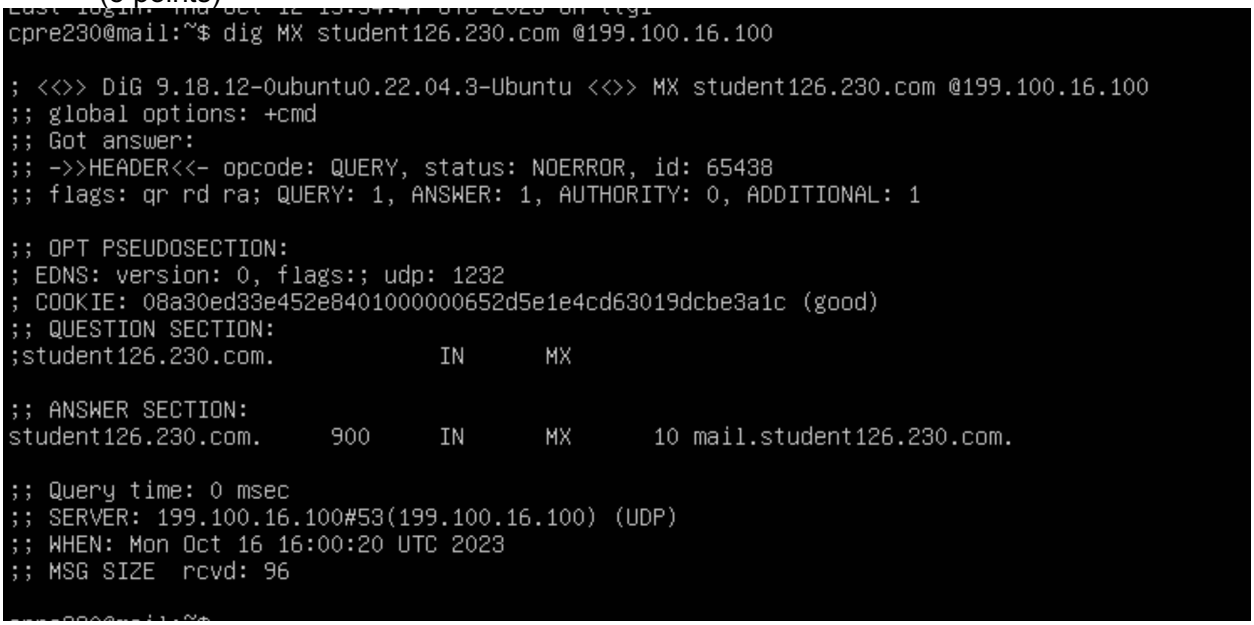
Lab 07 Template – Ethan Roepke

1. **Screenshot of properly configured DNS MX query**
   (5 points)



2. **Screenshot of output from** `netstat -tnl`
   (5 points)

3. **Screenshot of Sending mail from cpre230a --> cpre230b in terminal**
   (10 points)

```
cpre230@mail:~$ telnet mail.student126.230.com 25
Trying 192.168.1.204...
Connected to mail.student126.230.com.
Escape character is '^]'.
220 mail.student126.230.com ESMTP Postfix (Ubuntu)
helo student126.230.com
250 mail.student126.230.com
mail from: <cpre230a@student126.230.com>
250 2.1.0 Ok
rcpt to: <cpre230b@student126.230.com>
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Subject: You are a failure
Why did you get arrested.....
.
