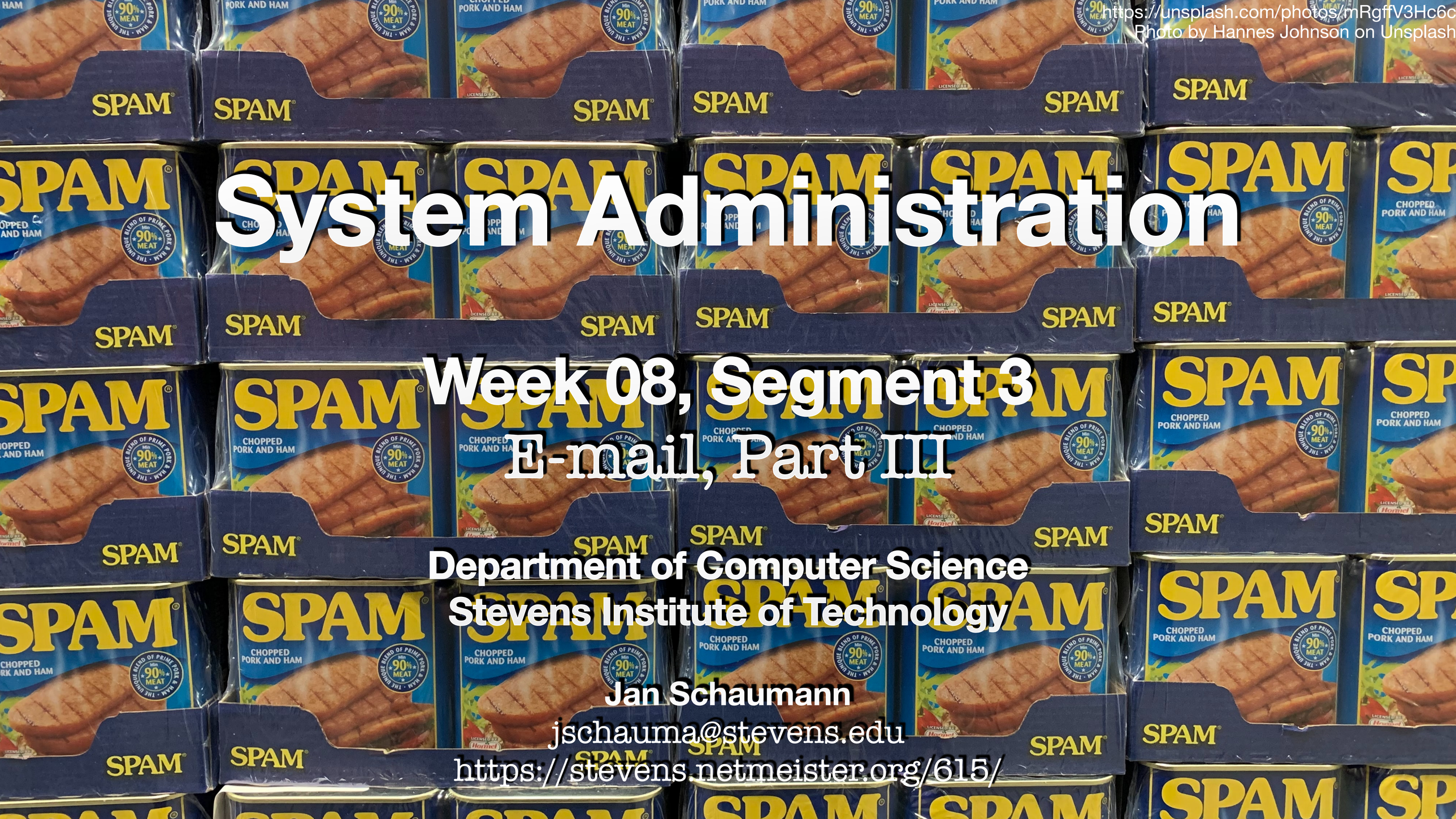


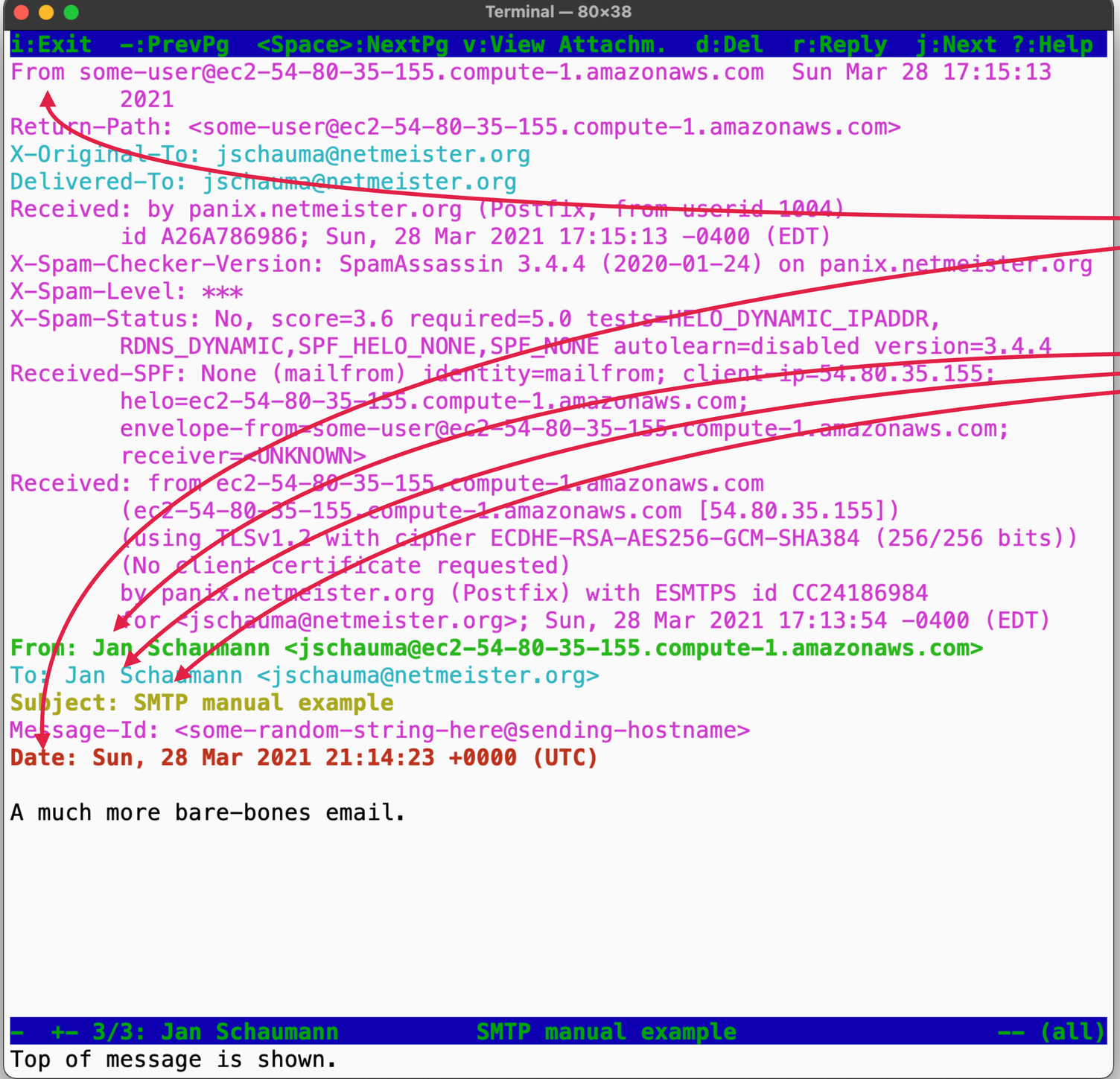
System Administration

