



Digital Footprints: Emerging Issues in Computer Forensics

Peter Sommer



A few figures ...

- **2006: 13.9m UK households have Internet access (57%); 69% of Internet connections use broadband access**
- **Internet sales to households = £21.4bn**
- **14.6% UK businesses sold over the Internet; 56.3% made purchases; Business purchases over the Internet + £72.8bn**
- **70% UK businesses had a website**
- **50.5% UK businesses interact with central and local government over the Internet**



Cost of Personal Computers...



Packard Bell 2380 Desktop PC + 15" TFT Monitor

This great value desktop PC comes complete with a powerful AMD Athlon 64 3800+ processor, a huge 1GB of RAM and a 160GB hard drive that can hold up to 40,000 songs! Plus burn all of your files, music and films to disc with the built-in DVD ReWriter.

Save a total of over £100 only when you reserve online or order for delivery only for a limited time!

Web Exclusive Price inc VAT
£399.98



Compaq Intel Pentium Dual Core Laptop PC
Fantastic Value

This unbeatable value Compaq laptop has a powerful Dual Core processor, a massive 1GB memory and 80GB hard drive. This laptop also comes pre-installed with Windows Vista Home Premium, perfect for all your home and office computing needs. Don't miss out on this fantastic deal.

- 1GB Memory
- 80GB Hard Drive

(C542EA)

Price inc VAT
£479.99

- £400 = 5 days' earnings @ £30,000 pa
- Many households now have several PCs, including obsolete ones

→ The lowest speed of DSL service available in west European and North American markets costs households 1% or less of median monthly income (EIU, 2007)

LSE

Cost of Media Storage



Freecom 4GB DATABAR USB 2

In stock now
quicklink: 4BCV18
mfr#: 28154

**Reduced!!!
Reduced!!!
£21.15 inc vat**

1 ADD



Maxtor Personal Storage 400GB 7200RPM USB2 16MB

In stock now
quicklink: 4HVK18
mfr#: STM304004EHC201

**Fantastic Price!!!
£79.99 inc vat**



Hitachi Deskstar T7250 320GB U133 7200RPM 3.5inch 8MB

In stock now
quicklink: 4D1G18
mfr#: 0A33405

£58.46 inc vat



Buffalo 1TB Terastation Pro

In stock now
quicklink: 419Q18
mfr#: TS-1.0TGL/R5-1

**Fantastic Value, Whilst Stocks Last!!!
£439.99 inc vat**

1 ADD

image for illustration only

**18p / 1000 MB!
1 MB=100,000 items of
correspondence; 20,000
medium-res pictures; 250
songs**

LSE

Non-conventional computers and/or storage media



LSE

Overview

- Types of Crime
- Sources and Types of Digital Evidence
- Some Challenging cases
- Emerging Problems
- How to Instruct a Computer Expert

LSE

Types of Crimes

- New Hi-Tech Crimes
- Old Crimes / New Methods
- Almost Any Crime / Digital Evidence is important



Crimes

- “Computer Fraud”
- “Hacking”



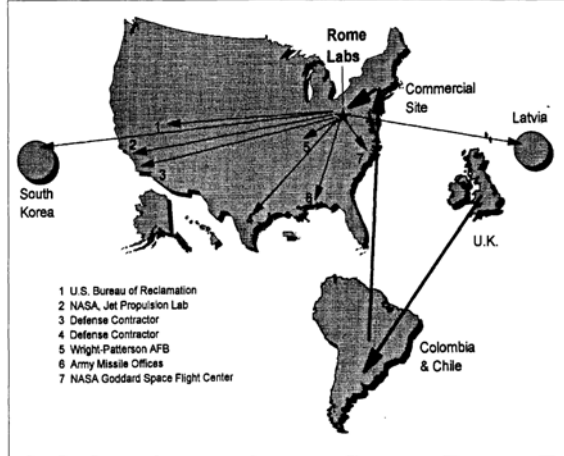
1994 multiple-site global hack
– DataStream
Cowboy/Kuji –
“information warfare”

Computer program which deducts 1p from many accounts and deposits them to fraudster’s benefit

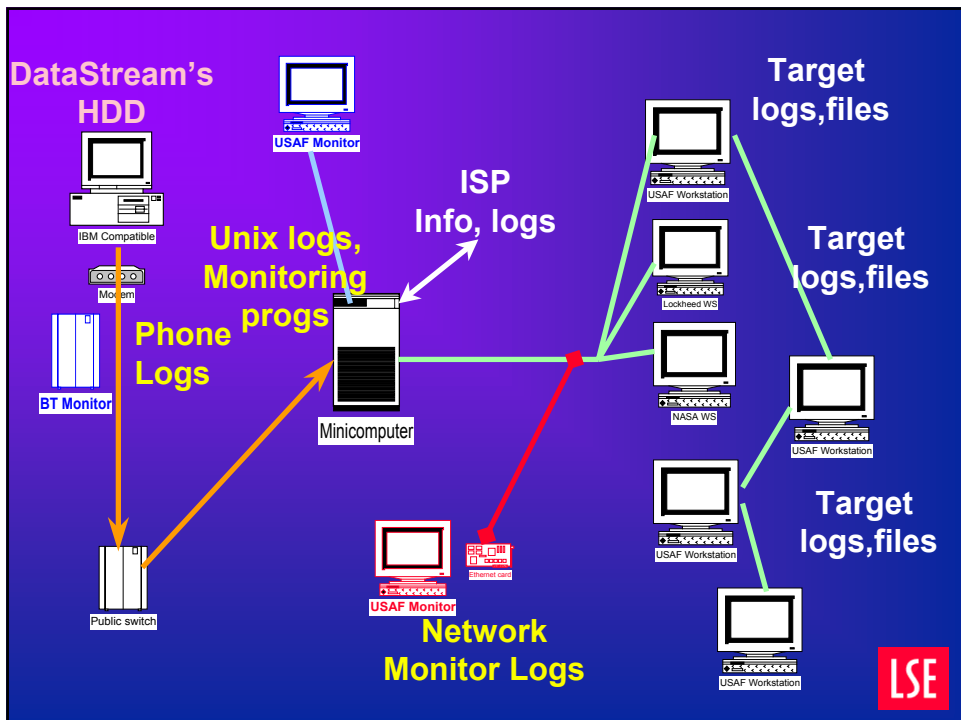


GAO Report

Figure 2.3: Computer Sites Attacked During Rome Laboratory Incident



LSE



LSE

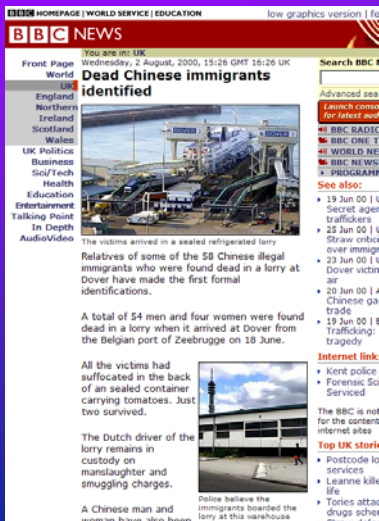
Crimes



Multiple murder to acquire haulage business as cover for narcotics trafficking – Regan convicted via cellsite evidence but computer held drafts of a document agreeing sale of business



