



Garage Sale Forensics: Data Discovery Through Discarded Devices

John Michael Wright

“Mike”

County of Butte

Session ID: DAS-403

Session Classification: Intermediate

RSACONFERENCE2012

Objectives - What I hope you take away

- Better awareness of media device threats



Objectives - What I hope you take away

- Better awareness of media device threats
- The Importance of a policy



Objectives - What I hope you take away

- Better awareness of media device threats
- The Importance of a policy
- Understanding that devices are easy to get



Objectives - What I hope you take away

- Better awareness of media device threats
- The Importance of a policy
- Understanding that devices are easy to get
- Introduction to cheap and free tools and methods



Objectives - What I hope you take away

- Better awareness of media device threats
- The Importance of a policy
- Understanding that devices are easy to get
- Introduction to cheap and free tools and methods
- Preventing data loss is easy and fun



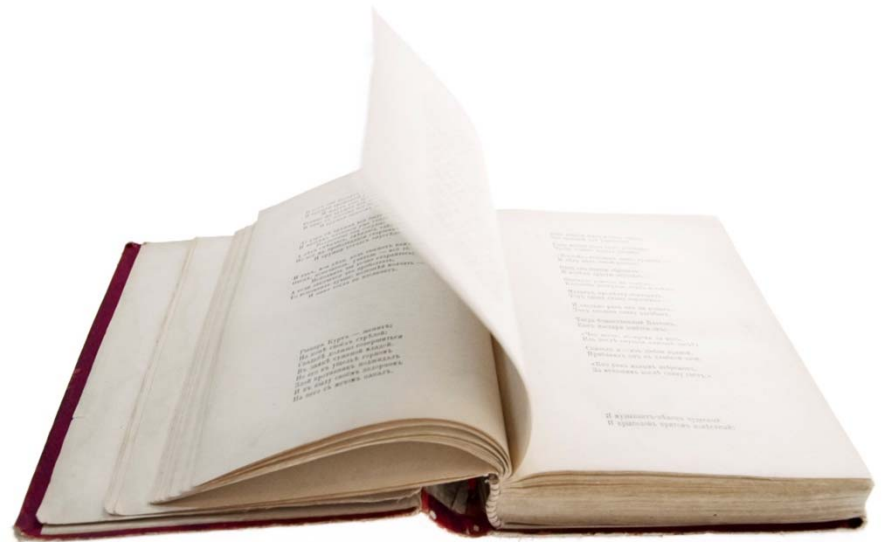


The Data

RSACONFERENCE2012

The Data

- Electronic Data Storage Devices – Defined



The Data

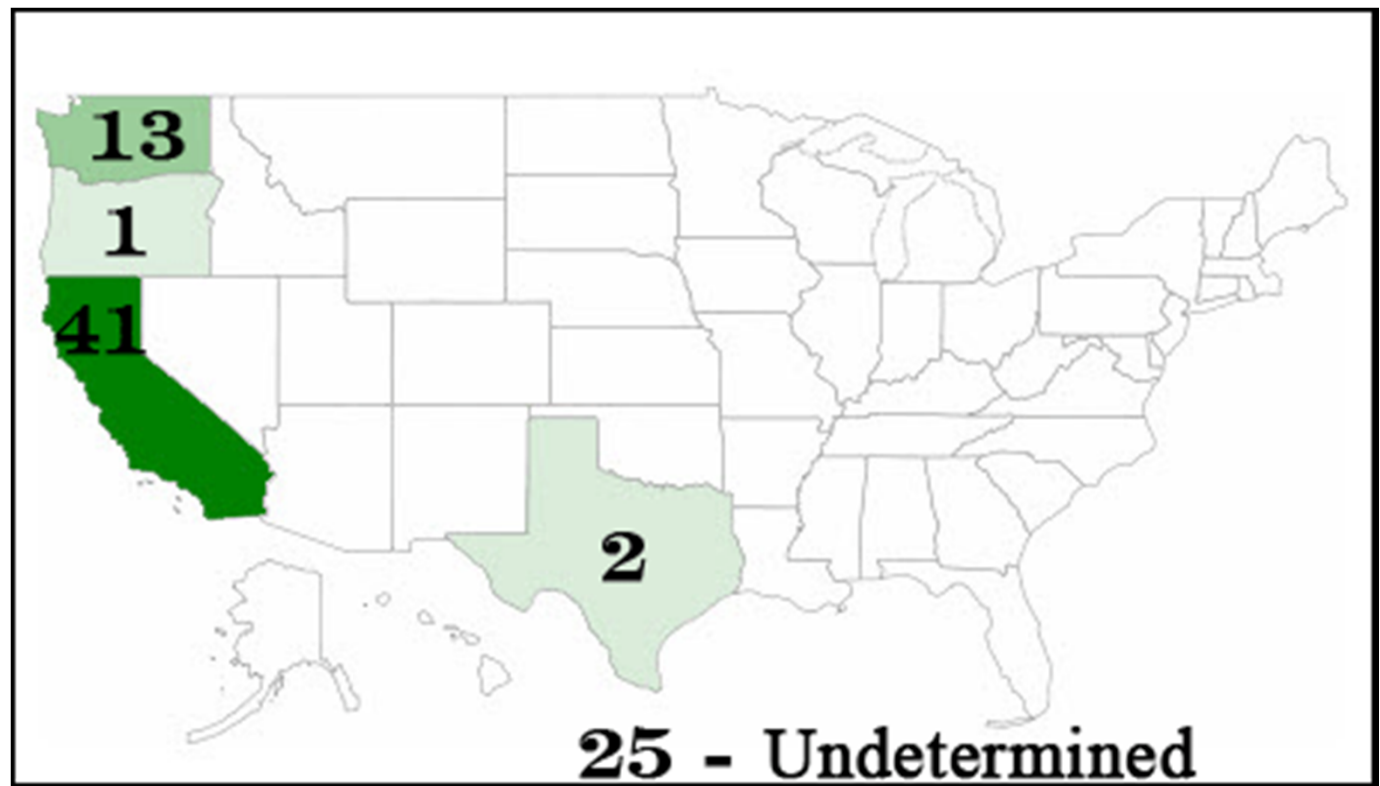
- Electronic Data Storage Devices – Defined
- Statistics

Table <i>Device Condition</i>	
Devices in Working Condition	77 (of 89 total devices)
Devices in Non-Working Condition	12
Devices with Recoverable Data	51
Devices Securely Wiped, no Recoverable Data	20
Devices Physically Destroyed	1
Devices Bootable to VMware	28
Devices with Data Only, No Operating System	14



