



A note from the student behind this lab

This is an **independent, free, learning-only student project**. It respects every company and vendor, and every trademark belongs to its owner. It is **not affiliated with or endorsed by** any of them.

If anyone has a concern, the content will be removed or corrected promptly: please write via <https://cyphermonkeylabs.com/#contact>. Nothing here is sold, and I am happy to volunteer for any organization.

Wireshark and sngrep

Filter the capture with sip, rtp, and sip.Method, and confirm sip.CSeq.method in the SIP display-filter reference.

Filters this lesson will name

The display filters you may type from this lesson are sip, rtp, and sip.Method. A common way to see INVITE requests is sip.CSeq.method == "INVITE". Confirm that field in the Wireshark SIP display-filter reference before you trust it in a ticket. The reference for SIP fields is the page this lesson cites as ws-sip. RTP display fields have their own page, ws-rtp.

sip.Method is the safe method field when you want the request method. This lesson does not invent other field names. If a blog names a filter you have not found on those two reference pages, leave it out of the write-up until you confirm it there.

What you read after the filter hits

Select one packet and read the SIP headers in order: Call-ID, CSeq, Via branch, To tag. The filter got you to the packet. The match rules from the ladder lesson decide whether the next packet is the same transaction.

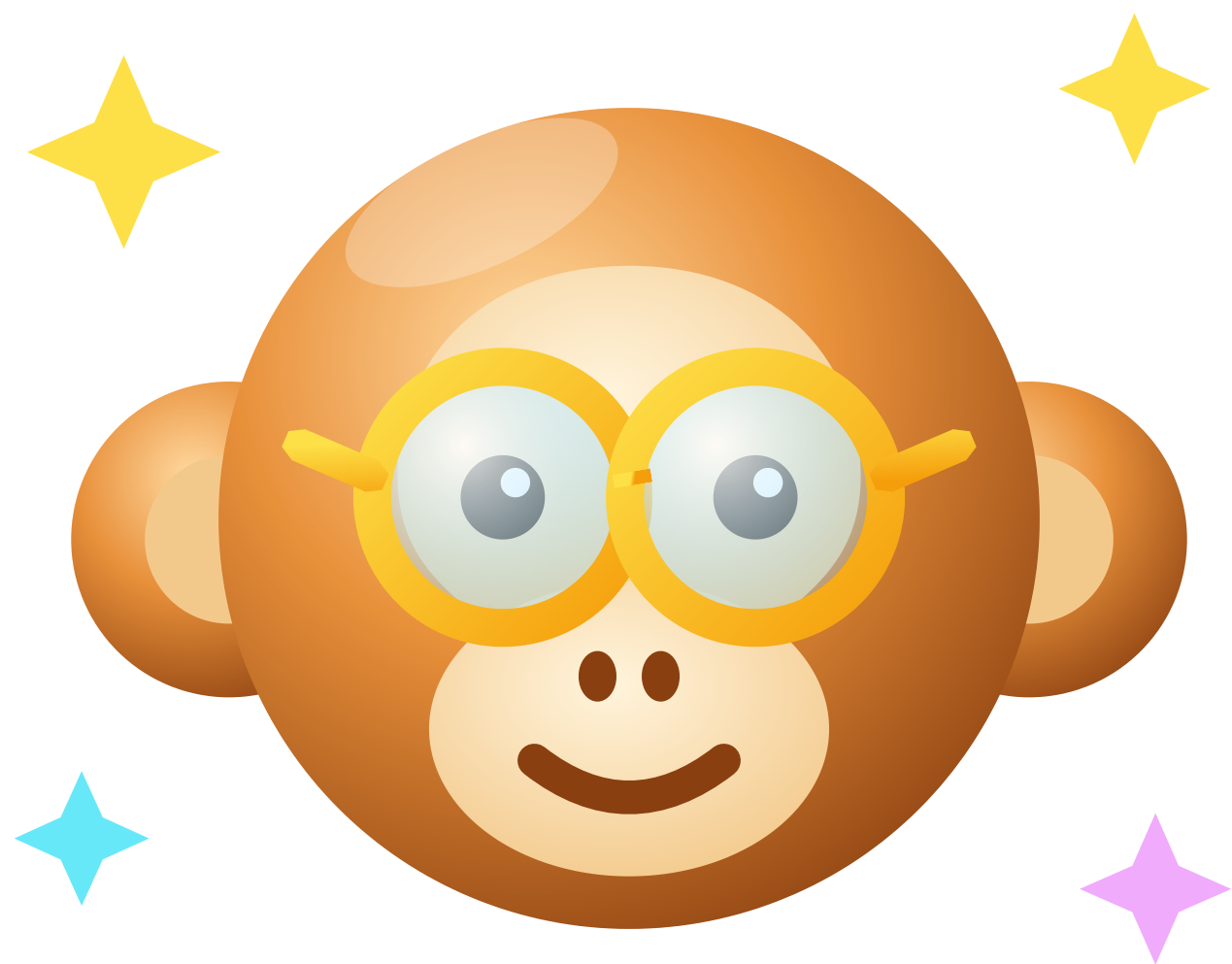
rtp shows the media packets. SIP showing a 200 OK with an m= line does not mean those RTP packets are in the capture. When the call is silent, keep the SIP filter long enough to read the negotiated address and port, then use the rtp display filter to see whether media arrived. Cite the RTP reference for RTP fields and the SIP reference for SIP fields.

Room: [Display filters for SIP and RTP](#)

Sources and go deeper

- [Wireshark SIP display filter reference](#) — last checked 2026-10
- [Wireshark RTP display filter reference](#) — last checked 2026-10
- [RFC 3550](#) — last checked 2026-10
- [RFC 3264](#) — last checked 2026-10
- [RFC 3261 §8](#) — last checked 2026-10
- [RFC 6026](#) — last checked 2026-10

CypherMonkey Labs







© 2026 CypherMonkeyLabs 🐒

[Open app](#) · [View repo](#)