Crimes



"People smuggling" / snakesheads
58 dead Chinese immigrants at Dover in 2002; on computer of 2nd defendant: apparent draft asylum applications + email usage by third party



Crimes

Last Updated: Monday, 30 April 2007, 13:34 GMT 14:34 UK
 E-mail this to a friend Printable version

Five get life over UK bomb plot

Five men have been jailed for life for a UK bomb plot linked to al-Qaeda that could have killed hundreds of people.

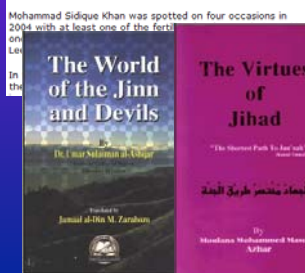
Jurors in the year-long Old Bailey trial heard of plans to target a shopping centre, nightclub and the gas network with a giant fertiliser bomb.

The judge, Sir Michael Auld, said the men, all British citizens, had "betrayed their country".

It has also been revealed some of the plotters met two of the 7 July London suicide bombers.

• Omar Khyam, 35
 • Jawad Akbar, 23
 • Salahuddin Amin, 32
 • Waheed Mahmood, 35
 • Anthony Garcia, 24

Full special report



Operation Crevise:
 Evidence of research, CD viewing, Terrorist Manuals, Inspirational videos and texts, email, Internet cafes

LSE

International version | About the versions

BBC News 24

Last Updated: Tuesday, 25 July 2006, 14:25 GMT 15:25 UK
 E-mail this to a friend Printable version

Trio cleared of red mercury plot

Three men have been cleared of trying to procure a substance which police claimed could have made a "dirty bomb".

They were arrested in September 2004 after trying to buy "red mercury" from an undercover reporter.

But Roque Fernandes, 44, Abdurahman Kanyare, 53, both of Edgware, and Dominic Martins, 45, of Stanmore, had denied three terror-related charges.

They denied being interested in a radioactive or toxic substance and claimed they had been tricked.

A joint statement by the defence solicitors said: "This is a great tribute to the jury system and English justice and a dark day for the News of the World."

The court heard how Mazher Mahmood, better known as the News of the World's "fake sheikh", played the part of a Muslim, called Mohammed, who claimed to have nearly a kilogram of red mercury which he was looking to sell.

Mr Mahmood set up a meeting and then contacted officers from the Metropolitan Police's anti-terrorist squad, who arrested the men at the Holiday Inn in Brent Cross on 24 September 2004.

Defence lawyers



Roque Fernandes (left) and Dominic Martins have walked free from court



"This is a great tribute to the jury system and English justice and a dark day for the News of the World"

Crimes

"Fake Sheikh" / News of the World / "Red Mercury" plot
 (one def's relation was legit chemistry academic)

LSE

BBC NEWS

You are in: UK
Tuesday, 13 February, 2001, 16:12 GMT

Front Page
World
UK
England
Northern Ireland
Scotland
Wales
UK Politics
Business
Sci/Tech
Health
Education
Entertainment
Talking Point
In Depth
AudioVideo

Paedophiles jailed for porn ring



Club members 'paid' an entry fee of 10,000 images

Seven British men who peddled child pornography on the internet have been jailed for between 12 and 30 months each.

The paedophile ring - called The Wonderland Club - was smashed by Operation Cathedral, the largest international operation to be co-ordinated by the National Crime Squad in London.

The BBC's Crime Correspondent, Stephen Cape
There were 750,000 images of abused children discovered.
Hi real 56k

John Carr, Internet Security Adviser
"Catching them had nothing to do with the internet"
Hi real 28k

Ray Wynn, Sexual Crimes Consultant
"These men are going to do it again"
Hi real 28k

Raids were staged around the world on 2 September 1998, leading to a total of 107 arrests being made across the UK, Australia, Austria, Belgium, Finland, France, Germany, Italy, Norway, Portugal, Sweden and the United States.

Judge Kenneth Macrae
"You directly or indirectly exploited the most vulnerable in our society."

But child rights groups in the UK described the sentences as a "joke" that suggested the crimes were not being taken seriously.

Under laws applying at the time the men were charged, they could only have faced a maximum of three years in jail.

Crimes

W0nderland Club: NCS-lead Operation **Cathedral** – global investigation – lead to changes in sentencing and setting-up of NCS/POLIT and CEOP > Op Ore:

Libraries of pictures; email + chats; "Traders' Handbook"

LSE

Crimes

- **Money Laundering**
- **Deception / Fraud**
 - Consumer, Business, Investment, Carousel
- **Narcotics Importation / Distribution**
- **Handling Stolen Goods**
- **Harassment**
- **Sexual assault**
- **Representation of the People Act**
- **Perjury**
- **Attempt to pervert course of justice**
- **Police Disciplinary Proceedings**

LSE

Sources of Computer Evidence



How to Acquire Evidence

- **By pre-planning – system design**
 - Access Control Systems
 - Audit logs
 - Serialing of transactions
 - Authentication of People, Files, Transactions
 - Digital Finger-printing of documents, logs, etc
- **Forensic Computing**
 - Unintended “digital footprints”
 - Evidence identification
 - Evidence Preservation
 - Evidence Analysis, often based on reverse-engineering of OS, apps, etc



Hard Disk Evidence

- **Substantive Documents**
 - Files, graphics, photos, etc
- **Recovery of deleted documents**
- **Emails**
- **Installed Programs**
- **Internet Activity**
 - Sites visited, files downloaded
- **Timeline of activity**
- **Registration issues**
- **Passwords**
- **Earlier installations**

**Facts,
Corroboration.
Inferences,
Interpretations.
Indications of
Intent,
Research,
Planning,
“Bad
Character”**

LSE

Forensic procedures..

