

CSE 469: Computer and Network Forensics

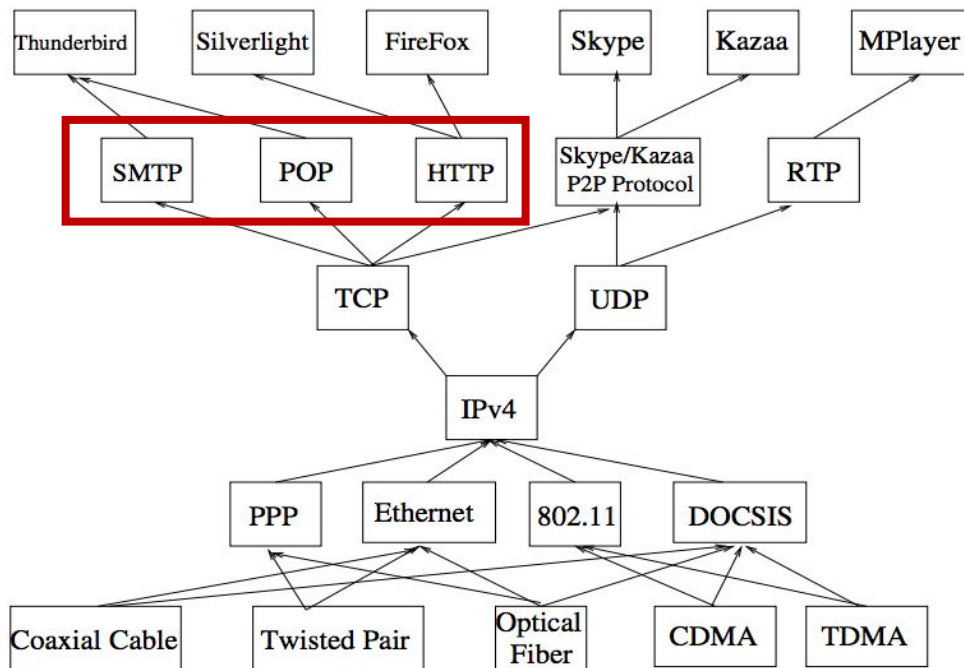
Topic 6: Email Forensics

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)

Settings

[General](#)
[Labels](#)
[Inbox](#)
[Accounts and Import](#)
[Filters and Blocked Addresses](#)
[Forwarding and POP/IMAP](#)
[Chat](#)
[Lab](#)

Forwarding:
[Learn more](#)

[Add a forwarding address](#)

Tip: You can also forward only some of your mail by [creating a filter!](#)

POP Download:
[Learn more](#)

1. Status: **POP is enabled** for all mail that has arrived since 9/22/05

☐ Enable POP for **all mail** (even mail that's already been downloaded)
☐ Enable POP for **mail that arrives from now on**
☐ **Disable POP**

2. When messages are accessed with POP keep Gmail's copy in the Inbox ▾

3. Configure your email client (e.g. Outlook, Eudora, Netscape Mail)
[Configuration instructions](#)

IMAP Access:
(access Gmail from other clients using IMAP)
[Learn more](#)

Status: **IMAP is enabled**

☒ Enable IMAP
☐ Disable IMAP

When I mark a message in IMAP as deleted:

☒ Auto-Expunge on - Immediately update the server. (default)
☐ Auto-Expunge off - Wait for the client to update the server.

When a message is marked as deleted and expunged from the last visible IMAP folder

☒ Archive the message (default)
☐ Move the message to the Trash
☐ Immediately delete the message forever

Folder Size Limits

☒ Do not limit the number of messages in an IMAP folder (default)
☐ Limit IMAP folders to contain no more than this many messages 1,000 ▾

Configure your email client (e.g. Outlook, Thunderbird, iPhone)

Configuring Email Clients (2)

Change Account

Internet E-mail Settings
Each of these settings are required to get your e-mail account working.

User Information

Your Name:

E-mail Address:

Server Information

Account Type:

Incoming mail server:

Outgoing mail server (SMTP):

Test Account Settings

After filling out the information on this screen, we recommend you test your account by clicking the button below. (Requires network connection)

☒ Test Account Settings by clicking the Next button

Logon Information

User Name:

Password:

☒ Remember password

☐ Require logon using Secure Password Authentication (SPA)

