UNSW SYDNEY | Australia's Global University

sec edu

security
engineering
capability

COMP6445 – Digital Forensics

Term 3 2019 - Week 1 part 2

17 September 2019

Topics for this lecture

1. Forensic copying

2. Windows forensics #1
    1. Windows file system
    2. Software data recovery

Forensic copying

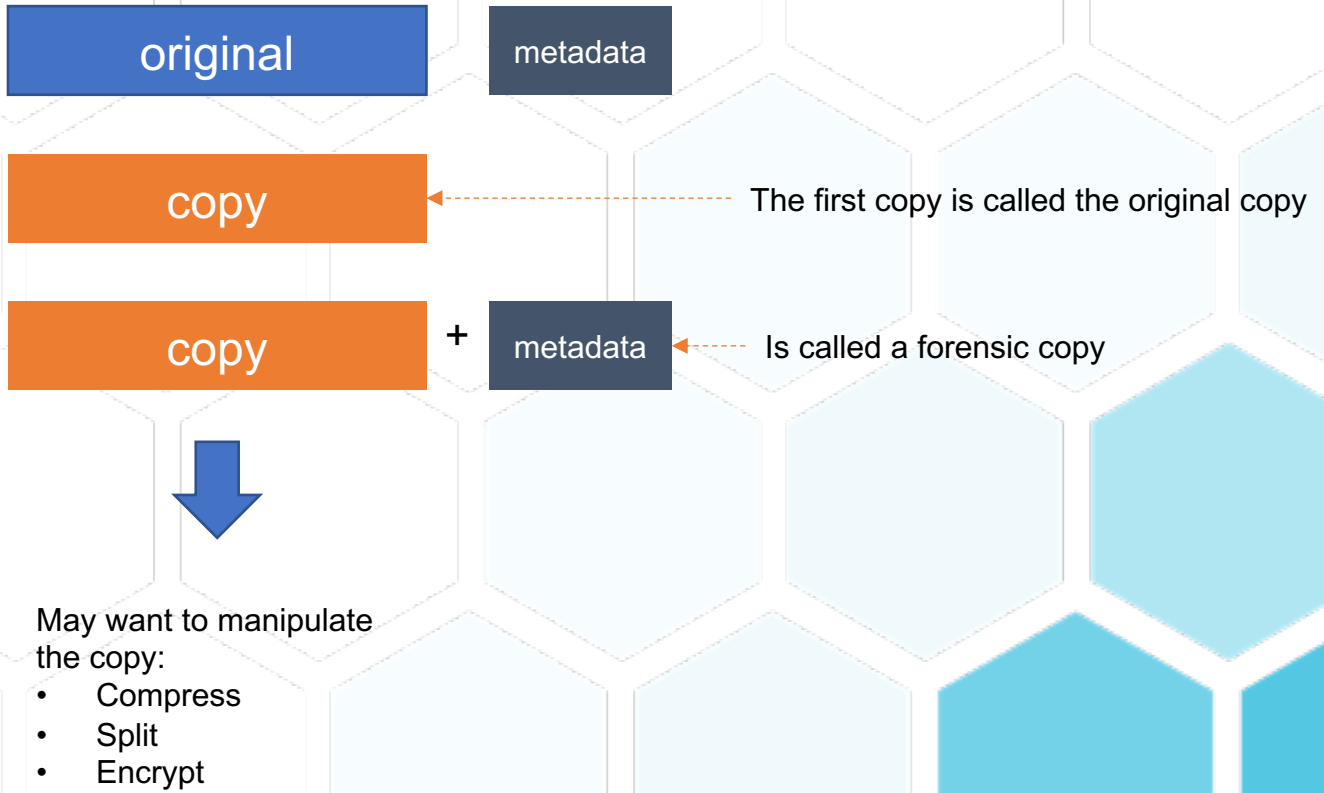
Why is forensic copying so important?