- **Freezing the scene**
 - a formal process
 - imaging
- **Maintaining continuity of evidence**
 - controlled copying
 - controlled print-out
- **Contemporaneous notes > witness statements**
- **ACPO Good Practice Guide – 4th edition due**

LSE

Disk Forensics

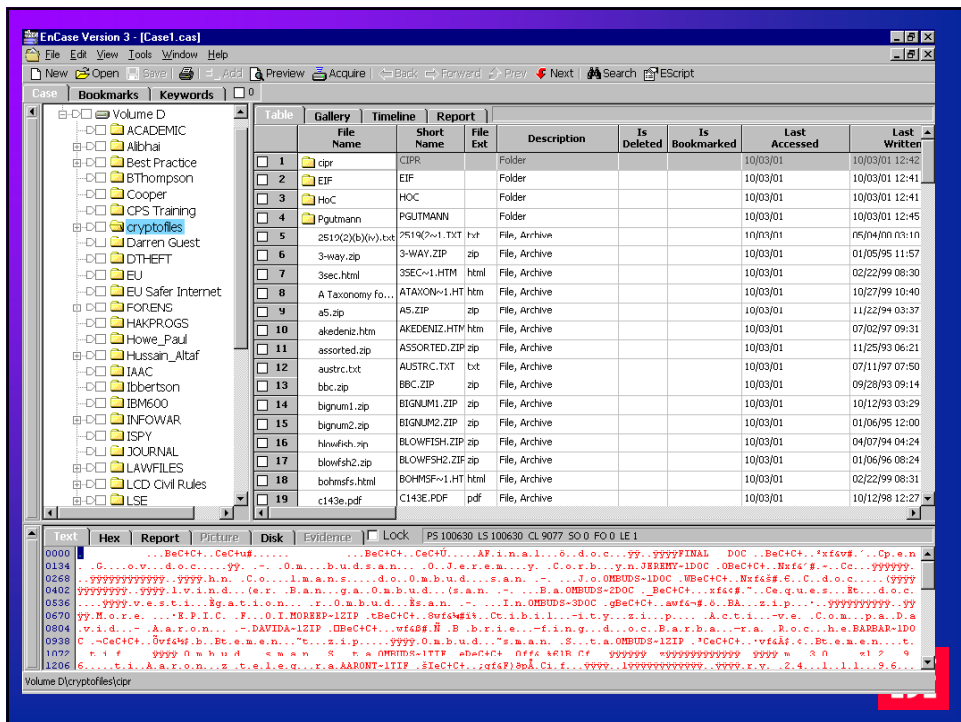
- **Forensic imaging**
 - Captures every element on disk media
 - Write-protect to prevent contamination
 - Imaging products need to be able to cope with many disk operating systems
- **Subsequent Analysis**

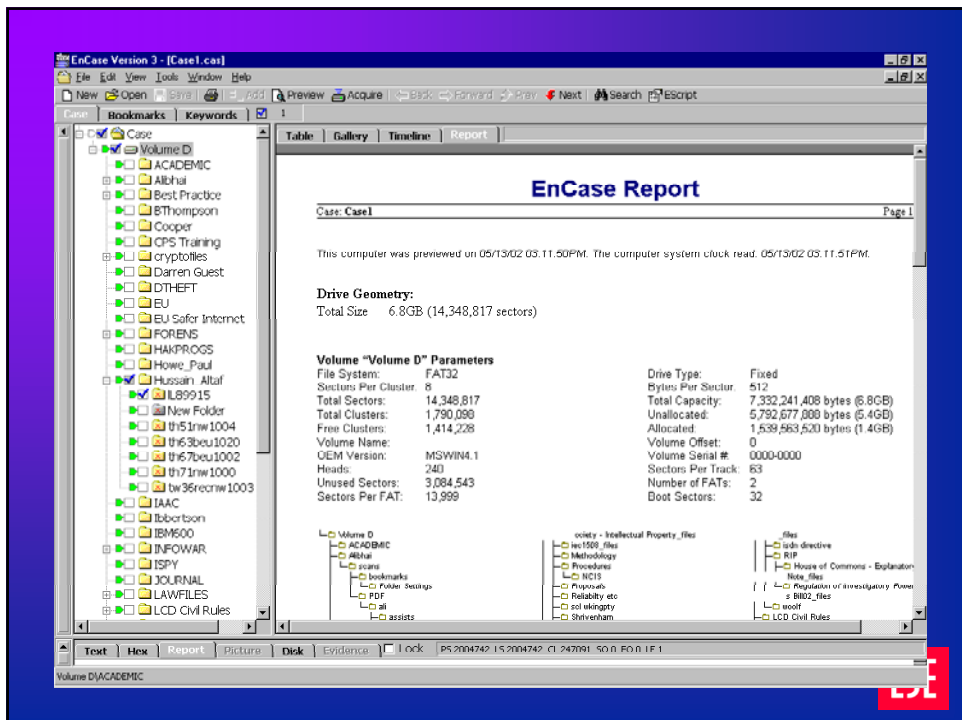
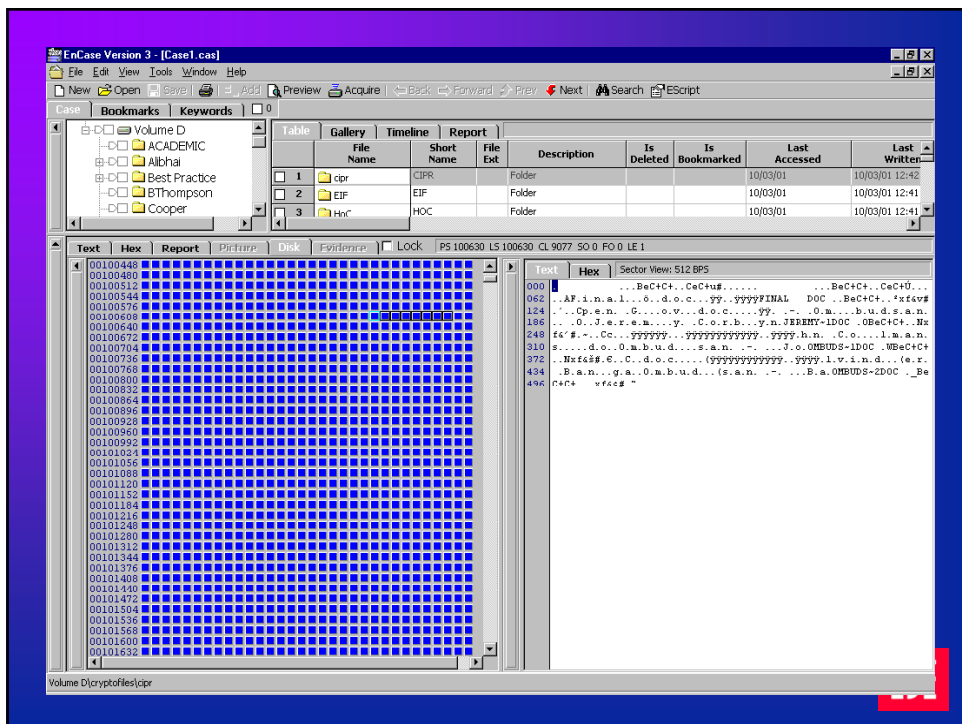
LSE

