DIGITAL EVIDENCE

Emerging Problems in Forensic Computing

Peter Sommer

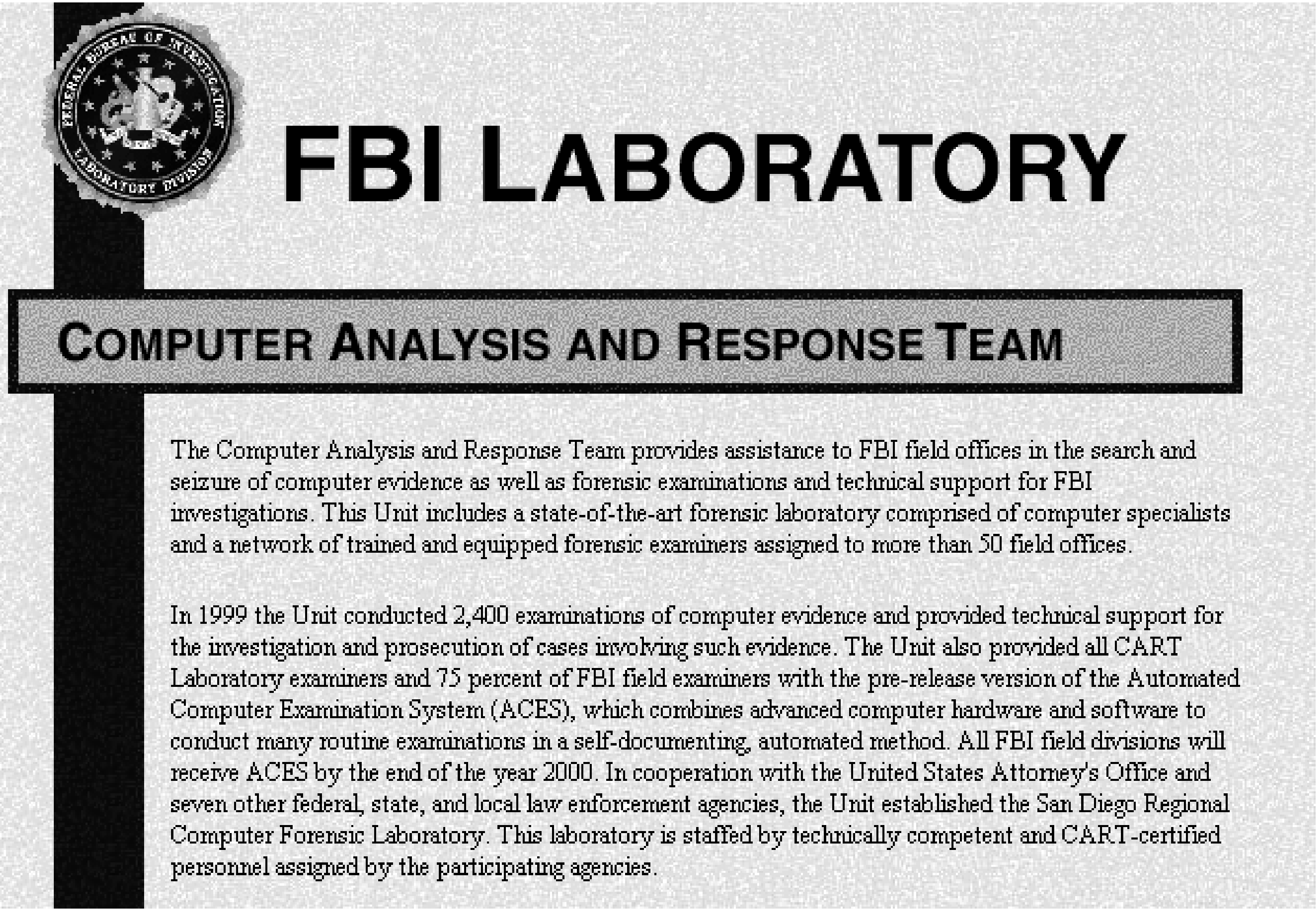
p.m.sommer@lse.ac.uk

Computer Forensics ….

Mostly a success story - < 14 years

- Data from computers can be reliably preserved and presented in court
- Deleted data can be recovered
- Events can be reconstructed
- Intentions can be inferred

Lots of good products and procedures to support ….