- Also referred to as:
  - Acquisition
  - Imaging
  - Duplication

A three part process

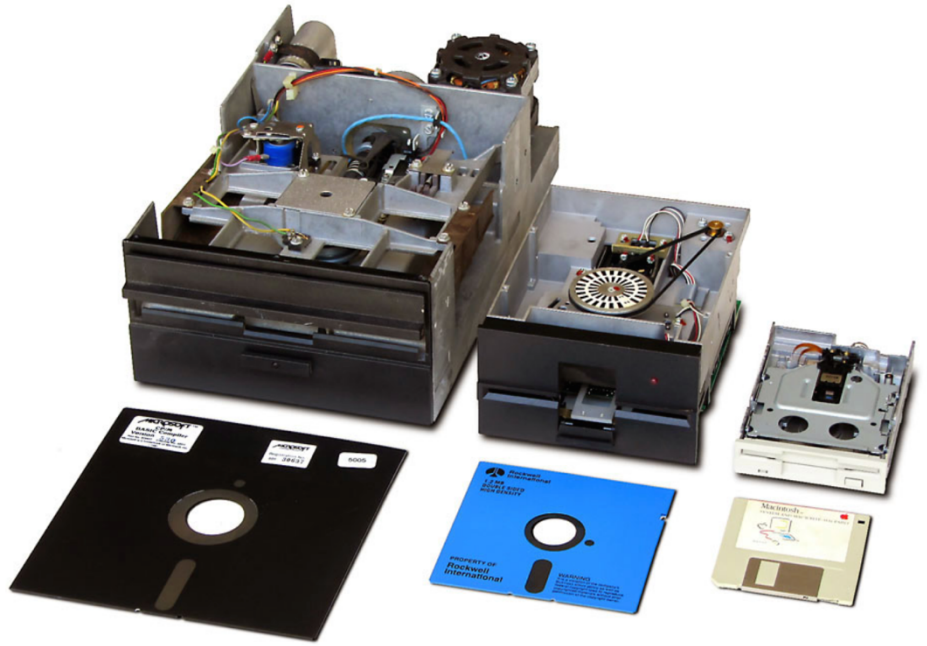
1. Make a copy
   - Duplicate data
   - Reliable + Sufficient
2. Make verification metadata
   - Create metadata (i.e. data about the data) that can be used later to verify that the data has not changed
3. Demonstrate the copy is a reliable copy

There are many different ways to create a forensic copy – so long as the there is a duplicate and verification metadata



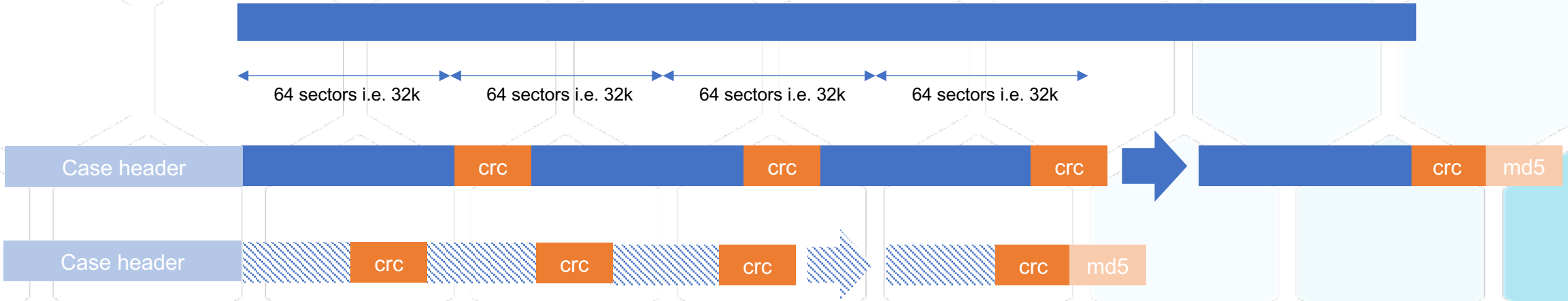
But a hard disk or USB key is most common but also…