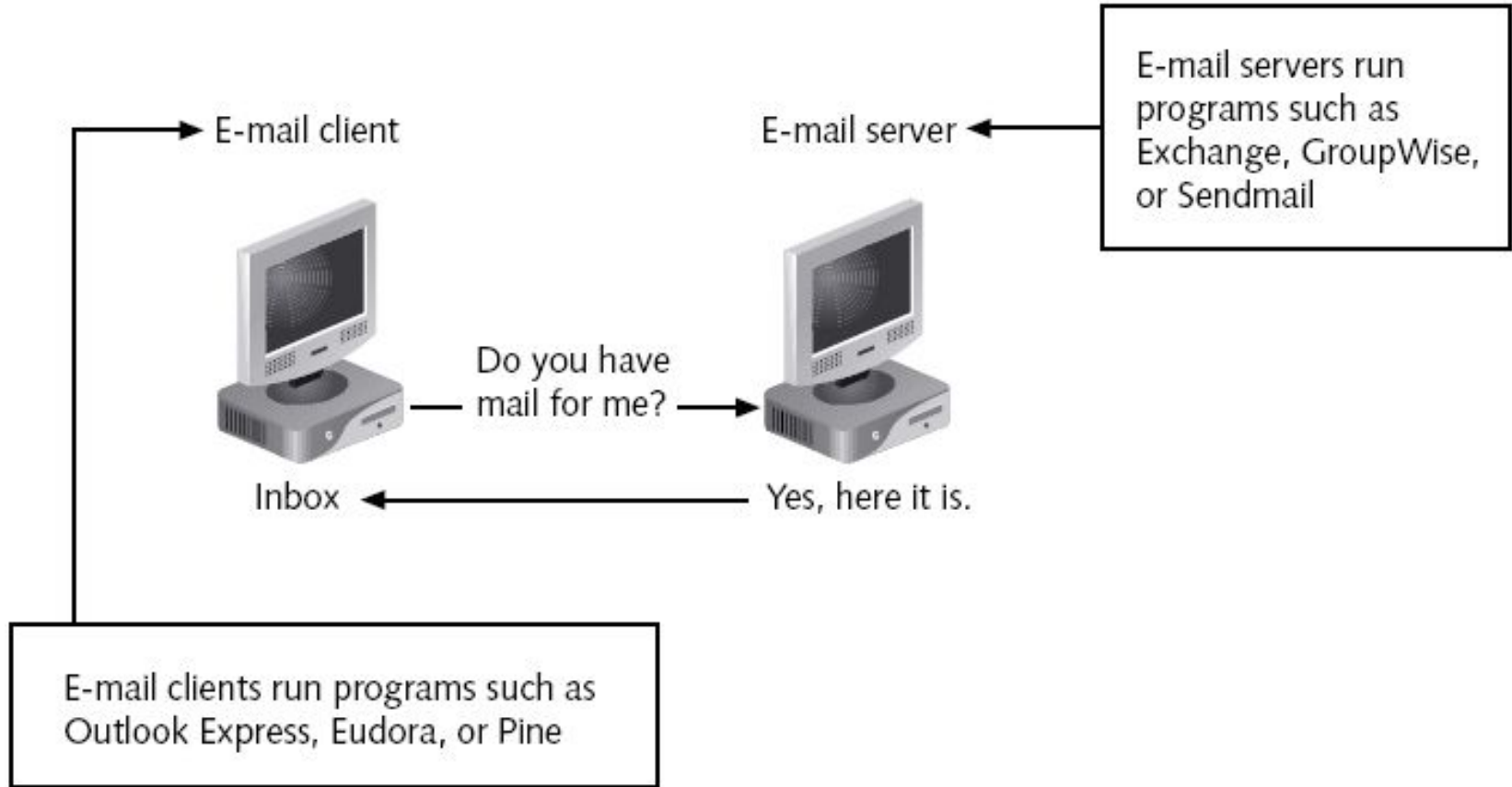
Email Client and Server Roles

- Email used in two environments:
 - Open (Internet).
 - Controlled (LAN, WAN).
- Both use client-server architecture:
 - **Central server** distributes email...
 - To many **distributed clients**.

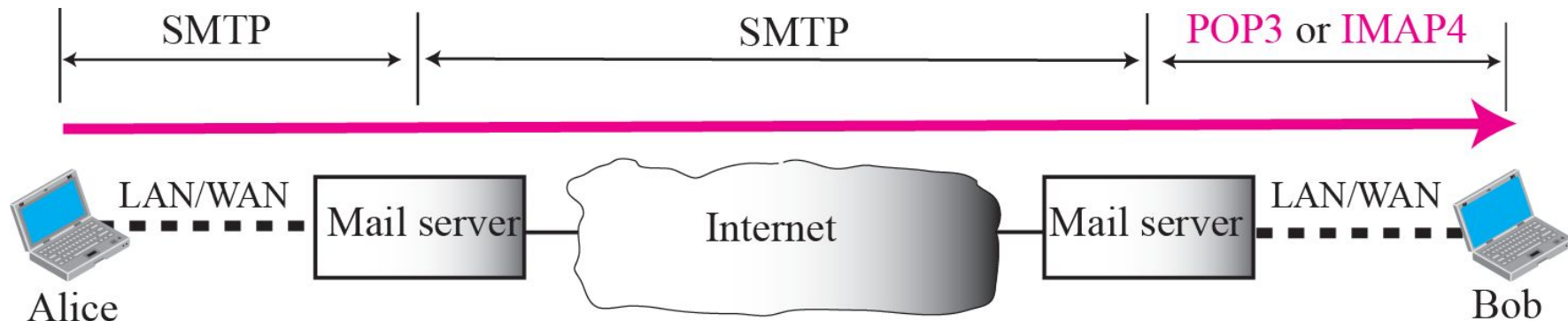
Email Client and Server Roles

- 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.