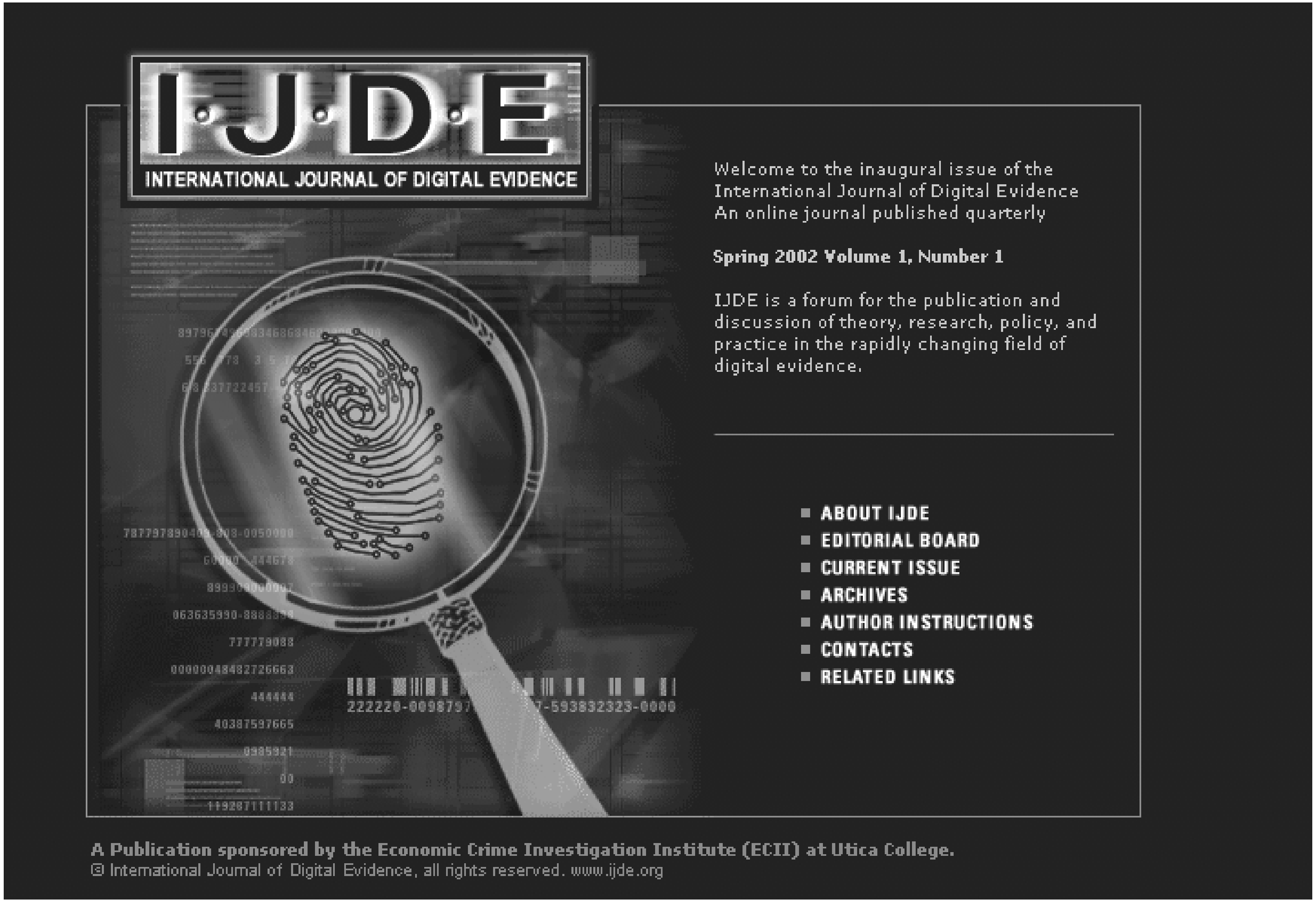


FBI LABORATORY

COMPUTER ANALYSIS AND RESPONSE TEAM

The Computer Analysis and Response Team provides assistance to FBI field offices in the search and seizure of computer evidence as well as forensic examinations and technical support for FBI investigations. This Unit includes a state-of-the-art forensic laboratory comprised of computer specialists and a network of trained and equipped forensic examiners assigned to more than 50 field offices.

