

Forensically Speaking

Security Camp

August 2011



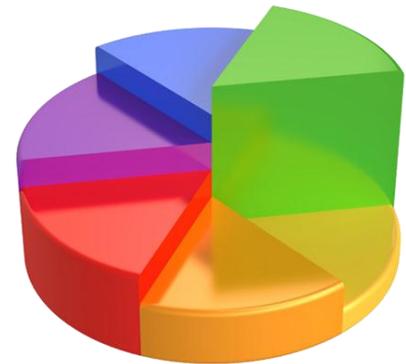
Who are you?

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



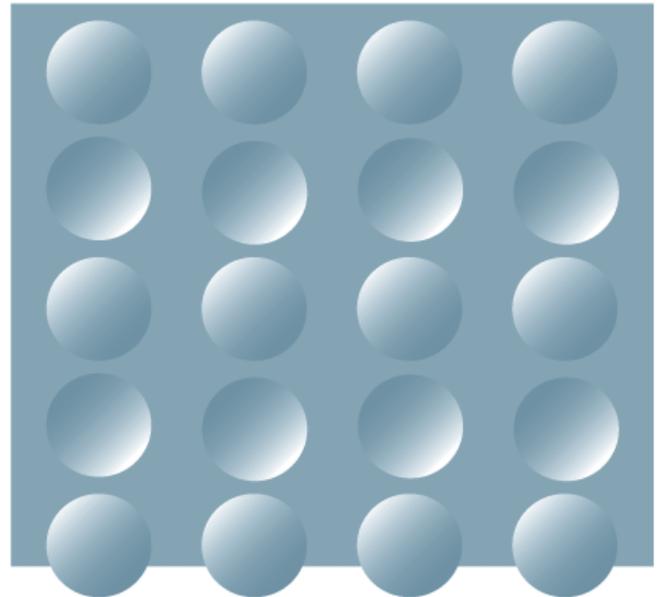
Common Cases in Higher Ed

- 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

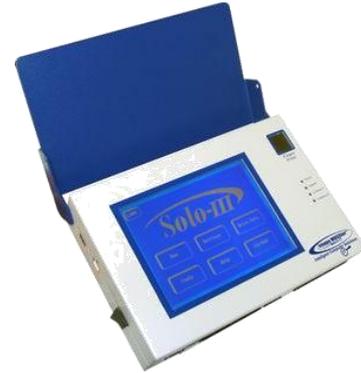


The question is...

“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

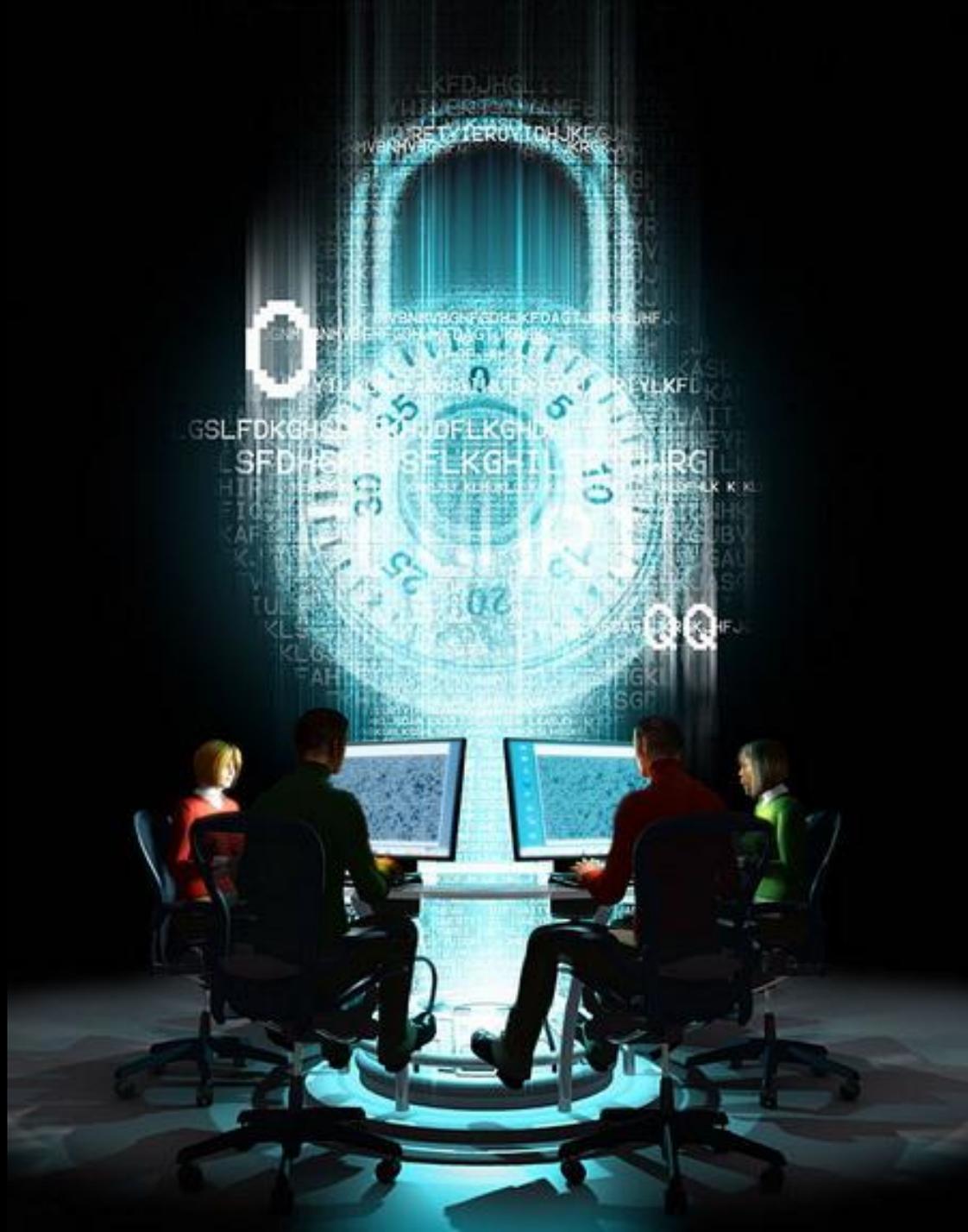
- Request from authorized authority
- Need to know, covert action or overt?
- Surveillance of the scene
- Record the scene with a camera
- Memory capture
- Pull power and remove hard drive, image
- Replace hard drive, boot test, compare scene to photo, leave

