

May 13, 2019

**“Safe Disposal of Computers & Mobile  
Devices”**

Joel Ewing, BVCC

See <http://bvcompclub.org>  
for Bits & Bytes Newsletter, meeting information,  
Help Sessions & class information

# Safe Disposal of Computers & Mobile Devices

- **Applies when re-purposing a device for use by someone else**  
**or**
- **"Trashing" a device that is too obsolete to be of use to others or which is no longer functional (which may restrict your options for erasing data)**

# Safe Disposal of Computers & Mobile Devices

- **Environmental considerations – electronic devices contain a mix of toxic heavy metals: lead, mercury, cadmium, beryllium, gallium, selenium, arsenic, zinc, cobalt, tin, palladium, plus other hazardous materials.**
- **Deletion of personal information – devices can retain account login information, documents and images of a personal nature that should be properly erased to make inaccessible to others.**

# Environmental Considerations

- **Do not throw out with ordinary trash – use a service or facility for disposal or recycling of electronics (which applies to other devices with electronics as well)**
- **Benton County, AR main disposal site for Electronics is the "Centerton" facility at 5702 Brookside Rd, Bentonville, AR, Monday thru Saturday 8:00 am to 3:30 pm.**

# Centerton Disposal Site



# Security of Personal Information

- **Types of info one wants to protect:**
  - Financial and other personal records
  - login and account information for on-line accounts
  - Email archives & contacts list
  - Purchased software and registration codes that have been transferred to another device
  - Any information that might put you, your family, or your friends at risk for ID theft, financial loss, or other risks
- **You may not know everything stored on the device – safest to secure-erase everything possible before the device leaves your control, or find someone you can trust to do a secure erase.**

# Security of Personal Information

- **Desktop & laptop computers have a hard drive which can contain a large amount information almost indefinitely and which needs to be securely erased when you will no longer use the device.**
- **Smart phones and computer pads have non-volatile solid state storage that needs to be erased.**
- **Specialized computer devices like Roku & Apple TV streaming devices, routers, etc. may not contain much personal information, but should be factory-reset to erase any account logins for streaming services and WiFi passwords.**

# How Paranoid Should You Be

- **If you are wealthy, famous, powerful, or deal with highly classified material, paranoia is probably justified. Employ DoD, 7-pass overwrite secure erase and if that is not possible, physically destroy mechanical or solid-state storage devices.**
- **For the rest of us, a 3-pass DoD overwrite is probably more than adequate**
- **Superuser.com has claim that a single random-data overwrite on modern hard drives is sufficient. Not yet able to confirm that claim, which may depend on what constitutes "modern"**



# Functional Desktops & Laptops

- **Backup and/or migrate all data of possible interest (including license keys for retained software).**
- **Boot a stand-alone utility to securely erase the hard drive – solid state hard drives typically require a special utility from the SSD manufacturer**
- **Optionally install a new Operating System**
  - **Additional obfuscation possible – enable encryption, add large bogus files, destroy partitions & quick reformat to encourage someone to waste time recovering useless data.**

# Non-Functional Desktops & Laptops

- **If unable to boot successfully even from external media, it is still possible the hard drive(s) might be OK and contain data you should wipe.**
- **Need to remove hard drive(s), which may still be functional, from device, and try using an adapter to make the internal drive into an external USB drive or install drive in another computer and see if it can be accessed from a different functional computer.**
- **If hard-drive can be accessed, use another computer for backup and secure erase of old drive; otherwise, physical destruction of drive is required (as repair of hard drive or recovery of some data from physical platters inside drive might be possible)**