In 1999 the Unit conducted 2,400 examinations of computer evidence and provided technical support for the investigation and prosecution of cases involving such evidence. The Unit also provided all CART Laboratory examiners and 75 percent of FBI field examiners with the pre-release version of the Automated Computer Examination System (ACES), which combines advanced computer hardware and software to conduct many routine examinations in a self-documenting, automated method. All FBI field divisions will receive ACES by the end of the year 2000. In cooperation with the United States Attorney's Office and seven other federal, state, and local law enforcement agencies, the Unit established the San Diego Regional Computer Forensic Laboratory. This laboratory is staffed by technically competent and CART-certified personnel assigned by the participating agencies.



Welcome to the inaugural issue of the International Journal of Digital Evidence
An online journal published quarterly

Spring 2002 Volume 1, Number 1

IJDE is a forum for the publication and discussion of theory, research, policy, and practice in the rapidly changing field of digital evidence.

A Publication sponsored by the Economic Crime Investigation Institute (ECII) at Utica College.

© International Journal of Digital Evidence, all rights reserved. www.ijde.org

Computer Forensics ….

deployed in:

- hacking
- fraud
- paedophiliac rings
- defamation
- immigration fraud
- narcotics trafficking
- credit card cloning
- software piracy
- electoral law
- obscene publication
- perjury
- forgery
- murder
- sexual harassment
- data theft – industrial espionage
- divorce

Computer Forensics ….

But this has been mostly about DISK forensics, specifically disks in PCs

What about:

- evidence from large systems?
- evidence from remote sites?
- evidence from networks?
- evidence from data eavesdropped in transmission?

Computer Forensics ….

Are the very high standards now existing for disk forensics creating unrealistic expectations for all other forms of computer-derived evidence?

Some essential background

- "Admissibility"
- Science vs Forensic Science vs What Courts Do
- The role of expert evidence
- Short history of forensic computing

“Admissibility”

- **Legal rules which determine whether potential evidence can be considered by a court**
- **Admissibility / weight of evidence**
- **Develops in England in 18th Century - to distinguish the roles of witness and juror**
- **Trend was towards increasing formality, though this has reversed over last 20 years**

“Admissibility”

- **Admissibility of “documents”**
- **Banker’s Books Act, “business documents in CJA 1988**
- **Computer documents and admissibility**
- **“Proper working” tests s 5 CEA, 1965, s 69 PACE**
- **US: problems of “novel scientific evidence” (Frye, Daubert) dealt with as admissibility issue**

US approach to novel scientific evidence

- **Judge acts as gate-keeper; evidence is inadmissible unless it is "generally scientifically acceptable"** ***Frye, 1923***
- **Updated in** ***Daubert v. Merrell Dow Pharmaceuticals Inc 113 S.Ct. 2786 (1993) ; Kumho Tire Company, Ltd et al v Patrick Carmichael, et al (Supreme Court, 1999)***

US approach to novel scientific evidence

Daubert tests:

- **whether the theory or technique can be (and has been) tested;**
- **the error rate associated with the method;**
- **publication in a peer-reviewed journal;**
- **whether the technique has gained widespread acceptance.**

“Admissibility”

- UK trend towards “free admissibility” - Auld Report
- Admissibility rules in computer and “scientific” evidence as a means of shielding lay juries from complex technical issues

Science vs Forensic Science vs What Courts Do

- Science: providing generalised descriptions which reduce the chaos of the observable world
  - ➔ major discoveries
  - ➔ minor discoveries
- Forensic science: (almost) a series of technologies to aid legal process
  - ➔ major discoveries
  - ➔ minor discoveries

Science vs Forensic Science vs What Courts Do

- **Forensic science, like regular science, advances by means of peer-reviewed publication**

Science vs Forensic Science vs What Courts Do

- In court: the decisions to be made are not “scientific” - judges and juries decide on:
  - ➔ was a contract broken?
  - ➔ was there a breach of duty of care?
  - ➔ was some-one defamed?
  - ➔ were the tests for a specific criminal offence satisfied?

