Unix and Linux Forensics

- Files are objects with properties and methods
- Block is a disk allocation unit of at least 512 bytes, Contains the bootstrap code
- Data blocks - Where directories and files are stored
- Superblock - Indicates disk geometry, available space, and location of the first inode
- Types of linux distributors - Desktop distributions
  Server or enterprise distributions
  §Live-CD distributions
- Linux boot storage - Loading the kernel
  Soft link to the current kernel image is available in the /boot
  directory and is referenced by the Linux Loader (LILO)
  Initialisation: file that controls initialisation is /etc/inittab
- Why linux - Greater control, flexibility, power
- Advantages of linux in forensics - Software availability, Efficiency, Support
- Disadvantages of linux in forensics - Investigator may need to be specially trained,
- Ext4fs and Ext3fs are improvements over Ext
- Precautions during investigation - Avoid running programs on a compromised system
- Recognizing partitions in linux - Standard IDE disk connected to the primary IDE controller as the master will be referred to as hda, If the disk is connected to the primary IDE controller as a slave device it will be referred to as hdb
- Forensic investigators use their own forensic toolkit to find important data from a compromised system
- Toolkit - nc, dd, datecat, pcat,Hunter.o, insmod
- Steps to collect data - media mounting, collect current date, cache tables,