Digital Forensics

Module 3
CS 996
Review from Module #2

- Spam investigations
- Analyzing message headers
- Tools
  - NetScan Tools Pro
  - Sam Spade
  - Geolocation service (Quova)
- Methods to reduce spam
  - Legal—CANSPAM
  - Technical
- How to delete email on desktop
Sample IP Addresses: Geolocation

- **66.8.129.0/24**
  - Whois lookup: Roadrunner
  - Reverse DNS using Spade: cpe-66-8-129-1.hawaii.rr.com
  - Traceroute using Spade: fas1-0-kauihikheo-ubr1.hawaii.rr.com
    - Guess location: Kauihi is a stream on north shore of Honolulu; Kheo is manufacturer of kite boards
Traceroute to 66.8.129.0

1 10.125.216.1 100ms 10ms 10ms TTL: 0 (No rDNS)
2 67.83.229.161 10ms 10ms 10ms TTL: 0 (dstswrl-vlan2.rh.mmrnny.cv.net ok)
3 67.83.229.129 10ms 10ms 10ms TTL: 0 (r1-gell-1.mhe.whplny.cv.net ok)
4 65.19.120.17 10ms 10ms 10ms TTL: 0 (r1-srp1-0.cr.whplny.cv.net bogus rDNS)
5 65.19.120.2 10ms 10ms 10ms TTL: 0 (r2-srp5-0.wan.whplny.cv.net ok)
6 167.206.12.166 20ms 20ms 10ms TTL: 0 (r2-srp-5-0.wan.prnynj.cv.net ok)
7 65.19.96.56 10ms 20ms 20ms TTL: 0 (r2-srp5-0.in.nycmnyzr.cv.net ok)
8 65.19.97.194 30ms 30ms 30ms TTL: 0 (r1-pos3-0.in.chcgildt.cv.net ok)
9 65.19.100.130 40ms 30ms 30ms TTL: 0 (pop2-chi-P5-1.atdn.net bogus rDNS: host)
10 66.185.148.64 40ms 40ms 30ms TTL: 0 (bb1-chi-P1-0.atdn.net bogus rDNS: host)
11 66.185.152.125 50ms 50ms 50ms TTL: 0 (bb1-kcy-P7-0.atdn.net bogus rDNS: host)
12 66.185.152.127 50ms 40ms 50ms TTL: 0 (bb2-kcy-P1-0.atdn.net bogus rDNS: host)
13 66.185.152.188 60ms 60ms 50ms TTL: 0 (bb2-den-P7-0.atdn.net bogus rDNS: host)
14 66.185.152.136 60ms 60ms 61ms TTL: 0 (bb1-den-P1-0.atdn.net bogus rDNS: host)
15 66.185.152.253 80ms 90ms 80ms TTL: 0 (bb1-sun-P5-0.atdn.net bogus rDNS: host)
16 66.185.152.6 140ms 151ms 150ms TTL: 0 (bb1-hon-E2-2.atdn.net bogus rDNS: host)
17 66.185.137.65 151ms 140ms 140ms TTL: 0 (pop2-hon-P0-0.atdn.net bogus rDNS: host)
18 66.185.149.150 140ms 150ms 150ms TTL: 0 (RR-Mililani.atdn.net bogus rDNS: host)
19 24.25.225.254 140ms 150ms 160ms TTL: 0 (hnl-rdc-rtr-a.rdc-hawaii.rr.com ok)
20 66.8.160.37 150ms 160ms 161ms TTL: 0 (fas1-0-kauikhkeo-ubr1.hawaii.rr.com ok)
21 No Response * * *
22 No Response * * *
23 No Response * * *
24 No Response * * *
25 No Response * * *
Sample IP Address

- 24.112.120.0/25
  - Whois lookup: Rogers Cable, Toronto, CA
  - Reverse DNS: tlgw3.mtbo.phub.net.cable.rogers.com
  - Traceroute: reaches host
  - Google finds: mtbo = Bolton, ON
Overview of Module #3

