DBAN

What is DBAN?

- DBAN short for Darik’s Boot and Nuke
- Developed by Darik Horn
- Live bootable Linux distribution for erasing magnetic media

Where to get DBAN

- It can be downloaded for free at dban.org

What can DBAN do?

- Erase magnetic media: Hard drives, floppy drives.
- Contains multiple options for erasing:
- PRNG (pseudo random number generator)
- Wipe method
- Verifying wipe
- Number of rounds

Autonuke

- Typing in “autonuke” at the DBAN home screen starts a automatic wipe using default settings of all the connected drives.
- These settings are “DOD 5220.22M short wipe” of three passes, and of the last of three passes it verifies the wipe.

PRNG

- PRNG is short for pseudo random number generator.
- The PRNG is used for generating random data to write to the disk.
- The two PRNG’s in DBAN are:
- Mersenne Twister
- ISAAC

PRNG

- Neither of the PRNG’s found in DBAN are cryptographically secure.
- However since the purpose of the PRNG’s in DBAN is to just generate random data they serve the purpose just fine, since DBAN isn’t encrypting anything.

Wipe Method

- **Quick Erase: Fills the drive with zeros.**
- **RCMP TSSIT OPS-II: The Royal Canadian Mounted Police spec for erase data. Overwrite the data with zeroes, ones, zeroes, ones, zeroes, ones, and random data, and verify the final write.**
- **DoD Short: Short Department of Defense spec. Overwrite the data with a value, then with the inverse of that value, then with a random value, verifying the write after each step. The first two wipes theoretically pull the magnetic field fully one direction, then fully the other, eliminating any residue of the original value.**

Wipe Method

- DOD 5220.22-M: A 7 pass version of the DoD Short.
- Gutmann 35-pass: Does a 35 passes of writing zeros.
- PRNG Stream: Does a pass using the PRNG. It is just as fast a the Quick Erase, and is more secure.

Verify

- The Verify screen gives you options on how you want to verify the wipe process.
- You can have it set to verify the last pass, every pass, or set it to not verify at all.
- Verifying does increase the amount of time it takes to wipe a disk.

Rounds

- **The rounds screen is for setting how many times you want DBAN to run through a wipe session using the settings you have selected.**

What can’t DBAN do?

- Erase flash media. This is due to the way flash storage controllers work. In an attempt to extend drive life, flash media controllers will use something called wear leveling to evenly spread out the writes.
- Erase spare sectors. Spare sectors is extra space not seen by the user to be swapped out for in case of a bad sector.

