AMCIS 2011 Proceedings - All Submissions

8-5-2011

Testing Data Sanitization Practices of Retired Drives with The Digital Forensics Data Recovery Project

Dr. Asley L. Podhradsky
Drexel University

Cindy Casey
Drexel University

Testing Data Sanitization Practices of Retired Drives with The Digital Forensics Data Recovery Project

Dr. Ashley Podhradsky and Cindy Casey

Drexel University

Abstract

There are several empirical studies that have focused on the analysis of retired digital media on the secondary market which has had historical impact on not only the technology community, but the business community alike. This research will introduce the Digital Forensics Recovery (DFDR) study, where five key industries- government, education, businesses, electronic recycle centers, and individual home users were targeted to test effectiveness of data sanitization practices with used media. While previous work analyzed any device, the DFDR study aims to analyze on media in which due diligence has been taken to ensure data privacy

Introduction

Given the migration from paper based storage to digital media, coupled with the movement of increased computer based personal and business practices; virtually all forms of communication are stored on some type of digital media. Improper data sanitization practices can result in the release of confidential data and identity theft

- Digital media capacity continues to increase while the cost per GB continues to decrease [2]. Toshiba developed a 2.5 terabyte density per square inch [16]

- The; shorter replacement lifecycle directly results in a higher number discarded digital devices which in turn needs to be sanitized before it is retired or reused.

- Residual data, is data that remains on digital media after a sanitization process was taken. It can be found in slack and unallocated space, or could simply be marked for deletion but not actually deleted.

- Properly adopted and integrated data sanitization policies and practices are essential to ensuring discarded media does not contain personal identifying information or sensitive corporate data. Practically all aspects of our lives are held on digital media somewhere, whether the media is in our control or not.

- Current beliefs on formatting, f-disking or imaging (aka ghosting or cloning), are that these approaches result in properly sanitized digital media; however research has shown that residual data can be recovered from these drives [3,18]. In special cases, even zero fill utilities can leave residual data in slack and unallocated space.

Accidental Data Disclosure Examples

- In 2009, Chris Ogle purchased a used iPod for $15.00 from a store in New Zealand. The iPod contained current personal information of different military personnel, war mission briefings and deployment information. [11]

- In 2002, the US Veterans Administration Medical Center, located in Indianapolis, disposed of 139 computer desktop systems. The systems were either sold or donated to needy school districts. A reporter purchased three of the systems. The drives were littered with confidential and personal data including medical records on veterans with mental health concerns, AIDS, and other serious health ailments [12].

- In Garfinkel and Shelat's research study published in 2003,10 used systems were purchased from a computer store which contained files from a law firm, records on mental health patients, and confidential financial files [1]

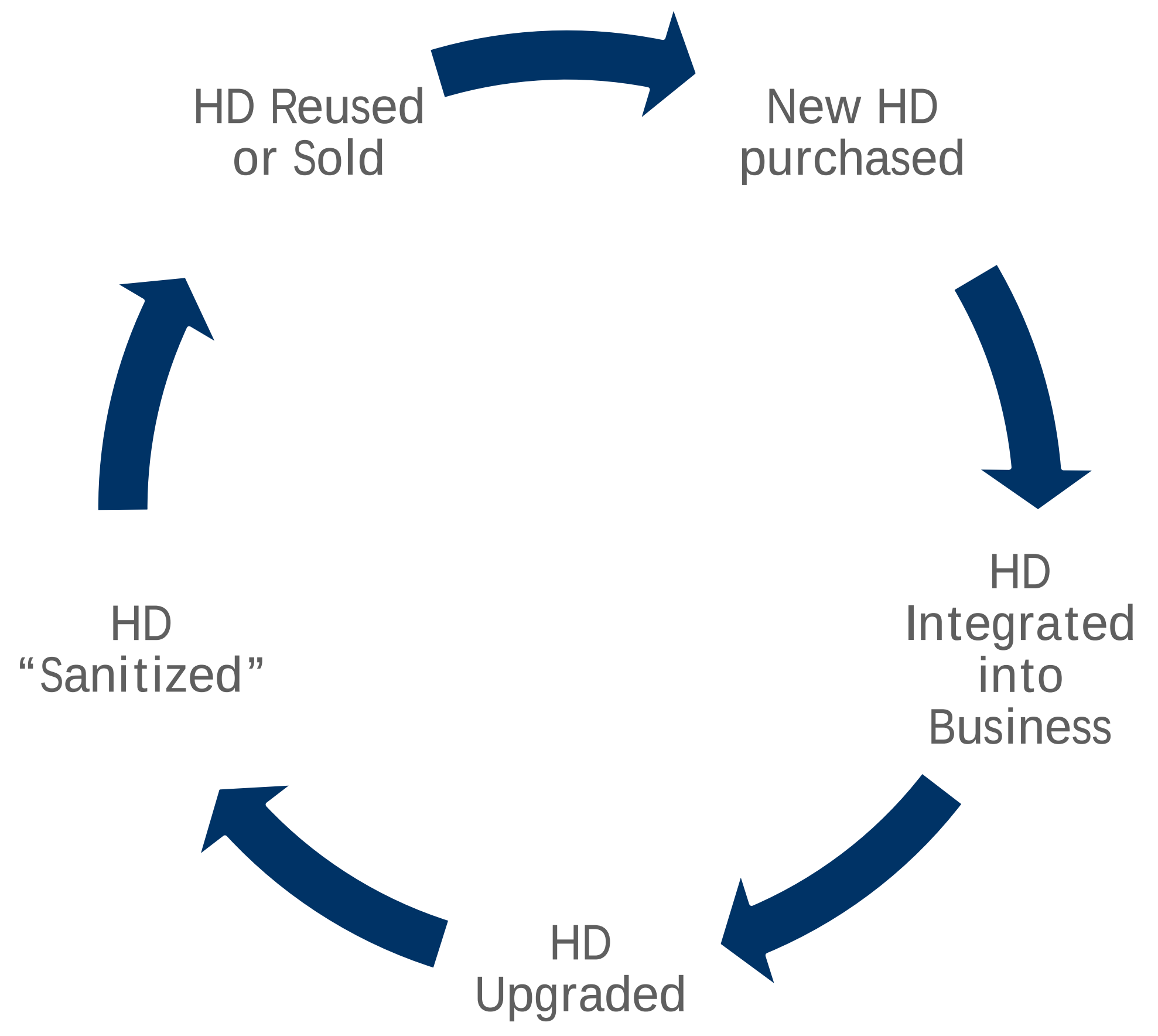
- In 2009, researchers purchased used desktop machines on eBay, the systems contained health records and financial records from a major healthcare provider.[3]