250 2.0.0 Ok: queued as 709673DB5
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

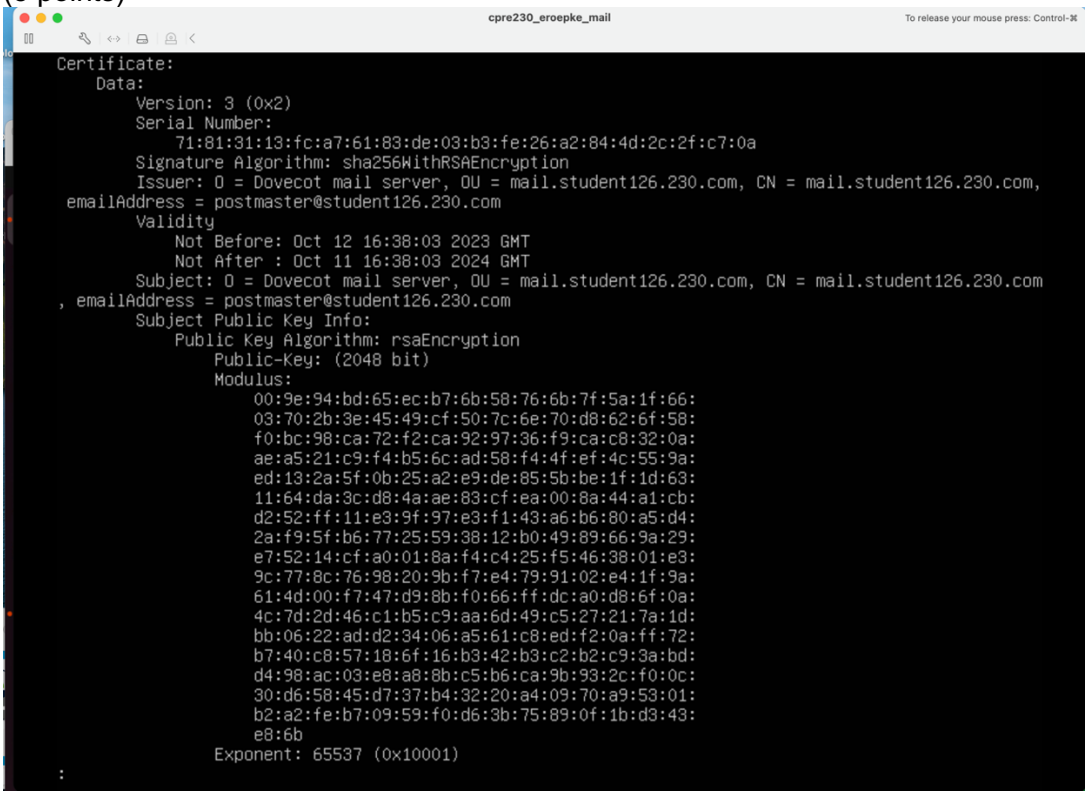
4. **Screenshot of reading the previously sent message in terminal**
(10 points)

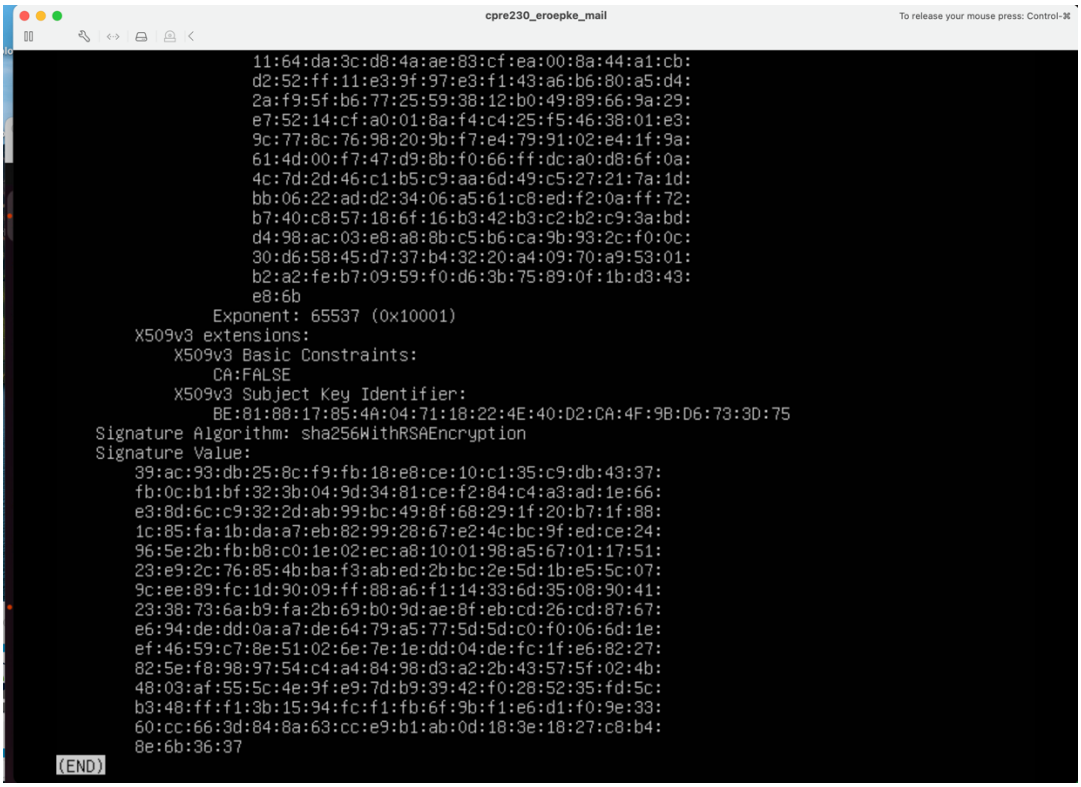
```
cpre230@mail:~$ telnet mail.student126.230.com 110
Trying 192.168.1.204...
Connected to mail.student126.230.com.
Escape character is '^]'.
