When tapes go missing.....

"It is important for customers to note that these tapes cannot be read without specific computer equipment and software."

"The missing tapes require a tape drive to be read, and cannot be viewed from a PC"

"The administration continues to maintain that it does not believe the information has been accessed because it would require specific hardware, software and expertise."

Robert Stoudt

IBM-ISS
RStoudt@us.ibm.com

Game Time

“It is important for customers to note that these tapes cannot be read without specific computer equipment and software.”

President & CEO Hortica Robert McClellan

“The missing tapes require a tape drive to be read, and cannot be viewed from a PC”

IBM spokesman Fred McNeese

“.... continues to maintain that it does not believe the information has been accessed because it would require specific hardware, software and expertise.”

Ohio State "The administration"

When tapes go missing..... Agenda

- Reported cases in the media
- Cost of losing media
- Data Breach Laws
- Recovering the data
- Protecting Your Media

'Reported' cases of lost media

- ***July 4, 2007 – Ohio – 400,000 State employees, Taxpayers, Schools,...***
- ***Apr. 6, 2007 – Hortica – SSN, DL, Bank Acc***
- ***May 15, 1007 – IBM – SSN, DOB, Addresses***
- ***Jan. 19, 2007 – U.S. IRS via City of Kansas City – 26 tapes.....***
- ***Sept. 7, 2006 – Circuit City and Chase – 2.6 million cardholders***
- ***June 6, 2005 – CitiFinancial – 3,900,000***

**** http://www.privacyrights.org/ar/ChronDataBreaches.htm***

At what COST

- Impact to the company:
  - trade secrets
  - confidential financial information
  - customer data
  - employee data
  - company image
- Civil Damages
  - Tech//404® Data Loss Cost Calculator
    - examples given ranging from $1,000-$21,000 pp
    - http://www.tech-404.com/calculator.html

Case in point - Ohio

- Akron Beacon Journal - Stolen tape
  - The state is paying more than $700,000 to provide all state employees with identity-theft protection services and to hire an independent computer expert to review what data the tape contained.
  - Tape stolen June 10 from unlocked car of a intern “who had been designated to take the backup device home as part of a **standard security procedure**”.
  - ***"The administration continues to maintain that it does not believe the information has been accessed because it would require specific hardware, software and expertise.”***

http://www.ohio.com/mld/beaconjournal/news/state/17395223.htm

Losing the tapes

- Theft
- Lost in Transit
- End of Life/Discarding media
  - Ebay
  - Corporate auctions
  - Dumpster Diving

Case study

- Out of 20 DLT tapes purchased from various vendors on e-bay
  - 1 physically damaged
  - 2 data unreadable due to hardware
  - 5 were short erased
  - 12 were corporate backups
- Do you securely erase your data?
- Do you securely DESTROY your tapes?

Data Breach Notification Laws:

Disclaimer: I am not a lawyer nor do I wish to be one. Consult your legal counsel.

