



Computer  
Forensics

# Who I am and what I do!

**Ian Pomfret - Computer Fraud Investigation Manager**

Employed by BT for the last 15 years.

10 years on IBM mainframe Operations, Storage Management and RACF Security admin.

5 years working in Security, Crime Intelligence and Computer Forensics.

69

# Our Organisation

## BT UK Security - Investigation

**Revenue  
team**

**Asset Protection  
team**

**e-Crime & Computer Forensics  
team**

**CERT**

**Computer forensics**

**e-crime investigators**



# Types of cases investigated

## **Internal cases**

Misuse of company services

Breaches of security policy

Disclosure

Fraud

Internal audits

Building 'health checks'

## **External cases**

Hacking

Denial of service attacks

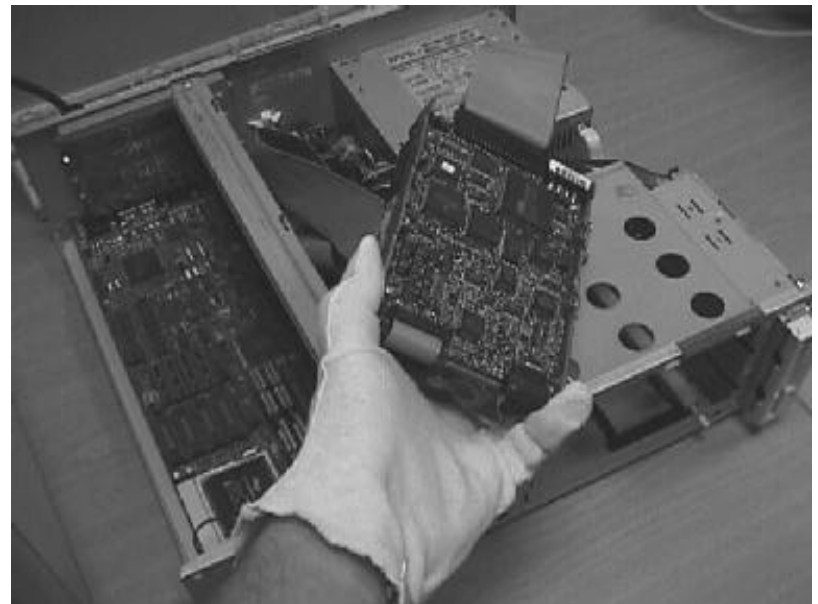
Theft of service

External Fraud



# What is Computer Forensics ?

“Identification and retrieval of evidence from computer based systems”



# The need for a forensic computing capability

- Increased reliance on computers in the work place and at home.
- Valuable source of evidence.
- Need to ensure integrity and continuity of computer based evidence to be used in a court of law.
- Expanding area - 5 years ago average 10 machines / year currently 60-80 / year.

# Securing the evidence - DO

- Note or photograph equipment setup and connections
- Allow printing to finish
- Record what is on the screen
- Record telephone number if modem connected
- Seize other media - backups etc
- Store in cool dry atmosphere
- Bag and seal

# Securing the evidence - DON'T

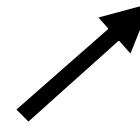
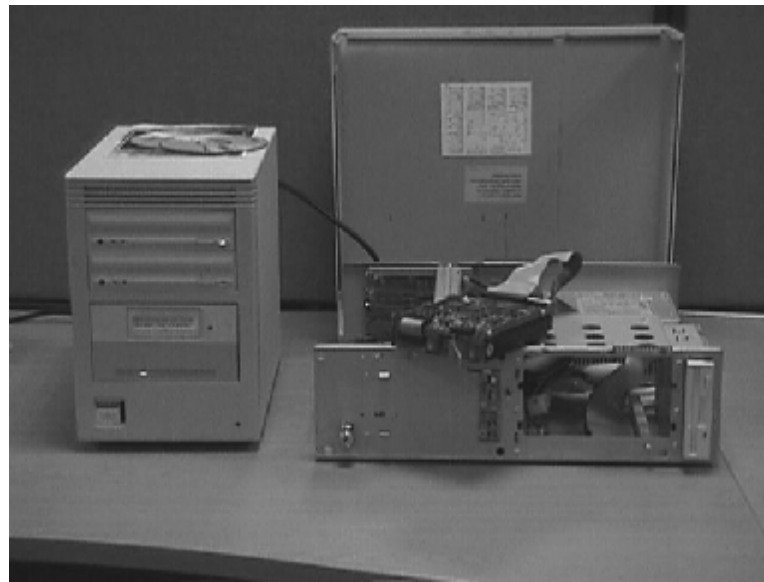
- Place media near mobile phones and electrical sources
- Start investigating
- Start closing programs and shutting down the machine
- Allow suspect to alter state of the machine
- Move computer whilst powered on

# The Armchair Detective !

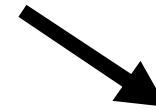


“I’ve been  
carrying out an  
investigation !!!”

# Imaging process



Master (sealed)



Working

# Disk Imaging utilities

Imaging software : DIBS

SafeBack

Vogon

Encase

UNIX dd

bit copy of whole drive including: Freespace

Slackspace

System Space

69

.

# Handheld disk imager



*Image Master Solo*

Images IDE, EIDE, SCSI  
Transfer rate 1GB/Min  
Audit trail

# Possible problems encountered

- Boot passwords
- Encrypted drives

# Imaging - DO

- Note CMOS setting: Boot sequence  
Date & time  
Disk geometry
- For continuity note seal numbers and when broken
- Note equipment and hdd serial numbers

# Examination process



- Word searches across the image
- Search for filetypes e.g image files
- Recover deleted files
- Recover deleted partitions
- View slackspace

# Type of digital evidence

Data files

Recovered deleted files

Recovered data from slack space

Digital photographs and videos

Server log files

Email

Chat/IM/IRC logs

Internet history

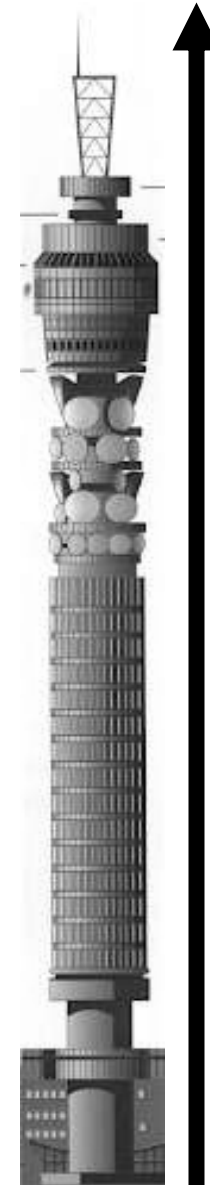
Web pages

Registration records

Subscriber records

# Volume of data

The BT Tower is 580 ft tall.  
If you printed out a 6GB hard disk drive the a  
stack of paper would be taller than the tower !



580 ft

DEMO

69

# The Evidence

- From which computer did it come, and how do we know that the data you are presenting is the data that you seized or copied.
- Keep it simple
- Proof not truth

# Witness Evidence

## **Analogies are critical:**

A computer is a file cabinet and an audio record.

Use the file cabinet analogy for explaining that everybody keeps documentary records on their computer.

Use the audio record to explain technical issues like slack space.

# Attacks on Evidence

Attack on the software / hardware used to collect the data

Qualifications of analyst / expert

Attack on the :chain of evidence

authentication

alteration

Questions ?

69