- James Hardie
  - ~10,000 backup tapes
  - ~900 hard disk drives
  - ~10 computers
- Floppy disks
  - 3 ½ inch – still common
  - 5 ¼ inch – still common
  - 8 inch – last time in 2017
- ZIP drives
- A land dispute
  - Copy punched cards and restore data to PDP3 (i.e. valve computer)



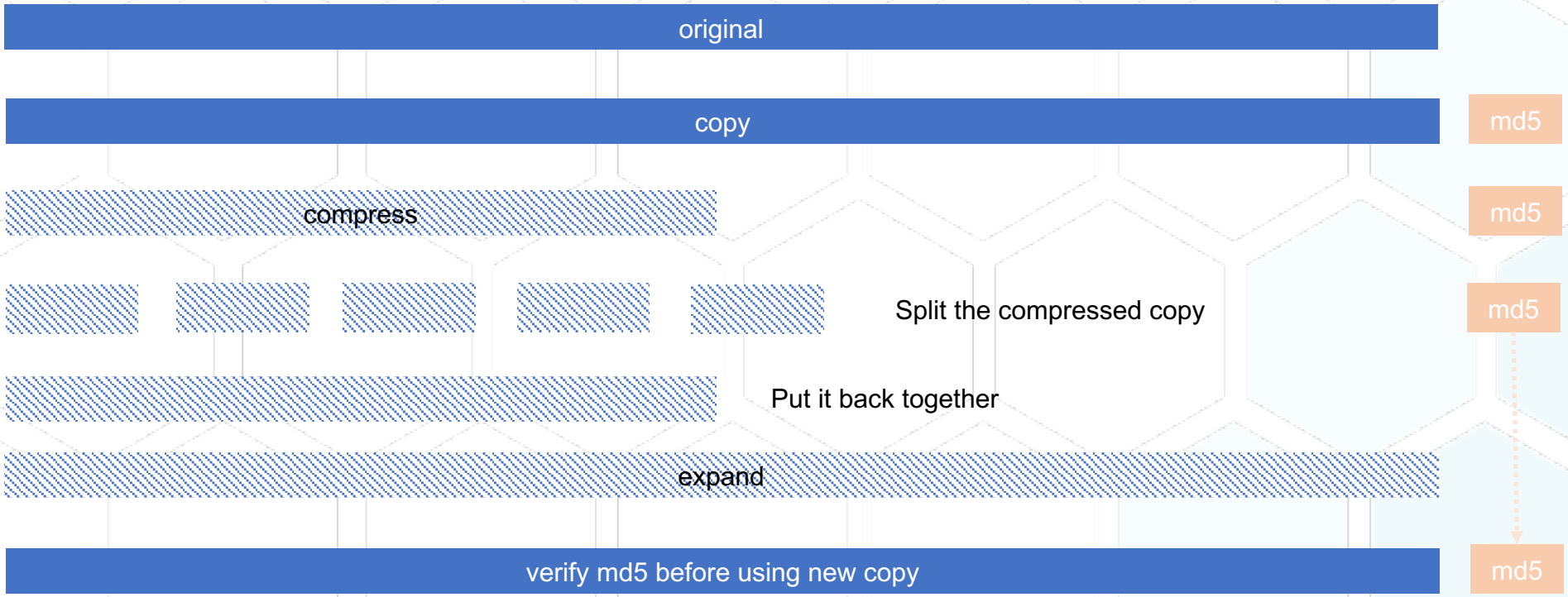
Expert witness or E01 format

- Is commonly used and supported by many open source and commercial tools



Alternate using dd

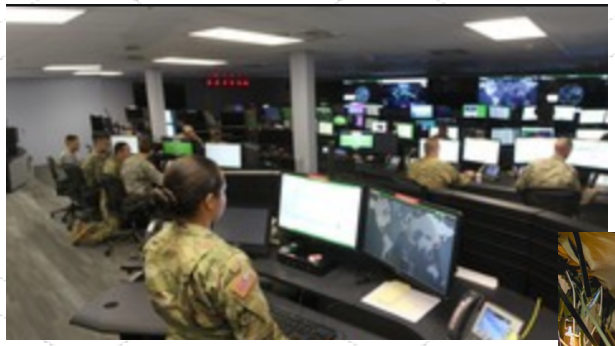
- Readily available across many devices

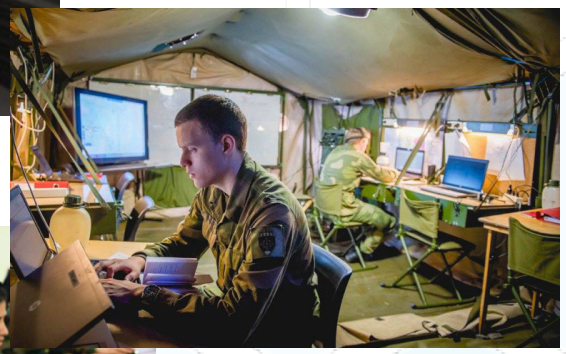


dcfldd

- Defense Computer Forensic Labs dd

- An extended version of dd. Adds features useful for forensics:
  - Hashing on the fly
  - Progress indicator





Write blocking

- Used to ensure that original cannot be written onto i.e. cannot be changed

- Hardware or software
  - Hardware tested by NIST[1]

1. https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/cftt-technical/hardware