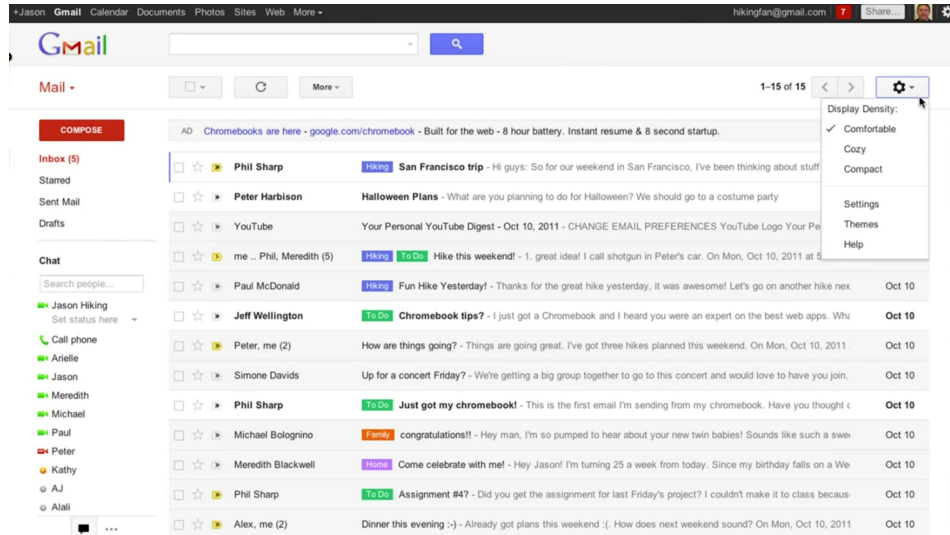
Email Client and Server Roles



User Agents / Email Client



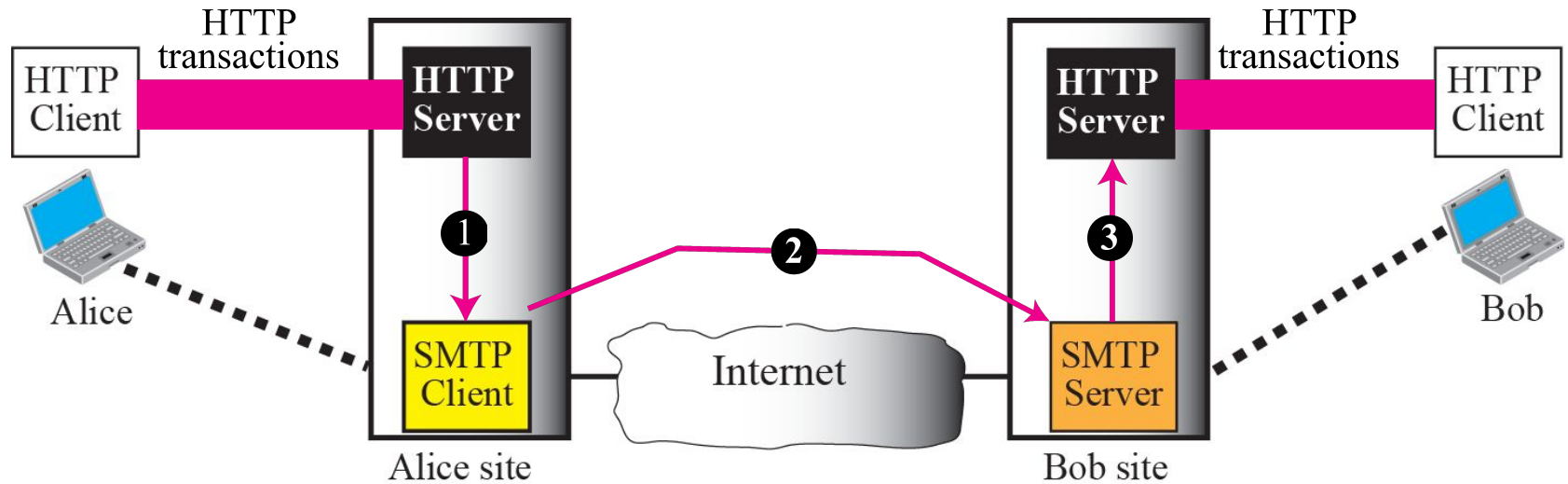
Webmail



Visit using browser



Webmail



Format of Email

Behrouz Forouzan
De Anza College
Cupertino, CA 96014

Firouz Mosharraf
Com-Net
Cupertino, CA 95014

Firouz Mosharraf
Com-Net
Cupertino, CA 95014
Jan. 5, 2005

Subject: Network

Dear Mr. Mosharraf
We want to inform you that
our network is working properly
after the last repair.

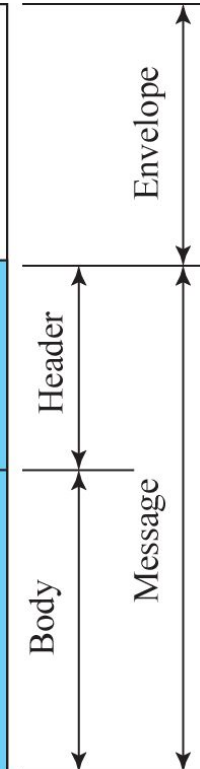
Yours truly,
Behrouz Forouzan

Mail From: forouzan@deanza.edu
RCPT To: firouz@net.edu

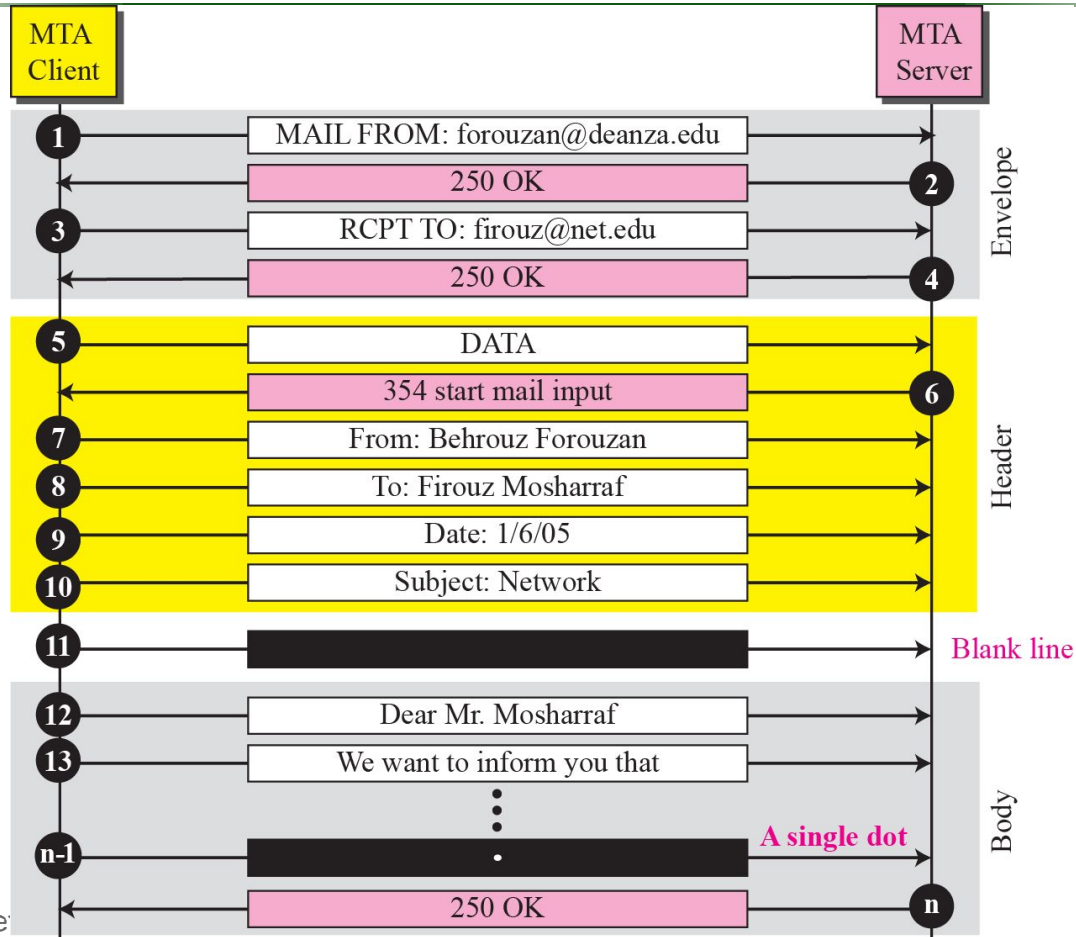
From: Behrouz Forouzan
To: Firouz Mosharraf
Date: 1/5/05
Subject: Network

Dear Mr. Mosharraf
We want to inform you that
our network is working properly
after the last repair.