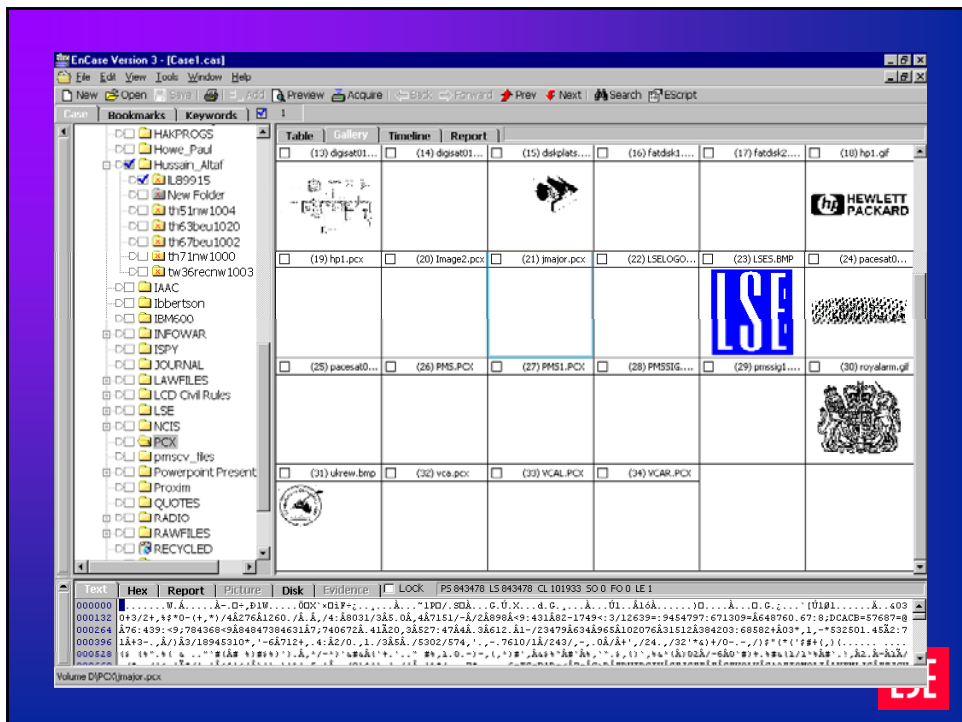
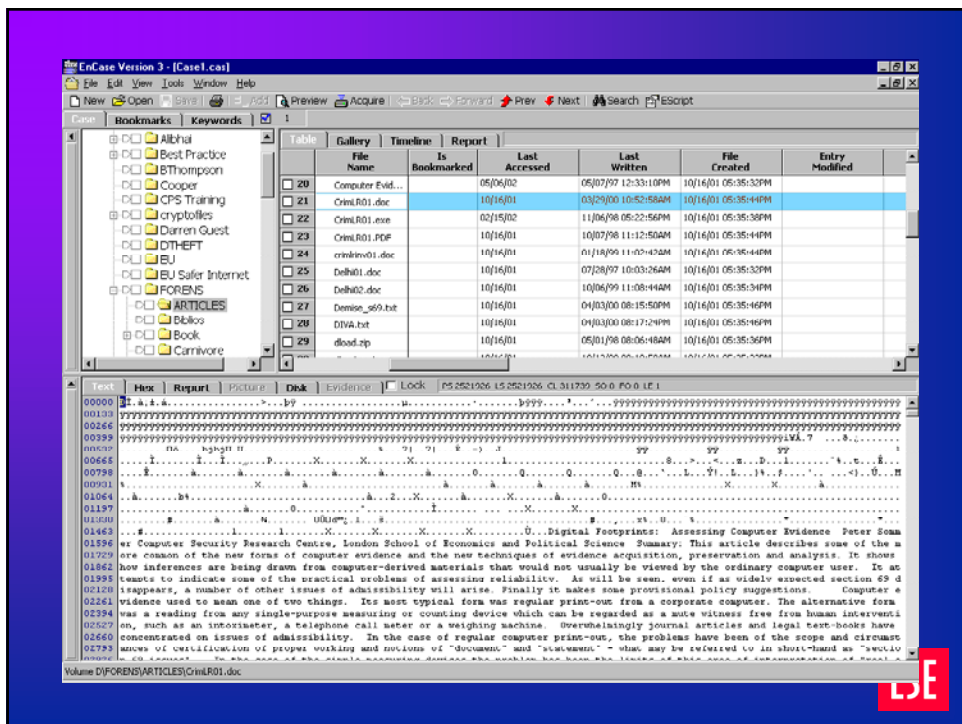
Disk Forensics

- **First products appear end 1980s**
- **Disk “imaging” / bit-copy**
- **Subsequent analysis**
- **Report Creation**
- **“Tool-box” / “Integrated”**
- **Live Analysis**
- **DIBS / Safeback / Maresware / NTI**
Authentec (Vogon) / EnCase / AccessData
FTK / ILOOK / ProDiscover

LSE







Disk Forensics

Most products for PC/Windows, but:

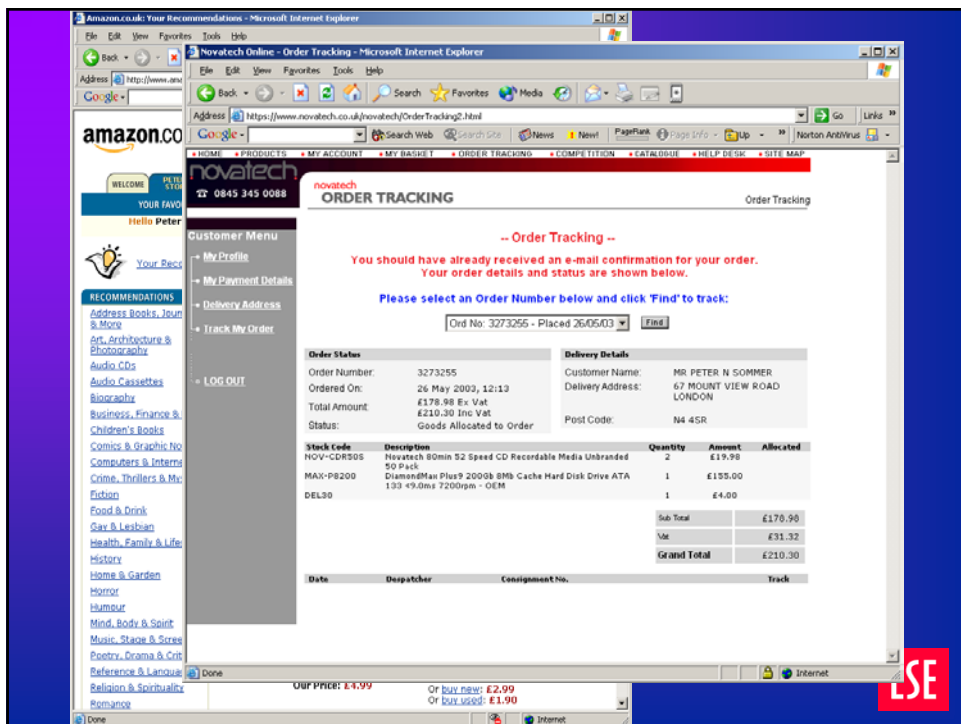
- **TCT - Coroner's Toolkit** by Dan Farmer and Wietse Venema
- **TASK**
- **SMART – ASRData**
- **Sleuthkit**
- **Helix**
- **Farmerdude**
- **Blackbag (Apple OSX)**



File from remote computer

- **But how do you demonstrate that the download is “reliable”?**
 - admissible
 - authentic
 - accurate
 - complete
- **What happens if you are downloading from a www site?**
 - caches - local and at ISP
 - dynamic pages, etc etc, XML etc

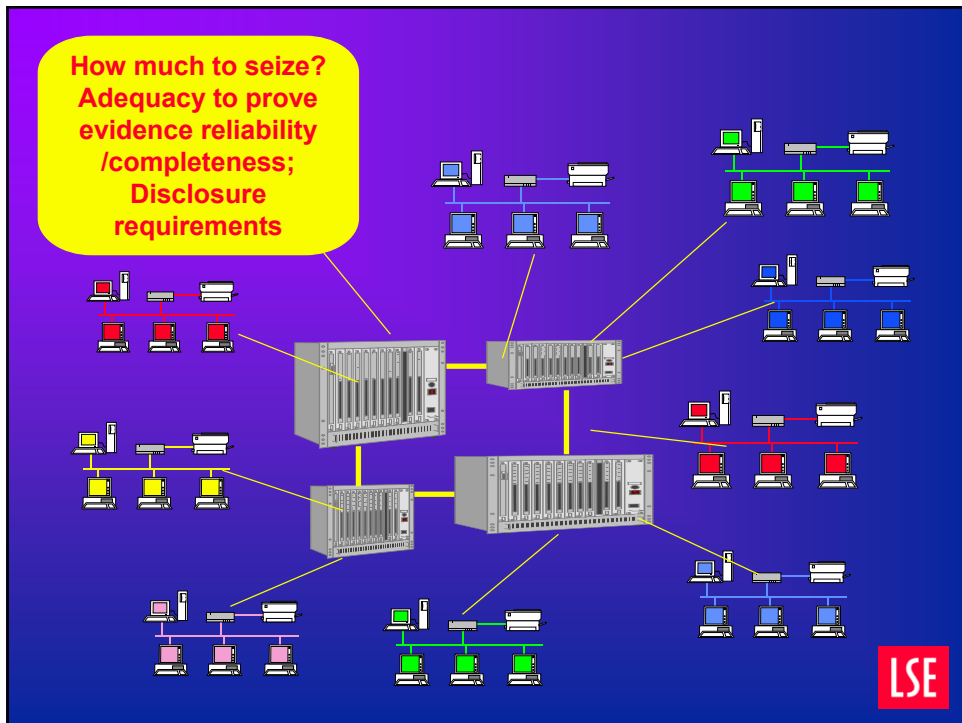




Controlled print-out from large mainframes

eg from banks, larger companies, government organisations

- we can't "image" a clearing bank
- can we take a live "snapshot"?
- how do demonstrate the system is working properly?
- what forms might "improper working" take?
- is the evidence complete?
- how can the other side test?
- Disclosure – CPIA compliance



Customer information from ISPs/CSPs

- usually by notice under RIPA, Chapter II or certificate under DPA, 1998, s 29(4) or production order under PACE
- evidence admissible under CJA, 2003, s 117
- customer identity
- time and duration of connection
- ?? IP address assigned ??
- Data Retention legislation
- warrants to seize ISP equipment possible, but would have huge impact on ISP - and all its customers
- reliability / testing ??

External Logs

- System Logs
- Web Logs
- Intrusion Detection System Logs
- Anti-Virus Logs
- ISP Logs
 - RADIUS
 - Web-Logs

Subject to
DPA/ RIPA
authorisation!