What happens when verification fails?

- It sometimes happens that the copy is changed

- How can a copy change?
  - Spoilage = accidental
  - Tampering = purposeful

⇩

  - Was the examiner reckless or negligent?
  - Was it wear and tear?

- A single bad sector will cause the hash to be different
  - Given that the probability of spoilage of a particular sector (due to hardware failure) is constant, then the larger the data set, the greater the probability of a bad sector
  - Can be as high as 20% for older media e.g. backup tapes

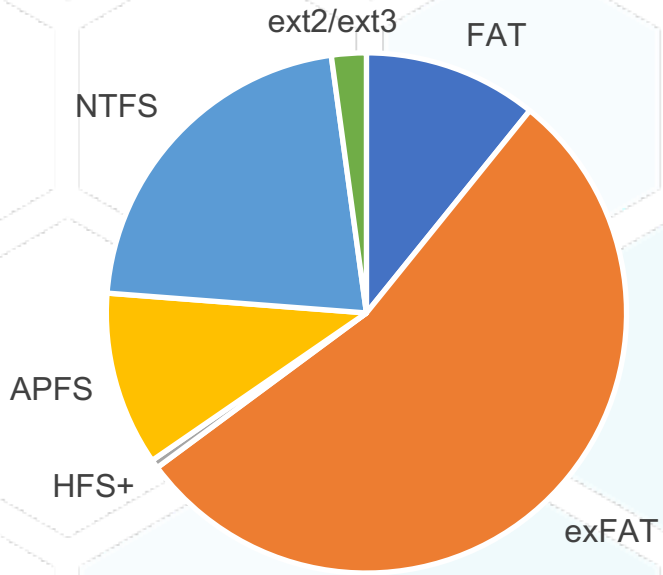
Windows forensics #1

Common file systems

- **FAT** – FAT12, FAT16, FAT32
- **NTFS** – Microsoft
- **exFAT** – for flash drives
- **ext2, ext3, ext3** – genesis in Unix now linux. Still popular on devices
- **HPFS** – High performance file system IBM
- **HFS** and **HFS+** - Apple's early file systems
- **APFS** – Apple file system
- **ISO 9660** and **Joliet** – CD/DVD