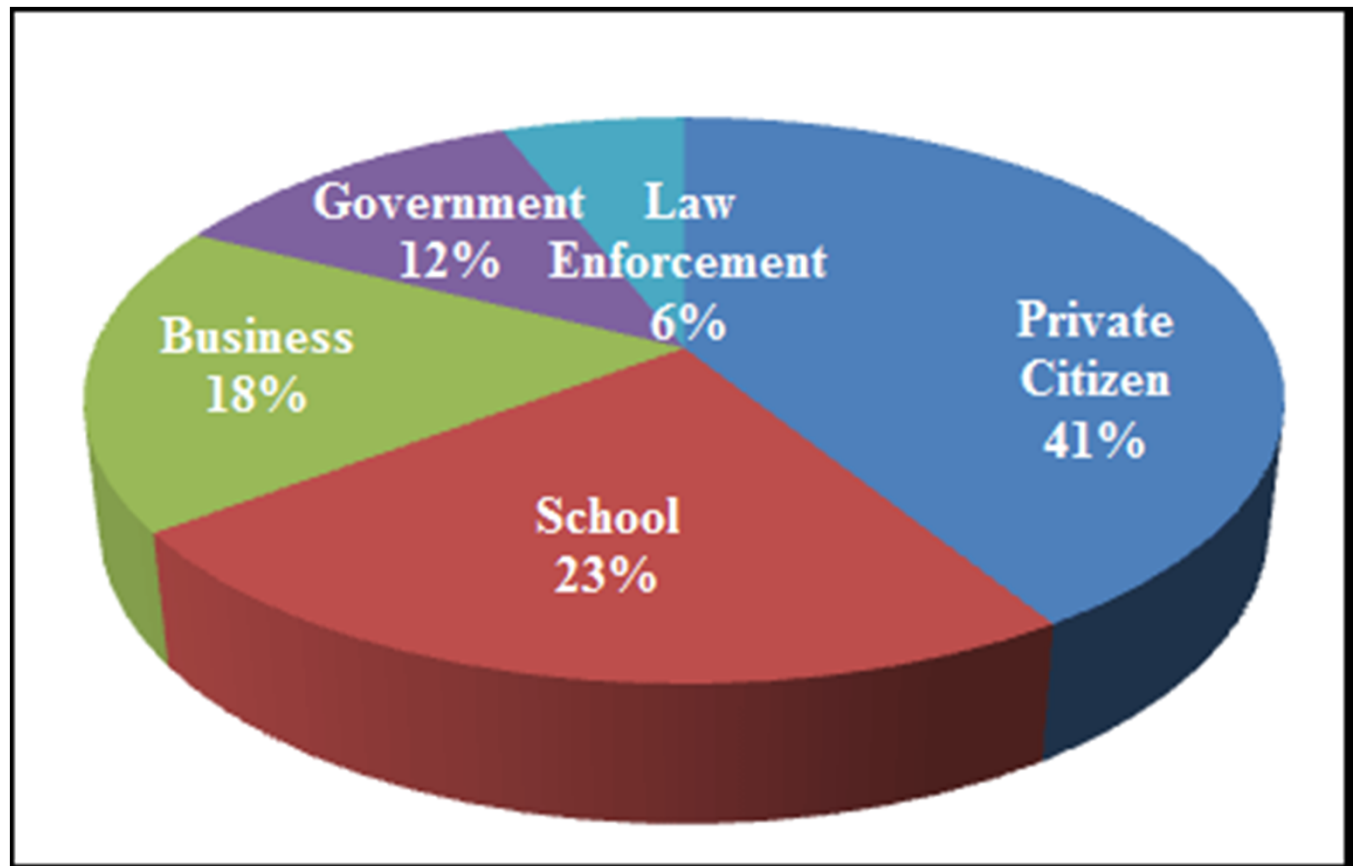
The Data

- Electronic Data Storage Devices – Defined
- Statistics
- Where



The Data

- Electronic Data Storage Devices – Defined
- Statistics
- Where
- Who



The Data

- Electronic Data Storage Devices – Defined
- Statistics
- Where
- Who
- What

Table <i>Data of Interest and PII</i>	
Site	Total
Addresses	5,392
Phone Numbers	2,415
Date of Birth	823
Social Security Numbers	1092
Driver's License Numbers	3
Insurance Information	6
Bank Account Numbers	62
Credit Card / ATM Numbers	151
Tax Returns	9
Accounting Files (Quicken, TurboTax, etc.)	122



The Data

- Electronic Data
- Statistics
- Where
- Who
- What
 - Passwords

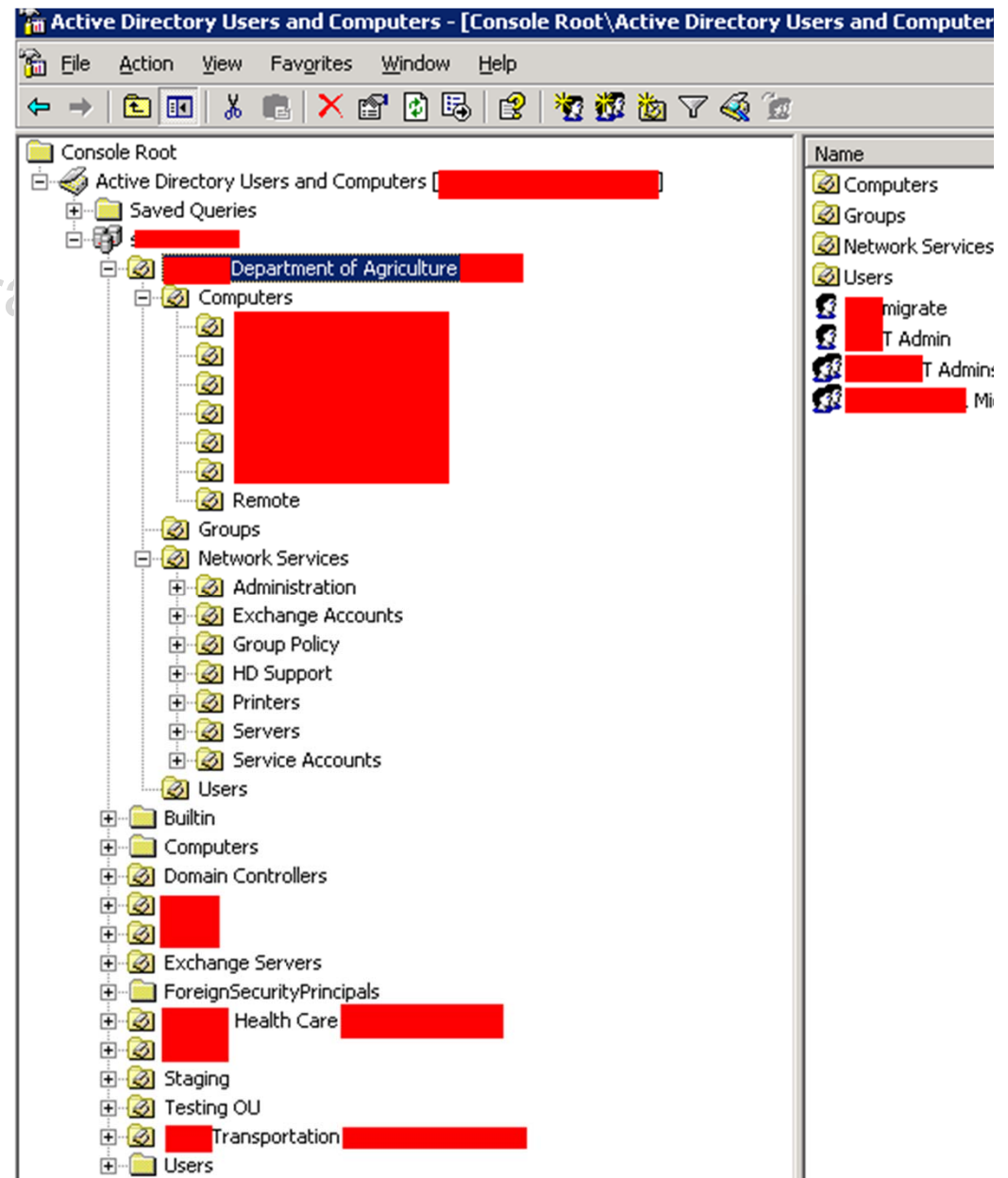
Window Title	Password	Date/Time	Application
Properties for E [REDACTED]	→→→ abcdefg	1/11/2011 10:40:48 AM	Cisco Systems VPN Client
Properties for E [REDACTED]	→→→ abcdefg	1/11/2011 10:40:48 AM	Cisco Systems VPN Client

Type	Stored In	User Name	Password
AutoComplete	Protected Storage	[REDACTED]	global.net cleavage →→→
AutoComplete	Protected Storage	[REDACTED]	global.net cleavage →→→
AutoComplete	Protected Storage	[REDACTED]	cleavage →→→
AutoComplete	Protected Storage	[REDACTED]	4444 →→→
AutoComplete	Protected Storage	[REDACTED]	global.net cleavage →→→
AutoComplete	Protected Storage	[REDACTED]	cleavage →→→
AutoComplete	Protected Storage	[REDACTED]	cleavage →→→
AutoComplete	Protected Storage	[REDACTED]	cleavage →→→
AutoComplete	Protected Storage	[REDACTED]	global.net cleavage →→→
AutoComplete	Protected Storage	[REDACTED]	global.net cleavage →→→
AutoComplete	Protected Storage	[REDACTED]	global.net sage687 →→→
AutoComplete	Protected Storage	[REDACTED]	mail.com kriket14 →→→
AutoComplete	Protected Storage	[REDACTED]	il.com jenna28 →→→
AutoComplete	Protected Storage	[REDACTED]	com →→→
AutoComplete	Protected Storage	[REDACTED]	mail.com kriket14 →→→
AutoComplete	Protected Storage	[REDACTED]	il.com jenna28 →→→
AutoComplete	Protected Storage	[REDACTED]	com →→→
AutoComplete	Protected Storage	[REDACTED]	global.net cleavage →→→
AutoComplete	Protected Storage	[REDACTED]	comdholtz →→→



The Data

- Electronic Data Storage
- Statistics
- Where
- Who
- What
 - Domain Information



