The Malicious Exploitation of Information Systems:

Preventing the Rise of the Insider Threat

6-7 November 2008, UCL

Issues in the Technologies of Digital Investigation

Peter Sommer

London School of Economics, Open University

peter@pmsommer.com

p.m.sommer@lse.ac.uk

LSE

Incidents

- Frauds by employees and 3rd parties
- Contractual disputes
- Allegations of failure of duty of care
- E-mail and Internet abuse
- Breach of confidentiality
- Online defamation
- Employee / HR disputes
- Sexual harassment
- Acquisition and storage of child abuse images
- Datatheft / Industrial Espionage
- Software piracy
- Theft of source code

LSE

Incidents

- Unauthorised access by employees
- Unauthorised access by 3rd parties – “hacking”
- Unauthorised data modification – incl viruses and trojans
- Abuse of corporate IT resources for private gain
- Use of corporate IT resources as one stage in a complex criminal act and where a 3rd party is victimised
- Use of corporate IT resources for illegal file-sharing
- DoS and DdoS attacks
- “Phishing” and “Pharming” attempts
- Etc etc
- **Requirements of disclosure in civil litigation**

LSE

Incidents

- Rare, Spectacular Events
- Events that occur everywhere to everyone… but still cause panic, distress, loss
- High Impact / Low Frequency
- High Frequency / Individually, Medium-to-Low Impact

LSE

Something suspicious is happening in and around your computer systems…

- What do you do?
- Where do you find help?
- How do you assess the investigator market?
- Is the person you want available?
- What are you really asking them to do?
- Is it going to be enough?

LSE

The Insider Threat: The Investigator's Perspective

- What are the suspicions?
- How likely is it that the client has mis-interpreted the situation?
- What powers do I have?
  - ➔ I start out with no powers, I need to acquire them from the client
- Now to try and locate evidence …

LSE

The Investigator's Perspective

- Now to try and locate evidence …
- How does the client's organisation work?
  - What functions does it perform?
  - How do I relate business functions to bits of hardware, software, computer records?
- Given the suspicions, what should I go for?
  - Transaction records
  - Emails
  - Web usage
  - Contents of PC, laptop, mobile phone, PDA, memory sticks, etc

LSE

The Investigator's Perspective

- **Are there any restrictions on my access?**
  - → **Client authorisation as employer**
  - → **Limits on employer's powers**
    - **Human Rights Act 1998**
    - **Data Protection Act,**
    - **Protection from Harassment Act, 1997**
    - **Regulation of Investigatory Powers Act 2000**

      Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
  - → **Computer Misuse Act 1990**
    - **as amended**

LSE

The Investigator's Perspective

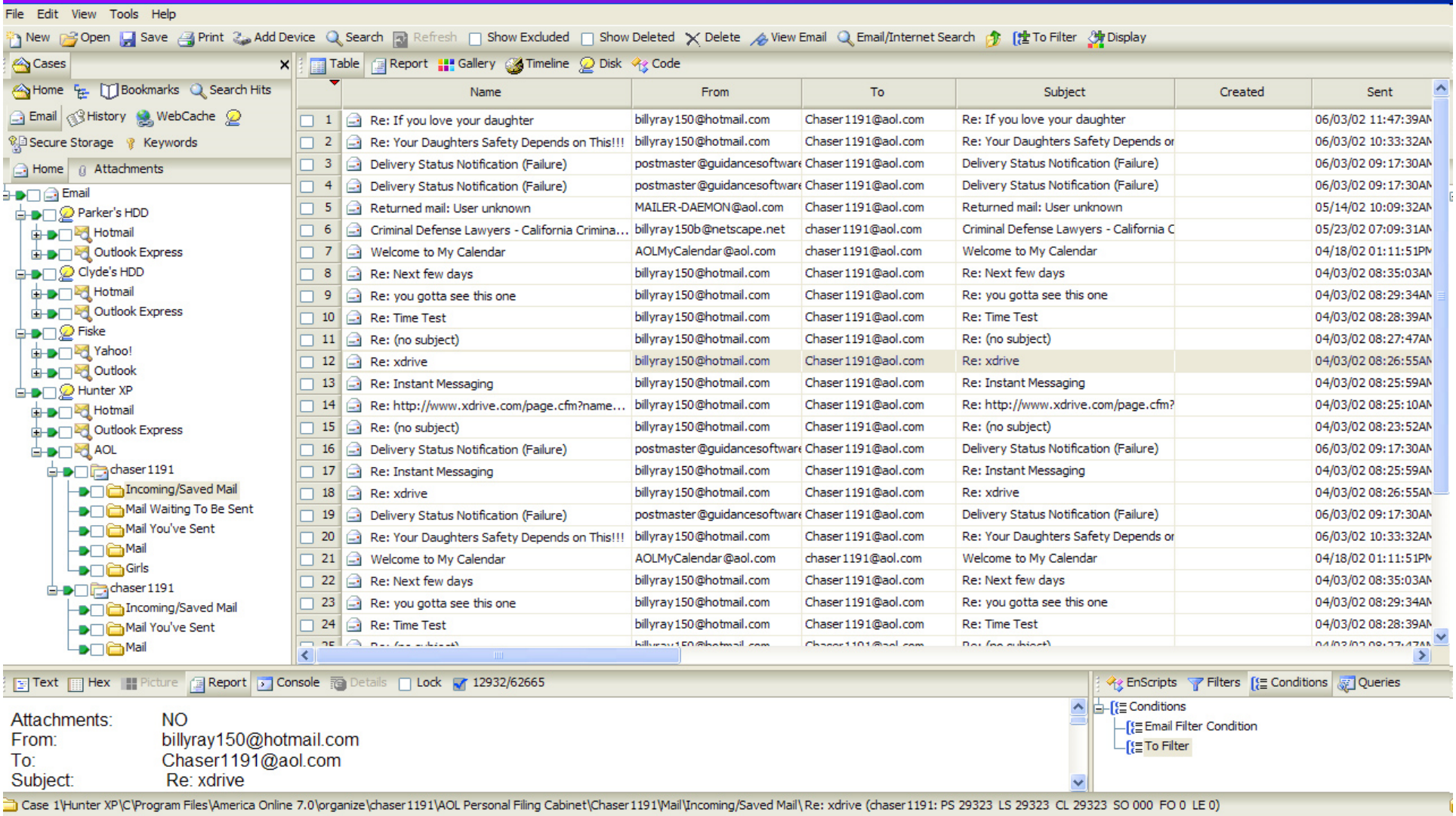
- Are there any restrictions on my access?
- Penalties for breach of powers:
  - → Criminal
  - → Abuse of Process
  - → Admissibility
  - → Harassment
  - → Etc etc

