK (0 bindings)
505	7.346143	163.22.16.47	140.113.131.29	SIP	Request: REGISTER sip:140.113.131.29
512	7.399067	140.113.131.29	163.22.16.47	SIP	Status: 200 OK (1 bindings)
704	14.595007	163.22.16.47	140.113.131.29	SIP	Request: REGISTER sip:140.113.131.29
705	14.647330	140.113.131.29	163.22.16.47	SIP	Status: 200 OK (0 bindings)
792	18.859500	163.22.16.47	140.113.131.29	SIP	Request: REGISTER sip:140.113.131.29

Frame 512 (433 bytes on wire (433 bytes captured) on interface 0):

- Ethernet II, Src: 10.10.16.254 (00:03:31:e4:2c:00), Dst: 163.22.16.47 (00:11:d8:27:91:42)
- Internet Protocol, Src: 140.113.131.29 (140.113.131.29), Dst: 163.22.16.47 (163.22.16.47)
- User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
- Session Initiation Protocol
  - Status-Line: SIP/2.0 200 OK
    - Status-Code: 200
    - [Resent Packet: False]
  - Message Header
    - Call-ID: 0ED86700464F41E9A9D8474C6C64E31E@140.113.131.29
    - Contact: <sip:22300@163.22.16.47:5060>; expires=1800
    - Content-Length: 0
    - CSeq: 24730 REGISTER
    - From: Ying-shun <sip:22300@140.113.131.29>; tag=271102178
    - To: Ying-shun <sip:22300@140.113.131.29>; tag=7e0bdc3f
    - Via: SIP/2.0/UDP 163.22.16.47:5060;rport=5060;received=163.22.16.47;branch=z9hg4bk3134C5EFB6144AF5BE4E

```

0000  00 11 d8 27 91 42 00 03 31 e4 2c 00 08 00 45 00  ... .B.. 1.....E.
0010  01 a3 12 bc 40 00 3b 11 68 ba 8c 71 83 1d a3 16  ....@.;. h..q...
0020  10 2f 13 c4 13 c4 01 8f 6e 1b 53 49 50 2f 32 2e  ./..... n.SIP/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 30 45 44 38 36 37 30 30 34 36 34 46 34 31  D:0ED867 00464F41
0050  45 39 41 39 44 38 34 37 34 43 36 43 36 34 45 33  E9A9D847 4C6C64E3
    
```

File: "C:\DOCUME~1\SMARTD~1\LOCALS~1\Temp\ether\0000N2015S" 633 ... P: 980 D: 8 M: 0 Drops: 0

# INVITE

The screenshot shows the Wireshark interface with a packet capture of SIP messages. The main pane displays a list of packets, with packet 247 selected. The packet list is as follows:

No.	Time	Source	Destination	Protocol	Info
177	9.476298	163.22.16.47	140.113.131.29	SIP/SD	Request: INVITE sip:22400@140.113.131.29,
178	9.487270	140.113.131.29	163.22.16.47	SIP	Status: 100 Trying
179	9.512073	140.113.131.29	163.22.16.47	SIP	Status: 480 Temporarily Unavailable
180	9.513771	163.22.16.47	140.113.131.29	SIP	Request: ACK sip:22400@140.113.131.29
247	18.783144	163.22.16.47	140.113.131.29	SIP/SD	Request: INVITE sip:22200@140.113.131.29,
248	18.792467	140.113.131.29	163.22.16.47	SIP	Status: 100 Trying

The details pane for the selected packet (Frame 247) shows the following structure:

- Ethernet II, Src: 163.22.16.47 (00:11:d8:27:91:42), Dst: 10.10.16.254 (00:03:31:e4:2c:00)
- Internet Protocol, Src: 163.22.16.47 (163.22.16.47), Dst: 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:22200@140.113.131.29 SIP/2.0
  - Method: INVITE
  - [Resent Packet: False]
  - Message Header
    - Via: SIP/2.0/UDP 163.22.16.47:5060;rport;branch=z9hG4bK9A71B8628387452CA5072DD377BABAEA
    - From: Ying-shun <sip:22300@140.113.131.29>;tag=1638012823
    - To: <sip:22200@140.113.131.29>
    - Contact: <sip:22300@163.22.16.47:5060>
    - Call-ID: 02736DD3-1565-4A3C-9B4C-92164F694B62@163.22.16.47
    - CSeq: 45809 INVITE
    - Max-Forwards: 70
    - Content-Type: application/sdp
    - User-Agent: X-Lite release 1105x
    - Content-Length: 281
  - Message body