- Email fraud
  - Analyze message headers
  - Outlook metadata
- Tony Blair’s Iraq dossier
  - Document metadata
- Investigations using concept search
- Email discovery in practice
Case of the $25M Email

- Signal Lake Venture Fund  
  - General Partner: Bart Stuck
- Suni Munshani, Independent Investor
- Terago Communications, Inc.  
  - President: Hemant Trivedi
- Munshani sues for $25M
- www.signallake.com/litigation
The August 3, 2000 Email

“Suni, the importance of keeping you excited about Terago is hard to overstate. As CEO and founder I am personally committing to deliver these warrants to you at the last round of funding. The period we discussed will be two years. Please let me manage this with Signal Lake. “ Regards, Hemant
Questionable Message Header

Return-Path: hemant_trivedi@terago.com
Received: from mail.terago.com (mail.terago.com [208.141.104.1])
  by hedgefund.ushedgefund.com (8.11.0/8.11.0) with ESMTP id
e73MfZ331592
  for suni@ushedgefund.com; Thu, 3 Aug 2000 15:45:31 -0400 (EDT)
Received: from webmail.terago.com (webmail.terago.com [10.0.1.8])
  by mail.terago.com (Switch-2.0.1/Switch-2.0.1) with ESMTP id
e73MfW903843;
  Thu, 3 Aug 2000 14:41:32 -0500 (CDT)
Received: from terago.com (ostrich.terago.com [10.0.20.18])
  by webmail.terago.com (8.8.8+Sun/8.8.8) with ESMTP id RAA01318;
  Thu, 3 Aug 2000 14:41:31 -0500 (CDT)
Message-ID: <3989e793.87BDEEE2@terago.com>
Comparator Message Header

Return-Path; hemant_trivedi@terago.com
Received: from mail.terago.com (mail.terago.com [208.141.104.1])
    by hedgefund.ushedgefund.com (8.11.0/8.11.0) with ESMTP id
    e73MfZ331592
    for suni@ushedgefund.com; Thu, 3 Aug 2000 18:41:35 -0400 (EDT)
Received: from webmail.terago.com (webmail.terago.com [10.0.1.8])
    by mail.terago.com (Switch-2.0.1/Switch-2.0.1) with ESMTP id
    e73MfW903843;
    Thu, 3 Aug 2000 17:41:32 -0500 (CDT)
Received: from terago.com (ostrich.terago.com [10.0.20.18])
    by webmail.terago.com (8.8.8+Sun/8.8.8) with ESMTP id RAA01318;
    Thu, 3 Aug 2000 17:41:31 -0500 (CDT)
Message-ID:  <3989F5A3.87BDEEE2@terago.com>
<table>
<thead>
<tr>
<th>SERVER</th>
<th>ESMTP ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>hedgefund.ushedgefund.com</td>
<td>e73MfZ331592</td>
</tr>
<tr>
<td>mail.terago.com</td>
<td>e73MfW903843</td>
</tr>
<tr>
<td>webmail.terago.com</td>
<td>RAA01318</td>
</tr>
</tbody>
</table>
## SMTP Server Transmission Times

<table>
<thead>
<tr>
<th>SERVER</th>
<th>ESMTP ID</th>
<th>TRANSMISSION TIME: QUESTIONED MESSAGE</th>
<th>TRANSMISSION TIME: COMPARATOR MESSAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>hedgefund.ushedgefund.com</td>
<td>e73MfZ331592</td>
<td>15:45:31 (EDT)</td>
<td>18:41:35 (EDT)</td>
</tr>
<tr>
<td>mail.terago.com</td>
<td>e73MfW903843</td>
<td>14:41:32 (CDT)</td>
<td>17:41:32 (CDT)</td>
</tr>
<tr>
<td>webmail.terago.com</td>
<td>RAA01318</td>
<td>14:41:31 (CDT)</td>
<td>17:41:31 (CDT)</td>
</tr>
</tbody>
</table>
Investigating Outlook Metadata

