SIPv6 Analyzer

Whai-En Chen
Research Assistant Professor
Dept. of Computer Science and Information Engineering
National Chiao Tung University
wechen@mail.nctu.edu.tw

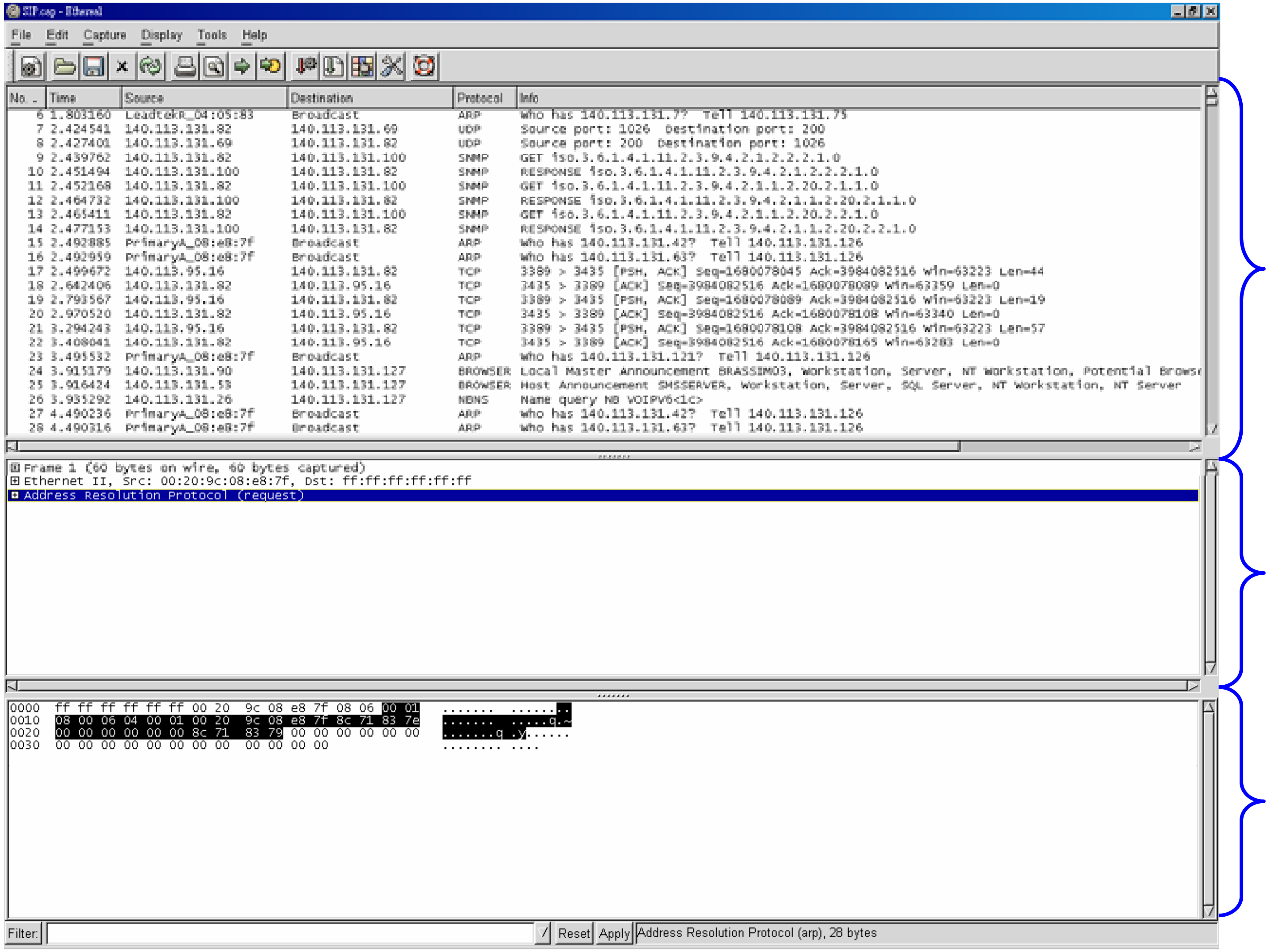
Outline

- Introduction
- Install and Uninstall Procedures
- Quick Start- User Guide
- Filtering Rules
- SIPv6 Analyzer Demo
  - Capturing Packets
  - SIP Functions: SIP Viewer and Flowcharts
  - RTP Function: RTP Spy (Playback)
- Conclusions
- Future Works

Introduction

- 構想：針對SIP與IPv6通訊協定，開發出一個簡單易用的分析工具
- SIPv6 Analyzer特色
  - 以call leg整理SIP信令
  - 繪出SIP信令流程圖
  - 重現RTP語音串流
  - 可調式Jitter Buffer
- 開發成員：賴健利、翁瑞鴻、蘇家永、宋岳鑫、蔡昌裕
- 目前維護：宋岳鑫 (yhsung@csie.nctu.edu.tw)
- 榮譽：2003國網盃程式設計比賽冠軍
  2004 IPv6 Appli-Contest實作組冠軍

A General Protocol Analyzer- Ethereal



```
No. . Time     Source                Destination        Protocol Info
    6 1.803160 LeadtekR_04:05:83     Broadcast          ARP      who has 140.113.131.7?  Tell 140.113.131.75
    7 2.424541 140.113.131.82        140.113.131.69     UDP      Source port: 1026  Destination port: 200
    8 2.427401 140.113.131.69        140.113.131.82     UDP      Source port: 200  Destination port: 1026
    9 2.439762 140.113.131.82        140.113.131.100    SNMP     GET iso.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
   10 2.451494 140.113.131.100       140.113.131.82     SNMP     RESPONSE iso.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
   11 2.452168 140.113.131.82        140.113.131.100    SNMP     GET iso.3.6.1.4.1.11.2.3.9.4.2.1.1.2.20.2.1.1.0
   12 2.464732 140.113.131.100       140.113.131.82     SNMP     RESPONSE iso.3.6.1.4.1.11.2.3.9.4.2.1.1.2.20.2.1.1.0
   13 2.465411 140.113.131.82        140.113.131.100    SNMP     GET iso.3.6.1.4.1.11.2.3.9.4.2.1.1.2.20.2.2.1.0
   14 2.477153 140.113.131.100       140.113.131.82     SNMP     RESPONSE iso.3.6.1.4.1.11.2.3.9.4.2.1.1.2.20.2.2.1.0
   15 2.492885 PrimaryA_08:e8:7f     Broadcast          ARP      who has 140.113.131.42?  Tell 140.113.131.126
   16 2.492959 PrimaryA_08:e8:7f     Broadcast          ARP      who has 140.113.131.63?  Tell 140.113.131.126
   17 2.499672 140.113.95.16         140.113.131.82     TCP      3389 > 3435 [PSH, ACK] Seq=1680078045 Ack=3984082516 Win=63223 Len=44
   18 2.642406 140.113.131.82        140.113.95.16      TCP      3435 > 3389 [ACK] Seq=3984082516 Ack=1680078089 Win=63359 Len=0
   19 2.793567 140.113.95.16         140.113.131.82     TCP      3389 > 3435 [PSH, ACK] Seq=1680078089 Ack=3984082516 Win=63223 Len=19
   20 2.970520 140.113.131.82        140.113.95.16      TCP      3435 > 3389 [ACK] Seq=3984082516 Ack=1680078108 Win=63340 Len=0
   21 3.294243 140.113.95.16         140.113.131.82     TCP      3389 > 3435 [PSH, ACK] Seq=1680078108 Ack=3984082516 Win=63223 Len=57
   22 3.408041 140.113.131.82        140.113.95.16      TCP      3435 > 3389 [ACK] Seq=3984082516 Ack=1680078165 Win=63283 Len=0
   23 3.495532 PrimaryA_08:e8:7f     Broadcast          ARP      who has 140.113.131.121?  Tell 140.113.131.126
   24 3.915179 140.113.131.90        140.113.131.127    BROWSER  Local Master Announcement BRASSIM03, Workstation, Server, NT Workstation, Potential Browse
   25 3.916424 140.113.131.53        140.113.131.127    BROWSER  Host Announcement SMSSERVER, Workstation, Server, SQL Server, NT Workstation, NT Server
   26 3.935292 140.113.131.26        140.113.131.127    NBNS     Name query NB VOIPV6<1c>
   27 4.490236 PrimaryA_08:e8:7f     Broadcast          ARP      who has 140.113.131.42?  Tell 140.113.131.126
   28 4.490316 PrimaryA_08:e8:7f     Broadcast          ARP      who has 140.113.131.63?  Tell 140.113.131.126
```

```
⊞ Frame 1 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: 00:20:9c:08:e8:7f, Dst: ff:ff:ff:ff:ff:ff
⊞ Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 20  9c 08 e8 7f 08 06 00 01   ........ ........
0010  08 00 06 04 00 01 00 20  9c 08 e8 7f 8c 71 83 7e   ........ ......q.~
0020  00 00 00 00 00 00 8c 71  83 79 00 00 00 00 00 00   .......q .y......
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

Address Resolution Protocol (arp), 28 bytes

Packet List

Protocol Parser

Hex Dump

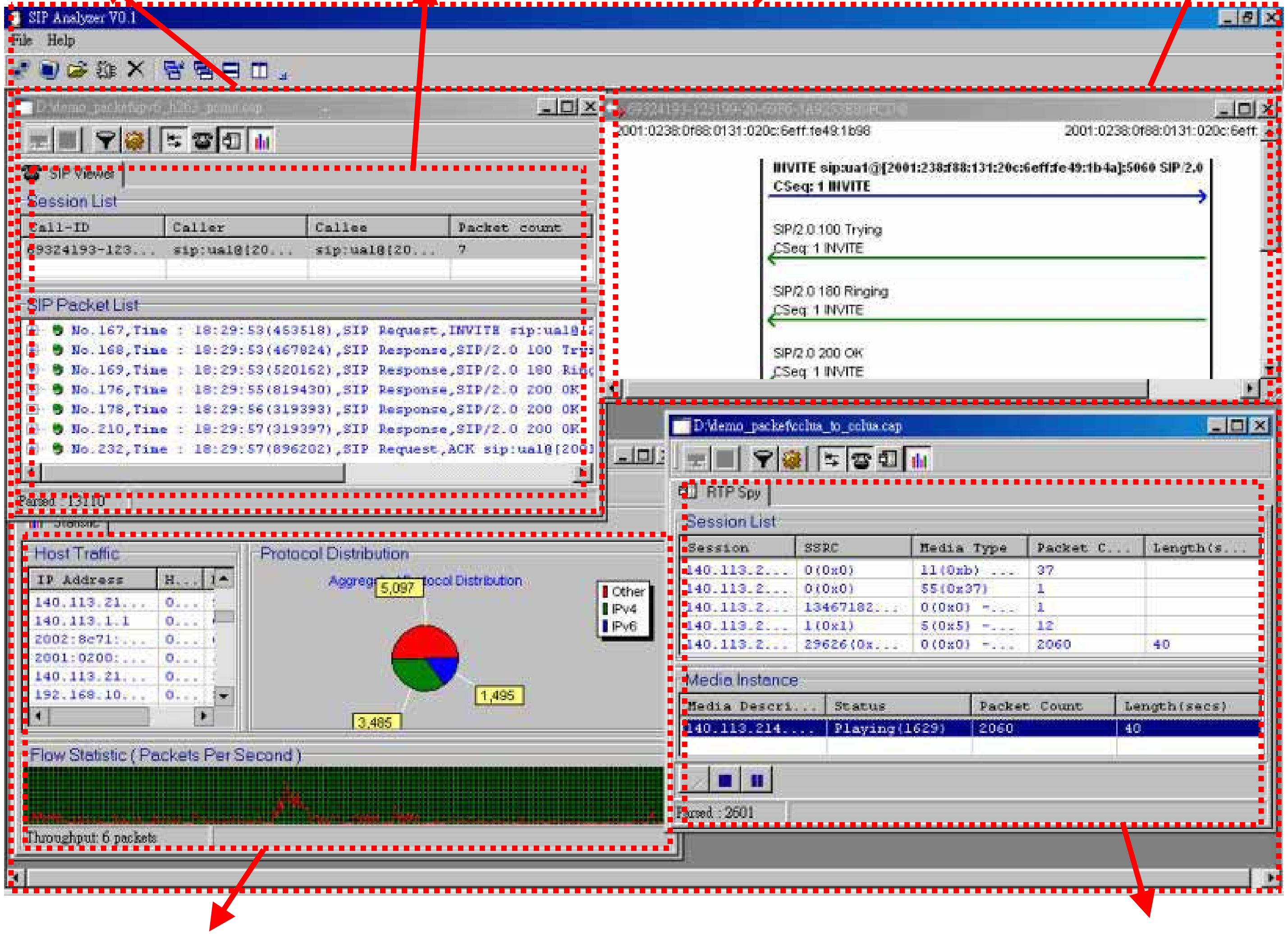
SIPv6 Analyzer

分析專案子視窗

封包解析子頁面

分析器主視窗

SIP信令圖形流程子視窗



Session List

Call-ID	Caller	Callee	Packet count
69324193-123...	sip:ua1@[20...	sip:ua1@[20...	7

SIP Packet List

```
No.167,Time : 18:29:53(463518),SIP Request,INVITE sip:ua1@[2
No.168,Time : 18:29:53(467824),SIP Response,SIP/2.0 100 Tryi
No.169,Time : 18:29:53(520162),SIP Response,SIP/2.0 180 Ring
No.176,Time : 18:29:55(819430),SIP Response,SIP/2.0 200 OK
No.178,Time : 18:29:56(319393),SIP Response,SIP/2.0 200 OK
No.210,Time : 18:29:57(319397),SIP Response,SIP/2.0 200 OK
No.232,Time : 18:29:57(896202),SIP Request,ACK sip:ua1@[200]
```

2001:0238:0f88:0131:020c:6eff:fe49:1b98 2001:0238:0f88:0131:020c:6eff:

INVITE sip:ua1@[2001:238:f88:131:20c:6eff:fe49:1b4a]:5060 SIP/2.0
CSeq: 1 INVITE

SIP/2.0 100 Trying
CSeq: 1 INVITE

SIP/2.0 180 Ringing
CSeq: 1 INVITE

SIP/2.0 200 OK
CSeq: 1 INVITE

Host Traffic

IP Address	H...
