Capturing DTMF using Wireshark

Select often, when you call company helpdesk line, there is an IVR System asking to press a number on a dial pad to select a specific servicehttp://en.wikipedia.org/wiki/Interactive_voice_response. On an analogue, the use of voice codecs in VoIP affects seriously these audio signals. After encoding and decoding, the signals are often not recognized as DTMF signals anymore. The solution is to recognize DTMF at the emitting and transmit them digitally and generate them at the receiving end. Those numbers are modulated into double frequency sounds and are transmitted as audio signals according to their DTMF signal.

- Start the capture
- Filter SIP packets
- In this example, X-Lite was used to make a phone call to **Orange-Swiss Hotline** "**0800700700**"

Select **Telephony➔VoIP Calls** in the menu bar

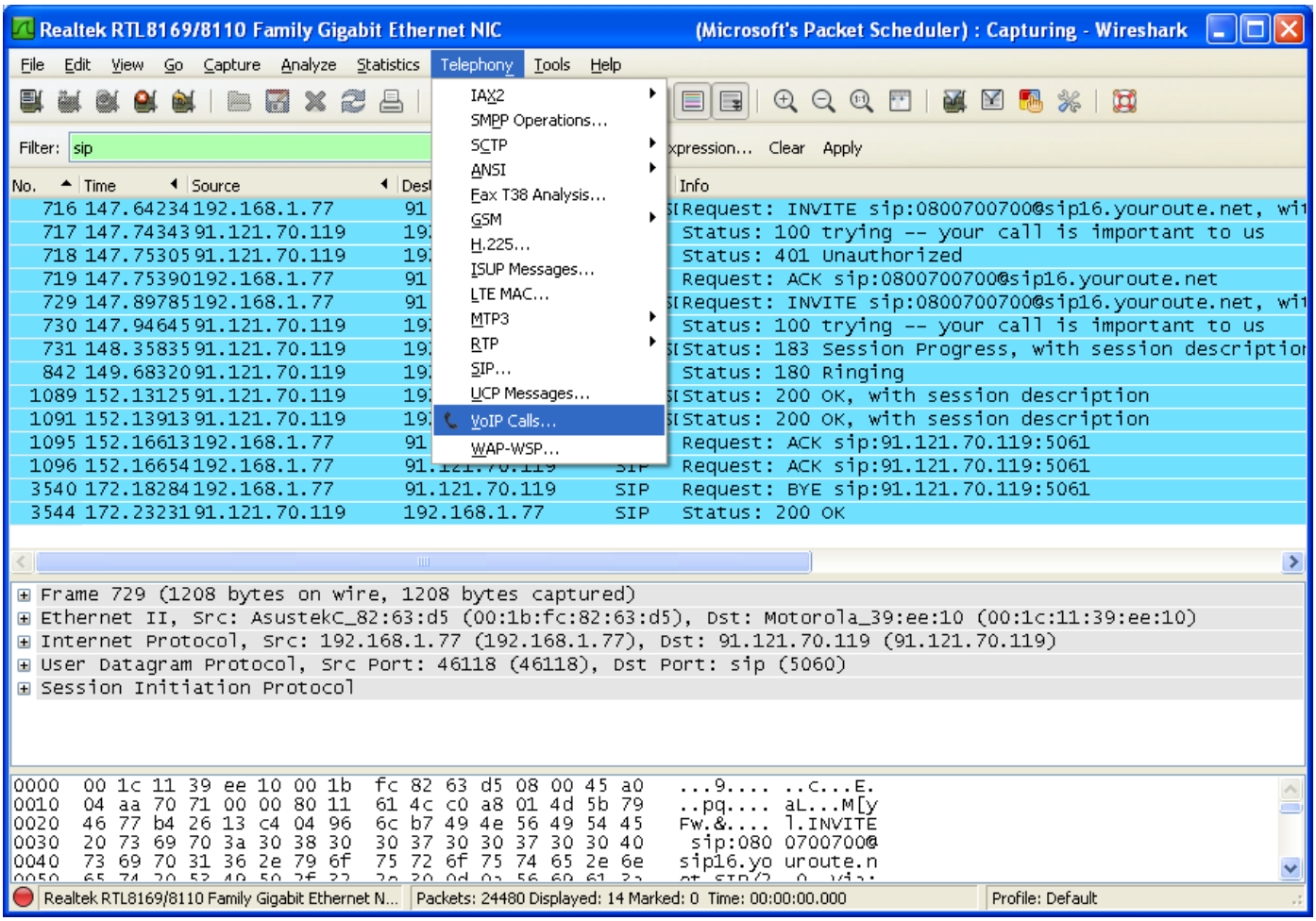

Figure 28: VoIP calls selection

Select the exact phone call to trace and click the "**Flow**" button

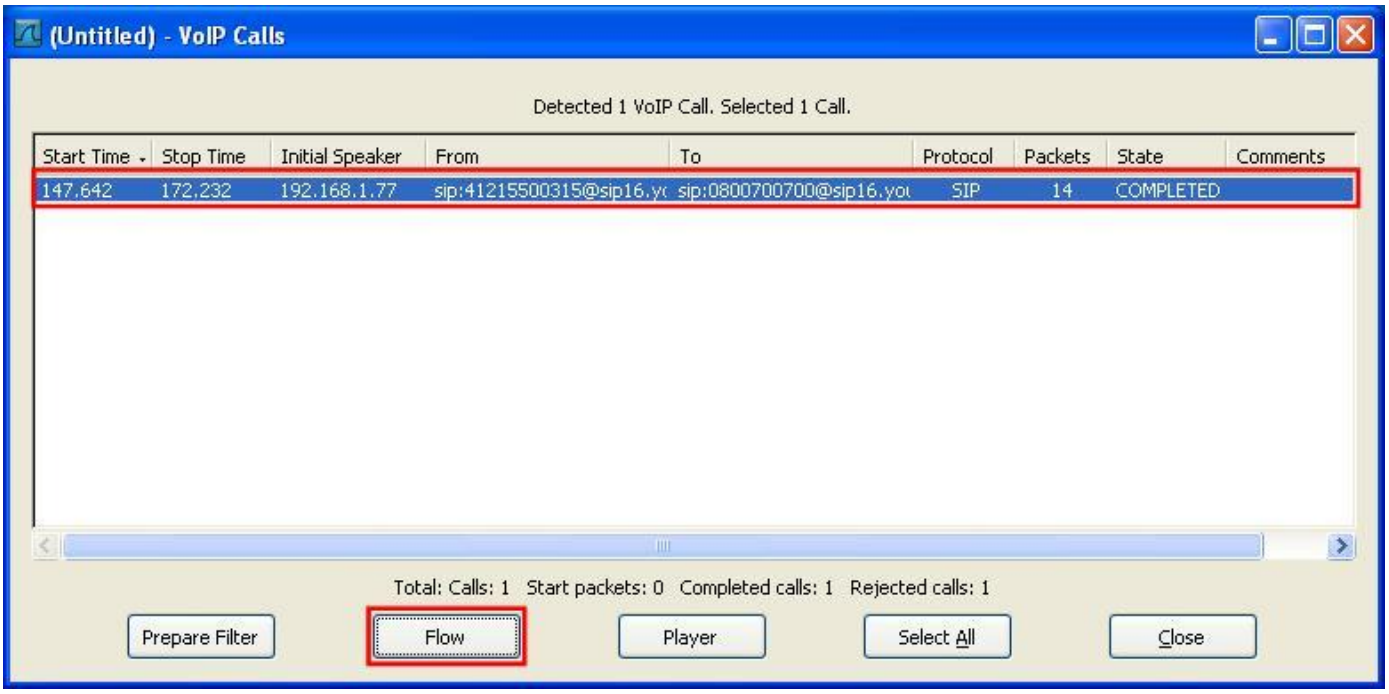

Figure 29: VoIP Calls analysis

There we go. As shown in the graphic, X-Lite transmits the DTMF signals digitally within the RTP stream. Most of UA can be configured to transmit DTMF via one or combination of the following methods: RTP, SIP, and audio.