+OK Dovecot (Ubuntu) ready.
USER cpre230b
+OK
PASS cpre230
+OK Logged in.
LIST
+OK 2 messages:
1 542
2 550
.
RETR 2
+OK 550 octets
Return-Path: <cpre230a@student126.230.com>
X-Original-To: cpre230b@student126.230.com
Delivered-To: cpre230b@student126.230.com
Received: from student126.230.com (mail.student126.230.com [192.168.1.204])
        by mail.student126.230.com (Postfix) with SMTP id 709673DB5
        for <cpre230b@student126.230.com>; Thu, 12 Oct 2023 16:27:13 +0000 (UTC)
Subject: You are a failure
Message-Id: <20231012162741.709673DB5@mail.student126.230.com>
Date: Thu, 12 Oct 2023 16:27:13 +0000 (UTC)
From: cpre230a@student126.230.com

Why did you get arrested.....
.
QUIT
+OK Logging out.
Connection closed by foreign host.
cpre230@mail:~$
```

5. **Screenshot of Dovecot cert raw contents**
(5 points)

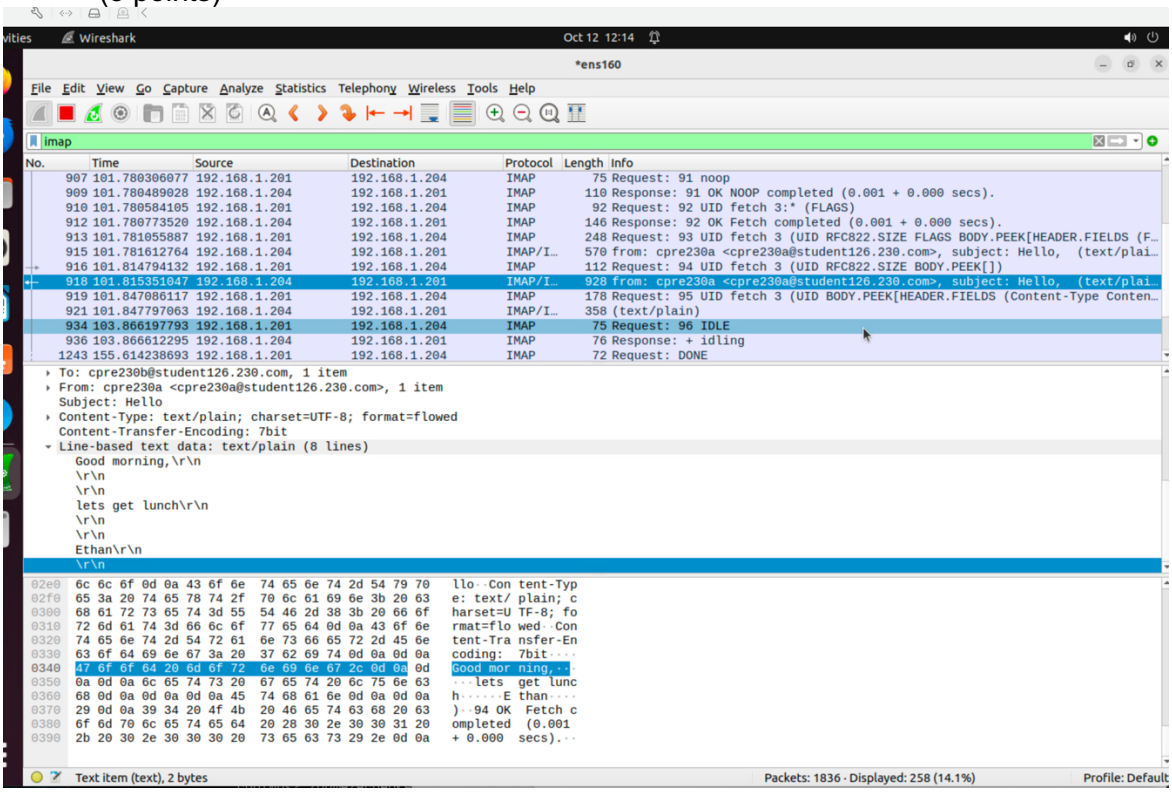
```
root@mail:/usr/share/dovecot# cd /etc/dovecot/ssl
root@mail:/etc/dovecot/ssl# sudo cat dovecot.pem
-----BEGIN CERTIFICATE-----
MIID3DCCAsSgAwIBAgIUcYExE/ynYYPeA7P+JqKETSwvxwowDQYJKoZIhvcNAQEL
BQAwgZAxHDAaBgNVBAoME0RvdmVjb3QgbWFpbCBzZXJ2ZXIxIDAeBgNVBAsMF21h
aWwuc3R1ZGVudDEyNi4yMzAuY29tMSAwHgYDVQQDDBdtYWlsLnN0dWRlbnQxMjYu
MjMwLmNvbTEsMCoGCSqGSIb3DQEJARYdcG9zdG1hc3RlckBzdHVkZW50MTI2LjIz
MC5jb20wHhcNMjMxMDEyMTYzODAzWhcNMjQxMDExMTYzODAzWjCBkDEcMBoGA1UE
CgwTRG92ZWNvdCBtYWlsIHNlcnZlcjEgMB4GA1UECwwXbWFpbC5zdHVkZW50MTI2