140.113.21...	0...
140.113.1.1	0...
2002:8c71:...	0...
2001:0200:...	0...
140.113.21...	0...
192.168.10...	0...

Protocol Distribution

Aggregate Protocol Distribution

Flow Statistic (Packets Per Second)

Session List

Session	SSRC	Media Type	Packet C...	Length(s...
140.113.2...	0(0x0)	11(0xb) ...	37	
140.113.2...	0(0x0)	55(0x37)	1	
140.113.2...	13467182...	0(0x0) -...	1	
140.113.2...	1(0x1)	5(0x5) -...	12	
140.113.2...	29626(0x...	0(0x0) -...	2060	40

Media Instance

Media Descri...	Status	Packet Count	Length(secs)
140.113.214....	Playing(1629)	2060	40

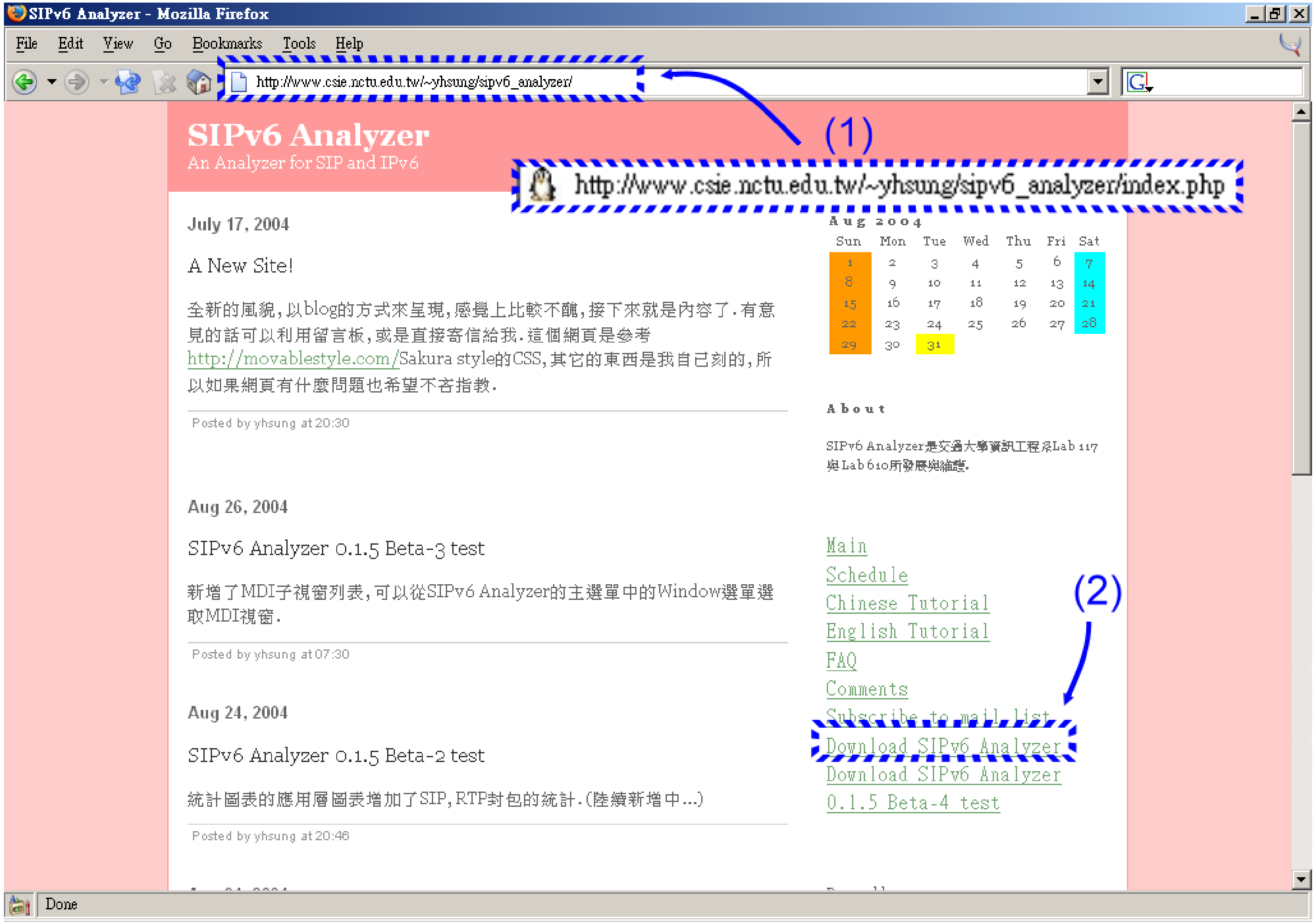
流量與通訊協定統子頁面

RTP監控與撥放子頁面

系統功能特點

- 安裝與反安裝功能
- 人性化之圖形使用介面
- 解析之通訊協定分析包括Ethernet2 Header、ARP、ICMPv4、IPv4、ICMPv6、IPv6、IPv6 Options 、IP(v4/v6)-in-IP(v4/v6) Tunnel、Teredo、 TCP、UDP、HTTP、FTP、DNS、SIP、SDP、RTCP、RTP
- SIP信令流程圖形化分析
- RTP串流監聽分析
- 流量與通訊協定統計
- 精靈式封包產生器
- 跨網路之遠端分析

Download the SIPv6 Analyzer



SIPv6 Analyzer - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
Done
(1)
(2)

http://www.csie.nctu.edu.tw/~yhsung/sipv6_analyzer/

http://www.csie.nctu.edu.tw/~yhsung/sipv6_analyzer/index.php

SIPv6 Analyzer

An Analyzer for SIP and IPv6

July 17, 2004

A New Site!

全新的風貌，以blog的方式來呈現，感覺上比較不醜，接下來就是內容了．有意見的話可以利用留言板，或是直接寄信給我．這個網頁是參考http://movablestyle.com/Sakura style的CSS，其它的東西是我自己刻的，所以如果網頁有什麼問題也希望不吝指教．

Posted by yhsung at 20:30

Aug 26, 2004

SIPv6 Analyzer 0.1.5 Beta-3 test

新增了MDI子視窗列表，可以從SIPv6 Analyzer的主選單中的Window選單選取MDI視窗．

Posted by yhsung at 07:30

Aug 24, 2004

SIPv6 Analyzer 0.1.5 Beta-2 test

統計圖表的應用層圖表增加了SIP，RTP封包的統計．(陸續新增中...)

Posted by yhsung at 20:46

Aug 2004

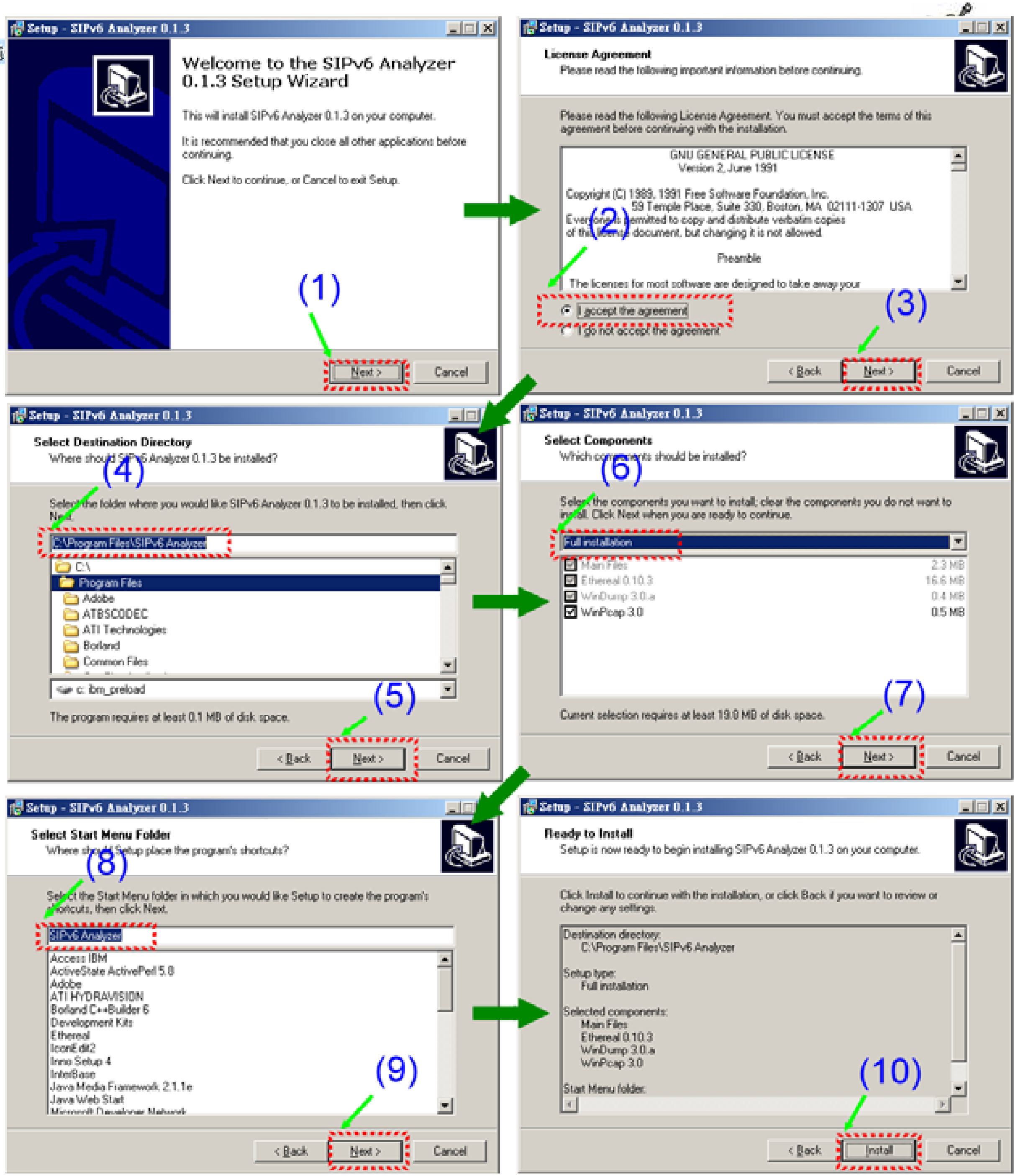
Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

About

SIPv6 Analyzer是交通大學資訊工程系Lab 117與Lab 610所發展與維護.

