**21. Use any open-source software to capture the data of the application. For reference, from a pcap file, use any opensource software to extract each email (POP, IMAP, and SMTP protocols), all HTTP contents, each VoIP call.**

**----------------------------------------- ---------------------------------------------**

Here are the steps to capture information utilizing Wireshark:

Download and introduce Wireshark from the official site: https://www.wireshark.org/download.html.

Dispatch Wireshark and select the arrange interface merely want to capture information on. This might be a wired or remote association.

Begin capturing data by clicking the "Start" button within the fundamental window.

Utilize the application merely need to capture information from. Wireshark will capture all the data packets that are sent and received by the application.

Once you've got captured enough data, halt the capture by clicking the "Stop" button within the primary window.

You'll be able presently analyze the captured information by selecting a parcel and seeing its subtle elements within the lower sheet of the Wireshark window. You'll moreover utilize the different channels and insights devices given by Wireshark to analyze the information in more detail.

Note that capturing information from an application may require a few specialized information and may moreover be subject to legitimate limitations. Be beyond any doubt to get any fundamental authorizations and take after all significant laws and directions some time recently endeavoring to capture information.

Download and install NetworkMiner from the official website: https://www.netresec.com/?page=NetworkMiner.

Launch Network Miner and open the PCAP file containing the email traffic.

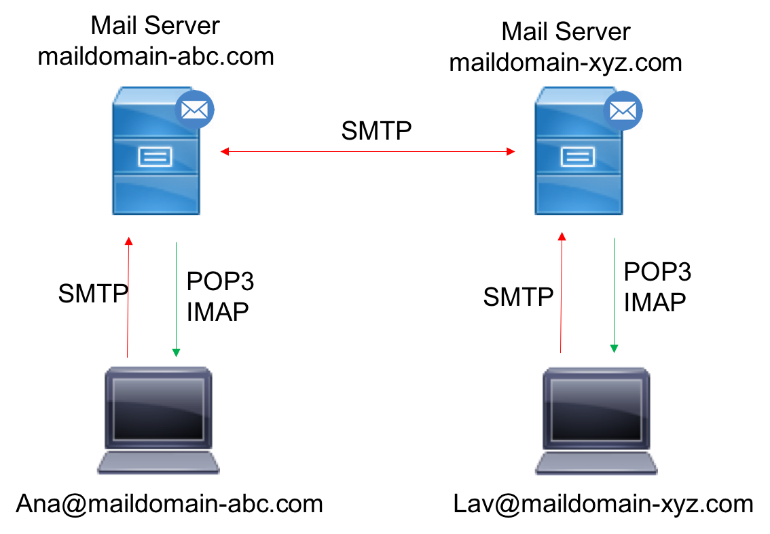
In the "Files" tab, select the "SMTP", "POP3", and "IMAP" checkboxes to filter the captured traffic for these protocols.

Network Miner will automatically extract any emails it finds in the captured traffic and display them in the "Emails" tab.

Click on an email to view its details, including the sender, recipient, subject, and message body.

You can also export the extracted emails to a file by clicking on the "Export" button in the "Emails" tab.

Note that extracting emails from a PCAP file may require some technical knowledge and may also be subject to legal restrictions. Be sure to obtain any necessary permissions and follow all relevant laws and regulations before attempting to extract emails from a PCAP file.



One of the contributing components within the advancement of computerized promoting and commerce is e-mail. E-mail permits clients to trade real-time messages and other advanced data such as records and pictures over the web in an proficient way. Each client is required to have a human-readable e-mail address within the shape of username@domainname.com. There are different e-mail suppliers accessible on the web, and any client can enlist to induce a free mail address.

There are distinctive mail application-layer conventions accessible for sending and getting sends, and the combination of these conventions makes a difference with end-to-end mail exchange between users within the same or diverse mail spaces. In this article, we are going see at the typical operation of e-mail conventions and how to utilize Wireshark for essential investigation and investigating.

This article is an portion from Arrange Investigation utilizing Wireshark 2 Cookbook – Moment Version composed by Nagendra Kumar Nainar, Yogesh Ramdoss, Yoram Orzach.