Science vs Forensic Science vs What Courts Do

- Tests in court:
  - ➔ balance of probabilities
  - ➔ beyond a reasonable doubt
- Evidence from “scientists” and “experts” only *part* of the overall mix

Science vs Forensic Science vs What Courts Do

- Legal proof is what is demonstrated before the court
- Legal proof is about arriving at a conclusion from a specific set of circumstances
- Limits of Scientific Evidence: R v Adams, R v Dohenny (1996) AC
  - ➔ DNA evidence, Bayesian probabilities

Computer Evidence

Two situations

- Reliability of intended computer records
- Reliability of forensically located and recovered data

Intended Computer Records

- Regular computer “documents”
- Regular computer “reports” (from databases)
- Records of transactions
  - ➔ has transaction occurred?
  - ➔ what authentication was sought and acquired?
- Reproduction of stored images (eg from scanned paper-based originals)

Computer Forensics

Where there was no explicit intention to create computer records, but a "story" can be told: locating computer-derived materials for use in legal proceedings

- **data from seized computers**
- **audit trails / activity logs**
- **monitoring activities within computers**
- **monitoring networks and comms**

Computer Forensics

- **analysis of existing files, incl time and date stamps etc**
- **recovering deleted data stored on disk, etc**
- **analysis of log files (on local disks, on LANs, on Internet, from Telcos, etc**
- **interpretation thereof**

Characteristics of “Evidence”

Computer Evidence...

...is like any other evidence, it must be:

- admissible
- authentic
- accurate
- complete
- convincing to juries

Computer Evidence...

admissible

- common / civil code traditions
- adversarial / inquisitorial trials
- “proving” documents, copies
- US: 4th amendment rights / Federal Rules of Evidence
- UK: PACE, 1984; “business records” (s 24 CJA, 1988) etc etc

Computer Evidence...

authentic

- **can we explicitly link files, data to specific individuals and events?**
  - ➔ **access control**
  - ➔ **logging, audit logs**
  - ➔ **collateral evidence**
  - ➔ **crypto-based authentication**

Computer Evidence...

accurate

- reliability of computer process *not* data content
- can we explain how an exhibit came into being?
  - ➔ what does the computer system do?
  - ➔ what are its inputs?
  - ➔ what are the internal processes?
  - ➔ what are the controls?

Computer Evidence...

complete

- tells within its own terms a complete story of particular circumstances

Computer Evidence...

convincing to juries

- have probative value
- a subjective, practical test of presentation

Computer Evidence...

...is different from other evidence - computer data:

- **can change from moment to moment within a computer and along a transmission line**
- **can be easily altered without trace**
- **can be changed during evidence collection**

Computer Evidence...

...is different from other evidence:

- much immediate computer evidence cannot be read by humans
  - ➔ many exhibits are print-out derived from primary electronic material
- computers create evidence as well as record it
- rate of change of technology

Computer Evidence...

...creates as many opportunities as it provides threats:

- many more commercial transactions are recorded
- it is much easier to trace a person’s history and activities
- computer-assisted investigation methods become possible...

Brief History of Computer Evidence

- Mainframes
- PCs
- LANs
- Internet

Brief History of Computer Evidence

- Mainframes

- Controlled print-out
- Early problem of admissibility
- How do we test reliability?

Brief History of Computer Evidence

- PCs

- Can be seized
- Disks can be “imaged” and then analysed
- “Real” evidence
- can we trust the “imaging”?
- Quality of inferences

Brief History of Computer Evidence

- LANs

- Too complex to seize
- How do we ensure completeness?
- How do we ensure reliability?

Brief History of Computer Evidence

- Internet

- We can seize individual PCs, but we may also rely on:
- evidence from remote computers
- evidence from investigators' computers
- intercepts

Forensic procedures..

- Freezing the scene
    - ➔ a formal process
    - ➔ imaging
- Maintaining continuity of evidence
    - ➔ controlled copying
    - ➔ controlled print-out
- Contemporaneous notes > witness statements

Forensic procedures..

authenticity, accuracy, completeness, admissibility

- repeatability
- independent checking / auditing
- well-defined procedures
- check-lists
- novel scientific methods / juridicial quality
- anticipation of criticism

Disk Forensics

- First products appear end 1980s
- Disk "imaging" / bit-copy
- Subsequent analysis
- Report Creation
- "Tool-box" / "Integrated"
- DIBS / Safeback / Maresware / NTI Authentec / EnCase / AccessData FTK / ILOOK

Disk Forensics

Most products for PC/Windows, but:

- TCT - Coroner’s Toolkit by Dan Farmer and Wietse Venema
- TASK - @stake Sleuth Kit

Disk Forensics

Lots of work done on:

- file formats
- inner workings of operating systems, esp Windows
- inner workings of applications
- extreme forms of data recovery
- timelines, interpretation of events

Disk Forensics

Problems of using proprietary / “law enforcement only” products:

- disclosure of method
- protection of commercial interests of vendor
- “parity of arms” for defence
- paedophilia and “secrets” cases - release of material to the defence

General problems of inference

ACPO Good Practice Guide

1st edition: 1998

Principle 1: No action taken by Police or their agents should change data held on a computer or other media which may subsequently be relied upon in Court.

