Arizona State University

CSE 469: Computer and Network Forensics

Topic 6: Email Forensics

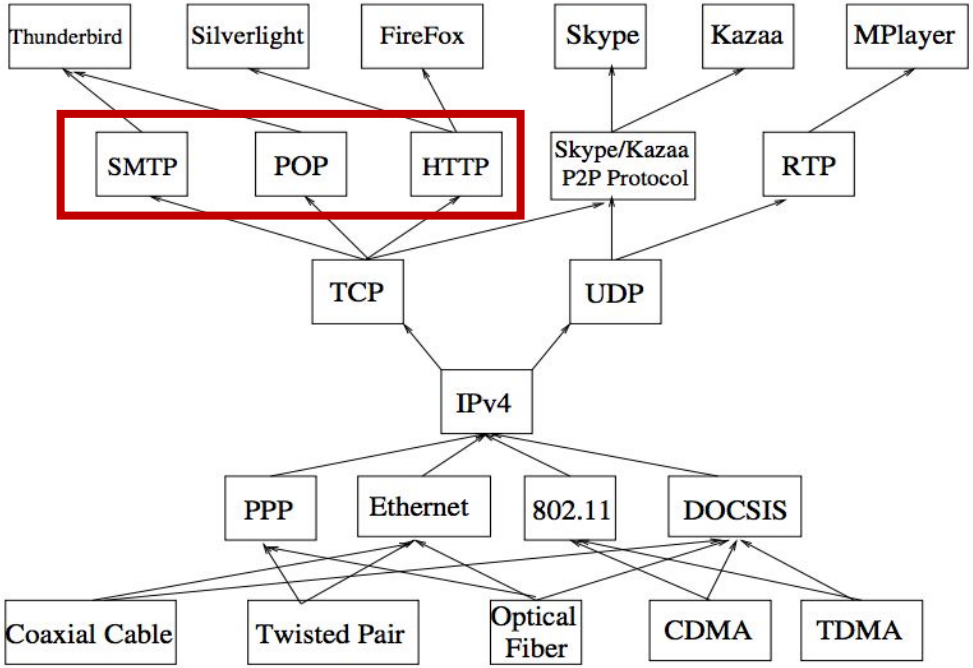
Dr. Mike Mabey | Spring 2019

Email System Components

- User agents / Webmail:
  - Composing, editing, and reading mail messages.
- Mail servers:
  - Send and receive email on user's behalf.
- Protocols:
  - SMTP: Simple mail transfer protocol.
  - POP3: Post Office Protocol.
  - IMAP4: Internet Message Access Protocol.

Application Layer Protocols

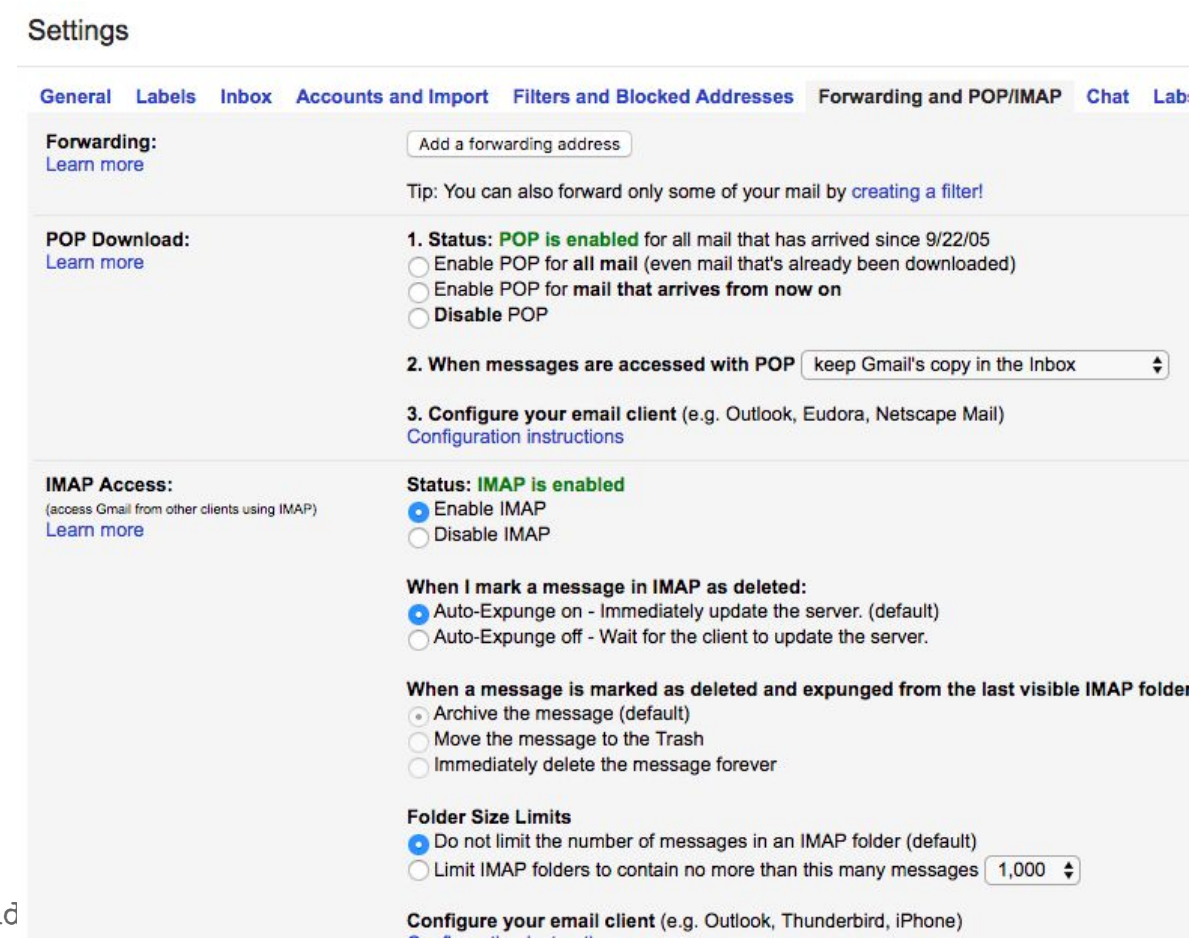
- SMTP: Simple mail transfer protocol, Port 25
- POP3: Post Office Protocol, Port 110
- IMAP4: Internet Message Access Protocol, Port 143



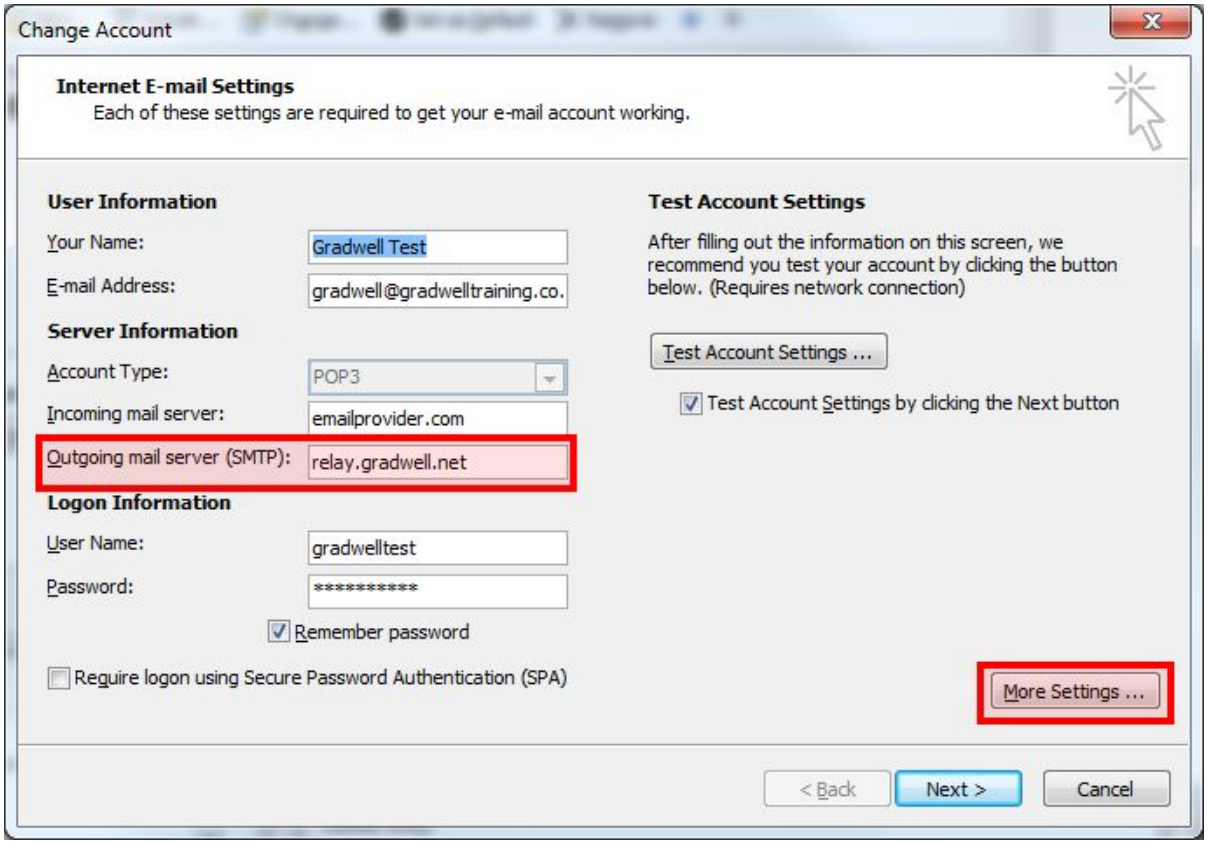
User Agents / Email Client

- Standalone application:
  - Use POP3 or IMAP4 to receive/download emails from a mail server.
  - Use SMTP to transmit outgoing emails to a mail server.

Configuring Email Clients (1)



Configuring Email Clients (2)



Email Client and Server Roles

- Email used in two environments:
  - Open (Internet).
  - Controlled (LAN, WAN).

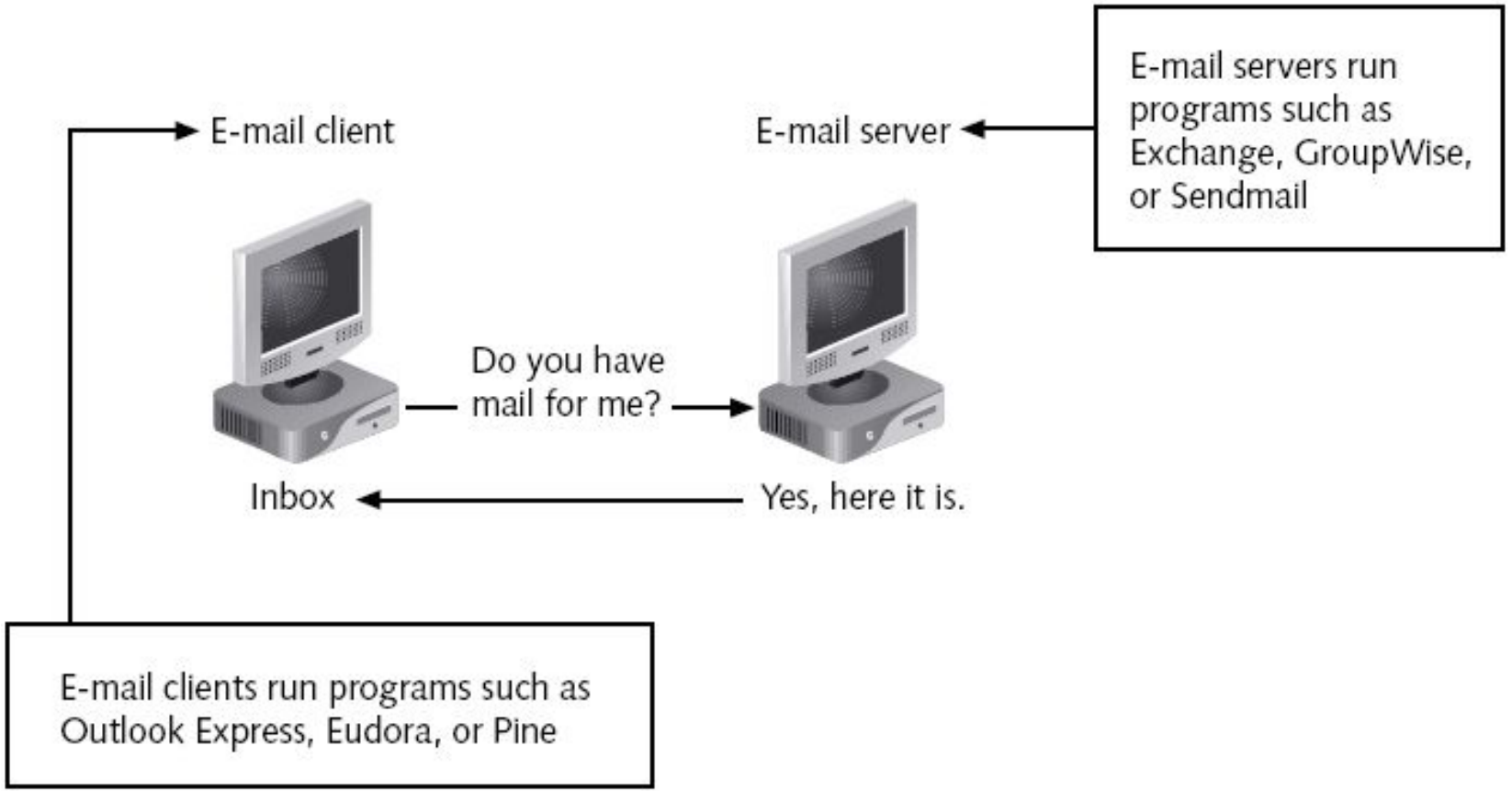
- Both use client-server architecture:
  - **Central server** distributes email…
  - To many **distributed clients**.