The three most commonly utilized application layer conventions are POP3, IMAP, and SMTP:

• POP3: Post Office Convention 3 (POP3) is an application layer convention utilized by mail frameworks to recover mail from e-mail servers. The mail client employments POP3 commands such as LOGIN, LIST, RETR, DELE, Stopped to get to and control (recover or erase) the mail from the server. POP3 employments TCP harbour 110 and wipes the mail from the server once it is downloaded to the nearby client.

• IMAP: Web Mail Get to Convention (IMAP) is another application layer convention utilized to recover mail from the mail server. Not at all like POP3, IMAP permits the client to studied and get to the mail concurrently from more than one client gadget. With current patterns, it is exceptionally common to see clients with more than one gadget to get to emails (portable workstation, smartphone, and so on), and the utilize of IMAP permits the client to get to mail any time, from any gadget. The current version of IMAP is 4 and it employments TCP harbour 143.

• SMTP: Basic Mail Exchange Convention (SMTP) is an application layer convention that's utilized to send email from the client to the mail server. When the sender and recipient are in numerous mail spaces, SMTP makes a difference to trade the mail between servers in several spaces. It employments TCP harbor 25:

As shown in the preceding diagram, SMTP is the email client used to send the mail to the mail server, and POP3 or IMAP is used to retrieve the email from the server. The email server uses SMTP to exchange the mail between different domains.

In order to maintain the privacy of end users, most email servers use different encryption mechanisms at the transport layer. The transport layer port number will differ from the traditional email protocols if they are used over secured transport layer (TLS). For example, POP3 over TLS uses TCP port 995, IMAP4 over TLS uses TCP port 993, and SMTP over TLS uses port 465.

**Normal operation of mail protocols**

As we saw above, the common mail protocols for mail client to server and server to server communication are POP3, SMTP, and IMAP4.

Another common method for accessing emails is web access to mail, where you have common mail servers such as Gmail, Yahoo!, and Hotmail. Examples include **Outlook Web Access** (**OWA**) and RPC over HTTPS for the Outlook web client from Microsoft.

In this recipe, we will talk about the most common client-server and server-server protocols, POP3 and SMTP, and the normal operation of each protocol.

Getting ready

Port mirroring to capture the packets can be done either on the email client side or on the server side.

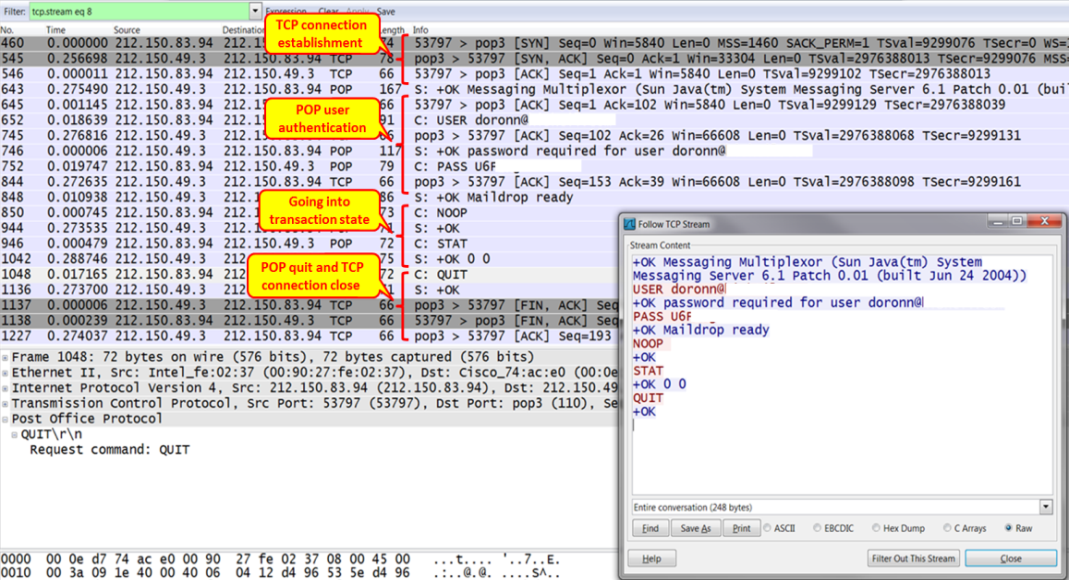
How to do it…

POP3 is usually used for client to server communications, while SMTP is usually used for server to server communications.