The hex dump at the bottom shows the raw bytes of the packet body:

```

0000  00 03 31 e4 2c 00 00 11 d8 27 91 42 08 00 45 00  ..1.,... .'.B..E.
0010  02 f4 02 e6 00 00 80 11 72 3f a3 16 10 2f 8c 71  .....r?.../.q
0020  83 1d 13 c4 13 c4 02 e0 90 7e 49 4e 56 49 54 45  .....~INVITE
0030  20 73 69 70 3a 32 32 32 30 30 40 31 34 30 2e 31  sip:222 00@140.1
0040  31 33 2e 31 33 31 2e 32 39 20 53 49 50 2f 32 2e  13.131.2 9 SIP/2.
0050  30 0d 0a 56 69 61 3a 20 53 49 50 2f 32 2e 30 2f  0..via: SIP/2.0/
    
```

File: "C:\Documents and Settings\smartderrick\桌面\3" 1497 KB 00:04:05 | P: 7676 D: 18 M: 0

# SDP in INVITE

The screenshot shows a network capture in Wireshark. The packet list pane shows several SIP messages. Packet 247 is selected, showing a SIP/SDP Request: INVITE. The packet details pane shows the following structure:

- Internet Protocol Version 4, Src: 163.22.16.47, Dst: 140.113.131.29
- User Datagram Protocol, Src Port: 5060, Dst Port: 5060
- Session Initiation Protocol
  - Request-Line: INVITE sip:22200@140.113.131.29 SIP/2.0
  - Message Header
  - Message body
    - Session Description Protocol
      - Session Description Protocol Version (v): 0
      - Owner/Creator, Session Id (o): 22300 103457132 103457146 IN IP4 163.22.16.47
      - Session Name (s): X-Lite
      - Connection Information (c): IN IP4 163.22.16.47
      - Time Description, active time (t): 0 0
      - Media Description, name and address (m): **audio 8000 RTP/AVP 0 8 3 98 101**
      - Media Attribute (a): rtpmap:0 pcmu/8000
      - Media Attribute (a): rtpmap:8 pcma/8000
      - Media Attribute (a): rtpmap:3 gsm/8000
      - Media Attribute (a): rtpmap:98 iLBC/8000
      - Media Attribute (a): rtpmap:101 telephone-event/8000
      - Media Attribute (a): fmp:101 0-15
      - Media Attribute (a): sendrecv

The hex dump at the bottom shows the raw bytes of the SDP line, with the text `: 281... .v=0..o=` visible.

# 200 OK

3 - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
180	9.513771	163.22.16.47	140.113.131.29	SIP	Request: ACK sip:22400@140.113.131.29
247	18.783144	163.22.16.47	140.113.131.29	SIP/SD	Request: INVITE sip:22200@140.113.131.29,
248	18.792467	140.113.131.29	163.22.16.47	SIP	Status: 100 Trying
249	18.824494	140.113.131.29	163.22.16.47	SIP	Status: 180 Ringing
267	20.518779	140.113.131.29	163.22.16.47	SIP/SD	Status: 200 Ok, with session description
268	20.525008	163.22.16.47	140.113.131.29	SIP	Request: ACK sip:22200@163.22.16.47

Frame 267 (821 bytes on wire, 821 bytes captured)