Email Client and Server Roles

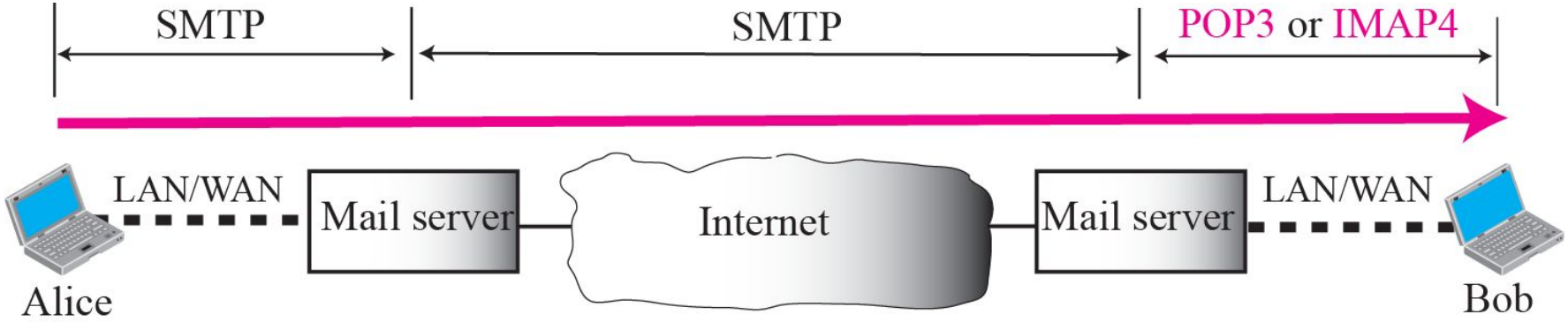
- Client's email software:
  - May be installed separately from OS:
    - Have their own directories and data files.
  - May use existing elements:
    - Browsers.

- Servers typically run specialized software.