- Main
- Schedule
- Chinese Tutorial
- English Tutorial
- FAQ
- Comments
- Subscribe to mail list
- Download SIPv6 Analyzer
- Download SIPv6 Analyzer 0.1.5 Beta-4 test

Install the SIPv6 Analyzer



Setup - SIPv6 Analyzer 0.1.3

Welcome to the SIPv6 Analyzer 0.1.3 Setup Wizard

This will install SIPv6 Analyzer 0.1.3 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

(1) Next >

Setup - SIPv6 Analyzer 0.1.3

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your

(2) ● I accept the agreement

○ I do not accept the agreement

(3) Next >

Setup - SIPv6 Analyzer 0.1.3

Select Destination Directory

Where should SIPv6 Analyzer 0.1.3 be installed?

Select the folder where you would like SIPv6 Analyzer 0.1.3 to be installed, then click Next.

(4) C:\Program Files\SIPv6 Analyzer

C:\
Program Files
Adobe
ATBSCODEC
ATI Technologies
Borland
Common Files

c: ibm_preload

The program requires at least 0.1 MB of disk space.

(5) Next >

Setup - SIPv6 Analyzer 0.1.3

Select Components

Which components should be installed?

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

(6) Full installation

☑ Main Files	2.3 MB
☑ Ethereal 0.10.3	16.6 MB
☑ WinDump 3.0.a	0.4 MB
☑ WinPcap 3.0	0.5 MB

Current selection requires at least 19.0 MB of disk space.

(7) Next >

Setup - SIPv6 Analyzer 0.1.3

Select Start Menu Folder

Where should Setup place the program's shortcuts?

Select the Start Menu folder in which you would like Setup to create the program's shortcuts, then click Next.

(8) SIPv6 Analyzer

Access IBM
ActiveState ActivePerl 5.8
Adobe
ATI HYDRAVISION
Borland C++Builder 6
Development Kits
Ethereal
IconEdit2
Inno Setup 4
InterBase
Java Media Framework 2.1.1e
Java Web Start
Microsoft Developer Network

(9) Next >

Setup - SIPv6 Analyzer 0.1.3

Ready to Install

Setup is now ready to begin installing SIPv6 Analyzer 0.1.3 on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

Destination directory:
C:\Program Files\SIPv6 Analyzer

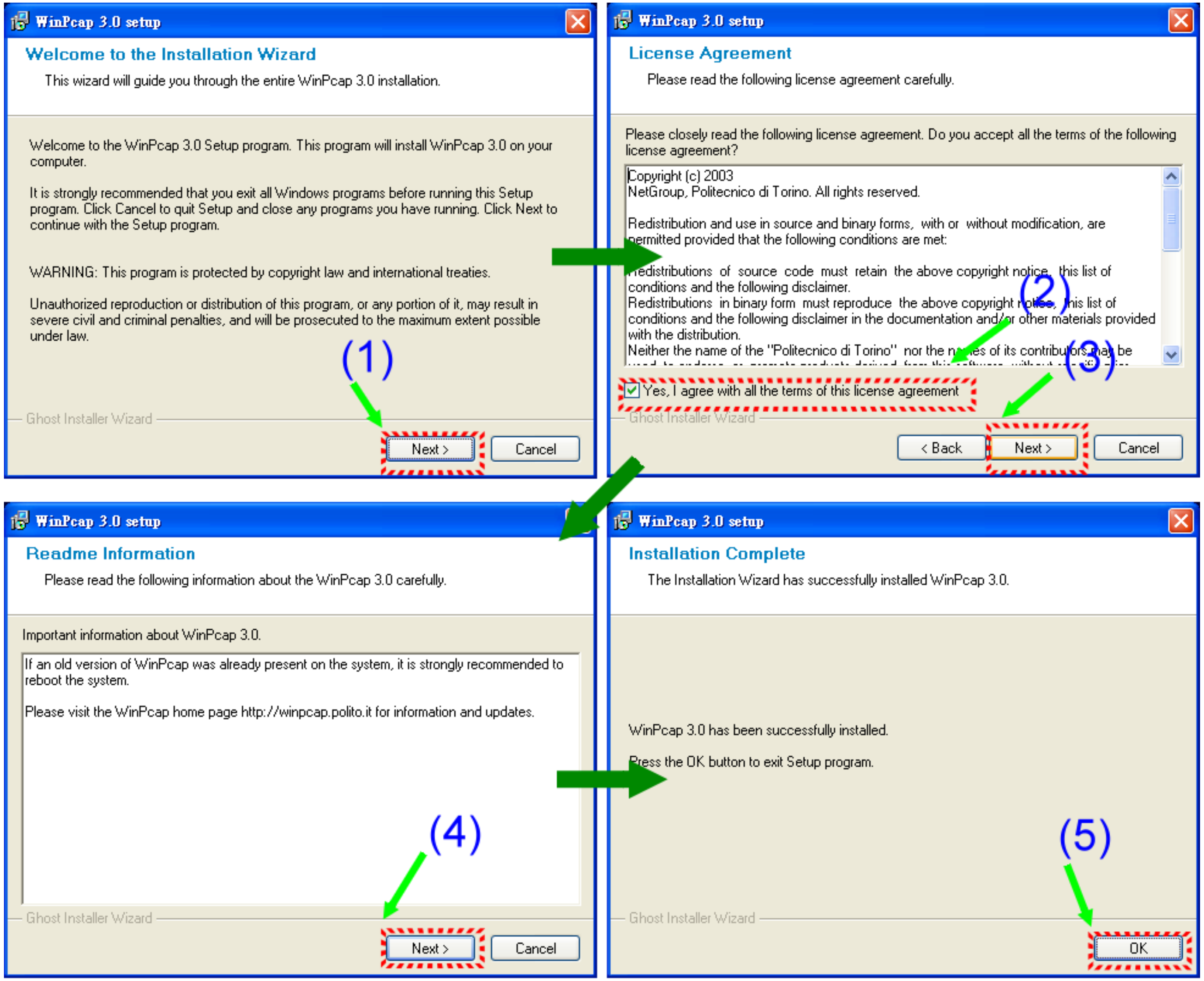
Setup type:
Full installation

Selected components:
Main Files
Ethereal 0.10.3
WinDump 3.0.a
WinPcap 3.0

Start Menu folder:

(10) Install

Install the WinPcap



WinPcap 3.0 setup

Welcome to the Installation Wizard

This wizard will guide you through the entire WinPcap 3.0 installation.

Welcome to the WinPcap 3.0 Setup program. This program will install WinPcap 3.0 on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup program. Click Cancel to quit Setup and close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

WinPcap 3.0 setup

License Agreement

Please read the following license agreement carefully.

Please closely read the following license agreement. Do you accept all the terms of the following license agreement?

Copyright (c) 2003
NetGroup, Politecnico di Torino. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
Neither the name of the "Politecnico di Torino" nor the names of its contributors may be

☑ Yes, I agree with all the terms of this license agreement

WinPcap 3.0 setup

Readme Information

Please read the following information about the WinPcap 3.0 carefully.

Important information about WinPcap 3.0.

If an old version of WinPcap was already present on the system, it is strongly recommended to reboot the system.

Please visit the WinPcap home page http://winpcap.polito.it for information and updates.

WinPcap 3.0 setup

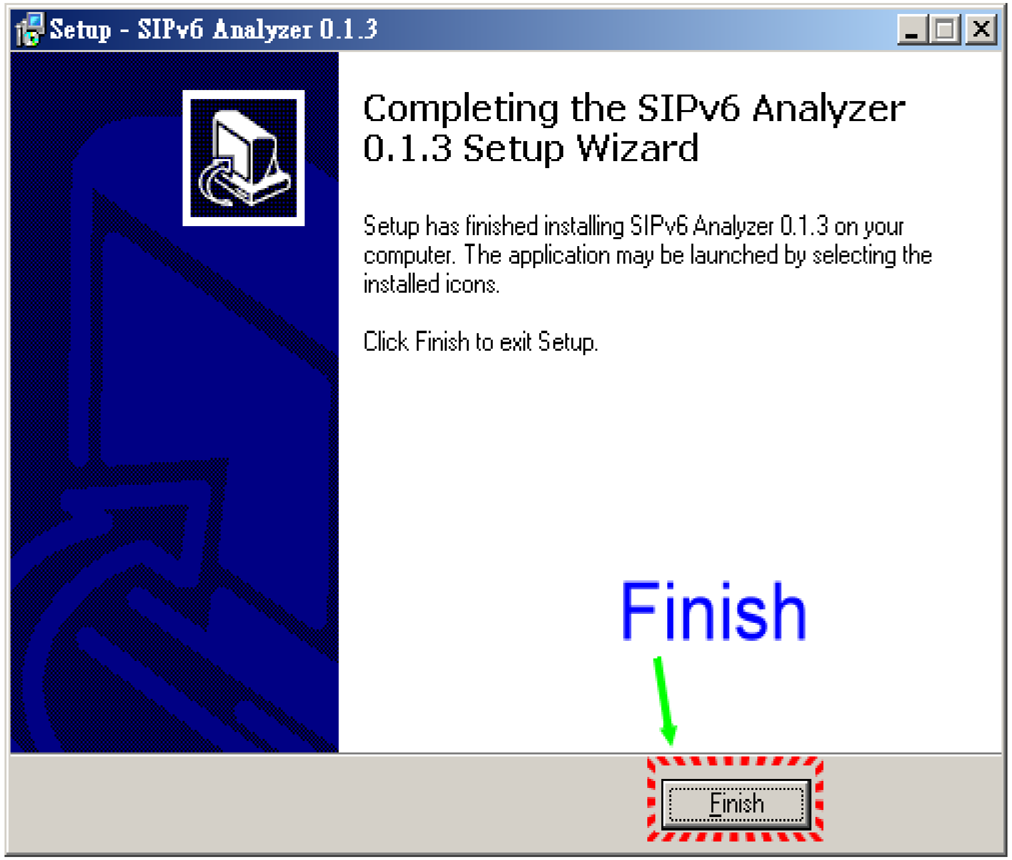
Installation Complete

The Installation Wizard has successfully installed WinPcap 3.0.

WinPcap 3.0 has been successfully installed.

Press the OK button to exit Setup program.

Finish Installation



Setup - SIPv6 Analyzer 0.1.3

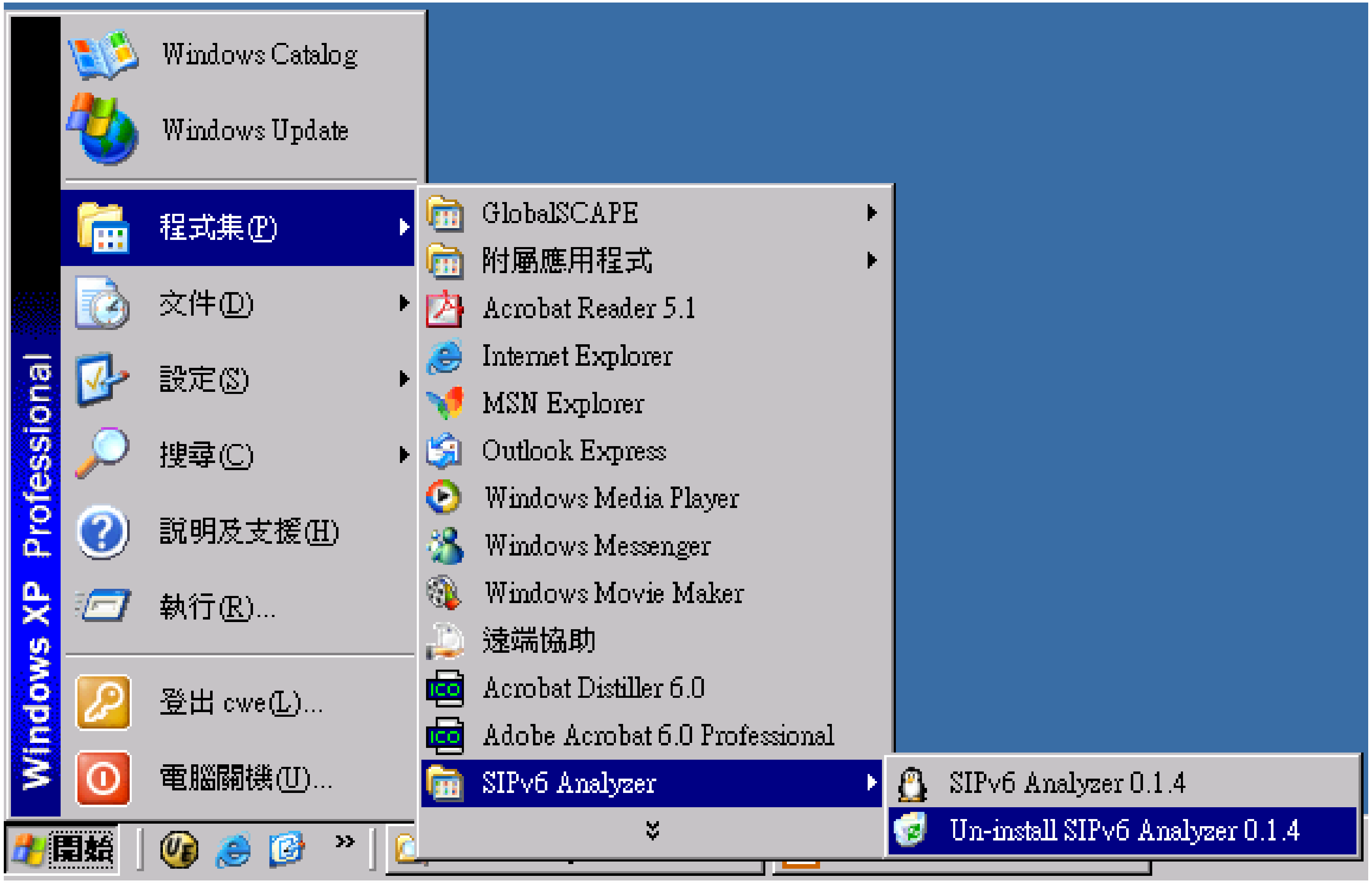
Completing the SIPv6 Analyzer 0.1.3 Setup Wizard

Setup has finished installing SIPv6 Analyzer 0.1.3 on your computer. The application may be launched by selecting the installed icons.