- Ethernet II, Src: 10.10.16.254 (00:03:31:e4:2c:00), Dst: 163.22.16.47 (00:11:d8:27:91:42)
- Internet Protocol, Src: 140.113.131.29 (140.113.131.29), Dst: 163.22.16.47 (163.22.16.47)
- 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: 02736DD3-1565-4A3C-9B4C-92164F694B62@163.22.16.47
    - Contact: <sip:22200@163.22.16.32:5060>
    - Content-Length: 304
    - Content-Type: application/sdp
    - Cseq: 45809 INVITE
    - From: Ying-shun <sip:22300@140.113.131.29>; tag=1638012823
    - Record-Route: <sip:140.113.131.29:5060;lr>
    - Server: X-Lite release 1105x
    - To: <sip:22200@140.113.131.29>; tag=721576328
    - Via: SIP/2.0/UDP 163.22.16.47:5060;rport=5060;received=163.22.16.47;branch=z9hg4bk9A71B8628387452CA507;
  - Message body

```

0030 30 20 32 30 30 20 4f 6b 0d 0a 43 61 6c 6c 2d 49 0 200 Ok .. call-I
0040 44 3a 30 32 37 33 36 44 44 33 2d 31 35 36 35 2d 0:02736D D3-1565-
0050 34 41 33 43 2d 39 42 34 43 2d 39 32 31 36 34 46 4A3C-9B4 C-92164F
0060 36 39 34 42 36 32 40 31 36 33 2e 32 32 2e 31 36 694B62@1 63.22.16
0070 2e 34 37 0d 0a 43 6f 6e 74 61 63 74 3a 3c 73 69 .47..Con tact:<si
0080 70 3a 32 32 32 30 30 40 31 36 33 2e 32 32 2e 31 p:22200@ 163.22.1
0090 36 2e 33 32 3a 35 30 36 30 3e 0d 0a 43 6f 6e 74 6.32:506 0>..Cont
00a0 65 6e 74 2d 4c 65 6e 67 74 68 3a 33 30 34 0d 0a
    
```

Message Header in SIP message (sip.msg\_hdr), 459 bytes | P: 7676 D: 18 M: 0



# SDP in 200 OK

The screenshot shows a Wireshark capture of a SIP 200 OK message. The packet list pane shows the following entries:

No.	Time	Source	Destination	Protocol	Info
180	9.513771	163.22.16.47	140.113.131.29	SIP	Request: ACK sip:22400@140.113.131.29
247	18.783144	163.22.16.47	140.113.131.29	SIP/SD	Request: INVITE sip:22200@140.113.131.29,
248	18.792467	140.113.131.29	163.22.16.47	SIP	Status: 100 Trying
249	18.824494	140.113.131.29	163.22.16.47	SIP	Status: 180 Ringing
267	20.518779	140.113.131.29	163.22.16.47	SIP/SD	Status: 200 ok, with session description
268	20.525908	163.22.16.47	140.113.131.29	SIP	Request: ACK sip:22200@163.22.16.47:5060

The packet details pane for the selected packet (No. 267) shows the following structure:

- User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
- Session Initiation Protocol
  - Status-Line: SIP/2.0 200 ok
  - Message Header
  - Message body
    - Session Description Protocol
      - Session Description Protocol Version (v): 0
      - Owner/Creator, session Id (o): 22200 4498358 4500066 IN IP4 163.22.16.32
      - Session Name (s): X-Lite
      - Connection Information (c): IN IP4 163.22.16.32
      - Time Description, active time (t): 0 0
      - Media Description, name and address (m): **audio 8000 RTP/AVP 0 8 3 98 97 101**
      - Media Attribute (a): rtpmap:0 pcmu/8000
      - Media Attribute (a): rtpmap:8 pcma/8000
      - Media Attribute (a): rtpmap:3 gsm/8000
      - Media Attribute (a): rtpmap:98 iLBC/8000
      - Media Attribute (a): rtpmap:97 speex/8000
      - Media Attribute (a): rtpmap:101 telephone-event/8000
      - Media Attribute (a): fmp:101 0-15
      - Media Attribute (a): sendrecv

The packet bytes pane shows the raw data for the SDP line, with the circled text corresponding to the SDP line in the details pane.

