Forensically Speaking

Security Camp

August 2011

BOSTON UNIVERSITY

Who are you?

- Quinn Shamblin
  - CISM, CISSP, GIAC-GCFA, PMP
  - Executive Director of Information Security
  - Boston University
  - qrs@bu.edu
  - 617 358-6310

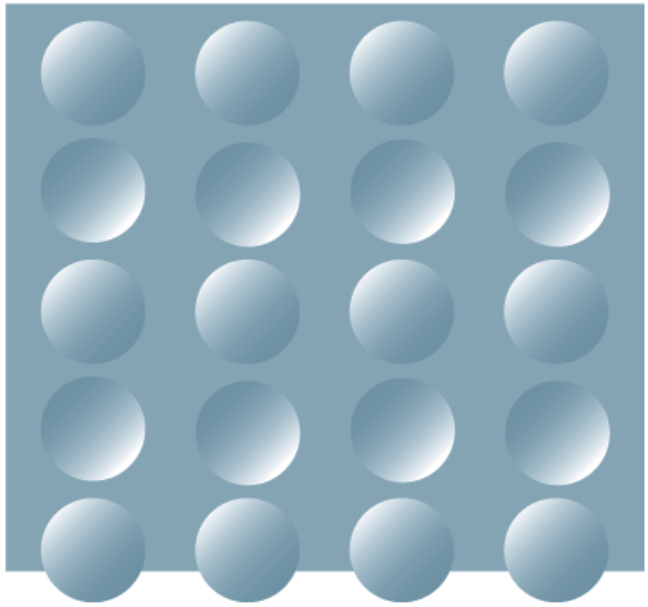
BOSTON UNIVERSITY

Common Cases in Higher Ed

- User account compromise
- Malware infections
- Breach analysis – Data exfiltration analysis
- Policy violations
  - Misuse of resources, theft of time, professionalism, research misconduct,
- Litigation holds
- Termination holds
- Criminal investigations
  - Fraud, stalking, more…

In-sourcing vs. out

- Suspicion vs knowledge
- OpSec
- Resources
- Training/experience
- Contract negotiations
- Cost




43
5.6

The question is…

"What is the total number of hard drives and total Terabytes of data that can be gathered covertly by a single investigator over a period of 11 hours when the right tools are available?", Alex.

And the proper tools are?

- It depends on a lot of factors.

Evidence Collection Process

- Request from authorized authority
- Need to know, covert action or overt?
- Surveillance of the scene
- Record the scene with a camera
- Memory capture
- Pull power and remove hard drive, image
- Replace hard drive, boot test, compare scene to photo, leave

To misquote a movie…

- “Passwords? We don’t need no stinkin’ passwords!”

- Usually…

Mitigations

- Memory imaging
- Network sniffing
- Network imaging
- Backtrack
- Metasploit
- Pictures of the scene
- Subject interviews
- Key Loggers
  - Specter Pro
  - Evil Maid Attack

Managing Expectations

- “What did you find out?”
  - Getting the image was just step 1…
  - Step 2: Automated processing
  - Step 3: Human analysis and reporting

- Modern storage devices contain massive storage.
  - People don’t understand what a terabyte is…

BOSTON UNIVERSITY

OK, so how much is a Terabyte?

- 1 Terabyte = 10^{12} Bytes
- With traditional binary approach:
  - 1,099,511,627,776 bytes or 2^{40} bytes
- If the thickness of a piece a paper is 1 byte…