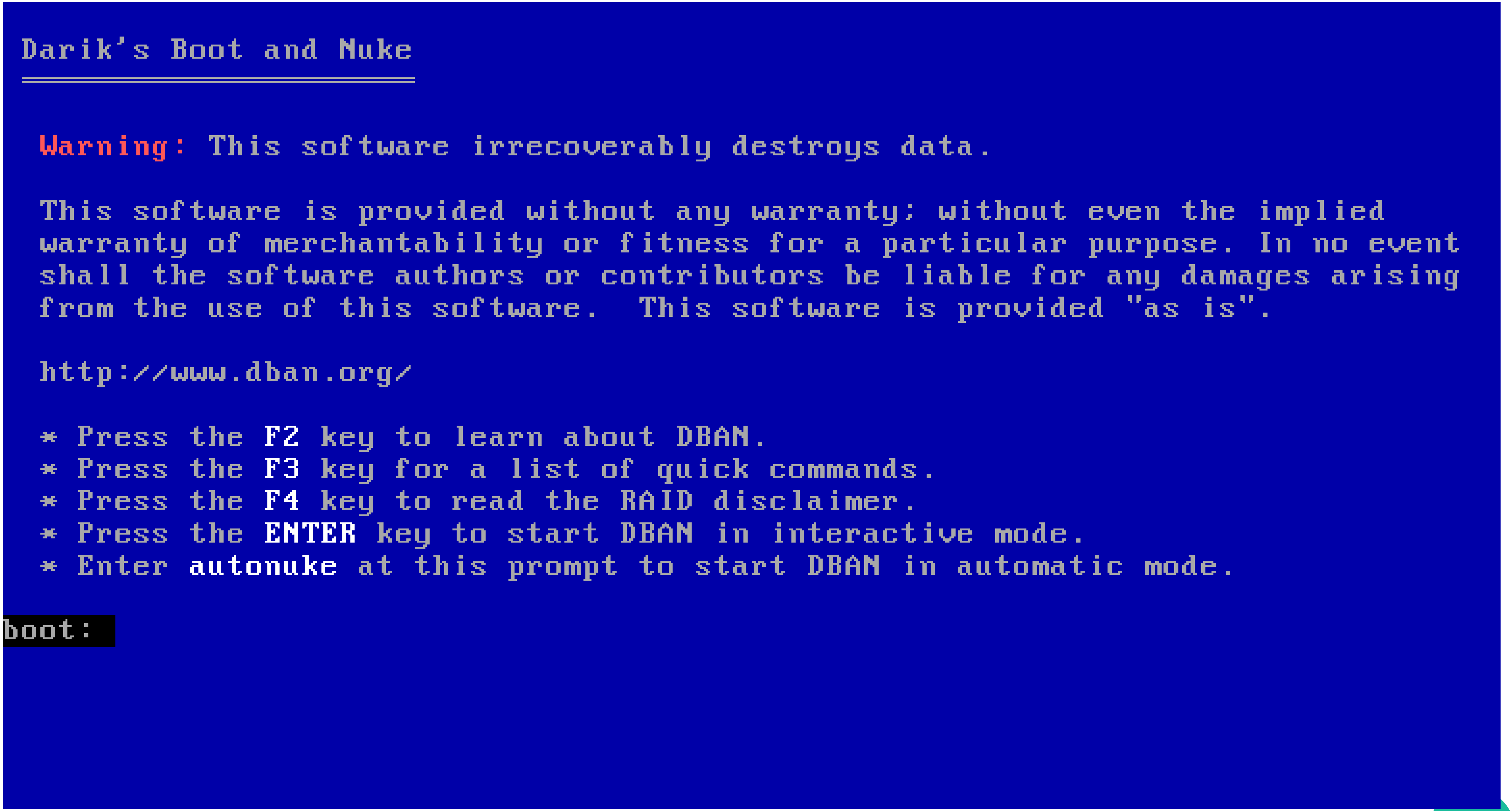
What can’t DBAN do?

- Flash media should be erased using the manufactures provided software. Most flash media manufactures will provide free software which can securely erase it.

Why erase hard drives?

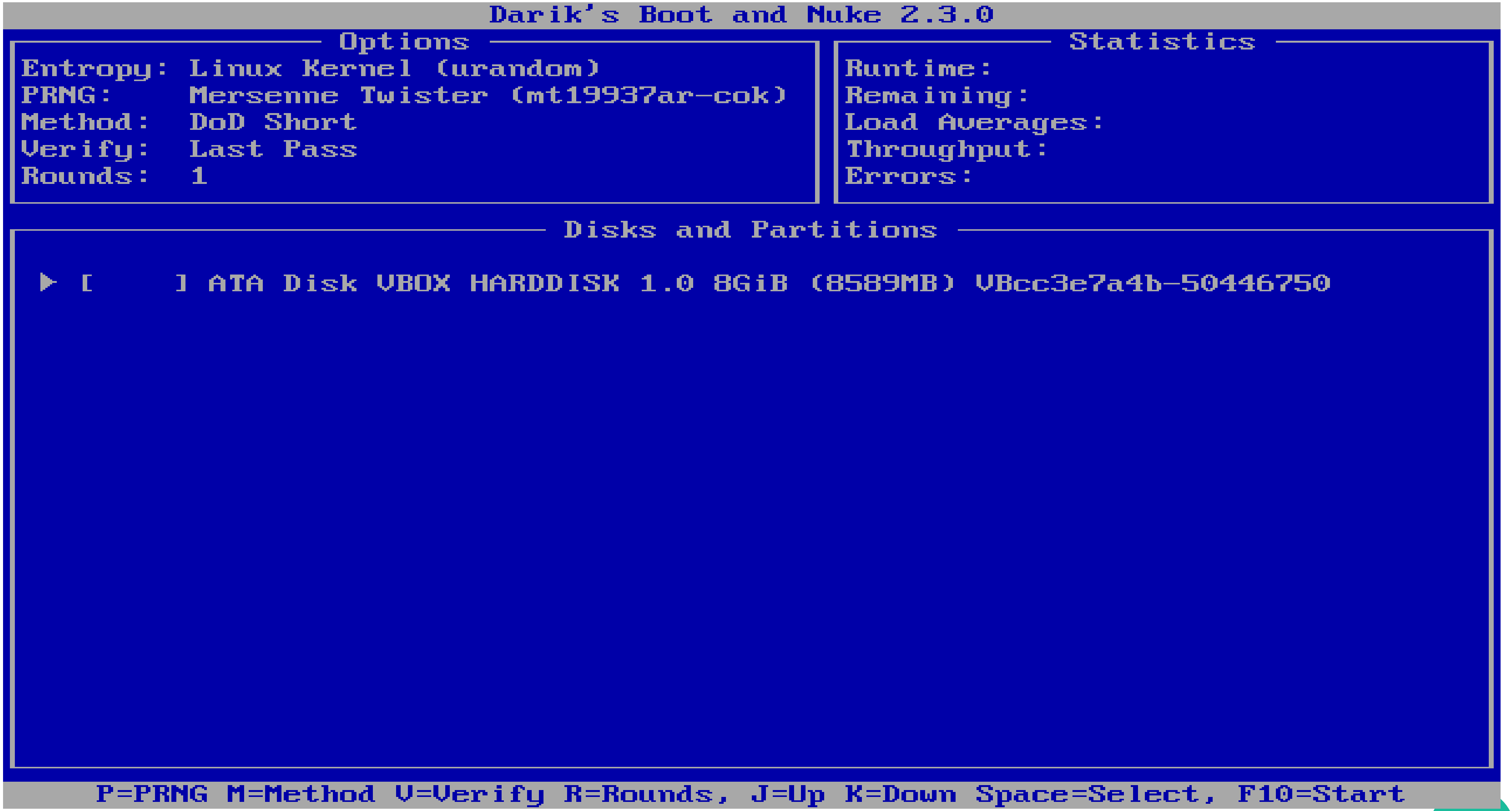
- A study by a computer security firm found that 40% of hard drives for sale on eBay still contained sensitive info.
- The info contained personal financial info, business finances, photos, and emails.
- https://www.computerworld.com/article/2530795/survey--40--of-hard-drives-bought-on-ebay-hold-personal--corporate-data.html