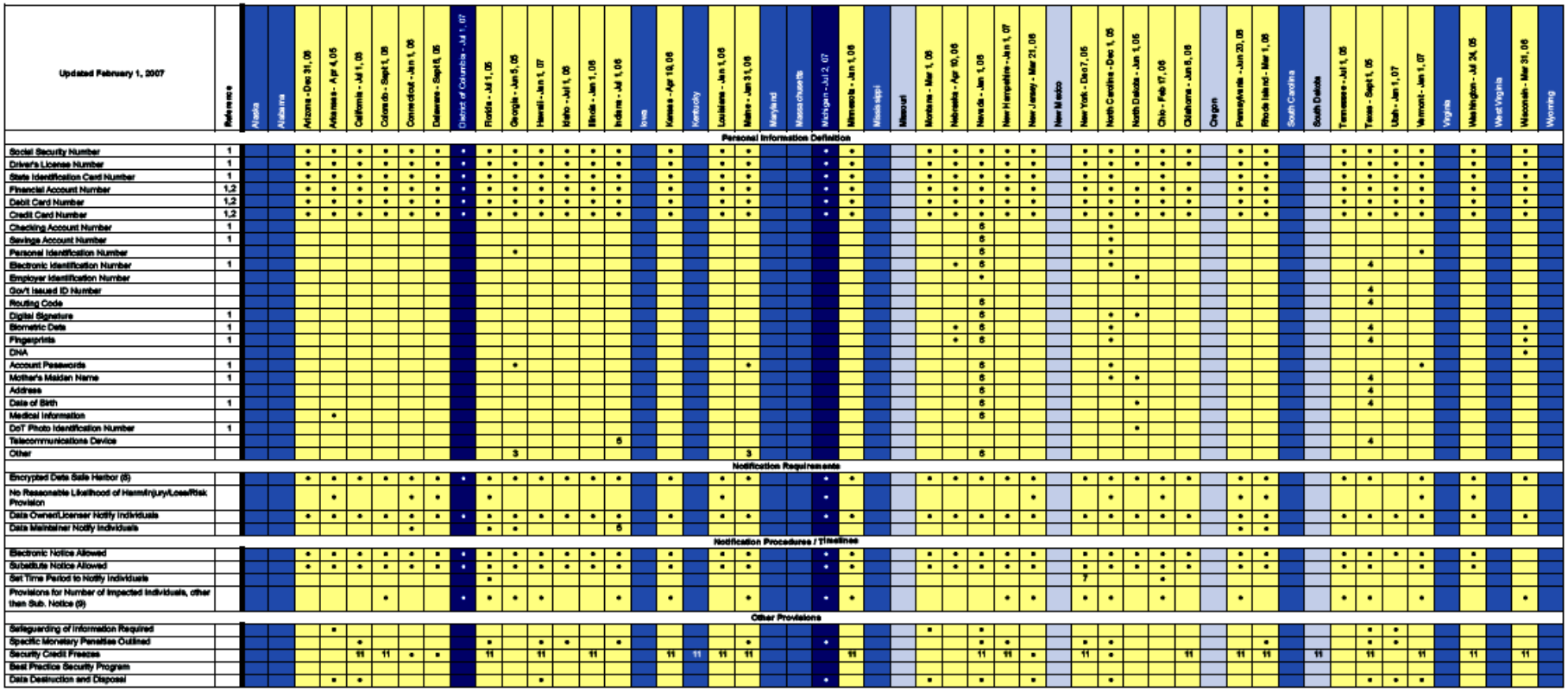
US State Laws

- Each state which has a Data Breach law can define:
  - What constitutes personal data
    - Name, Address, SSN, CC, Biometrics, Driver Lic num, account num,..... or a combination thereof
  - Encryption exemption (even poor encryption?)
  - Obfuscated data exempted
  - Timelines for notifications
  - Allowed methods of notification
- VigilantMinds has summarized laws as of Feb `07 by state at:
  http://www.solutionary.com/pdfs/vm/breach_matrix_feb07_email.pdf