Session Description Protocol (sdp), 304 bytes | P: 7676 D: 18 M: 0

# ACK

The screenshot shows the Wireshark interface with a packet capture of a SIP ACK. The packet list pane shows several packets, with packet 269 highlighted in blue. The packet details pane shows the structure of the ACK packet, including the Session Initiation Protocol (SIP) and Message Header fields. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Info
247	18.783144	163.22.16.47	140.113.131.29	SIP/SD	Request: INVITE sip:22200@140.113.131.29,
248	18.792467	140.113.131.29	163.22.16.47	SIP	status: 100 Trying
249	18.824494	140.113.131.29	163.22.16.47	SIP	status: 180 Ringing
267	20.518779	140.113.131.29	163.22.16.47	SIP/SD	status: 200 ok, with session description
269	20.525908	163.22.16.47	140.113.131.29	SIP	Request: ACK sip:22200@163.22.16.32:5060
6416	166.617252	163.22.16.47	140.113.131.29	SIP	Request: BYE sip:22200@163.22.16.32:5060

Frame 269 (470 bytes on wire, 470 bytes captured)  
 Ethernet II, Src: 163.22.16.47 (00:11:d8:27:91:42), Dst: 10.10.16.254 (00:03:31:e4:2c:00)  
 Internet Protocol, Src: 163.22.16.47 (163.22.16.47), Dst: 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:22200@163.22.16.32:5060 SIP/2.0  
 Method: ACK  
 [Resent Packet: False]  
 Message Header  
 Via: SIP/2.0/UDP 163.22.16.47:5060;rport;branch=29hg4bkc6222AD52BC24CEF92166F7E929BB8F8  
 From: Ying-shun <sip:22300@140.113.131.29>;tag=1638012823  
 To: <sip:22200@140.113.131.29>;tag=721576328  
 Contact: <sip:22300@163.22.16.47:5060>  
 Route: <sip:140.113.131.29:5060;lr>  
 Call-ID: 027360D3-1565-4A3C-9B4C-92164F694B62@163.22.16.47  
 CSeq: 45809 ACK  
 Max-Forwards: 70  
 Content-Length: 0

0000 00 03 31 e4 2c 00 00 11 d8 27 91 42 08 00 45 00 ..1.....'.B..E.  
 0010 01 c8 02 ea 00 00 80 11 73 67 a3 16 10 2f 8c 71 .....sg.../.q  
 0020 83 1d 13 c4 13 c4 01 b4 14 92 41 43 4b 20 73 69 .....ACK si  
 0030 70 3a 32 32 32 30 30 40 31 36 33 2e 32 32 2e 31 p:22200@ 163.22.1  
 0040 36 2e 33 32 3a 35 30 36 30 20 53 49 50 2f 32 2e 6.32:506 0 SIP/2.  
 0050 30 0d 0a 56 69 61 3a 20 53 49 50 2f 32 2e 30 2f 0..Via: SIP/2.0/  
 0060 55 44 50 20 31 36 33 2e 32 32 2e 31 36 2e 34 37 UDP 163. 22.16.47  
 0070 3a 35 30 36 30 3b 72 70 6f 72 74 3b 62 72 61 6e \*5060;rpo rport;bran

File: "C:\Documents and Settings\smartderrick\桌面\3" 1497 KB 00:04:05 P: 7676 D: 18 M: 0

# Capturing the packets of Media Data

# RTP Traffic (udp port 8000)

The screenshot displays the Wireshark interface with the following details:

- Filter:** Expression... Clear Apply
- Packet List:**

Time	Source	Destination	Protocol	Info
1 0.000000	163.22.16.47	163.22.18.105	UDP	Source port: 8000 Destination port: 8000
2 0.000029	163.22.16.47	163.22.18.105	UDP	Source port: 8000 Destination port: 8000
3 0.000055	163.22.16.47	163.22.18.105	UDP	Source port: 8000 Destination port: 8000
4 0.061467	163.22.16.47	163.22.18.105	UDP	Source port: 8000 Destination port: 8000
5 0.061496	163.22.16.47	163.22.18.105	UDP	Source port: 8000 Destination port: 8000
6 0.101525	10.10.54.125	163.22.16.47	UDP	Source port: 8000 Destination port: 8000
7 0.101545	10.10.54.125	163.22.16.47	UDP	Source port: 8000 Destination port: 8000
8 0.101765	10.10.54.125	163.22.16.47	UDP	Source port: 8000 Destination port: 8000
9 0.102458	163.22.16.47	163.22.18.105	UDP	Source port: 8000 Destination port: 8000
- Packet Details:**
  - Frame 1 (214 bytes on wire, 214 bytes captured)
  - Ethernet II, Src: 163.22.16.47 (00:11:d8:27:91:42), Dst: 10.10.16.254 (00:03:31:e4:2c:00)
  - Internet Protocol, src: 163.22.16.47 (163.22.16.47), dst: 163.22.18.105 (163.22.18.105)
    - Version: 4
    - Header length: 20 bytes
    - Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    - Total Length: 200
    - Identification: 0x1961 (6497)
    - Flags: 0x00
    - Fragment offset: 0
    - Time to live: 128
    - Protocol: UDP (0x11)
    - Header checksum: 0xb7ff [correct]
    - Source: 163.22.16.47 (163.22.16.47)
    - Destination: 163.22.18.105 (163.22.18.105)
  - User Datagram Protocol, Src Port: 8000 (8000), Dst Port: 8000 (8000)
    - data (172 bytes)
- Packet Bytes:**

```

0000  00 03 31 e4 2c 00 00 11 d8 27 91 42 08 00 45 00  ..1.....B..E.
0010  00 c8 19 61 00 00 80 11 b7 ff a3 16 10 2f a3 16  ..a...../.
0020  12 69 1f 40 1f 40 00 b4 7e e0 80 80 00 01 00 00  ..i.@.@.....
0030  00 a0 cb fb 70 a6 7e 7e 7e 7e 7e 7e 7e ff ff ff  ....p.....
0040  7e ff 7e 7e ff 7e 7e 7e 7e 7e 7e 7e 7e 7e 7e  ~,.....
0050  7e 7e 7e 7e 7e 7e 7e 7e 7e 7e 7e 7e 7e 7e 7e  ~,.....

```
- Summary:** Internet Protocol (ip), 20 bytes | P: 450 D: 450 M: 0

■ What's wrong?

# Tools – Decode As RTP

The screenshot shows the Wireshark interface with a packet capture of RTP traffic. The main pane displays a list of packets, and the packet details pane shows the structure of a selected packet. The 'Decode As' dialog box is open, allowing the user to specify the protocol to decode the selected packet as.

Time	Source	Destination	Protocol	Info
1 0.000000	163.22.16.47	163.22.18.105	RTP	Payload type=ITU-T G.711 PCMU, SSRC=3422253222
2 0.000029	163.22.16.47	163.22.18.105	RTP	Payload type=ITU-T G.711 PCMU, SSRC=3422253222
3 0.000055	163.22.16.47	163.22.18.105	RTP	Payload type=ITU-T G.711 PCMU, SSRC=3422253222
4 0.061467	163.22.16.47	163.22.18.105	RTP	Payload type=ITU-T G.711 PCMU, SSRC=3422253222
5 0.061496	163.22.16.47	163.22.18.105	RTP	Payload type=ITU-T G.711 PCMU, SSRC=3422253222
6 0.101525	10.10.54.125	163.22.16.47	RTP	Payload type=ITU-T G.711 PCMU, SSRC=2435591191
7 0.101545	10.10.54.125	163.22.16.47	RTP	Payload type=ITU-T G.711 PCMU, SSRC=2435591191
8 0.101765	10.10.54.125	163.22.16.47	RTP	Payload type=ITU-T G.711 PCMU, SSRC=2435591191
9 0.102458	163.22.16.47	163.22.18.105	RTP	Payload type=ITU-T G.711 PCMU, SSRC=3422253222

Packet Details for Frame 1 (214 bytes on wire, 214 bytes captured):