The Data

- Electronic
- Statistics
- Where
- Who
- What
 - Domain Information

```
passwd2 - Notepad
File Edit Format View Help
gryk:500:878C669DCCA8F76BAAD3B435B51404EE:C079405928A04D2E3
Gst:501:NO PASSWORD*****:NO PASSWORD*****
GZO$:1000:94BD3ECAEE9767ED776928121BA2A8A4:9E2B53DA1DF1257
IR_GONZO:1001:6D2EA74345632FFB7E35D1B9E1010E16:A63E560AB2F
Exchange Server:1002:DE82FE758B4A7B33AAD3B435B51404EE:0DCC57
member1:1004:B8388819CEE15CA9AAD3B435B51404EE:1FCC918725C62C
lckelb:1005:D953F1A9027CF29BAAD3B435B51404EE:1C91B4583702E
cylor:1006:AFAB016BE256D970AAD3B435B51404EE:BB66A268425540
john:1007:23BD4D22435EFB34AAD3B435B51404EE:A45BA9A5090E72EF
Edison:1008:0D891EBAE20607D31D71060D896B7A46:8071BC9560D82
SExecutiveCmdExec:1012:052C2644795373FA1104594F8C2EF12B:B3
fatters:1013:169FBCCFDB25BDBAAD3B435B51404EE:7740E522A8C99
ttman:1014:2D78002F3B35283FAAD3B435B51404EE:F9B2C8CB6AA1E
jason:1015:B3AA2630DC4F0948AAD3B435B51404EE:938C4200269D59
jyne:1016:DA0D91FA587E48F8AAD3B435B51404EE:603C6238E043462
me:1017:BD5784C589E3480FAAD3B435B51404EE:FC0B7E61B79BDB191
ettas:1018:BD9CB6DD
ccobs:1019:5751B598
drelli:1020:3BCDD89
jnk:1021:4C8A506BBB
jckes:1022:F19F3BC0
NMAN$:1023:*****
```

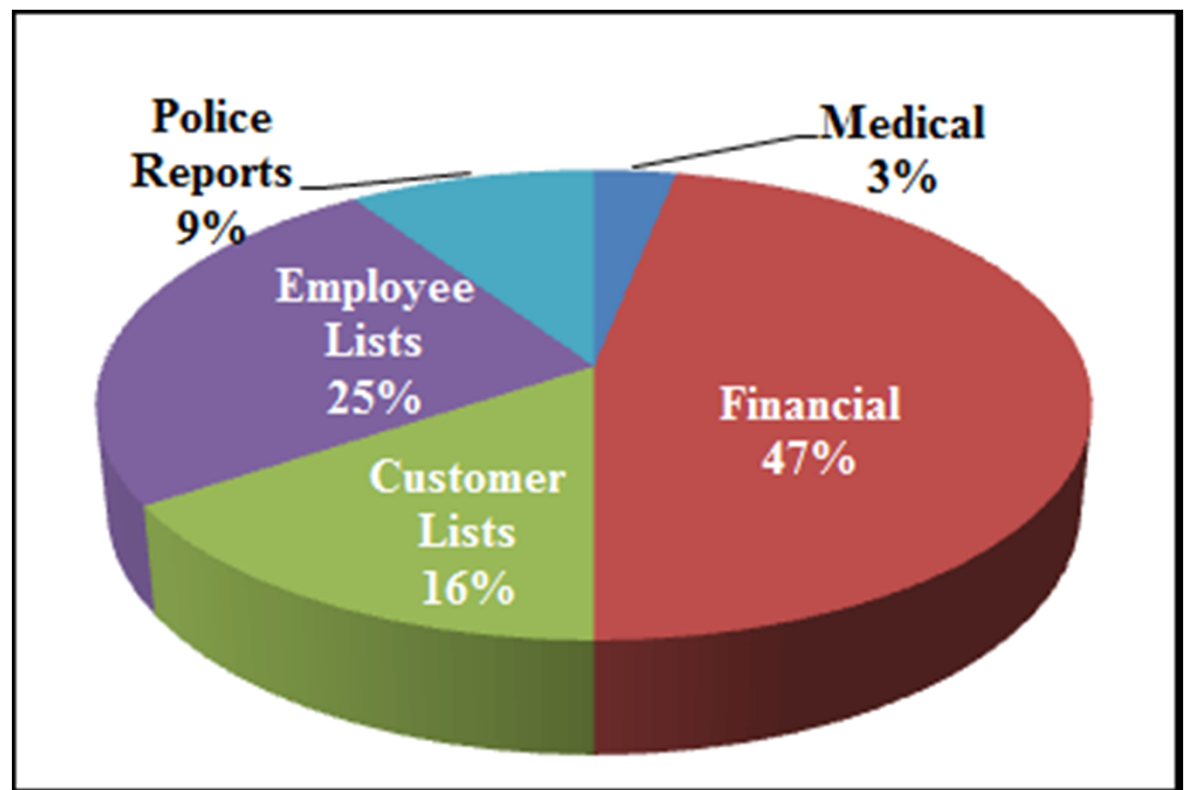
```
statistics
-----
plaintext found:          24 of 24 (100.00%)
total disk access time:   2043.83 s
total cryptanalysis time: 1155.05 s
total chain walk step:    1404925379
total false alarm:        140193
total chain walk step due to false alarm: 423757104

result
-----
gryk          loc8nar hex:6c6f63386e6172
GZO$          tqJ4IP0D9t0hG0 hex:74514a3449504f44397476684730
IR_GONZO      oIfI2G5c0Aobhc hex:6f3166493247356330416f626863
Exchange Server packard hex:7061636b617264
member1       dweebi hex:647765656231
lckelb        2pinky hex:3270696e6b79
cylor         trythis hex:74727974686973
john          trout hex:74726f7574
Edison        june1952 hex:6a756e6531393532
SExecutiveCmdExec WDWZURQF hex:5744575a56525146
fatters       weather hex:77656174686572
ttman         dropp hex:64726f7070
jason         ijf hex:696a66
jyne          theduke hex:74686564756b65
me            antfarm hex:616e7466661726d
ettas         power hex:706f776572
ccobs         sniffer hex:736e6966666572
drelli        tigger hex:746967676572
jnk           jazz hex:6a617a7a
jckes         books hex:626f6f6b73
Press any key to continue . . .
```



The Data

- Electronic Data Storage Devices – Defined
- Statistics
- Where
- Who
- What
 - Financial Data



The Data

- Electronic
- Statistics
- Where
- Who
- What
 - Health

SCHOOL DISTRICT NO. 10

Page: 1

SE Student List

Middle School-

Status: ACTIVE

Run Date: 02/26/2004 01:28 PM

Name	Pupil No.	Birth Date	Age	Grd	Eligibility	Eval Due	IEP Due	Case Mgr/Advisor
Basnight,	105	-1991	12	7	MULTIPLE DISABILITIES	05-21-2006	11-13-2004	
Least Restrictive Environment		Start Date	End Date	Special Education Services		Service Time	Service End Date	
MULTI-ORTHO PROGRAM		11-13-2003		SDI: ACADEMICS		1635	11-13-2004	
				SDI: ADAPTIVE PE		150	11-13-2004	
				SDI: OCCUPATIONAL THER		15	11-13-2004	
				SDI: SPEECH/LANGUAGE T		60	11-13-2004	
				RS: OCCUPATIONAL THER/		30	11-13-2004	
				RS: TRANSPORTATION		480	11-13-2004	
Charboneau,	101	-1989	14	8	MULTIPLE DISABILITIES	10-17-2004	03-11-2004	
Least Restrictive Environment		Start Date	End Date	Special Education Services		Service Time	Service End Date	
MULTI-ORTHO PROGRAM		03-11-2003		SDI: ADAPTIVE PE		150	03-10-2004	
				SDI: IN CLASSROOM SETTI		1650	03-10-2004	
				SDI: OCCUPATIONAL THER		15	03-10-2004	
				SDI: PHYSICAL THERAPY		60	03-10-2004	
				RS: SPEECH/LANGUAGE TH		0	03-10-2004	
				RS: TRANSPORTATION		300	03-10-2004	
Lehmann,	104	-1990	13	7	MULTIPLE DISABILITIES	10-16-2005	11-20-2004	
Least Restrictive Environment		Start Date	End Date	Special Education Services		Service Time	Service End Date	
MULTI-ORTHO PROGRAM		11-20-2003		SDI: ACADEMICS		295	11-20-2004	
				SDI: ADAPTIVE PE		150	11-20-2004	
				SDI: BASIC LVG. SKILLS		295	11-20-2004	
				SDI: COMMUNICATION-ATT		295	11-20-2004	
				SDI: OCCUPATIONAL THER		60	11-20-2004	
				SDI: PHYSICAL THERAPY		90	11-20-2004	
				SDI: SPEECH/LANGUAGE T		90	11-20-2004	
				RS: TRANSPORTATION		300	11-20-2004	
Lewis,	109	-1989	15	8	ORTHOPEDIC IMPAIRMENT	05-31-2004	01-09-2005	
Least Restrictive Environment		Start Date	End Date	Special Education Services		Service Time	Service End Date	
MULTI-ORTHO PROGRAM		01-09-2003		SDI: ADAPTIVE PE		135	01-09-2005	
				SDI: IN CLASSROOM SETTI		1665	01-09-2005	
				SDI: OCCUPATIONAL THER		60	01-09-2005	
				SDI: PHYSICAL THERAPY		60	01-09-2005	
				SDI: SPEECH/LANGUAGE T		30	01-09-2005	
				RS: TRANSPORTATION		600	01-09-2005	