Principle 2: In exceptional circumstances where a person finds it necessary to access original data held on a target computer that person must be competent to do so and to give evidence explaining the relevance and the implications of their actions.

ACPO Good Practice Guide

Principle 3: An audit trail or other record of all processes applied to computer based evidence should be created and preserved. An independent third party should be able to repeat those processes and achieve the same result.

Principle 4: The onus rests with the Officer in charge of the case to ensure compliance with any law pertaining to the possession of, or access to, information contained on a computer. The officer must be satisfied that the use of any copying device or actions of any person having access to the computer complies with these laws.

ACPO Good Practice Guide

<u>Principle 5:</u> **The onus of ensuring that these principles are adhered to and that the evidence is admissible rests with the Officer in charge of the case. The officer must be satisfied that the use of any copying device or actions of any person having access to the computer complies with these principles.**

ACPO Good Practice Guide

- In its present form - strongly biased towards disk forensics
- New version under preparation

Other Sources of Evidence

- Controlled print-out from large system
- File from remote computes
- Investigator scrutiny of the Internet
- Customer information from ISPs/CSPs under RIPA Part II and DPA s 29(4)
- Product of Interception Warrants under RIPA, 2000
- Product of “interference with property” warrants under Police Act, 1997, CMA, 1990 exceptions
- Testimony, admissions

Controlled print-out from large mainframes

eg from banks, larger companies, government organisations ….

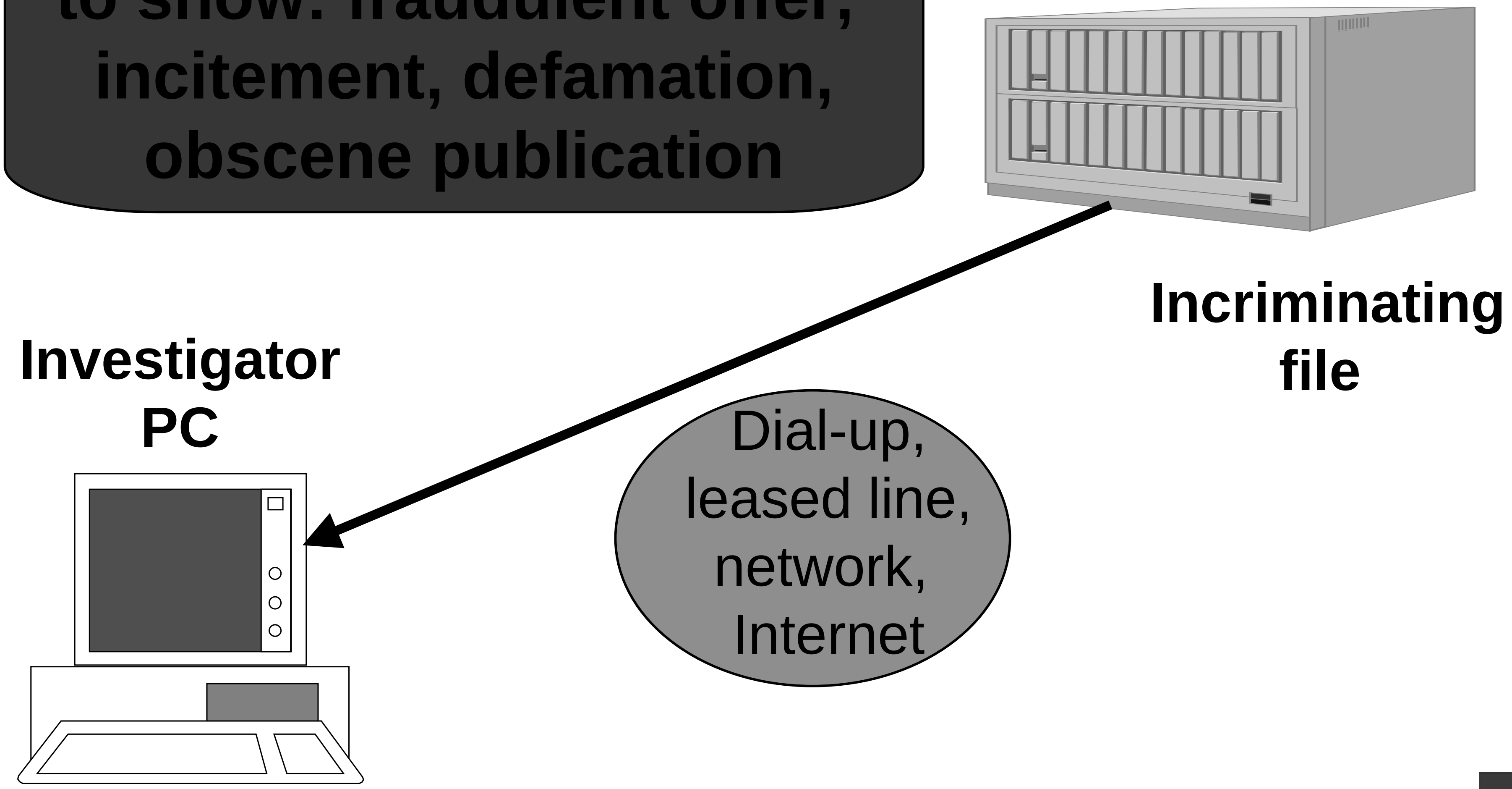
- how do demonstrate the system is working properly?
- what forms might “improper working” take?
- is the evidence complete?
- how can the other side test?