LSE

Squid Logs

```
1007949021,553      86 192.168.0.103 TCP_MEM_HIT/200 6947 GET http://us.a1.yimg.c
om/us.yimg.com/i/www/a5u6.gif graeme NONE/- image/gif
1007949022,484      4374 192.168.0.103 TCP_MISS/200 22349 GET http://www.yahoo.com/
graeme DIRECT/64,58,76,223 text/html
1007949022,884       74 192.168.0.103 TCP_HIT/200 4043 GET http://us.a1.yimg.com/u
s.yimg.com/a/ya/yahoo_promotions/fp2.gif graeme NONE/- image/gif
1007949027,488      4418 192.168.0.103 TCP_MISS/000 0 GET http://us.a1.yimg.com/us.
yimg.com/i/us/auc/b/auc16.1.gif graeme NONE/- -
1007949028,056      4569 192.168.0.103 TCP_MISS/000 0 GET http://us.i1.yimg.com/us.
yimg.com/i/us/sh/pr/hol01/r1b.gif graeme NONE/- -
1007949028,059      4604 192.168.0.103 TCP_MISS/000 0 GET http://us.i1.yimg.com/us.
yimg.com/i/us/sh/pr/hol01/bow.gif graeme NONE/- -
1007949028,061      4544 192.168.0.103 TCP_MISS/000 0 GET http://us.i1.yimg.com/us.
yimg.com/i/space.gif graeme NONE/- -
1007949028,063      4346 192.168.0.103 TCP_MISS/000 0 GET http://us.a1.yimg.com/us.
yimg.com/i/sh/h99/holly.gif graeme NONE/- -
1007949028,065      4258 192.168.0.103 TCP_MISS/000 0 GET http://us.a1.yimg.com/us.
yimg.com/a/an/anchor/shopping/ads/new37/dell.gif graeme NONE/- -
1007949029,233      1163 192.168.0.103 TCP_MISS/302 148 GET http://www.yahoo.com/r/
m1 graeme DIRECT/64,58,76,227 -
1007949032,096       73 192.168.0.103 TCP_HIT/200 1365 GET http://us.i1.yimg.com/u
s.yimg.com/i/us/pim/maillgin.gif graeme NONE/- image/gif
1007949032,324      3089 192.168.0.103 TCP_MISS/200 12044 GET http://mail.yahoo.com
[]
```

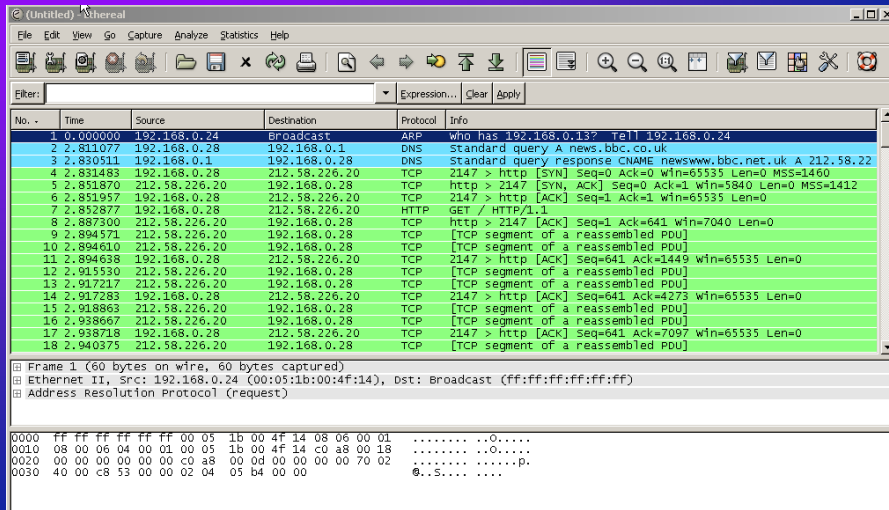
```
www.yahoo.com/r/m1
lun.net/images/sp.gif
H lun.net/images/linuxpower2.png
lun.net/images/rarrow.png
lun.net/images/eklektixsm.png
stats.lun.net/lp1xtrans.gif
lun.net/2002/0214/security.php3
lun.net/images/security.png
```

(96.03% to 100.00%) 60.00% Fri Feb 15 08:48 2002

| h = help

LSE

Network Logs



The screenshot shows the Wireshark interface with a list of captured packets. The first packet is an ARP request from 192.168.0.24 to the broadcast address 192.168.0.255. The detailed view shows the Ethernet II header, Internet Protocol Version 4 header, and the ARP request payload.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.24	Broadcast	ARP	who has 192.168.0.1? Tell 192.168.0.24
2	2.811077	192.168.0.28	192.168.0.1	DNS	Standard query A news.bbc.co.uk
3	2.830511	192.168.0.1	192.168.0.28	DNS	Standard query response CNAME newswww.bbc.net.uk A 212.58.22
4	2.831483	192.168.0.28	212.58.226.20	TCP	2147 > http [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460
5	2.851870	212.58.226.20	192.168.0.28	TCP	http > 2147 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1412
6	2.851957	192.168.0.28	212.58.226.20	TCP	2147 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
7	2.852877	192.168.0.28	212.58.226.20	HTTP	GET / HTTP/1.1
8	2.887300	212.58.226.20	192.168.0.28	TCP	http > 2147 [ACK] Seq=1 Ack=641 Win=7040 Len=0
9	2.894571	212.58.226.20	192.168.0.28	TCP	[TCP segment of a reassembled PDU]
10	2.894610	212.58.226.20	192.168.0.28	TCP	[TCP segment of a reassembled PDU]
11	2.894638	192.168.0.28	212.58.226.20	TCP	2147 > http [ACK] Seq=641 Ack=1449 Win=65535 Len=0
12	2.915530	212.58.226.20	192.168.0.28	TCP	[TCP segment of a reassembled PDU]
13	2.917217	212.58.226.20	192.168.0.28	TCP	[TCP segment of a reassembled PDU]
14	2.917283	192.168.0.28	212.58.226.20	TCP	2147 > http [ACK] Seq=641 Ack=4273 Win=65535 Len=0
15	2.918863	212.58.226.20	192.168.0.28	TCP	[TCP segment of a reassembled PDU]
16	2.938607	212.58.226.20	192.168.0.28	TCP	[TCP segment of a reassembled PDU]
17	2.938718	192.168.0.28	212.58.226.20	TCP	2147 > http [ACK] Seq=641 Ack=7097 Win=65535 Len=0
18	2.940375	212.58.226.20	192.168.0.28	TCP	[TCP segment of a reassembled PDU]

Frame 1 (60 bytes on wire (60 bytes captured))
 Ethernet II, Src: 192.168.0.24 (00:05:1b:00:4f:14), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 Address Resolution Protocol (request)

```

0000  ff ff ff ff ff ff 00 05 1b 00 4f 14 08 06 00 01  .....0.....
0010  08 00 06 04 00 01 00 05 1b 00 4f 14 c0 a8 00 13  .....0.....
0020  00 00 00 00 00 00 c0 a8 00 0d 00 00 00 00 70 02  .....p.....
0030  40 00 c8 53 00 00 02 04 05 b4 00 00 00 00 00 00  0..S.....
  
