SSD Data Evaporation

DEF CON 21
August 2, 2013
Sam Bowne
@sambowne

I teach Ethical Hacking at City College San Francisco. My statements are my own, not official positions of CCSF.

San Francisco

http://samsclass.info
Twitter page
Data Remanence
Deleted Data

• On magnetic hard disks, data remains till it is overwritten

• Image from www.howstuffworks.com
DEMO on Windows

• Observing data on a magnetic hard disk after
  – Moving to Recycle Bin
  – Emptying Recycle Bin
  – Formatting Drive (Quick)
  – Formatting Drive (Slow)
Forensics & Data Recovery

• We can recover deleted data
• Find evidence of crimes
• Even after a format
• Very few criminals know enough to use encryption or forensic erasure
Useful Free Data Recovery Tools

• Recuva for PC
• Disk Drill for Mac
Your 24/7 Data Recovery Heroes

Need recovery help now? We’re available 24 hours a day, 7 days a week, 365 days a year. Give us a call—a data recovery advisor is ready to assist you.
SSDs
How SSDs Work

• Data can be read and written one page at a time, but can only be erased a block at a time
• Each erasure degrades the flash—it fails around 10,000 erasures
• From http://www.anandtech.com/show/2738/5
Garbage Collection

• SSD controller erases pages all by itself, *when it knows they are empty*

• The **TRIM** command is sent to the SSD when a file is deleted
  – But only if you use a the correct OS, Partition type, and BIOS settings

• Yuri Gubanov calls this “Self-Corrosion” – I call it **Data Evaporation**
Demo on Mac: Disk Drill

- Deleted files from desktop evaporate in 30-60 min
Data Evaporation From MacBook Air Desktop

# Recoverable Files

Time (min)

Test2
Test3
Test4
Test5
Test 6
Demo on PC

• Save data on an SSD
• Watch it evaporate!
• How to test TRIM
  – `fsutil behavior query DisableDeleteNotify`
  – Zero = TRIM enabled
When Does TRIM Work?

- **BIOS**: Drive must be SATA in AHCI mode, not in IDE emulation mode
- **SSD** must be new (Intel: 34 nm only)
- **Windows 7** or later
  - NTFS volumes, not FAT
- **Mac OS X 10.6.8** or later
  - Must be Apple-branded SSD
When Does TRIM Work?

• **External Drives** must use SATA or SCSI, not USB

• **PCI-Express & RAID** does not support TRIM
Expert Witness Testimony
Experience

• In court, an expert witness can state an opinion
• Must be based on personal experience
  – “I read it in a book” **NO**
  – “A teacher said it in a class” **NO**
  – “I know this because I tested it” **YES**
• So forensic examiners do a lot of testing
Summary

• SSDs retain deleted data sometimes
• Other times they don’t
• It depends on
  – Manufacturer
  – OS
  – BIOS
  – Interface
  – Who knows what else
The evap Tool

For Mac OS X Only
Sams-MacBook-Air:e0 sambowne$ sudo ./evapl

*******************************************************************************
* BEFORE USING THIS TOOL, DO THESE TWO STEPS:                              *
* 1. Use Disk Utility to create a 1 GB partition on your SSD named ssd, so it appears in df as /Volumes/ssd *
* 2. Edit the evapl file to adjust the HOMEDIR variable to your working directory (I recommend /e) *
*******************************************************************************

Option (? for help): ?
Run with sudo!

C - Count X's on /Volumes/ssd
D - Delete Test Files from /Volumes/ssd
E - Erase /Volumes/ssd with diskutil eraseVolume JHFS+
F - Erase /Volumes/ssd with diskutil eraseVolume HFS+
L - List Test Files on /Volumes/ssd
Q - Quit
S - Scan SSD
T - Adjust TRIM settings (Risky!)
W - Write Test Files to /Volumes/ssd
X - Write Test Files Containing X's to /Volumes/ssd

Option (? for help):
Evaporation on JHFS+
No Evaporation on HFS+

Option (? for help): F
  Erasing test partition...
Started erase on disk0s4 ssd
Unmounting disk
Erasing
Initialized /dev/rdisk0s4 as a 950 MB HFS Plus volume
Mounting disk
Finished erase on disk0s4 ssd
  Test Volume Erased with diskutil eraseVolume HFS+

Option (? for help): W
Volume ssd on /dev/disk0s4 mounted
  2.25 real    1.59 user    0.39 sys
  Test Files Written to /Volumes/ssd (From /e0/fill.gz)

Option (? for help): S
  Volume ssd on disk0s4 unmounted

    SCAN: -\]^^^^--------AABBCCDDEEFFGGHHIIJJKKLLLLMMNN0000PPQQRRRSSSTUUUVVwWXXYYZZZ[[--

    Volume ssd on /dev/disk0s4 mounted
Option (? for help): D
  0.01 real    0.00 user    0.00 sys
  Test Files Deleted from /Volumes/ssd

Option (? for help): S
  Volume ssd on disk0s4 unmounted

    SCAN: -\]^^^^--------AABBCCDDEEFFGGHHIIJJKKLLLLMMNN0000PPQQRRRSSSTUUUVVwWXXYYZZZ[[--

    Volume ssd on /dev/disk0s4 mounted
Option (? for help): 
More Info

• Slides, instructions for the attacks, & more at Samsclass.info