Week 08, Segment 3

E-mail, Part III

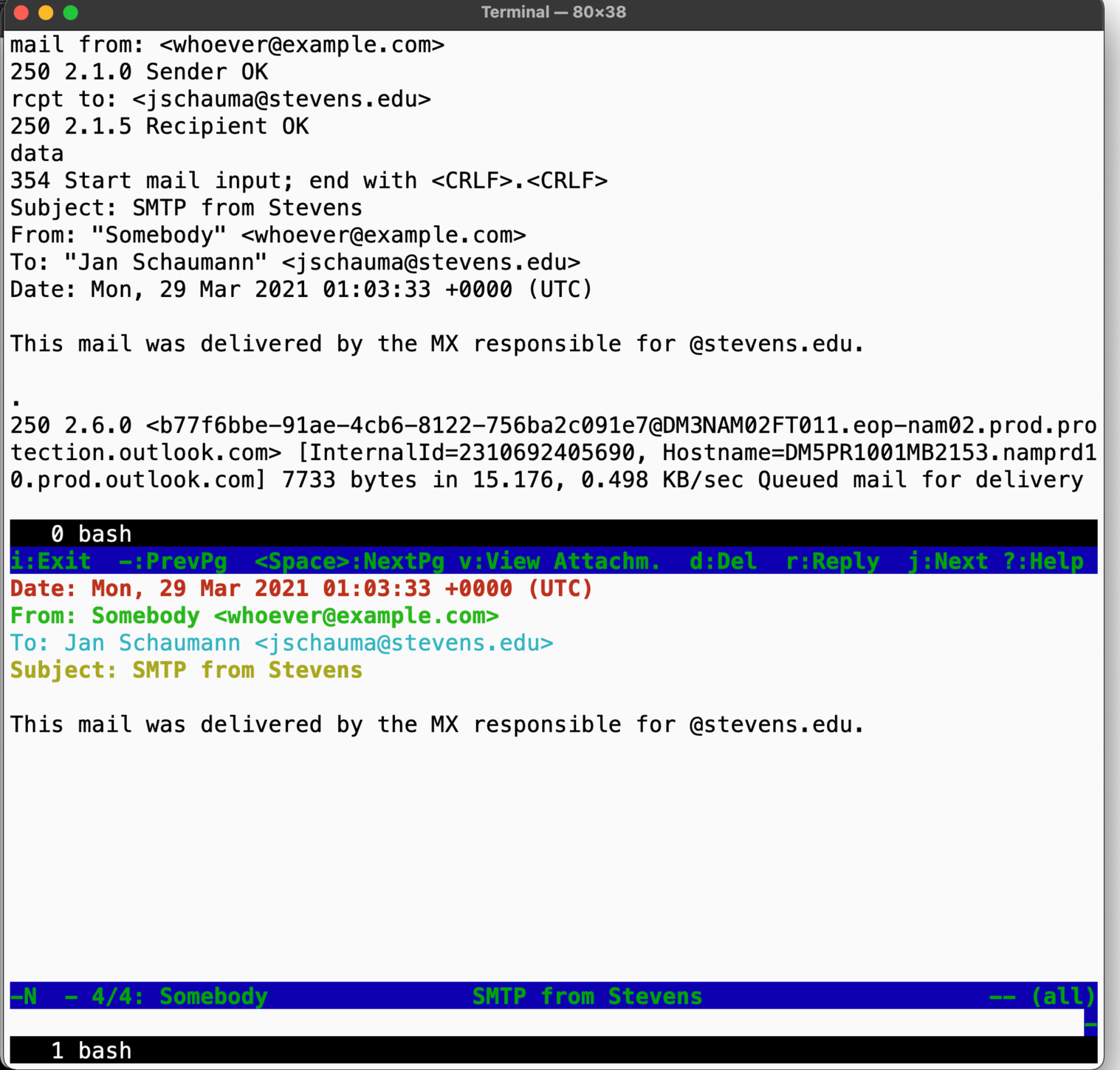
Department of Computer Science
Stevens Institute of Technology

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



An email consists of:

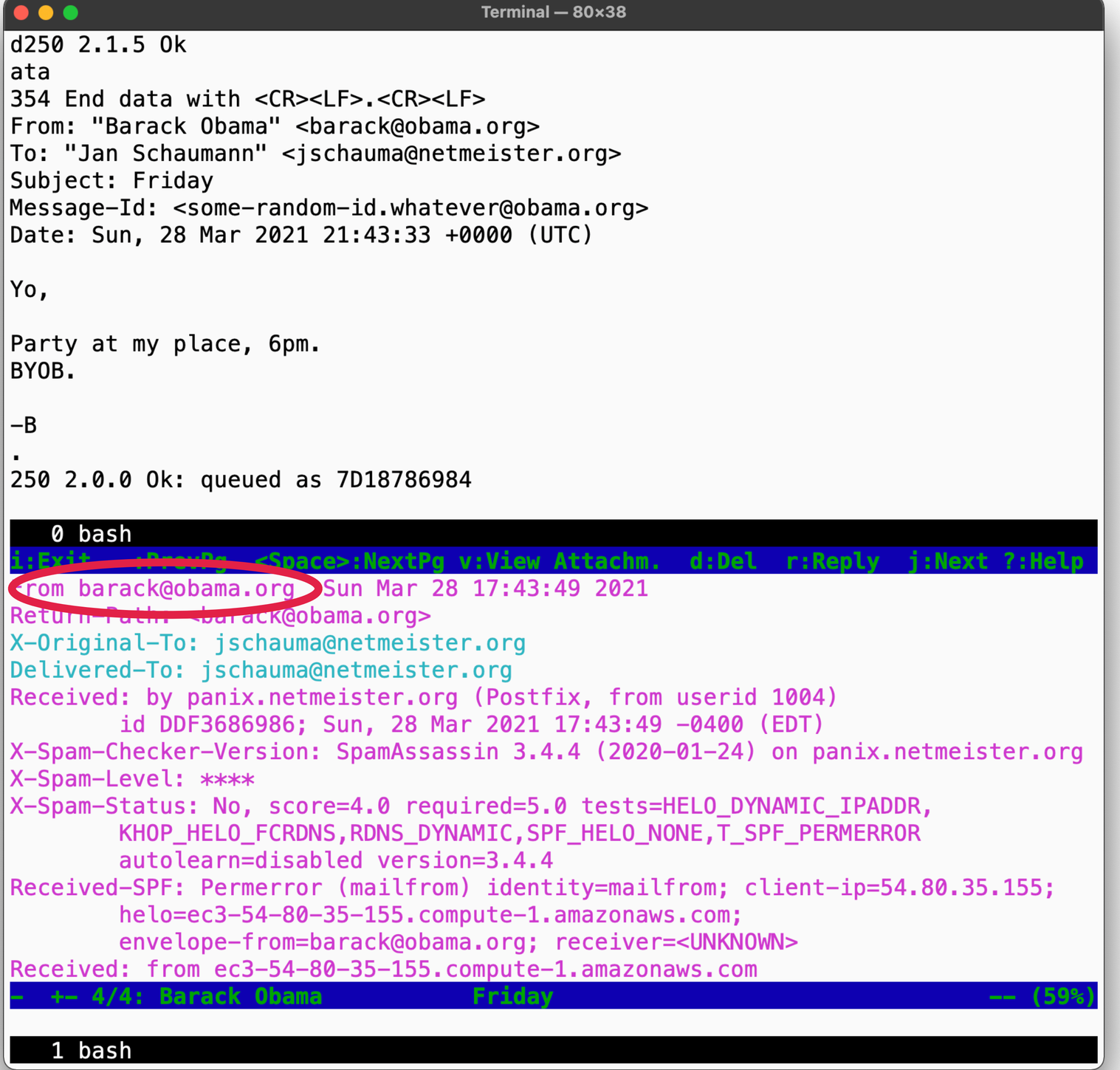
- mandatory headers
  - “From “, “Date: “
- optional headers
  - “From: “, “To: “, “Subject: “, …
- content of the message:
  - content independent of SMTP
  - Multipurpose Internet Mail Extensions (MIME) enables non-ascii, multipart, encodings, ...



Back in the old days, any SMTP MTA would accept and *relay* mail from anybody for anybody.

This lead to a lot of abuse; today, most mail servers only accept mail for domains they consider themselves responsible for.

There are a few so-called “open relays” still operating on the internet, but reputation-based Spam detection systems diminish their usefulness.



SMTP provides no authenticity guarantees whatsoever.

- “From “ can be set to anything
- “From: “ can be different from “From “

- The receiver can decide who it will accept (*relay*) mail for, but how can the receiver decide who should be allowed to *send* mail *from*?

Terminal — 80×38

```
Connected to panix.netmeister.org.
Escape character is '^]'.
220 panix.netmeister.org ESMTP Po
ehlo ec2-54-80-35-155.compute-1.a
250-panix.netmeister.org
250-PIPELINING
250-SIZE 102400000
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
mail from: <gates@microsoft.com>
250 2.1.0 Ok
rcpt to: <jschauma@netmeister.org>
550 5.7.23 <ec2-54-80-35-155.compute-1.amazonaws.com[54.80.35.155]>: Client host
 rejected: Message rejected due to: SPF fail - not authorized.

   0 bash
$ host -t txt _spf-a.microsoft.com | grep spf
_spf-a.microsoft.com descriptive text "v=spf1 ip4:216.99.5.67 ip4:216.99.5.68 ip
4:202.177.148.100 ip4:203.122.32.250 ip4:202.177.148.110 ip4:213.199.128.139 ip4
:213.199.128.145 ip4:207.46.50.72
.233.182 include:spf.protection.o
$ host -t txt netmeister.org | gr
netmeister.org descriptive text "
$ host -t txt gmail.com | grep sp
gmail.com descriptive text "v=spf
$ host -t txt _spf.gmail.com | gr
Host _spf.gmail.com not found: 3(
$ host -t txt _spf.google.com | g
_spf.google.com descriptive text "v=spf1 include:_netblocks.google.com include:_
netblocks2.google.com include:_netblocks3.google.com ~all"
$ host -t txt obama.org | grep spf
obama.org descriptive text "v=spf1 include:_spf.salesforce.com include:_spf.goog
le.com include:bounce.bluestatedigital.com include:sendgrid.net ~all"
$
   1 bash
```