Yours truly,
Behrouz Forouzan



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

The screenshot shows an email client window with a sidebar on the left containing folders like 'Junk E-mail (17)', 'Calendar', 'Contacts', and 'BACKUP FOLDERS'. The main pane displays an email from 'Crimes, Electronic' with the subject 'DHS Cyber Report 22 March 2010'. The email body is marked 'UNCLASSIFIED' and contains the following text:

UNCLASSIFIED

This document was prepared by the Office of Intelligence and Analysis to facilitate a greater understanding of the nature and scope of threats and hazards to the homeland. It is provided to Federal, State, local and private sector officials to aid in the identification and development of appropriate actions, priorities and follow-on measures. This product may contain U.S. person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Some content may be copyrighted. These materials, including copyrighted materials, are intended for "fair use" as permitted under Title 17, Section 107 of the United States Code ("The Copyright Law"). Use of copyrighted material for unauthorized purposes requires permission from the copyright owner. Any feedback regarding this report or requests for changes to the distribution list should be directed to the Open Source Enterprise via unclassified e-mail at: OSINTBranchMailbox@hq.dhs.gov.

UNCLASSIFIED Page 1 of 2 DHS Open Source Enterprise Daily Cyber Report

22 March 2010

CRITICAL INFRASTRUCTURE PROTECTION:

- Nothing significant to report

INFORMATION SYSTEMS BREACHES:

- As health data goes digital, security risks grow: Over the next four years, the amount of personal medical information online will increase exponentially, opening up new avenues for hackers to expose personal data that, unlike financial information, can result in a permanent violation of privacy. The U.S. Department of Health and Human Services (HHS) has set a deadline of 2015 for healthcare facilities to be using electronic health records (EHRs), thereby ushering in the digitalization of all patient information. As patient data is aggregated on health networks, it becomes a bigger target for those who want to steal it and exploit it on the Internet, experts say. ... It's not so much the quantity of information that could be a problem; it's the different sources of data, its diversity of data and the various network infrastructures on which it resides that could overwhelm the U.S. health system and pose significant risks to privacy.... [Date: 22 March 2010; Source: <http://www.computerworld.com/s/article/9173198/>]

Viewing Email Headers

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

Viewing Email Headers

I like your post -- gHacks technology news contact form

Inbox | X

★
beatsjames
cheaksale15@
show details
3:22 AM (5 hours ago)

Reply

Reply to all

Forward

Filter messages like this

Print

Add beatsjames to Contacts list

Delete this message

Report phishing

Show original

Message text garbled?

Mark as unread

Translate message

Great job with the article, I've been stopping by h
href="http://www.beatsbydrdreshopping.com/lady-
>Lady GaGa Heartbeats just wanted to let y
post. I discovered it quite useful to me. I is going t
blog once again some day.

Sender info:

IP: 211.143.200.89 <http://ws.arin.net/whois/?que
Browser/OS: Opera/7.11 (Windows NT 5.1; U) [en