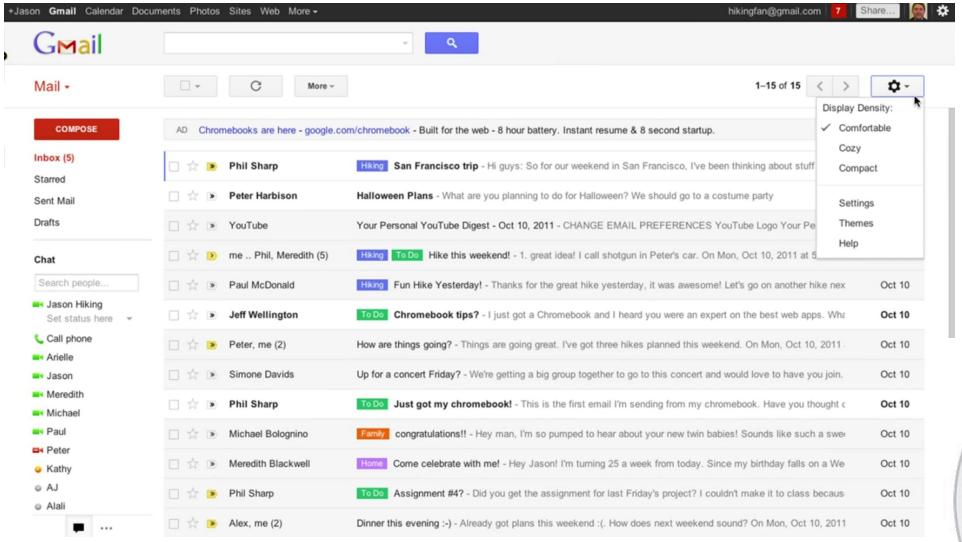
Email Client and Server Roles



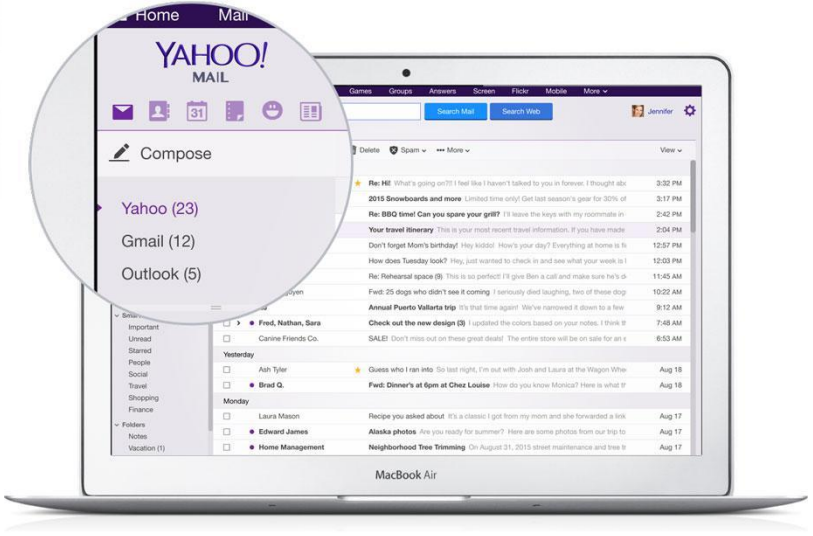
User Agents / Email Client



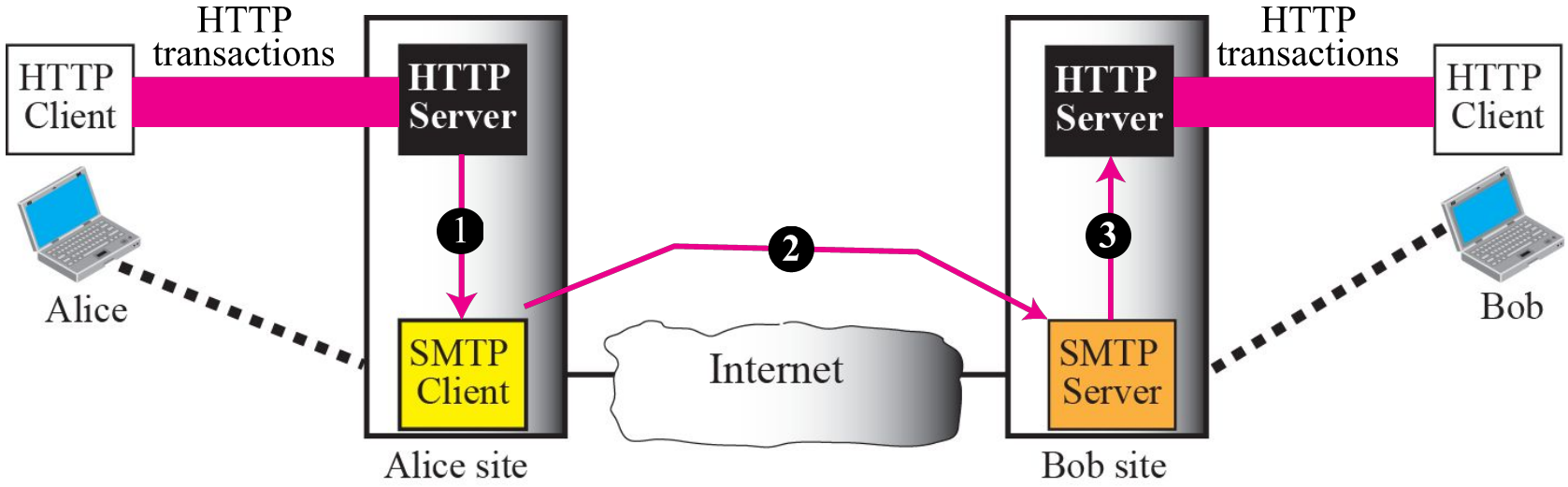
Webmail



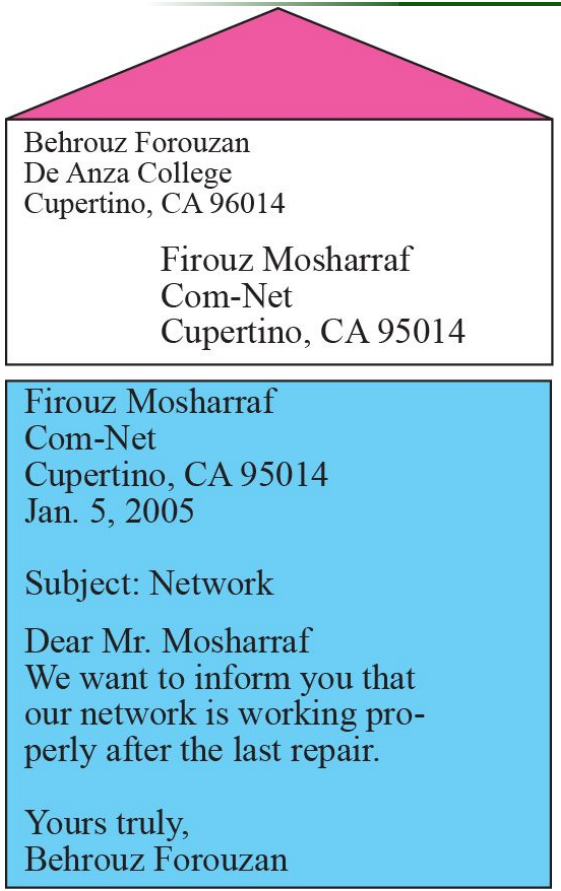
Visit using browser

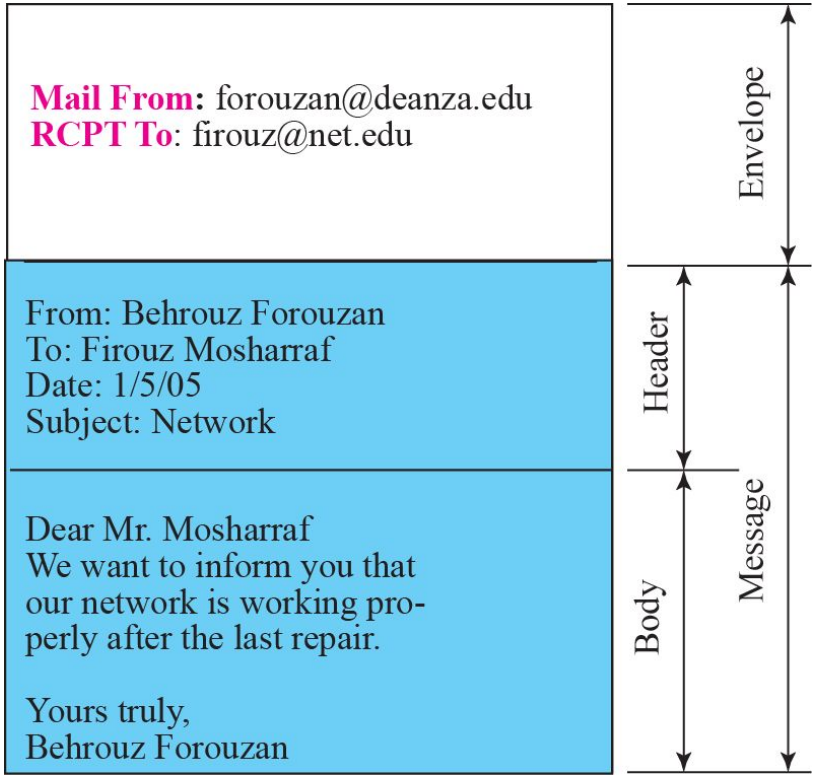


Webmail

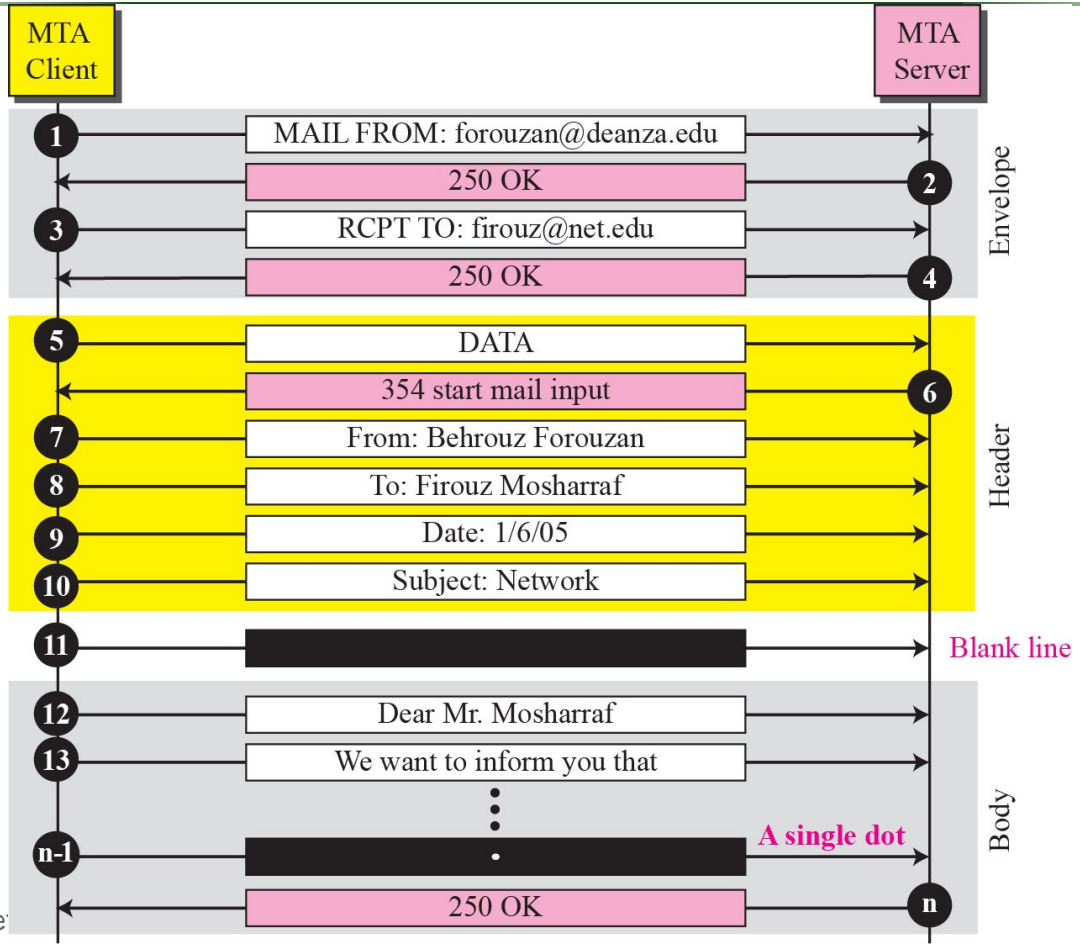

HTTP transactions
HTTP Client
HTTP Server
HTTP transactions
HTTP Client
HTTP Server
1
2
3
Alice
SMTP Client
Internet
SMTP Server
Bob
Alice site
Bob site

Format of Email





Transmission of Email (SMTP)



Corporate vs Public Email

- Tracing **corporate** emails is easier:
  - Standard names.
  - Assigned by local administrator.

- Contrast with **public** email:
  - Non-standard names.
  - Usually not informative.

Identifying Email Crimes/Violations

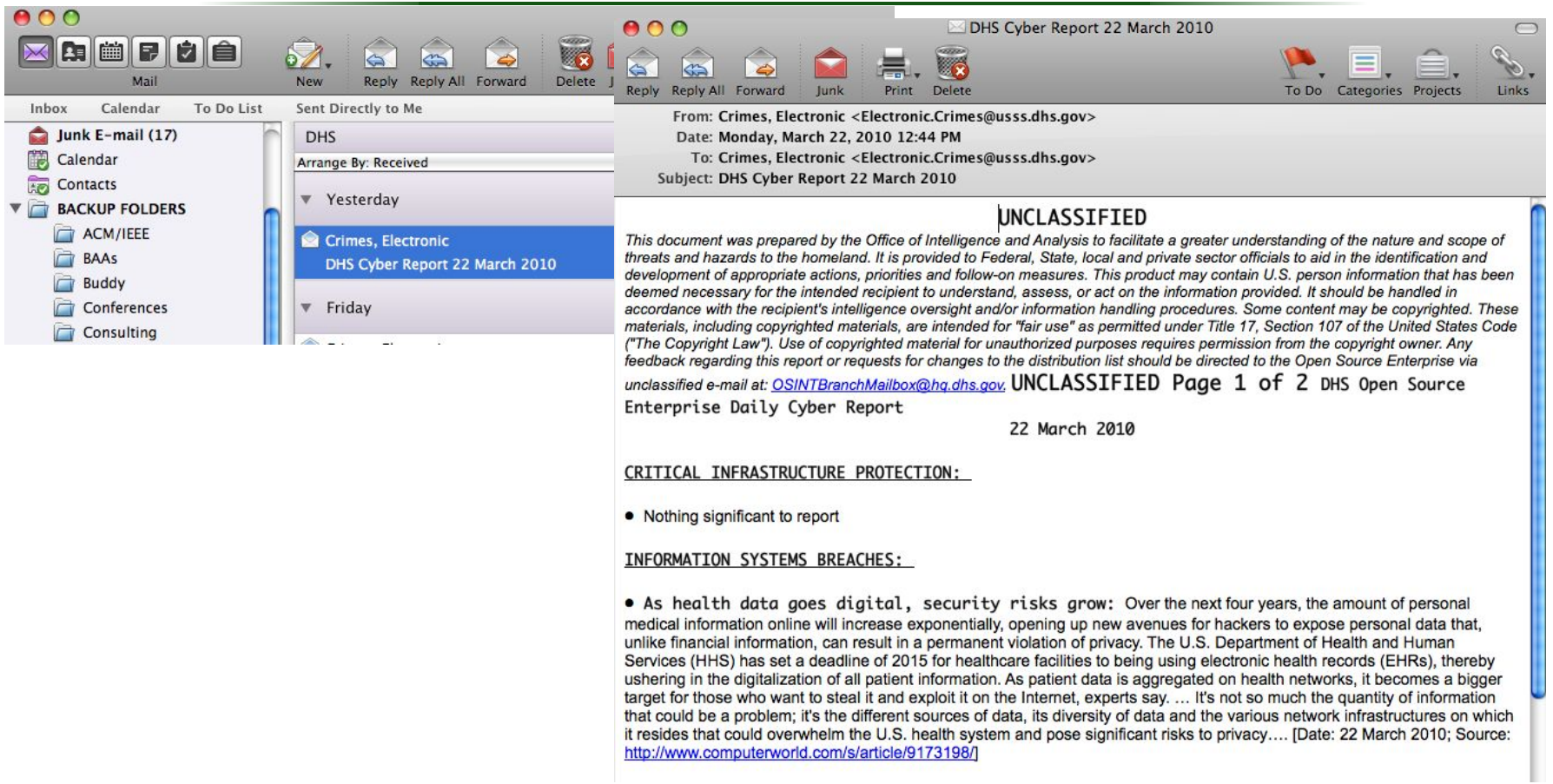
- "Crime" may depend on jurisdiction:
  - Spam:
    - Illegal in Washington state
    - Elsewhere?
- Email crime is becoming commonplace:
  - Narcotics trafficking
  - Sexual harassment
  - Child pornography
  - Fraud
  - Terrorism

Examining Email Messages

- Access the victim's computer and retrieve evidence.

- Use the victim's email client:
  - Find and copy evidence in the email.
  - Access protected or encrypted material.
  - Carve emails:
    - Including header.
    - Why?

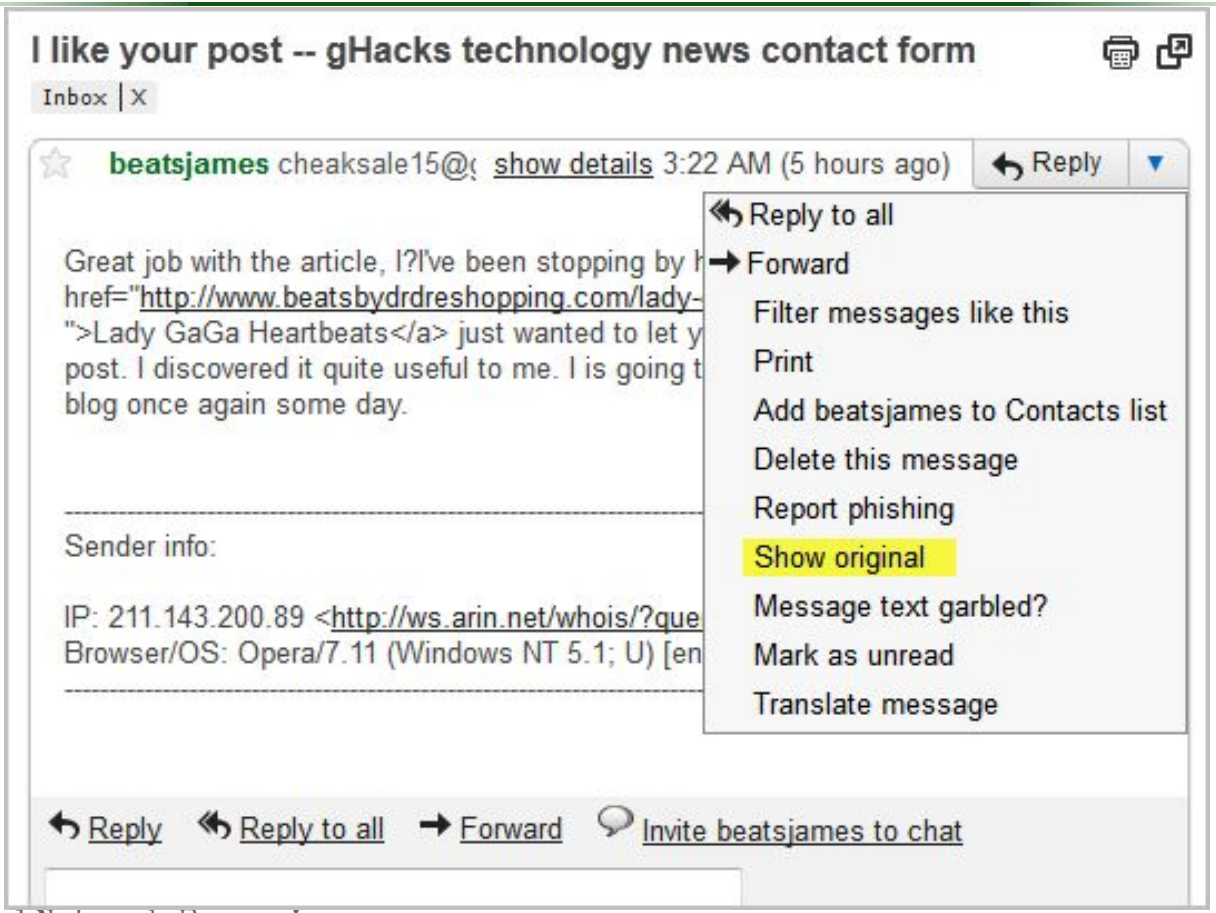
Examining Email Messages



Viewing Email Headers

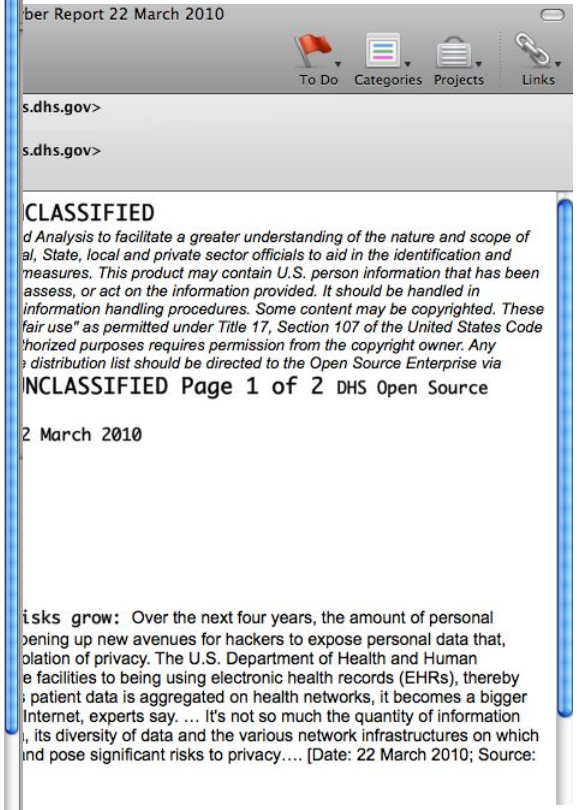
- Learn how to find email headers:
  - GUI clients.
  - Command-line clients.
  - Web-based clients.
- Headers contain useful information.