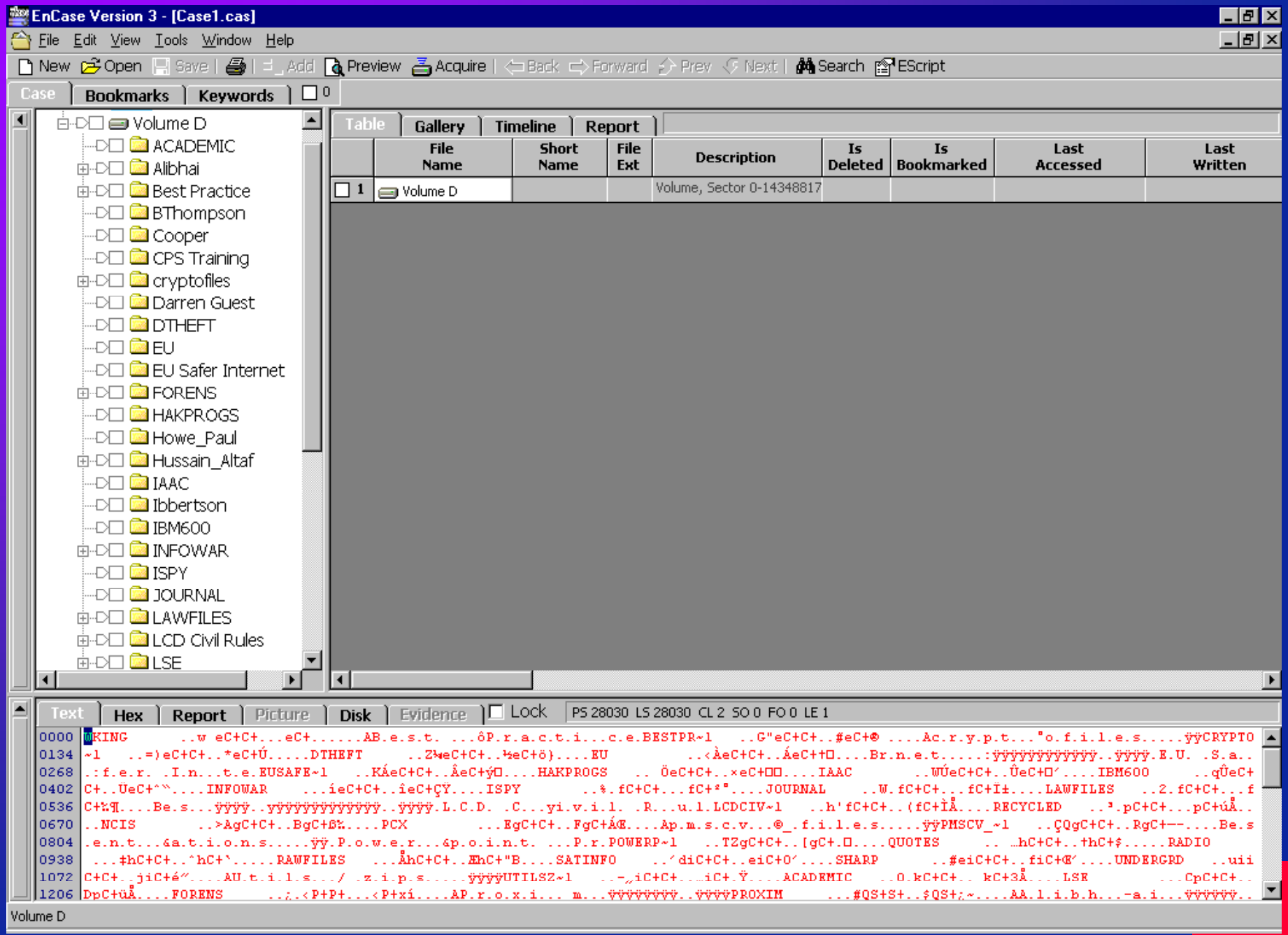
LSE

