How to decode SIP over TLS with Wireshark

For security reasons, some customers may choose to use TLS for the SIP transport. TLS encrypts the SIP signaling messages, but a packet capture will not reveal their content. To troubleshoot this, the signaling messages must be decrypted.

Step-by-step guide

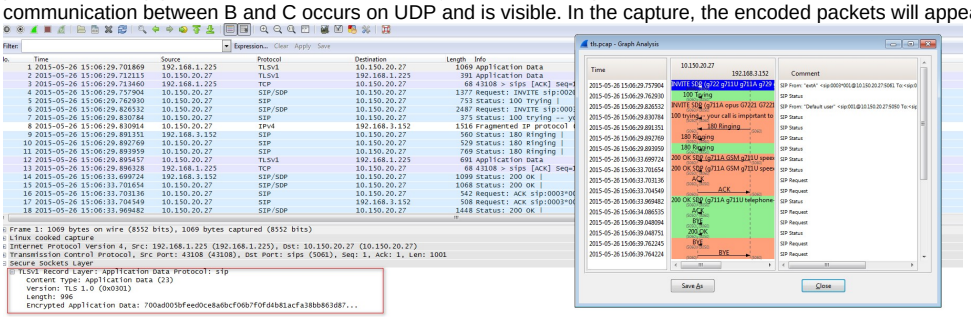
Take the capture

The first step is to capture the call. The call can have legs over TLS, UDP or TCP. Also, the ports can be 5060 or 5061 for Kamailio or 5050 for Asterisk.

1. To capture all of them, run the following command:

```
tcpdump -nni any -s 0 port 5050 or port 5060 or port 5061 -w /usr/local/voipnow/admin/htdocs/tls.pcap
```

2. When you open the capture, you'll see that the TLS part of the call is not even recognized by Wireshark as SIP.
In the capture below, we had a call from phone terminal (A) 192.168.1.225 through the VoipNow server (B) at 10.150.20.27 and towards another phone terminal (C) on UDP at 192.168.3.152. As you can see, the part between A and B is missing because it's using TLS, whereas the communication between B and C occurs on UDP and is visible. In the capture, the encoded packets will appear as TLS.



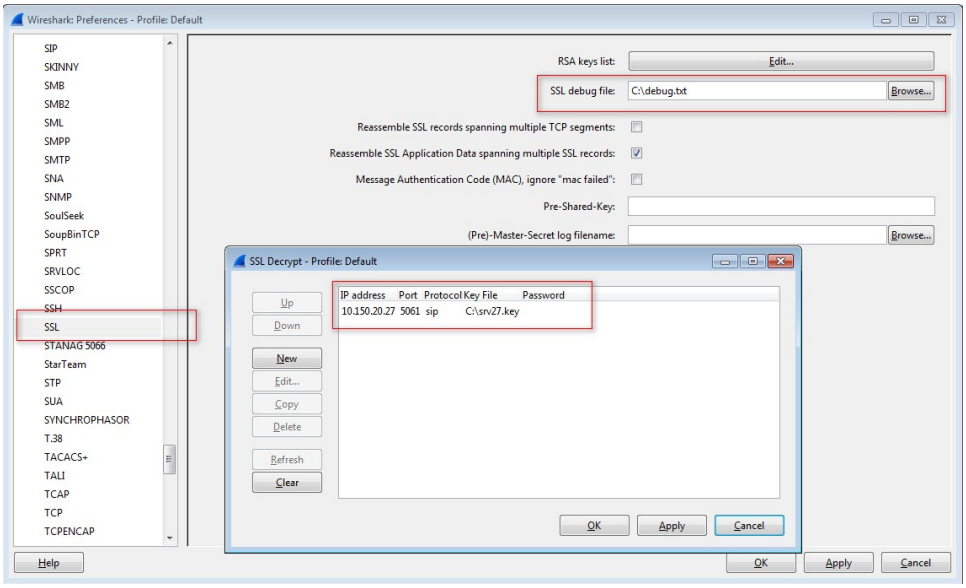
3. Beside the filters, when you're capturing TLS, you need to make sure you capture the SSL handshake between the phone terminal and the VoipNow server. Otherwise, you won't be able to decrypt the capture.