VigilantMinds Law Matrix

VIGILANTMINDS

Security Breach Disclosure Law Matrix By State



Updated February 1, 2007	Reference	Alaska	Alabama	Arizona - Dec 31, 06	Arkansas - Apr 4, 05	California - Jul 1, 03	Colorado - Sept 1, 06	Connecticut - Jan 1, 06	Delaware - Sept 9, 05	District of Columbia - Jul 1, 07	Florida - Jul 1, 05	Georgia - Jan 5, 05	Hawaii - Jan 1, 07	Idaho - Jul 1, 05	Illinois - Jan 1, 06	Indiana - Jul 1, 06	Iowa	Kansas - Apr 19, 06	Kentucky	Louisiana - Jan 1, 06	Maine - Jan 31, 06	Maryland	Massachusetts	Michigan - Jul 2, 07	Minnesota - Jan 1, 06	Mississippi	Missouri	Montana - Mar 1, 06	Nebraska - Apr 10, 06	Nevada - Jan 1, 06	New Hampshire - Jan 1, 07	New Jersey - Mar 21, 06	New Mexico	New York - Dec 7, 05	North Carolina - Dec 1, 05	North Dakota - Jan 1, 06	Ohio - Feb 17, 06	Oklahoma - Jan 5, 06	Oregon	Pennsylvania - Jun 20, 05	Rhode Island - Mar 1, 06	South Carolina	South Dakota	Tennessee - Jul 1, 05	Texas - Sept 1, 05	Utah - Jan 1, 07	Vermont - Jan 1, 07	Virginia	Washington - Jul 24, 05	West Virginia	Wisconsin - Mar 31, 06	Wyoming
Personal Information Definition																																																			
Social Security Number	1			•	•	•	•	•	•	•	•	•	•	•	•	•		•		•	•			•	•			•	•	•	•	•		•	•	•	•	•		•	•			•	•	•	•		•		•	
Driver's License Number	1			•	•	•	•	•	•	•	•	•	•	•	•	•		•		•	•			•	•			•	•	•	•	•		•	•	•	•	•		•	•			•	•	•	•		•		•	
State Identification Card Number	1			•	•	•	•	•	•	•	•	•	•	•	•	•		•		•	•			•	•			•	•	•	•	•		•	•		•	•		•	•			•	•	•	•		•		•	
Financial Account Number	1,2			•	•	•	•	•	•	•	•	•	•	•	•	•		•		•	•			•	•			•	•	•	•	•		•	•	•	•	•		•	•			•	•	•	•		•		•	
Debit Card Number	1,2			•	•	•	•	•	•	•	•	•	•	•	•	•		•		•	•			•	•			•	•	•	•	•		•	•	•	•	•		•	•			•	•	•	•		•		•	
Credit Card Number	1,2			•	•	•	•	•	•	•	•	•	•	•	•	•		•		•	•			•	•			•	•	•	•	•		•	•	•	•	•		•	•			•	•	•	•		•		•	
Checking Account Number	1																													6					•																
Savings Account Number	1																													6					•																
Personal Identification Number												•																		6					•																
Electronic Identification Number	1																												•	6					•											4			•			
Employer Identification Number																														•						•															
Gov't Issued ID Number																																														4					
Routing Code																														6																	4					
Digital Signature	1																													6					•	•																
Biometric Data	1																												•	6					•											4				•	
Fingerprints	1																												•	6					•											4				•	
DNA																																																			•	
Account Passwords	1											•									•									6					•																
Mother's Maiden Name	1																													6					•	•											4					
Address																														6																	4					
Date of Birth	1																													6						•											4					
Medical Information					•																									6																						
DoT Photo Identification Number	1																																			•																
Telecommunications Device																5																															4					
Other												3									3									6																						
Notification Requirements																																																			
Encrypted Data Safe Harbor (8)				•	•	•	•	•	•	•	•	•	•	•	•	•		•		•	•			•	•			•	•	•	•	•		•	•					•	•			•		•			•		•	
No Reasonable Likelihood of Harm/Injury/Loss/Risk Provision					•			•	•		•										•			•							•			•						•	•						•					
Data Owner/Licenser Notify Individuals				•	•	•	•	•	•	•	•	•	•	•	•	•		•		•	•			•	•			•	•	•	•	•		•	•	•	•			•	•			•	•	•	•		•		•	
Data Maintainer Notify Individuals								•			•	•				5																																				
Notification Procedures / Timelines																																																			
Electronic Notice Allowed				•	•	•	•	•	•	•	•	•	•	•	•	•		•		•	•			•	•			•	•	•	•	•		•	•	•	•	•		•	•			•	•	•	•		•		•	
Substitute Notice Allowed				•	•	•	•	•	•	•	•	•	•	•	•	•		•		•	•			•	•			•	•	•	•	•		•	•	•	•	•		•	•			•	•		•		•			
Set Time Period to Notify Individuals											•													•										7			•													
Provisions for Number of Impacted Individuals, other than Sub. Notice (9)							•			•	•	•	•			•		•			•			•	•						•	•		•	•		•			•						•			•		•	
Other Provisions																																																			
Safeguarding of Information Required					•																			•				•		•																	•	•			
Specific Monetary Penalties Outlined						•					•		•	•		•					•			•						•	•															•	•			
Security Credit Freezes						11	11	•	•		11				11				11	11	11			•	11					11	11	•		11	•			11			11			11		11		11		11	
Best Practice Security Program																																																			
Data Destruction and Disposal					•	•							•																•		•				•											•	•	•			

ENACTED & IN EFFECT

ENACTED & PENDING

PROPOSED LEGISLATION

LITTLE / NO ACTIVITY

(1) In combination with individual's first name or first initial and last name.

