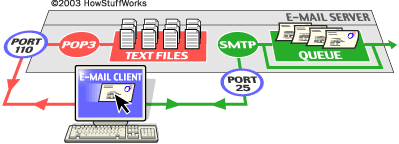
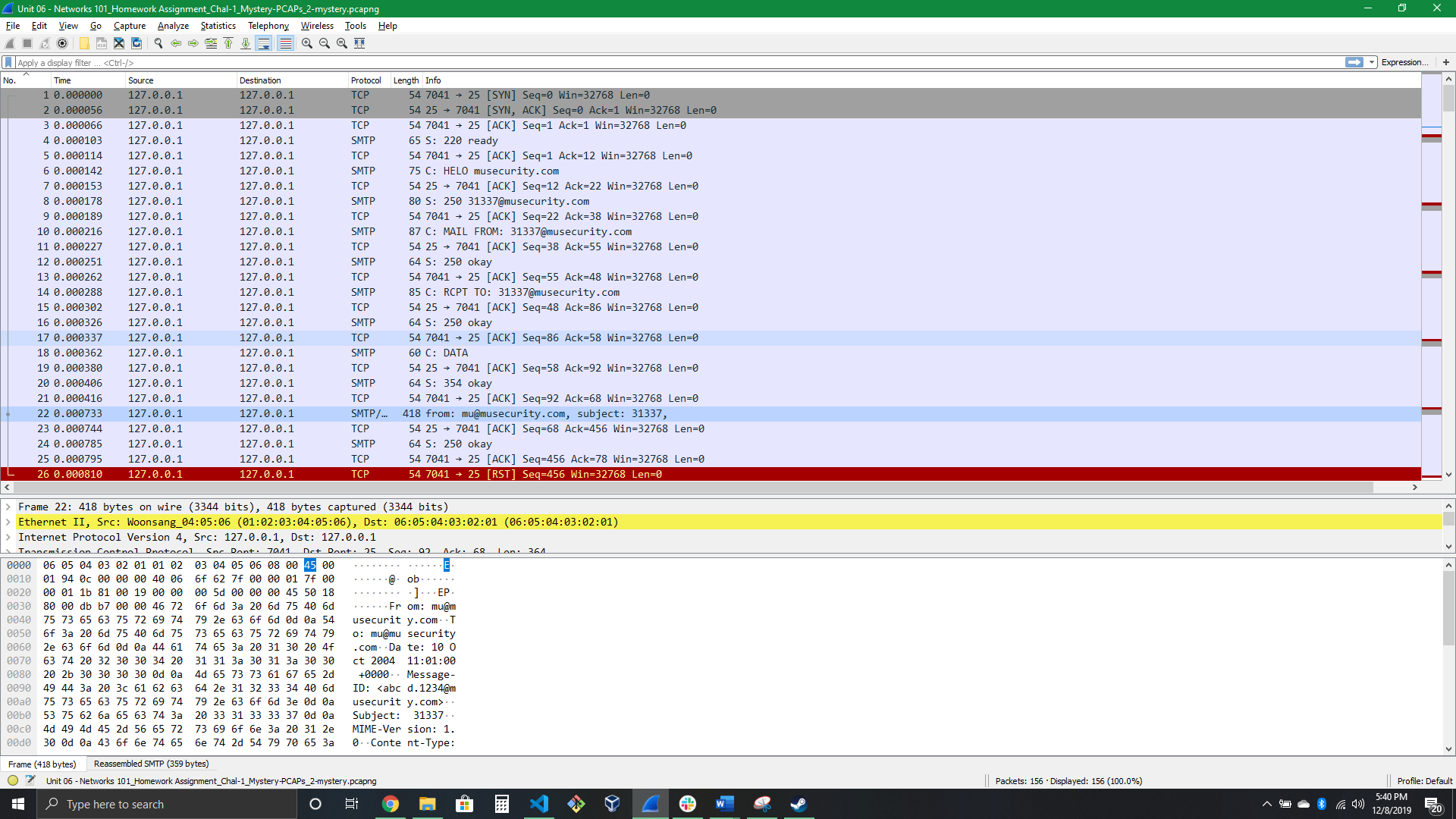
SMTP Application Layer