The Data

- Electronic Data
- Statistics
- Where
- Who
- What
 - Other

	A	B	C	D	E	F	G	H
1	Master Student Roster							
2								
3	Number	Student Name	Student SSN	Phone #	Employed	Company	Wage	Benefits
4								
5	1st class							
6	1	Au	Chastity	576-2	Unkr	YES		? ?
7	2	Bu		265-6	Unkr	Dropped	n/a	n/a n/a
8	3	Ca		524-6	770-	YES	Health N	10/hr Yes
9	4	Jo		543-4	983-	307-5 YES	Veriz	12.50/hr Yes
10	5	Ma	ine	429-9	360-	2270 Did not complete	n/a	n/a n/a
11	6	Ma		317-60	475-	YES	Health N	10/hr Yes
12	7	Sn		534-1	473-	NO	n/a	n/a n/a
13	8	St	e	536-8	227-	NO	n/a	n/a n/a
14	9	Wi		535-8	Unkr	Dropped	n/a	n/a n/a
15								
16	Total Completed: 6		Total Dropped: 2		Total Employed: 4			
17								
18	2nd class							
19	1	Ba		415-2	732-	YES	CS	11.50/hr Yes
20	2	Ba	a	537-6	536-	NO	n/a	n/a n/a
21	3	Ba		605-3	unkr	Dropped	n/a	n/a n/a
22	4	Ba	e	265-6	unkr	Dropped	n/a	n/a n/a
23	5	Ca		536-0	253-	26 YES	Medical billing from home	? ?
24	6	Da	nia	537-8	unkr	Dropped	n/a	n/a n/a
25	7	Fa	er	535-8	503-	YES	CS	11.50/hr Yes
26	8	Fa		574-1	548-	YES	Tru	10.50/hr NO
27	9	Fr		539-9	472-	NO	n/a	n/a n/a
28	10	Ga	ia	531-7	537-	YES	Tru	10.50/hr NO
29	11	Gi	elle	331-0	536-	NO	?	? ?
30	12	Jo	onna	340-6	503-	NO	n/a	n/a n/a
31	13	Ja		531-8	unkr	Dropped	n/a	n/a n/a
32	14	Le		539-8	unkr	Dropped	n/a	n/a n/a
33	15	Si	elli	533-1	475-	NO	n/a	n/a n/a
34	16	Si	onia	537-8	396-	NO	n/a	n/a n/a
35	17	Si		533-9	unkr	Dropped	n/a	n/a n/a
36	18	Ta		490-8	unkr	Dropped	n/a	n/a n/a
37	19	To	ie	575-1	unkr	Dropped	n/a	n/a n/a
38	20	Tu	oufa	575-1	unkr	Dropped	n/a	n/a n/a
39	21	W	se	579-8	752-	NO	n/a	n/a n/a
40	22	W	e	539-8	548-	YES	Tru	10.50/hr NO
41								
42	Total Completed: 13		Total Dropped: 9		Total Employed: 6			
43								
44	3rd class							
45	1	Bu	Mikisa	537-6	475-3	Currently enrolled	n/a	n/a n/a
46	2	Ca	a	567-6	unkn	Dropped	n/a	n/a n/a
47	3	Ch	y	515-7	?	Currently enrolled	n/a	n/a n/a
48	4	Co		533-2	983-0	Currently enrolled	n/a	n/a n/a
49	5	Da		537-7	588-2	Currently enrolled	n/a	n/a n/a



The Data

- Electronic Data Storage Devices – Defined
- Statistics
- Where
- Who
- What
- Value

Table <i>Black Market Value of Data</i>			
Site	Value Each	Discovered	Total Value
Social Security Numbers	\$10 (Desai, 2011)	1,092	\$10,920
Credit Card / ATM Accounts	\$2-\$90 (Perna, 2011)	213	\$426 - \$19,170
Logons with Password	\$1 (Bar-Yosef, 2011)	220	\$220
		Total	\$11,566 - \$30,310



The Data

- Electronic Data Storage Devices – Defined
- Statistics
- Where
- Who
- What
- Value
- Legal



The Data

- Electronic Data Storage Devices – Defined
- Statistics
- Where
- Who
- What
- Value
- Legal





Policy

RSACONFERENCE2012

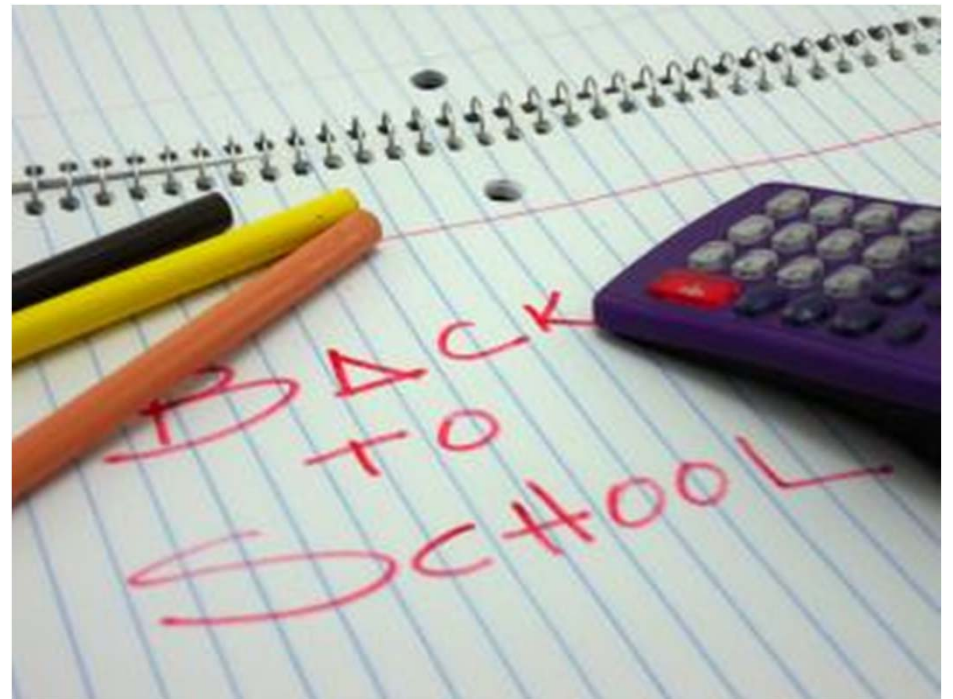
Policy

- Importance



Policy

- Importance
- Education



Policy

- Importance
- Education
- Management



Policy

- Importance
- Education
- Management
- Policy Design



Policy

- Importance
- Education
- Management
- Policy Design
 - Purpose

Appendix B: Computer Equipment and Storage Media Disposal Policy

Information Systems Policies and Procedures

Computer Equipment and Storage Media Disposal Policy

Why?

1. Purpose

The purpose of this policy is to describe how to dispose of computers and electronic storage media and prevent the inadvertent disclosure of information that often occurs because of inadequate cleansing and disposal of computers and electronic storage media.



Policy

- Importance
- Education
- Management
- **Policy Design**
 - Purpose
 - **Scope**

Who?

2. Procedure Scope

This policy shall apply to any computer equipment, electronic equipment, or storage media owned or managed by any department or division. This equipment shall include any device capable of storing any information, such as, but not limited to: Hard disk drives, floppy disk drives, CD's, DVD's, cellular telephones, PDA's, smart phones, fax machines, printers, USB devices, telephones, etc.



Policy

- Importance
- Education
- Management
- Policy Design
 - Purpose
 - Scope
 - Policy

How?