LjIzMC5jb20xIDAeBgNVBAMMF21haWwuc3R1ZGVudDEyNi4yMzAuY29tMSwwKgYJ
KoZIhvcNAQkBFh1wb3N0bWFzdGVyQHN0dWR1bnQxMjYuMjMwLmNvbTCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ6UvWXst2tYdmt/Wh9mA3ArPkVJz1B8
bnDYYm9Y8LyYynLyypKXNvnKyDIKrqUhyfS1bK1Y9E/vTFWa7RMqXwslounehVu+
Hx1jEWTaPNhKroPP6gCKRKHL0lL/EeOfl+PxQ6a2gKXUKvlftnclWTgSsEmJZpop
51IUz6ABivTEJfVGOAHjnHeMdpggm/fkeZEC5B+aYUOA9OfZi/Bm/9yg2G8KTHOt
RsG1yaptScUnIXoduwYirdIOBqVhyO3yCv9yt0DIVxhvFrNCs8KyyTq91JisA+io
i8W2ypuTLPAMMNZYRdc3tDIgpAlwqVMBsqL+twlZ8NY7dYkPG9ND6GsCAwEAAaMs
MCowCQYDVR0TBAIwADAdBgNVHQ4EFgQUvoGIF4VKBHEYIk5AOspPm9ZzPXUwDQYJ
KoZIhvcNAQELBQADggEBADmsk9sljPn7GOjOEME1ydtDN/sMsb8yOwSdNIHO8oTE
o60eZuONbMkyLauZvEmPaCkfILcfiByF+hvap+uCmShn4ky8n+3OJJZeK/u4wB4C
7KgQAZilZwEXUSPpLHaFS7rzq+OrvC5dG+VcB5zuifwdkAn/iKbxFDNtNQiQQSM4
c2q5+itpsJ2uj+vNJs2HZ+aU3t0Kp95keaV3XV3A8AZtHu9GWceOUQJufh7dBN78
H+aCJ4Je+JiXVMSkhJjToitDV18CSOgDr1VcTp/pfbk5QvAoUjX9XLNI//E7FZT8
8ftvm/HmOfCeM2DMZj2EimPM6bGrDRg+GCfItI5rNjc=
-----END CERTIFICATE-----
root@mail:/etc/dovecot/ssl#
```

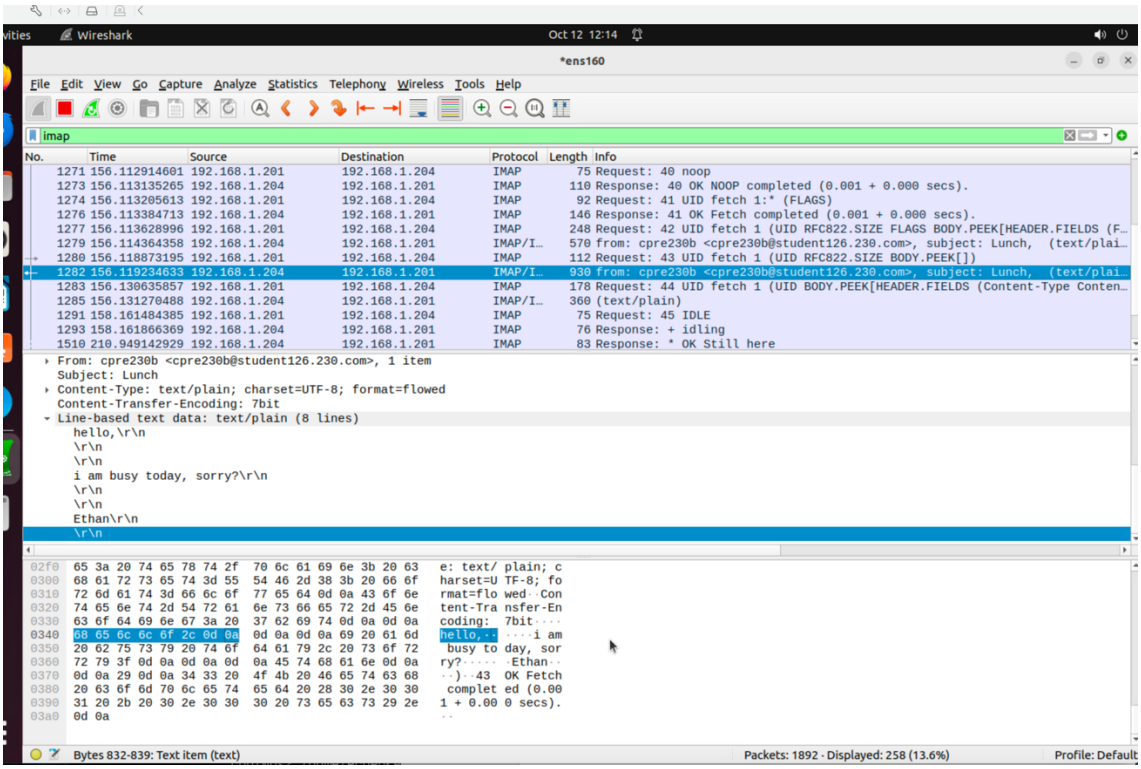
6. **Screenshot of Dovecot cert parsed as X.509**
(5 points)





7. **Screenshot of plaintext IMAP - Wireshark**
(5 points)





8. **Screenshot of Base64 decode of password**
(10 points)

Decode from Base64 format

Simply enter your data then push the decode button.