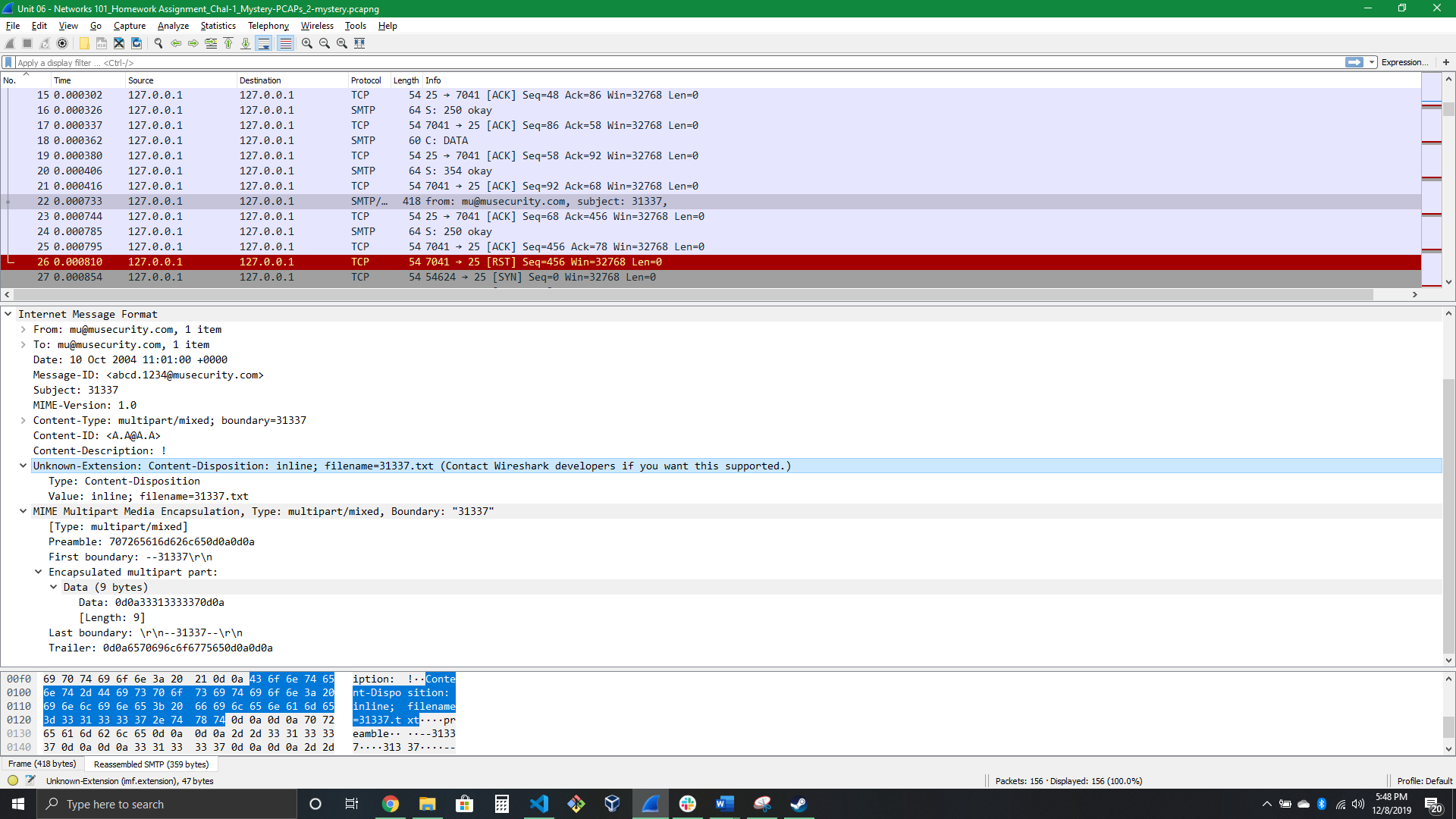
Simple Mail Transport Protocol is part of the application layer of the TCP/IP protocol. Using a process called "store and forward," SMTP moves your email on and across networks. It works closely with something called the Mail Transfer Agent (MTA) to send your communication to the right computer and email inbox. (whatismyipaddress)

 (Howstuffworks)