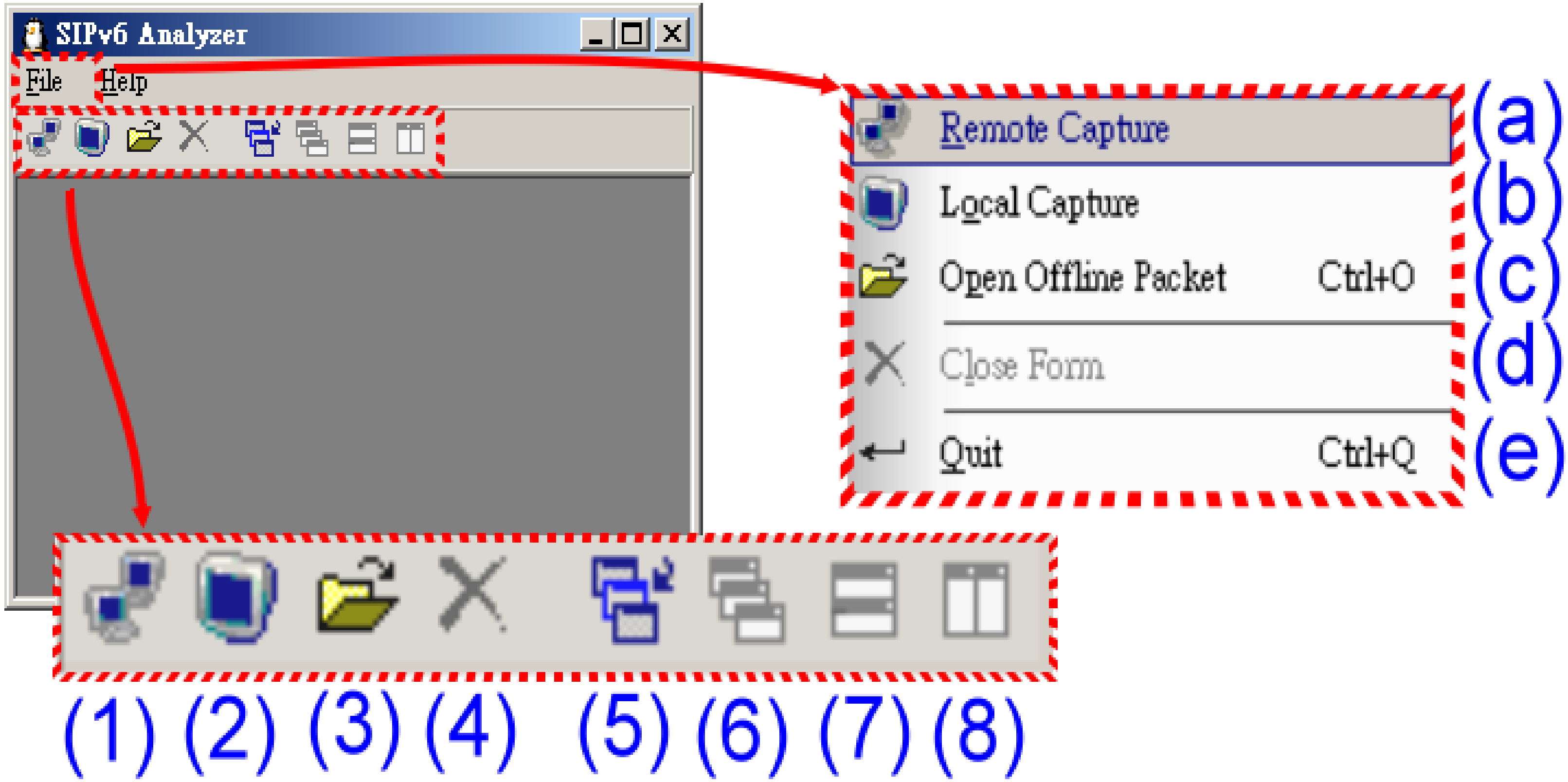
Click Finish to exit Setup.

Finish

Uninstall Procedure



Menu and Speed Buttons (1)



Menu and Speed Buttons (2)

Remote Capture(a)開啟遠端擷取封包功能

Local Capture (b)開啟本機擷取封包功能

Open Offline Packet (c)開啟已儲存之封包擷取檔案

Close Form (d)關閉擷取封包畫面

Quit (e)離開SIPv6 Analyzer

快捷按鈕(1)的功能與選單中的「Remote Capture」相同。

快捷按鈕(2)的功能與選單中的「Local Capture」相同。

快捷按鈕(3)的功能與選單中的「Open Offline Packet」相同。

快捷按鈕(4)的功能與選單中的「Close Form」相同。

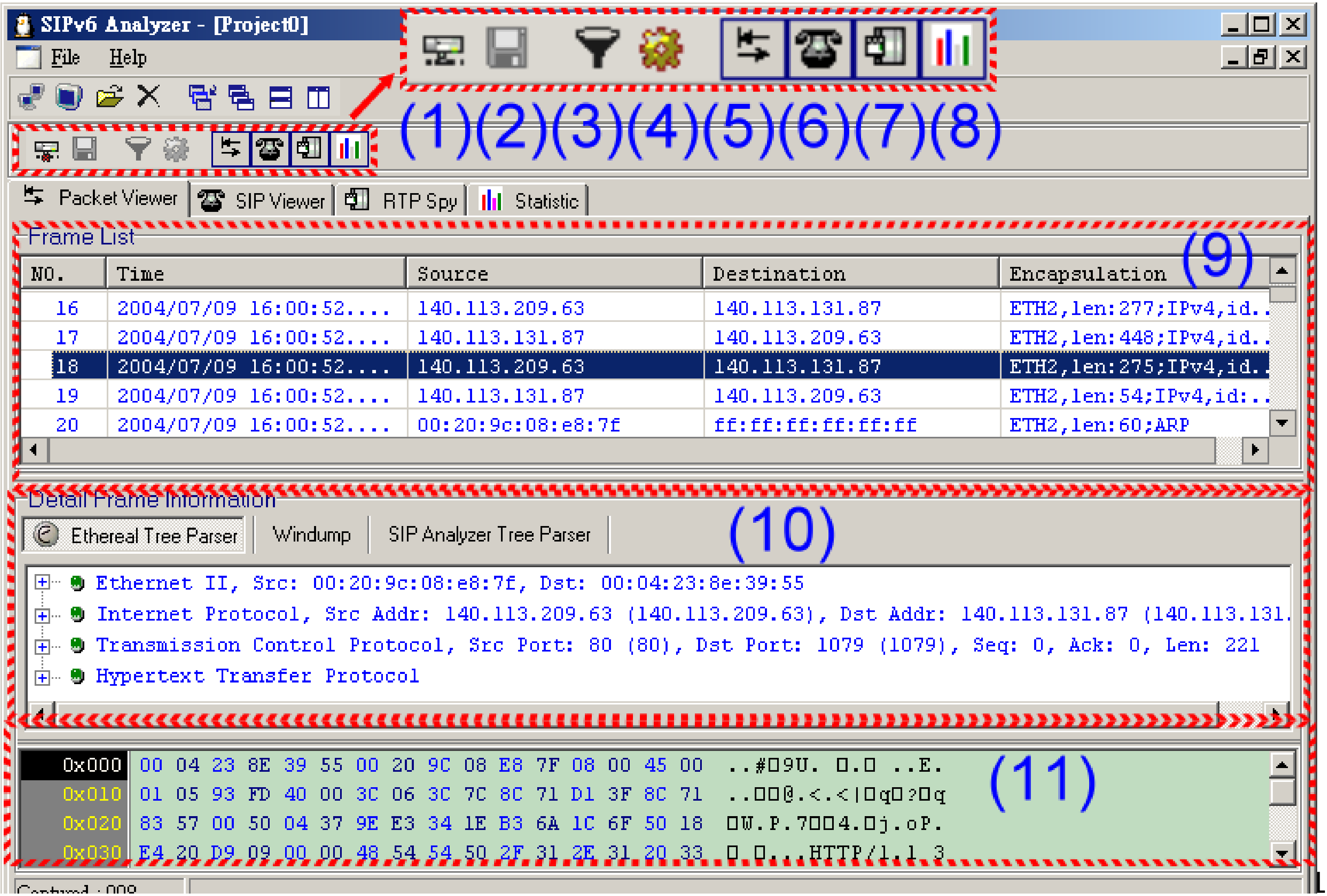
快捷按鈕(5)可以切換到下一個專案視窗。

快捷按鈕(6)可以將專案視窗重疊顯示。

快捷按鈕(7)可以將專案視窗做水平切割式的排列。

快捷按鈕(8)可以將專案視窗做垂直切割式的排列。

Analysis Project (1)



NO.	Time	Source	Destination	Encapsulation
16	2004/07/09 16:00:52....	140.113.209.63	140.113.131.87	ETH2,len:277;IPv4,id..
17	2004/07/09 16:00:52....	140.113.131.87	140.113.209.63	ETH2,len:448;IPv4,id..
18	2004/07/09 16:00:52....	140.113.209.63	140.113.131.87	ETH2,len:275;IPv4,id..
19	2004/07/09 16:00:52....	140.113.131.87	140.113.209.63	ETH2,len:54;IPv4,id:..
20	2004/07/09 16:00:52....	00:20:9c:08:e8:7f	ff:ff:ff:ff:ff:ff	ETH2,len:60;ARP

```
⊞ Ethernet II, Src: 00:20:9c:08:e8:7f, Dst: 00:04:23:8e:39:55
⊞ Internet Protocol, Src Addr: 140.113.209.63 (140.113.209.63), Dst Addr: 140.113.131.87 (140.113.131.
⊞ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 1079 (1079), Seq: 0, Ack: 0, Len: 221
⊞ Hypertext Transfer Protocol
```

```
0x000  00 04 23 8E 39 55 00 20 9C 08 E8 7F 08 00 45 00  ..#□9U. □.□ ..E.
0x010  01 05 93 FD 40 00 3C 06 3C 7C 8C 71 D1 3F 8C 71  ..□□@.<.<|□q□?□q
0x020  83 57 00 50 04 37 9E E3 34 1E B3 6A 1C 6F 50 18  □W.P.7□□4.□j.oP.