(2) In combination with any required security code, access code, or password that would permit access to an individual's financial account

(3) Any of the items listed when not in connection with the individual's first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.

(4) Does not directly relate to security breach notification. Law merely prohibits use without person's prior consent.

(5) Applies only to State Agencies of Indiana

(6) The State of Nevada includes a large listing of applicable data types and defines "personal information" in two different sections of their bill

(7) The State of New York has notification policy provisions for state entities/agencies requiring notification within 120 days

(8) Some states require disclosure if the encrypted data is accessed in an unencrypted form, the breach is linked to a breach of the encryption, or if the encryption key is compromised

(9) Many states require notification to credit bureaus or credit reporting agencies if the number of impacted individuals reaches a certain threshold

(10) HR 4127 requires that individuals be provided, at no cost, consumer credit reports beginning not later than 2 months following a breach of security, and continuing on a quarterly basis for 2 years thereafter.

(11) Consumer credit freeze legislation was enacted, independent of a security breach notification law, and is now in effect

US Federal Laws

- Current Federal laws are lax
- Safe Harbor
  - ***Allows companies to "self-certify"***
  - http://www.export.gov/safeharbor/
- At least 6 new House/Senate bills are being proposed
  - ***Senate Bill 239 (the Notification of Risk to Personal Data Act of 2007)***
  - ***Senate Bill 1178 (the Identity Theft Prevention Act)***

The other 193 Countries

- EU Privacy Directive 95/46/EC
  - Attempting to “harmonize” data protection legislation
  - ***Requires data transferred out be limited to only those countries that ensure an adequate level of protection.***

http://ec.europa.eu/justice_home/fsj/privacy/overview/index_en.htm

- http://www.informationshield.com/intprivacylaws.html
- http://www.privacyinternational.org *search on ”Data Protection and Privacy Laws”*

Recovering the data

Drives
- DLT, 8mm, 4mm, LTO.....

Recording Formats
- Helical scan
- Longitudinal Recording
- .....

Does it matter?

SuperDLT	110
Magstar MP 3570	5
Magstar 3590-B	10
Magstar 3590-E	20
IBM 3580 (Ultrium)	100
DAT - DDS1	2
DAT - DDS2	4
DAT - DDS3	12
DAT - DDS4	40
Exabyte	2.3/5/7
Exabyte - Mammoth	20
Exabyte - Mammoth II	60
Sony AIT - 1	25/35
Sony AIT - 2	50

Forensics

- Papers
  - Forensic acquisition and analysis of magnetic tapes by Bruce J. Nikkelf
    - http://www.digitalforensics.ch/nikkel05.pdf
  - Tape Media Forensic Analysis
    - http://www.expertlaw.com/library/forensic_evidence/tape_media.html
- 3rd party services
  - Neohapsis
    - http://www.neohapsis.com/services/5.html
  - Vogon
    - http://www.vogon-international.com/tape-recovery/tape-recovery.htm