AGNwcmUyMzBiAGNwcmUyMzA=

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

Decode each line separately (useful for when you have multiple entries).

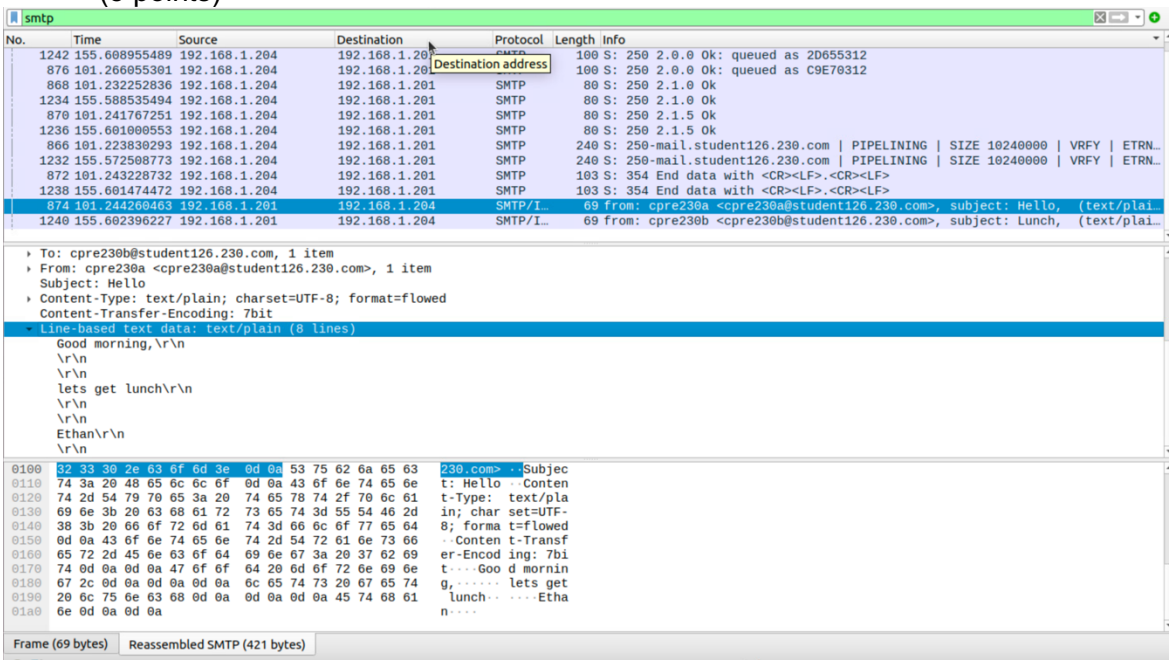
Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

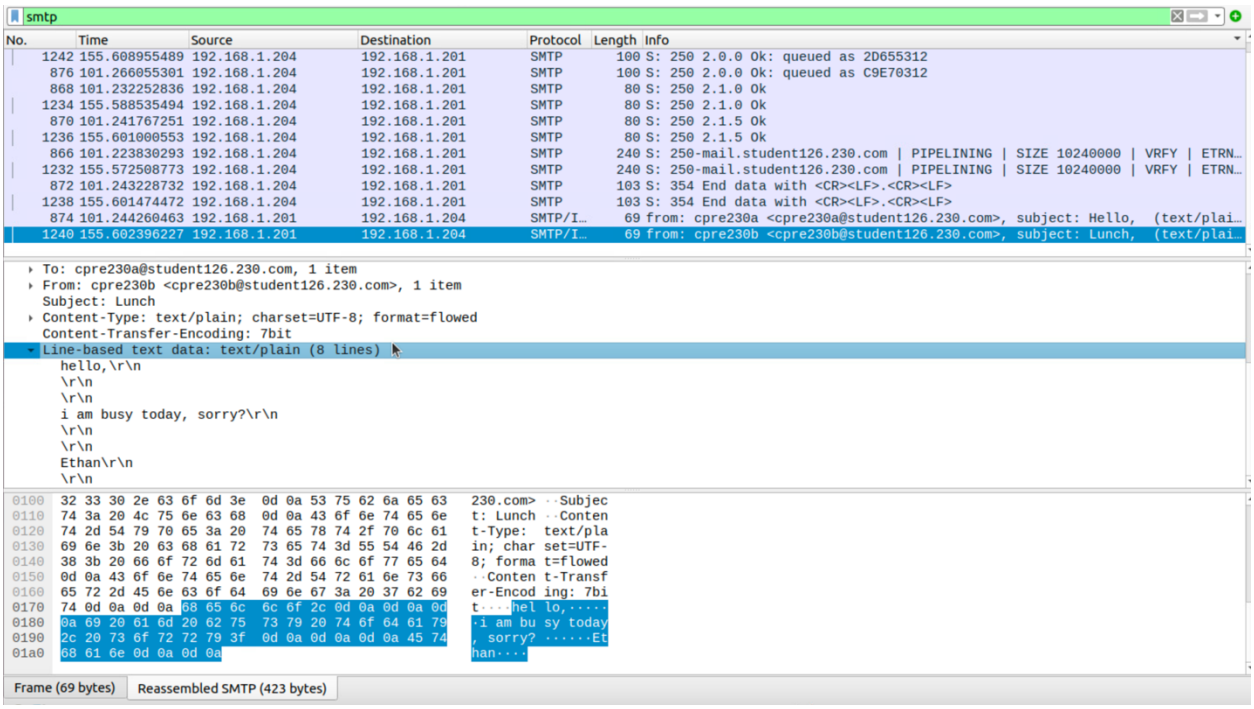
DECODE Decodes your data into the area below.

Copy to clipboard

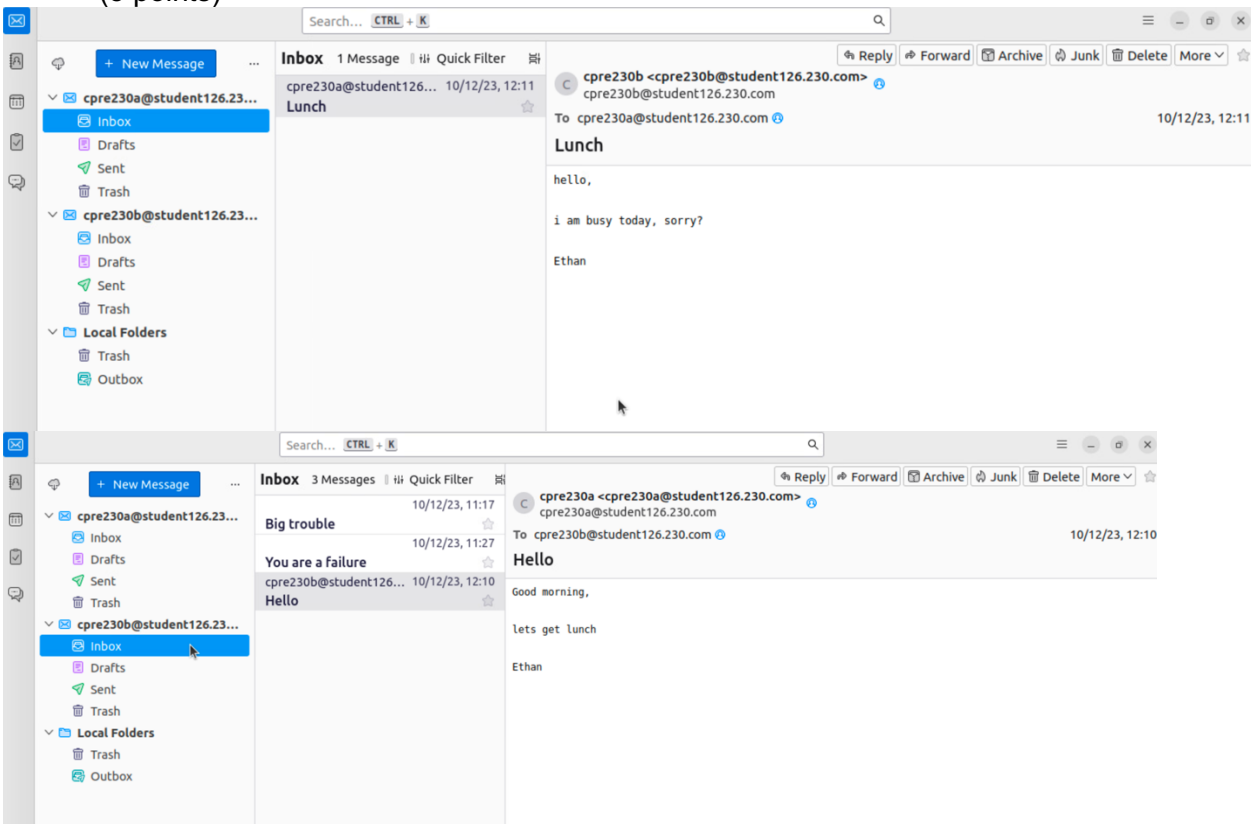
Decode files from Base64 format

9. **Screenshot of plaintext SMTP - Wireshark**
(5 points)

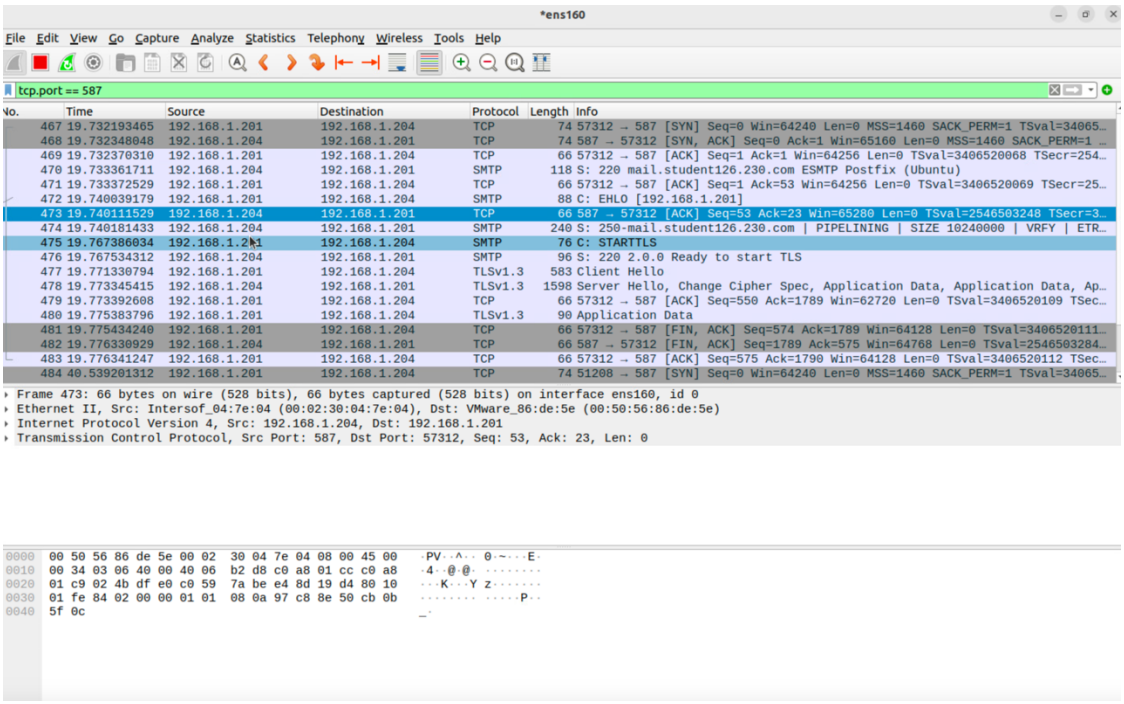




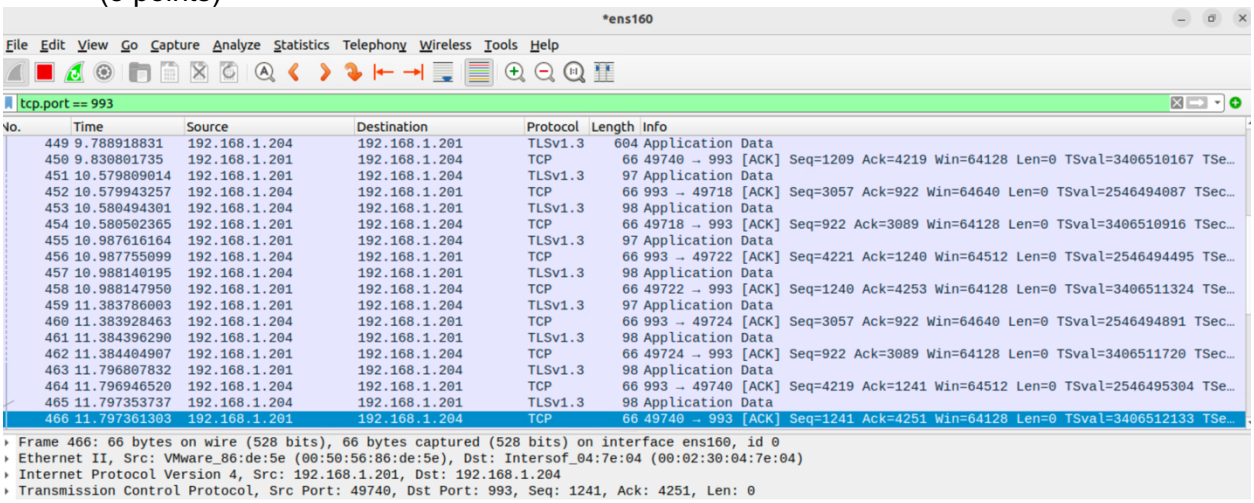
10. **Screenshot of test messages in Thunderbird**
(5 points)

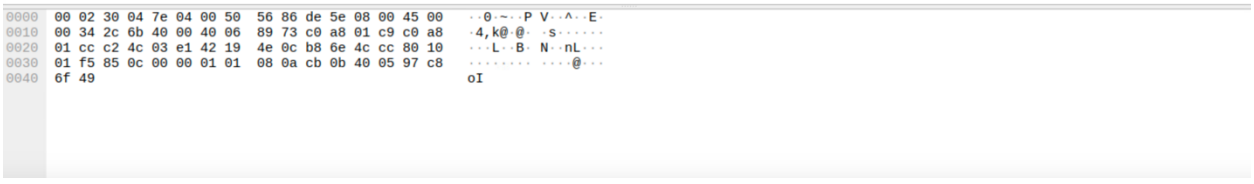