DBAN Boot Screen



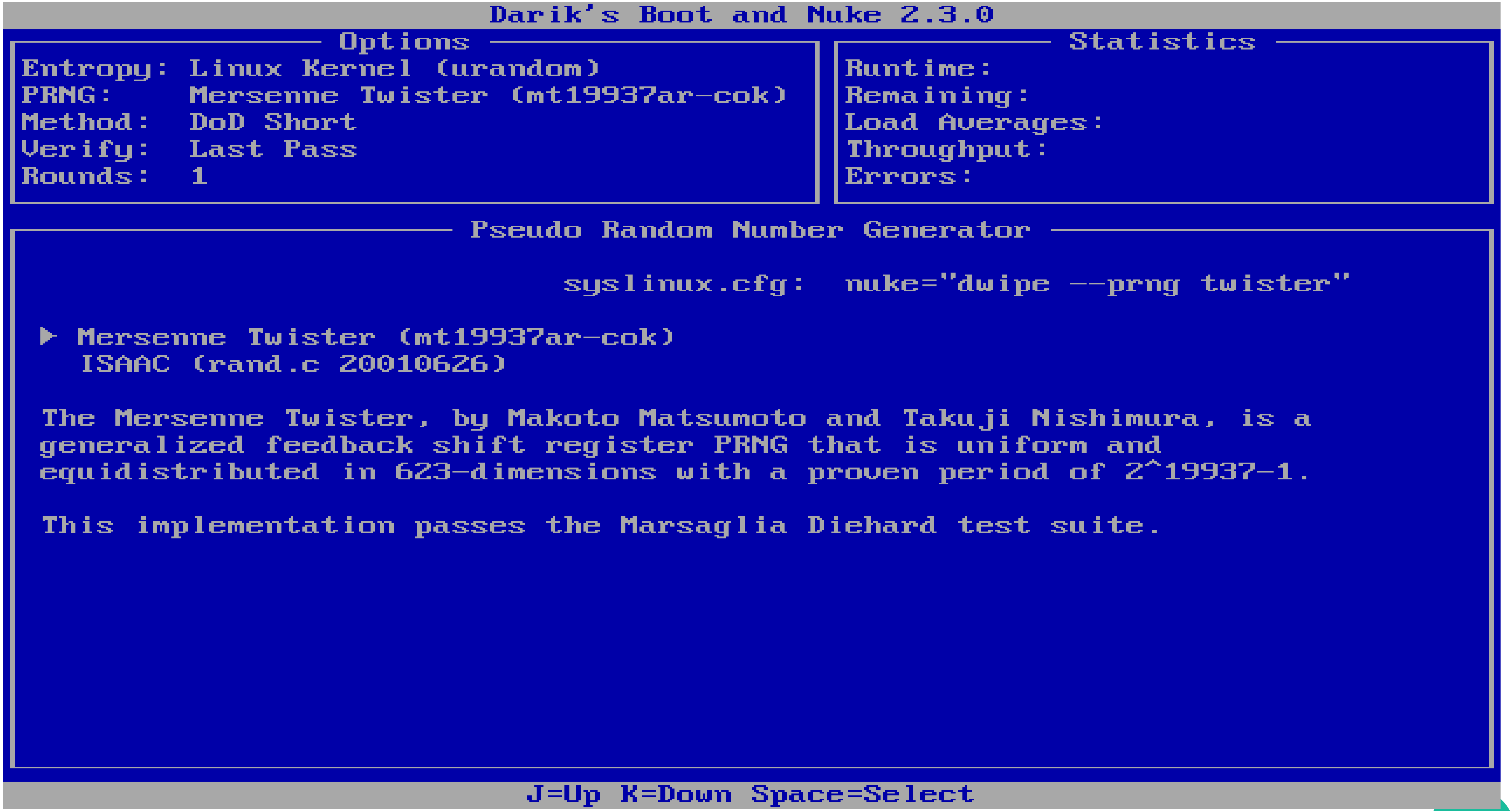
```
Darik's Boot and Nuke

 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:
```