Forensics

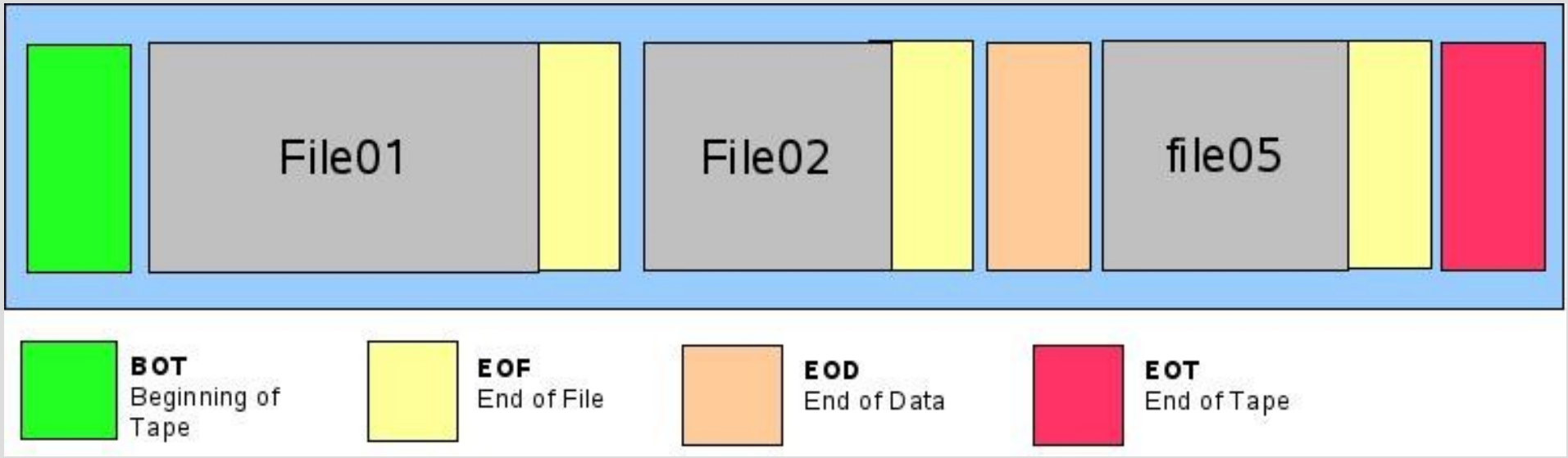
- Not as simple nor complete as HDD forensics

- DD can create a 'near complete' image
  - Miss Slack space in EOF and EOD markers
  - Limited to what tape drive is able to read

- Drive firmware can prevent access to significant portions of media
  - Short erase
  - EndofData (EOD) marker

    Defeatable with customized firmware and ....

Recovering the data



- EOD's enforcement based on drive and firmware
- Powering drive off during write *may* overwrite EOD marker

Recovering the data

- Steps under Linux to baseline a tape
  - Obtain tape information
    - tapeinfo -f <SGTapeDrive>
  - Set tape block size to be variable
    - mt -f <TapeDrive> setblk 0
  - Using 'dd' aquire a copy of data
    - dd if=<TapeDrive> of=<localcopy> bs=256k
  - Repeat 'dd' to image every file on tape upto EOD