Controlled print-out from large complex systems

- how do demonstrate the system is working properly?
- what forms might “improper working” take?
- is the evidence complete?
- how can the other side test?

File from remote computer

to show: fraudulent offer, incitement, defamation, obscene publication



Incriminating file

Investigator PC

Dial-up, leased line, network, Internet

File from remote computer

- Remote computer correctly working?
- Provenance of computer source?
- Content/Party authentication?
- Acquisition Process?
- Investigator computer correctly working?
- Continuity of Evidence?
- Quality of Forensic Processing/ Presentation?

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

Investigator scrutiny of the Internet

- **investigator has no more or less access than ordinary user**
- **must conform to prevailing law and Codes of Practice -**
  - ➔ **can’t break the law**
  - ➔ **must avoid acting as *agent provocateur***
- **evidence is usually in the form of logs and downloads >> problems of establishing reliability - US *Tank* case**

Customer information from ISPs/CSPs

- customer identity
- time and duration of connection
- ?? IP address assigned ??
- usually by notice under RIPA, Chapter II or certificate under DPA, 1998, s 29(4) or production order under PACE
- evidence admissible under CJA, 1988, s 24
- warrants to seize ISP equipment possible, but would have huge impact on ISP - and all its customers
- reliability / testing ??

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,** ***but***
  - ➔ **content can only be used for intelligence and investiga**
  - ➔ **commun**

problems of evidence reliability;
problems of disclosure

Network Forensics

- Evidence collected “in normal operations”
  - ➔ logs
  - ➔ IDS outputs
- Evidence collected under specific surveillance
  - ➔ extended logs
  - ➔ “sniffers” etc

Network Forensics

- Specific Tools or careful use of regular tools ??
- Expectations of ISPs/CSPs who will contribute to the surveillance activities ??

Network Forensics

- Methods of surveillance
  - ➔ **active interception** direct, very local interception of individual at ISP or LAN
  - ➔ **semi-active interception** targeted on the basis of access to means of dynamic allocation of IP addresses
  - ➔ **passive interception** no information from ISP etc about dynamically allocated IP address - requires further information to link packet to individual

Network Forensics

Problems of disclosure

- specific methods
- network topology / configuration

(Problems of using proprietary products

- disclosure of method
- protection of commercial interests of vendor
- “parity of arms” for defence)

