https://www.pexels.com/photo/art-notebook-mail-business-5706021/
Photo by Karolina Grabowska from Pexels

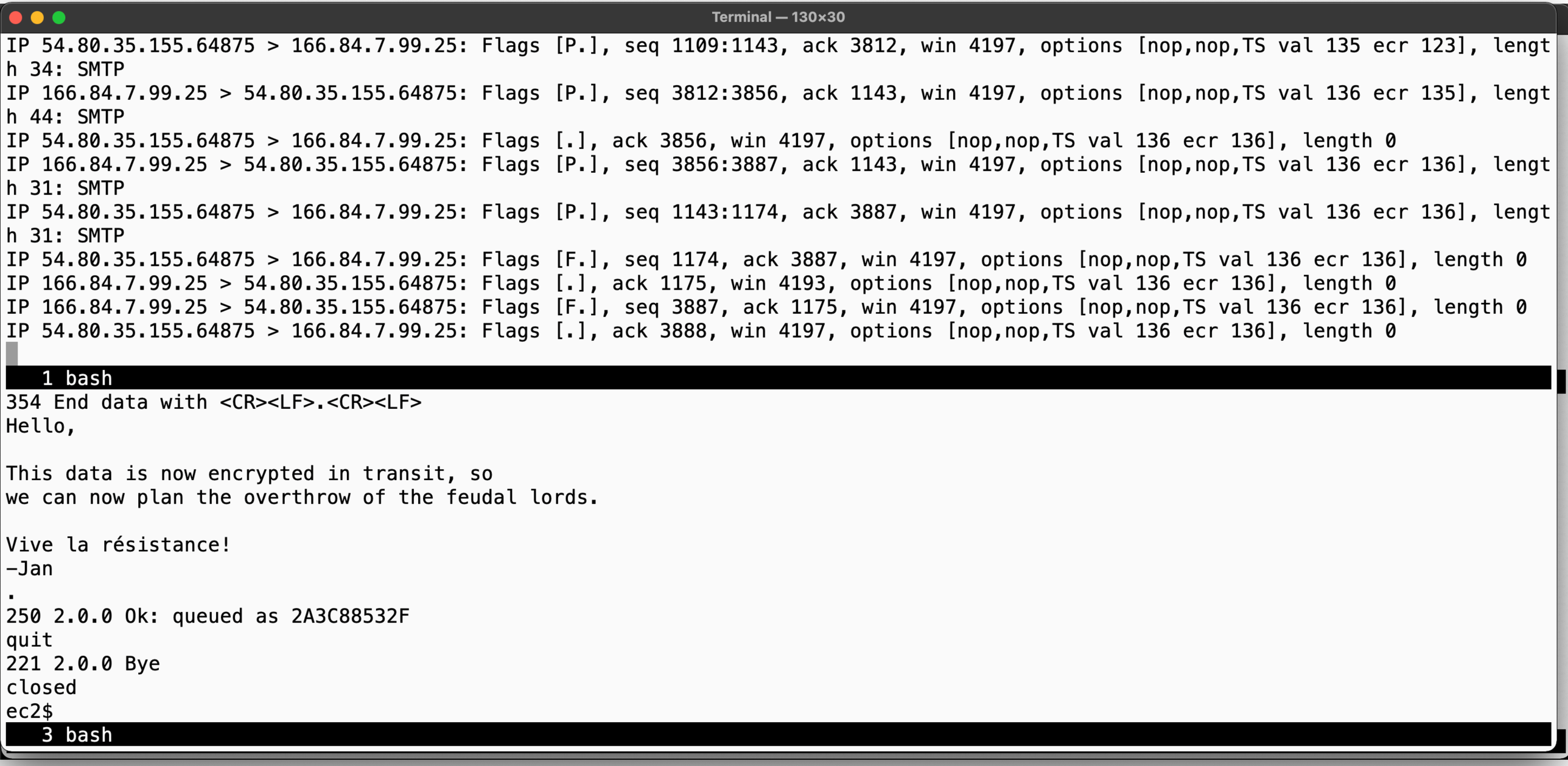