- Ethernet II, Src: 163.22.16.47 (00:11:d8:27:91:42), Dst: 163.22.18.105 (08:00:45:00:00:11)
- Internet Protocol, Src: 163.22.16.47 (163.22.16.47), Dst: 163.22.18.105 (163.22.18.105)
- Version: 4
- Header length: 20 bytes
- Differentiated Services Field: 0x00 (DSCP 0x00: Default)
- Total Length: 200
- Identification: 0x1961 (6497)
- Flags: 0x00
- Fragment offset: 0
- Time to live: 128
- Protocol: UDP (0x11)
- Header checksum: 0xb7ff [correct]
- source: 163.22.16.47 (163.22.16.47)
- Destination: 163.22.18.105 (163.22.18.105)
- User Datagram Protocol, src Port: 8000 (8000), dst Port: 8000 (8000)
- Real-Time Transport Protocol

Hex dump:

```

0000  00 03 31 e4 2c 00 00 11 d8 27 91 42 08 00 45 00 ...
0010  00 c8 19 61 00 00 80 11 b7 ff a3 16 10 2f a3 16 ...
0020  12 69 1f 40 1f 40 00 b4 7e e0 80 80 00 01 00 00 ...
0030  00 a0 cb fb 70 a6 7e 7e 7e 7e 7e 7e 7e ff ff ff ...
0040  7e ff 7e 7e 7e 7e 7e 7e 7e 7e 7e 7e 7e 7e 7e ...
0050  7e 7e 7e 7e 7e 7e 7e 7e 7e 7e 7e 7e 7e 7e 7e ...
    
```

The 'Decode As' dialog box shows the 'Transport' tab selected. The 'Decode' radio button is chosen. The protocol list on the right includes RTP, which is highlighted. The 'Show Current' and 'Clear' buttons are visible.

# Display Filter

The screenshot shows the Wireshark 3.0 interface. The display filter is set to `ip.src==140.113.131.29`. The packet list pane shows several RTP packets from source 140.113.131.29 to destination 163.22.16.47. The packet details pane shows the structure of one of these packets: Ethernet II, Internet Protocol, User Datagram Protocol, and Session Initiation Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Info
6820	203.68568	140.113.131.29	163.22.16.47	RTP	Payload type=ITU-T G.711 PCMU, SSRC=850327
6821	203.70246	140.113.131.29	163.22.16.47	RTP	Payload type=ITU-T G.711 PCMU, SSRC=850327
6822	203.72898	140.113.131.29	163.22.16.47	RTP	Payload type=ITU-T G.711 PCMU, SSRC=850327
6824	203.74259	140.113.131.29	163.22.16.47	RTP	Payload type=ITU-T G.711 PCMU, SSRC=850327
6825	203.76035	140.113.131.29	163.22.16.47	RTP	Payload type=ITU-T G.711 PCMU, SSRC=850327
6826	203.78880	140.113.131.29	163.22.16.47	RTP	Payload type=ITU-T G.711 PCMU, SSRC=850327

```

+ Frame 178 (337 bytes on wire (337 bytes captured) on interface 0
+ Ethernet II, Src: 10.10.16.254 (00:03:31:e4:2c:00), Dst: 163.22.16.47 (00:11:d8:27:91:42)
+ Internet Protocol, Src: 140.113.131.29 (140.113.131.29), Dst: 163.22.16.47 (163.22.16.47)
+ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
+ Session Initiation Protocol
  
```

Offset	Hex	ASCII
0000	00 11 d8 27 91 42 00 03 31 e4 2c 00 08 00 45 00	... .B.. 1.....E.
0010	01 43 09 89 40 00 3b 11 72 4d 8c 71 83 1d a3 16	.C..@.;. rm.q....
0020	10 2f 13 c4 13 c4 01 2f c8 32 53 49 50 2f 32 2e	./...../ .2SIP/2.
0030	30 20 31 30 30 20 54 72 79 69 6e 67 0d 0a 43 61	0 100 Tr ying..Ca
0040	6c 6c 2d 49 44 3a 30 37 44 33 41 44 38 37 2d 31	71-ID:07 D3AD87-1
0050	33 37 42 2d 34 45 34 41 2d 39 39 42 43 2d 37 42	37B-4E4A -99BC-7B
0060	35 45 46 33 44 46 31 36 33 44 40 31 36 33 2e 32	5EF3DF16 3D@163.2
0070	32 2e 31 36 2e 34 37 0d 0a 43 6f 6e 74 65 6e 74	2.16.47. .Content