3. Procedure

3.1. Overview

The potential for loss of data exists for many types of computer equipment and storage media including: desktop computers, laptops, servers, disk drives, tapes, cellular telephones, PDAs, smart phones, CDs, DVDs, telephones, printers, fax machines, answering machines, etc.

There are many laws and regulations that require information be protected, HIPPA and the California Information Practices Act of 1977 are just a couple of examples. Social Security Numbers, credit card information, health related data, drivers license numbers, phone numbers, other personal identifying information, and systems or network information are examples of sensitive information requiring protection from disclosure.

Sensitive documents and data containing personally identifiable information can be stored electronically in multiple formats and locations. For example, the information might first exist on a CD then be copied to a computer hard disk drive, then subsequently backed up to a tape drive, while also being synchronized with a PDA or smart phone.

Simply deleting a file does not erase the information. Information that is deleted from a computer may be retrieved by the use of forensics or other recovery tools that are widely available. As new computers or equipment is purchased, older equipment may be replaced, discarded, or surplused. It must be assumed that at some point sensitive data may have been stored on the equipment and is still recoverable.

3.2. Procedure

For the purpose of this policy, disposal of computer equipment, electronic equipment or storage media is defined as the removal of equipment or media from service for a particular department. Equipment transferring to another department will require compliance with this procedure by the originating department. Computer equipment or storage media to be disposed of shall be cleaned in accordance with the standards referenced in the table below. If the equipment or media cannot be cleaned to the standard, then it is to be physically destroyed.

Wipe is the process of overwriting the space where files are located with random data. Read/Writeable media should be “wiped” using a utility that is compliant with the Department of Defense (DoD) 5220.22-M Standard.

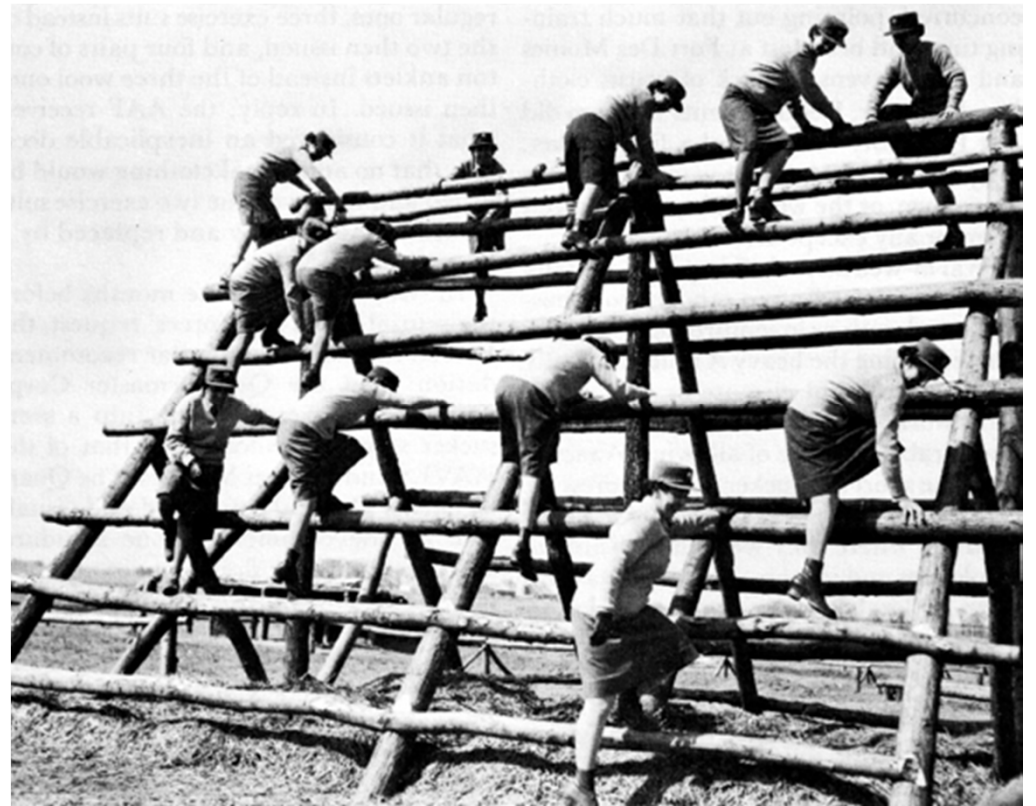
Degaussing is the erasure of information through the use of a very strong magnet. Degaussing is generally used for erasing of magnetic media. Magnetic media to be “Degaussed” shall be degaussed using a Department of Defense (DoD) rated unit.

Physical Destruction may be required if the equipment or storage media cannot be wiped or degaussed. Any equipment or storage media can be physically destroyed through burning, crushing, or pulverizing.

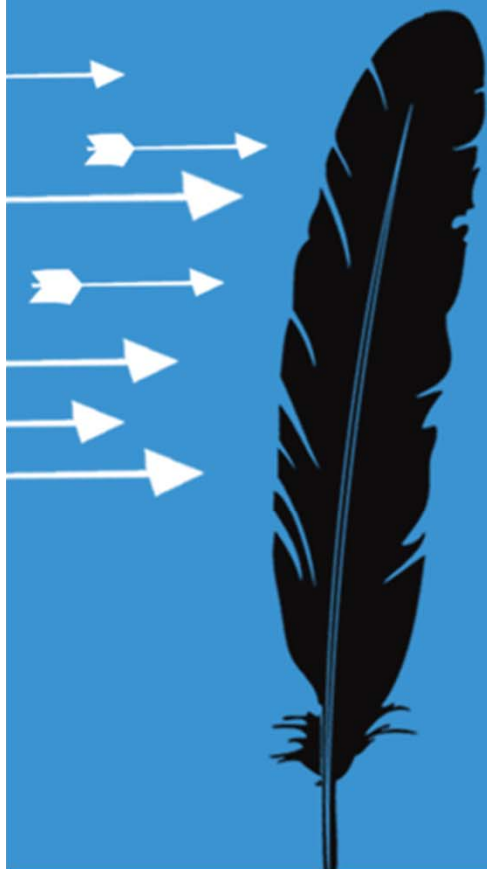


Policy

- Importance
- Education
- Management
- Policy Design
 - Purpose
 - Scope
 - Policy
- Training



The Hunt for Devices



The Hunt for Devices

- Devices are Cheap and Easy to Find



The Hunt for Devices

- Devices are Cheap and Easy to Find
- Where to Find Devices
 - Garage Sales



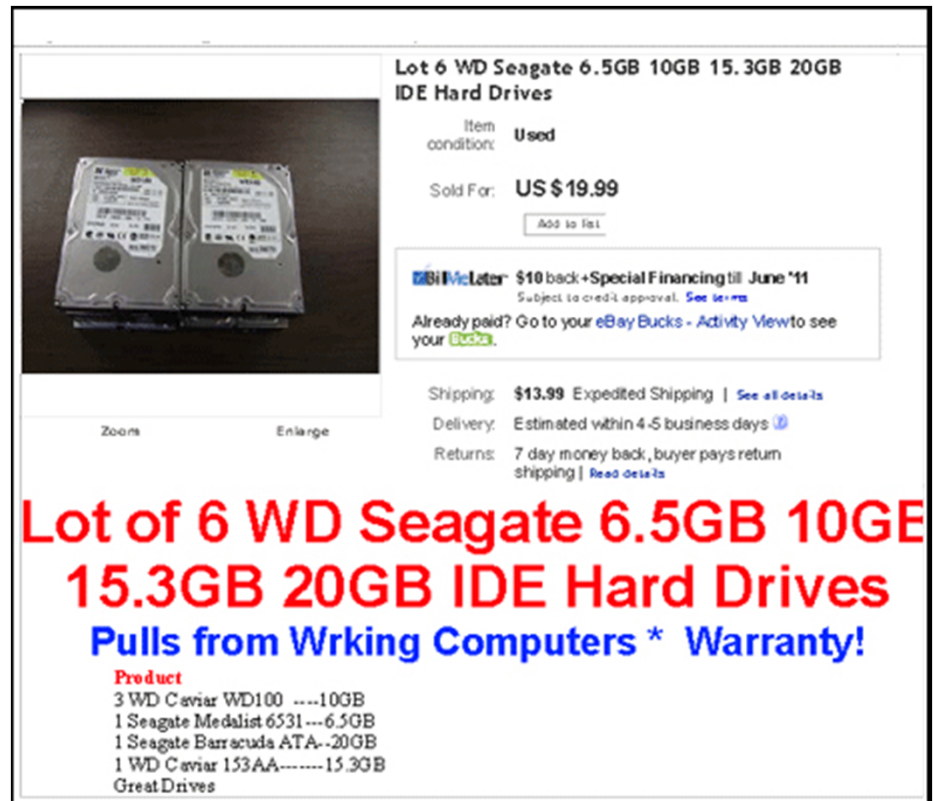
The Hunt for Devices

- Devices are Cheap and Easy to Find
- Where to Find Devices
 - Thrift Shops
 - Second Hand
 - Goodwill



The Hunt for Devices

- Devices are Cheap and Easy to Find
- Where to Find Devices
 - ebay



Lot of 6 WD Seagate 6.5GB 10GB 15.3GB 20GB IDE Hard Drives

Item condition: **Used**

Sold For: **US \$19.99**

[Add to list](#)

Buy It Now \$10 back + Special Financing till June '11
Subject to credit approval. [See terms](#)

Already paid? Go to your [eBay Bucks](#) - [Activity View](#) to see your [Bucks](#).

