Why a bitstream copy

- When a device (computer or phone) is identified as possibly containing evidence for investigation, it is imperative to ensure a proper (i.e. court admissible) copy of any evidence that exists on device, including deleted data.

Why a bitstream copy (Con't)

- Copy metadata and datablocks in their entirety – regardless of whether they' re allocated to an active file or not
  - Copy slack space @ end of files
  - Copy blocks of previously deleted files
    - evidence can be hidden in slack space
    - Log files are usually the first thing deleted (or replaced) by attackers

What is a bitstream copy

- Bitstream copy means to image the subject media by making a bit-for-bit copy of all sectors on the media
- It is performed on the hard drive level, therefore ignores the EOF marker.
- It is often called a hard drive imaging, bit stream imaging or forensic imaging.

Examples of copies that are not bitstream copy

- *cp*, *tar*, *cpio*, d*ump, restore*
- These tools will copy all the content until the End-of-File marker
- They do not copy any deleted data
- They have their place – it' s NOT in forensics!

Examples of bitstream copy

- Bit-image copy gets every single bit of every byte on a device partition
- Examples
  - Unix utility: *dd*
  - *FTK imager*
  - *EnCase Forensic imager*