Viewing Email Headers



Viewing Email Headers

```
Received: from 70.190.237.75 ([70.190.237.75]) by EX11.asurite.ad.asu.edu
([129.219.103.21]) via Exchange Front-End Server exchange.asu.edu ([129.219.103.52]) with
Microsoft Exchange Server HTTP-DAV ;
 Tue, 23 Mar 2010 00:43:50 +0000
Received:  from post2.inre.asu.edu (129.219.19.179) by exhub.asu.edu (129.219.103.58) with
Microsoft SMTP Server (TLS) id 8.1.375.2; Mon, 22 Mar 2010 12:48:13 -0700
MIME-Version: 1.0
Received:  from bcnet1.asu.edu (bcnet1-inside [10.0.5.31]) by post2.inre.asu.edu
(Switch-3.3.0/Switch-3.1.7/asu-postoffice-prod) with ESMTP id o2MJmDa3006803 for
<gahn@asu.edu>; Mon, 22 Mar 2010 12:48:13 -0700
Content-Type: text/html;
 charset="Windows-1252"
Content-Transfer-Encoding: quoted-printable
Received:  from mta1.dhs.gov (localhost [127.0.0.1]) by bcnet1.asu.edu (Spam & Virus
Firewall) with ESMTP id 997861A75F3D for <gahn@asu.edu>; Mon, 22 Mar 2010 12:48:11 -0700
(MST)
X-MimeOLE: Produced By Microsoft Exchange V8.1
Received:  from mta1.dhs.gov (mta1.dhs.gov [152.121.181.36]) by bcnet1.asu.edu with ESMTP
id VfCVX5E9OODP8QGy for <gahn@asu.edu>; Mon, 22 Mar 2010 12:48:11 -0700 (MST)
Received:  from dhsmail2.dhs.gov (dhsmail2.dhs.gov [161.214.63.27]) by mta1.dhs.gov with
ESMTP for gahn@asu.edu; Mon, 22 Mar 2010 15:48:11 -0400
Received:  from dhsmail2.dhs.gov (localhost.localdomain [127.0.0.1]) by localhost (Postfix)
with SMTP id 790C2859823D for <gahn@asu.edu>; Mon, 22 Mar 2010 15:48:11 -0400 (EDT)
Received:  from IA-Proxy-Blade1.usss.dhs.gov (IA-Proxy-Blade1.usss.dhs.gov
[161.214.104.6]) by dhsmail2.dhs.gov (Postfix) with SMTP id C0E4E8598236 for
<gahn@asu.edu>; Mon, 22 Mar 2010 15:48:10 -0400 (EDT)
Received:  from (unknown [10.200.70.12]) by IA-Proxy-Blade1.usss.dhs.gov with smtp  id
31f9_0edf_d0b646a8_35eb_11df_af8b_001f29c6c9fc; Mon, 22 Mar 2010 15:47:57 -0400
Received:  from 45prod21-ssnet.SSNET.USSS.DHS.GOV (45prod21-ssnet.ssnet.usss.dhs.gov
[10.200.70.21]) by barracuda12.usss.dhs.gov (Spam & Virus Firewall) with ESMTP id
DA38963DB88; Mon, 22 Mar 2010 15:43:15 -0400 (EDT)
Received:  from 45prod21-ssnet.SSNET.USSS.DHS.GOV (45prod21-ssnet.ssnet.usss.dhs.gov
[10.200.70.21]) by barracuda12.usss.dhs.gov with ESMTP id XKHZ5gMT3RpdmXKe; Mon, 22 Mar
2010 15:43:15 -0400 (EDT)
Received:  from 40WAS54-SSNET ([10.130.200.131]) by 45prod21-ssnet.SSNET.USSS.DHS.GOV with
Microsoft SMTPSVC(6.0.3790.3959); Mon, 22 Mar 2010 15:44:08 -0400
x-ms-exchange-organization-authas: Anonymous
x-ms-exchange-organization-authsource: exhub2.asurite.ad.asu.edu
x-originalarrivaltime: 22 Mar 2010 19:44:08.0408 (UTC) FILETIME=[09A0B580:01CAC9F8]
x-barracuda-start-time: 1269287292
x-barracuda-connect: mta1.dhs.gov[152.121.181.36]
x-asg-debug-id: 1269287291-771500d20000-9h9pOT
x-barracuda-spam-status: No, SCORE=1.05 using global scores of TAG_LEVEL=1000.0
QUARANTINE_LEVEL=1000.0 KILL_LEVEL=5.5 tests=HTML_MESSAGE, HTML_MIME_NO_HTML_TAG,
MIME_HTML_ONLY
x-barracuda-virus-scanned: by ASU Barracuda1 at asu.edu
x-barracuda-spam-score: 1.05
x-asg-orig-subj: DHS Cyber Report 22 March 2010
x-barracuda-spam-report: Code version 3.2, rules version 3.2.2.25569 Rule breakdown below
```



Email Headers

- **From**: Who the message is from. This is the easiest to forge, and thus the least reliable.
- **Reply-To**: The address to which replies should be sent. Often absent from the message, and very easily forgeable.
- **Return-Path**: The email address for return mail. Same as Reply-To:
- **Message-ID**: A unique string assigned by the mail system when the message is first created. The format of a Message-ID: field is <uniquestring>@<sitename>
- **Received**: They form a list of all sites (MTA) through which the message traveled in order to reach you.

Examining Email Headers

- Gather supporting evidence and track suspect:
  - Return path.
  - Recipient's email address.
  - Type of sending email service.
  - IP address of sending server.
  - Name of the email server.
  - Unique message number.
  - Date and time email was sent.
  - Attachment files information.

Email Header

- **Received**: from **string** (**hostname** [**host IP address**])
  by **recipient host**
  with **protocol** id **message ID**
  for **recipient**;
  timestamp

- **Received**: from **cidse.asu.edu** (**cidse.asu.edu** [**201.12.16.3**])
  by **gateway.asu.edu** (8.11.6/8.11.6)
  with **ESMTP** id **j21IBV720506**
  for **<ABC@asu.edu>**;
  Mon, 20 Feb 2019 10:11:31 -0700

Examining Additional Email Files

- Email messages are saved on the client side or left at the server:
  - Microsoft Outlook .pst and .ost files
  - .pst – Sent, received, deleted, draft
  - .ost – Offline files

- Personal address book also has valuable information.

Tracing an Email Message

- Preliminary Steps:
  - Examine each field in the email header, especially the recorded IP address of sender.
  - Content analysis on suspicious email(s):
    - Determine if crime/violation of policy has been committed.
  - Investigate attachments.
- Verification and validation
  - Email route - may include clues about sender's origin, location, methods.
  - Analyze domain name's point of contact.
  - Aggregate suspect's contact information.
  - Acquire attributes against network logs.

Using Network Email Logs

```
11:43:35 DROP UDP 192.168.1.106 239.255.255.250 1900 1900 424 - - - - - - - -
11:43:35 DROP UDP 192.168.1.104 239.255.255.250 1900 1900 430 - - - - - - - -
11:43:35 DROP UDP 192.168.1.106 239.255.255.250 1900 1900 385 - - - - - - - -
11:43:35 DROP UDP 192.168.1.106 239.255.255.250 1900 1900 430 - - - - - - - -
11:43:35 DROP UDP 192.168.1.104 239.255.255.250 1900 1900 448 - - - - - - - -
11:43:35 DROP UDP 192.168.1.106 239.255.255.250 1900 1900 448 - - - - - - - -
11:43:35 DROP UDP 192.168.1.104 239.255.255.250 1900 1900 385 - - - - - - - -
11:43:35 DROP UDP 192.168.1.106 239.255.255.250 1900 1900 385 - - - - - - - -
11:43:35 DROP UDP 192.168.1.104 239.255.255.250 1900 1900 376 - - - - - - - -
11:43:35 DROP UDP 192.168.1.106 239.255.255.250 1900 1900 376 - - - - - - - -
11:43:38 DROP TCP 207.46.248.249 192.168.1.104 80 3218 40 R 4247099263 2102237511 0 -
11:43:40 OPEN UDP 192.168.1.104 204.127.202.19 1026 53 - - - - - - - - -
11:43:40 OPEN TCP 192.168.1.104 206.16.6.252 3221 80 - - - - - - - - -
11:43:41 OPEN TCP 192.168.1.104 206.16.0.136 3222 80 - - - - - - - - -
11:43:41 OPEN TCP 192.168.1.104 206.16.0.45 3223 80 - - - - - - - - -
11:43:41 OPEN TCP 192.168.1.104 206.16.0.45 3224 80 - - - - - - - - -
11:43:41 OPEN TCP 192.168.1.104 209.249.123.229 3225 80 - - - - - - - - -
11:43:41 OPEN TCP 192.168.1.104 209.249.123.229 3226 80
11:43:42 OPEN TCP 192.168.1.104 216.239.39.102 3227 80
11:43:43 OPEN TCP 192.168.1.104 209.249.123.229 3228 80
11:43:43 OPEN TCP 192.168.1.104 209.249.123.229 3229 80
11:43:43 OPEN TCP 192.168.1.104 206.16.0.45 3230 80 -
11:43:43 OPEN TCP 192.168.1.104 206.16.0.45 3231 80 -
11:43:43 OPEN TCP 192.168.1.104 206.16.0.45 3232 80 -
11:43:43 OPEN TCP 192.168.1.104 206.16.0.45 3233 80 -
11:43:43 OPEN TCP 192.168.1.104 206.16.0.147 3234 80 -
11:43:43 OPEN TCP 192.168.1.104 206.16.0.147 3235 80 -
11:43:43 OPEN TCP 192.168.1.104 206.16.0.45 3236 80 -
11:43:43 OPEN TCP 192.168.1.104 206.16.0.45 3237 80 -
11:43:43 OPEN TCP 192.168.1.104 206.16.0.45 3238 80 -
11:43:43 OPEN TCP 192.168.1.104 206.16.0.45 3239 80 -
11:43:43 OPEN TCP 192.168.1.104 206.16.0.147 3240 80 -
11:43:43 OPEN TCP 192.168.1.104 206.16.0.45 3241 80 -
11:43:43 OPEN TCP 192.168.1.104 206.16.0.45 3242 80 -
11:43:43 OPEN TCP 192.168.1.104 206.16.0.45 3243 80 -
```

L...	Destination IP	Destination Port	Protocol	Action	Rule	Client IP	Client Username
7/24/...	209.217.36.3	110	POP3	Initiated...	SMTP/POP3/DNS	10.0.0.5	ISALOCAL\tshinder
7/24/...	10.0.0.1	1745	Unidentified IP Tra...	Initiated...		10.0.0.5	
7/24/...	209.217.36.3	110	POP3	Initiated...	SMTP/POP3/DNS	10.0.0.5	ISALOCAL\tshinder
7/24/...	209.217.36.3	110	POP3	Closed ...	SMTP/POP3/DNS	10.0.0.5	ISALOCAL\tshinder
7/24/...	192.168.1.255	138	NetBios Datagram	Denied ...	Default rule	192.168.1.34	
7/24/...	192.168.1.255	138	NetBios Datagram	Denied ...	Default rule	192.168.1.8	
7/24/...	192.168.1.255	138	NetBios Datagram	Denied ...	Default rule	192.168.1.23	
7/24/...	192.168.1.102	25	SMTP	Initiated...	SMTP/POP3/DNS	10.0.0.5	ISALOCAL\tshinder
7/24/...	192.168.1.255	137	NetBios Name Ser...	Denied ...	Default rule	192.168.1.101	
7/24/...	209.217.36.3	110	POP3	Closed ...	SMTP/POP3/DNS	10.0.0.5	ISALOCAL\tshinder
7/24/...	192.168.1.102	25	SMTP	Closed ...	SMTP/POP3/DNS	10.0.0.5	ISALOCAL\tshinder
7/24/...	10.0.0.1	1227	Unidentified IP Tra...	Denied ...		10.0.0.5	
7/24/...	209.217.36.3	110	POP3	Initiated...	SMTP/POP3/DNS	10.0.0.5	ISALOCAL\tshinder

Understanding Email Servers

- Log information:
  - Email content.
  - Sending IP address.
  - Receiving and reading date and time.
  - System-specific information.
- Servers can recover deleted emails:
  - Similar to deletion of files on a hard drive.