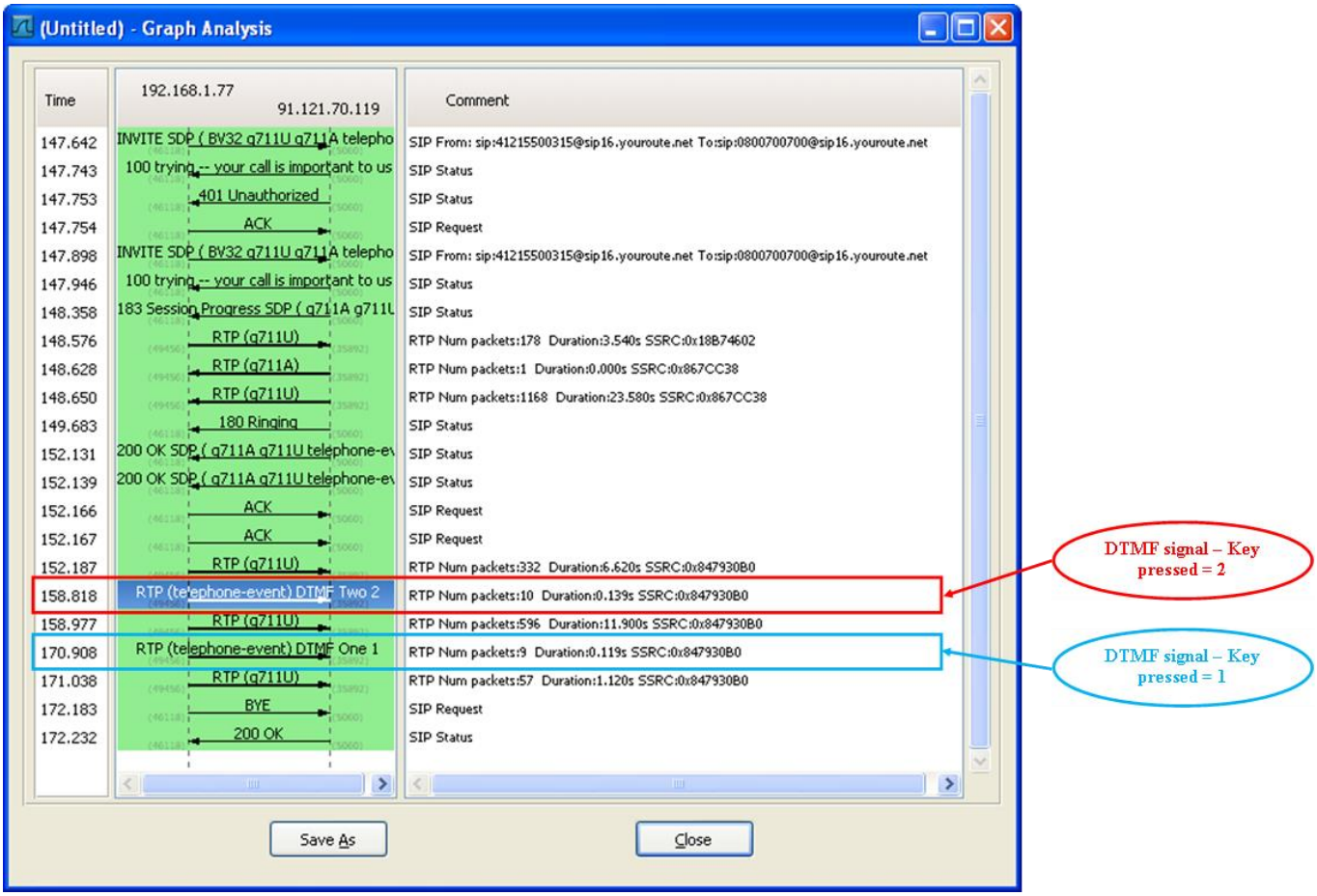

Figure 30: VoIP Graph-Analysis-DTMF signal observation

We can also filter RTP and then open its Graph Analysis. The windows should look like this