+ Emerging file systems for cloud

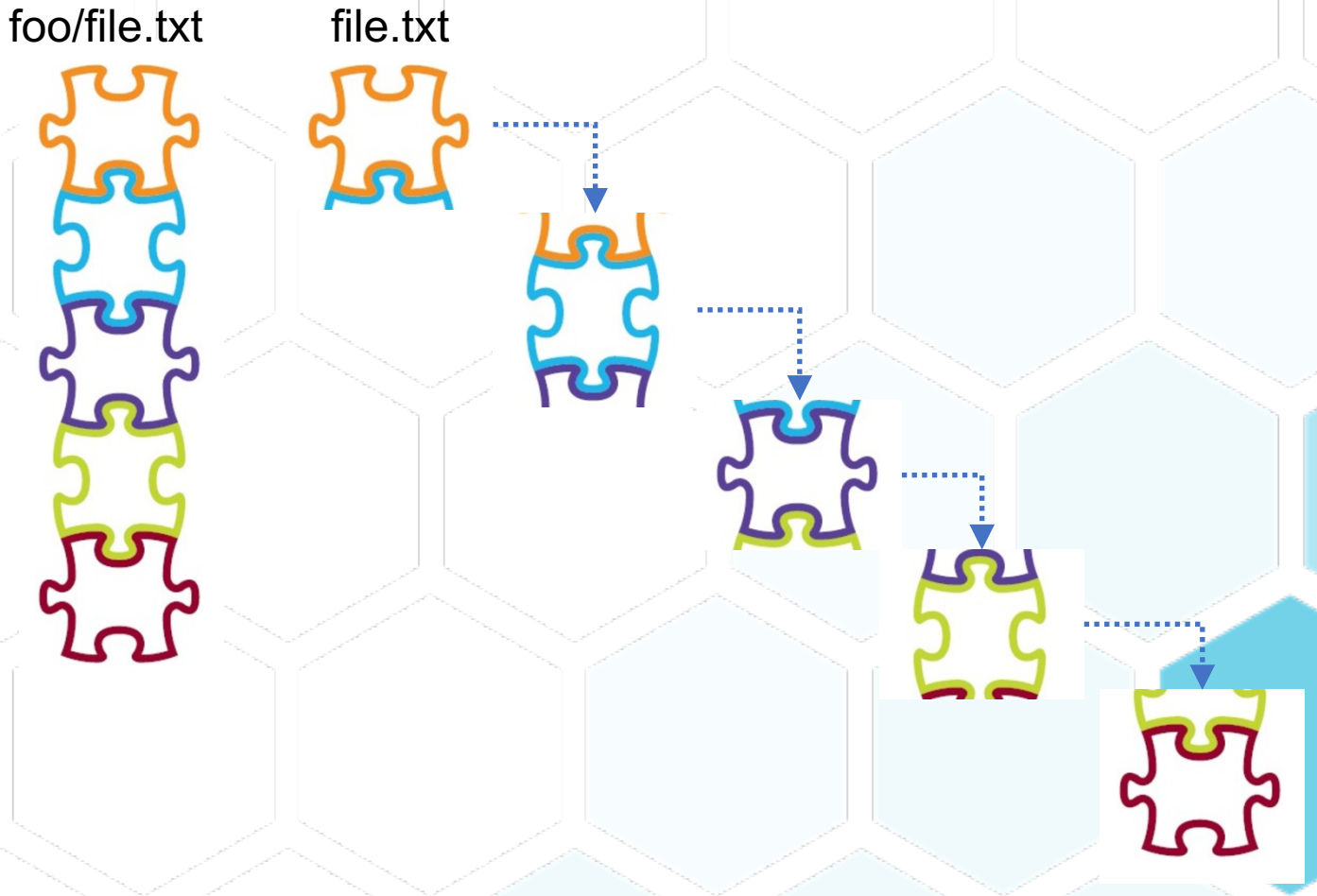
In my professional practice, by filesystem across 2018