DBAN Home Screen



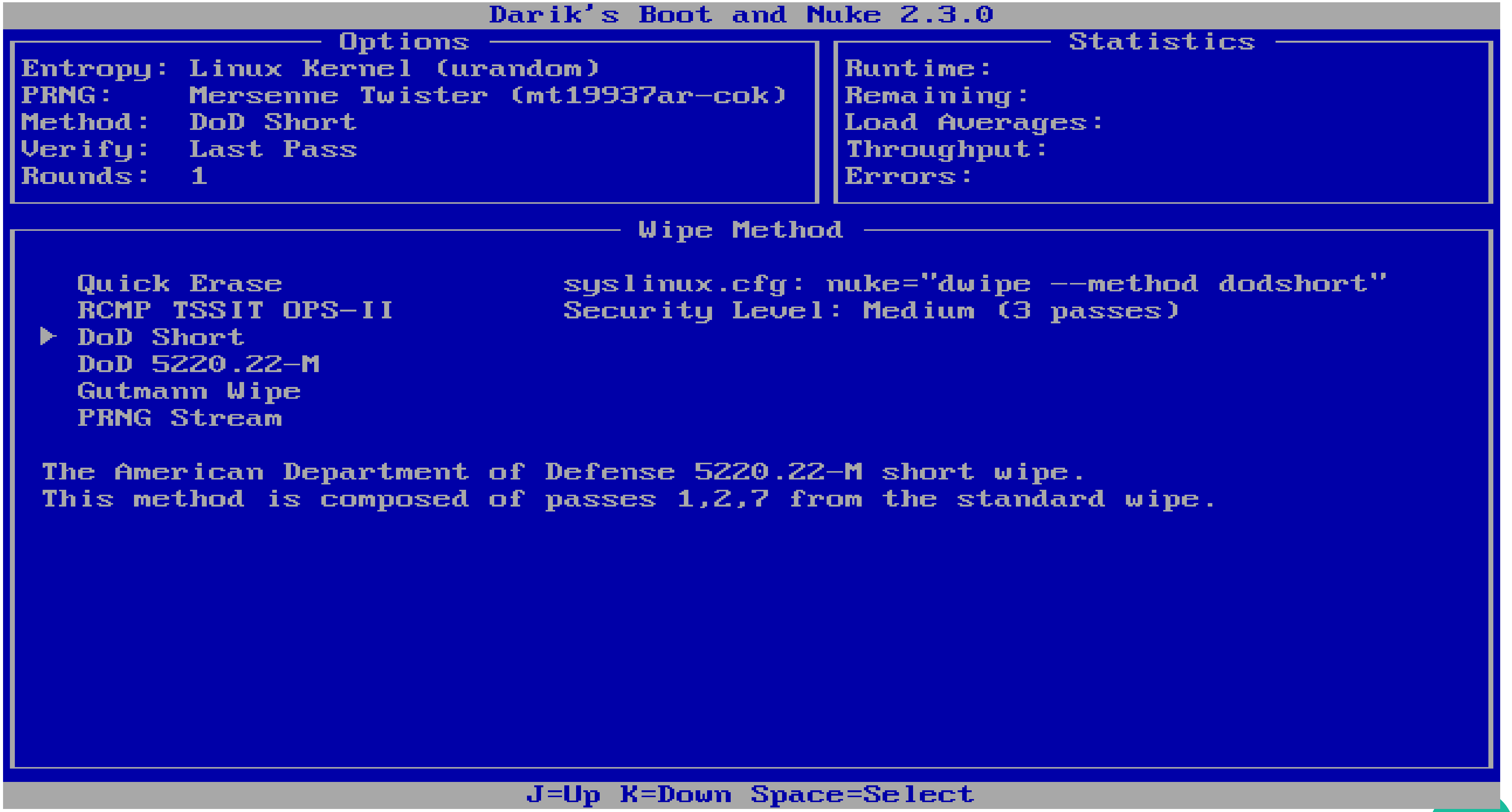
```
                         Darik's Boot and Nuke 2.3.0
                Options                                       Statistics
Entropy: Linux Kernel (urandom)               Runtime:
PRNG:    Mersenne Twister (mt19937ar-cok)     Remaining:
Method:  DoD Short                            Load Averages:
Verify:  Last Pass                            Throughput:
Rounds:  1                                    Errors:

                         Disks and Partitions

 ▶ [     ] ATA Disk VBOX HARDDISK 1.0 8GiB (8589MB) VBcc3e7a4b-50446750

   P=PRNG M=Method V=Verify R=Rounds, J=Up K=Down Space=Select, F10=Start
```

