NAME: Megan Leonard

TODAY’S DATE: 4/2/2023

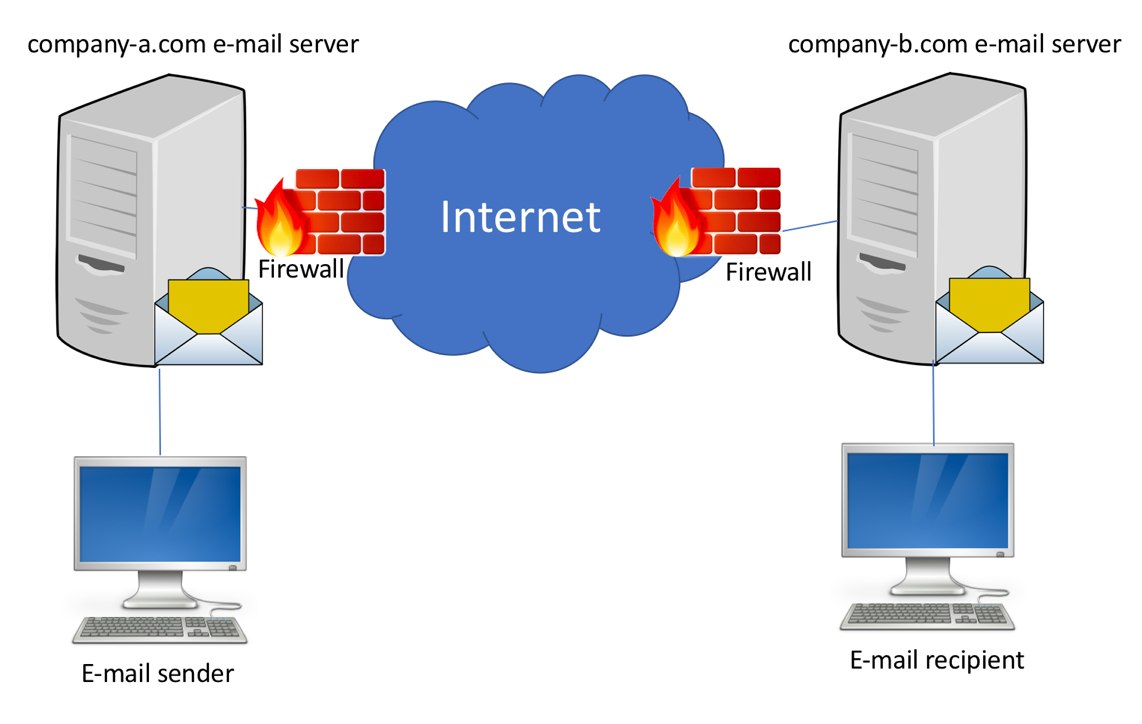
# ISEC 375 Homework 9

Answer the following questions based on your reading of the textbook, the module key points, and the instructor’s presentation this week.

1. **[9 points]** You are investigating an e-mail scam case. You want to check the “source IP address” and “timestamp” of a specific e-mail message. You have direct access to the UNIX e-mail server. Which places and log files do you check to confirm source IP address and timestamp?

To check for the source IP address and timestamp we would need to look into /var/log/maillog in the server as they should be stored there. If they were moved, we would need to use the find command to find their new location. We would also look at the /etc/syslog.conf to make sure that the e-mail we are looking for has actually passed through the server.

1. **[12 points]** You are investigating a stalking case. You have to make e-mail forensics in the scope of this case. The suspect is working in company-a, the victim is working in company-b. As a forensic investigator, you want to collect as much evidence as possible to corroborate your findings. You are on the premises of the company-b. Please list the source and type of evidence by using the topology below.

******

As we are on the premise of company b we can start with the e-mail recipient’s computer and e-mail. We start with creating a copy of the email itself from the computer and we can look at the e-mail header with a text editor, this should allow us to get the originating e-mail’s IP address, date and time the message was sent and any files sent with it. We turn to the company-b.com e-mail server which the e-mail passed through to get to the recipient. Here, we can contact the network e-mail administrator to help us with accessing the server. We can then look into the log maillog to double check the information we acquired from the e-mail recipient. We can mark when it arrived at the server and when it was sent out to the recipient. We can now look at the firewall logs to see if the e-mail has traveled through the firewall that we know connects the server to the internet.

1. **[9 points]** What are the challenges of social media investigations?

There are many challenges of social media investigations with the first being the jurisdiction as networks can cross multiple borders and have different sections of the network enter different jurisdictions. There are also the evidence artifacts that are different depending on the social media and the device. There is a lack of software for social media forensics and a warrant can be harder to acquire.