```

Interception

- **Product of Interception Warrants under RIPA, 2000**
 - material comes from ISPs/CSPs, whose technical co-operation is needed
 - conditions of warrant issue must be met
 - communications data (who is connected to what, when and for how long) plus content (what is said or transmitted) can both be collected
 - content can only be used for the purposes of the investigation
 - communications data is admissible

How, in the digital domain, can we differentiate “communications” data and content?

Computer Intrusion

- **Product of “interference with property” warrant under Police Act, 1997, Computer Misuse Act, 1990, exceptions**
 - covers covert entry into computers
 - installation of keystroke monitors, etc
 - legally tricky because relatively untried
 - evidence from suspect’s computers has been compromised and may therefore be questioned
 - s 78 PACE, 1984
 - in cross examination

LSE

Computer Intrusion

“Remote Management Tools”

- Back Orifice
- Sub Seven
- Hack’a’Tack
- D.I.R.T
- Magic Lantern
- SpectorSoft Pro

But investigator has the opportunity, covertly to alter data – or may be doing so inadvertently



LSE

Some challenging cases



Paedophile cases

Typical evidence:

- investigating Officer's logs - IRC, newsgroups etc
- ISP data - RADIUS logs etc
- Credit Card transactions
- On accused's HDD
 - Offending files
 - Email, Internet cache, Internet search terms, Chat, Peer-to-Peer activity
 - "Bad character"/propensity indications



Evidence in W0nderland

- Seized computers, data media
- Substantive files
 - pictures
 - texts
- Recovered “undeleted” material
- IRC, FTP
 - chat, configuration, logs
- Bestcrypt encryption
 - configuration, logs
- Zip (file compression)
 - configuration, logs

To demonstrate conspiracy:

- *Content of transactions*
- *Commonality of material*
- *Commonality of modus operandi*
- *Form and extent of “transactions”*



Operation Ore

- Landslide was an Internet subscription fulfilment service for websites offering obscene and indecent material
- Investigated by US Postal Service during 1999
- Raided September 1999
- Databases of customer transaction records found on various Sun Servers



Operation Ore

- **Database contained customer names, addresses & credit card details – 300,000**
transaction representing 100,000 individual, 7,200 in UK
- **Details passed to UK National Crime Squad; National Criminal Intelligence Service obtained background on each suspect**
- **Individual cases handled by UK local police forces**



Operation Ore

- **Most successful prosecutions depended on what was found on suspects' hard-drives etc**
 - “making”, “possession”
- **Some prosecutions – “incitement” - on the basis of the US work**
 - 7 computers, 11 hard-disks
 - “propensity” evidence



Credit Card Scams



Garages,
restaurants, etc

Perps normally
caught via pattern-
seeking software

Skimmer has memory to
hold card numbers; is
linked to PC which
downloads for later use

LSE

Credit Card Factories

Found on computer:

- Credit card numbers
- Downloading software
- Designs for cards
- Specialist card-printing software

Found on premises:

- Card printers
- Card embossers

LSE

Credit Card Scams

- 4408 0412 3456 7890
- 4 40804 123456789 0

MMI

Issuer

Customer

Check

JavaScript Credit Card Validation Function

The JavaScript function checks the validity of a credit card specified by the supplied parameters containing the card number and card type. Note that this routine does not supply credit card verification functionality, which can only be provided from within the server. It is, however, useful for intercepting user errors, and hence help provide a friendlier user-interface.

The specifications for valid credit cards have been taken from various sources on the web. The commonest credit cards are supported in this implementation, but more may be added as required. One of the advantages of this routine is the ease with which additional cards may be added, as it is totally data dependent.

Try the Routine. The following are credit cards numbers in a valid format:

American Express	2400 0000 0000 0000
Carte Blanche	3000 0000 0000 0000
Discover	6011 0000 0000 0000
Diners Club	3000 0000 0000 0000
eduhole	0000 0000 0000 0000
JCB	2131 0000 0000 0000
Mastercard	5000 0000 0000 0000
Novus	4000 0000 0000 0000
Switch	4000 0000 0000 0000
VISA	4000 0000 0000 0000

Select credit card: Enter number:

LSE



Warez Conspiracy



- Large-scale software piracy – Operation Buccaneer in the US, Operation Blossom in the UK
- “DrinkorDie”
- Several TB of disks seized during investigation of linked warez groups
- UK case lasted several months
- Significant problems of managing and analysing large quantities of data



LSE

Op Blossom

- Essentially a US investigation,, with UK local aspects
- Problems of proving a “conspiracy”
- 3rd party disclosure
- Disclosure from overseas agencies
- US witnesses had made plea bargains
- Suspicion of *agent provocateur* activity
- Problems of multiple defence teams
- =£11 m in costs (??)



Software Piracy in general

- Cracked files
- NFO “boast” files
- Serials lists
- (Rarely) specialist analysis software
- Emails
- Chat Logs
- FTP and web-servers, etc



Computer Forensics & Terrorism Cases

- Terrorism prosecutions present very little difficulty if an attack has taken place – provided you can find the perpetrators
- But most actual terrorism trials depend on proving *intentions*
 - To incite
 - To conspire
 - To prepare
- Typical defences are:
 - I am sympathetic but hadn't formed an intention; I knew the others but



Computer Forensics & Terrorism Cases

- Interception Evidence inadmissible, Bugging and surveillance evidence risky and expensive
- You can show intent (and propensity) by reference to:
 - Files found on disk
 - Terrorism manuals
 - "Intelligence"
 - Circuit diagrams
 - Web searches
 - Emails
 - Chat etc



Computer Forensics & Terrorism Cases

- **Crevice:**
 - Instructed after trial start
 - Precise prosecution evidence unclear until very late
 - LSC/VHCC procedures
 - How far can defence teams co-operate?
 - What happens when counsel thinks defendant isn't being candid – and worries what a computer investigation might find?

Emerging Problems

Emerging Problems

- **Ever larger quantities requiring analysis**
 - Current platforms inadequate in terms of computer resources
 - Can we select?
- **“Live” examinations**
 - How do we execute?
 - Are they reliable?
 - How does other side test?