Shipping: **\$13.99** Expedited Shipping | [See all details](#)

Delivery: Estimated within 4-5 business days [📅](#)

Returns: 7 day money back, buyer pays return shipping | [Read details](#)

Lot of 6 WD Seagate 6.5GB 10GB 15.3GB 20GB IDE Hard Drives
Pulls from Wrking Computers * Warranty!

Product
3 WD Caviar WD100 ----10GB
1 Seagate Medalist 6531 ----6.5GB
1 Seagate Barracuda ATA--20GB
1 WD Caviar 153AA-----15.3GB
Great Drives



The Hunt for Devices

- Devices are Cheap and Easy to Find
- Where to Find Devices
 - Craigslist



The Hunt for Devices

- Devices are Cheap and Easy to Find
- Where to Find Devices
 - Recycle Centers
 - Recycle Drives

Coming to your neighborhood

FREE Curbside pick-up service

Date of pick-up:
August 29, 2010
(Between 10:00a.m. and 8:00p.m)

ITEMS WE TAKE FREE:

Televisions	Car Batteries
Computer	Console T.V.'s
Towers and	Big Screens
Monitors	
Laptops	

NO LIMIT!

Take advantage of this ONE TIME ONLY
Free curbside pick-up



The Hunt for Devices

- Devices are Cheap and Easy to Find
- Where to Find Devices
 - Dumpster Diving



The Hunt for Devices

- Devices are Cheap and Easy to Find
- Where to Find Devices

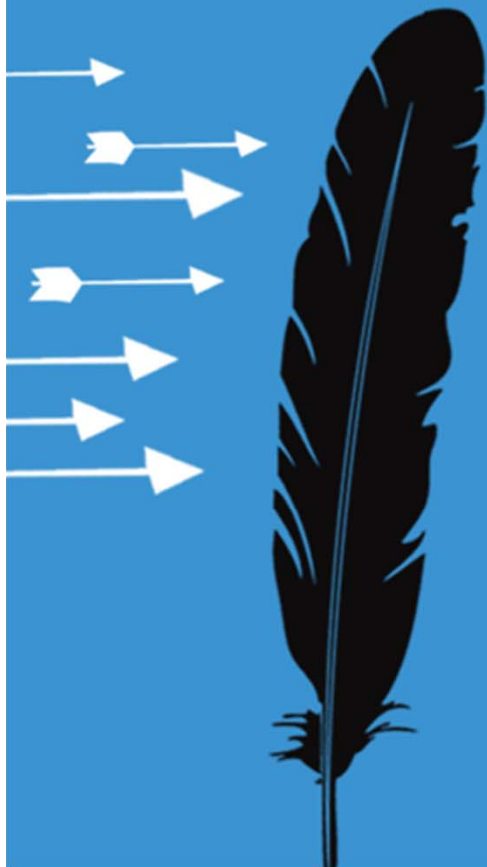


The Hunt for Devices

- Devices are Cheap and Easy to Find
- Where to Find Devices
- Does it Even Matter?



