Info:

One of our DFIR-Guys is analyzing an infected host but is kinda stuck. We know this host is communicating with

some form of C2 but we do not know how it works. We need to crack this to get to the encryption key. Can you help us?

Task:

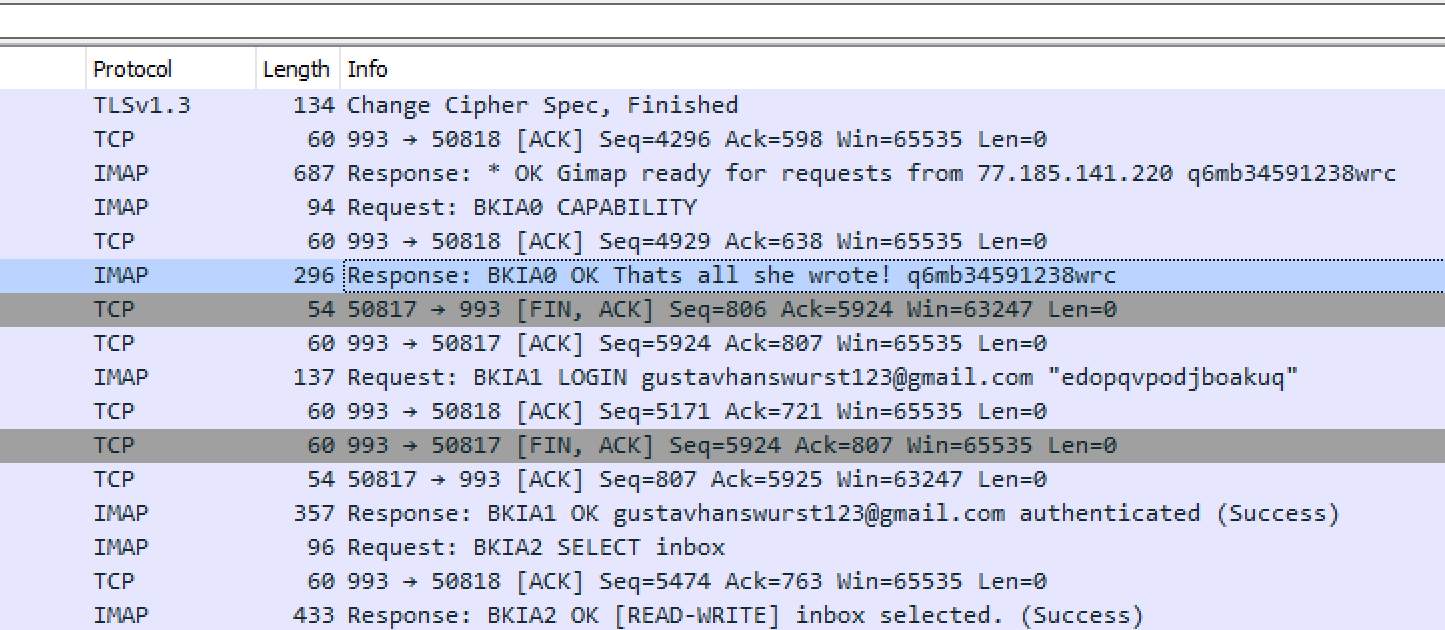
Find the Key (Flag)

1. Provided are 2 files. Forensic1.pcapng and ssl-keys.log. Both can be analyzed with Wireshark. PCAPNG is the captured traffic and ssl-keys.log can be used to decrypt encrypted traffic.
2. Open up Wireshark and load the pcap-file.
3. Edit > Preferences > Protocols > TLS > (Pre)-Master-Secret log filename > Select the ssl-keys.log