# System Administration

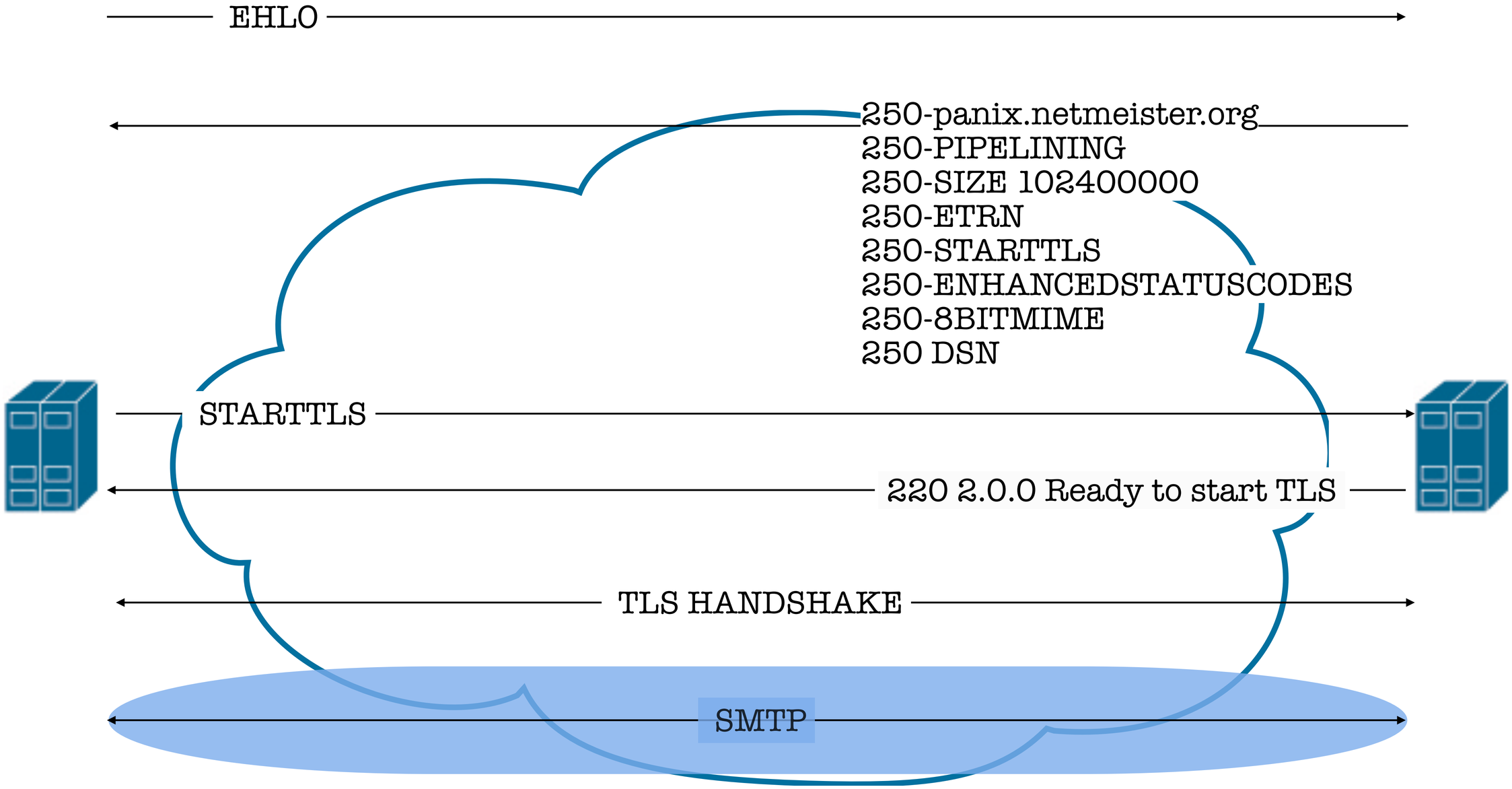
## Week 08, Segment 2
## E-mail, Part II