Another thing…

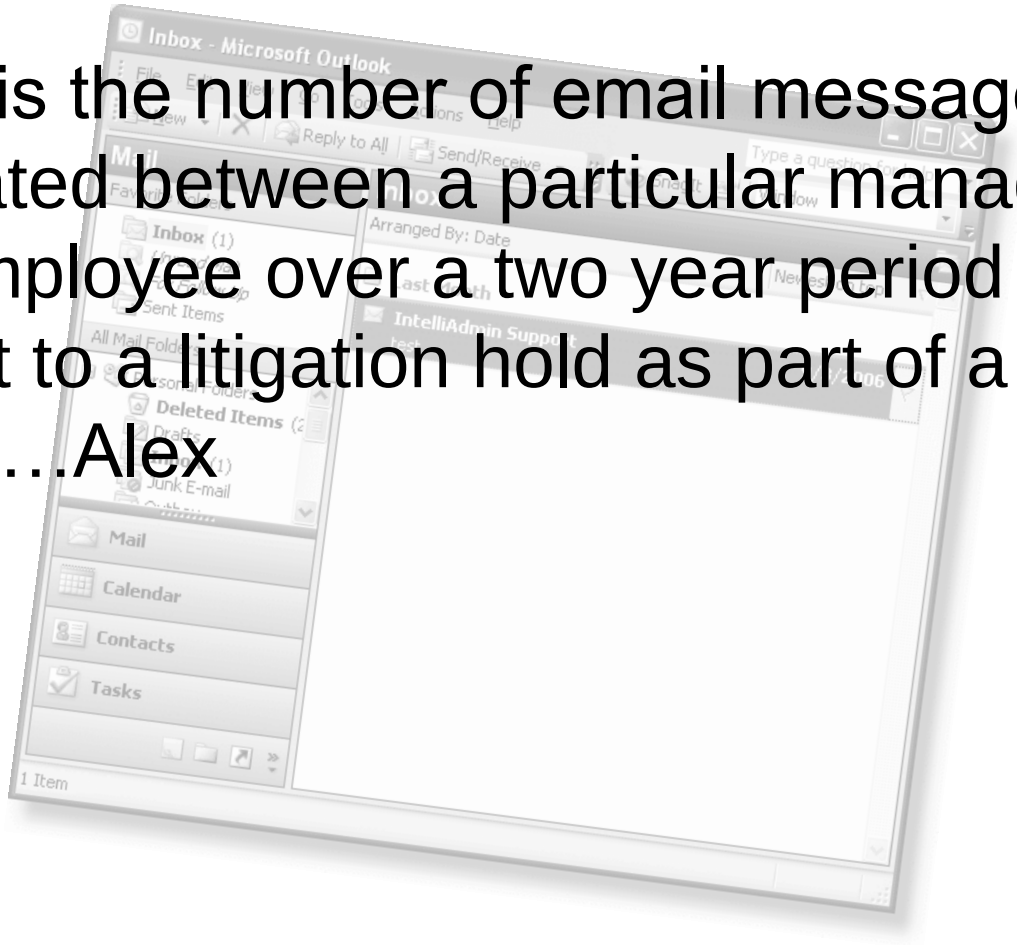
- People don't understand the shear volume of email that is generated in a modern workplace…

68,792

BOSTON UNIVERSITY

68,792

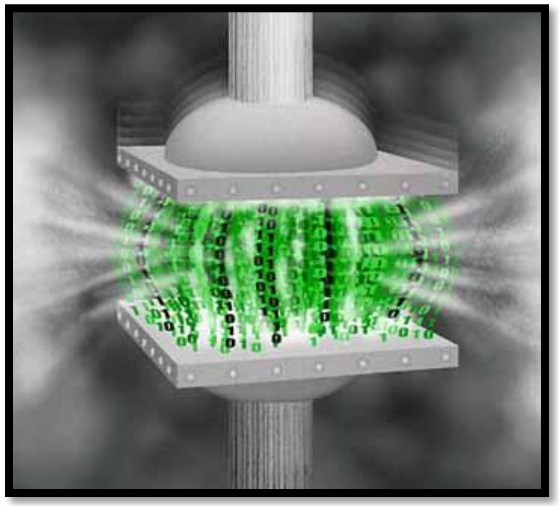
- “What is the number of email messages generated between a particular manager and one employee over a two year period and are subject to a litigation hold as part of a civil suit?” …Alex