Reply

Reply to all

Forward

Invite beatsjames to chat

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 ESMTTP id o2MmDa3006803 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 ESMTTP 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 ESMTTP
id VFCVXSE900DP8Q0y 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
ESMTTP 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.ussd.dhs.gov (IA-Proxy-Blade1.ussd.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.ussd.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.ssnnet.ussd.dhs.gov
[10.200.70.21]) by barracuda12.ussd.dhs.gov (Spam & Virus Firewall) with ESMTTP id
DA38963DB88; Mon, 22 Mar 2010 15:43:15 -0400 (EDT)
Received: from 45prod21-ssnet.SSNET.USSS.DHS.GOV (45prod21-ssnet.ssnnet.ussd.dhs.gov
[10.200.70.21]) by barracuda12.ussd.dhs.gov with ESMTTP id XKHZ5gMT3RpdmXKe; Mon, 22 Mar
2010 15:43:15 -0400 (EDT)
Received: from 40WASS4-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
```

ber Report 22 March 2010



s.dhs.gov>

s.dhs.gov>

CLASSIFIED

*d Analysis to facilitate a greater understanding of the nature and scope of
al, State, local and private sector officials to aid in the identification and
measures. This product may contain U.S. person information that has been
assess, or act on the information provided. It should be handled in
information handling procedures. Some content may be copyrighted. These
fair use" as permitted under Title 17, Section 107 of the United States Code
thorized purposes requires permission from the copyright owner. Any
distribution list should be directed to the Open Source Enterprise via*

INCLASSIFIED Page 1 of 2 DHS Open Source

2 March 2010

Risks grow: Over the next four years, the amount of personal
opening up new avenues for hackers to expose personal data that,
olation of privacy. The U.S. Department of Health and Human
e facilities to being using electronic health records (EHRs), thereby
patient data is aggregated on health networks, it becomes a bigger
Internet, experts say. ... It's not so much the quantity of information