SPF Hard Fail

```
Authentication-Results: spf=fail (sender IP is 54.80.35.155)
        smtp.mailfrom=microsoft.com; stevens.edu; dkim=none (message not
        signed)
        header.d=none;stevens.edu; dmarc=fail action=oreject
        header.from=microsoft.com;
Received-SPF: Fail (protection.outlook.com: domain of microsoft.com does not
        designate 54.80.35.155 as permitted sender)
        receiver=protection.outlook.com;
        client-ip=54.80.35.155; helo=localhost;
```

SPF Soft Fail

```
Authentication-Results: spf=softfail (sender IP is 54.80.35.155)
        smtp.mailfrom=obama.org; stevens.edu; dkim=none (message not signed)
        header.d=none;stevens.edu; dmarc=fail action=oreject
        header.from=obama.org;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
        obama.org discourages use of 54.80.35.155 as permitted sender)
```

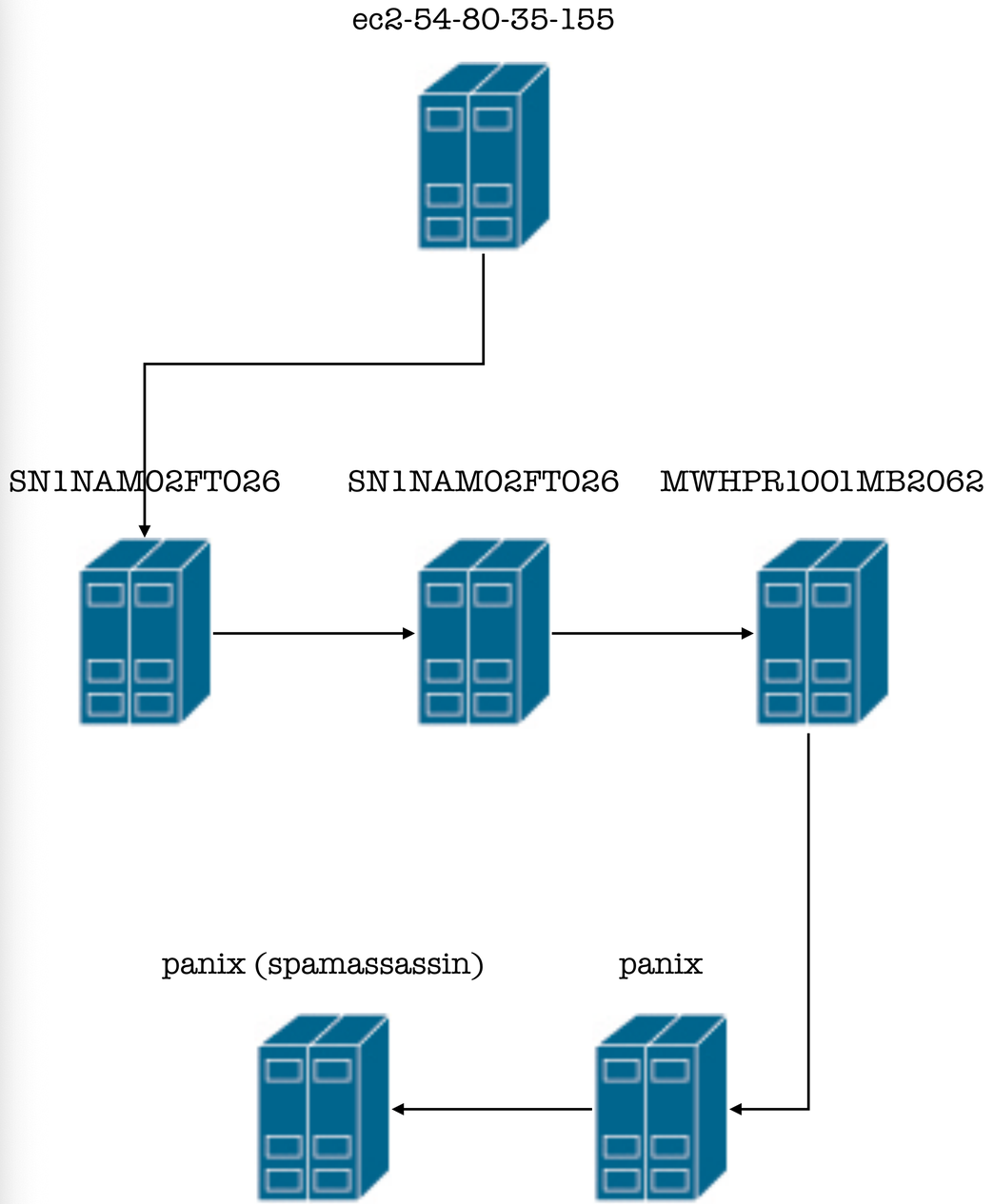
Terminal — 80×38

```
i:Exit  -:PrevPg  <Space>:NextPg v:View Attachm.  d:Del  r:Reply  j:Next ?:Help
Date: Mon, 29 Mar 2021 04:00:24 +0000 (UTC)
From: Jan Schaumann <jschauma@ec2-54-80-35-155.compute-1.amazonaws.com>
To: jschauma@stevens.edu
Subject: SMTP forwarding
Received: by panix.netmeister.org (Postfix, from userid 1004) id 5FBC286986;
        Mon, 29 Mar 2021 00:02:09 -0400 (EDT)
Received: from NAM11-BN8-obe.outbound.protection.outlook.com
        (mail-bn8nam11on2060b.outbound.protection.outlook.com
        [IPv6:2a01:111:f400:7eae::60b]) (using TLSv1.2 with cipher
        ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits)) (No client certificate
        requested) by panix.netmeister.org (Postfix) with ESMTPS id 4D24F86984
        for <jschauma@netmeister.org>; Mon, 29 Mar 2021 00:02:07 -0400 (EDT)
Received: from SN7PR04CA0026.namprd04.prod.outlook.com (2603:10b6:806:f2::31)
        by MWHPR1001MB2062.namprd10.prod.outlook.com (2603:10b6:301:2f::30)
        with Microsoft SMTP Server (version=TLS1_2,
        cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3977.29; Mon, 29
        Mar 2021 04:02:03 +0000
Received: from SN1NAM02FT026.eop-nam02.prod.protection.outlook.com
        (2603:10b6:806:f2:cafe::72) by SN7PR04CA0026.outlook.office365.com
        (2603:10b6:806:f2::31) with Microsoft SMTP Server (version=TLS1_2,
        cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3977.25 via
        Frontend Transport; Mon, 29 Mar 2021 04:02:03 +0000
Received: from ec2-54-80-35-155.compute-1.amazonaws.com (54.80.35.155) by
        SN1NAM02FT026.mail.protection.outlook.com (10.152.72.97) with Microsoft
        SMTP Server id 15.20.3977.25 via Frontend Transport; Mon, 29 Mar 2021
        04:02:03 +0000
Received: by ec2-54-80-35-155.compute-1.amazonaws.com (Postfix, from userid
        1002) id 58B7F1CEC6; Mon, 29 Mar 2021 04:00:24 +0000 (UTC)

This mail will be forwarded by Stevens to my personal mail server.




-   - 5/5: Jan Schaumann          SMTP forwarding                    -- (all)
```