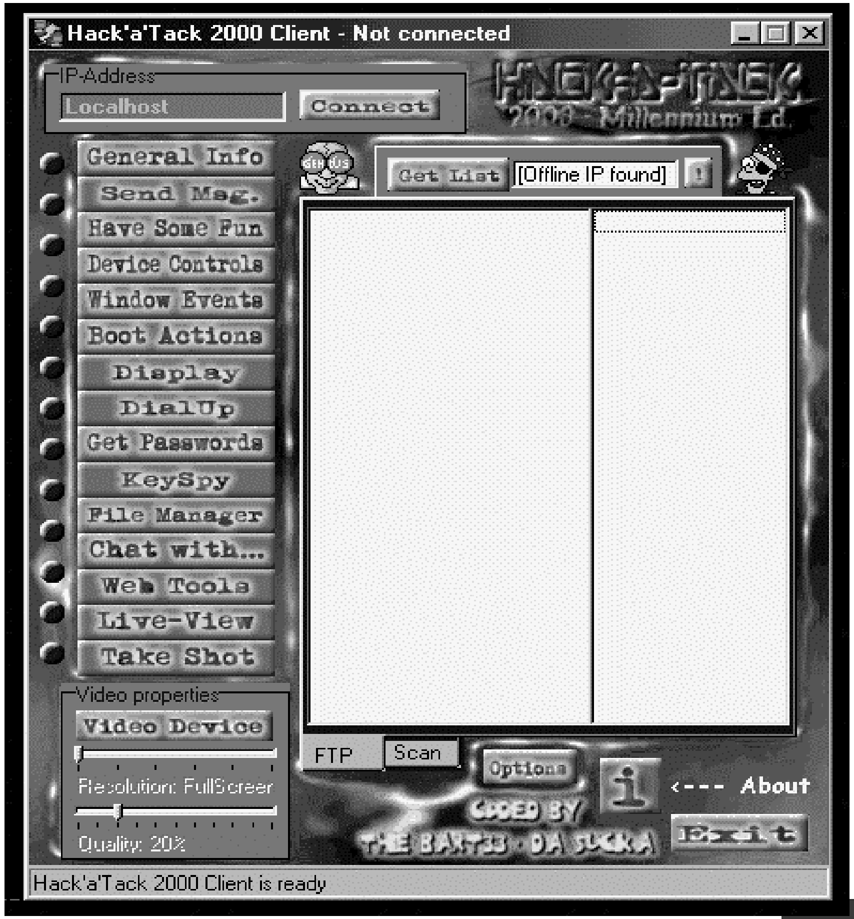
Computer Intrusion

- 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

Computer Intrusion

“Remote Management Tools”

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



Hack'a'Tack 2000 Client is ready

Conclusions

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

Issues of disclosure, testing, repeatability have been neglected – or not applied uniformly

Conclusions

The high standards in disk forensics are not matched in other areas:

- Records from big computers and networks
- Integrity of log files
- Integrity of products of surveilance activities

Conclusions

Problems of expert evidence:

- How do we explain accurately difficult stuff to lay audiences?
- Specialist juries?
- Pre-trial meetings between experts?
- Certification of experts?

Conclusions

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

Conclusions

- Disk forensics now of a very high standard - so much so that it creates expectations of other types of computer evidence
- For operational reasons, we can’t always work to the highest possible standards - how do we decide what is “enough”?

Conclusions

- We need better protocols for "controlled print-out" from mainframes and complex systems
  - ➔ this is still one of the most important operations, even more so in the civil, private sector

Conclusions

- How do we cope with downloaded evidence from remote computers?
  - ➔ www sites
  - ➔ ftp
  - ➔ newsgroups
  - ➔ mailing lists
  - ➔ etc etc
- Reliability, completeness, absence of tampering

Conclusions

- Investigators need to consider how to make the products of their monitoring and intercepts more reliable
  - ➔ disclosure of tools and precise methods
  - ➔ completeness of log
  - ➔ prevention of post-collection tampering
  - ➔ (proof of non-contamination of target)

Conclusions

- IETF RFC 3227: Guidelines for Evidence Collection and Archiving
- Proof of correct decryption?

Conclusions

Law enforcement problems:

- **proper role of police investigators**
- **multi-skilled investigations - forensics plus ???**
- **proper role of civilian technicians**
- **relationship with private sector**
- **training**

Conclusions

Practical investigations tend to rely on multiple streams of evidence which corroborate each other - each stream may have its weaknesses, but taken together may point to a single conclusion

Disk forensics may remain for some time the single most important form of digital evidence

DIGITAL EVIDENCE

Emerging Problems in Forensic Computing

Peter Sommer

p.m.sommer@lse.ac.uk