Guruprasad Sivagurunatha Krishnan
107391284
sguru@iastate.edu

HOMEWORK 3

Experiment 1

1) Sending an email to sguru@spock.ee.iastate.edu

```
> telnet spock.ee.iastate.edu 25
Trying 129.186.215.48...
Connected to spock.ee.iastate.edu.
Escape character is '^]'.
220 spock.ee.iastate.edu ESMTP Sendmail 8.13.4/8.13.4; Mon,26 Nov 2012 12:37:54 -0600
(CST)
Welcome bones.ee.iastate.edu
250 spock.ee.iastate.edu Hello bones.ee.iastate.edu [129.186.215.41], Nice to meet you
MAIL FROM: sguru@bones.ee.iastate.edu
250 2.1.0 sguru@bones.ee.iastate.edu... Sender ok
rcply to: sguru
250 2.1.5 sguru... Recipient ok
data
354 Enter mail, end with "." on a line by itself
Hello Welcome
.
250 2.0.0 mA7LksIL096730 Message accepted for delivery
```

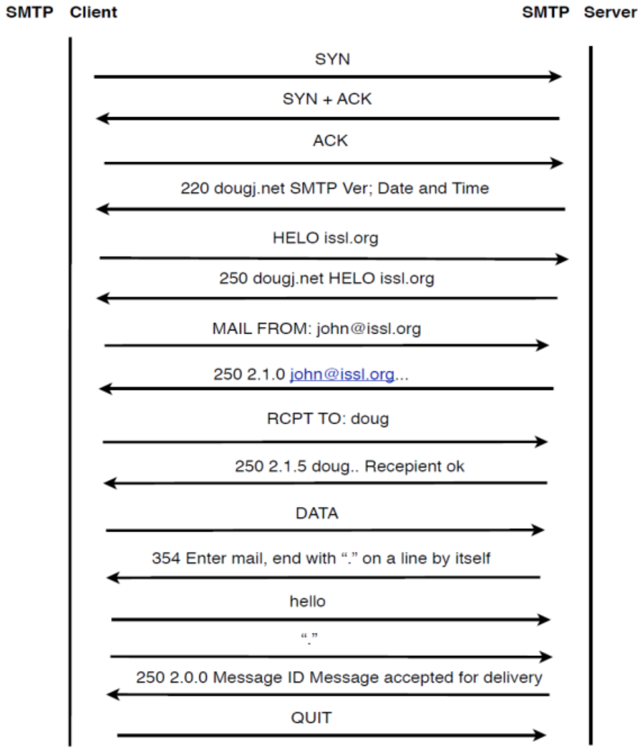
2) Commands to Retrieve Mail from spock.ee.iastate.edu

```
> telnet spock.ee.iastate.edu 110
Trying 129.186.215.48...
Connected to spock.ee.iastate.edu.
Escape character is '^]'.
+OKQPOP(version2.53)atspock.ee.iastate.edustarting.
<76848.1226096425@spock.ee.iastate.edu>
user sguru
+OK Password required for sguru.
pass cpre530
+OK sguru has 1 message (520 octets).
list
+OK 1 messages (520 octets)
1 520
.
retr 1
+OK 520 octets
Return-Path: sguru@bones.ee.iastate.edu
Received: from bones.ee.iastate.edu (bones.ee.iastate.edu [129.186.215.41])
by spock.ee.iastate.edu (8.13.4/8.13.4) with SMTP id mA7LksIL096730
for sguru; Mon,26 Nov 2012 12:27:54 -0600 (CST)
(envelope-from sguru@bones.ee.iastate.edu)
Date: Mon,26 Nov 2012 12:38:57 -0600 (CST)
From: sguru@bones.ee.iastate.edu
Message-Id: <201211262147.mA7LksIL096730@spock.ee.iastate.edu>
```

To: undisclosed-recipients:;
X-UIDL: 66bdfd8413c8100bd537c5ba22b05a26
Hello Welcome
.

3) Tracing back emails-
Email Message From Source Traced To
sgpharish@gmail.com 72.33 .87.233 – Dallas, Texas
arvindm@gmail.com 214.233.20.59 – Bangalore, India
annamalai@hotmail.com 81.32.65.43 – San Jose, California
rajinikanth@microsoft.com 202.138.127.106 – Hyderabad, India

1)
a)


SMTP Client
SMTP Server
SYN
SYN + ACK
ACK
220 dougj.net SMTP Ver; Date and Time
HELO issl.org
250 dougj.net HELO issl.org
MAIL FROM: john@issl.org
250 2.1.0 john@issl.org...
RCPT TO: doug
250 2.1.5 doug.. Recepient ok
DATA
354 Enter mail, end with "." on a line by itself
hello
"."
250 2.0.0 Message ID Message accepted for delivery
QUIT

b)
Assuming each message is sent as one TCP packet, the total number of bytes (TCP payload) required to send this message is 55 bytes.

c)
936 is the total number of bytes transmitted on the network including all packets – 30 bytes for IP header and 25 bytes of Ethernet header per TCP packet

d)
The total overhead (total number of bytes sent on the wire versus the total size of the payload) is 936 bytes vs 55 bytes.

e)
The total overhead (total number of bytes sent on the wire versus the total size of the user message) is – 936 bytes vs 5 bytes.

12)
Every MTA that passes the email, attaches its own header to it. The header would contain information such as the machine name and/or IP address of every MTA along the way. As long as the IP address is a public IP, we can trace. By tracing back to the MTA and with the knowledge of the IP address of the sender, we can get the physical location of the IP address of the sender from network registration authorities. However, if the sender IP address is a private IP address, tracing back to the physical location would not be possible.

To find out someone who is using email for illegal purposes would not be really useful because the attacker should be smart enough to use a public machine to carry out the illegal activity. If it is a public computer, it would be impossible to carry out the trace to the person. However, we could trace back to the owner of the IP address as long as it is not a private address.

13)

27 SPAM email headers were traced.