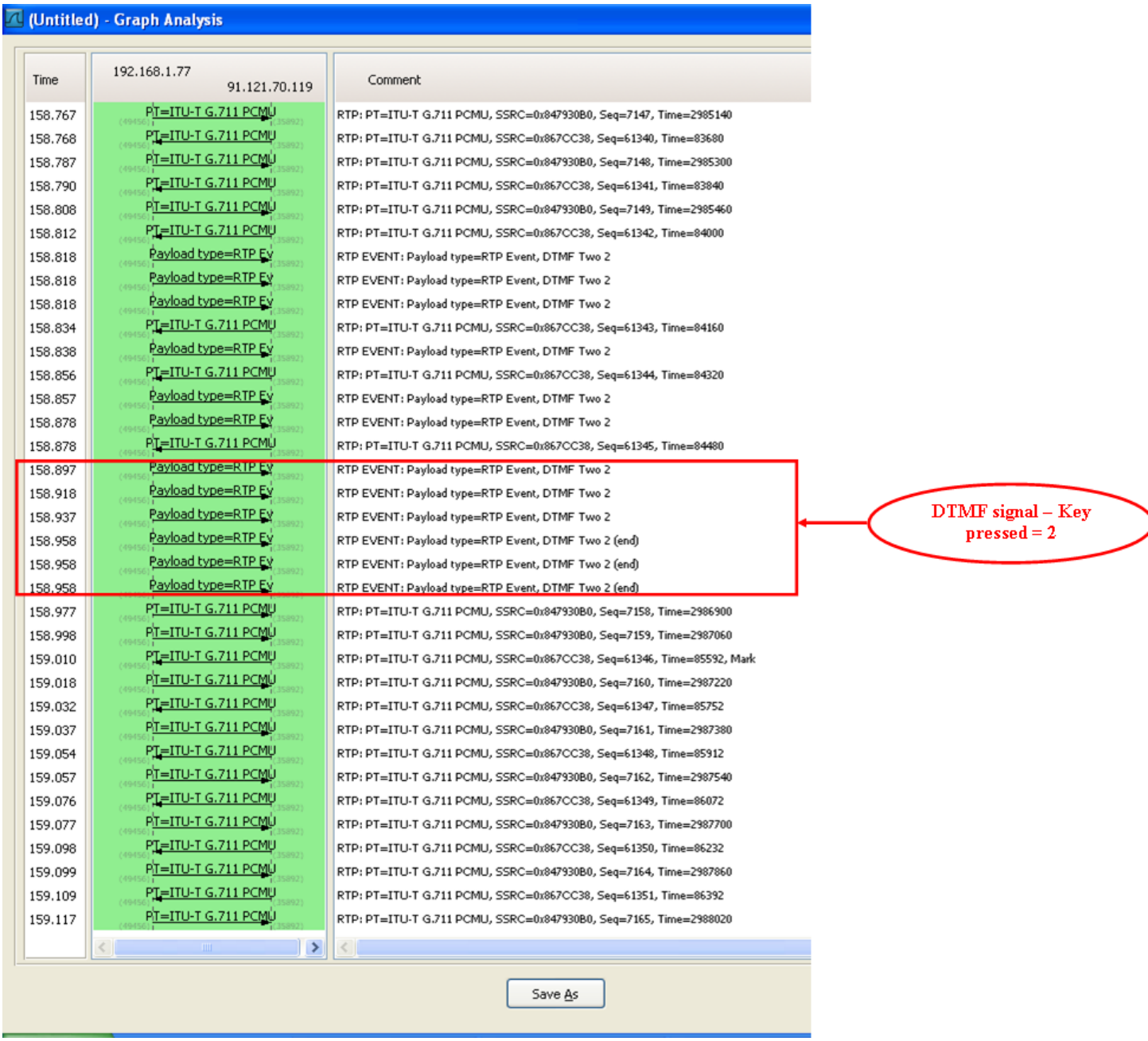

Figure 31: RTP Graph-Analysis-DTMF signal observation

Conclusion

On this document, we have shown how to install Wireshark and X-Lite, capture and understand basic SIP exchange, difference between SIP and RTP, capture and saving of voice as well as capture of DTMF signals.