11. **Screenshot of encrypted SMTP - Wireshark**
(5 points)



12. **Screenshot of encrypted IMAP - Wireshark**
(5 points)





13. **Screenshot of NAT rules**
(5 points)

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
Desktop - Nagios check										
	WAN	TCP	*	*	105.148.172.201	22 (SSH)	192.168.1.201	22 (SSH)	desktop1 - SSH check	
NS2 - Nagios checks										
	WAN	TCP/UDP	37.56.23.100	*	105.148.172.199	53 (DNS)	192.168.1.200	53 (DNS)	ns2 - Nagios DNS for inside machines	
ldap - nagios check										
	WAN	TCP	37.56.23.100	*	105.148.172.205	389 (LDAP)	192.168.1.205	389 (LDAP)	ldap - nagios check from outside network	
mail - nagios check										
	WAN	TCP	37.56.23.100	*	105.148.172.204	25 (SMTP)	192.168.1.204	25 (SMTP)	mail - nagios secure SMTP	
	WAN	TCP	37.56.23.100	*	105.148.172.204	993 (IMAP/S)	192.168.1.204	993 (IMAP/S)	mail - nagios secure imap login	
	WAN	TCP	37.56.23.100	*	105.148.172.204	587 (SUBMISSION)	192.168.1.204	587 (SUBMISSION)	mail - nagios secure IMAP	
	WAN	TCP	37.56.23.100	*	105.148.172.204	110 (POP3)	192.168.1.204	110 (POP3)	mail - nagios mail pop	

14. **Screenshot of Nagios queries with green indicated for all mail services** (20 points)

www.student125.230.com	www http, www https, www login	
www2.student125.230.com	www2 django, www2 ssh	

Student 126 (student126)

Host	Services	Actions
desktop1.student126.230.com	desktop1 ssh	
ldap.student126.230.com	ldap Bezos, ldap Gates, ldap Jobs, ldap Musk, ldap Zuckerberg, ldap service	
mail.student126.230.com	dns MX, mail pop, secure imap, secure imap login, secure smtp	
ns1.student126.230.com	dns mail, dns ns1, dns www, dns www2, reverse dns mail, reverse dns ns1, reverse dns www, reverse dns www2	
ns2.student126.230.com	dns desktop1, dns ldap, dns ws, reverse dns desktop1, reverse dns ldap, reverse dns ws	
www.student126.230.com	www http, www https, www login	
www2.student126.230.com	www2 django, www2 ssh	

Student 127 (student127)

Host	Services	Actions
desktop1.student127.230.com	desktop1 ssh	