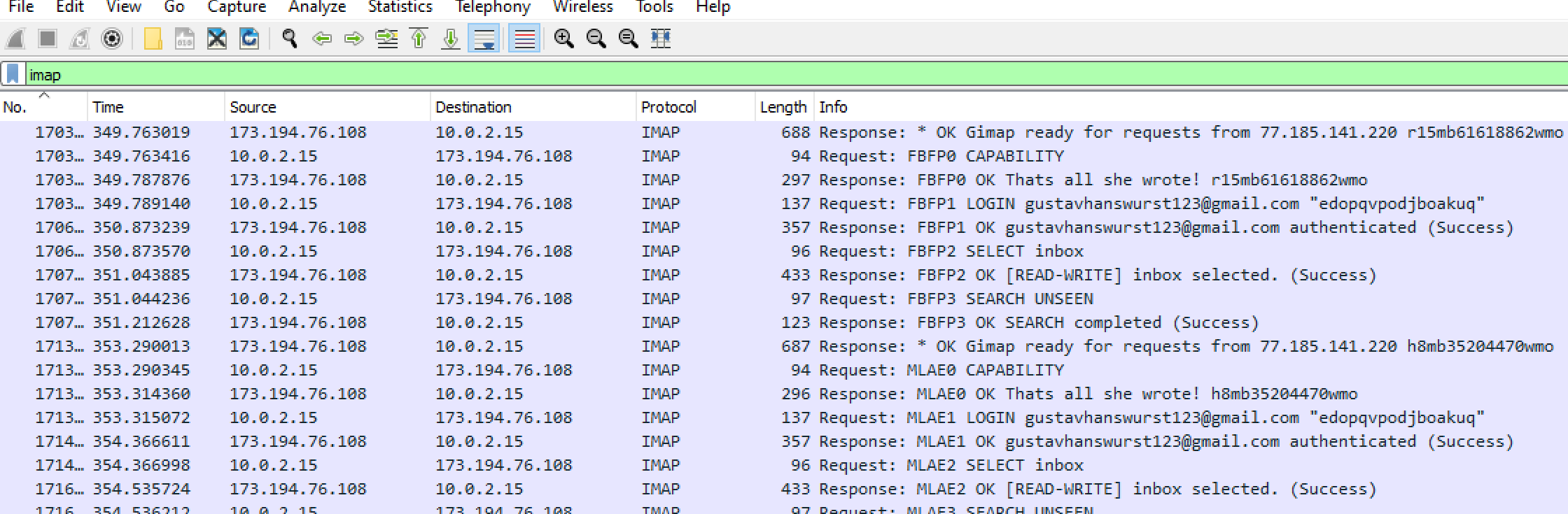
A screenshot of a computer

Description automatically generated

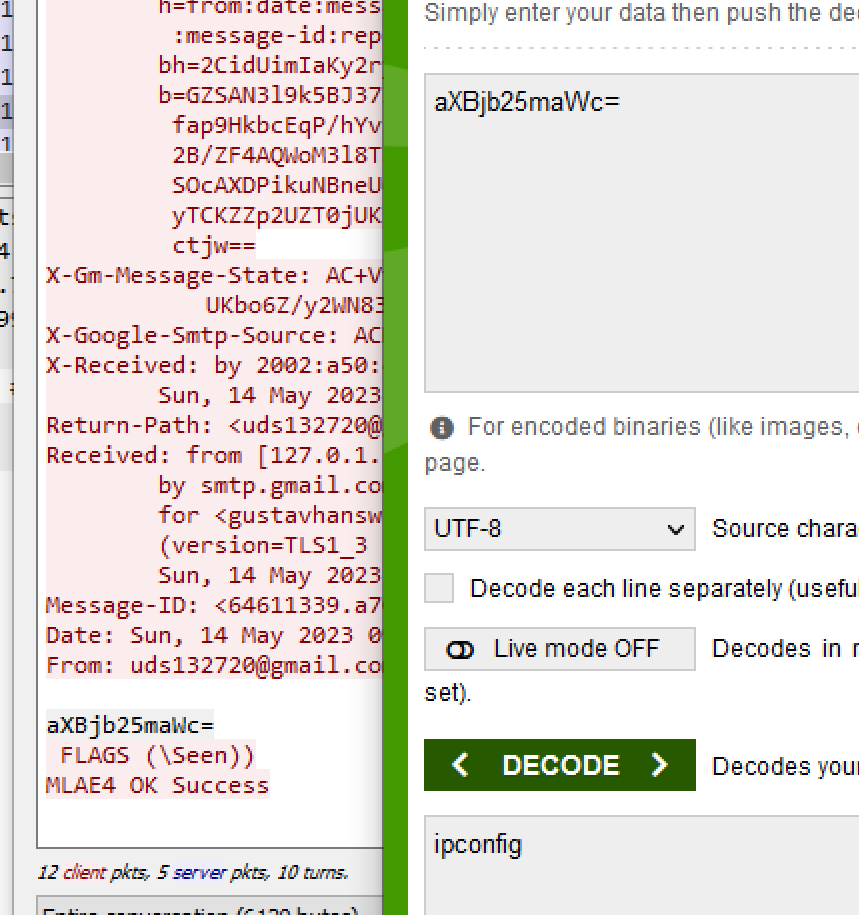
1. Go through the traffic and check if you find anything suspicious. There are several ways to filter out the traffic. In this case we find a lot of irrelevant data belonging to twitch.tv and usual browsing. Going through the traffic you will also find IMAP-Traffic with seemingly encrypted content.



1. Filtering out IMAP-Traffic will leave you with a lot of encrypted content



1. At first some of the message seem to include base64-encoded data, in this case the command ipconfig. It seems the C2 is communicating over Email.



1. Going through the IMAP-Traffic we can not find anything looking like a flag so we need to check if the client send anything via mail to the C2 and inspect SMTP.
2. Filtering out SMTP will give you several base64-encoded data. One of them is the flag

DS-CTF{d4mnwh0w0u1dh4v37h0u9h7h3yu53dm411}