Inbox - Microsoft Outook

View Summary

Fields... Importance, Icon, Flag Status, Attachment, From, S...
Group By... None
Sort... Received (descending)
Filter... Off
Other Settings... Fonts and other Table View settings
Automatic Formatting... User defined fonts on each message

Show Fields

Available fields:
- Auto Forwarded
- Bcc
- Billing Information
- Categories
- Cc
- Changed By
- Contacts
- Conversation
- Defer Until
- Do Not AutoArchive
- Due By
- E-mail Account
- Expires
- Follow Up Flag

Select available fields from:
All Mail Fields

Show these fields in this order:
- Importance
- Flag Status
- Attachment
- From
- Subject
- Received
- Size
- Created
- Read
- Modified
As Fred mentions, until recently I was with Avaya; before that Dell and Exxon. I would enjoy getting together when you have a few minutes and
Timeline of Events

- August 3, 2000: Message transmission
- December 18, 2000: Munshani files $25M lawsuit
- December 19, 2000: Message creation date in Munshani’s .pst file
- Conclusion??
Result

- Email to Munshani determined to be fraudulent
- Judge dismisses his case
- New case March 2003
  - US v. Munshani
  - Obstruction of justice
  - Criminal contempt of court
Takeaways from Munshani Case

- Necessary to save emails
  - Retention policy
  - Other party may save the evidence
  - Court may order email discovery

- Consider digital IDs
  - Include disclaimer
  - Verisign digital ID
MetaData in Documents

- Revision history
- Document authors
- Document changes
- Custom fields that you may have added!

- Use in investigations
- Eliminate from documents sent outside organization!
Case Study: Tony Blair’s Iraq Intelligence Dossier

- Presented as intelligence document to help justify war: February, 2003
- Word doc posted on: www.number-10.gov.uk/
- Investigation showed that US grad student—Ibrahim al-Marashi--wrote it!
- Metadata analysis: document edited by junior staffers!
- Reference: www.computerbytesman.com
Metadata Analysis of Iraq Dossier

- Rev #1: cic22\phamill edited file
- Rev #2: cic22\phamill edited file
- Rev #3: cic22\phamill edited file
- Rev. #4: JPratt edited file
- Rev. #5: JPratt edited file
- Rev. #6: abblackshaw edited file
- Rev. #7: abblackshaw edited file
- Rev. #8: MKhan edited file
- Rev. #10: MKhan edited file
Who Are These Guys?

- Paul Hamill - Foreign Office official
- John Pratt – Downing Street official
- Alison Blackshaw – press secretary’s personal assistant
- Murtaza Khan – junior press officer

No one with any intelligence background!
Result: Parliamentary investigation!!
Search Methods

- Why need for better methods?
  - 40GB hard drive = 1000 boxes of paper = 2 million pages

- Key word search: tried and true
- Boolean (security AND forensics)
- Concept Search
  - Retrieve document relevant to topic
  - Process: index; search
<table>
<thead>
<tr>
<th>Date</th>
<th>Relevancy</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 10, 2003</td>
<td><img src="image" alt="Relevancy" /></td>
</tr>
<tr>
<td>December 3, 2003</td>
<td><img src="image" alt="Relevancy" /></td>
</tr>
<tr>
<td>August 12, 2003</td>
<td><img src="image" alt="Relevancy" /></td>
</tr>
<tr>
<td>December 1, 2003</td>
<td><img src="image" alt="Relevancy" /></td>
</tr>
</tbody>
</table>
Concept Search Vendors

- DolphinSearch (www.dolphinsearch.com)
- Platformedia (www.platformedia.com)
- WizSoft (www.wizsoft.com)
Restoring Deleted Email