Examining UNIX Email Server Logs

- `/etc/sendmail.cf`
  - Configuration information for Sendmail
- `/etc/syslog.conf`
  - Specifies how and which events Sendmail logs
- `/var/log/maillog`
  - **SMTP** and **POP3** communications
    - IP address and time stamp

Using Specialized Email Forensics Tools

- FINALeMAIL
  - Scans email database files
  - Recovers deleted emails
  - Search computer for lost or delete emails
- FTK
  - All-purpose program
  - Filters and finds files specific to email clients and servers
- InBoxer
  - Systematic analysis of emails

Using Specialized Email Forensics Tools

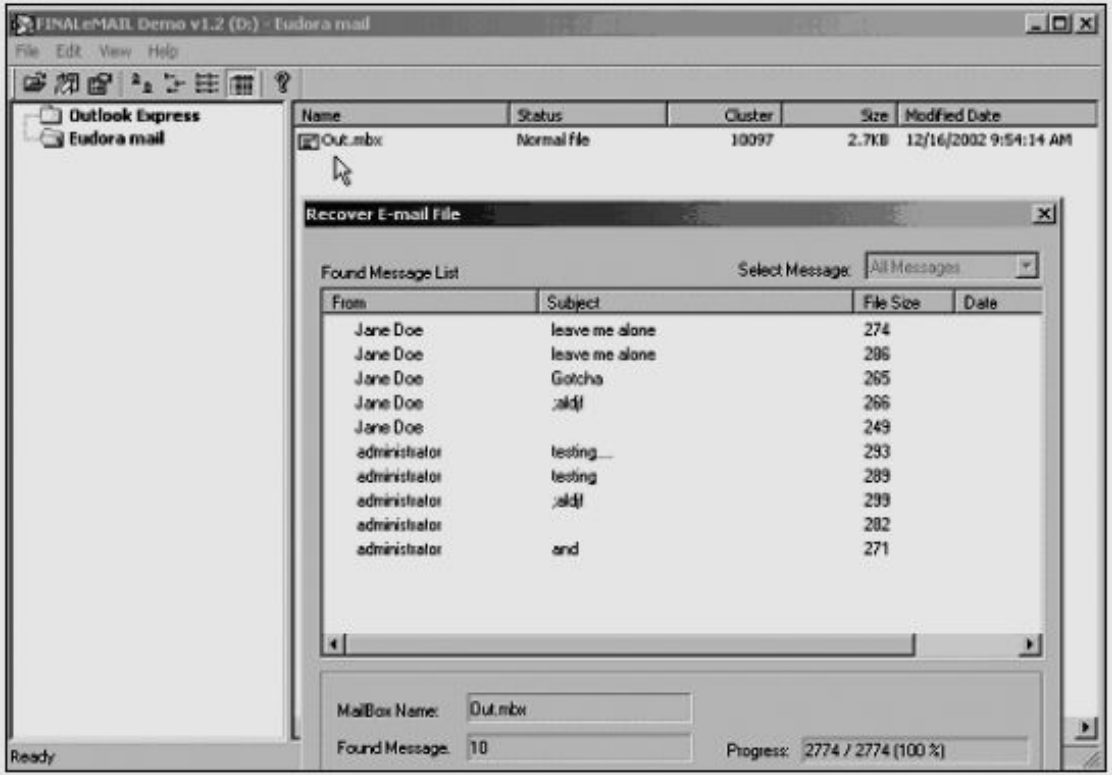
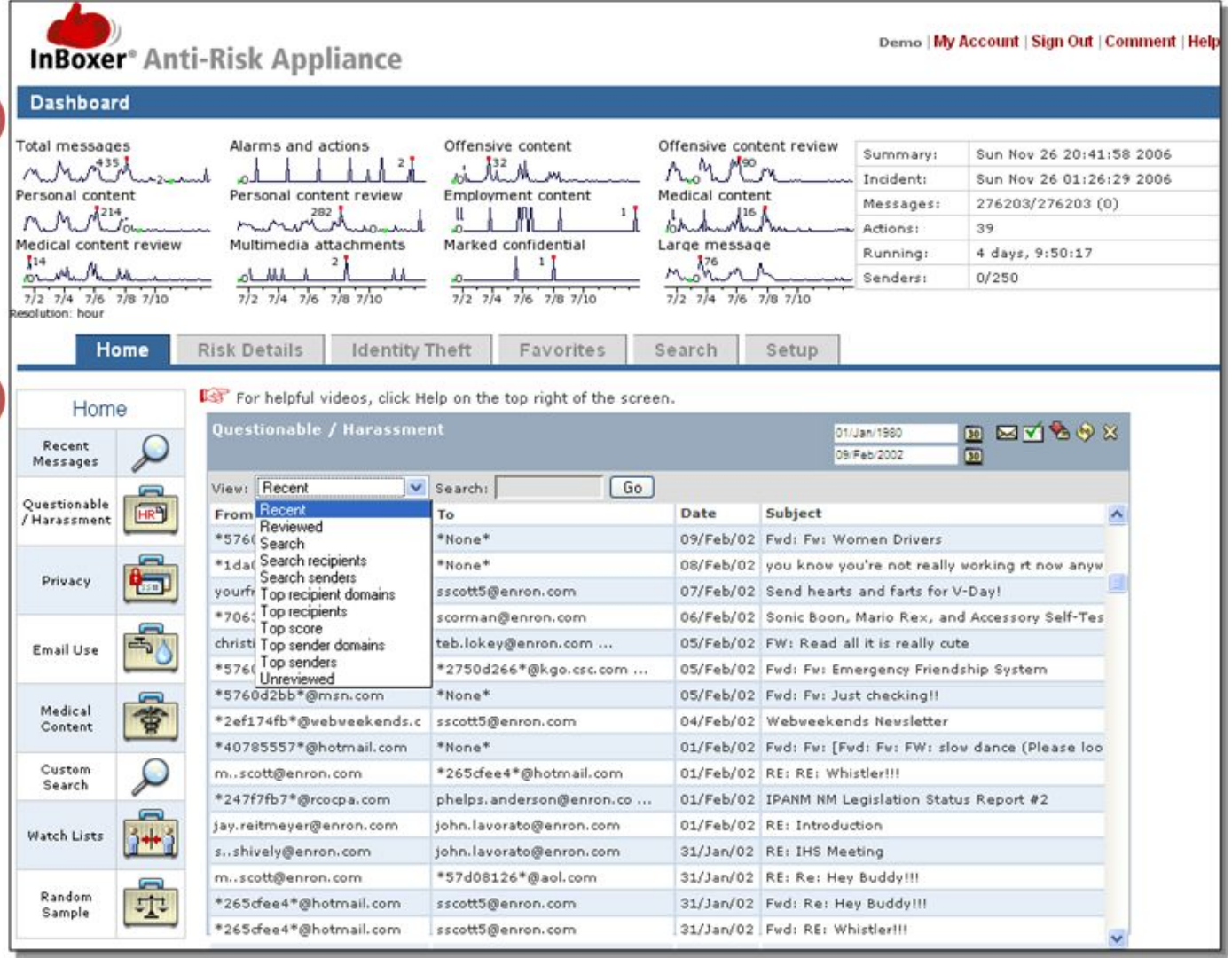