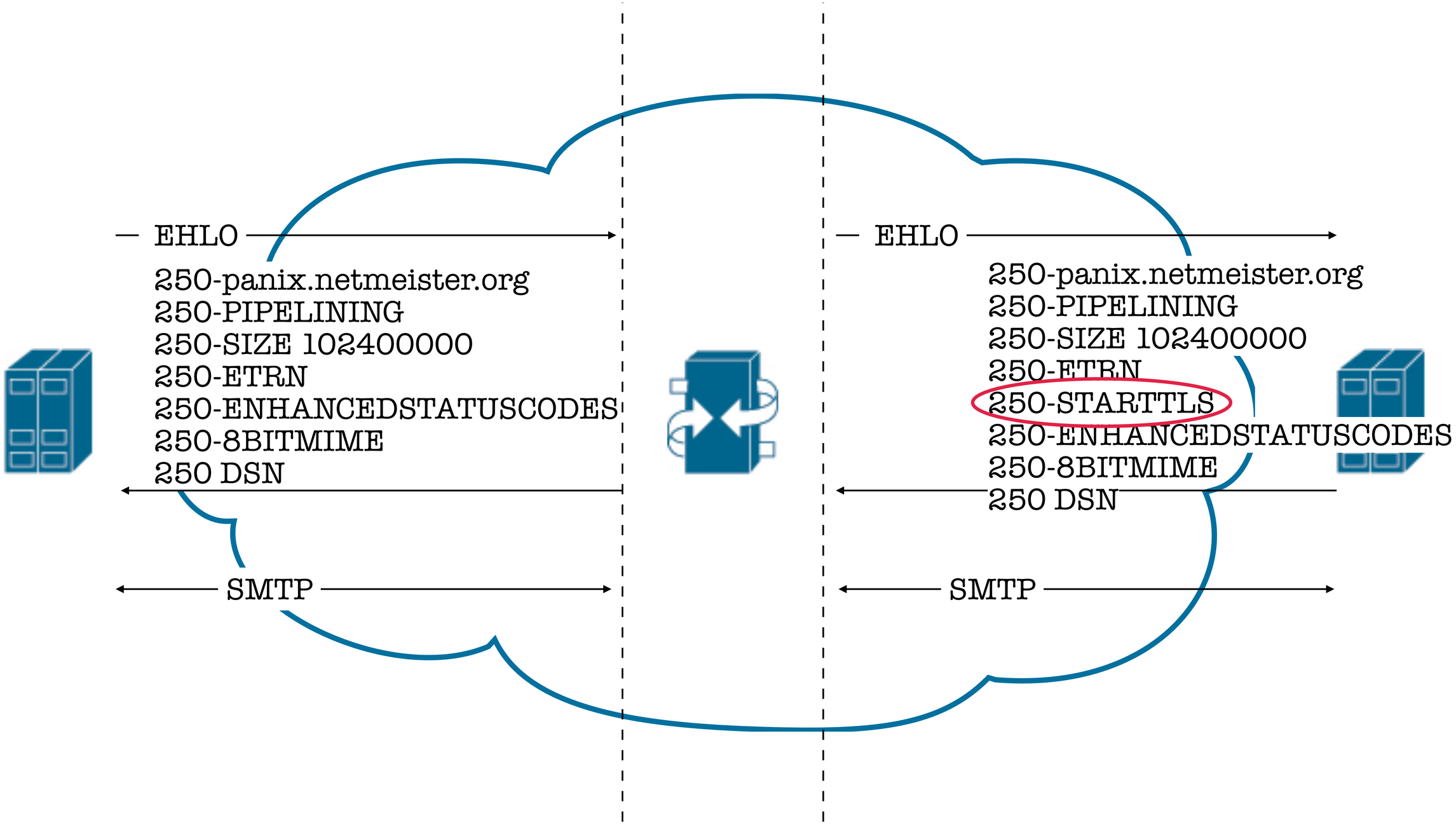

**Department of Computer Science**
**Stevens Institute of Technology**

**Jan Schaumann**
jschauma@stevens.edu
https://stevens.netmeister.org/615/


Terminal — 130×30
IP 166.84.7.99.32877 > 166.84.67.2.53: 24081+ [1au] TXT? _adsp._domainkey.cs615asa.netmeister.org. (69)
IP 166.84.67.2.53 > 166.84.7.99.32877: 24081 NXDomain 0/1/1 (143)
IP 166.84.7.99.32877 > 166.84.67.2.53: 55663+ [1au] MX? cs615asa.netmeister.org. (52)
IP 166.84.67.2.53 > 166.84.7.99.32877: 55663 0/1/1 (112)
IP 166.84.67.2.53 > 166.84.7.99.32877: 56828 NXDomain 0/1/1 (134)
IP 166.84.67.2.53 > 166.84.7.99.32877: 46246 NXDomain 0/1/1 (128)
IP 166.84.67.2.53 > 166.84.7.99.32877: 52923 NXDomain 0/0/1 (58)
IP 166.84.67.2.53 > 166.84.7.99.32877: 35992 NXDomain 0/0/1 (58)
1 bash
<mail.info>Mar 24 16:53:32 panix postfix/qmgr[4196]: 675C585316: removed
<mail.info>Mar 24 16:53:32 panix postfix/cleanup[3723]: 01F9B85A22: message-id=<20210324205200.F037B1CEAD@cs615asa.netmeister.org>
<mail.info>Mar 24 16:53:32 panix postfix/qmgr[4196]: 01F9B85A22: from=<jschauma@cs615asa.netmeister.org>, size=1014, nrcpt=1 (queue active)
<mail.info>Mar 24 16:53:32 panix postfix/local[22901]: 01F9B85A22: to=<jschauma@netmeister.org>, relay=local, delay=0.26, delays=0.04/0.04/0/0.18, dsn=2.0.0, status=sent (delivered to command: /usr/pkg/bin/procmail)
<mail.info>Mar 24 16:53:32 panix postfix/qmgr[4196]: 01F9B85A22: removed
<mail.info>Mar 24 16:55:08 panix postfix/smtpd[6310]: connect from unknown[111.75.149.221]
<mail.info>Mar 24 16:55:09 panix postfix/smtpd[6310]: disconnect from unknown[111.75.149.221] ehlo=1 auth=0/1 quit=1 commands=2/3
2 bash
Hello,
This is a plain text message, transmitted in the clear.
Nothing to see here.
-Jan
.
EOT
ec2$
3 bash