# Mechanical Hard Drive Erase Utility

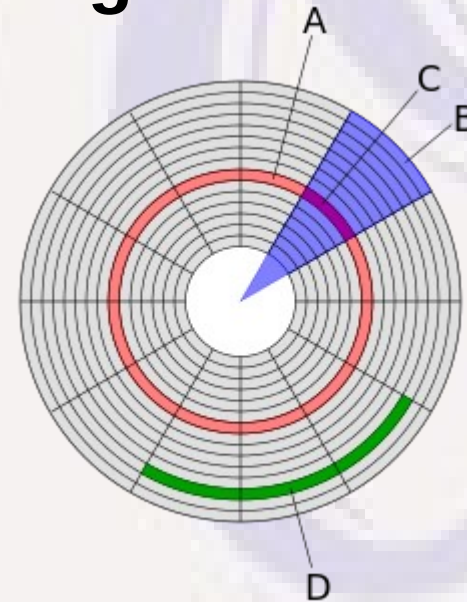
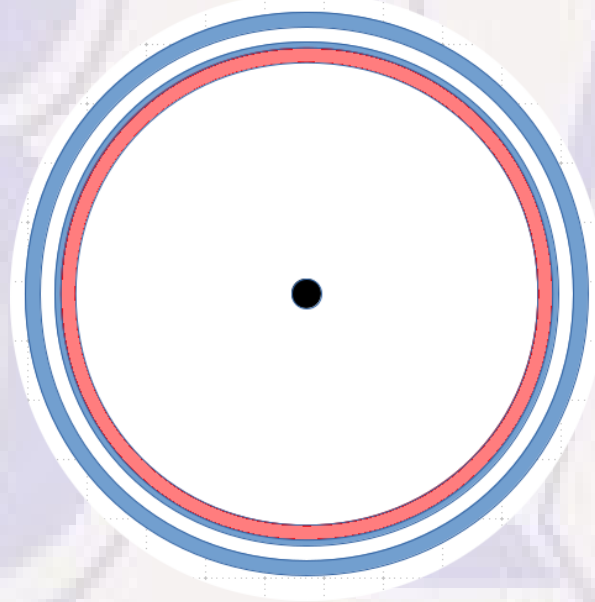
- **Both free and non-free utilities that can be run on a functional computer to erase a hard drive by multiple overwrites of all tracks**
- **Hard drive can either be mounted internally or be accessed as an external USB drive**

# Mechanical Hard Drive Erase Utility

- **Free Utility DBAN (Darik's Boot & Nuke)**  
<https://sourceforge.net/projects/dban/>
  - iso image can be burned to CD or DVD
  - Can be burned to bootable USB thumb drive, but finding a way that works is non-trivial
- **If a business requires a formal "certificate" of secure erasure printed by an erase utility, that may require a non-free utility**

# Mechanical Drive Erase Utility

- **Why multiple overwrites?**
  - **Read/Write head positioning is precise enough for reliable operation but not precise enough to guarantee that one overwrite won't leave traces of previous contents at the edges of a track.**




# Darik's Boot and Nuke (DBAN)

## Darik's Boot and Nuke

**Warning:** This software irrecoverably destroys data.

This software is provided without any warranty; without even the implied warranty of merchantability or fitness for a particular purpose. In no event shall the software authors or contributors be liable for any damages arising from the use of this software. This software is provided "as is".

<http://www.dban.org/>

- \* Press the F2 key to learn about DBAN.
- \* Press the F3 key for a list of quick commands.
- \* Press the F4 key to read the RAID disclaimer.
- \* Press the ENTER key to start DBAN in interactive mode. 
- \* Enter autonuke at this prompt to start DBAN in automatic mode.

**boot:**

**WARNING: Erases ALL accessible drives** 

# Darik's Boot and Nuke (DBAN)

- **Interactive mode allows choice of device and wipe options.**
- **Wipe Method common choices**
  - **DoD Short – 3 passes, adequate for most**
  - **DoD 5220.22-M – 7 passes, overkill for most**
  - **Quick Erase – single pass, not that secure**
- **Time required proportional to tracks x passes, inversely proportional to hard drive RPM. Access as USB drive slower.**
  - **DoD Short erase on 320GB drive took almost 5 hrs**
  - **Some combinations could take over 24 hours**

# Darik's Boot and Nuke (DBAN)

```
Darik's Boot and Nuke 2.3.0
----- Options -----
Entropy: Linux Kernel (urandom)
PRNG:    Mersenne Twister (mt19937ar-cok)
Method:  DoD Short
Verify:  Last Pass
Rounds:  1
----- Statistics -----
Runtime:    00:02:18
Remaining:  04:06:25
Load Averages: 1.86 0.87 0.34
Throughput: 107245 KB/s
Errors:     0

ATA Disk SAMSUNG HD322HJ 1113 298GiB (320GB) S1GXJ90QA00321
[00.92%, round 1 of 1, pass 1 of 3] [writing] [107245 KB/s]
```