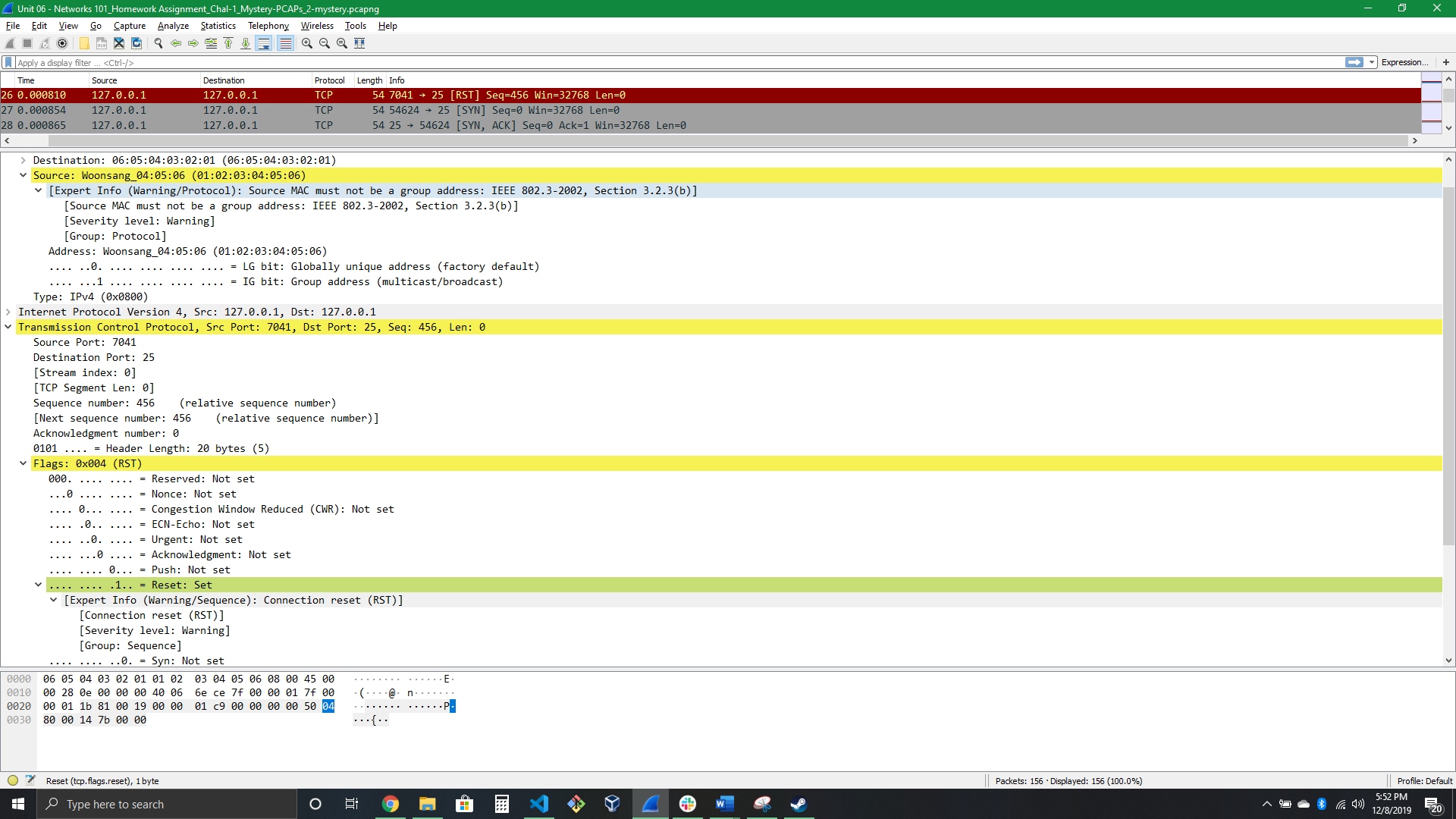
IP Address 127.0.0.1 on port 7041 is sending information to the IPaddress 127.0.0.1 on port 25. Port 7041 is [31337@musecurity.com](mailto:31337@musecurity.com) who is trying to send info to the general [mu@musecurity.com](mailto:mu@musecurity.com) which means that 31337 is a potential threat actor. Port 25 responds with a 220 telling port 7041 to go ahead. Port 7041 then specifies who the message is from who the message is going to and what the message encapsulates with port 25 give acks during the entire process.



Now the message gets pushed to the client where you can see port 7041 included a very suspicious looking 31337.txt which you should TOTALLY CLICK ON (**NOT**). The worst part about this is that the email appears to be coming from your email address or from your network email.



Finally, you can see where port 4071 issues a reset command to port 25 and aborts the connection. You can also see that there are 2 flags being raised by wire shark. Flag 1 is that 7041 Source MAC is set to be a group address, which tells us that they are trying to send information to multiple people. Flag 2 is that port 7041 issues a reset command. Considering what we have learned so far this is an example of a spear phishing attack.



Fun note: [31337@musecurity.com](mailto:31337@musecurity.com) is a reference to port number 31337. This port number means "elite" in hacker/cracker spelling (3=E, 1=L, 7=T) and because of the special meaning is often used for interesting stuff... Many backdoors/trojans run on this port, the most notable being Back Orifice. (speedguide)

# References

What is Simple Mail Transfer Protocol (SMTP)? (n.d.). Retrieved December 8, 2019, from <https://whatismyipaddress.com/smtp>.

How stuff works, Crosby, T. (2007, October 18). How E-mail Works. Retrieved December 8, 2019, from <https://computer.howstuffworks.com/e-mail-messaging/email3.htm>.

Speed Guide. (n.d.). Port 31337 (tcp/udp). Retrieved December 8, 2019, from <https://www.speedguide.net/port.php?port=31337>.