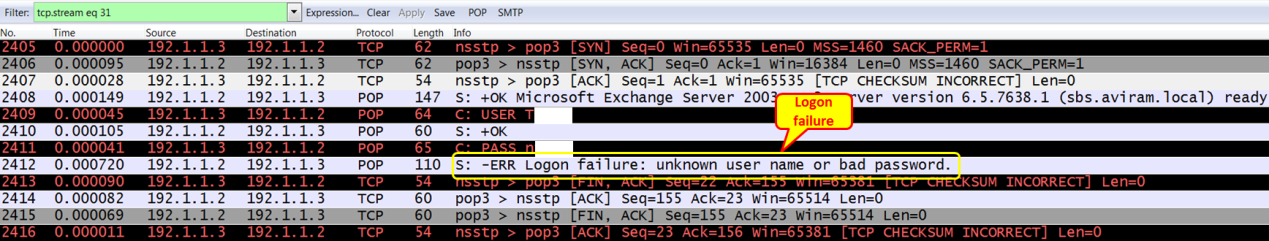
**POP3 communications**

POP3 is usually used for mail client to mail server communications. The normal operation of POP3 is as follows:

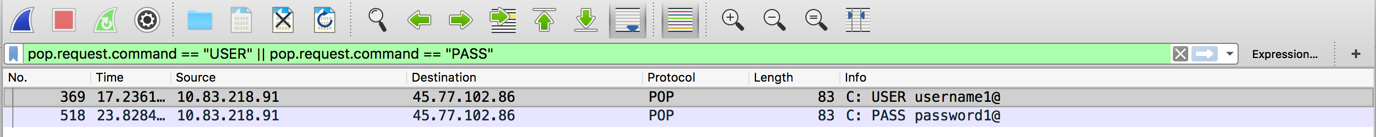
1. Open the email client and enter the username and password for login access.
2. Use POP as a display filter to list all the POP packets. It should be noted that this display filter will only list packets that use TCP port 110. If TLS is used, the filter will not list the POP packets. We may need to use tcp.port == 995 to list the POP3 packets over TLS.
3. Check the authentication has been passed correctly. In the following screenshot, you can see a session opened with a username that starts with doronn@ (all IDs were deleted) and a password that starts with u6F.
4. To see the TCP stream shown in the following screenshot, right-click on one of the packets in the stream and choose Follow TCP Stream from the drop-down menu:



1. Any error messages in the authentication stage will prevent communications from being established. You can see an example of this in the following screenshot, where user authentication failed. In this case, we see that when the client gets a Logon failure, it closes the TCP connection:



1. Use relevant display filters to list the specific packet. For example, pop.request.command == "USER" will list the POP request packet with the username and pop.request.command == "PASS" will list the POP packet carrying the password. A sample snapshot is as follows:



1. During the mail transfer, be aware that mail clients can easily fill a narrow-band communications line. You can check this by simply configuring the I/O graphs with a filter on POP.
2. Always check for common TCP indications: retransmissions, zero-window, window-full, and others. They can indicate a busy communication line, slow server, and other problems coming from the communication lines or end nodes and servers. These problems will mostly cause slow connectivity.

When the POP3 protocol uses TLS for encryption, the payload details are not visible. We explain how the SSL captures can be decrypted in the *There’s more…* section.

**IMAP communications**

IMAP is similar to POP3 in that it is used to retrieve the mail from the server by the client. The normal behavior of IMAP communication is as follows:

1. Open the email client and enter the username and password for the relevant account.
2. Compose a new message and send it from any email account.
3. Retrieve the email on the client that is using IMAP. Different clients may have different ways of retrieving the email. Use the relevant button to trigger it.
4. Check you received the email on your local client.