# Darik's Boot and Nuke (DBAN)

```
Darik's Boot and Nuke 2.3.0
----- Options -----
Entropy: Linux Kernel (urandom)
PRNG: Merseenne Twister (mt19937ar-cok)
Method: DoD Short
Verify: Last Pass
Rounds: 1
----- Statistics -----
Runtime:
Remaining:
Load Averages:
Throughput:
Errors:
----- Wipe Method -----
▶ Quick Erase          syslinux.cfg: nuke="dwipe --method zero"
  RCMP TSSIT OPS-II   Security Level: Low (1 pass)
  DoD Short
  DoD 5220.22-M
  Gutmann Wipe
  PRNG Stream

This method fills the device with zeros. Note that the rounds option does
not apply to this method. This method always runs one round.

Use this method to blank disks before internal redeployment, or before
reinstalling Microsoft Windows to remove the data areas that the format
utility preserves.

J=Up K=Down Space=Select
```

# SSD Erase Utilities

- **Use of HD multiple overwrite techniques with SSD will shorten lifespan of SSD and potentially leave residual data**
- **Need to download free utility from manufacturer**
  - **Example: search for " Samsung 860 EVO secure erase utility" finds "Samsung SSD Magician"**
  - **Can be run from a Windows system to erase a secondary drive or create a bootable CD or USB drive to erase a primary drive**
  - **Consider download of appropriate utility for newly acquired SSD before your SSD becomes obsolete**