Figure 12-22 E-mail search results in FINALeMAIL

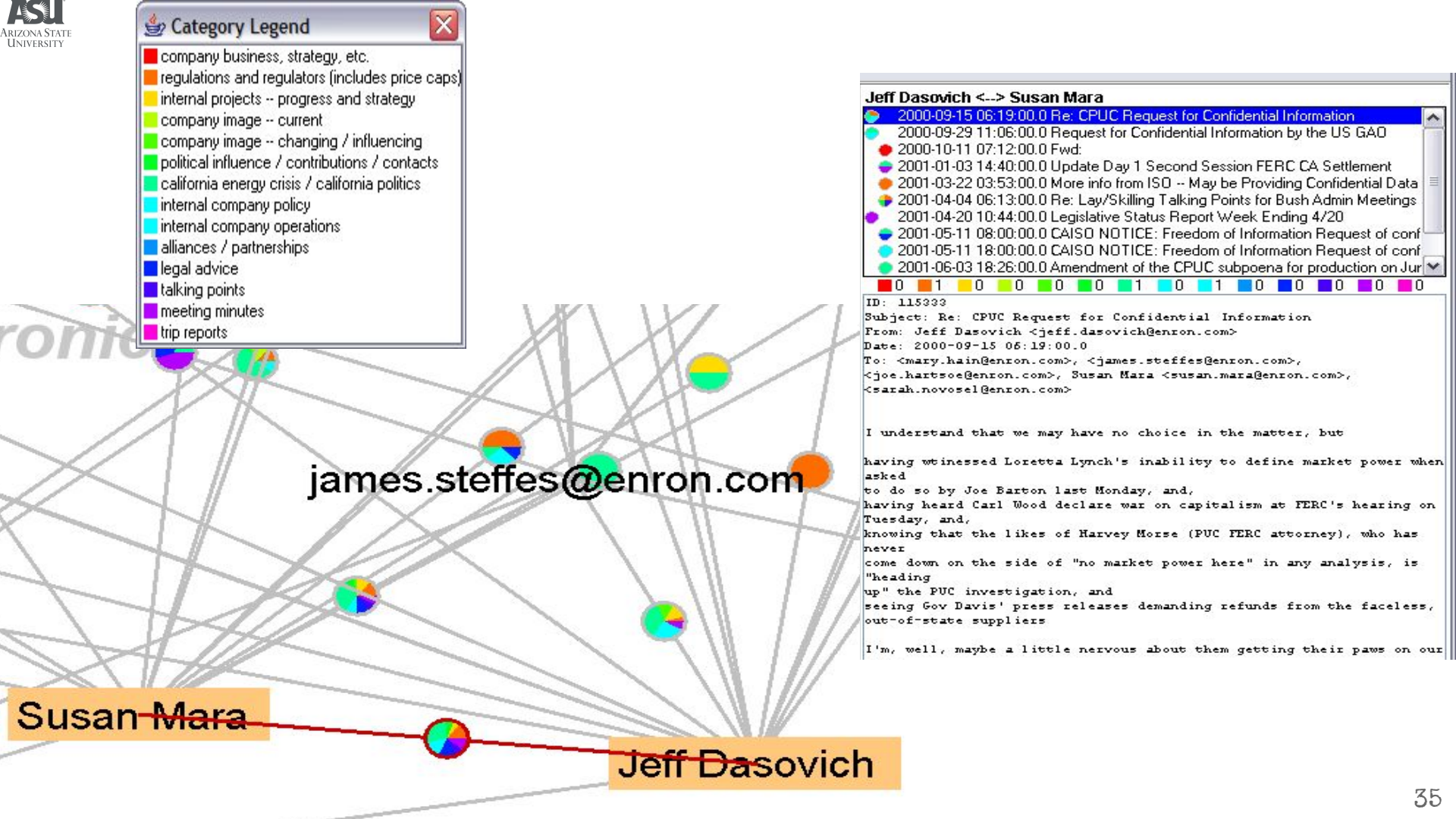

InBoxer® Anti-Risk Appliance
Demo | My Account | Sign Out | Comment | Help
1
Dashboard
Total messages
Alarms and actions
Offensive content
Offensive content review
Personal content
Personal content review
Employment content
Medical content
Medical content review
Multimedia attachments
Marked confidential
Large message
7/2 7/4 7/6 7/8 7/10
Resolution: hour
Summary: Sun Nov 26 20:41:58 2006
Incident: Sun Nov 26 01:26:29 2006
Messages: 276203/276203 (0)
Actions: 39
Running: 4 days, 9:50:17
Senders: 0/250
Home
Risk Details
Identity Theft
Favorites
Search
Setup
2
Home
Recent Messages
Questionable / Harassment
Privacy
Email Use
Medical Content
Custom Search
Watch Lists
Random Sample
For helpful videos, click Help on the top right of the screen.
Questionable / Harassment
01/Jan/1980
09/Feb/2002
View: Recent
Search:
Go
Recent
Reviewed
Search
Search recipients
Search senders
Top recipient domains
Top recipients
Top score
Top sender domains
Top senders
Unreviewed
From
To
Date
Subject
None 09/Feb/02 Fwd: Fw: Women Drivers
None 08/Feb/02 you know you're not really working rt now anyw
sscott5@enron.com 07/Feb/02 Send hearts and farts for V-Day!
scorman@enron.com 06/Feb/02 Sonic Boon, Mario Rex, and Accessory Self-Tes
teb.lokey@enron.com ... 05/Feb/02 FW: Read all it is really cute
2750d266@kgo.csc.com ... 05/Feb/02 Fwd: Fw: Emergency Friendship System
5760d2bb@msn.com *None* 05/Feb/02 Fwd: Fw: Just checking!!
2ef174fb@webweekends.c sscott5@enron.com 04/Feb/02 Webweekends Newsletter
40785557@hotmail.com *None* 01/Feb/02 Fwd: Fw: [Fwd: Fw: FW: slow dance (Please loo
m..scott@enron.com *265cfee4*@hotmail.com 01/Feb/02 RE: RE: Whistler!!!
247f7fb7@rcocpa.com phelps.anderson@enron.co ... 01/Feb/02 IPANM NM Legislation Status Report #2
jay.reitmeyer@enron.com john.lavorato@enron.com 01/Feb/02 RE: Introduction
s..shively@enron.com john.lavorato@enron.com 31/Jan/02 RE: IHS Meeting
m..scott@enron.com *57d08126*@aol.com 31/Jan/02 RE: Re: Hey Buddy!!!
265cfee4@hotmail.com sscott5@enron.com 31/Jan/02 Fwd: Re: Hey Buddy!!!
265cfee4@hotmail.com sscott5@enron.com 31/Jan/02 Fwd: RE: Whistler!!!

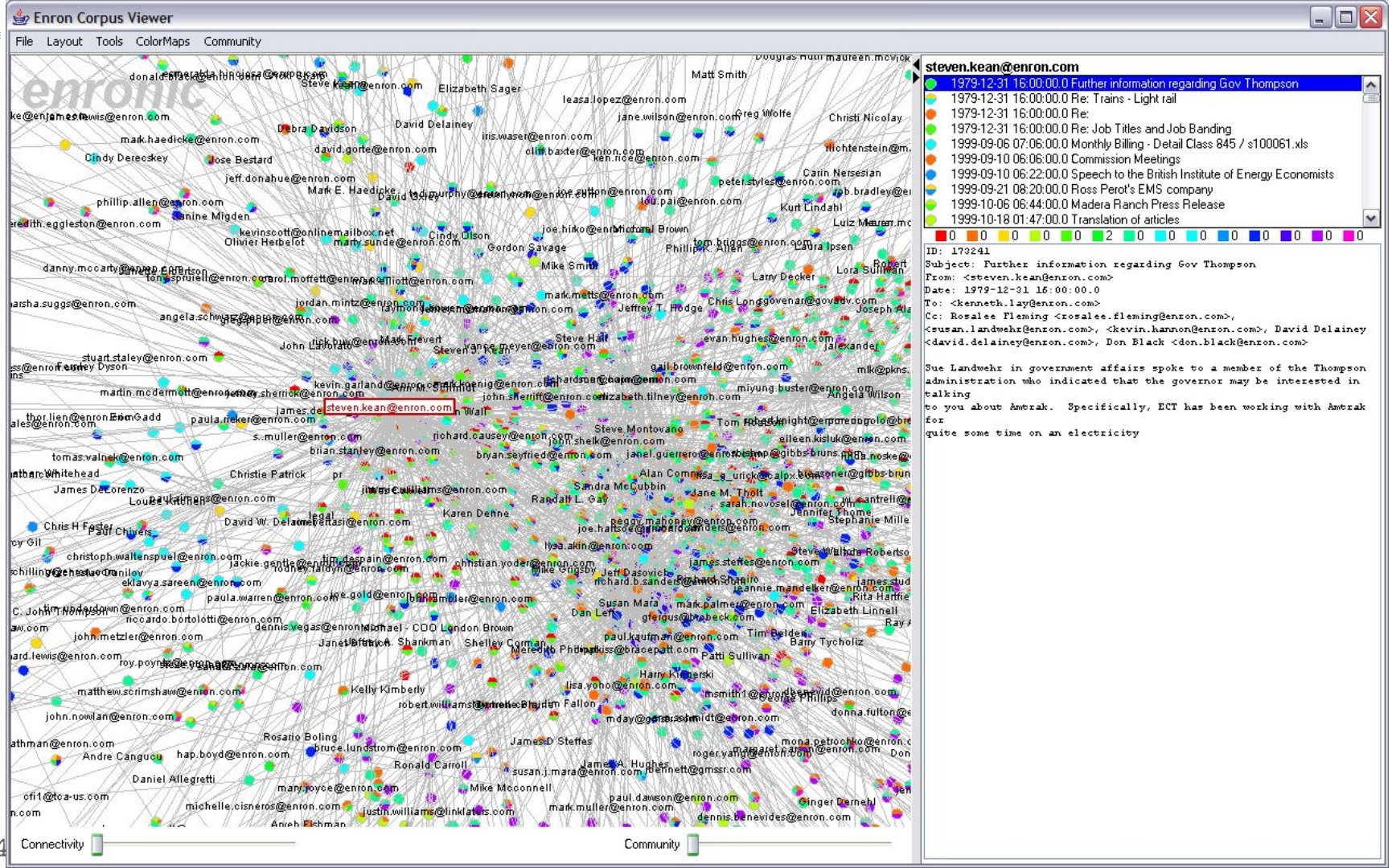
Carving Email Messages

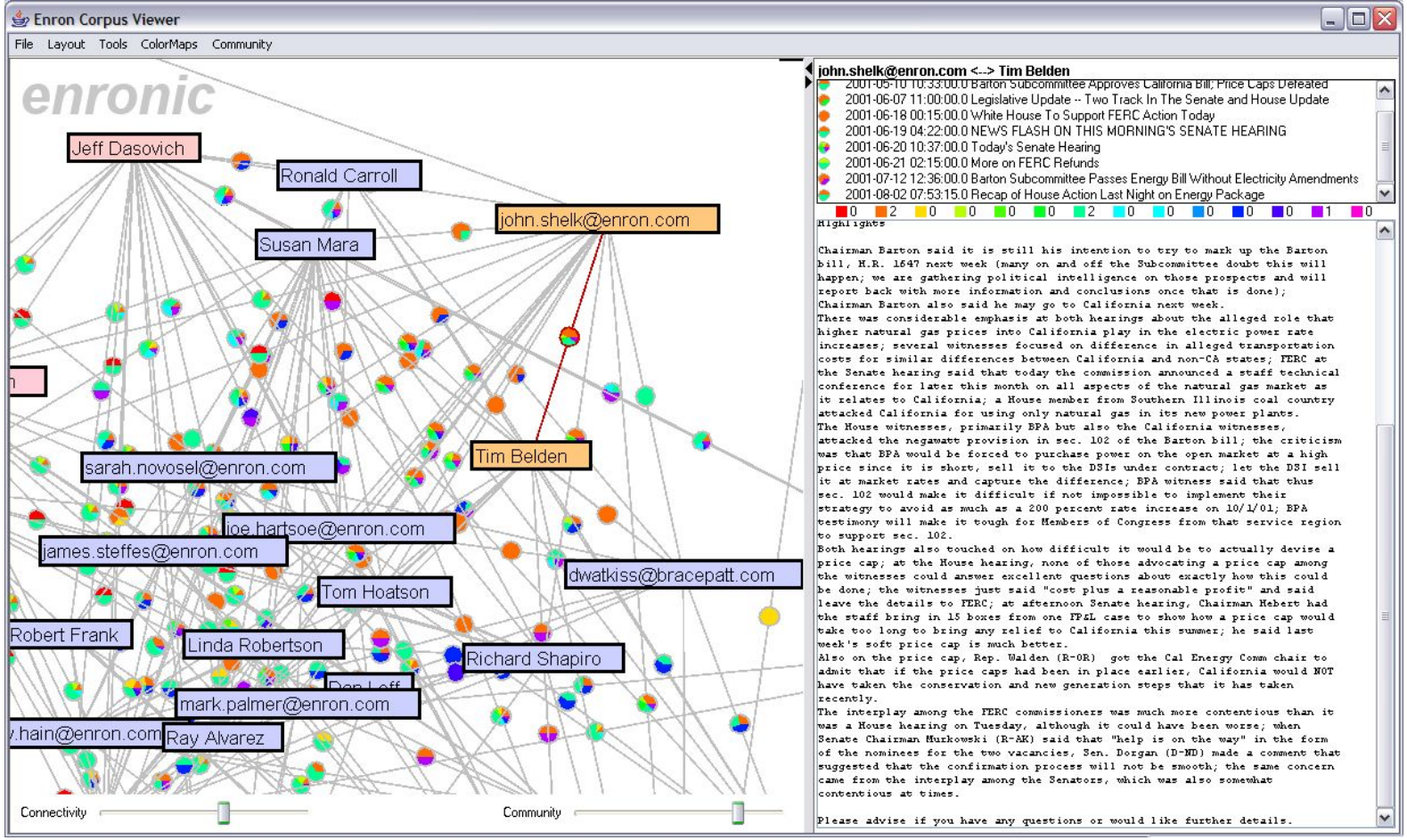
- Very few vendors have products for analyzing email in systems other than Microsoft
- **mbox** format
  - Stores emails in flat plaintext files
- **Multipurpose Internet Mail Extensions (MIME)** format
  - Used by vendor-unique email file systems, such as Microsoft .pst or .ost

What other information can be extracted from emails?