File: "C:\Documents and Settings\smartderrick\桌面\3" 1497 KB 00:04:05 | P: 7676 D: 234 M: 0

# Hold/Unhold of X-Lite



# Hold

Filter: sip

No.	Time	Source	Destination	Protocol	Info
614	9.894945	163.22.16.47	140.113.131.29	SIP/SD	Request: INVITE sip:22200@140.113.131.29, with sess
615	9.903660	140.113.131.29	163.22.16.47	SIP	Status: 100 Trying
616	9.968356	140.113.131.29	163.22.16.47	SIP	Status: 180 Ringing
639	13.251409	140.113.131.29	163.22.16.47	SIP/SD	Status: 200 Ok, with session description
640	13.259076	163.22.16.47	140.113.131.29	SIP	Request: ACK sip:22200@163.22.16.32:5060
3623	46.788267	140.113.131.29	163.22.16.47	SIP/SD	Request: INVITE sip:22300@163.22.16.47:5060, with s
3624	46.790676	163.22.16.47	140.113.131.29	SIP	Status: 100 Trying
3628	46.805196	163.22.16.47	140.113.131.29	SIP	Status: 180 Ringing
4147	56.656099	163.22.16.47	140.113.131.29	SIP/SD	Request: INVITE sip:22200@163.22.16.32:5060, with s
4148	56.664950	140.113.131.29	163.22.16.47	SIP	Status: 100 Trying
4149	56.668262	163.22.16.47	140.113.131.29	SIP/SD	Status: 200 Ok, with session description
4153	56.691699	140.113.131.29	163.22.16.47	SIP/SD	Status: 200 Ok, with session description
4154	56.694462	163.22.16.47	140.113.131.29	SIP	Request: ACK sip:22200@163.22.16.32:5060
4155	56.700447	140.113.131.29	163.22.16.47	SIP	Request: ACK sip:22300@163.22.16.47:5060
9030	108.832461	163.22.16.47	140.113.131.29	SIP/SD	Request: INVITE sip:22100@163.22.16.33:5060, with s
9031	108.838351	163.22.16.47	140.113.131.29	SIP/SD	Request: INVITE sip:22200@163.22.16.32:5060, with s
9032	108.842541	140.113.131.29	163.22.16.47	SIP	Status: 100 Trying
9035	108.847651	140.113.131.29	163.22.16.47	SIP	Status: 100 Trvina

Session Description Protocol version (v): 0

- Owner/Creator, Session Id (o): 22300 47093792 47140566 IN IP4 163.22.16.47
- Session Name (s): X-Lite
- Connection Information (c): IN IP4 0.0.0.0
- Time Description, active time (t): 0 0
- Media Description, name and address (m): audio 8000 RTP/AVP 0 8 3 98 97 101
- Media Attribute (a): rtpmap:0 pcmu/8000
- Media Attribute (a): rtpmap:8 pcma/8000
- Media Attribute (a): rtpmap:3 gsm/8000
- Media Attribute (a): rtpmap:98 iLBC/8000
- Media Attribute (a): rtpmap:97 speex/8000
- Media Attribute (a): rtpmap:101 telephone-event/8000

0000 00 03 31 e4 2c 00 00 11 d8 27 91 42 08 00 45 00 ..1.... .B..E.  
 0010 03 3f 87 29 00 00 80 11 ed b0 a3 16 10 2f 8c 71 ?.)..... ..../.q  
 0020 83 1d 13 c4 13 c4 03 2b a5 60 49 4e 56 49 54 45 .....+ . INVITE  
 0030 20 73 69 70 3a 32 32 32 30 30 40 31 36 33 2e 32 sip:222 00@163.2  
 0040 32 2e 31 36 2e 33 32 3a 35 30 36 30 20 53 49 50 2.16.32: 5060 SIP  
 0050 2f 32 2e 30 nd na 56 69 61 3a 20 53 49 50 2f 32 /? 0 vi a SIP/?