Device Analysis & Data Recovery



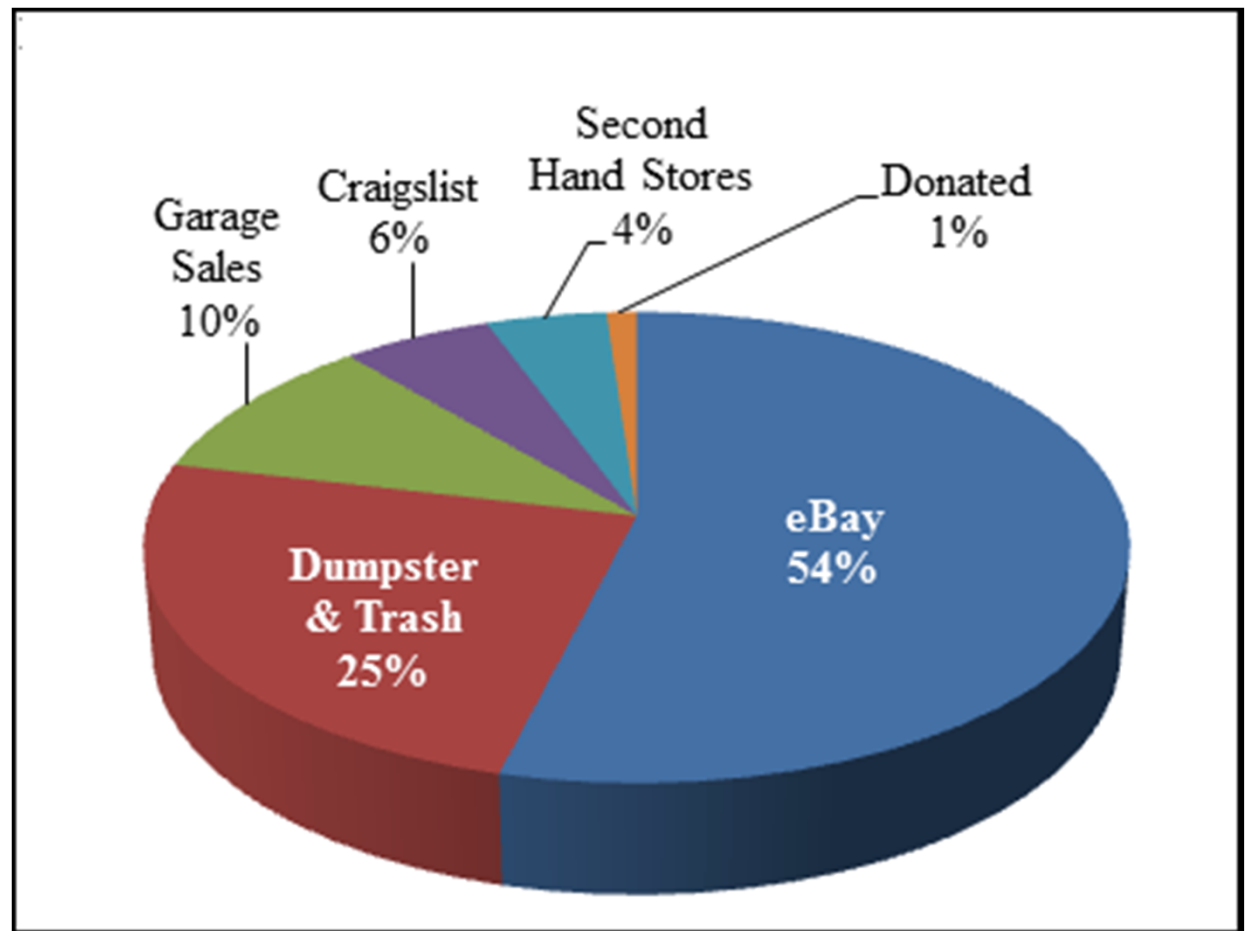
Device Analysis & Data Recovery

- Organization



Device Analysis & Data Recovery

- Organization
- Where



Device Analysis & Data Recovery

- Organization
- Where
- Tools

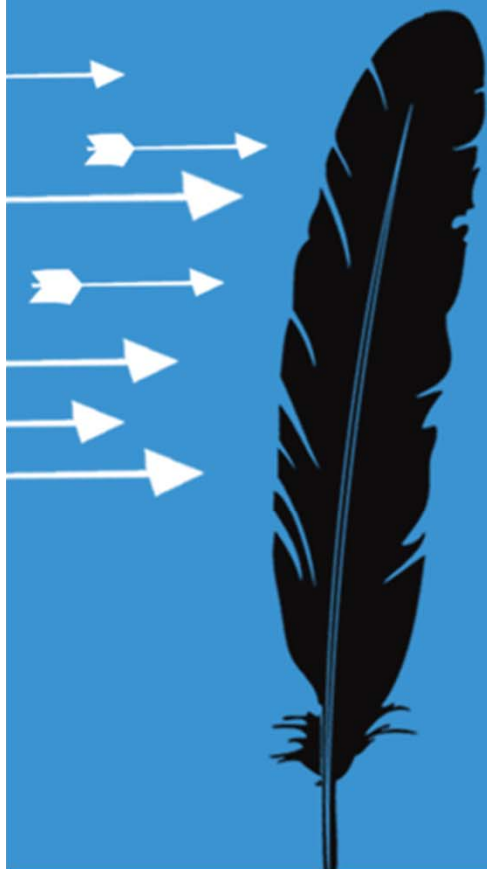


Device Analysis & Data Recovery

- Organization
- Where
- Tools
- **Software**

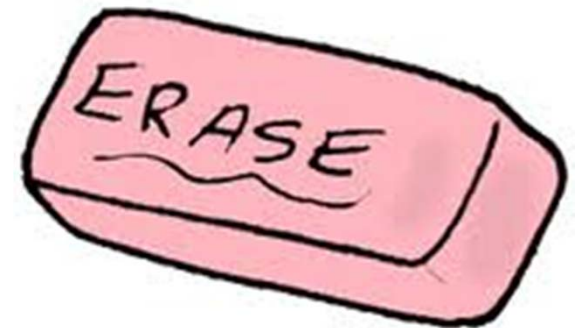


Proper Disposal Methods



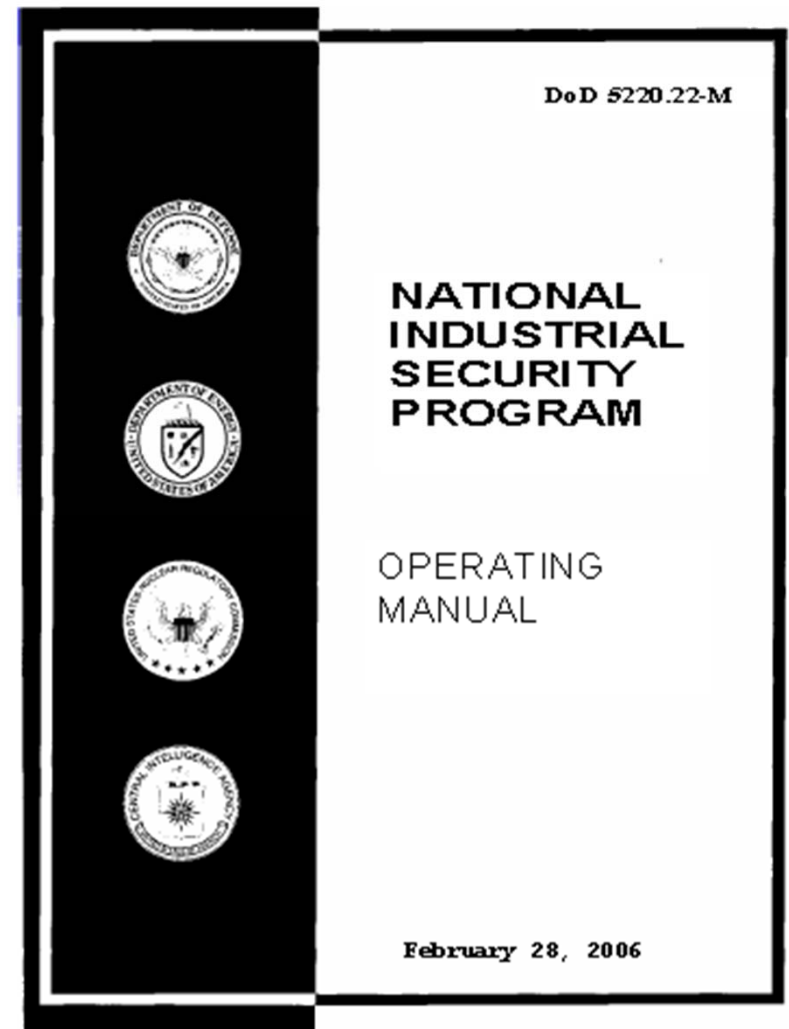
Proper Disposal Methods

- Format



Proper Disposal Methods

- Format
- DoD 5220.22-M



Proper Disposal Methods

- Format
- DoD 5220.22-M
- NIST Pub 800-88

Erasure and Disposal Technique Matrix			
Media Type	Wipe	Degauss	Physical Destruction
Hard Disk Drive	X	X	X
Fax Machine Printer Copier	X		X
Telephone Telecommunication Equipment	X		X
CD DVD			X
USB Drive Thumb Drive Memory Stick/Card	X		X
Floppy Disk	X	X	X
Tape	X	X	X
PDA Cell Phone	X		X



Proper Disposal Methods

- Format
- DoD 5220.22-M
- NIST Pub 800-88
- Sanitization

Wipe



Degauss



Destroy



Proper Disposal Methods

- Format
- DoD 5220.22-M
- NIST Pub 800-88
- Sanitization

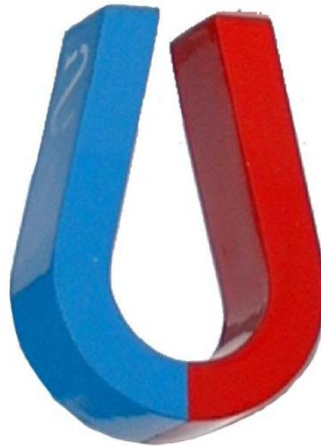
- Wipe

```
0x0000:  0000 0000 0000 0000 - 0000 0000 0000 0000 | .....  
0x0010:  0000 0000 0000 0000 - 0000 0000 0000 0000 | .....  
0x0020:  0000 0000 0000 0000 - 0000 0000 0000 0000 | .....  
0x0030:  0000 0000 0000 0000 - 0000 0000 0000 0000 | .....  
0x0040:  0000 0000 0000 0000 - 0000 0000 0000 0000 | .....  
0x0050:  0000 0000 0000 0000 - 0000 0000 0000 0000 | .....  
0x0060:  0000 0000 0000 0000 - 0000 0000 0000 0000 | .....  
0x0070:  0000 0000 0000 0000 - 0000 0000 0000 0000 | .....  
0x0080:  0000 0000 0000 0000 - 0000 0000 0000 0000 | .....  
0x0090:  0000 0000 0000 0000 - 0000 0000 0000 0000 | .....  
0x00A0:  0000 0000 0000 0000 - 0000 0000 0000 0000 | .....  
0x00B0:  0000 0000 0000 0000 - 0000 0000 0000 0000 | .....  
0x00C0:  0000 0000 0000 0000 - 0000 0000 0000 0000 | .....
```