Terminal — 130×30
IP 54.80.35.155.64875 > 166.84.7.99.25: Flags [P.], seq 1109:1143, ack 3812, win 4197, options [nop,nop,TS val 135 ecr 123], length 34: SMTP
IP 166.84.7.99.25 > 54.80.35.155.64875: Flags [P.], seq 3812:3856, ack 1143, win 4197, options [nop,nop,TS val 136 ecr 135], length 44: SMTP
IP 54.80.35.155.64875 > 166.84.7.99.25: Flags [.], ack 3856, win 4197, options [nop,nop,TS val 136 ecr 136], length 0
IP 166.84.7.99.25 > 54.80.35.155.64875: Flags [P.], seq 3856:3887, ack 1143, win 4197, options [nop,nop,TS val 136 ecr 136], length 31: SMTP
IP 54.80.35.155.64875 > 166.84.7.99.25: Flags [P.], seq 1143:1174, ack 3887, win 4197, options [nop,nop,TS val 136 ecr 136], length 31: SMTP
IP 54.80.35.155.64875 > 166.84.7.99.25: Flags [F.], seq 1174, ack 3887, win 4197, options [nop,nop,TS val 136 ecr 136], length 0
IP 166.84.7.99.25 > 54.80.35.155.64875: Flags [.], ack 1175, win 4193, options [nop,nop,TS val 136 ecr 136], length 0
IP 166.84.7.99.25 > 54.80.35.155.64875: Flags [F.], seq 3887, ack 1175, win 4197, options [nop,nop,TS val 136 ecr 136], length 0
IP 54.80.35.155.64875 > 166.84.7.99.25: Flags [.], ack 3888, win 4197, options [nop,nop,TS val 136 ecr 136], length 0
1 bash
354 End data with <CR><LF>.<CR><LF>
Hello,
This data is now encrypted in transit, so
we can now plan the overthrow of the feudal lords.
Vive la résistance!
-Jan
.
250 2.0.0 Ok: queued as 2A3C88532F
quit
221 2.0.0 Bye
closed
ec2$
3 bash


EHLO
250-panix.netmeister.org
250-PIPELINING
250-SIZE 102400000
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
STARTTLS
220 2.0.0 Ready to start TLS
TLS HANDSHAKE
SMTP


EHLO
250-panix.netmeister.org
250-PIPELINING
250-SIZE 102400000
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
SMTP
EHLO
250-panix.netmeister.org
250-PIPELINING
250-SIZE 102400000
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
SMTP

```
SSL handshake has read 3429 bytes and written 481 bytes
Verification: OK
Verified peername: panix.netmeister.org
DANE TLSA 3 1 1 ...1c09946d116439a421bfbb7b matched EE certificate at depth 0
---
New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID: ADE1980C3BE3F5EC974D9751AB8E597589894D6DDE893E57BD3BDD04A698A9BB
    Session-ID-ctx:
    Master-Key: 160970EC3482F0E04843FBC4C7F9ED587502A87DFD334CA62E7F7C8D98B2CA39
BF2260CFBCFCD20F9F14AB51D0DFA4B5
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - 02 a7 2e 6e 6f 6a 5a 6b-23 76 33 e4 cd 0a d8 5e   ...nojZk#v3....^
```

## Summary

- `STARTTLS` may be used to add encryption in transit
- `STARTTLS` may be used to add authenticity guarantees to the client
- MitM can strip `STARTTLS`
  - SMTP MTA Strict Transport Security (MTA-STS) (RFC8461)
- MitM can present fraudulent certificate
  - DNS-Based Authentication of Named Entities (DANE) (RFC7672)

- Should failure to verify certificate lead to mail to being delivered?

# Links

- http://www.postfix.org/SMTPD_ACCESS_README.html
- https://tools.ietf.org/html/rfc8461
- https://en.wikipedia.org/wiki/Opportunistic_TLS
- https://www.netmeister.org/blog/dnssec-dane.html