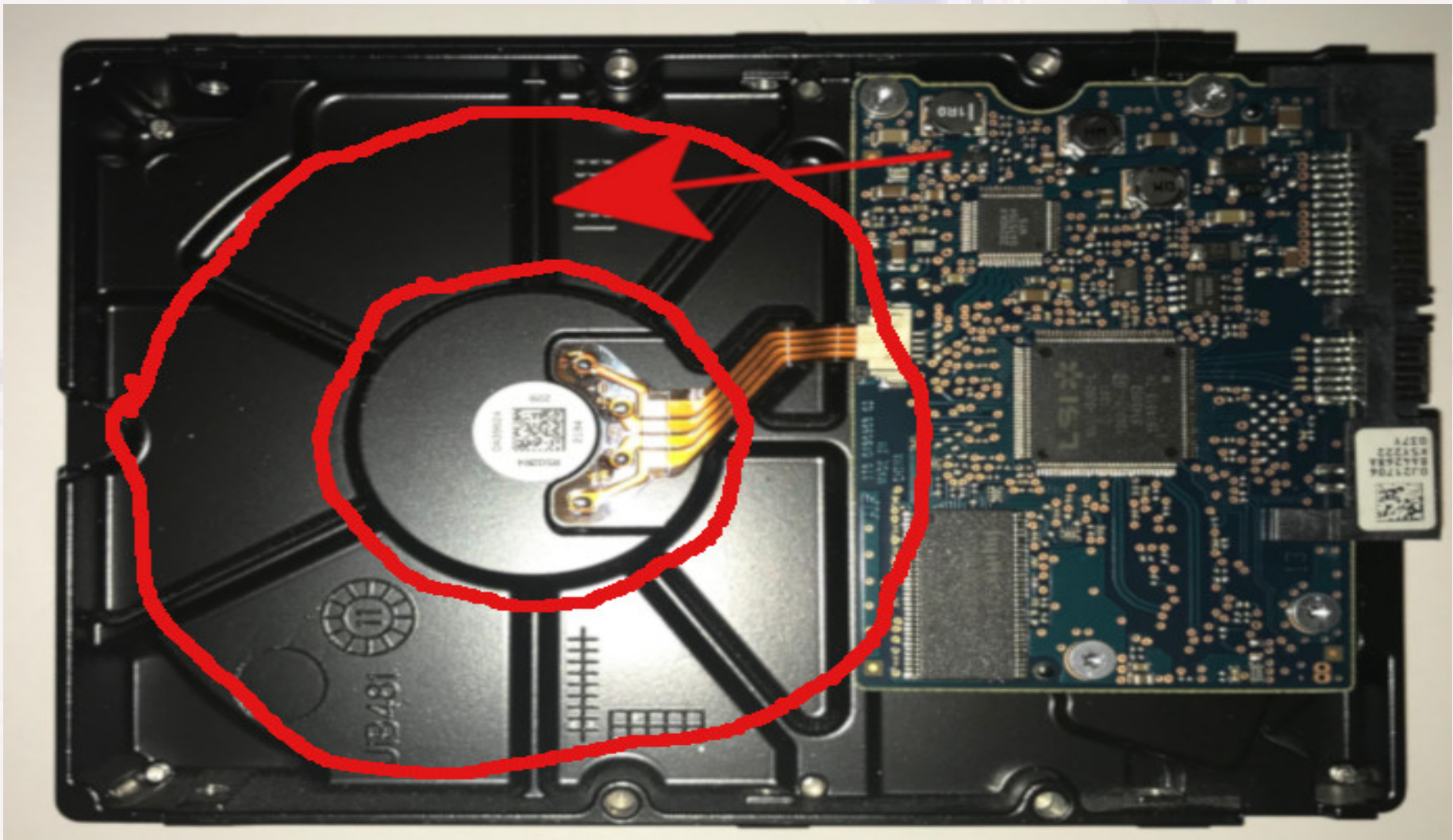
# Physical Destruction of a Hard Drive

- **When hard drive not functional to overwrite:**
- **Heat not practical – extreme heat req + toxic fumes**
- **Sledge hammer may seriously damage outer case but still leave internal platter surfaces OK**
- **Best practical option – using protective glasses, drill holes through the hard drive so that data portion of platters damaged (Search "destroy hard drive " for Youtube videos)**
- **High-security Alternative (need set of TORX driver bits) – disassemble hard drive, remove individual platters, sand off surface of platters – hard drive construction details see [http://hddscan.com/doc/HDD\\_from\\_inside.html](http://hddscan.com/doc/HDD_from_inside.html)**



# Physical Destruction of a Hard Drive

- **Where to Drill holes**



# Physical Destruction of a Hard Drive

- **What you're trying to destroy**



# Secure Erase of iPhone & iPad

- **Backup or migrate data to new device (iCloud, iTunes)**
- **Remove SIM card from the old device (typically need a pin-like tool). May be able to use same SIM in new device to transfer cell service.**
- **Verify old device was protected by passcode or Touch ID**
- **On old device, Use Settings → General → Erase all Contents and Settings to clear all your data**
  - **On IOS 8 or later, if passcode or Touch ID in use, all personal data is encrypted. "Erase all Contents and Settings" does a secure erase of the encryption key which guarantees any residual data left in storage is unreadable**

# Android Phones and Tablets

- **After backup and migration of data of interest:**
  - **Disable Factory Reset Protection (FRP) for Android 5.0 and later**
  - **Remove your Google account. If Samsung Galaxy, also remove your Samsung account**
  - **If prior to Android 6.0, enable encryption of data if not already enabled (make take several hours, so phone should be plugged in or fully charged)**
  - **Perform a Factory Data Reset to "erase" data. Any residual data should be useless without encryption key**
  - **Reference:**  
**<https://www.digitaltrends.com/mobile/how-to-wipe-your-android-phone-or-tablet/>**

# Other Devices on Your LAN

- **Routers, Smart TVs, TV Streaming Boxes, Home Automation Controllers, wireless printers, etc.**
  - All know your home LAN access codes
  - Some know account login codes for subscription streaming services or for free accounts. Good idea to keep a record of what accounts are known to a device in case it breaks.
  - Each of these devices has its own way to "reset to factory state", a reset button or "settings" access. Save or find on-line copy of manual and reset the device before disposing, if device sufficiently functional to do so. No way to know how securely old data is erased.
  - If device not functional, decide whether exposure is serious enough to warrant changing passwords on affected accounts.
    - One should not give such devices login information that could compromise any email account that is used as a user name for unrelated on-line accounts



# Plan Ahead For Added Security

- **To avoid need for multiple overwrites on extremely large HD, or special utilities for SSD secure erase, use partition encryption for all partitions containing sensitive data**
  - Linux comes with support for encryption setup at install time
  - Windows 10 Pro has "Bit Locker" that can be turned on after install – easy to use if hardware has a special Trusted Platform Module chip, takes research otherwise.  
<https://www.windowscentral.com/how-use-bitlocker-encryption-windows-10>
  - Secure destruction of encryption key effectively destroys data access and makes even a single overwrite of HD more than adequate
  - Can also keep data secure if device lost or stolen (provided key must be supplied by user)

Questions?

BWS