Proper Disposal Methods

- Format
- DoD 5220.22-M
- NIST Pub 800-88
- **Sanitization**
 - Wipe
 - Degauss



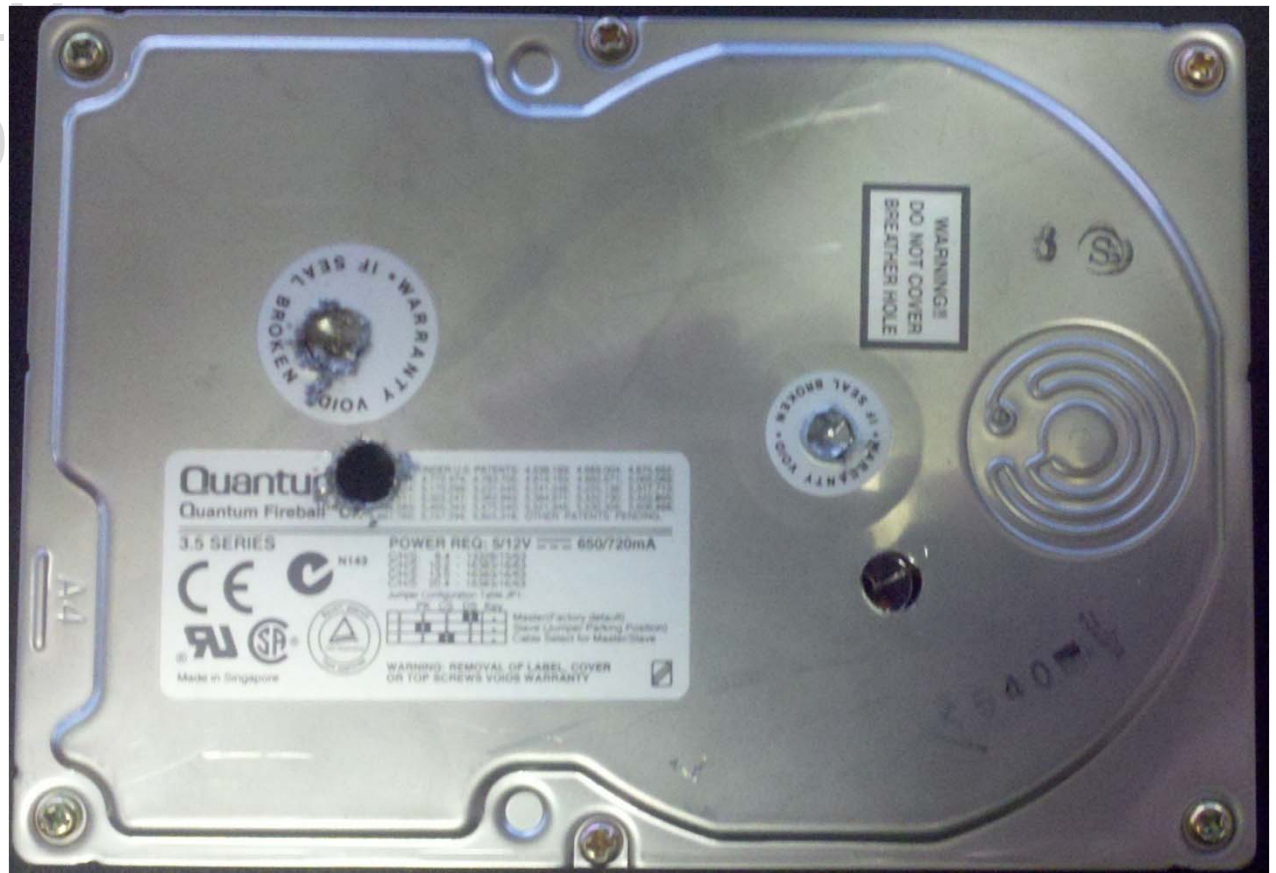
Proper Disposal Methods

- Format
- DoD 5220.22-M
- NIST Pub 800-88
- Sanitization
 - Wipe
 - Degauss



Proper Disposal Methods

- Format
- DoD 5220.22-
- NIST Pub 800
- **Sanitization**
 - Wipe
 - Degauss
 - **Destroy**



Proper Disposal Methods

- Format
- DoD 5220.22-M
- NIST Pub 800-88
- **Sanitization**
 - Wipe
 - Degauss
 - **Destroy**



Proper Disposal Methods

- Format
- DoD 5220.22-M
- NIST Pub 800-8
- **Sanitization**
 - Wipe
 - Degauss
 - **Destroy**



Proper Disposal Methods

- Format
- DoD 5220.22-M
- NIST Pub 800
- **Sanitization**
 - Wipe
 - Degauss
 - **Destroy**



Proper Disposal Methods

- Format
- DoD 5220.22-M
- NIST Pub 800-88
- **Sanitization**
 - Wipe
 - Degauss
 - **Destroy**



Proper Disposal Methods

- Format
- DoD 5220.22-M
- NIST Pub 800-88
- **Sanitization**
 - Wipe
 - Degauss
 - **Destroy**



Proper Disposal Methods

- Format
- DoD 5220.22-M
- NIST Pub 800-88
- **Sanitization**
 - Wipe
 - Degauss
 - **Destroy**



Proper Disposal Methods

- Format
- DoD 5220.2
- NIST Pub 800-88
- Sanitization
 - Wipe
 - Degauss
 - Destroy



Proper Disposal Methods

- Format
- DoD 5220.2
- NIST Pub 800-88
- Sanitization
 - Wipe
 - Degauss
 - Destroy





Apply

How to Apply What You Have Learned Today

- In the first three months following this presentation you should:
 - Identify Current Policy and Procedures
 - Identify Devices (Threats)



How to Apply What You Have Learned Today

- In the first three months following this presentation you should:
 - Identify Current Policy and Procedures
 - Identify Devices (Threats)
- Within six months you should:
 - Identify Workflow
 - Create or Update Policy and Procedures
 - Educate Staff





Conclusion

Conclusion

- Devices may contain data



Conclusion

- Devices may contain data
- Devices are cheap and easy to find



Conclusion

- Devices may contain data
- Devices are cheap and easy to find
- Device owners don't understand the risk



Conclusion

- Devices may contain data
- Devices are cheap and easy to find
- Device owners don't understand the risk
- **Tools are easy to find and use**



Conclusion

- Devices may contain data
- Devices are cheap and easy to find
- Device owners don't understand the risk
- Tools are easy to find and use
- **Tools can be used to sanitize**



Conclusion

- Devices may contain data
- Devices are cheap and easy to find
- Device owners don't understand the risk
- Tools are easy to find and use
- Tools can be used to sanitize
- Physical destruction is better (more fun)



Thank You

John Michael Wright
“Mike”



mwright@buttecounty.net (work)
mike@rollnpc.com (not work)

<http://www.rollnpc.com/rsa2012>
(Links & References)

March 2, 2012 – DAS-403



References

- Bar-Yosef, N. (2011). The commodities of underground markets. Retrieved on April 19, 2011 from <http://www.securityweek.com/commodities-underground-markets>
- California v. Greenwood. (1988). 486 U.S. 35 California v. Greenwood et.al. Certiorari to the Court of Appeal of California, Fourth Appellate District, No. 86-684. Retrieved on April 15 from <http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=US&vol=486&invol=35>
- CCC. (n.d.). California civil code section 1798.56. Retrieved on April 19, 2011 from <http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.55-1798.57>
- CCISDA. (2011). Program best practices. Retrieved on June 3, 2011 from <http://www.ccisda.org/bestpractice/>
- CMRR. (2011). Secure erase. Retrieve on April 19, 2011 from <http://cmrr.ucsd.edu/people/Hughes/SecureErase.shtml>
- Desai, A. (2011). Commercial hacking: The mafia returns. Retrieved on April 19, 2011 from <http://www.articleclick.com/Article/Commercial-Hacking-The-Mafia>Returns/1478593>



References Continued

- DoD 5220.22-M. (2006). National industry security program, operating manual. Retrieved on April 19, 2011 from <http://www.dss.mil/isp/odaa/documents/nispom2006-5220.pdf>
- Messmer, E. (2010). Data breach costs top \$200 per customer record. Retrieved on June 7, 2011 from <http://www.networkworld.com/news/2010/012510-data-breach-costs.html>
- Mitnick, K. D. (2003). *The art of deception controlling the human element of security*. Hoboken, NJ: John Wiley & Sons Inc.
- NIST Pub 800-88. (2006). NIST special publication 800-88, guidelines for media sanitation. Retrieved on April 19, 2011 from http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf
- Perna, G. (2011). Black market prices: The low cost of stolen credit cards. Retrieved on April 19, 2011 from <http://www.ibtimes.com/articles/103739/20110121/cybercrime-black-market-cost-of-data-stolen-credit-card-information.htm>
- Wei, M., Grupp, L. M., Spada, F. E., & Swanson, S. (2011). Reliably erasing data from flash-based solid state drives. Retrieved on April 19, 2011 from http://www.usenix.org/events/fast11/tech/full_papers/Wei.pdf



Tools

- Access Data: FTK Imager 2.5.3: <http://accessdata.com/support/previous-releases#FTKImager>
- Darik's Boot and Nuke: <http://www.dban.org/>
- DiskInternals Uneraser: <http://www.diskinternals.com/order/uneraser/>
- Disk Wipe: <http://diskwipe.org/>
- Helix 2009 R1: https://www.e-fense.com/store/index.php?_a=viewProd&productId=11
- Identity Finder: <http://www.identityfinder.com/>
- Kon-Boot: <http://www.piotrbania.com/all/kon-boot/>
- NirSoft: <http://www.nirsoft.net/>
- Recuva: <http://www.piriform.com/recuva>
- Secure Erase: <http://cmrr.ucsd.edu/people/Hughes/SecureErase.shtml>
- Trinity Rescue Kit (TRK): <http://trinityhome.org/>
- WinTaylor: <http://www.caine-live.net/page2/page2.html>