- Client side restoration
- Mail deleted from delete folder; not compacted
- Paraben Email Examiner (free download)
  - Does every format except .pst
- Include key word search
<table>
<thead>
<tr>
<th>UTC</th>
<th>Who</th>
<th>E-Mail Address</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000/07/12 09:21</td>
<td>{Frederick Scholl}</td>
<td><a href="mailto:freds@monarch-info.com">freds@monarch-info.com</a></td>
<td>{Testing}</td>
</tr>
<tr>
<td>2000/08/15 08:03</td>
<td>{Frederick Scholl}</td>
<td><a href="mailto:freds@monarch-info.com">freds@monarch-info.com</a></td>
<td>{Testing}</td>
</tr>
<tr>
<td>2000/08/17 08:10</td>
<td>{Frederick Scholl}</td>
<td><a href="mailto:freds@monarch-info.com">freds@monarch-info.com</a></td>
<td>{mykeynote}</td>
</tr>
<tr>
<td>2000/08/23 10:49</td>
<td>{Frederick Scholl}</td>
<td><a href="mailto:freds@monarch-info.com">freds@monarch-info.com</a></td>
<td>{}</td>
</tr>
<tr>
<td>2000/08/23 11:38</td>
<td>[No Name]</td>
<td>[No Address]</td>
<td></td>
</tr>
<tr>
<td>2000/08/24 10:15</td>
<td>[No Name]</td>
<td>[No Address]</td>
<td></td>
</tr>
<tr>
<td>2002/05/30 20:46</td>
<td>Christie Cooney</td>
<td><a href="mailto:gotocustomercare@expertcity.com">gotocustomercare@expertcity.com</a></td>
<td>Set Up GoToMyPC</td>
</tr>
<tr>
<td>2002/10/19 09:49</td>
<td>[No Name]</td>
<td>[No Address]</td>
<td></td>
</tr>
<tr>
<td>2002/12/09 14:21</td>
<td>{Frederick Scholl}</td>
<td><a href="mailto:freds@monarch-info.com">freds@monarch-info.com</a></td>
<td>{Re: Network Forensics}</td>
</tr>
<tr>
<td>2003/02/19 09:17</td>
<td>{Frederick Scholl}</td>
<td><a href="mailto:freds@monarch-info.com">freds@monarch-info.com</a></td>
<td>{Fw: Rules Scenarios - Intellitactics NSM}</td>
</tr>
<tr>
<td>2003/02/19 09:18</td>
<td>{Frederick Scholl}</td>
<td><a href="mailto:freds@monarch-info.com">freds@monarch-info.com</a></td>
<td>{Fw: Intellitactics Technical White Paper}</td>
</tr>
<tr>
<td>2003/02/19 09:35</td>
<td>{Frederick Scholl}</td>
<td><a href="mailto:freds@monarch-info.com">freds@monarch-info.com</a></td>
<td>{Fw: Firewall performance}</td>
</tr>
<tr>
<td>2003/02/24 19:34</td>
<td>{Frederick Scholl}</td>
<td><a href="mailto:freds@monarch-info.com">freds@monarch-info.com</a></td>
<td>{Re: Whitepaper}</td>
</tr>
<tr>
<td>2003/04/07 09:46</td>
<td>{Frederick Scholl}</td>
<td><a href="mailto:freds@monarch-info.com">freds@monarch-info.com</a></td>
<td>{Fw: }</td>
</tr>
<tr>
<td>2003/04/09 10:08</td>
<td>{Frederick Scholl}</td>
<td><a href="mailto:freds@monarch-info.com">freds@monarch-info.com</a></td>
<td>{Re: Fw: LOOKING For Love? Find LOVE here}</td>
</tr>
<tr>
<td>2003/04/14 11:34</td>
<td>{Frederick Scholl}</td>
<td><a href="mailto:freds@monarch-info.com">freds@monarch-info.com</a></td>
<td>{Re: NDA}</td>
</tr>
<tr>
<td>2003/04/16 18:33</td>
<td>{Frederick Scholl}</td>
<td><a href="mailto:freds@monarch-info.com">freds@monarch-info.com</a></td>
<td>{Re: Introduction}</td>
</tr>
<tr>
<td>2003/04/17 21:45</td>
<td>{Frederick Scholl}</td>
<td><a href="mailto:freds@monarch-info.com">freds@monarch-info.com</a></td>
<td>{Re: Follow up on Forensic Auditing}</td>
</tr>
<tr>
<td>2003/04/19 06:26</td>
<td>{Frederick Scholl}</td>
<td><a href="mailto:freds@monarch-info.com">freds@monarch-info.com</a></td>
<td>{Re: Renew Your LES Membership}</td>
</tr>
<tr>
<td>Date</td>
<td>From</td>
<td>Subject</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------</td>
<td>-----------------------</td>
<td></td>
</tr>
<tr>
<td>2003/09/11 01:19</td>
<td>Bergstrom, Len (1)</td>
<td>RE: Friday Lunch Date</td>
<td></td>
</tr>
<tr>
<td>2003/01/03 16:14</td>
<td>Donald Don Smith (1)</td>
<td>Get together</td>
<td></td>
</tr>
</tbody>
</table>