0x030  E4 20 D9 09 00 00 48 54 54 50 2F 31 2E 31 20 33  □.□...HTTP/1.1 3
```

Analysis Project (2)

快捷按鈕(1)是開始/停止擷取封包的控制按鈕。

快捷按鈕(2)可以將擷取下來的封包儲存成檔案。

快捷按鈕(3)套用/取消Capture filter 或Display filter 的設定。

快捷按鈕(4)可以設定Capture filter或Display filter。

快捷按鈕(5)是開啟/關閉「Packet Viewer」頁面的控制按鈕。

快捷按鈕(6)是開啟/關閉「SIP Viewer」頁面的控制按鈕。

快捷按鈕(7)是開啟/關閉「RTP Spy」頁面的控制按鈕。

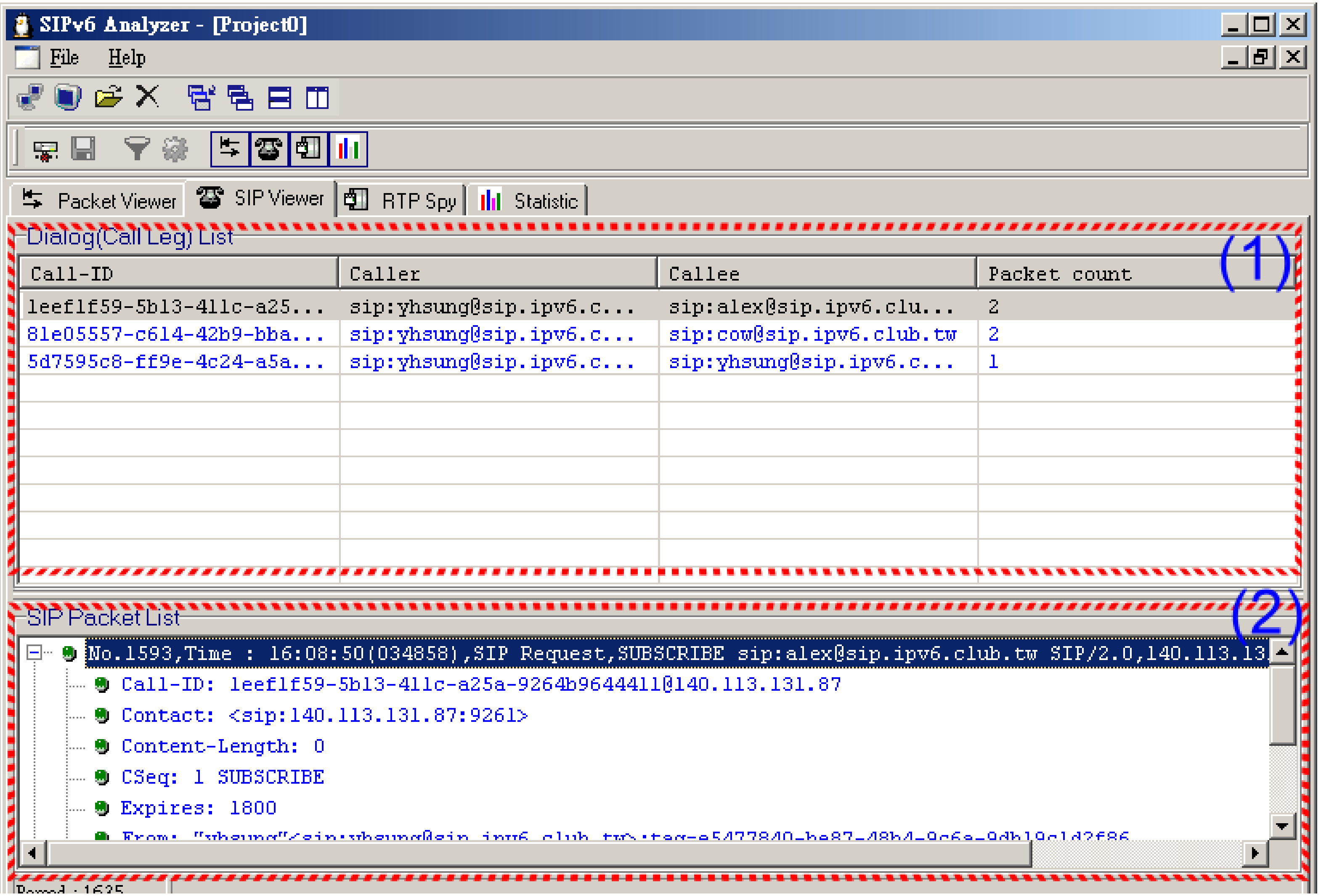
快捷按鈕(8)是開啟/關閉「Statistics」頁面的控制按鈕。

「Frame List」區塊(9)將所擷取到的封包都會列在上面，並顯示擷取到的封包編號、擷取到的時間、來源位址、目的位址以及封包的封裝。

「Detail Frame Information」區塊(10)顯示出被選擇封包的詳細內容。

「Hex Information」區塊(11)將封包的原始內容直接以十六進位方式表現。

SIP Viewer (1)



Dialog(Call Leg) List

Call-ID	Caller	Callee	Packet count
leef1f59-5b13-411c-a25...	sip:yhsung@sip.ipv6.c...	sip:alex@sip.ipv6.clu...	2
81e05557-c614-42b9-bba...	sip:yhsung@sip.ipv6.c...	sip:cow@sip.ipv6.club.tw	2
5d7595c8-ff9e-4c24-a5a...	sip:yhsung@sip.ipv6.c...	sip:yhsung@sip.ipv6.c...	1

SIP Packet List

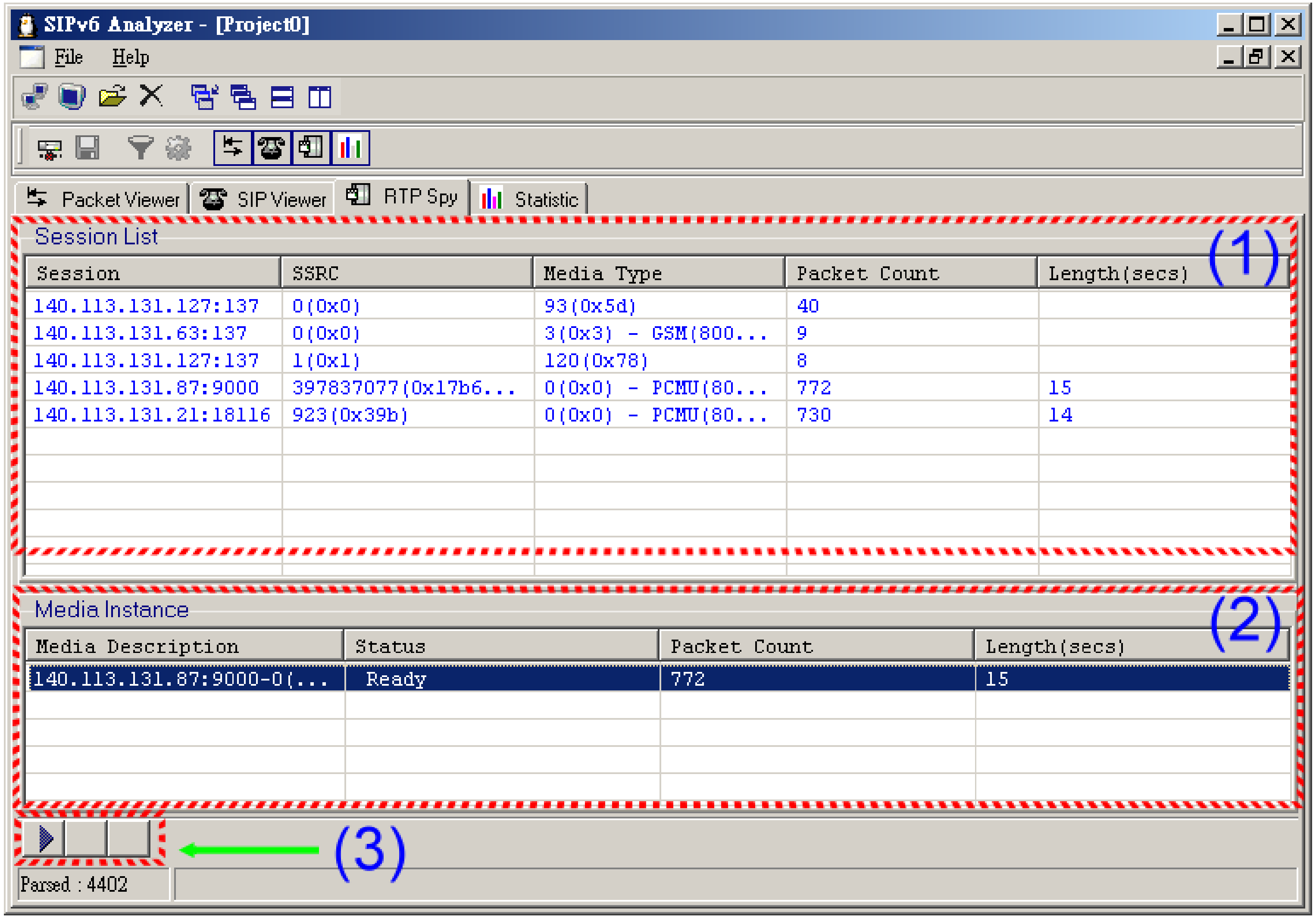
```
No.1593,Time : 16:08:50(034858),SIP Request,SUBSCRIBE sip:alex@sip.ipv6.club.tw SIP/2.0,140.113.13
    Call-ID: leef1f59-5b13-411c-a25a-9264b9644411@140.113.131.87
    Contact: <sip:140.113.131.87:9261>
    Content-Length: 0
    CSeq: 1 SUBSCRIBE
    Expires: 1800
    From: "yhsung"<sip:yhsung@sip.ipv6.club.tw>;tag=e5477840-be87-48b4-9c6a-9db19c1d2f86
```

Parsed : 1635

SIP Viewer (2)

- 「Dialog(Call-leg) List」區塊(1)將SIP訊息整理成Dialog (call leg)的方式顯示。「Call-ID」欄位是SIP訊息中的Call-ID標頭，「Caller」欄位(表示發話方)是SIP訊息中的From標頭。「Callee」欄位(表示受話方)是SIP訊息中的To標頭。
- 「SIP Packet List」區塊(2)為同一個Dialog中，所有SIP訊息的清單。

RTP Spy (1)



Session List

Session	SSRC	Media Type	Packet Count	Length(secs)
140.113.131.127:137	0(0x0)	93(0x5d)	40	
140.113.131.63:137	0(0x0)	3(0x3) - GSM(800...	9	
140.113.131.127:137	1(0x1)	120(0x78)	8	
140.113.131.87:9000	397837077(0x17b6...	0(0x0) - PCMU(80...	772	15
140.113.131.21:18116	923(0x39b)	0(0x0) - PCMU(80...	730	14

Media Instance

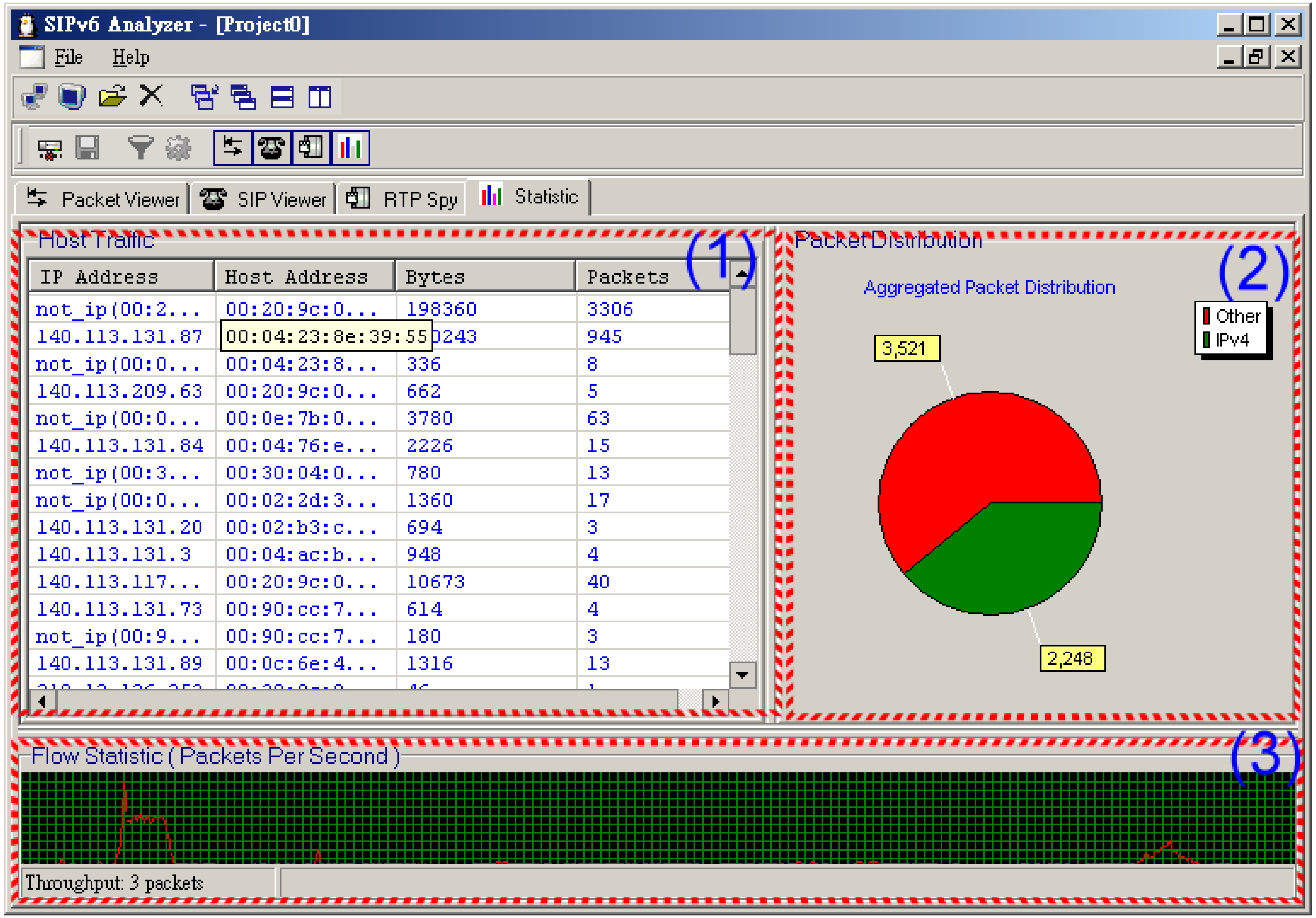
