



# Capturing VOIP

# Capturing VOIP

## » What is VOIP?

## » Common issues with VOIP

- Dropped calls
- Incomplete calls
- Jitter or poor quality
- Network QoS

# Capturing VOIP

No.	Time	Source	Destination	Protocol	Expert	Length	Info
20	32.141694	212.242.33.35	192.168.1.2	SIP		528	Status: 401 Unauthorized (0 bindings)
30	49.420564	192.168.1.2	212.242.33.35	SIP		722	Request: REGISTER sip:sip.cybercity.dk
31	49.566655	212.242.33.35	192.168.1.2	SIP		348	Status: 100 Trying (0 bindings)
32	49.616489	212.242.33.35	192.168.1.2	SIP		388	Status: 403 Wrong password (0 bindings)
107	139.349155	192.168.1.2	212.242.33.35	SIP		509	Request: REGISTER sip:sip.cybercity.dk
108	139.491380	212.242.33.35	192.168.1.2	SIP		528	Status: 401 Unauthorized (0 bindings)
121	156.629834	192.168.1.2	212.242.33.35	SIP		722	Request: REGISTER sip:sip.cybercity.dk
122	156.781808	212.242.33.35	192.168.1.2	SIP		533	Status: 401 nonce has changed (0 bindings)
143	306.829874	192.168.1.2	212.242.33.35	SIP		509	Request: REGISTER sip:sip.cybercity.dk
144	306.970027	212.242.33.35	192.168.1.2	SIP		528	Status: 401 Unauthorized (0 bindings)
154	324.155054	192.168.1.2	212.242.33.35	SIP		722	Request: REGISTER sip:sip.cybercity.dk
155	324.305849	212.242.33.35	192.168.1.2	SIP		533	Status: 401 nonce has changed (0 bindings)
169	398.071097	192.168.1.2	212.242.33.35	SIP		509	Request: REGISTER sip:sip.cybercity.dk
170	398.208501	212.242.33.35	192.168.1.2	SIP		528	Status: 401 Unauthorized (0 bindings)
180	415.396135	192.168.1.2	212.242.33.35	SIP		722	Request: REGISTER sip:sip.cybercity.dk
181	415.541671	212.242.33.35	192.168.1.2	SIP		348	Status: 100 Trying (0 bindings)
182	415.567606	212.242.33.35	192.168.1.2	SIP		512	Status: 200 OK (1 bindings)
222	508.240681	192.168.1.2	200.68.120.81	SIP/SIP		864	Request: INVITE sip:07220287044@voip.brussels.net

Filter: sip Expression... Clear Apply Save TCP Full

Frame 154: 722 bytes on wire (5776 bits), 722 bytes captured (5776 bits)

- Ethernet II, Src: Silicom\_01:6e:bd (00:e0:ed:01:6e:bd), Dst: Castlene\_00:34:56 (00:30:54:00:34:56)
- Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 212.242.33.35 (212.242.33.35)
- User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
- Session Initiation Protocol (REGISTER)
  - Request-Line: REGISTER sip:sip.cybercity.dk SIP/2.0
  - Message Header
    - Via: SIP/2.0/UDP 192.168.1.2;branch=z9hG4bkn122028667-481b9fc8192.168.1.2;rport
    - From: <sip:voi18062@sip.cybercity.dk>;tag=7460288
    - To: <sip:voi18062@sip.cybercity.dk>
    - Call-ID: 578222729-4665d775@578222732-4665d772
    - Contact: <sip:voi18062@192.168.1.2:5060;line=aca6b97ca3f5e51a>;expires=1200;q=0.500
    - Expires: 1200
    - CSeq: 73 REGISTER

# Capturing VOIP

## » Wireshark tools

- Capture windows
- Flow Graph
- Telephony menu
- Analyze menu

## » What is SIP?

- SIP, or Session Initiation Protocol, is a signaling protocol that allows VOIP calls to be initiated

# Capturing VOIP

aaa.pcap - VoIP Calls

Detected 4 VoIP Calls. Selected 0 Calls.

Start Time	Stop Time	Initial Speaker	From	To	Protocol	Packets	State	Comments
508.349681	575.439777	192.168.1.2	"arik" <sip:816666@voip.b	<sip:97239287044@voip.b	SIP	18	CANCELLED	
692.955151	727.341644	192.168.1.2	"arik" <sip:voi18062@sip.c	<sip:0097239287044@sip.c	SIP	8	REJECTED	
1307.689521	1359.221244	192.168.1.2	"arik" <sip:35104723@sip.	<sip:0097239287044@sip.c	SIP	7	REJECTED	
1425.604602	1443.513774	192.168.1.2	"arik" <sip:35104723@sip.	<sip:35104724@sip.cyberc	SIP	8	REJECTED	

Total: Calls: 4 Start packets: 0 Completed calls: 0 Rejected calls: 6

Prepare Filter Flow Player Select All Close

# Questions?