Digital Forensics Data Recovery Project

Digital media was purchased or acquired through a variety of venues within the United States, including government auctions, eBay, craigslist, dumpsters, curbs with "free sign", and data recycle centers. The purchase of the media was funded through the National Center for the Protection of the Financial Industry. The media, including hard drives and flash drives, was forensically imaged with FTK Imager and stored and cataloged on a DROBO.

The Digital Forensics Data Recovery (DFDR) project, however, is focused on taking data remanence a step further to analyze residual data on sanitized media within the secondary market. Prior research analyzed any discarded media, this research aims to acquire drives in which due diligence has been taken to ensure data privacy.

Hard Drive Replacement Lifecycle



HD Reused or Sold

New HD purchased

HD Integrated into Business

HD Upgraded

HD "Sanitized"

- New HD Purchased
  - Organizations purchase HD as singles or in new systems
  - HD's are implemented into existing or new systems
- HD Integrated into Business or Organization Production
  - HD's are given the organizations "image" to shorten implementation phase
  - Confidential and regulated data is stored on HD's
- HD Upgraded
  - Upgrades include software, operating system, or hardware
  - Upgrades could be due to a virus, new technology, or planned upgrades
- HD Sanitized
  - Existing confidential and regulated organization data is "sanitized"
  - Organizations "sanitize" drives with commonly accepted practices
    - Imaging, Ghosting, or Cloning
    - F-disking
    - Formatting
    - Reinstalling OS
- HD Reused or Sold
  - Old HD is either installed in existing system within the organization or is sold on the secondary market
  - Drives "sanitized" with commonly accepted practices unknowingly contain confidential and heavily regulated data are either reused or sold

DFDR Phase One Results

- Government Drive:
  - Two credit cards with CV codes
  - Two social security numbers
  - Four addresses,
  - Dozens of emails
  - Hundreds of personal images
  - Over 60 profiles, including the domain administrator.
    - The SAM files were recovered and the domain administrator account password was cracked using FTK's PRTK tool.
  - Employees used the computer to process travel reservations,
  - System used by an employee who was updating immigration files –
  - All the personal data need to steal two complete identities was recovered.
- Educational Drive:
  - This drive contained enough data to steal *three* complete identities;
  - Countless confidential files, emails, and personnel images were found. If released this data could be extremely embarrassing for the educational site, even illegal in situations
- Business Drive:
  - Employee records, payroll, banking files, confidential internal memos, and budget information.
  - Tax data- file found on the computer that contained a master record for tax and payroll. The full names, addresses, DOB's, SSN 's, and banking data (direct deposit) was found for 23 employees.
- Electronic Recycle Site:
  - Photos of an underage teenager participating in illegal drug activities.
- Homes User
  - Confidential tax data, banking records, personal files, FAFSA forms, National Guard Data