DBAN PRNG Screen



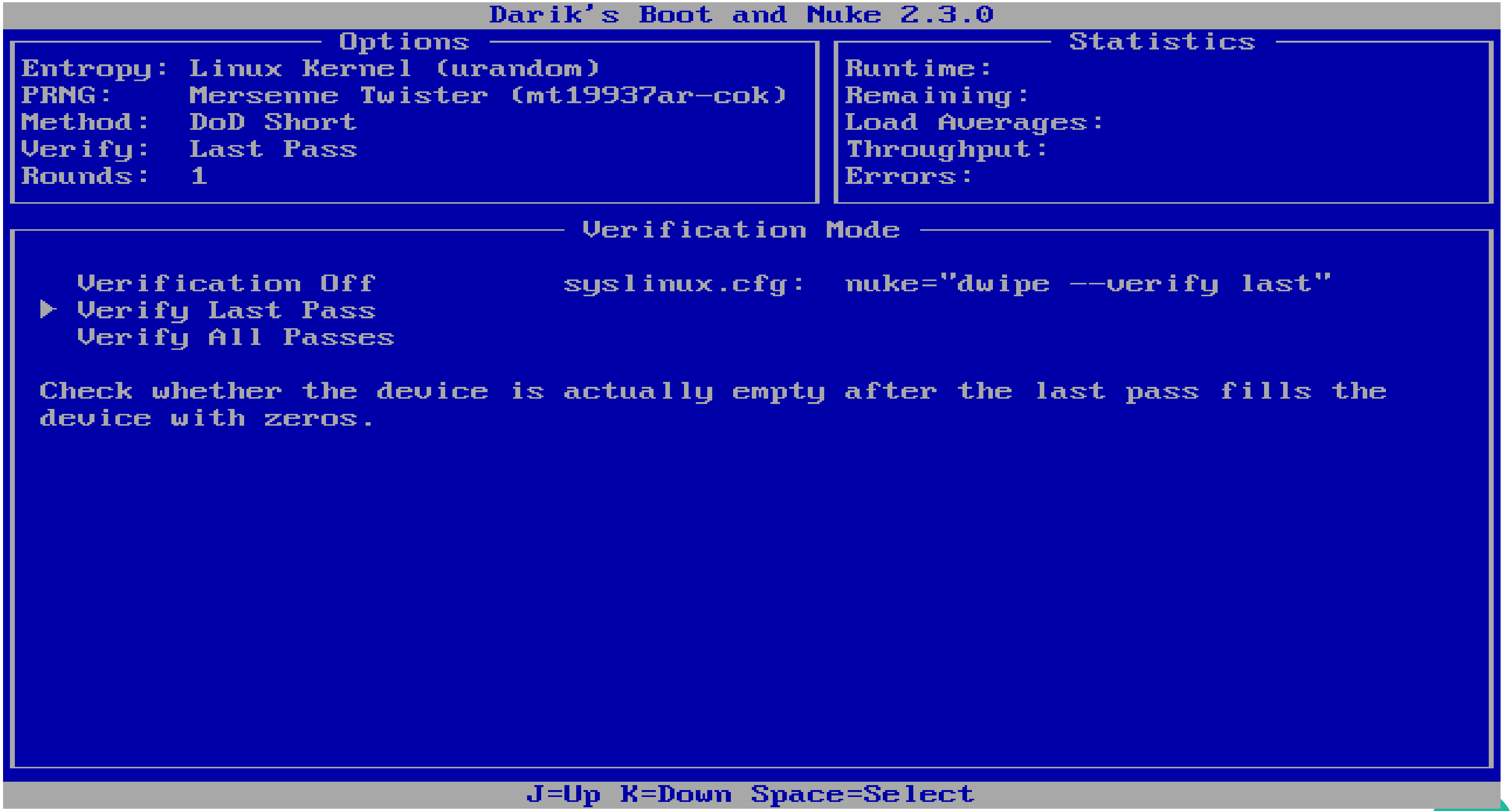
```
                        Darik's Boot and Nuke 2.3.0
 ------------------- Options -------------------  ----------- Statistics -----------
 Entropy: Linux Kernel (urandom)                   Runtime:
 PRNG:    Mersenne Twister (mt19937ar-cok)         Remaining:
 Method:  DoD Short                                Load Averages:
 Verify:  Last Pass                                Throughput:
 Rounds:  1                                        Errors:

 ---------------------- Pseudo Random Number Generator ----------------------

                              syslinux.cfg:  nuke="dwipe --prng twister"

  ▶ Mersenne Twister (mt19937ar-cok)
    ISAAC (rand.c 20010626)

  The Mersenne Twister, by Makoto Matsumoto and Takuji Nishimura, is a
  generalized feedback shift register PRNG that is uniform and
  equidistributed in 623-dimensions with a proven period of 2^19937-1.

  This implementation passes the Marsaglia Diehard test suite.

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

DBAN Method Screen



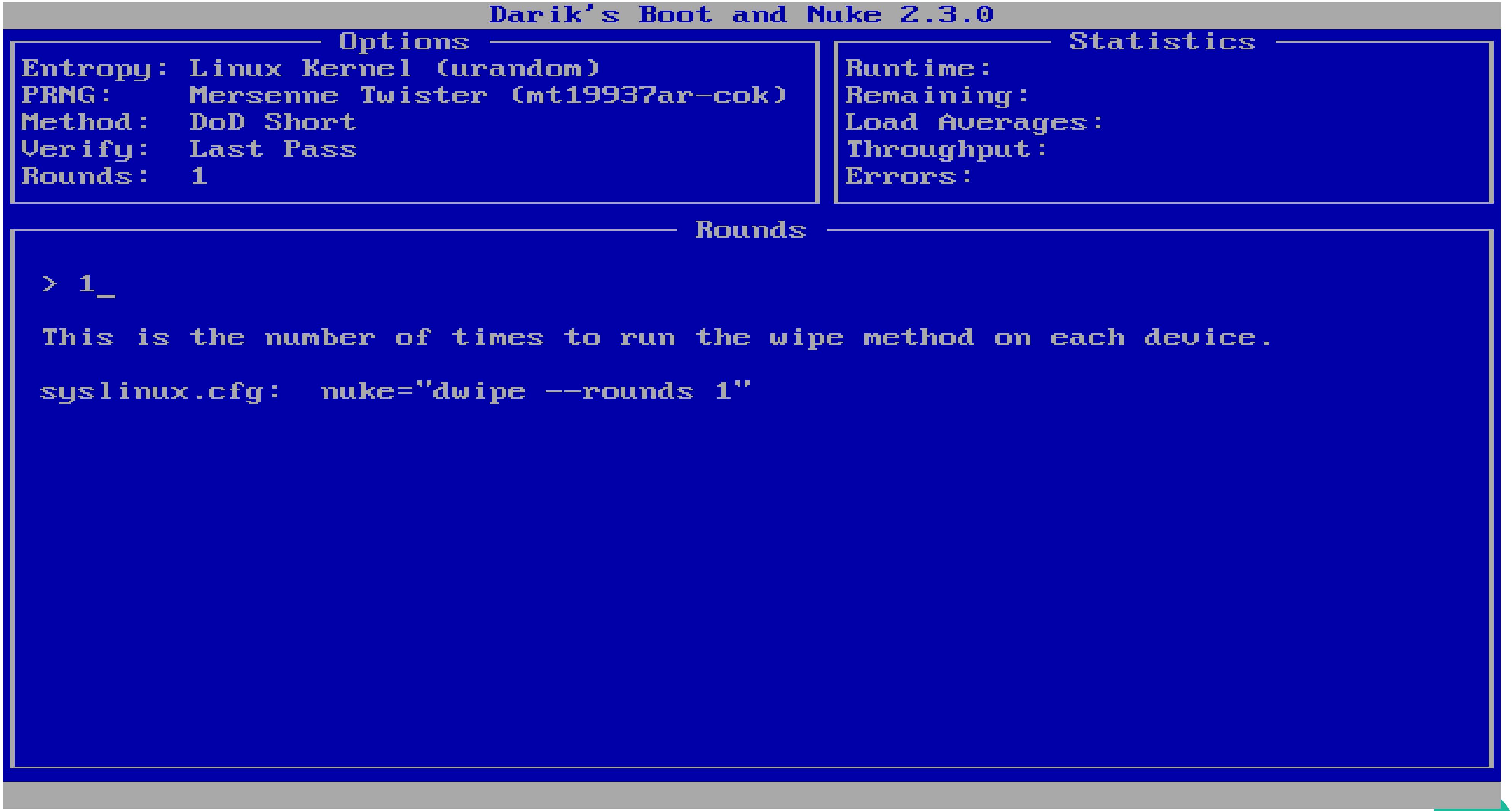
```
                        Darik's Boot and Nuke 2.3.0
 ---------------- Options ------------ ------------ Statistics -------------
| Entropy: Linux Kernel (urandom)        | Runtime:                          |
| PRNG:    Mersenne Twister (mt19937ar-cok) | Remaining:                     |
| Method:  DoD Short                     | Load Averages:                    |
| Verify:  Last Pass                     | Throughput:                       |
| Rounds:  1                             | Errors:                           |
 ---------------------------------------- -----------------------------------
 ------------------------------- Wipe Method --------------------------------
|                                                                            |
|   Quick Erase                 syslinux.cfg: nuke="dwipe --method dodshort" |
|   RCMP TSSIT OPS-II           Security Level: Medium (3 passes)            |
| ▶ DoD Short                                                                |