**SMTP communications**

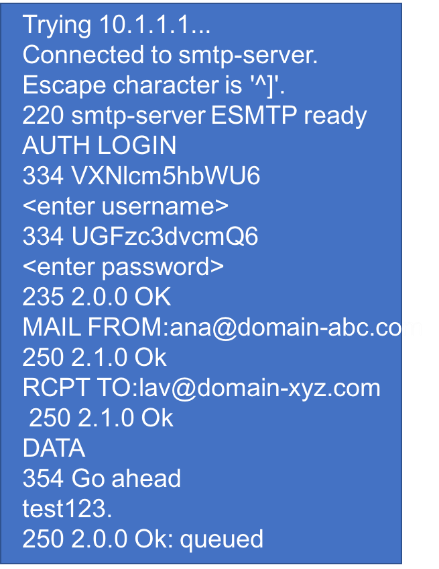
SMTP is commonly used for the following purposes:

* Server to server communications, in which SMTP is the mail protocol that runs between the servers
* In some clients, POP3 or IMAP4 are configured for incoming messages (messages from the server to the client), while SMTP is configured for outgoing messages (messages from the client to the server)

The normal behavior of SMTP communication is as follows:

* The local email client resolves the IP address of the configured SMTP server address.
* This triggers a TCP connection to port number 25 if SSL/TLS is not enabled. If SSL/TLS is enabled, a TCP connection is established over port 465.
* It exchanges SMTP messages to authenticate with the server. The client sends AUTH LOGIN to trigger the login authentication. Upon successful login, the client will be able to send mails.
* It sends SMTP message such as "MAIL FROM:<>", "RCPT TO:<>" carrying sender and receiver email addresses.
* Upon successful queuing, we get an OK response from the SMTP server.

The following is a sample SMTP message flow between client and server:



How it works…

In this section, let’s look into the normal operation of different email protocols with the use of Wireshark.

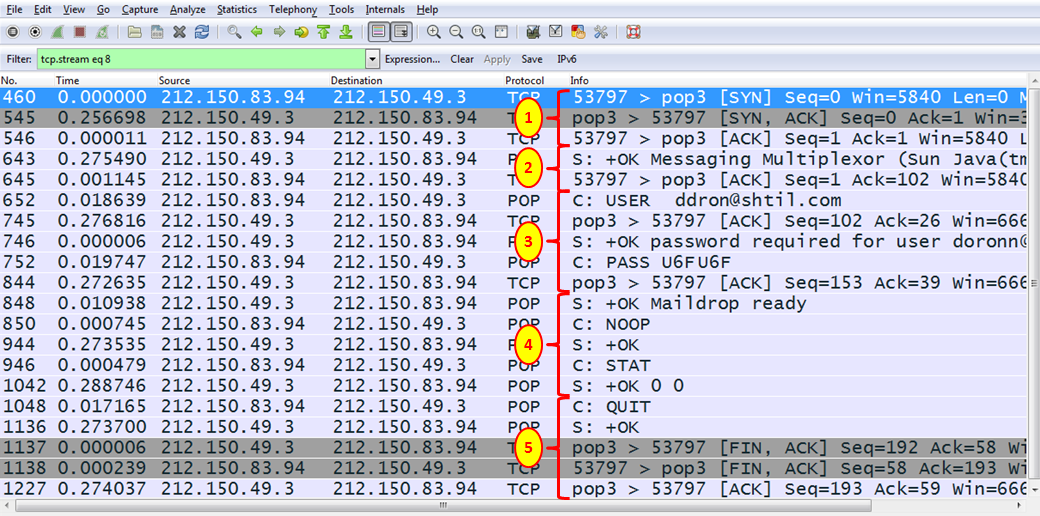
Mail clients will mostly use POP3 for communication with the server. In some cases, they will use SMTP as well. IMAP4 is used when server manipulation is required, for example, when you need to see messages that exist on a remote server without downloading them to the client. Server to server communication is usually implemented by SMTP.

The difference between IMAP and POP is that in IMAP, the mail is always stored on the server. If you delete it, it will be unavailable from any other machine. In POP, deleting a downloaded email may or may not delete that email on the server.

In general, SMTP status codes are divided into three categories, which are structured in a way that helps you understand what exactly went wrong. The methods and details of SMTP status codes are discussed in the following section.