- Buddygraph
  - Social network analysis based on emails
- Enron investigation
  - Email visualization in Enron investigations:


Category Legend
company business, strategy, etc.
regulations and regulators (includes price caps)
internal projects -- progress and strategy
company image -- current
company image -- changing / influencing
political influence / contributions / contacts
california energy crisis / california politics
internal company policy
internal company operations
alliances / partnerships
legal advice
talking points
meeting minutes
trip reports
Jeff Dasovich <--> Susan Mara
2000-09-15 06:19:00.0 Re: CPUC Request for Confidential Information
2000-09-29 11:06:00.0 Request for Confidential Information by the US GAO
2000-10-11 07:12:00.0 Fwd:
2001-01-03 14:40:00.0 Update Day 1 Second Session FERC CA Settlement
2001-03-22 03:53:00.0 More info from ISO -- May be Providing Confidential Data
2001-04-04 06:13:00.0 Re: Lay/Skilling Talking Points for Bush Admin Meetings
2001-04-20 10:44:00.0 Legislative Status Report Week Ending 4/20
2001-05-11 08:00:00.0 CAISO NOTICE: Freedom of Information Request of conf
2001-05-11 18:00:00.0 CAISO NOTICE: Freedom of Information Request of conf
2001-06-03 18:26:00.0 Amendment of the CPUC subpoena for production on Jur
0 1 0 0 0 0 1 0 1 0 0 0 0 0
ID: 115333
Subject: Re: CPUC Request for Confidential Information
From: Jeff Dasovich <jeff.dasovich@enron.com>
Date: 2000-09-15 06:19:00.0
To: <mary.hain@enron.com>, <james.steffes@enron.com>,
<joe.hartsoe@enron.com>, Susan Mara <susan.mara@enron.com>,
<sarah.novosel@enron.com>
I understand that we may have no choice in the matter, but
having wtinessed Loretta Lynch's inability to define market power when
asked
to do so by Joe Barton last Monday, and,
having heard Carl Wood declare war on capitalism at FERC's hearing on
Tuesday, and,
knowing that the likes of Harvey Morse (PUC FERC attorney), who has
never
come down on the side of "no market power here" in any analysis, is
"heading
up" the PUC investigation, and
seeing Gov Davis' press releases demanding refunds from the faceless,
out-of-state suppliers
I'm, well, maybe a little nervous about them getting their paws on our
james.steffes@enron.com
Susan Mara
Jeff Dasovich

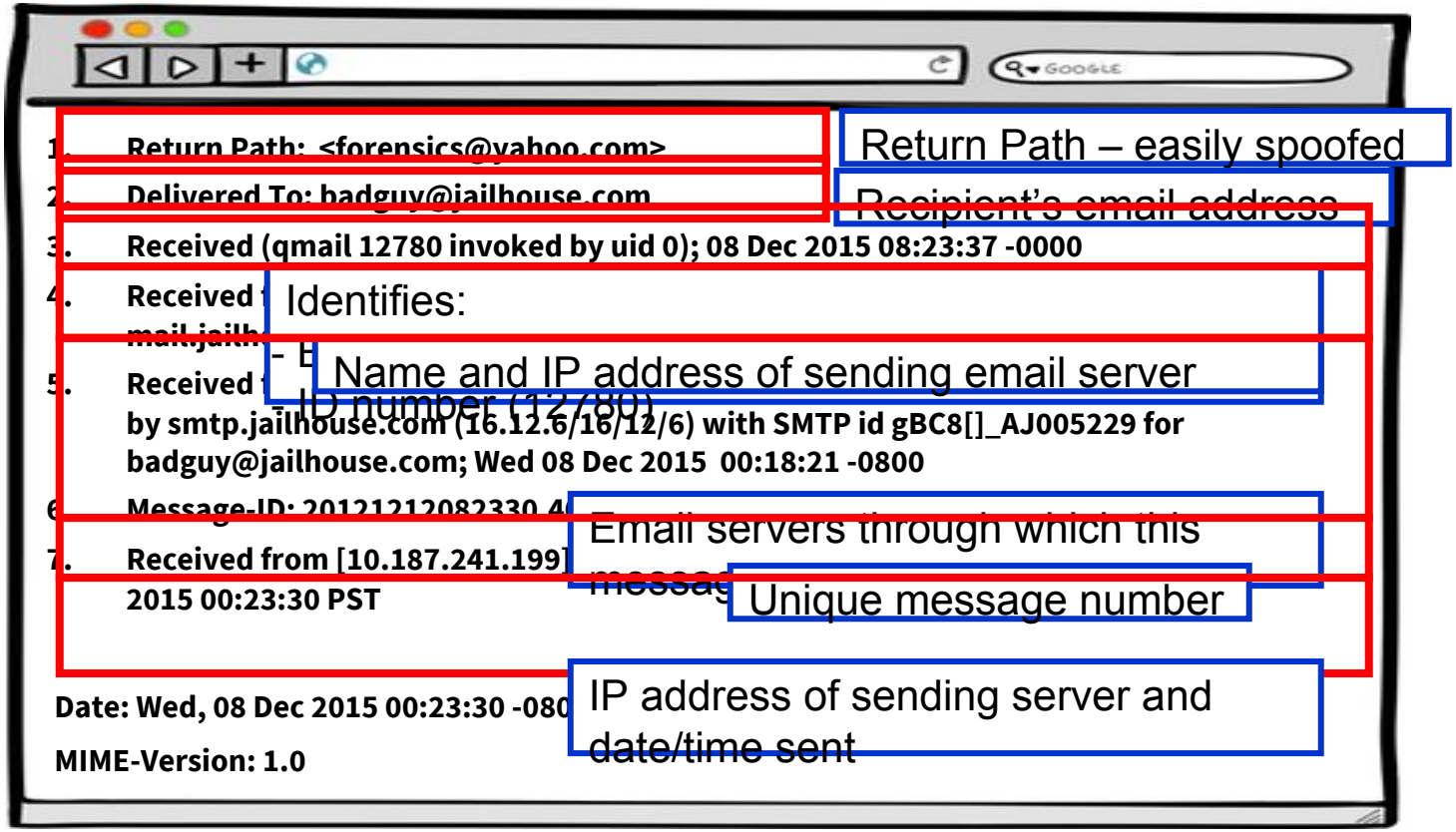

Enron Corpus Viewer
File Layout Tools ColorMaps Community
enronic
steven.kean@enron.com
1979-12-31 16:00:00.0 Further information regarding Gov Thompson
1979-12-31 16:00:00.0 Re: Trains - Light rail
1979-12-31 16:00:00.0 Re:
1979-12-31 16:00:00.0 Re: Job Titles and Job Banding
1999-09-06 07:06:00.0 Monthly Billing - Detail Class 845 / s100061.xls
1999-09-10 06:06:00.0 Commission Meetings
1999-09-10 06:22:00.0 Speech to the British Institute of Energy Economists
1999-09-21 08:20:00.0 Ross Perot's EMS company
1999-10-06 06:44:00.0 Madera Ranch Press Release
1999-10-18 01:47:00.0 Translation of articles
0 0 0 0 0 0 2 0 0 0 0 0 0 0 0 0
ID: 173241
Subject: Further information regarding Gov Thompson
From: <steven.kean@enron.com>
Date: 1979-12-31 16:00:00.0
To: <kenneth.lay@enron.com>
Cc: Rosalee Fleming <rosalee.fleming@enron.com>,
<susan.landwehr@enron.com>, <kevin.hannon@enron.com>, David Delainey
<david.delainey@enron.com>, Don Black <don.black@enron.com>
Sue Landwehr in government affairs spoke to a member of the Thompson
administration who indicated that the governor may be interested in
talking
to you about Amtrak. Specifically, ECT has been working with Amtrak
for
quite some time on an electricity
Connectivity
Community



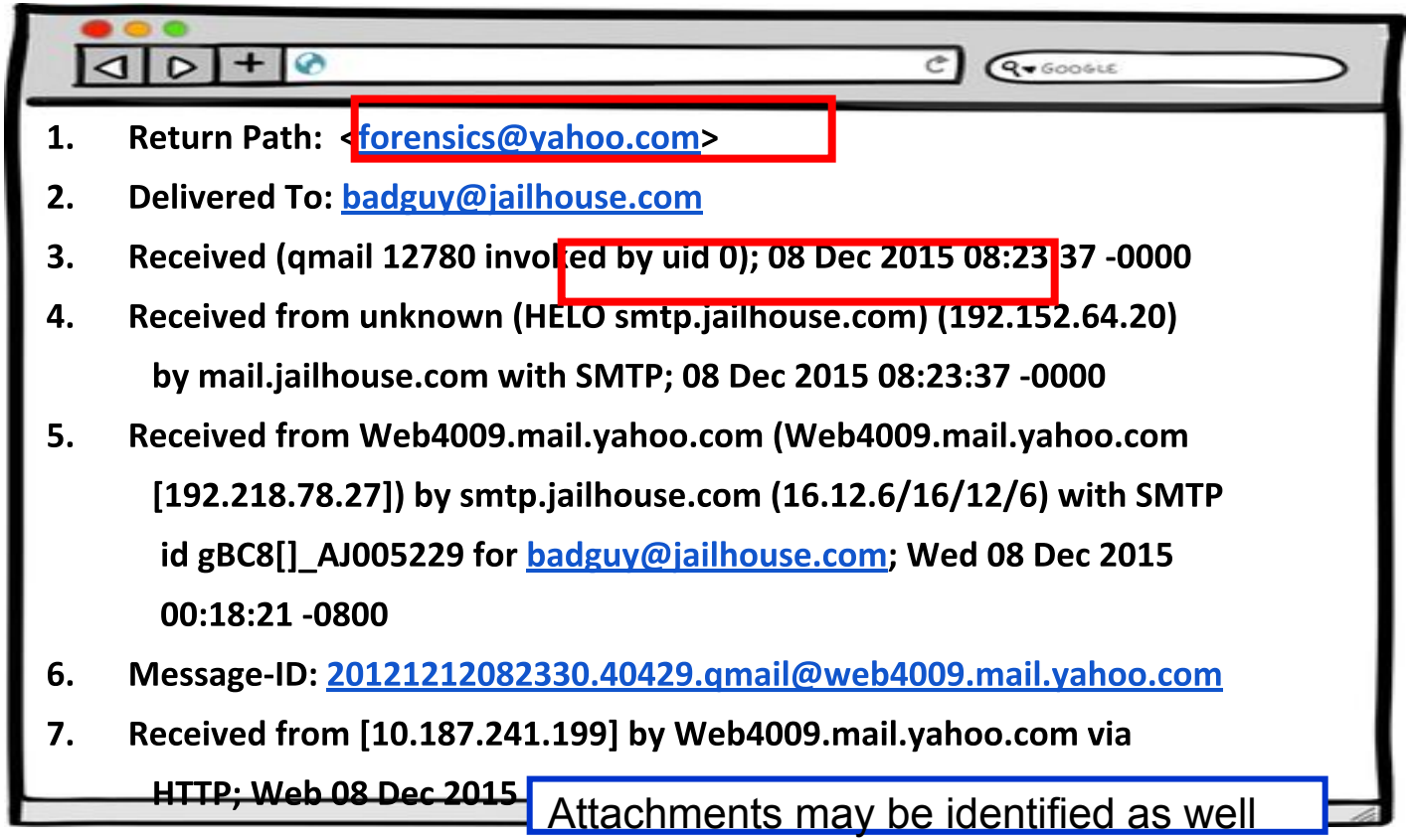
All one way emails to Tim Belden

Slides from Previous Years

Examining Email Headers



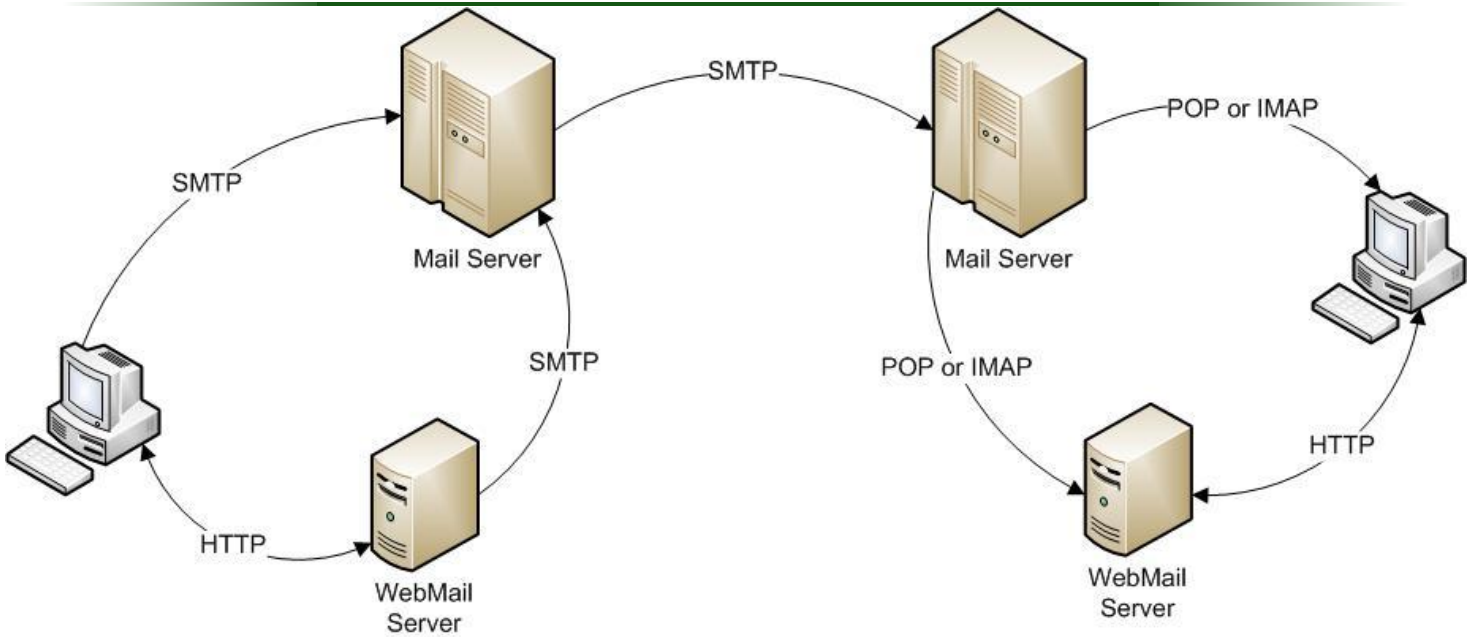
Examining Email Headers



1. Return Path: <forensics@yahoo.com>
2. Delivered To: badguy@jailhouse.com
3. Received (qmail 12780 invoked by uid 0); 08 Dec 2015 08:23:37 -0000
4. Received from unknown (HELO smtp.jailhouse.com) (192.152.64.20) by mail.jailhouse.com with SMTP; 08 Dec 2015 08:23:37 -0000
5. Received from Web4009.mail.yahoo.com (Web4009.mail.yahoo.com [192.218.78.27]) by smtp.jailhouse.com (16.12.6/16/12/6) with SMTP id gBC8[]_AJ005229 for badguy@jailhouse.com; Wed 08 Dec 2015 00:18:21 -0800
6. Message-ID: 20121212082330.40429.qmail@web4009.mail.yahoo.com
7. Received from [10.187.241.199] by Web4009.mail.yahoo.com via HTTP; Web 08 Dec 2015

Attachments may be identified as well

Network Protocols Related to Email



- SMTP: Simple Mail Transfer Protocol.
- POP: Post Office Protocol.
- IMAP: Internet Message Access Protocol.