Glossary

B2BUA:
Back to Back User Agent is a SIP call controlling component logically positioned between the IMS (IP Multimedia Subsystem) and external networks. It handles all SIP (Session Initiation Protocol) signalling, including session attempts, subscriptions, instant messaging, etc, as well as including signalling where the flows may be forward without B2BUA intervention.

Downstream:
The speed at which information is received from the Internet. The speed is sometimes shown as X /Y where X is the downstream speed and Y is the upstream speed.

DTMF:
Dual Tone Multiple Frequency is a signaling method developed by Bell Labs for sending telephone dialing information over the same analog, voice-quality phones lines that carry voice. Each digit is encoded as the sum of two sinewave bursts, of different frequencies. The two-tone method was chosen because it can be reliably distinguished from voice and normal phone conversations are highly unlikely to falsely trigger the DTMF receiver.DTMF was the basis for "TouchTone" (a former trademark of AT&T), the pushbutton system that replaced mechanical rotary dial telephones.

IP:
Internet Protocol defines the way data packets, also called datagrams, should be moved between the destination and the source. More technically, it can be defined as the network layer protocol in the TCP/IP communicationsprotocol suite.

Packet:
A packet is a unit of data transmitted over the network in a packet-switched system. It consists of a header that stores the destination address, a data area which carries the information that is being transmitted, and a trailer which contains information to prevent errors during transmission.

Payload:
Information contained in a packet

Protocol:
It is a convention or standard that defines the procedures to be adopted regarding the transmission of data between two computing end points. These procedures include the way the sending device should sign off a message or how the receiving device should indicate the receipt of a message. Similarly, the protocols also lay down guidelines for error checking, data compression, and other relevant operational details.

RTP:
Real-Time Transport Protocol. Real-Time Transport Protocol. One of the IPv6 protocols. RTP is designed to provide end-to-end network transport functions for applications transmitting real-time data, such as audio, video, or simulation data, over multicast or unicast network services. RTP provides services such as payload type identification, sequence numbering, time-stamping, and delivery monitoring to real-time applications.

SIP:
SIP, which is the acronym of Session Initiation Protocol, is an IP telephony signaling protocol. It is primarily used for voice over IP (VoIP) calls, though with some extensions it can also be used for instant messaging. It is less complex than H.323, the other IP telephonyprotocol.

Softphone:
This is a software application that is installed in the user's PC. It uses the Voice over IP technology to route voice calls over the net and provides several value added features, such as call forwarding, conference calling, and integration with applications such as Outlook for automatic dialing The audio is provided through a microphone and speakers plugged into the sound card. The only limitation of a Softphone is that the phone call has to made through a PC. Many softphone are free VOIP software downloads.

UAC:
User Agent Client is the cllient application that initiates the SIP request.

UAS:
User Agent Server is the server application that contacts the user when a SIP request is received, and then returns a response on behalf of the user. The response accepts, rejects, or redirects the request.

Upstream:
This refers to sending of data from a client machine across the Internet. With cable modems and ADSL, upstream speeds are slower than downstream speeds.

VoIP:
Voice over IP: VoIP or Voice over IP is the technology that is used to transmit voice over the Internet. The voice is first converted into digital data which is then organized into small packets. These packets are stamped with the destination IP address and routed over the Internet. At the receiving end the digital data is reconverted into voice and fed into the user's phone.

References

[1] http://wiki.wireshark.org/VoIP_calls: Play RTP sounds with Wireshark

[2] http://www.markwilson.co.uk/blog/2008/11/recording-voip-calls-using-wireshark.htm : Recording voice sound using wireshark

[3] http://www.voip-info.org/wiki/view/DTMF : DTMF usage in VoIP and VoIP tutorials