its diversity of data and the various network infrastructures on which
and pose significant risks to privacy.... [Date: 22 March 2010; Source:

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

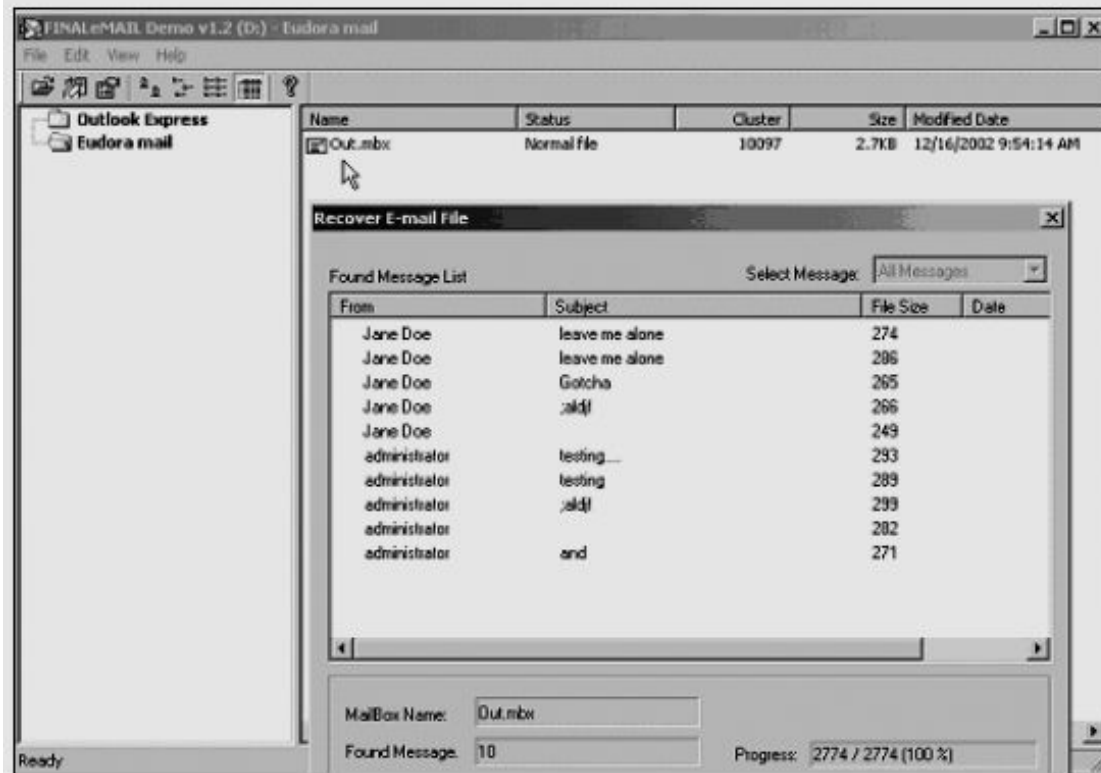
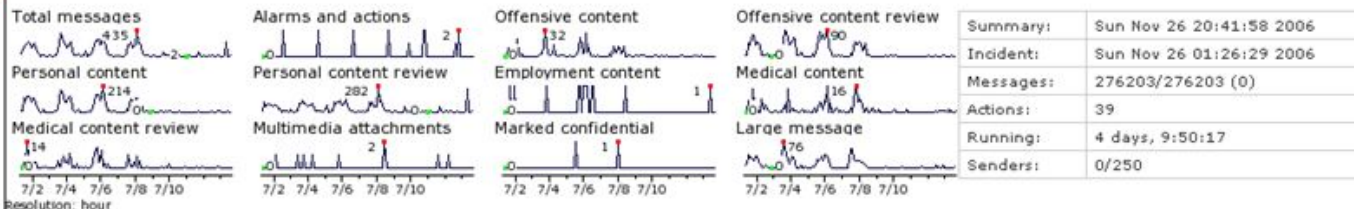


Figure 12-22 E-mail search results in FINALEMAIL

1

Dashboard



2

Home | **Risk Details** | **Identity Theft** | **Favorites** | **Search** | **Setup**

For helpful videos, click Help on the top right of the screen.

Questionable / Harassment

View: **Recent** | Search: | **Go**

From	To	Date	Subject
5760d2bb@msn.com	*None*	09/Feb/02	Fwd: Fw: Women Drivers
*1da...	*None*	08/Feb/02	you know you're not really working rt now anyw
yourf...	sscott5@enron.com	07/Feb/02	Send hearts and farts for V-Day!
*706...	scorman@enron.com	06/Feb/02	Sonic Boon, Mario Rex, and Accessory Self-Tes
christi...	teb.lokey@enron.com ...	05/Feb/02	FW: Read all it is really cute
5760d2bb@msn.com	*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	*265dfee4*@hotmail.com	01/Feb/02	RE: RE: Whistler!!!
247f7fb7@rcopa.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!!!
265dfee4@hotmail.com	sscott5@enron.com	31/Jan/02	Fwd: Re: Hey Buddy!!!
265dfee4@hotmail.com	sscott5@enron.com	31/Jan/02	Fwd: RE: Whistler!!!

Carving Email Messages

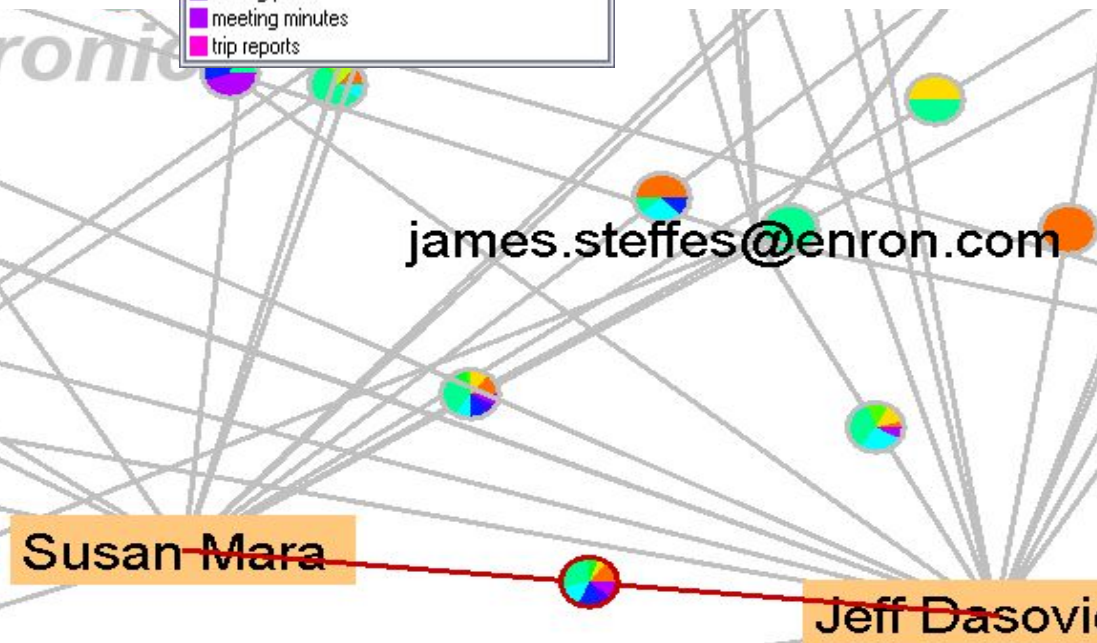
- Very few vendors have products for analyzing email in systems other than Microsoft
- **mbox** format
 - Stores emails in flat plaintext files
- **Multipurpose Internet Mail Extensions (MIME)** format
 - Used by vendor-unique email file systems, such as Microsoft .pst or .ost

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

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>

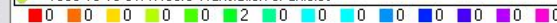
I understand that we may have no choice in the matter, but

having witnessed 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



- 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



ID: 173241

Subject: Further information regarding Gov Thompson

From: <steven.kean@enron.com>

Date: 1979-12-31 16:00:00.0