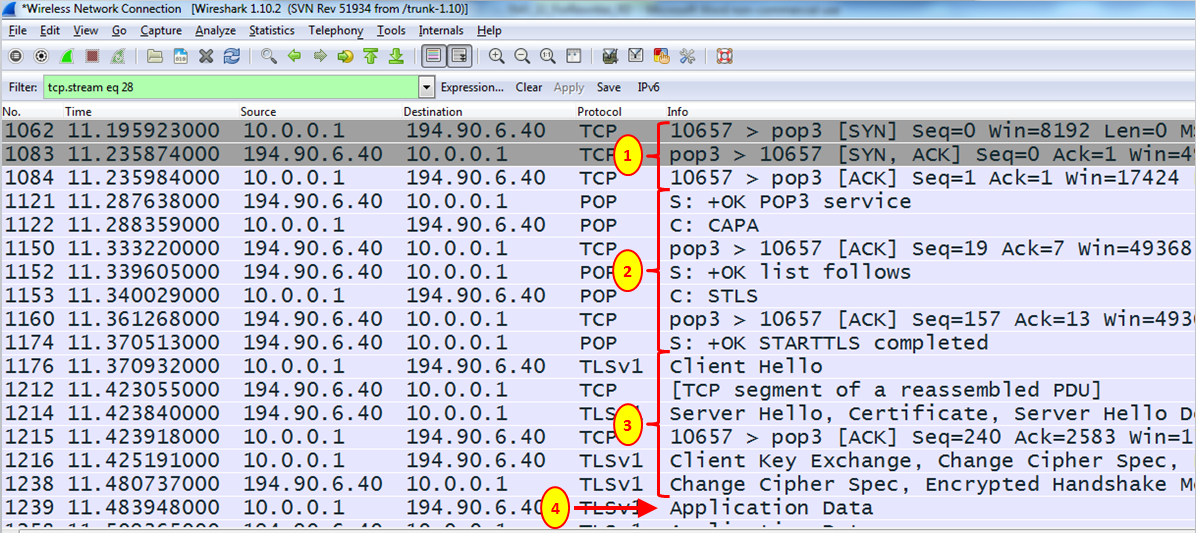
**POP3**

POP3 is an application layer protocol used by mail clients to retrieve email messages from the server. A typical POP3 session will look like the following screenshot:



It has the following steps:

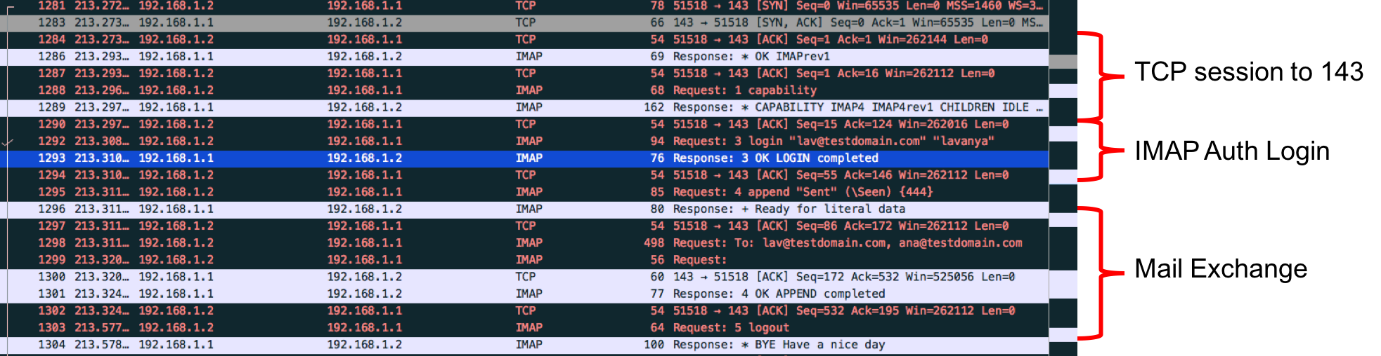
1. The client opens a TCP connection to the server.
2. The server sends an OK message to the client (OK Messaging Multiplexor).
3. The user sends the username and password.
4. The protocol operations begin. NOOP (no operation) is a message sent to keep the connection open, STAT (status) is sent from the client to the server to query the message status. The server answers with the number of messages and their total size (in packet 1042, OK 0 0 means no messages and it has a total size of zero)
5. When there are no mail messages on the server, the client send a QUIT message (1048), the server confirms it (packet 1136), and the TCP connection is closed (packets 1137, 1138, and 1227).
6. In an encrypted connection, the process will look nearly the same (see the following screenshot). After the establishment of a connection (**1**), there are several POP messages (**2**), TLS connection establishment (**3**), and then the encrypted application data:



**IMAP:-**

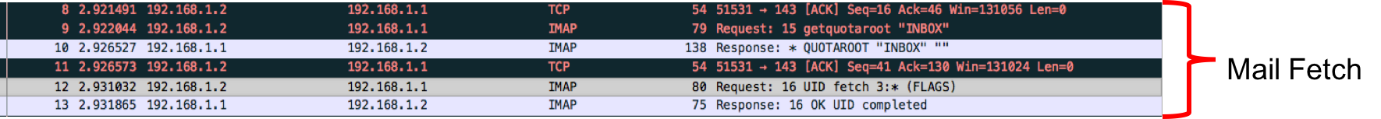
The normal operation of IMAP is as follows:

1. The email client resolves the IP address of the IMAP server:



As shown in the preceding screenshot, the client establishes a TCP connection to port 143 when SSL/TSL is disabled. When SSL is enabled, the TCP session will be established over port 993.

1. Once the session is established, the client sends an IMAP capability message requesting the server sends the capabilities supported by the server.
2. This is followed by authentication for access to the server. When the authentication is successful, the server replies with response code 3 stating the login was a success:

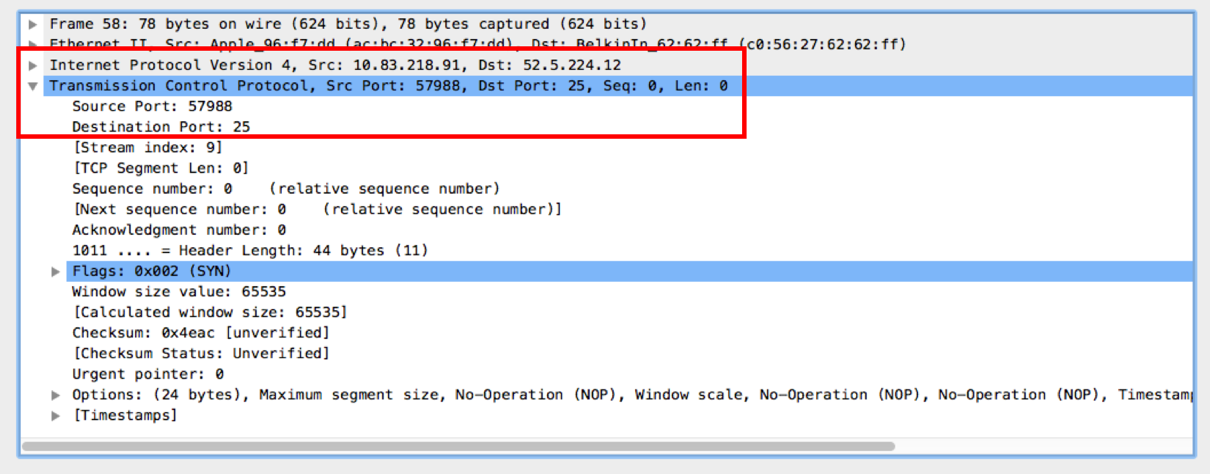


1. The client now sends the IMAP FETCH command to fetch any mails from the server.
2. When the client is closed, it sends a logout message and clears the TCP session.

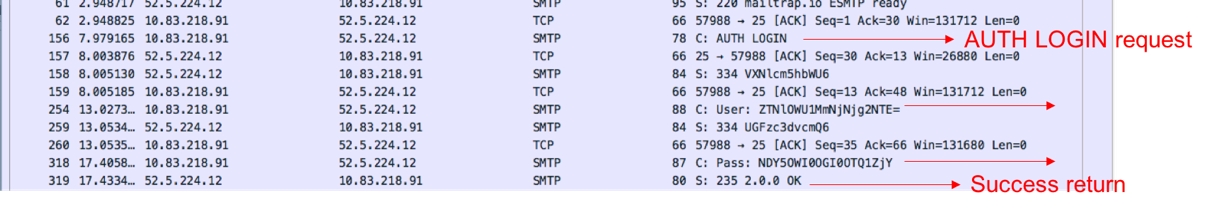
SMTP

The normal operation of SMTP is as follows:

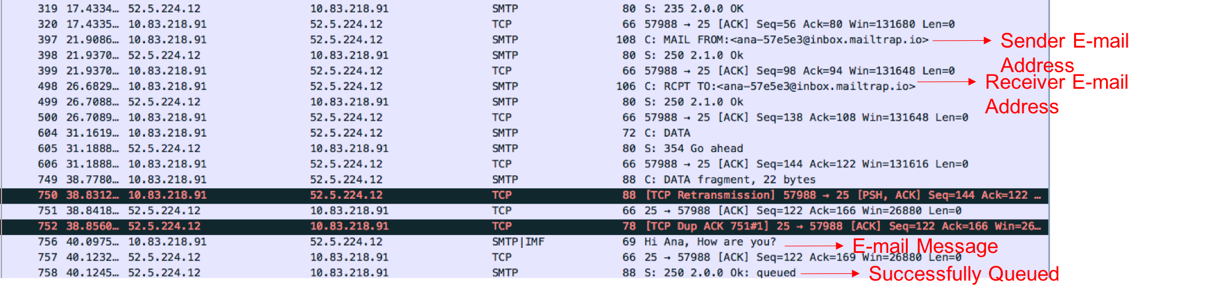
1. The email client resolves the IP address of the SMTP server:



1. The client opens a TCP connection to the SMTP server on port 25 when SSL/TSL is not enabled. If SSL is enabled, the client will open the session on port 465:



1. Upon successful TCP session establishment, the client will send an AUTH LOGIN message to prompt with the account username/password.
2. The username and password will be sent to the SMTP client for account verification.
3. SMTP will send a response code of 235 if authentication is successful:



1. The client now sends the sender’s email address to the SMTP server. The SMTP server responds with a response code of 250 if the sender’s address is valid.
2. Upon receiving an OK response from the server, the client will send the receiver’s address. SMTP server will respond with a response code of 250 if the receiver’s address is valid.
3. The client will now push the actual email message. SMTP will respond with a response code of 250 and the response parameter OK: queued.
4. The successfully queued message ensures that the mail is successfully sent and queued for delivery to the receiver address.

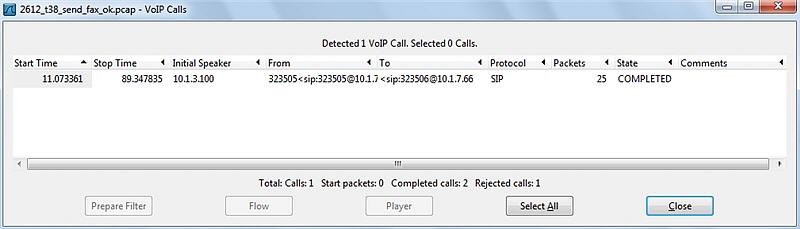
**Analyzing Voip using Wireshark:-**

The Wireshark program implements a convenient mechanism for diagnosing (analyzing) VoIP calls, in particular, you can get a graphical diagram of calls and see how data was exchanged. Wireshark allows you to analyze the SIP protocol and its RTP traffic.

Suppose that during the execution of a VoIP call using Wireshark, network packets were captured and this dump should be analyzed.

**Walktrough Steps:**  
  
1. Select a SIP or RTP packet from the list (in our example, analyze the RTP traffic). To filter packets, you can enter a value in the **Filter** field.  **sip** or **rtp** to display only a certain type of traffic.

2. Go to the **Statistics** menu (or **Telephony** , depending on the version of the program) **> VoIP Calls** .  
The **VoIP Calls** window opens with a list of VoIP calls.



The list of VoIP calls shows the following information for each call:

* + Start Time: The time the call started.
  + Stop Time: The end time of the call.
  + Initial Speaker: The IP address of the packet source that initiated the call.
  + From: For SIP calls, the INVITE request is displayed in the "From" field.
  + To: For SIP calls, the INVITE request is displayed in the "To" field.
  + Protocol: Protocol.
  + Packets: The number of packets participating in the call.
  + State: Call status.
  + Comment: Additional comments.

3. Select a VoIP call and then click the **Graph** button (or **Flow** , depending on the version of the program). The **Graph Analysis** window will appear with a graphical diagram of the VoIP call data exchange.