Media Description	Status	Packet Count	Length(secs)
140.113.131.87:9000-0(...	Ready	772	15

Parsed : 4402

RTP Spy (2)

- 「Session List」區塊(1)將一次通話中相同來源的RTP封包整理成一筆資料。「Session」欄位代表的是目的位址與通訊埠，「SSRC」欄位即RTP封包中所帶的SSRC (Synchronization Source)，「Media Type」欄位為RTP封包所使用的語音編碼，「Packet Count」欄位代表此Session所包含的RTP封包總數，「Length」欄位代表該次通話所進行的時間。
- 「Media Instance」區塊(2)在滑鼠左鍵雙擊點選「Session List」中的一筆資料後，可以在這個列表中選擇所要播放的RTP串流，「Media Description」欄位代表的是此RTP串流的目的位址與通訊埠，「Status」欄位代表此RTP串流的狀態為播放中/播放完畢/可以播放，「Packet Count」欄位代表此RTP串流的封包總數，「Length」欄位代表此RTP串流的時間。
- 「Play Control Panel」區塊(3)用來控制使用者所要播放的RTP串流，由左而右有播放、停止以及暫停。

Statistic (1)



Host Traffic

IP Address	Host Address	Bytes	Packets
not_ip(00:2...	00:20:9c:0...	198360	3306
140.113.131.87	00:04:23:8e:39:55	0243	945
not_ip(00:0...	00:04:23:8...	336	8
140.113.209.63	00:20:9c:0...	662	5
not_ip(00:0...	00:0e:7b:0...	3780	63
140.113.131.84	00:04:76:e...	2226	15
not_ip(00:3...	00:30:04:0...	780	13
not_ip(00:0...	00:02:2d:3...	1360	17
140.113.131.20	00:02:b3:c...	694	3
140.113.131.3	00:04:ac:b...	948	4
140.113.117...	00:20:9c:0...	10673	40
140.113.131.73	00:90:cc:7...	614	4
not_ip(00:9...	00:90:cc:7...	180	3
140.113.131.89	00:0c:6e:4...	1316	13

Packet Distribution

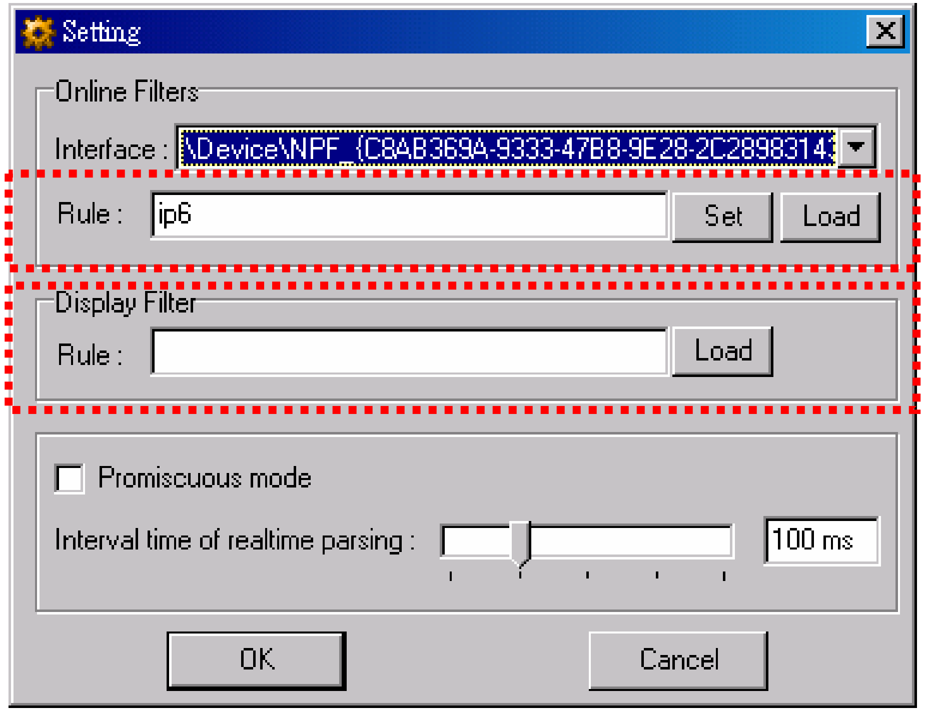
Flow Statistic (Packets Per Second)

Throughput: 3 packets

Statistic (2)

- 「Host Traffic」區塊(1)是對於各個主機位址的網路流量列表，「IP Address」欄位代表的是主機的IP位址，「Host Address」欄位代表的是主機的資料連結層位址，如Ethernet中的MAC (Media Access Control) 位址。「Bytes」欄位代表對該主機傳送的總位元組個數，「Packets」欄位代表對該主機傳送的總封包數。
- 「Packet Distribution」區塊(2)是IPv4/IPv6/otheres通訊協定的封包分佈圓餅圖。
- 「Flow Statistics」區塊(3)是目前網路流量的輸出速率圖表。

Set Filtering Rules



Interface : \Device\NPF_{C8AB369A-9333-47B8-9E28-2C2898314

Rule : ip6

Rule :

□ Promiscuous mode

Interval time of realtime parsing : 100 ms

Set Capture Filter

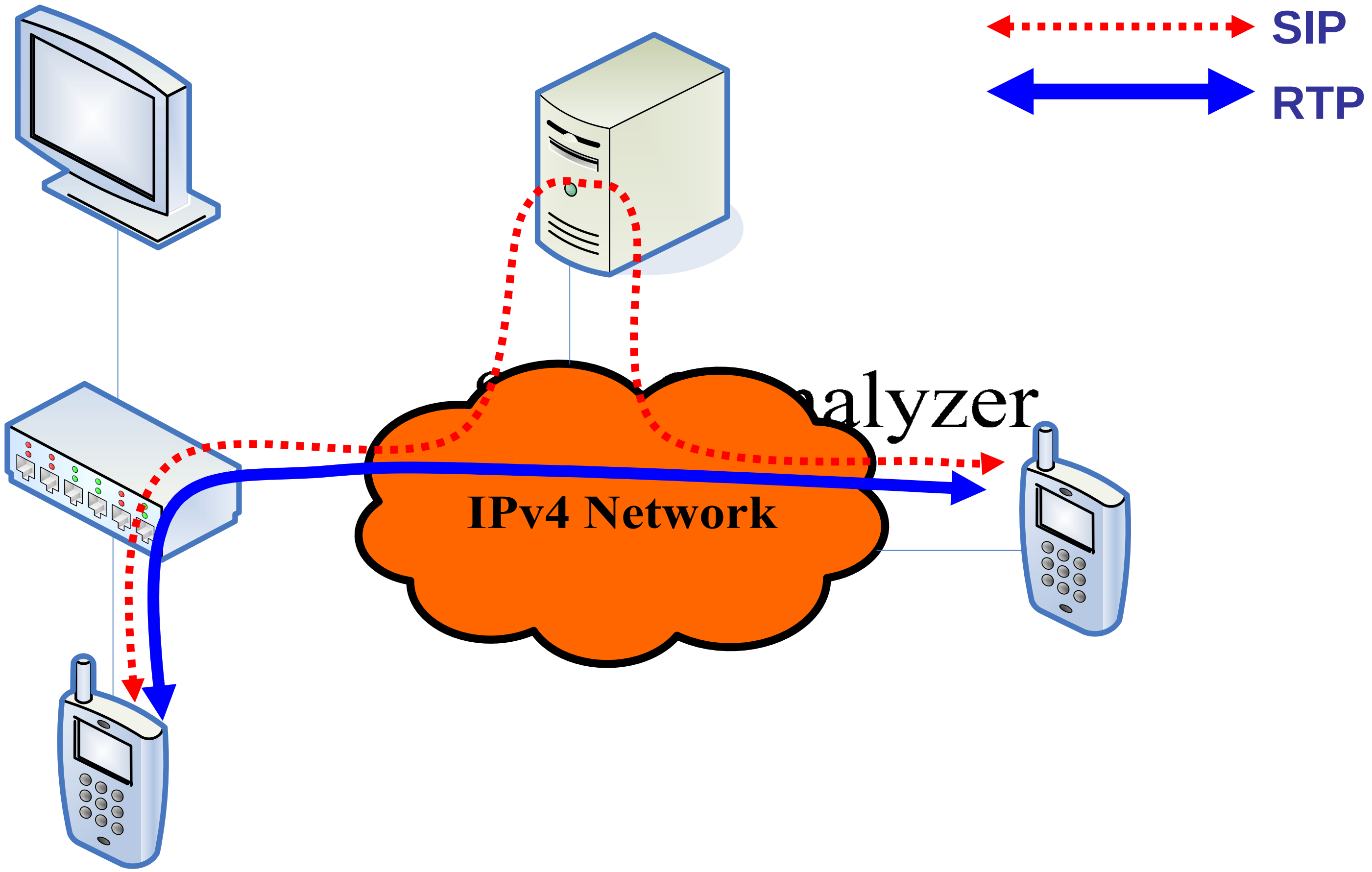
Set Display Filter

Filtering Rules

- SIPv6 Analyzer provides two Filters: Capture Filter and Display Filter.
- The filter rule is the same as the tcpdump.