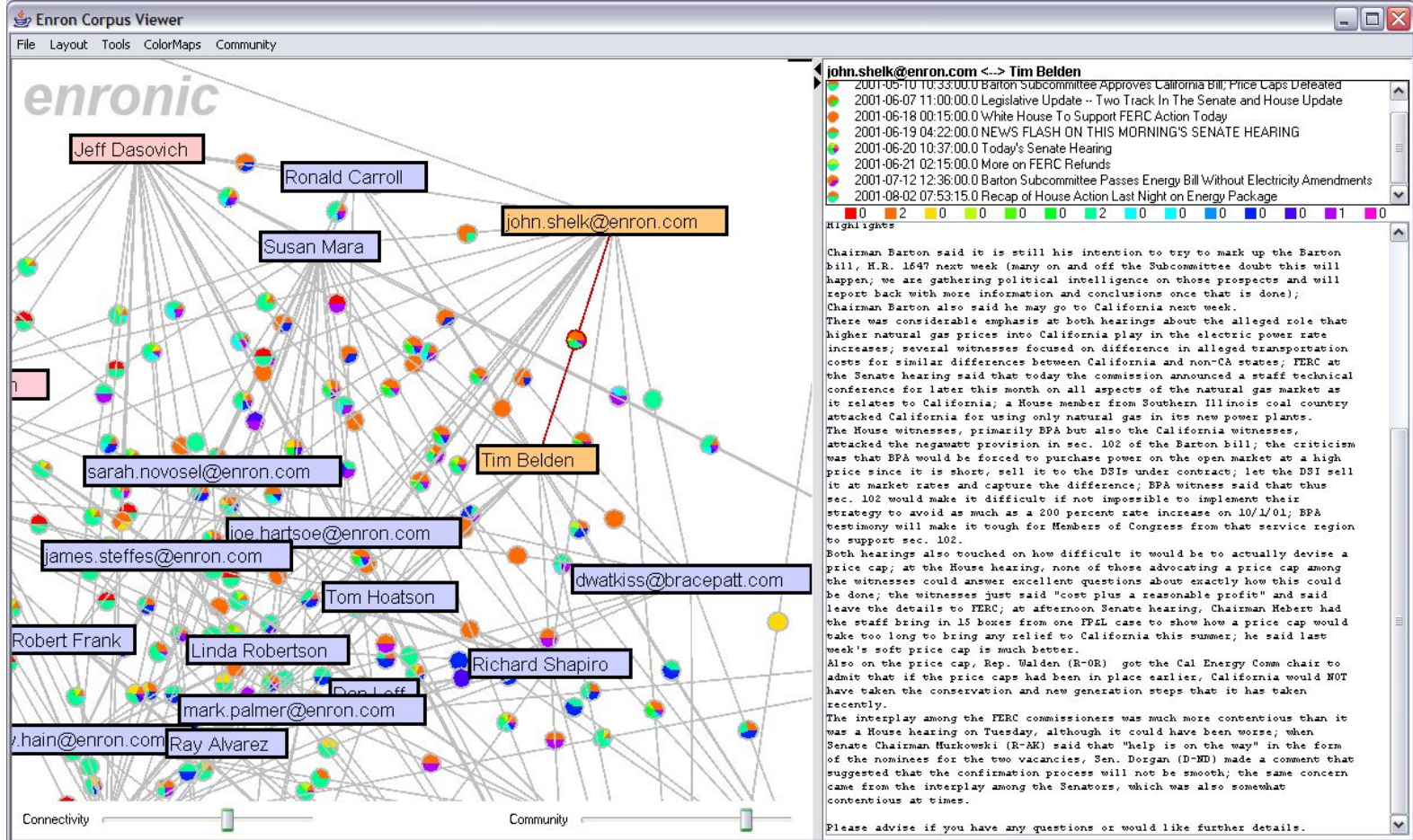
To: <kenneth.lay@enron.com>

Cc: Rosalee Fleming <rosalee.fleming@enron.com>

<susan.landwehr@enron.com>, <kevin.hannon@enron.com>, David

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



All one way emails to Tim Belden

Slides from Previous Years

Examining Email Headers

The diagram shows an email header in a browser window. The header text is as follows:

- 1. Return Path: <forensics@yahoo.com>
- 2. Delivered To: badguy@jailhouse.com
- 3. Received (gmail 12780 invoked by uid 0); 08 Dec 2015 08:23:37 -0000
- 4. Received from mail.jailhouse.com
- 5. Received from 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: 20121212082330.41000@jailhouse.com
- 7. Received from [10.187.241.199] 2015 00:23:30 PST

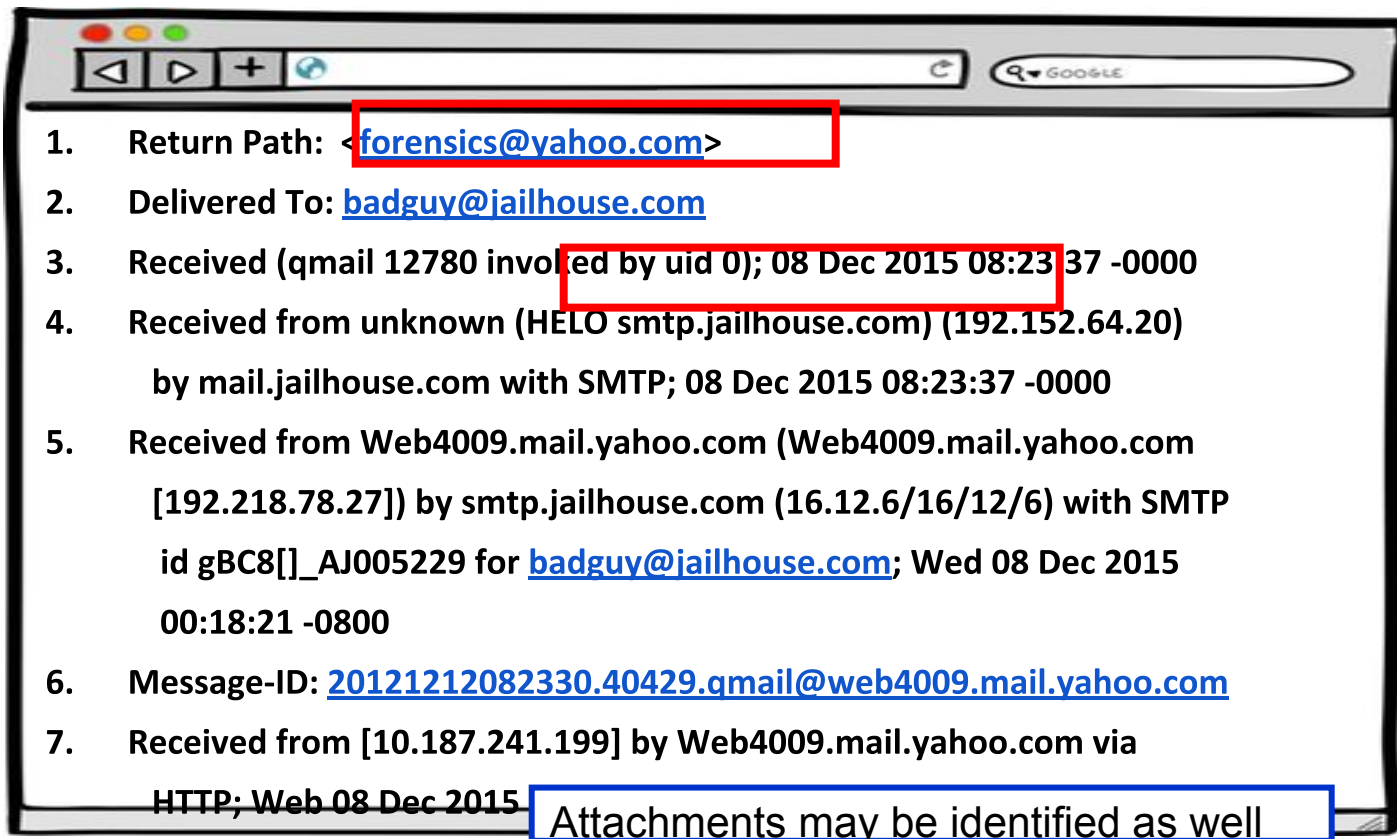
Callout boxes provide the following explanations:

- Return Path – easily spoofed
- Recipient's email address
- Identifies:
 - Name and IP address of sending email server
 - ID number (12780)
- Email servers through which this message
- Unique message number
- IP address of sending server and date/time sent

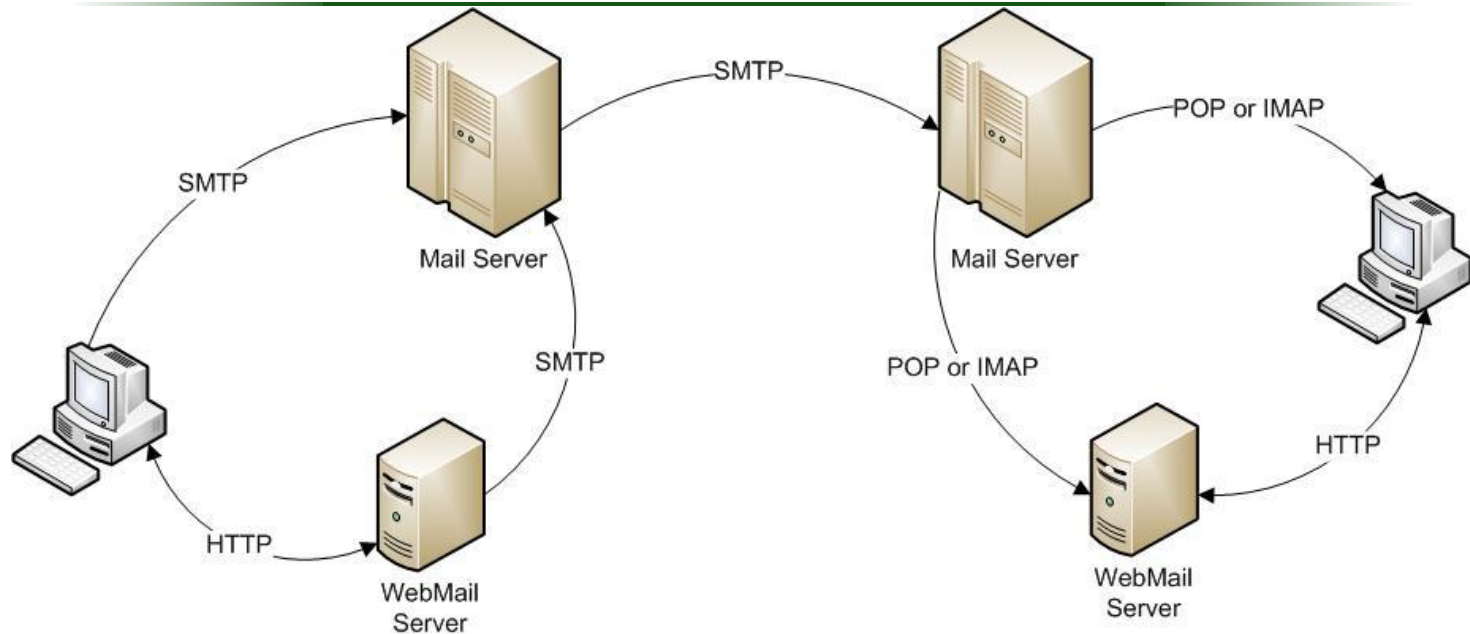
Additional header information shown at the bottom:

- Date: Wed, 08 Dec 2015 00:23:30 -0800
- MIME-Version: 1.0

Examining Email Headers



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

Exploring - mdbdata

File Edit View Tools Help

mdbdata

All Folders

(E:) (F:) (W:) Exchsrvr Deadata Mdbdata mldata

(Y:) exchsrvr Add-ins Address bin comdata Connect Deadata dadata inodata insdata Kmsdata mdbdata Mldata Res Tracking.log WebTemp Recycler

Contents of 'mdbdata'

Name	Size	Type	Modified	Attrib
edb.log	5.120KB	Text Document	9/22/98 11:54 AM	
edb00654.log	5.120KB	Text Document	9/21/98 6:12 AM	
edb00655.log	5.120KB	Text Document	9/21/98 8:52 AM	
edb00656.log	5.120KB	Text Document	9/21/98 10:18 AM	
edb00657.log	5.120KB	Text Document	9/21/98 10:21 AM	
edb00658.log	5.120KB	Text Document	9/21/98 11:12 AM	
edb00659.log	5.120KB	Text Document	9/21/98 12:45 PM	
edb0065A.log	5.120KB	Text Document	9/21/98 1:54 PM	