Emerging Problems

- **Encryption**
 - VISTA, etc
 - Trusted Computing techniques
 - Consequences of DRM
 - Will computers of the future be encrypted by default?
- **IP-protecting legislation makes reverse engineering more difficult**
 - May have impact on forensic analysis software



Emerging Problems

Large Case Management

- 60 plus “critical” computers not uncommon
- Police and LE have permanent teams, defence do not
- Not feasible for everything to be printed out
- Popular “forensic” software too complex for untrained to use
- But case may rely on forensic artefacts
- Disclosure rules difficult to interpret for computer hard-disks
- Should be discussed fully at Case Management hearings



Forensic Computing

Forensic Computing / Computer Forensics has developed outside the main traditions of “Forensic Science”

Speed of change makes “peer reviewed” testing of methods difficult

- do we ignore new modes of crime because we haven’t tested our forensic tools?
- do we expose juries to lengthy technical disputes between experts?



Forensic Computing

Constant novelty:

- Forensic computing tracks all changes in technology – and social structures and conventions
- Insufficient time for usual cycle of peer-reviewed publication of new and tested forensic techniques and discoveries
- The greater the novelty, the greater the need for testability

LSE

Rate of Change ..

```
E:\>dir
Volume in drive E is IMAGE
Volume Serial Number is FE83-FD45

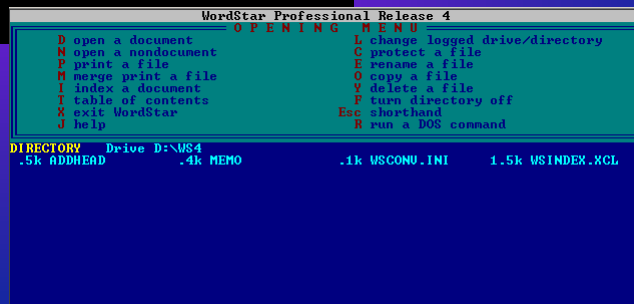
Directory of E:\

15/12/2005  21:01    <DIR>          booksmp3
35/11/2005  18:51    1,839,043,833  DUD_VIDEO_RECORDER.cdi
14/01/2007  09:44    <DIR>          FarmerDude
17/05/2006  14:17    <DIR>          Maps_v5
15/12/2005  21:01    <DIR>          MP3tmp
13/12/2005  11:54    <DIR>          MP3_2
04/09/2006  16:31    <DIR>          Retell Recordings
               1 File(s)  1,839,043,833 bytes
               6 Dir(s)  119,086,022,656 bytes free

E:\>
```

MsDos 3: 1984

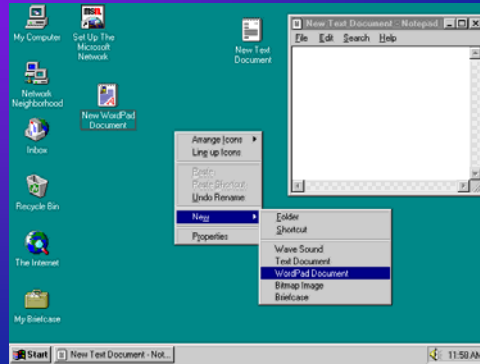
MsDos 5: 1991



LSE

Rate of Change ..

Windows 3.1: 1992



Windows 95: 1995

LSE

Rate of Change ..

Windows 98: 1998

Windows ME: 2000



Windows XP: 2001
Windows XP SP2: 2004



LSE

Rate of Change ..



Windows Vista: 2007



Windows Vista

- **Changed folder locations**
- **New file and disk back-up facilities** (disk imaging plus "shadow copy")
- **New means of recording date and time stamps**
- **In-built file indexing**
- **Drive encryption**
- **Email storage wholly changed**
- **Increased use of metadata or tags**
- **Changed thumbnails database, etc etc**



Rates of Change: Social Structures

- **Bulletin Boards**
- **Email**
- **Newsgroups**
- **Mail List Servers**
- **Internet Relay Chat - IRC**
- **Commercial Online Communities** – CompuServe, AOL, Yahoo Groups
- **Commercial Chat**
- **Peer-to-Peer** – 3 + generations
- **Blogs**
- **Modern Online Communities** – MySpace, Bebo, etc

For each of these are specialist items of software; and forensic artefacts from which inferences can be drawn



Rates of Change: Types of E-commerce

- **Web-sites + phone call**
- **Web-sites + email purchase**
- **Web-sites + use of 3rd party credit validation**
- **Web-sites + immediate fulfilment via credit card**
- **Internet-only payment schemes** – PayPal etc
- **Web-sites that track their customers and offer recommendations**
- **Web-based auction services**



Instructing Forensic Computing Experts



Instructing Forensic Computing Experts

- **What role?**
 - **Prosecution**
 - **Decision may already have been made by LE investigators**
 - Imaging, Evidence Capture
 - Analysis
 - Investigations
 - **Evidence production**
 - **Background explanations and opinion**
 - **Defence**



Instructing Forensic Computing Experts

Defence

- **What role?**
 - Due diligence
 - Explanations to Defence Team
 - Investigation to support defendant's claims
 - Expert-to-Expert Meetings
 - Provision of in-person testimony
- **What expertise?**
 - Hard-disks / data recovery
 - Hard-disks / computer and internet usage
 - Internet activity
 - Big / specialist commercial applications
 - Socio/cultural/commercial explanations
- **Tech Support**



Instructing Forensic Computing Experts

Defence

- **Tech Support**
 - Facilities for counsel
 - Will counsel need to use forensic software; should material be extracted to DVD etc?
 - Case Management hearings / co-operation with Prosecution on technical matters
 - Facilities for court
 - Verification of Pros technical presentation exhibits



Instructing Forensic Computing Experts

- **Defence**

- Shortage of skilled practitioners
- Remember the best experts are constantly having to make “availability” promises
- Start early!
- LSC
- Shared Experts in Conspiracy cases
- Staged Instructions
- Case Management Requirements
- Meetings between Experts
- When the client may be lying to counsel ... do you want an expert examination?



When the client may be lying to counsel ... do you want an expert examination?

- Careful instruction of expert...
- Range of places an expert will look, techniques used, difficult to forecast
- Don't try to second-guess what an expert may find / be restricted from finding
- Staged instructions run the risk that you run out of time / funding
- Warn the defendant of the risks!



Certification of Experts

- **What is the role for certification of experts?**
 - Who certifies?
 - Against what criteria?
 - Excellence vs competence
 - obsolescence?
- **Practicalities**
 - Complexity and rigour
 - Who assesses?
 - Cost to applicant / payment to assessor / scheme needs to be self-funded
- **CRFP assesses “current competence”**



Digital Footprints: Emerging Issues in Computer Forensics

Peter Sommer

peter@pmsommer.com

p.m.sommer@lse.ac.uk

