

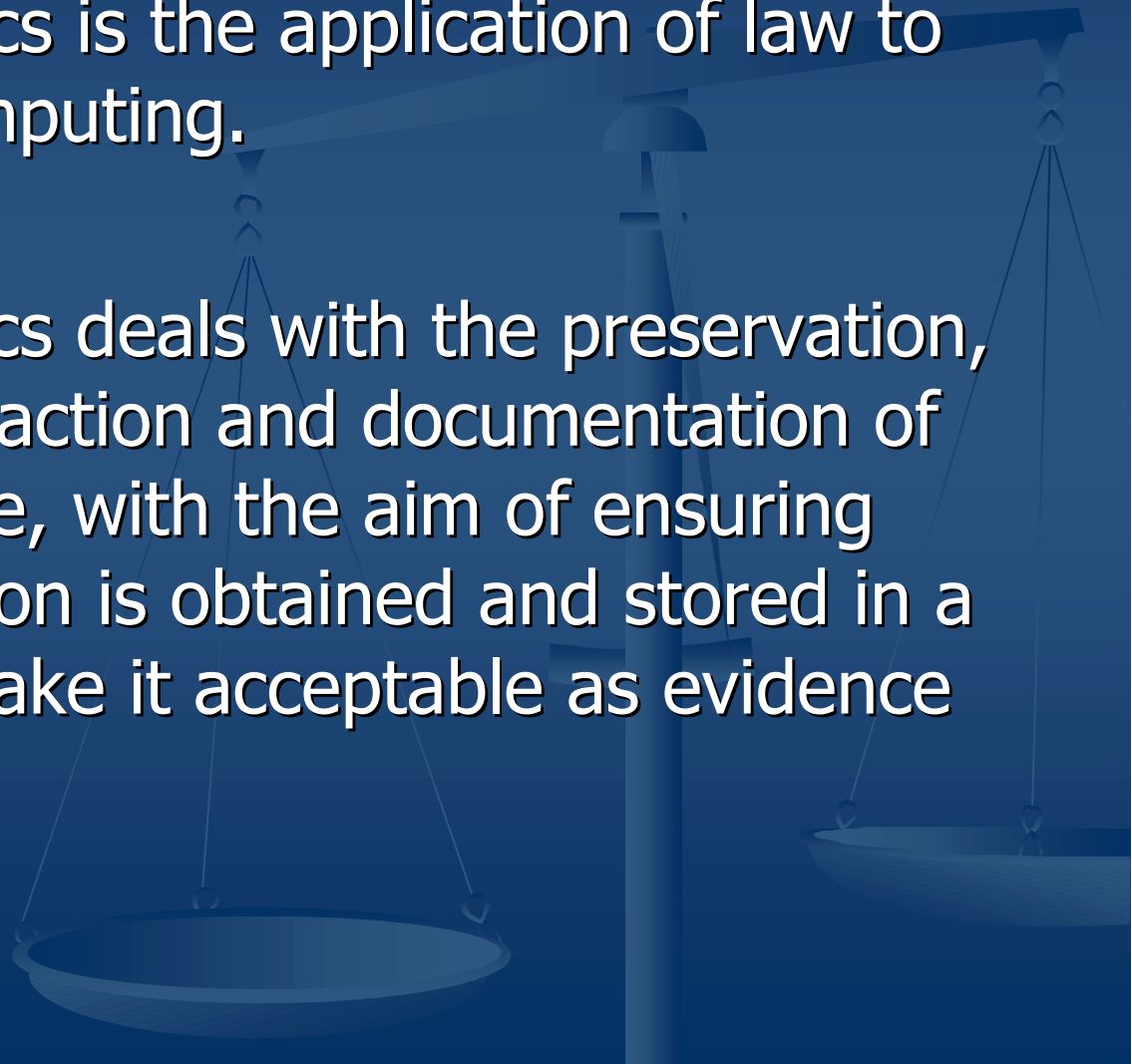
# TO CATCH A THIEF



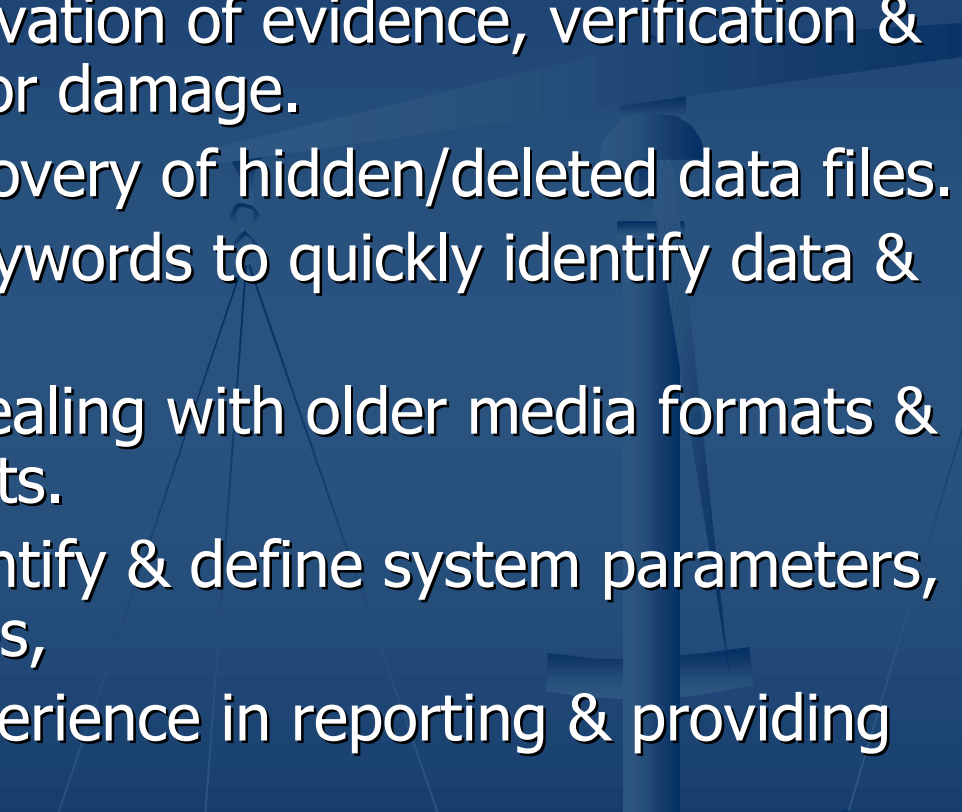
An Introduction to Computer  
Forensics

# What is Forensic Computing?

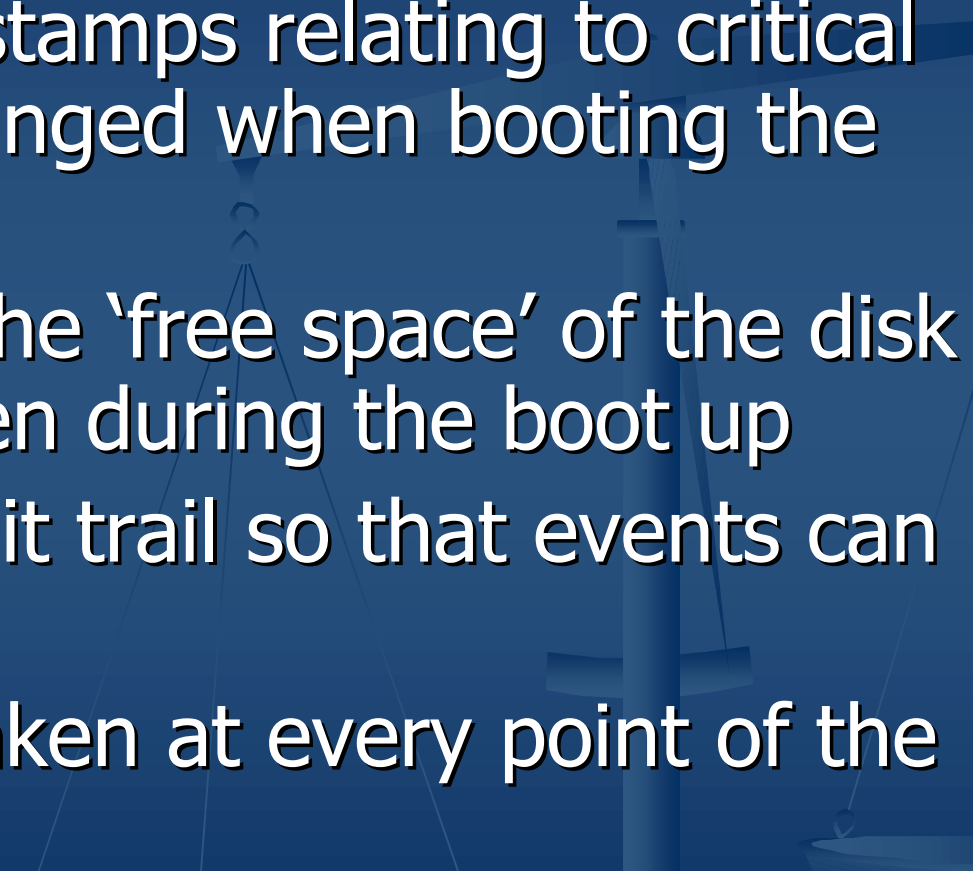
- Computer Forensics is the application of law to the science of computing.
- Computer Forensics deals with the preservation, identification, extraction and documentation of computer evidence, with the aim of ensuring that any information is obtained and stored in a format that will make it acceptable as evidence in a Court of Law.