File: "C:\DOCUME~1\SMARTD~1\LOCALS~1\Temp\ether\XXXX0ZDM6S" 2188 KB ... | P: 10757 D: 38 M: 3 Drops: 0



# Retrieve

Filter: sip

No.	Time	Source	Destination	Protocol	Info
614	9.894945	163.22.16.47	140.113.131.29	SIP/SD	Request: INVITE sip:22200@140.113.131.29, with sess
615	9.903660	140.113.131.29	163.22.16.47	SIP	Status: 100 Trying
616	9.968356	140.113.131.29	163.22.16.47	SIP	Status: 180 Ringing
639	13.251409	140.113.131.29	163.22.16.47	SIP/SD	Status: 200 ok, with session description
640	13.259076	163.22.16.47	140.113.131.29	SIP	Request: ACK sip:22200@163.22.16.32:5060
3623	46.788267	140.113.131.29	163.22.16.47	SIP/SD	Request: INVITE sip:22300@163.22.16.47:5060, with s
3624	46.790676	163.22.16.47	140.113.131.29	SIP	Status: 100 Trying
3628	46.805196	163.22.16.47	140.113.131.29	SIP	Status: 180 Ringing
4147	56.656099	163.22.16.47	140.113.131.29	SIP/SD	Request: INVITE sip:22200@163.22.16.32:5060, with s
4148	56.664950	140.113.131.29	163.22.16.47	SIP	Status: 100 Trying
4149	56.668262	163.22.16.47	140.113.131.29	SIP/SD	Status: 200 ok, with session description
4153	56.691699	140.113.131.29	163.22.16.47	SIP/SD	Status: 200 ok, with session description
4154	56.694462	163.22.16.47	140.113.131.29	SIP	Request: ACK sip:22200@163.22.16.32:5060
4155	56.700447	140.113.131.29	163.22.16.47	SIP	Request: ACK sip:22300@163.22.16.47:5060
9030	108.832461	163.22.16.47	140.113.131.29	SIP/SD	Request: INVITE sip:22100@163.22.16.33:5060, with s
9031	108.838351	163.22.16.47	140.113.131.29	SIP/SD	Request: INVITE sip:22200@163.22.16.32:5060, with s
9032	108.842541	140.113.131.29	163.22.16.47	SIP	Status: 100 Trying
9035	108.847651	140.113.131.29	163.22.16.47	SIP	Status: 100 Trvina

Session Description Protocol Version (v): 0

- Owner/Creator, session Id (o): 22300 47093792 47192749 IN IP4 163.22.16.47
- Session Name (s): X-Lite
- Connection Information (c): IN IP4 163.22.16.47
- Time Description, active time (t): 0 0
- Media Description, name and address (m): audio 8000 RTP/AVP 0 8 3 98 97 101
- Media Attribute (a): rtpmap:0 pcmu/8000
- Media Attribute (a): rtpmap:8 pcma/8000
- Media Attribute (a): rtpmap:3 gsm/8000
- Media Attribute (a): rtpmap:98 iLBC/8000
- Media Attribute (a): rtpmap:97 speex/8000
- Media Attribute (a): rtpmap:101 telephone-event/8000

0000 00 03 31 e4 2c 00 00 11 d8 27 91 42 08 00 45 00 ..1.....'.B..E.

0010 03 44 90 c3 00 00 80 11 e4 11 a3 16 10 2f 8c 71 .D...../..q

0020 83 1d 13 c4 13 c4 03 30 de 2a 49 4e 56 49 54 45 .....0.\*INVITE

0030 20 73 69 70 3a 32 32 32 30 30 40 31 36 33 2e 32 sip:22 00@163.2

0040 32 2e 31 36 2e 33 32 3a 35 30 36 30 20 53 49 50 2.16.32: 5060 SIP

0050 2f 32 2e 30 0d 0a 56 69 61 3a 20 53 49 50 2f 32 /? 0 vi a\* SIP/?

File: "C:\DOCUME~1\SMARTD~1\LOCALS~1\Temp\ether\00000ZDM6S" 2188 KB ... | P: 10757 D: 38 M: 3 Drops: 0

# Summary

- We demonstrate the functions of Windows Messenger and X-Lite, 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