- Some useful examples:
  - host 140.113.1.1 (capture the packet from and to 140.113.1.1)
  - dst 140.113.1.1 / src 140.113.1.1 (to/from 140.113.1.1)
  - net 205.153.60.0 mask 255.255.255.0 (for a subnet)
  - udp port 5060 (for SIP; port 9000 for RTP)
  - host 140.113.1.1 and udp port 5060
  - ip6 (for IPv6 packets)

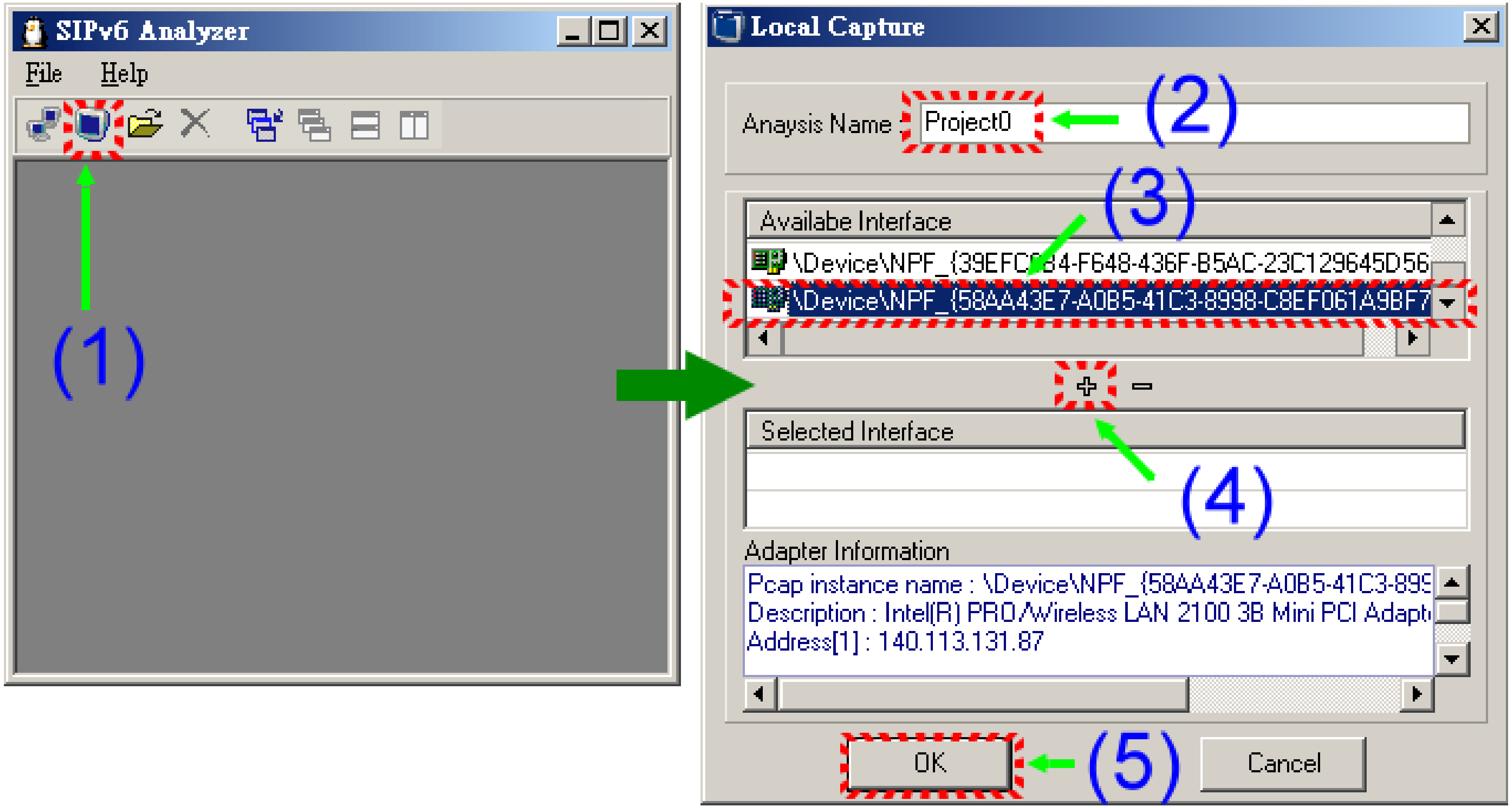
SIPv6 Analyzer Demo

Demo Environment



SI
140.

Operation (1)



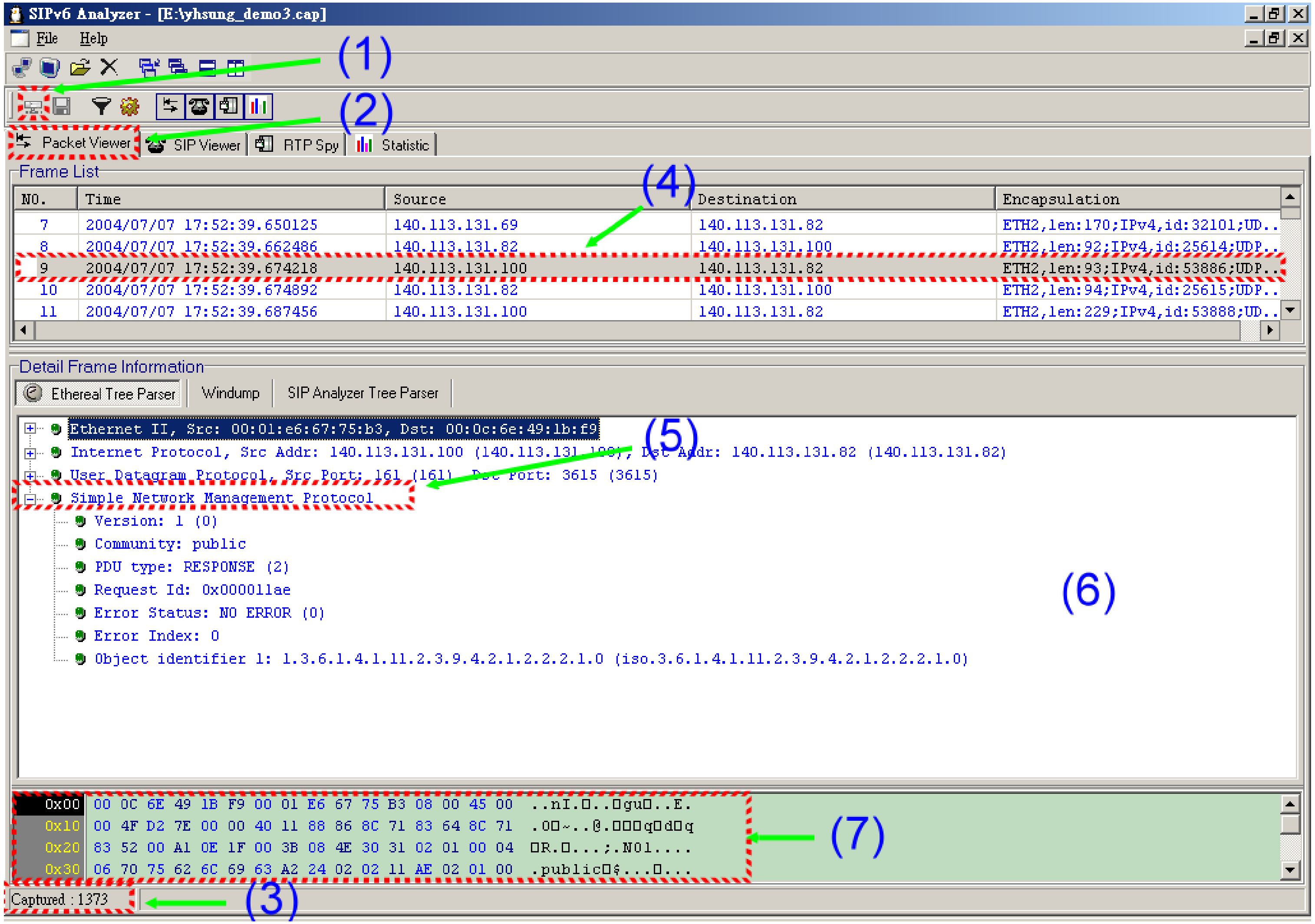
Anaysis Name : Project0

Availabe Interface
\Device\NPF_{39EFC6B4-F648-436F-B5AC-23C129645D56
\Device\NPF_{58AA43E7-A0B5-41C3-8998-C8EF061A9BF7

Selected Interface

Adapter Information
Pcap instance name : \Device\NPF_{58AA43E7-A0B5-41C3-899
Description : Intel(R) PRO/Wireless LAN 2100 3B Mini PCI Adapt
Address[1] : 140.113.131.87

Operation (2)



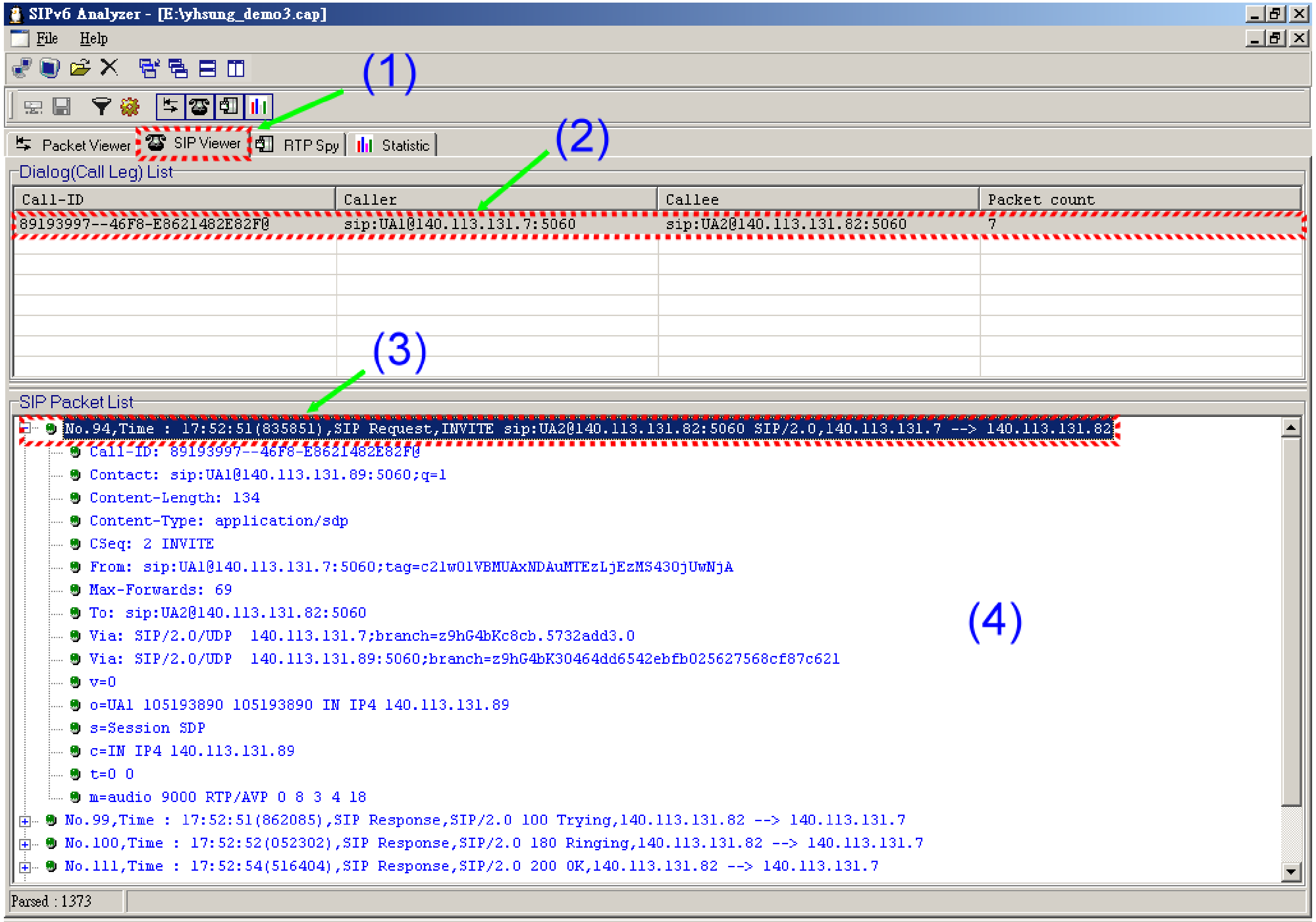
NO.	Time	Source	Destination	Encapsulation
7	2004/07/07 17:52:39.650125	140.113.131.69	140.113.131.82	ETH2,len:170;IPv4,id:32101;UD..
8	2004/07/07 17:52:39.662486	140.113.131.82	140.113.131.100	ETH2,len:92;IPv4,id:25614;UDP..
9	2004/07/07 17:52:39.674218	140.113.131.100	140.113.131.82	ETH2,len:93;IPv4,id:53886;UDP..
10	2004/07/07 17:52:39.674892	140.113.131.82	140.113.131.100	ETH2,len:94;IPv4,id:25615;UDP..
11	2004/07/07 17:52:39.687456	140.113.131.100	140.113.131.82	ETH2,len:229;IPv4,id:53888;UD..

```
Ethernet II, Src: 00:01:e6:67:75:b3, Dst: 00:0c:6e:49:1b:f9
Internet Protocol, Src Addr: 140.113.131.100 (140.113.131.100), Dst Addr: 140.113.131.82 (140.113.131.82)
User Datagram Protocol, Src Port: 161 (161), Dst Port: 3615 (3615)
Simple Network Management Protocol
    Version: 1 (0)
    Community: public
    PDU type: RESPONSE (2)
    Request Id: 0x000011ae
    Error Status: NO ERROR (0)
    Error Index: 0
    Object identifier 1: 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0 (iso.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0)
```

```
0x00  00 0C 6E 49 1B F9 00 01 E6 67 75 B3 08 00 45 00  ..nI.□..□gu□..E.
0x10  00 4F D2 7E 00 00 40 11 88 86 8C 71 83 64 8C 71  .O□~..@.□□□q□d□q
0x20  83 52 00 A1 0E 1F 00 3B 08 4E 30 31 02 01 00 04  □R.□...;.N01....
0x30  06 70 75 62 6C 69 63 A2 24 02 02 11 AE 02 01 00  .public□$...□...
