Reconnaissance & Tool Fingerprints

`sip.User-Agent contains "friendly-scanner"`	SIPVicious svmap / svwar default UA
`sip.User-Agent contains "voiphopper"`	VoIP Hopper VLAN-discovery tool
`sip.User-Agent contains "sundayddr"`	SIPVicious fork variant
`sip.User-Agent contains "sipsak"`	SIP-toolkit probes
`sip.Method == "OPTIONS"`	SIP probe sweeps (svmap pattern)
`sip.Method == "REGISTER" and sip.Status-Code == 401`	Auth challenge during enumeration
`cdp`	CDP advertisements (voice-VLAN leak)
`lldp`	LLDP advertisements (same risk class)

SIP Signaling Analysis

`sip`	All SIP traffic
`sip.Method == "INVITE"`	Call-setup messages
`sip.Method == "REGISTER"`	Endpoint registrations
`sip.Method == "CANCEL"`	Cancellations (wangiri check)
`sip.Identity`	STIR/SHAKEN PASSporT-bearing
`sip.Authorization contains "Digest"`	Digest auth (cleartext = crackable)
`sip.Authorization contains "Bearer"`	OAuth bearer token (RFC 8898)
`sip.Via`	Via stack (topology-leak check)

Media-Plane Analysis

`rtp`	All RTP audio (eavesdrop target)
`rtp.p_type == 0`	G.711 PCMU (most common codec)
`rtp.p_type == 101`	RFC 4733 telephone-event (DTMF)
`rtcp`	Plain RTCP (CNAME / SR disclosure)
`srtcp`	SRTCP (encrypted control plane)
`sdp.media_attr contains "crypto"`	SDES inline-key disclosure
`sdp.candidate`	ICE candidates (topology leak)
`sdp.fingerprint`	DTLS-SRTP fingerprint binding

Encryption Layer

`tls.handshake`	All TLS handshake records
`tls.handshake.type == 1`	ClientHello (version + SNI + ALPN)
`tls.handshake.type == 2`	ServerHello (chosen cipher)
`tls.handshake.type == 11`	Certificate (2/session = mTLS)
`tls.handshake.type == 20`	Finished (handshake success)
`tls.alert_message`	TLS error (handshake failure)
`dtls`	DTLS records (DTLS-SRTP key exchange)

Network & L2 Attacks

`arp.duplicate-address-detected`	Gratuitous-ARP MITM attempt
`vlan.id != 0`	802.1Q-tagged (VLAN-hop check)
`vlan.id == 200`	Specific voice-VLAN traffic

Management-Plane Attacks

`tcp.port == 5038`	Asterisk AMI (cleartext creds)
`snmp`	All SNMP traffic
`snmp and snmp.version != 3`	SNMPv1/v2c (cleartext community)
`tftp`	TFTP provisioning (cleartext config)
`http and tcp.port == 8088`	FreePBX admin web UI

Combined / Policy-Violation

`sip and ip.proto == 17`	Cleartext SIP/UDP (TLS-policy violation)
`sdp.media_attr contains "inline" and ip.proto == 17`	SDES key over cleartext transport
`sip.Authorization contains "Bearer" and ip.proto == 17`	OAuth token over cleartext transport

Statistical Detection Recipes

svwar extension enumeration	Statistics → Conversations → SIP; sort by Packets desc. Sequential To-URI from one source = enumeration.
svmap OPTIONS sweep	Statistics → Conversations → IPv4; filter `sip.Method == "OPTIONS"`. One source → many dests = scan.
Plaintext RTP vs SRTP	Statistics → Packet Lengths with `rtp`. Bimodal 200/214 B = RTP+SRTP coexisting; single 200 B peak = pure RTP.
Wangiri inbound-cancel	Filter `sip.Method == "CANCEL"`; right-click → Conversation Filter → SIP. INVITE→CANCEL delta < 2 s = wangiri.
ARP-spoof MITM	Statistics → Endpoints → IPv4. Any IP with > 1 MAC = duplicate-address disclosure.
SIP-DDoS botnet origin	Statistics → Endpoints → IPv4, enable GeoIP. Thousands of source IPs across 60+ countries = botnet.
AMI cleartext exposure	Filter `tcp.port == 5038`; right-click → Follow → TCP Stream. Banner + Action: Login visible in cleartext.
SNMP v2c brute-force	Filter `snmp and snmp.version != 3`; IO Graph grouped by `snmp.community` shows community rotation.
Identity-bearing call analysis	Filter `sip.Identity`; click any match → copy header → base64url-decode segments 1+2 for claims.

General Workflow Shortcuts

Reconstruct audio	Telephony → RTP → RTP Streams → select stream(s) → Play Streams
Extract DTMF digits	Telephony → RTP → Stream Analysis → DTMF tab
List all VoIP calls	Telephony → VoIP Calls → select → Flow Sequence / Player
Follow conversation	Right-click packet → Conversation Filter → SIP / TCP / UDP
Reassemble TFTP file	Right-click TFTP packet → Follow → UDP Stream
Decode UDP as RTP	Right-click packet → Decode As → RTP
Decode UDP as SRTP	Right-click → Decode As → SRTP (keys req. for full decrypt)
Export call as own pcap	File → Export Specified Packets → Selected / Filtered
Map source IPs to countries	Statistics → Endpoints → IPv4 → enable GeoIP plugin
Delta-time column	Preferences → Columns → +Custom: `frame.time_delta_displayed`

RFC 4733 Telephone-Event Payload

```
Byte 0: event code
  0–9   = DTMF digits 0–9
  10    = '*'
  11    = '#'
  12–15 = A–D
Byte 1: bit 7    = End-of-event flag
        bits 5–0 = volume in -dBm0
Bytes 2–3: duration in 8 kHz samples
  160 = 20 ms
  480 = 60 ms
  800 = 100 ms
```

TLS / DTLS Handshake Types

1	**ClientHello** — SNI, ALPN, supported_versions, key_share
2	**ServerHello** — chosen cipher in extensions
3	**HelloVerifyRequest** — DTLS-only (cookie exchange)
11	**Certificate** — two per session = mTLS
12	**ServerKeyExchange** — ECDHE params (TLS 1.2)
13	**CertificateRequest** — server asks for client cert
14	**ServerHelloDone** — end of server's initial msgs
15	**CertificateVerify** — client proves cert key
16	**ClientKeyExchange** — TLS 1.2 only
20	**Finished** — first encrypted handshake msg

Attack-Tool User-Agent Fingerprints

`friendly-scanner`	SIPVicious svmap / svwar — OPTIONS sweep recon, extension enum
`sipvicious-pro`	SIPVicious PRO commercial fork (varies)
`sundayddr`	SIPVicious fork variant
`sipsak`	SIP toolkit probes
`voiphopper/X.Y`	VoIP Hopper VLAN-hopping recon probe
`Mr.SIP`	Pentest framework (varies)

IRSF / Wangiri Country Codes

`+232`	Sierra Leone — highest-volume IRSF
`+252`	Somalia — recurring
`+371`	Latvia — Baltic cluster
`+53`	Cuba — recurring
`+960`	Maldives — Indian Ocean
`+677`	Solomon Islands — Pacific
`+509`	Haiti — Caribbean
`+882, +883`	Non-geographic int'l short-codes
`+268`	Eswatini — lower-frequency
`+500`	Falkland Islands — lower-frequency

Default SNMP Community Strings

`public`	Read — default on nearly all v1/v2c devices
`private`	Read-Write — classic write community
`cisco`	Read — Cisco-vendor default
`admin`	Read — lazy admin default
`voip`	Read — domain-specific guess
`manager`	Read — HP/management default