edb0065B.log	5.120KB	Text Document	9/21/98 3:24 PM	
edb0065C.log	5.120KB	Text Document	9/21/98 4:13 PM	
edb0065D.log	5.120KB	Text Document	9/21/98 5:28 PM	
edb0065E.log	5.120KB	Text Document	9/21/98 7:20 PM	
edb0065F.log	5.120KB	Text Document	9/21/98 7:59 PM	
edb00660.log	5.120KB	Text Document	9/21/98 9:04 PM	
edb00661.log	5.120KB	Text Document	9/21/98 10:43 PM	
edb00662.log	5.120KB	Text Document	9/22/98 12:58 AM	
edb00663.log	5.120KB	Text Document	9/22/98 1:25 AM	
edb00664.log	5.120KB	Text Document	9/22/98 4:00 AM	
edb00665.log	5.120KB	Text Document	9/22/98 7:28 AM	
edb00666.log	5.120KB	Text Document	9/22/98 9:58 AM	
edb00667.log	5.120KB	Text Document	9/22/98 10:58 AM	
edb00668.log	5.120KB	Text Document	9/22/98 11:54 AM	
res1.log	5.120KB	Text Document	6/16/98 1:35 PM	
res2.log	5.120KB	Text Document	6/16/98 1:35 PM	
tmp.edb	1.032KB	EDB File	9/18/98 5:00 PM	

26 object(s) 121MB (Disk free space: 3.65GB)

OpCode:
More Information: [EventLog Online Help](#)

Copy Close

Type Date Modified Attributes
Text Document 10/14/2005 8:53 PM A

stem Attendant version 6.5.7623.00#
stname Partner-Name Server-hostname
vent-ID MSGID Priority
umber-Recipients
ervice-version Linked-MSGID
14 18:53:52 GMT -
ERS/OU=FIRST ADMINISTRATIVE

on.nwtraders.msft 0 0
c=US;a= ;p=Northwind
Message Tracking Test EX:/O=NORTHWIND
RECIPIENTS/CN=ADMINISTRATOR -00
LONDON -
IVE GROUP/CN=RECIPIENTS/CN=Sean
466@London.nwtraders.msft 0
52 GMT 0 -
002005-10-14 18:53:53 GMT -
IND TRADERS/OU=FIRST ADMINISTRATIVE

on.nwtraders.msft 0 0
Exchange 0
0-14 18:53:53 GMT -
ERS/OU=FIRST ADMINISTRATIVE

on.nwtraders.msft 0 0
Exchange 0
0-14 18:53:53 GMT -
Ft 1033 -
on.nwtraders.msft 0 0
Exchange 0
raders.msft -002005-10-14

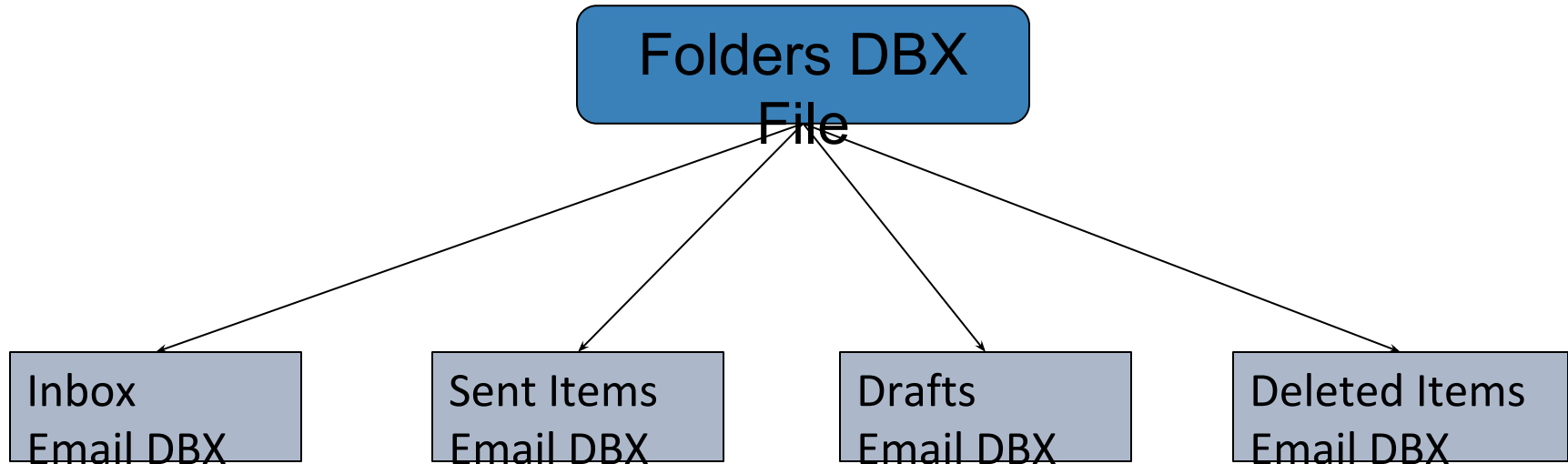
nt' to
stories
path

5-Exch/01.ExchangeShare.net/w3SVC/1/ROOT/owa/8.1.375.
Removing it.
Creating metabase entry
-Exch701.ExchangeShare.net/w3SVC/1/ROOT/owa/8.1.375.2
Configuring metabase entry

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

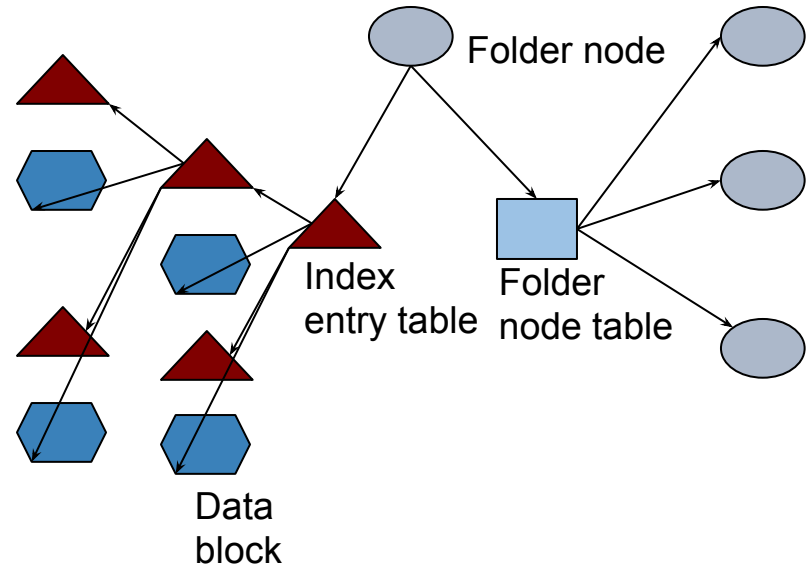
Outlook Express--Example



- 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