```

Captured : 1373

SIP Viewer: SIP Messages



Dialog(Call Leg) List

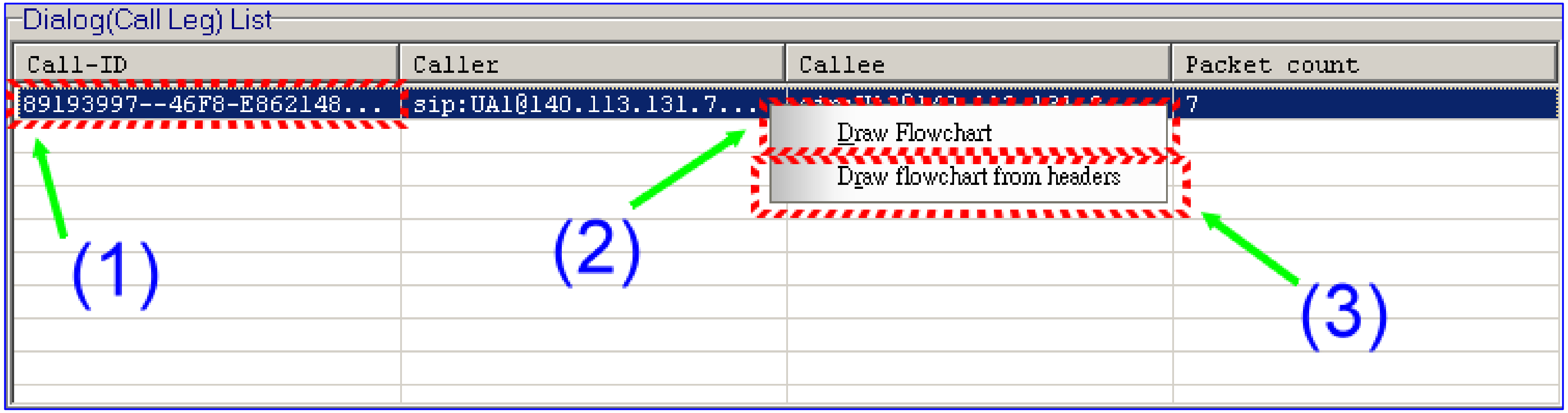
Call-ID	Caller	Callee	Packet count
89193997--46F8-E8621482E82F@	sip:UA1@140.113.131.7:5060	sip:UA2@140.113.131.82:5060	7

SIP Packet List

```
No.94,Time : 17:52:51(835851),SIP Request,INVITE sip:UA2@140.113.131.82:5060 SIP/2.0,140.113.131.7 --> 140.113.131.82
    Call-ID: 89193997--46F8-E8621482E82F@
    Contact: sip:UA1@140.113.131.89:5060;q=1
    Content-Length: 134
    Content-Type: application/sdp
    CSeq: 2 INVITE
    From: sip:UA1@140.113.131.7:5060;tag=c21w01VBMUAxNDAuMTEzLjEzMS430jUwNjA
    Max-Forwards: 69
    To: sip:UA2@140.113.131.82:5060
    Via: SIP/2.0/UDP  140.113.131.7;branch=z9hG4bKc8cb.5732add3.0
    Via: SIP/2.0/UDP  140.113.131.89:5060;branch=z9hG4bK30464dd6542ebfb025627568cf87c621
    v=0
    o=UA1 105193890 105193890 IN IP4 140.113.131.89
    s=Session SDP
    c=IN IP4 140.113.131.89
    t=0 0
    m=audio 9000 RTP/AVP 0 8 3 4 18
No.99,Time : 17:52:51(862085),SIP Response,SIP/2.0 100 Trying,140.113.131.82 --> 140.113.131.7
No.100,Time : 17:52:52(052302),SIP Response,SIP/2.0 180 Ringing,140.113.131.82 --> 140.113.131.7
No.111,Time : 17:52:54(516404),SIP Response,SIP/2.0 200 OK,140.113.131.82 --> 140.113.131.7
```

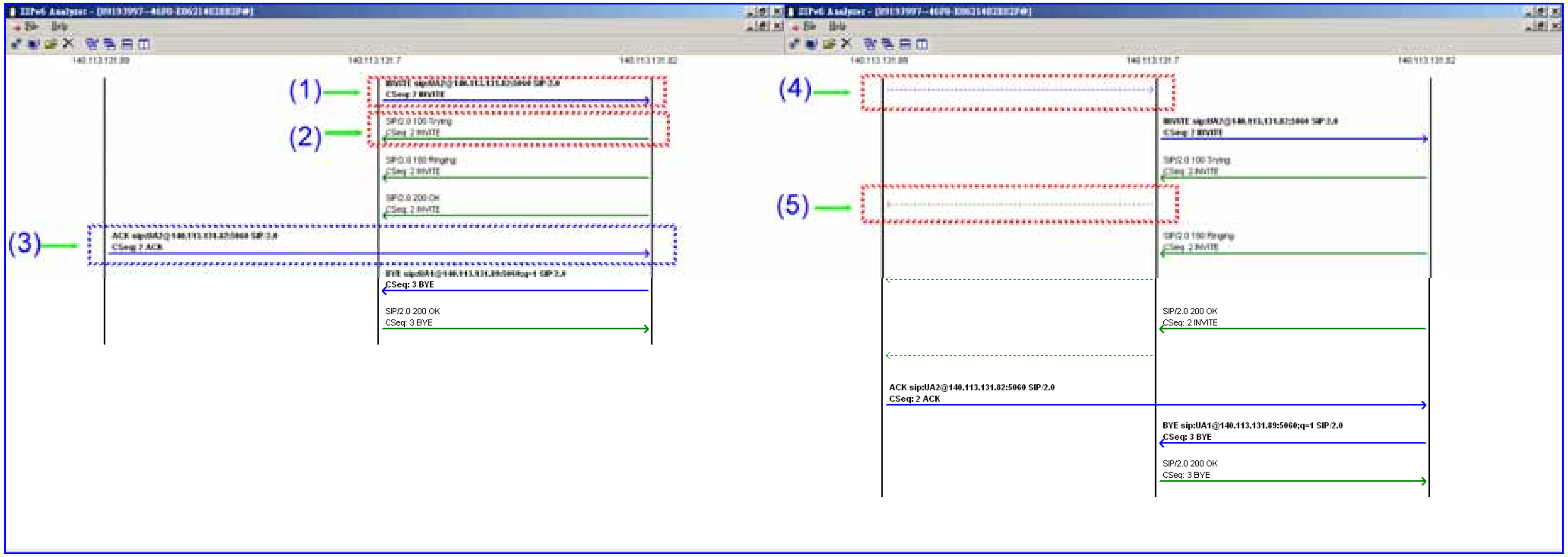
Parsed : 1373

SIP Flowcharts

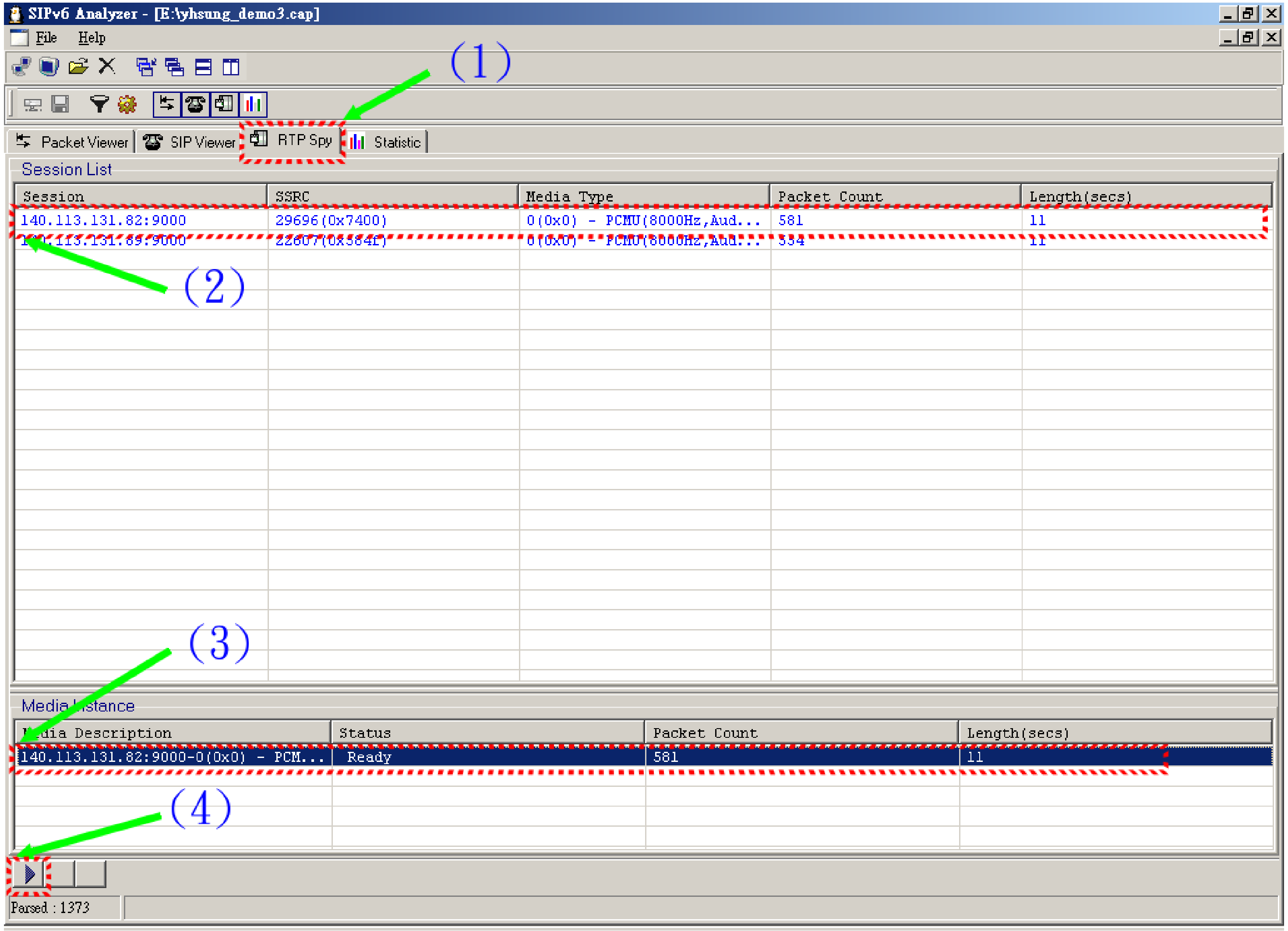


Dialog(Call Leg) List

Call-ID	Caller	Callee	Packet count
89193997--46F8-E862148...	sip:UA1@140.113.131.7...		7



RTP Spy: RTP Playback



Session List

Session	SSRC	Media Type	Packet Count	Length(secs)
140.113.131.82:9000	29696(0x7400)	0(0x0) - PCMU(8000Hz,Aud...	581	11
140.113.131.89:9000	22607(0x584f)	0(0x0) - PCMU(8000Hz,Aud...	334	11

Media Instance

Media Description	Status	Packet Count	Length(secs)
140.113.131.82:9000-0(0x0) - PCM...	Ready	581	11

Parsed : 1373

Conclusions

- SIPv6 Analyzer provides several functions (e.g., SIP Viewer and RTP Spy) for the users who attempt to debug the SIP VoIP network or the SIP devices.
- SIPv6 Analyzer can be downloaded in the web page (i.e. http://www.csie.nctu.edu.tw/~yhsung/sipv6_analyzer)
- Users can fills the registration form and will be informed when the SIPv6 Analyzer is upgraded.
- Users can contact Dr. Chen (wechen@mail.nctu.edu.tw) for any further research or cooperation possibility.
- Users can contact Mr. Sung (yhsung@csie.nctu.edu.tw) for the comments or bugs of SIPv6 Analyzer.

Future Works

- SIP message comparison
- Video playback for RTP packets
- G.723, G.729 and GSM codec translation
- Stable packet generator
- Script input interface
- Test patent for SIP applications
- IPv6 test tool
- Fast sort data structure and algorithm for RTP Spy
- Automatic jitter buffer adjustment algorithm

References

- RFC 3261. SIP: Session Initiation Protocol. J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler. June 2002
- RFC 3550. RTP: A Transport Protocol for Real-Time Applications. H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson. July 2003
- RFC 2327. SDP: Session Description Protocol. M. Handley, V. Jacobson. April 1998
- RFC 2460. IPv6: Internet Protocol, Version 6 Specification. S. Deering, R. Hinden. December 1998
- Ethereal. http://www.ethereal.com
- Windump. http://windump.polito.it/
- Winpcap. http://winpcap.polito.it/

Q & A

Thank You!