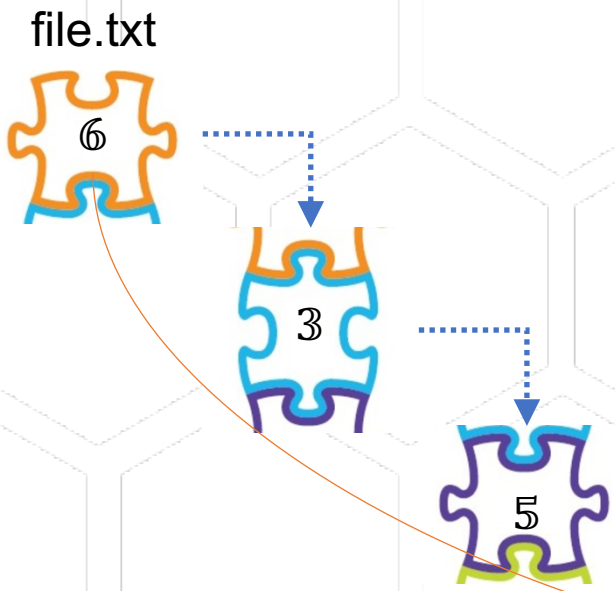


Excludes CCTV, drones and phones and rounded to nearest 10

How does a file system work?

- How would you explain a file system to a lawyer, judge and jury?





FILE ALLOCATION TABLE

Block	Used	Next
0	0	
1	1	-1
2	1	6
3	1	5
4	1	-1
5	1	-1
6	1	3
7	0	

marker for EOF

DIRECTORY TABLE
/

Name	Starting block	Metadata
foo	1	xxxxx

DIRECTORY TABLE
/foo

Name	Starting block	Metadata
file.txt	3	xxxxx

FILE ALLOCATION TABLE

Block	Used	Next
0	0	
1	1	-1
2	1	6
3	1	5
4	1	-1
5	1	-1
6	1	3
7	0	

Now image if the pieces were scattered across a disk. How do you sift thru putting blocks back together into files… and imaging doing this for many directory tables and a FAT with many thousands of blocks…

DIRECTORY TABLE
/

Name	Starting block	Metadata
foo	1	xxxxx

DIRECTORY TABLE
/

Name	Starting block	Metadata
foo	1	xxxxx

DIRECTORY TABLE
/

Name	Starting block	Metadata
foo	1	xxxxx

DIRECTORY TABLE
/

Name	Starting block	Metadata
foo	1	xxxxx

DIRECTORY TABLE
/

Name	Starting block	Metadata
foo	1	xxxxx

DIRECTORY TABLE
/

Name	Starting block	Metadata
foo	1	xxxxx

Block	Used	Next

Data recovery

- This is the essence of data recovery and forensic practitioners call it *data carving*

- Common data carving tools which you will use in the tutorial/lab
  - scalpel/foremost
  - recoverjpg
  - Photorec

- NIST provides standardised methods and test cases for data carving[1]

- Think about how you would explain this to a lawyer, judge or jury

- Some things barristers have said about me, or rather, about my testimony:
  - "One of the dark arts of computer forensics"
  - "Their computer geek causes pictures to materialise out of meaningless zeroes and ones. How do we know they are meaningful…and even if they were, how do we know the accused knew they were there?"
  - "Like the alchemists of past Mr Ghosh used a concoction of software to conjure up nuggets of evidence….how do we know that nugget is what Mr Ghosh claims it to be?" [edited for brevity]

1. https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/cftt-technical/deleted

Forensic software

- The good news is that you don't have to do this manually
  - Like any engineering – automate the easy stuff and let human experts focus on what needs thinking and judgment

- Popular open source distros
  - Kali Linux
  - CAINE
  - SIFT

- Commercial tools
  - enCase
  - FTK
  - Magnet
  - XRY
  - Forensic Explorer
  - OS Forensic

Australian

Short break – 5 mins

And then Week 1 part 3:

- Explain tutorial/lab
- Explain Week 1 activity (assessed)