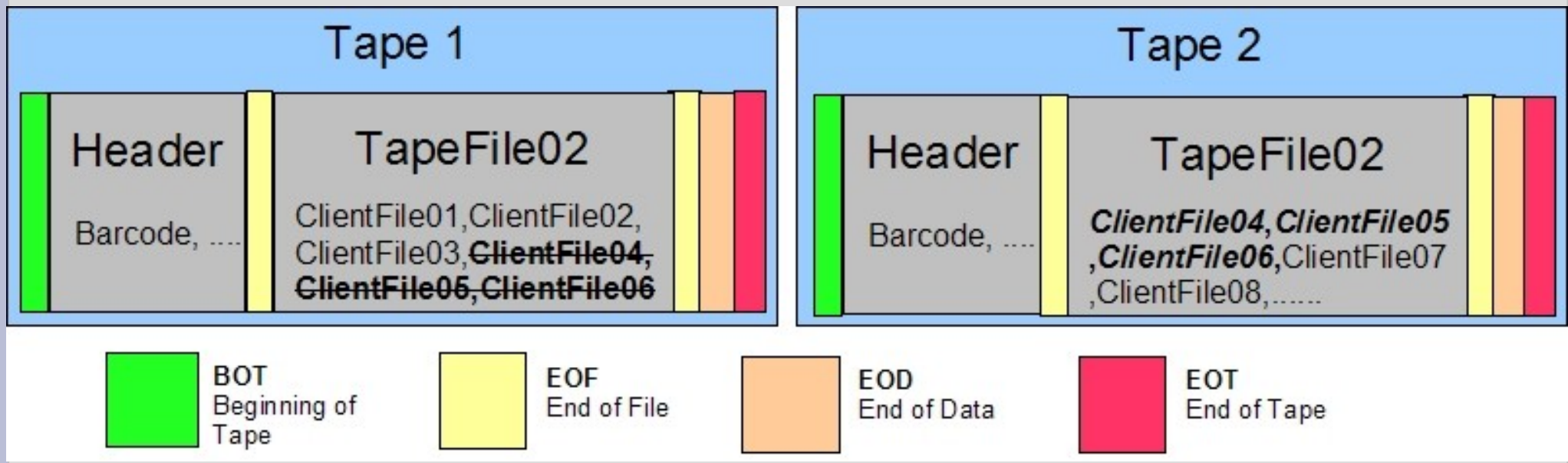
Recovering the data

- TAPECAT - Tape utility command
  - Automates review of the tape
  - Provides tape filesize and data type information
  - Has code to read detailed information on Amanda tapes
  - Able to dump portions of files
    - http://www.inventivetechnology.at/tapecat/
- Use original backup utility to restore data/obtain information
  - Common Backup Software
    - Amanda, ARCserve, TAR, ufsdump/dump, Windows NTBackup, Tivoli Storage Manager (TSM)
  - Cons
    - Cost of license
    - Not all applications can import rogue tapes

Tivoli Storage Manager (TSM)

- Unique backup solution in that it only performs incremental backups
- Database is the heart of TSM server, it tracks data's life on tapes
- No built-in method to 'import' data from an unknown tape (if its not in the DB it doesn’t exist)
- While tapes are filled with data TSM starts “expiring” old data

TSM expiration in action



- TSM Tracks 'current' files via DB
- When a file is 'expired' it still remains on tape
  - Unrestorable unless DB is reverted to time prior to expiration
- Causes tape utilization to drop until reclamation threshold is hit

TSM Tape Layout

- First file is the 'Tape Label'
  - Uses IBM871 character set
  - When translated into ISO-8859-1 it reads:
    VOL1100227
    HDR1ADSM.BFS.V000177A 0001
    006345 993650000000ADSM
    HDR2U2621400000 0

TSM Data files

```
<snipit>
000000b0  00 00 00 00 00 00 00 00  4d 41 59 41 4c 69 6e 75  |........MAYALinu|
000000c0  78 38 36 53 54 41 4e 44  41 52 44 2f 64 61 74 61  |x86STANDARD/data|
000000d0  31 2f 68 6f 6d 65 2f 72  65 70 6c 61 79 2f 2e 72  |1/home/replay/.r|
000000e0  65 70 6c 61 79 50 68 6f  74 6f 43 61 63 68 65 2f  |eplayPhotoCache/|
000000f0  46 61 6d 69 6c 79 20 52  6f 6f 6d 2f 44 75 62 6c  |Family Room/Dubl|
00000100  69 6e 2d 47 75 69 6e 65  73 73 20 4d 75 73 65 75  |in-Guiness Museu|
00000110  6d 2f 69 6d 61 67 65 73  2f 50 34 31 31 30 39 36  |m/images/P411096|
00000120  35 2e 4a 50 47 53 54 41  4e 44 41 52 44 44 45 46  |5.JPGSTANDARDDEF|
00000130  41 55 4c 54 72 65 70 6c  61 79 07 07 16 00 4e 0c  |AULTreplay....N.|
00000140  00 01 00 00 00 00 00 10  94 0b 02 49 04 00 05 00  |...........I....|
00000150  04 00 00 6b 62 00 00 81  a4 00 00 01 fb 00 00 27  |...kb..........'|
00000160  12 3f c1 8e 03 3f c1 8e  0d 00 00 00 00 3f c1 8e  |.?...?.......?..|
00000170  0c 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000180  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 80 03  |................|
000001a0  00 00 05 00 00 00 00 00  04 02 00 00 00 00 00 10  |................|
000001b0  94 0b ff d8 ff e1 38 45  45 78 69 66 00 00 49 49  |......8EExif..II|
<snipit>  ..........
```

Recovering TSM Tapes

- Able to recover client name, architecture and file name using simple dd | strings | grep
- Could manually save out each file to recover binary data
- Able to view text files (ie, passwd, shadow, ...)