BOSTON UNIVERSITY

Long term email collection

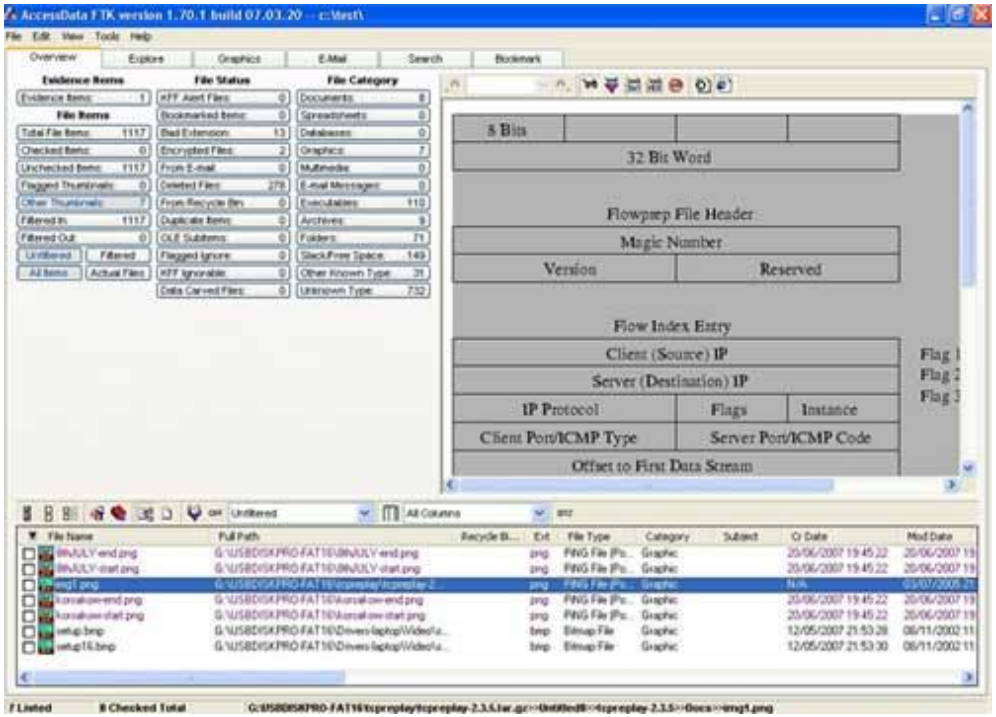
- Litigation hold requiring 10GB/day



- Email archival and journaling software

BOSTON UNIVERSITY

Automated Processing



Human Review and Analysis

Linux-based approaches

- Good tool sets and capabilities
  - Timelines
- Extremely flexible
- Low/no cost
- Less automation

BOSTON UNIVERSITY

Linux Tools

- cert.org tools
- Open Source Forensics
- Linux-Forensics
- SANS Investigative Forensic Toolkit – SIFT
- Helix
- Knoppix Security Tool Distribution

- Forensics Wiki Tools

Non-linux approaches

- Advantages
  - Greater automation
  - Accelerated human review (graphic, strings index)
  - Templates
- Popular Tool Suites
  - Access Data Forensic Toolkit
  - Encase
  - Blackbag Technologies
  - http://www.forensicswiki.org/wiki/Tools

Forensically Speaking…

- Time is your most important asset
- The right tools for the job
- Choose your toolset to fit your need, to save you time

BOSTON UNIVERSITY

Calculations

	0.1	thickness in mm		
	1099511627776.00	bytes per Terabye	Terabytes	
	109951162777.60	distance of 1 TB in mm		
1000	109951162.78	distance in m		
1000	109951.16	in km		
40,075.02	2.74	number of times around the earth for 1 TB		
5.6	15.36	number of times around the earth for 5.6 TBs		