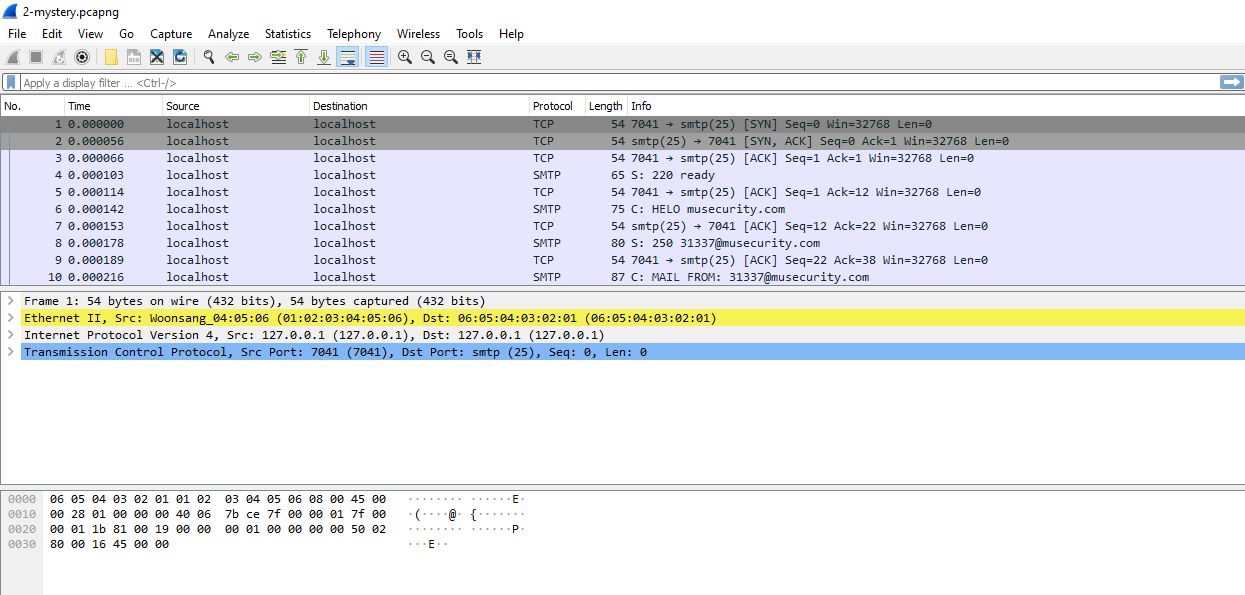
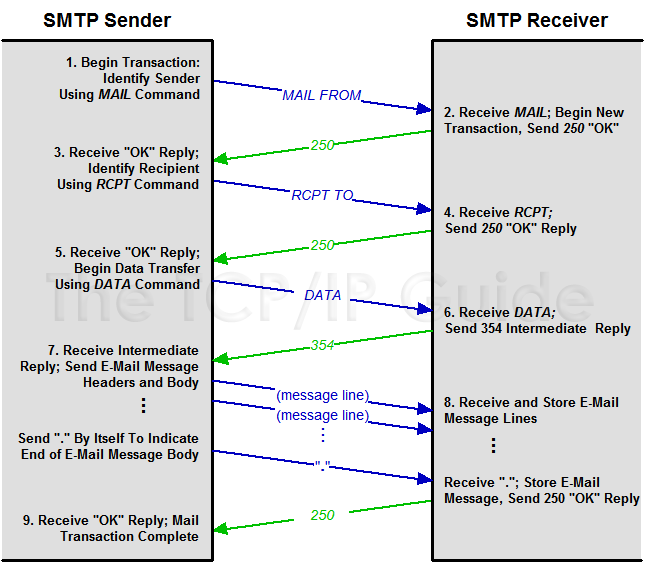
**Mystery 2**