- AdsmTape written by Thorhallur Sverrisson
  - Currently only supports ADSM v2 and v3
  - Written for AIX

    http://sourceforge.net/projects/adsmtape/

Introducing TSMtape

- TSMtape recovers files from a Tivoli Storage Manager (TSM) v5.x(tested against 5.2) tape.
- Based off adsmtape written by Thorhallur Sverrisson.
- It can restore your files or audit the tape
- Provides a csv report of file stats
- Download it now from http://sourceforge.net/projects/tsmtape

TSMtape

Usage:
./TSMtape [-R|restore] <device> <Files> <Restore Path>
or
./TSMtape [-A|--audittape] <device> <output file>

Options:
-h, --help display this help and exit
-A, --audit Output list of files stored on tape with supporting details in csv format
-R, --restore Restore "your" files ;-)
<Files> File parsing can be a partial or full path, Use a '/' as a catchall

-v[vv] Print additional debugging information

i.e.
./TSMtape --restore /dev/st0 /etc/shadow /tmp/recovered
./TSMtape --audit /dev/st0 / /tmp/tapefiles.csv

TSMtape output

./TSMtape --restore /dev/st0 / ./restore 2> ./restore/errors
Using device /dev/st0
Volume label: **100227**
Positioning to data
B MAYA - 1086475 **/data1/home/replay/.replayPhotoCache/Family Room/Dublin-Guiness Museum/images/P4110965.JPG**
Restoring ==> ./restore//data1/home/replay/.replayPhotoCache/Family Room/Dublin-Guiness Museum/images/P4110965.JPG
B MAYA - 1098848 /data1/home/replay/.replayPhotoCache/Family Room/Dublin-Guiness Museum/images/P4110966.JPG
Restoring ==> ./restore//data1/home/replay/.replayPhotoCache/Family Room/Dublin-Guiness Museum/images/P4110966.JPG
B MAYA - 1089845 /data1/home/replay/.replayPhotoCache/Family Room/Dublin-Guiness Museum/images/P4110967.JPG
Restoring ==> ./restore//data1/home/replay/.replayPhotoCache/Family Room/Dublin-Guiness Museum/images/P4110967.JPG

TSMtape restorelog.csv

./TSMtape started: Wed Aug 1 13:11:29 20

Volume label: 100227

Node	OS	Domain	Mgmt1	Mgmt2	User	File Type	Storage	inode
MAYA	**Linux86**	**STANDARD**	**STANDARD**	**DEFAULT**	**replay**	**-**	**B**	**27490**
MAYA	Linux86	STANDARD	STANDARD	DEFAULT	replay	-	B	27491
MAYA	Linux86	STANDARD	STANDARD	DEFAULT	replay	-	B	27492
MAYA	Linux86	STANDARD	STANDARD	DEFAULT	replay	-	B	27493

Permissions	UID	GID	Backup Date	Size	FileSpace	Filename
-rw-r--r--	**507**	**10002**	**11/24/03 04:50 AM**	**1086475**	**/data1**	**/..../images/P4110965.JPG**
-rw-r--r--	507	10002	11/24/03 04:50 AM	1098848	/data1	/..../images/P4110966.JPG
-rw-r--r--	507	10002	11/24/03 04:50 AM	1089845	/data1	/..../images/P4110967.JPG
-rw-r--r--	507	10002	11/24/03 04:50 AM	974922	/data1	/..../images/P4110968.JPG

Mitigation

- How to protect your data
  - Inventory, Can’t protect what you don’t know
  - Data encryption
    - **Client/server side**
    - Tape drive (LTO4)
  - Data Destruction standards/requirements

Mitigation

- Wiping/Erasing
  - The **Eliminator 4000FS** is a belt-driven Degausser specifically engineered to erase high-coercivity Hard Disk Drives, Super DLT tape, and DLT IV tape.

http://www.periphman.com/degaussing/degaussers/4000fs.shtml

Mitigation

- Complete Destruction
  - Do-it-yourself destruction
    - Bash it, Heat it, Smelt it, Microwave it, Shred it
      - http://www.networkworld.com/research/2007/041107-data-destruction-methods.html
  - The fine art of data destruction
    - Pulverize, then liquefy
      - http://www.techworld.nl/idgns/2924/the-fine-art-of-data-destruction.html
  - Personal favorite, Thermite!

Thermite

When tapes go missing.....

Q & A

Robert Stoudt

IBM-ISS
RStoudt@us.ibm.com