|   DoD 5220.22-M                                                            |
|   Gutmann Wipe                                                             |
|   PRNG Stream                                                              |
|                                                                            |
| The American Department of Defense 5220.22-M short wipe.                   |
| This method is composed of passes 1,2,7 from the standard wipe.            |
|                                                                            |
 ----------------------------------------------------------------------------
                       J=Up K=Down Space=Select
```

DBAN Verify Screen



```
                      Darik's Boot and Nuke 2.3.0
 ---------------- Options --------------   ----------- Statistics -----------
 Entropy: Linux Kernel (urandom)            Runtime:
 PRNG:    Mersenne Twister (mt19937ar-cok)  Remaining:
 Method:  DoD Short                         Load Averages:
 Verify:  Last Pass                         Throughput:
 Rounds:  1                                 Errors:

 -------------------------- Verification Mode --------------------------

     Verification Off          syslinux.cfg:  nuke="dwipe --verify last"
   ▶ Verify Last Pass
     Verify All Passes

   Check whether the device is actually empty after the last pass fills the
   device with zeros.

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

DBAN Rounds Screen



```
                        Darik's Boot and Nuke 2.3.0
──────────────── Options ───────────  ──────────── Statistics ──────────
Entropy: Linux Kernel (urandom)        Runtime:
PRNG:    Mersenne Twister (mt19937ar-cok)  Remaining:
Method:  DoD Short                     Load Averages:
Verify:  Last Pass                     Throughput:
Rounds:  1                             Errors:

─────────────────────────────── Rounds ───────────────────────────────

 > 1_

 This is the number of times to run the wipe method on each device.

 syslinux.cfg:  nuke="dwipe --rounds 1"
```

Questions?