# Core Skills & Expertise

- Data Seizure - Preservation of evidence, verification & protection from loss or damage.
  - Data Recovery – Recovery of hidden/deleted data files.
  - Searching – Using keywords to quickly identify data & file types.
  - Data Conversion – Dealing with older media formats & proprietary file formats.
  - Expert Reports – Identify & define system parameters, files found, MAC times,
  - Expert Witness – Experience in reporting & providing oral evidence.
- 

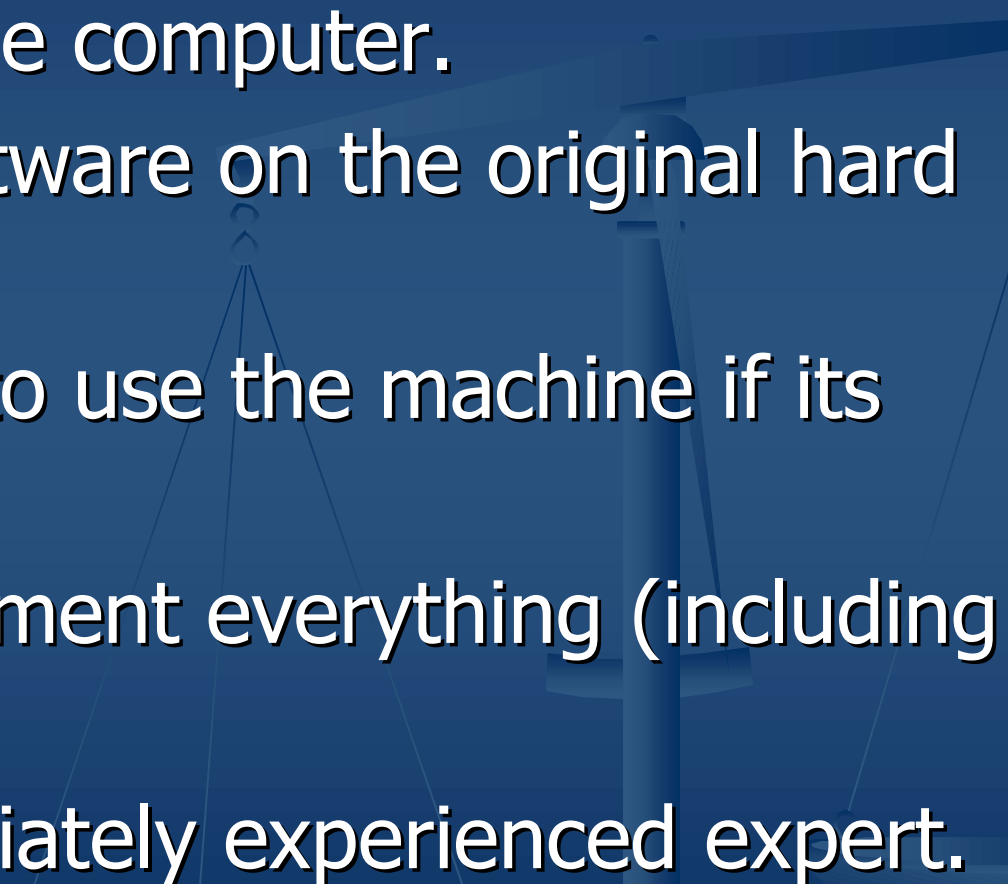
# Techniques & Protocols

- Time and date stamps relating to critical files are not changed when booting the machine.
  - Information in the 'free space' of the disk is not overwritten during the boot up
  - Maintain an audit trail so that events can be recreated.
  - Verify actions taken at every point of the investigation
- 

# Techniques & Protocols (2)

- Enable quick identification of information and evidence from the computer
- The image taken contains all the information that existed on the original machine without exception - data which may have been deleted, information hidden outside of the usual storage areas or partially overwritten areas of older data.

# Don't Learn The Hard Way!

- Don't turn on the computer.
  - Don't install software on the original hard disk drive.
  - Don't continue to use the machine if its turned on.
  - Detail and document everything (including photographs).
  - Find an appropriately experienced expert.
- 

# Who are Forensic Data?

- Forensic Data Services (FDS) specialise in the recovery of data from damaged media or in situations where information has been accidentally deleted, the conversion of data from older or more obscure media formats, and the Forensic Analysis of all major forms of electronic data storage media.
- Our team has given evidence of an expert nature in most Australian jurisdictions, including the Supreme Courts of New South Wales, Victoria, Queensland and Western Australia, and the District and Local Courts of New South Wales and Victoria. Forensic Data has also been involved with investigations in Papua New Guinea and parts of Asia.

# FDS Contact Details

- **SYDNEY** - Level 3, 145 William St  
Darlinghurst NSW 2010
- **MELBOURNE** - Unit 2, 20 Commercial Rd  
Melbourne VIC 3004
- **BRISBANE** - 1 Clunies Ross Circuit  
Brisbane Technology Park QLD 4113
- Australia Wide: 1800 824 444