ec2-54-80-35-155

From: Michelle Obama <michelle@obama.org>
To: Jan Schaumann <jschauma@netmeister.org>
Subject: Friday

Jan,

I'm afraid Barack has to cancel. He has other obligations that night.

Michelle

SPF Soft Fail

```
Authentication-Results: spf=softfail (sender IP is 54.80.35.155)
        smtp.mailfrom=obama.org; stevens.edu; dkim=none (message not signed)
        header.d=none;stevens.edu; dmarc=fail action=oreject
        header.from=obama.org;
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
        obama.org discourages use of 54.80.35.155 as permitted sender)
```

panix (spamassassin)

panix

From: Barack Obama <barack@obama.org>
To: Jan Schaumann <jschauma@netmeister.org>
Subject: Friday

Yo,

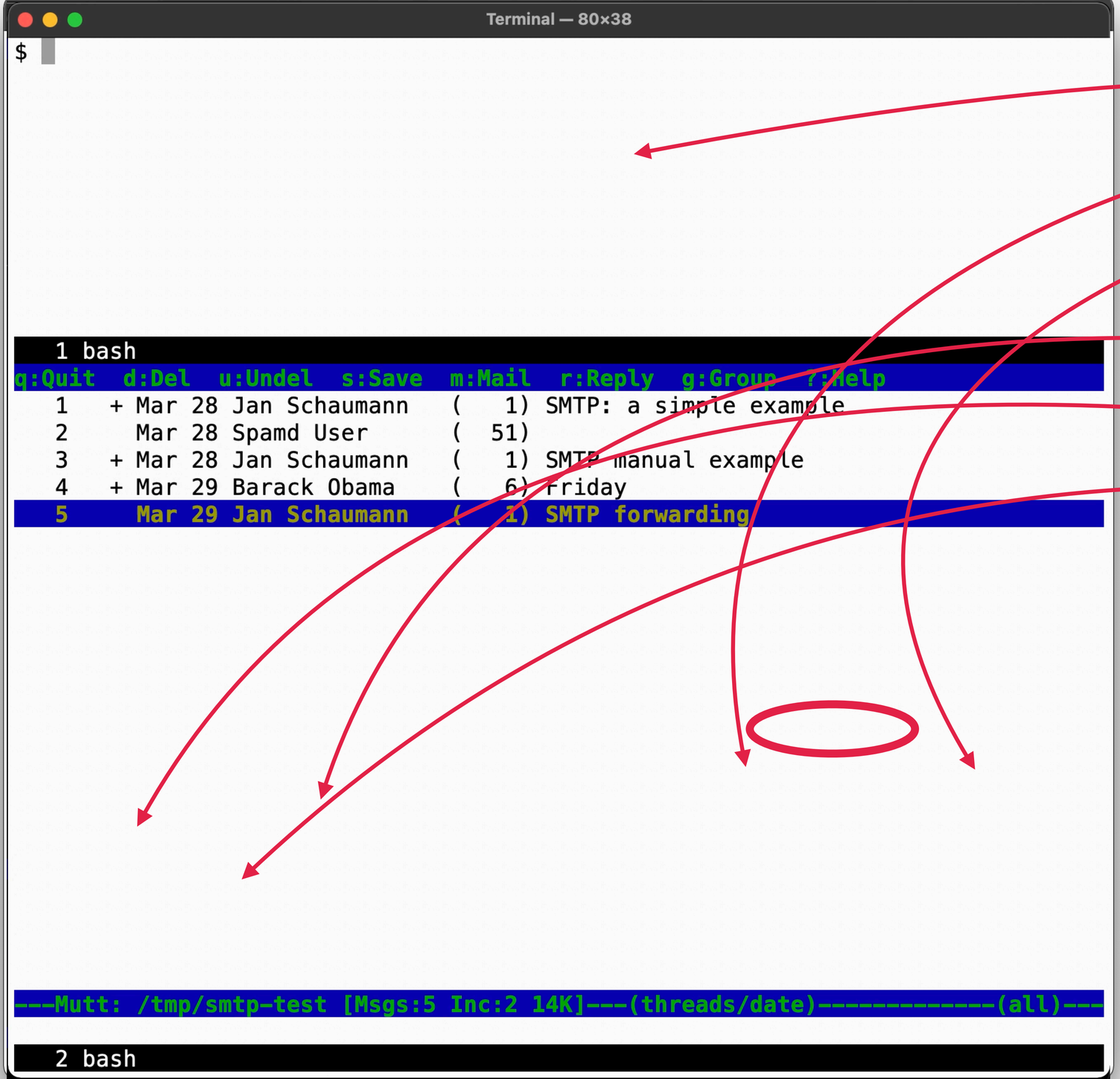
Party at my place, 6pm.
BYOB.

-B

DomainKeys Identified Mail aka DKIM

DKIM can help detect email spoofing by providing a *digital signature* across parts of the message.

- combines efforts by Yahoo ("enhanced DomainKeys”) and Cisco (“Identified Internet Mail”)
- original RFC4871, 2007; current RFC6376
- adds *DKIM-Signature* headers
- more DNS TXT records (<s>._domainkey.<domain>)



DKIM Signature includes:

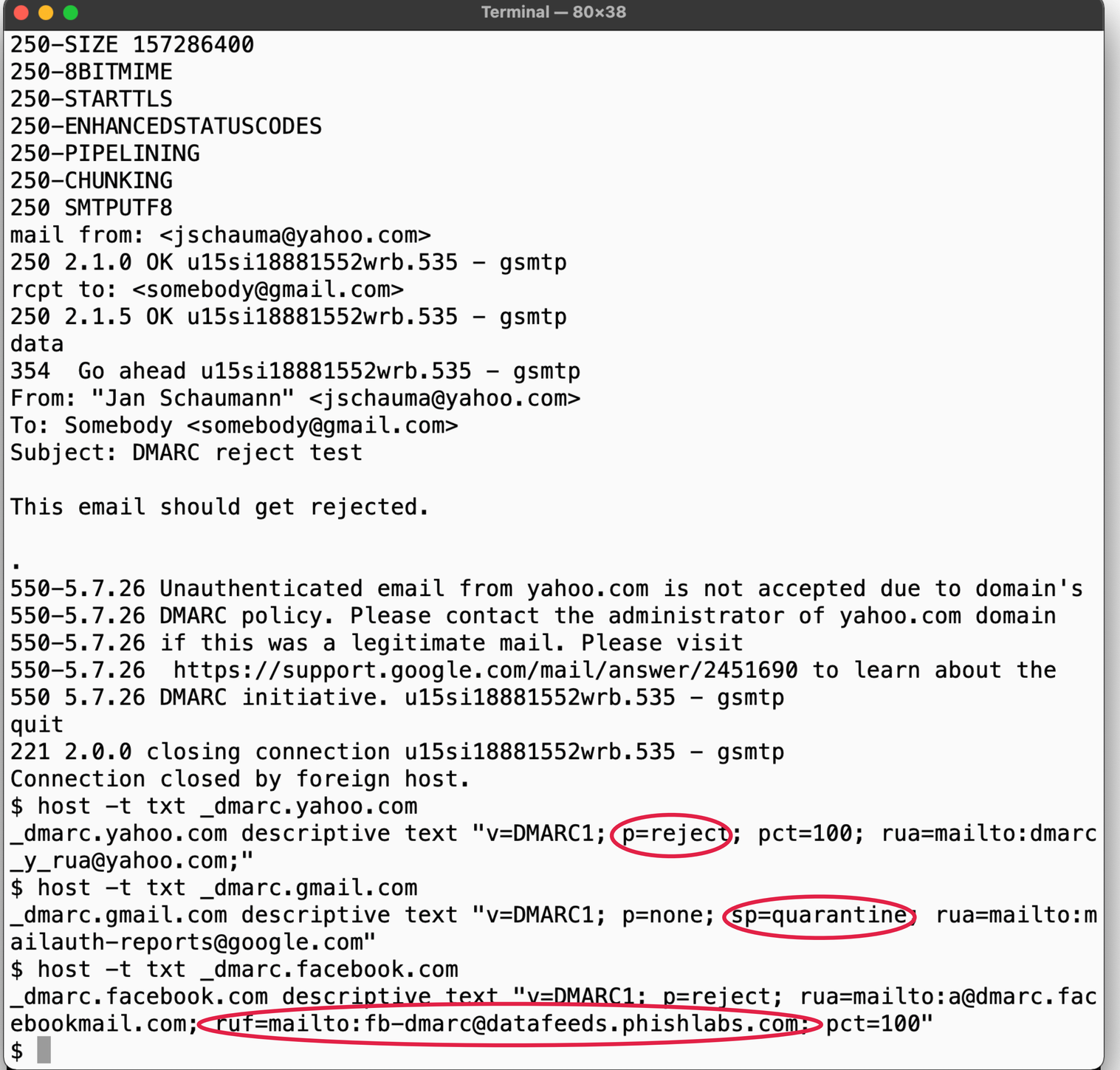
- the domain responsible (`d=...`)
- a “selector” to identify the correct public key (`s=...`)
- the hash of the email body (`bh=...`)
- the signed header fields (`h=...`)
- the actual signature data (`b=...`)

For validation, retrieve the correct public key via the DNS by combining the selector, the string “_domainkey”, and the domain.

Domain-based Message Authentication, Reporting and Conformance

DMARC (RFC7489) provides a policy of which validation mechanisms should be employed for a given domain.

- uses SPF and DKIM
- extends across “From “ and “From:” alignment
- provides report mechanism
- more DNS TXT records (`_dmarc.<domain>`)



- SPF checks that SMTP `MAIL FROM` is authorized; DMARC ensures *alignment* with “From:”
- DKIM allows parts of the message to be signed; DMARC allows the domain owner to specify what to do if e.g., the signature is wrong
- DMARC allows for aggregate reports of failed attempts

Summary

- SMTP headers:
  - some are mandatory, some optional
  - lack of some may be used as a signal of spamminess
  - each hop may add additional headers
- SPAM protections:
  - recipient restrictions (no open relays)
  - sender IP reputation (e.g., via DNS lookups in community databases)
  - Sender Policy Framework (SPF) specifies who is authorized to send mail on a domain's behalf
  - DomainKeys Identified Mail (DKIM) signs parts of the mail
  - DMARC lets responsible domain specify what recipients should do upon mismatches

E-Mail Service Implications

- spam protections
- phishing protections
- high volume traffic demands fine-tuned systems
- high volume traffic implications on logging
- mail delivery cannons for notifications vs. spam lists
- outsourcing versus in-house
- privacy considerations

Links

- Sender Policy Framework: http://www.open-spf.org/
- DomainKeys Identified Mail (DKIM): http://www.dkim.org/
- Domain-based Message Authentication, Reporting & Conformance: https://dmarc.org/
- https://en.wikipedia.org/wiki/Authenticated_Received_Chain
- https://www.m3aawg.org/sites/default/files/m3aawg-email-authentication-recommended-best-practices-09-2020.pdf
- https://postmaster.verizonmedia.com/faq