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...

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...

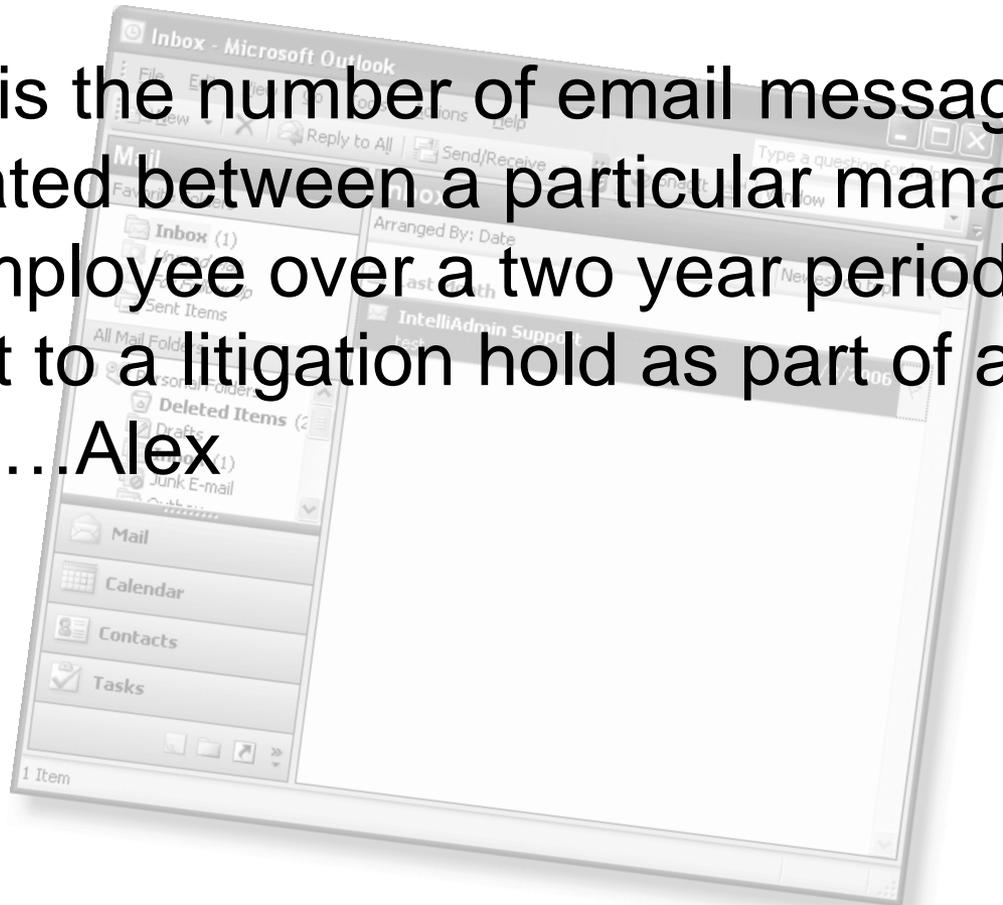
- People don't understand the sheer volume of email that is generated in a modern workplace...