Sanitization Tools: Open Source and Commercial

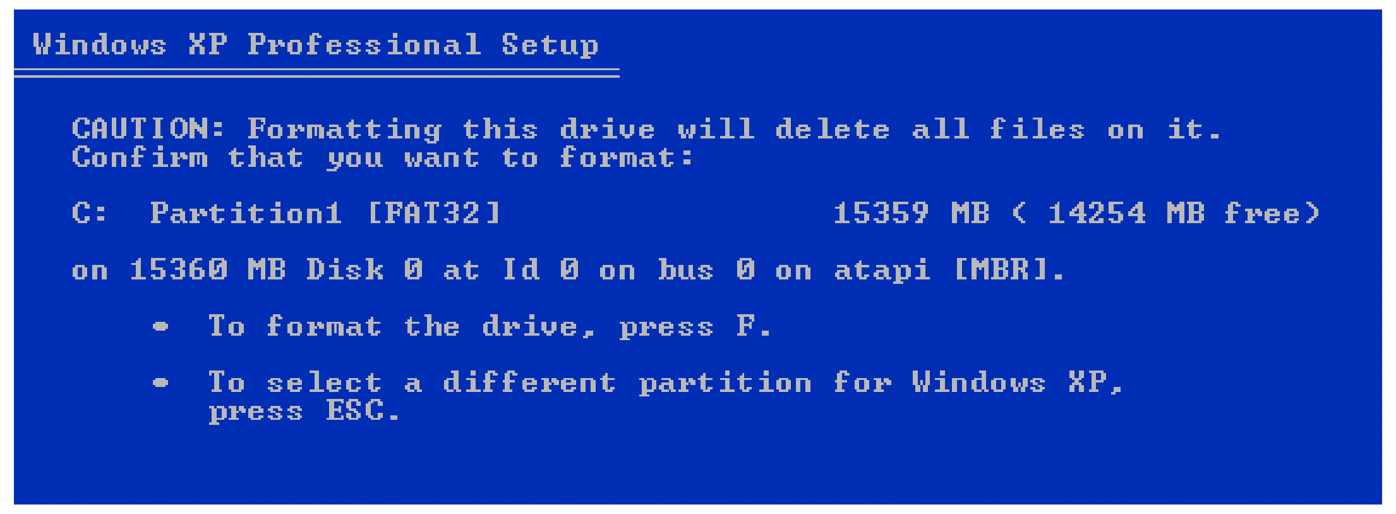
There are several options available for both open source and commercial data sanitization tools. When selecting a tool, the authors note it is important to select a tool that emphasizes patterns in write fill in addition to passes. This is imperative to making sure that slack and unallocated space is overwritten.
and no data was found.

Tool	Price	Platform	Where to Find the Tool
Darik's Boot & Nuke	Free	Unix/Linux, Mac, Windows	Tool can be found at http://www.dband.sourceforge.net
SecureClean	$39.95	Windows	Tool can be found at http://www.whitecanyon.com/secureclean-clean-hard-drive.php
Erase	Free	Windows	Tool can be found at http://eraser.heidi.ie/
Wipe	Free	Unix	Tool can be found at http://www.wipe.sourceforge.net

Who is Responsible? Legal Concerns

The concerns identified by the DFDR project are twofold, first the lack of regard of any sanitization practice whatsoever, and secondly the ineffectiveness of f-disk, format, and imaging [1].

When a computer is formatted, as part of a fresh install of Windows, there is a warning that informs the user that all of their data will be erased. If Microsoft is stating this, why shouldn't it be believed by the average user?



```
Windows XP Professional Setup

  CAUTION: Formatting this drive will delete all files on it.
  Confirm that you want to format:

  C:  Partition1 [FAT32]                 15359 MB ( 14254 MB free)

  on 15360 MB Disk 0 at Id 0 on bus 0 on atapi [MBR].

       •  To format the drive, press F.

       •  To select a different partition for Windows XP,
          press ESC.
```

Senate Bill S 1490 has been introduced several times for votes, but has yet to be signed into law. The bill aims to "**To prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information [22].**"

House bill H.R. 221 Data Accountability and Trust Act of 2009 (DATA), also aims to provide national coverage for victims of security breaches. Senate S. 3742 Data Security and Breach Notification Act, S 139, Data Breach Notification Act, and S 773 Cybersecurity Act of 2009 were also introduced into Congress in 2009. Passed into law.

Conclusion

Protect Your Data Yourself!

The DFDR project, which aimed to test sanitized drives only, found that those that were sanitized, were rarely done correctly. Digital media was acquired and analyzed to determine if one residual data was found, and also to determine if any residual data found can be used to steal an identity. The results demonstrated that proper data sanitization practices are not a key focus to most users, businesses, school districts, and government agencies. However, this was not the case for the electronic recycle center, which had great sanitization practices on lose media, but failed to apply the same process to drives internal to machines.

The ease of sanitization tools, such as Boot and Nuke, and their low-cost, if not free, should lead to more use of these tools to properly sanitize drives. The researches feel that if more people understood the ineffectiveness of current sanitation practices then more users, educational facilities, electronic recycle sites, and businesses would adopt proper procedures.