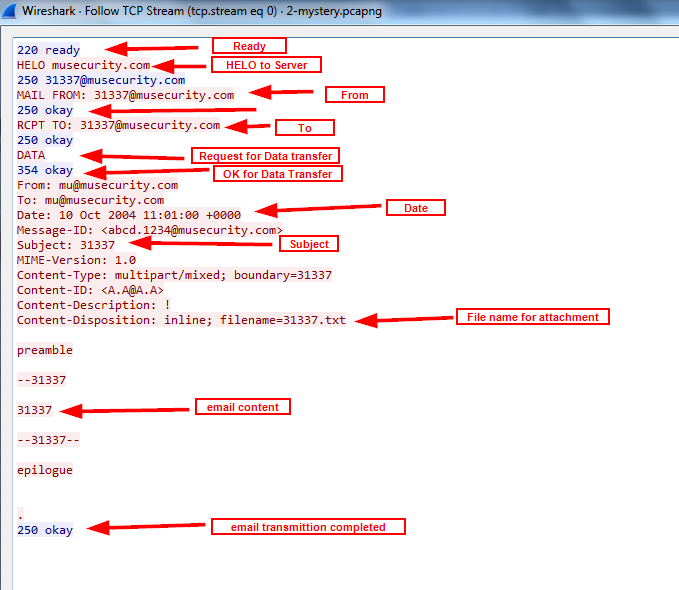
**Simple Mail Transfer Protocol (SMTP)**

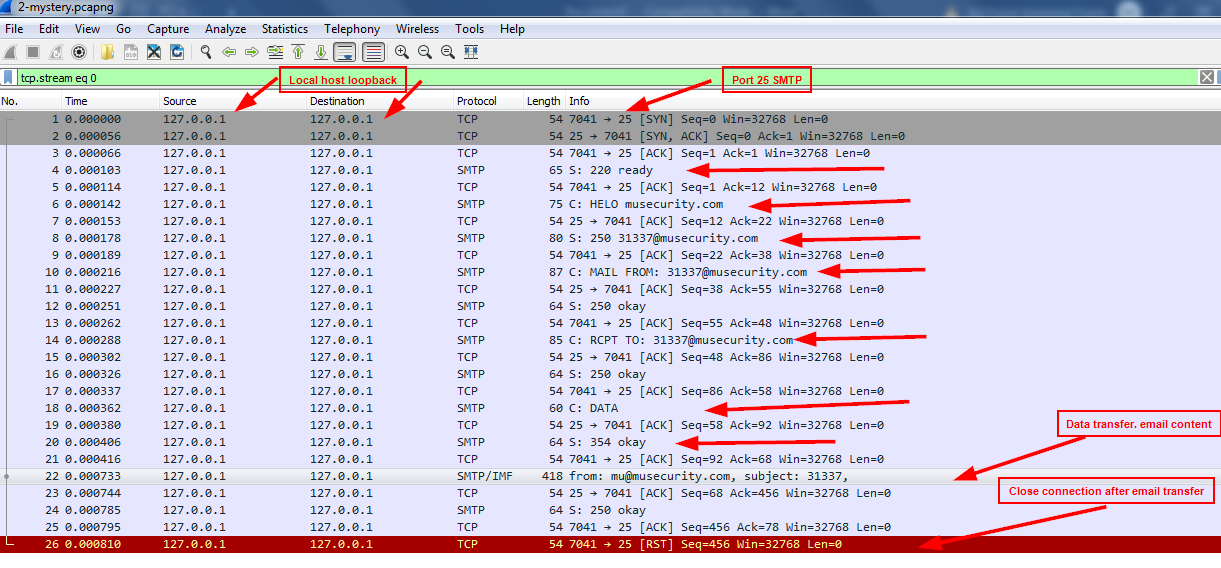
Simple Mail Transfer Protocol (SMTP) is the standard protocol for email services on a TCP/IP network. SMTP provides the ability to send and receive email messages. SMTP is an application-layer protocol that enables the transmission and delivery of email over the Internet. SMTP is created and maintained by the Internet Engineering Task Force (IETF). Simple Mail Transfer Protocol is also known as RFC 821 and RFC 2821

**Steps of SMTP Communication :**



**Analysis of the 2-mystery.pcapng capture and TCP stream dump**





The major steps have been highlighted in the two screen captures from the Wireshark logs.The Source and Destination IP addresses used are the localhost loopback IP addresses.

The server-side port is 25 for SMTP and a random port 7041 on client side is used. The SMTP server is musecurity.com. The email From and To is [31337@musecurity.com](mailto:31337@musecurity.com). The email subject is Subject: 31337. The file name of the text of email is filename=31337.txt. The content of the email is 31337