68,792



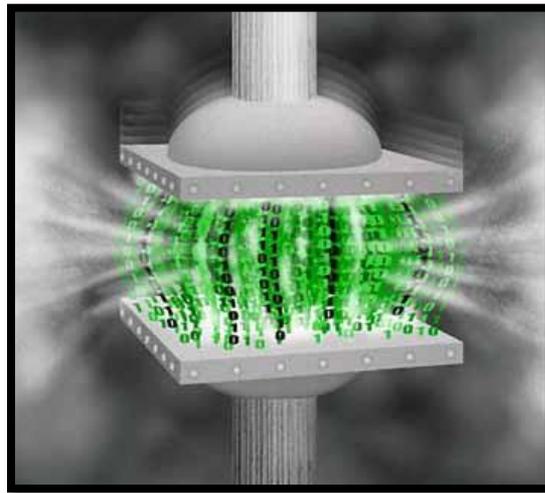
68,792

- “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



Long term email collection

- Litigation hold requiring 10GB/day



- Email archival and journaling software

Automated Processing



AccessData FTK version 1.70.1 build 07.03.20

File Edit View Tools Help

Overview Explorer Graphics E-Mail Search Bookmark

Evidence Items		File Status		File Category	
Evidence Items: 1	FTF Alert Files: 0	Documents: 8			
File Items	Bookmarked Items: 0	Spreadsheets: 0			
Total File Items: 1117	Bad Extension: 13	Databases: 0			
Checked Items: 0	Encrypted Files: 2	Graphics: 7			
Unchecked Items: 1117	From E-mail: 0	Multimedia: 0			
Flagged Thumbnails: 0	Deleted Files: 272	E-mail Messages: 0			
Other Thumbnails: 7	From Recycle Bin: 0	Executables: 110			
Filtered In: 1117	Duplicate Items: 0	Archives: 8			
Filtered Out: 0	OLE Subitems: 0	Folders: 71			
Unfiltered: 1117	Flagged Ignore: 0	Stack/Free Space: 149			
All Items: Actual Files	FTF Ignorable: 0	Other Known Type: 31			
	Data Carved Files: 0	Unknown Type: 752			

8 Bits

32 Bit Word

Flowprep File Header

Magic Number

Version Reserved

Flow Index Entry

Client (Source) IP

Server (Destination) IP

IP Protocol Flags Instance

Client Port/ICMP Type Server Port/ICMP Code

Offset to First Data Stream

File Name	Full Path	Recycle Bin	Ext	File Type	Category	Subject	O Date	Mod Date
img1-end.png	G:\USBDRKPRO-FAT16\img1-end.png		.png	PNG File (P...	Graphic		20/06/2007 19:45:22	20/06/2007 19:45:22
img1-start.png	G:\USBDRKPRO-FAT16\img1-start.png		.png	PNG File (P...	Graphic		20/06/2007 19:45:22	20/06/2007 19:45:22
img1.png	G:\USBDRKPRO-FAT16\img1.png		.png	PNG File (P...	Graphic		20/06/2007 19:45:22	20/06/2007 19:45:22
img2-end.png	G:\USBDRKPRO-FAT16\img2-end.png		.png	PNG File (P...	Graphic		20/06/2007 19:45:22	20/06/2007 19:45:22
img2-start.png	G:\USBDRKPRO-FAT16\img2-start.png		.png	PNG File (P...	Graphic		20/06/2007 19:45:22	20/06/2007 19:45:22
img1K.bmp	G:\USBDRKPRO-FAT16\img1K.bmp		.bmp	Bitmap File	Graphic		12/05/2007 21:53:28	06/11/2002 11:00:00
img2K.bmp	G:\USBDRKPRO-FAT16\img2K.bmp		.bmp	Bitmap File	Graphic		12/05/2007 21:53:30	06/11/2002 11:00:00

F Listed 8 Checked Total G:\USBDRKPRO-FAT16\img1\preplay\preplay-2.3.1\w.gr\Unfiltered\preplay-2.3.5\docs\img1.png

Human Review and Analysis



Linux-based approaches

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



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

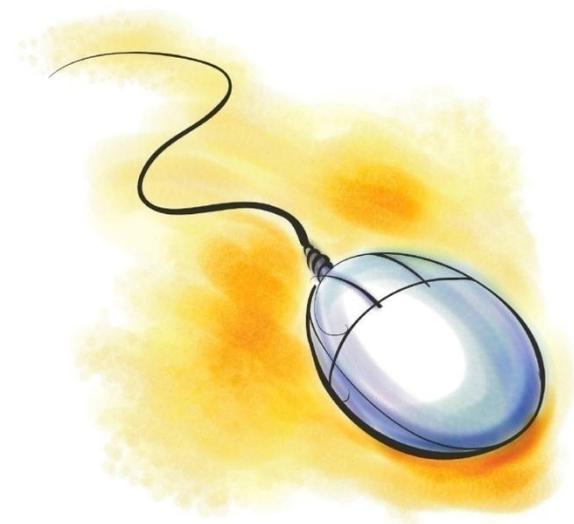
- Advantages
 - Greater automation
 - Accelerated human review (graphic, strings index)
 - Templates
- Popular Tool Suites
 - Access Data Forensic Toolkit
 - Encase
 - Blackbag Technologies
 - <http://www.forensicswiki.org/wiki/Tools>

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







Calculations

	0.1	thickness in mm		
	1099511627776.00	bytes per Terabyte	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		