Procedure for Sanitizing Hard Drives.

All hard drives should be sanitized and formatted before each use on new cases. The hard drive should be sanitized in accordance with DoD 5220.22-M standards prior to being formatted for use. If DoD 5220.22-M approved software is not available for the sanitization process the following procedure can be substituted as an interim solution. This procedure follows DoD guidelines in writing data to all the sectors on the disk 7 times. We are basically alternating the writing of 0's and random numbers to every sector on the disk for a total of 7 writes.

Step 1: Use the dd command to nullify the hard drive on the Forensic Workstation. Command: dd if=/dev/zero of=/dev/hd[b-d] bs=1024

Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46

Command Explanation: "dd" Invoke the dd command

"if=/dev/zero" this instructs dd to get input from file /dev/zero. This is a system device driver that will return binary zero's as data for every input read request.

"of=/dev/hd[b-d]" this instructs "dd" to direct output to the system device file of /dev/hd[b-d]". The operator performing this operation should be familiar with the forensic workstation and know the identity of new disk drives. Normally, the primary IDE hard drive is called "/dev/hda", the second IDE hard drive is called "/dev/hdb", the DVD/CD-R is called "/dev/hdc", and the third IDE drive is called "/dev/hdd". However, systems can be configured differently and the operator should have definitive knowledge of the workstation before attempting this procedure. If you do not know what you are doing – STOP and seek assistance.

"bs=1024" states that all IO operations will be in data blocks of 1024 bytes, which is the standard block size for most Linux and NTFS systems.

(The Forensic Workstation user needs to be familiar with all devices attached to the workstation and their physical IO requirements before attempting this procedure.)

Step 2: Use the dd- command to write random numbers to the removable media.

Command: dd if=/dev/urandom of=/dev/hd[b-d] bs=1024

Command Explanation: "dd" Invoke the dd command

"if=/dev/urandom" this instructs dd to get input from the file /dev/urandom. This is a system device driver that will return a continuous string of random numbers.

"of=/dev/hd[b-d]" this instructs "dd" to direct output to the system device file of /dev/hd[b-d] which should be your new hard drive.

"bs=512" states that all IO operations will be in data blocks of 512 bytes, which is the sector size on floppy disks.

Step 3: Repeat Step 1.
Step 4: Repeat Step 2.
Step 5: Repeat Step 1.
Step 6: Repeat Step 2.
Step 7: Repeat Step 1.
Step 8: Format the media for appropriate use (MSDOS/Windows or Linux/Unix). MSDOS Command: format C: /FS:NTFS /V:FOR_LAB_1 /X

Linux Command: mk.ext2fs –c /dev/hdd1

Step 9: Fill out the Hard Drive Equipment Tag and affix label to the exterior of the hard drive.