Using Network Logs Related to Email

- Router logs:
  - Record all incoming and outgoing traffic.
  - Have rules to allow or disallow traffic.
- Firewall logs:
  - Filter email traffic.
  - Verify whether the email passed through.
- We can use any text editor or specialized tools.

Examining UNIX Email Server Logs

```
# The following line will send all mail logs to the /var/log/maillog
directory
mail.*                          /var/log/maillog
# Log all emergency messages in the same place
*.emerg                         *
*.emerg                         @superiorbicycles.biz
# This line will put all news and e-mail encoded with uucp with
Critical errors in the #/var/log/spooler
uucp, news.crit
```

Figure 12-16 A typical syslog.conf file

```
May 21 10:10:32 poser sendmail[5365]: NOQUEUE: "wiz" command from
[10.0.1.1] (10.0.1.1)
May 21 10:10:32 poser sendmail[5365]: NOQUEUE: "debug" command from
[10.0.1.1] (10.0.1.1)
```

Figure 12-17 A sample maillog file with SMTP information

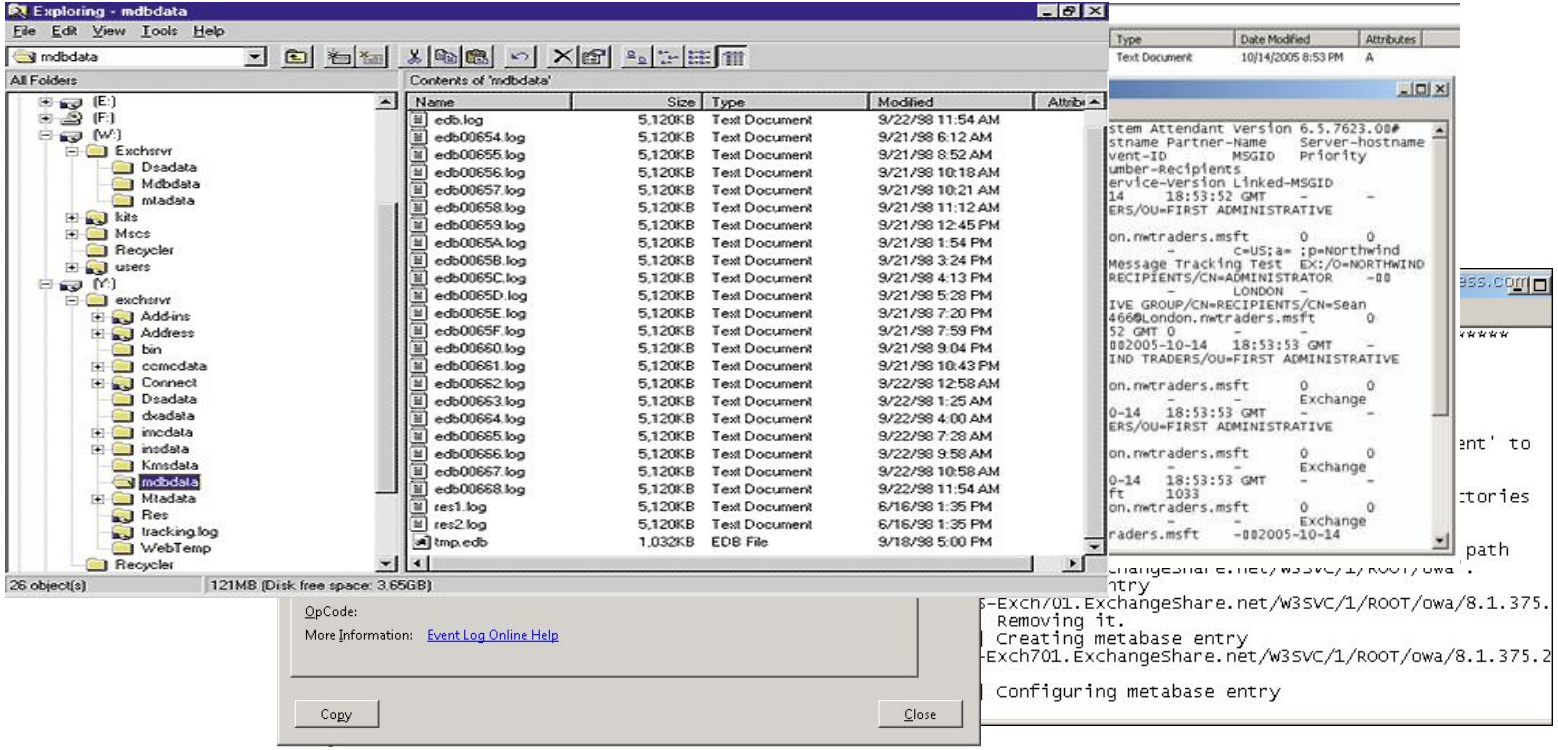
```
May 21 10:12:44 poser ipop3d[5373]: port 110 service init from 10.0.1.1
May 21 10:12:44 poser ipop3d[5373]: Login failure user=rich
host=[10.0.1.1]
```

Figure 12-18 A sample maillog file with POP3 information

Examining Microsoft Email Server Logs

- Microsoft Exchange Server (Exchange)
  - Based on Microsoft Extensible Storage Engine
  - Information Store files
    - Database files *.edb
      - Responsible for MAPI information
    - Database files *.stm
      - Responsible for non-MAPI information
- Logs
  - Transaction logs
    - Keep track of email databases
  - Checkpoints
    - Keep track of transaction logs
  - Temporary files
  - Email communication logs
    - res#.log
  - Tracking.log
    - Tracks messages

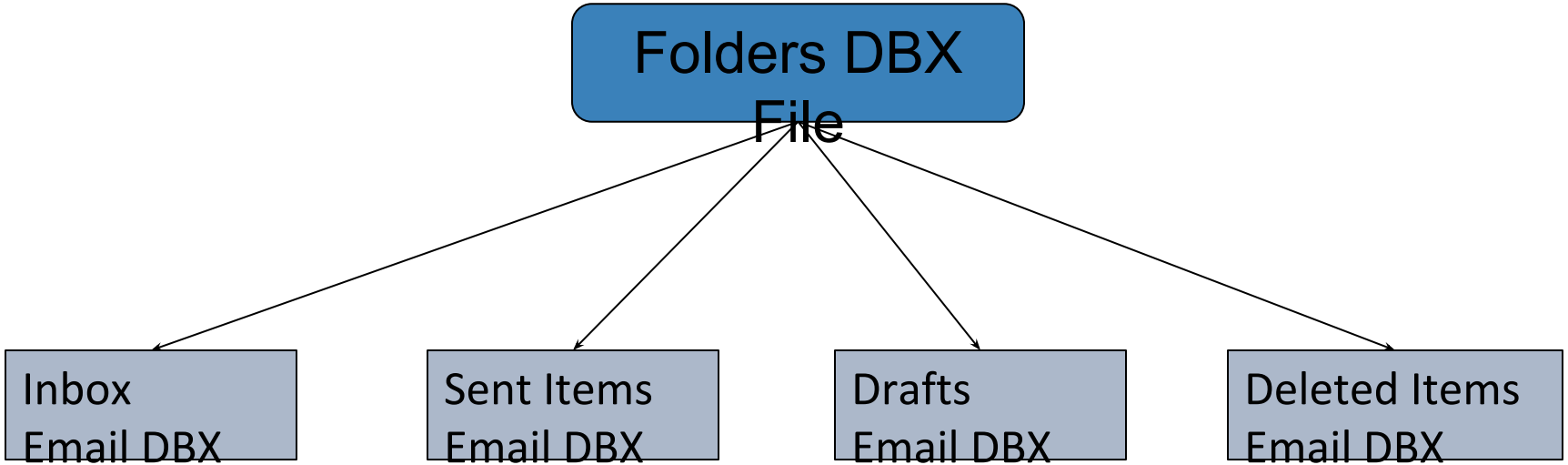
Examining Microsoft Email Server Logs



Outlook Express--Example

- Need to understand the internal structure of Outlook Express email repositories (DBX)
- Two types of DBX files
  - Folders DBX file
    - A catalog of the other DBX files
  - Email DBX file
    - Contains the actual email messages' content and attachments

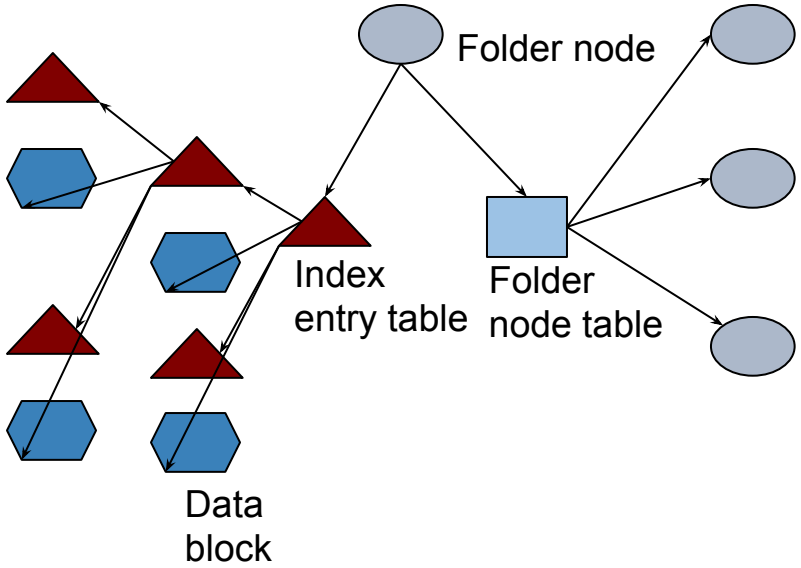
Outlook Express--Example



- Each Email DBX file is cataloged in the Folders DBX file so that Outlook Express can re-create the folder structure for the user

Outlook Express--Example

- Folders DBX file format
  - Header includes the file signature and the number & location of internal file structures
  - The header of a folder node is 0x18 bytes long
  - The signature is 16-bytes long
    - CF AD 12 FE C6 FD 75 6F 66 E3 D1 11 9A 4E 00 C0
  - At byte offset 0xC4, a 4-byte number signifies the number of folder nodes



Outlook Express--Example

- Email DBX file format
  - The signature is 16-bytes long
    - CF AD 12 FE C5 FD 75 6F 66 E3 D1 11 9A 4E 00 C0
  - Internal structure
    - A one-byte type field and a 3-byte value field
    - Data Entries
      - 0x0D: pointer to the name of the sender for the email message
      - 0x0E: pointer to the email address of the sender for the email message
      - 0x12: pointer to the time the email message was sent
      - 0x13: pointer to the name of the recipient for the email message
      - 0x14: pointer to the email address of the recipient for the email message
      - 0x1A: pointer to the server that the email message was retrieved from