Hi Fred:

Boxing Cat was fine with me. I can make it any time after 12 noon on the Friday 9/19. Do you want to make the reservation or should I? Might bring an associate so make it for 3. This way you will have someone on this continent to follow up with!

Cheers,
Len

-----Original Message-----
From: Frederick Sc???? [mailto:freds@monarch-info.com]
Sent: Tuesday, September 09, 2003 9:13 AM
To: Bergstrom, Len
Subject: RE: Friday Lunch Date
Email Discovery in Litigation

THE LEGAL PROCESS

DIGITAL FORENSICS

ELECTRONIC DISCOVERY

LITIGATION SUPPORT
Three approaches to collecting e-mail evidence

- “Litigation support”
  - Older method for non-electronic evidence
  - Paper documents: scan, OCR, search
  - Still needed for paper based evidence
E-mail evidence collection, cont.

- “Electronic Discovery”
  - Integrating information from diverse platforms
  - Live or active data: don’t need file restoration process
  - De-duplicating records
  - Transfer to one searchable database
  - Focuses on collecting, not analyzing data

- “Digital Forensics”
  - Recovering hidden information
  - Need bit by bit replica of media
  - Collecting and analyzing data
New Discovery Rules for E-Mail

- US District Court for Southern District
- Why is this case important
  - Set new guidelines for cost sharing
  - Illustrates difficulties with e-mail evidence
- [http://www.nysd.uscourts.gov/rulings/02cv1243_051803.pdf](http://www.nysd.uscourts.gov/rulings/02cv1243_051803.pdf)
Zubulake Facts

- **1999**: Laura Zubulake hired on Asian Equities Desk
- **2002**: Filed gender discrimination suit for $15M
- Requested all UBS communications concerning her, including e-mail
- UBS filed motion asking that court order Zubulake to pay for this discovery
UBS E-Mail System

- HP OPENMAIL
- TRADING DESK
- OPTICAL DISK BACKUP OF ALL EXTERNAL EMAIL FOR REGISTERED TRADERS
- VERITAS NETBACKUP DAILY, WEEKLY, MONTHLY TAPE BACKUP
Judge Scheindlin’s Decisions

- Set new rulings on cost-shifting
- In general, responding party must pay for discovery
  - Protects individual plaintiffs
  - Judge created new 7 part test for cost sharing
  - Allocated 75% of cost to UBS; 25% to plaintiff
- Ruled UBS negligent for losing tapes and deleting emails
New Archiving Solutions

- 7000 arbitration suits filed per year against brokerage firms!
- Traditional periodic mail backup may lose some messages when they are deleted
- Backup tapes may be lost
- Financial industry: email and IM must be saved for 3-6 years (SEC Rule 17a-4)
Zantaz Email Archiving

- All messages forwarded
- VPN connection
- Index for all messages
- Live, online data
- Can be reviewed through web browser
Takeaways from Module #3

- Know how to do geolocation using Sam Spade and Google
- Know how to read email message headers
- Understand how to find metadata
- Understand how to recover deleted email
- Understand problems and solutions for email archiving