Decode TLS

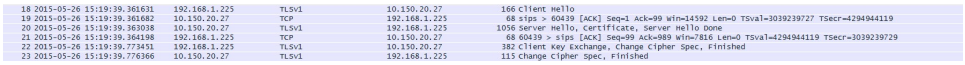
1. First you need the private key used by Kamailio. On VoipNow 3.5, you can find it in /etc/voipnow/certs/kamailio.pem.
2. Take the private key and save it on your PC in a filename.key file. It should look like this:

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkahkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDLsm335w5i+BiY
gg05NsBTR1ZTSbsMjkoprJoQ8KPxFvLGegwyWY+Fk25GmFCur7GfZYuYACXcU0H/
...
l7DtP+PYdC2Yz6lld8FO6LB6RgsZHnXlDj8yxhzeALDBRvZSt+of4iedEK1J+0pA
zuqB/sOrM+e1J8z3vsF9kikZ
-----END PRIVATE KEY----
```

3. Open Wireshark and go to **Edit >> Preferences >> Protocols >> SSL >>Edit** and do the exact setup you can see below. Use the file created earlier with the private key.

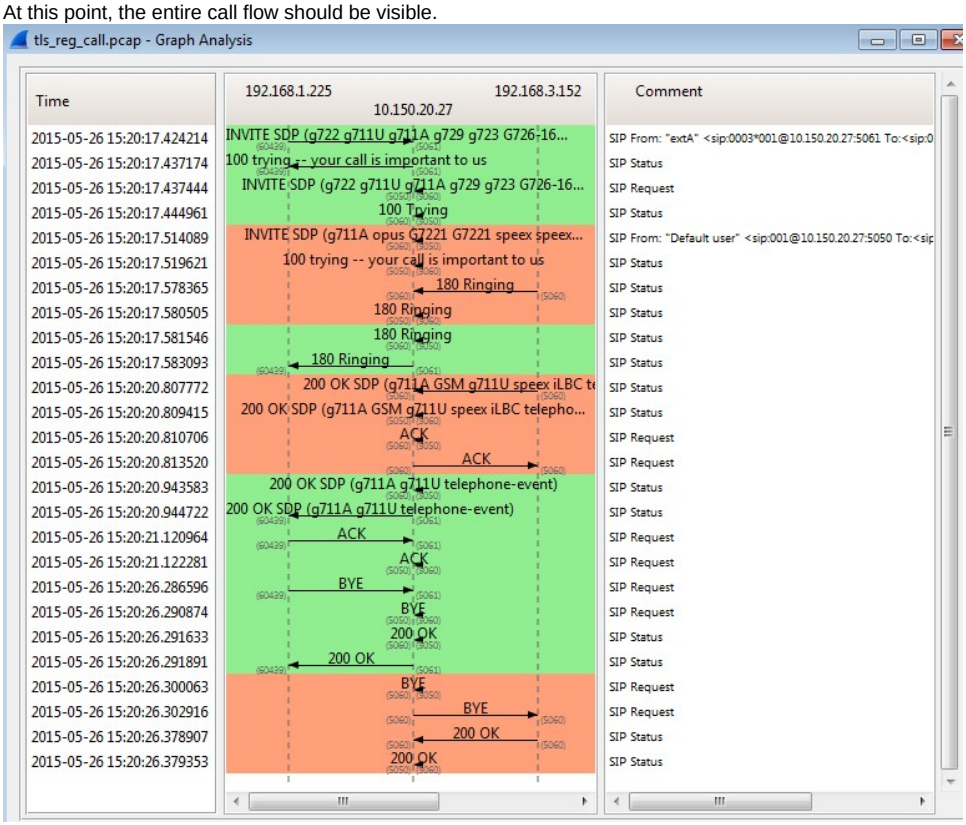


Now, Wireshark cannot decode the capture without the SSL handshake between the phone and the server included in the capture. The handshake looks like this:



This SSL handshake occurs during each phone reboot and following each TCP handshake.

At this point, the entire call flow should be visible.



Related articles

- How to create a configuration template for a certain SIP device
- How to set up a SIP channel to interconnect with Skype forBusiness account
- Understanding SIP devices provisioning permissions
- How to set up Snom 300/320/360 SIP phones to connect to VoipNow
- How to set up Cisco/Linksys SPA phones to connect to VoipNow