

#### **OUR PRIME OBJECTIVE:**

To successfully recover lost, damaged, hidden or deleted files from a computer system after an accidental, deliberate or malicious action.

25<sup>th</sup> September 2000

Presentation by Computer Forensics NZ Ltd for Auckland University 415.725SC

# THIS PRESENTATION

- \* What is computer forensics?
- \* Disk operating system considerations.
- \* How data is recovered.
- What to do when data can't be recovered, and how to prevent recovery.
- \* Commercial and paralegal aspects.
- \* The process.
- & Q & A.

25<sup>th</sup> September 2000

#### WHAT IS COMPUTER FORENSICS

Computer Forensics is the acquisition, preservation, preparation, analysis and presentation of computer-related evidence utilising secure, controlled methodologies and auditable procedures.

25<sup>th</sup> September 2000

Presentation by Computer Forensics NZ Ltd for Auckland University 415.725SC

#### THE FATHER OF FORENSICS

"For any two points of contact there is always a cross-transference of material from one to the other."

Edmond Locard 1877-1966

Every contact leaves a trace.

Presentation by Computer Forensics NZ Ltd for Auckland University 415.725SC

25<sup>th</sup> September 2000



## **MODERN PERSPECTIVE**

For ever interaction with a PC there will always be material left behind on that PC OR

> Presentation by Computer Forensics NZ Ltd for Auckland University 415.725SC

# **MODERN PERSPECTIVE #2**

# EVERY INTERACTION WITH A PC LEAVES TRACE DATA BEHIND

25<sup>th</sup> September 2000



# **GENERIC DISK OS**

Master Boot Record.
Partition table.
File Allocation Table.
Data storage area.

Presentation by Computer Forensics NZ Ltd for Auckland University 415.725SC

25<sup>th</sup> September 2000

## WHEN DELETE IS NOT DELETE

\* Reference only is deleted

 Space is flagged as available for re use.
 FDISK and FORMAT Urban myths

25<sup>th</sup> September 2000

# WHAT INFO CAN BE RECOVERED

Full files.ASCII text.Graphics.

25<sup>th</sup> September 2000

Presentation by Computer Forensics NZ Ltd for Auckland University 415.725SC

## WHEN IS THERE PROBABLY NO CHANCE

When the hard disc platter has been:

\* Badly distorted by fire.

\* Significant physical damage.

Subjected to abnormally high magnetic fields.

#### PROTECT AGAINST DATA RECOVERY??

Overwrite all sectors.
Once, many times.
Protect from whom.
Ultimate protection.

25<sup>th</sup> September 2000

Presentation by Computer Forensics NZ Ltd for Auckland University 415.725SC

#### DON'T GIVE THE COMPANY'S SECRETS AWAY

Case 1 – Avco.
Case 2 – Government departments.
Happens every day every where.

#### COMMERCIAL DATA RECOVERY

#### Main Causes:

- \* Accidental delete.
- \* Advised to reformat by IT advisor.
- \* Partition table corrupt.
- \* Disk hardware failure.
- \* Malicious damage.
- \* Viral contamination.

Presentation by Computer Forensics NZ Ltd for Auckland University 415.725SC

25<sup>th</sup> September 2000

#### PARALEGAL DATA RECOVERY

Unintended left evidence.
High usage of PCs at home.
Private use of company PC.
Files on archival backups.
Electronic media discovery.

25<sup>th</sup> September 2000

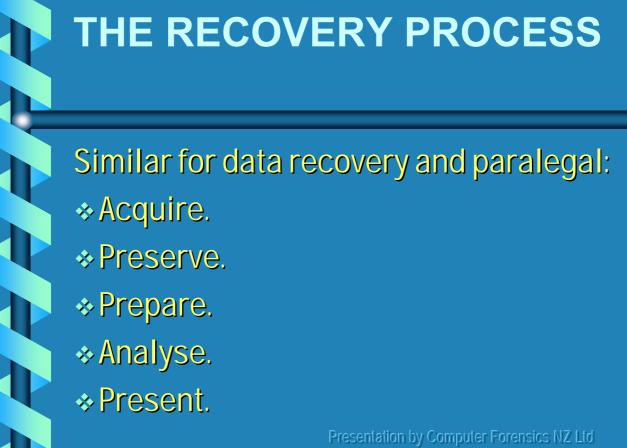
#### PARALEGAL DATA RECOVERY #2

#### Cases:

Professional practice 2 years ago.
Ex-employee using company data.
Senior manager and PA setting up competitive company.

Presentation by Computer Forensics NZ Ltd for Auckland University 415.725SC

25<sup>th</sup> September 2000



25th September 2000

#### RECAP

Three key points to leave with you.

- Data is rarely completely deleted from a hard disk.
- Implications for commercial security.
- Implications for prosecution and defence in court.

25<sup>th</sup> September 2000

Presentation by Computer Forensics NZ Ltd for Auckland University 415.725SC

# SUGGESTED SURFING

Paralegal

- \* www.forensic-computing. com/subjects.html
- http://www.dcfl.gov/
- **General Data Recovery**
- http://www.cs.auckland.ac.nz/~pgut001/
- http://www.cerberussystems.com/INFOSEC/ privacy.htm

25<sup>th</sup> September 2000