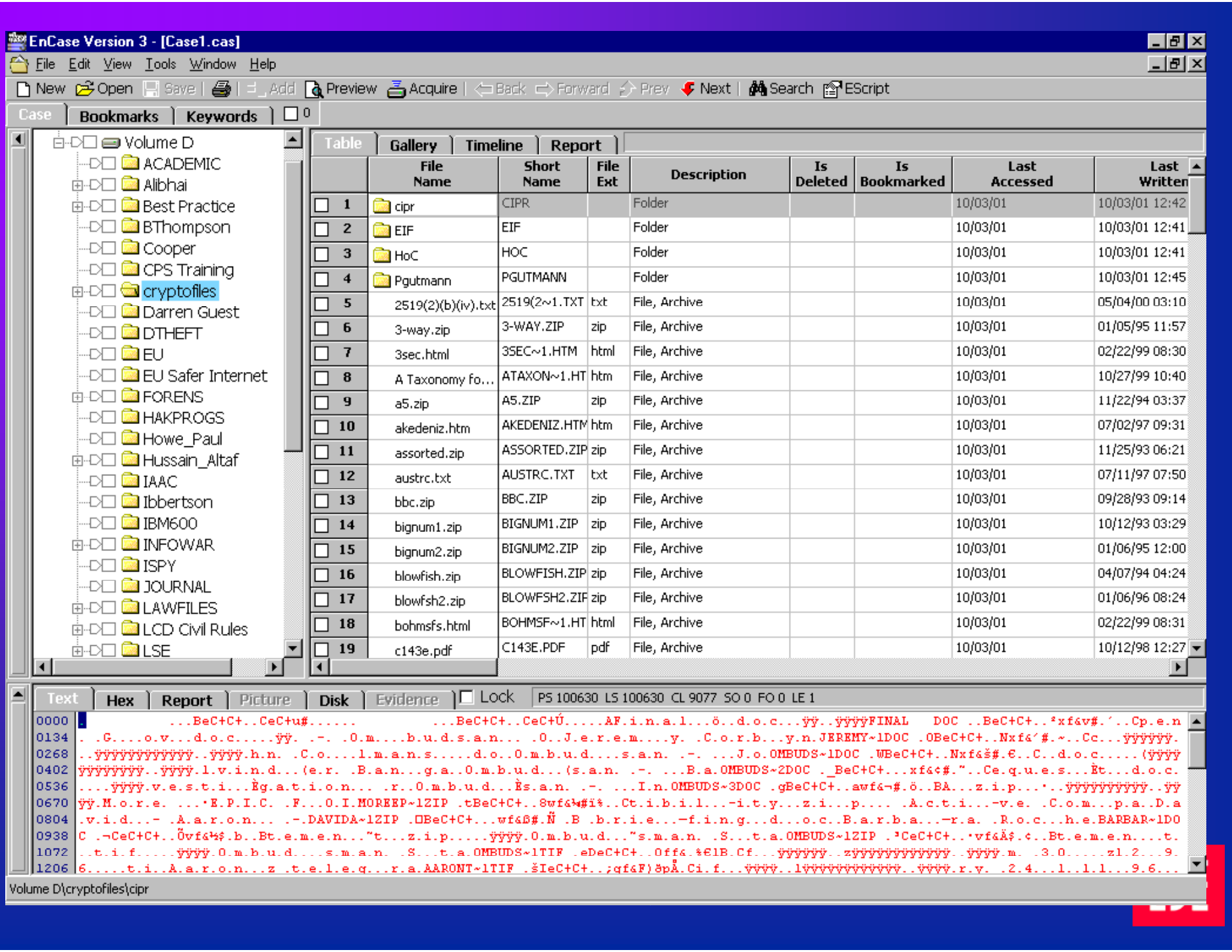
The Investigator's Perspective: Technologies

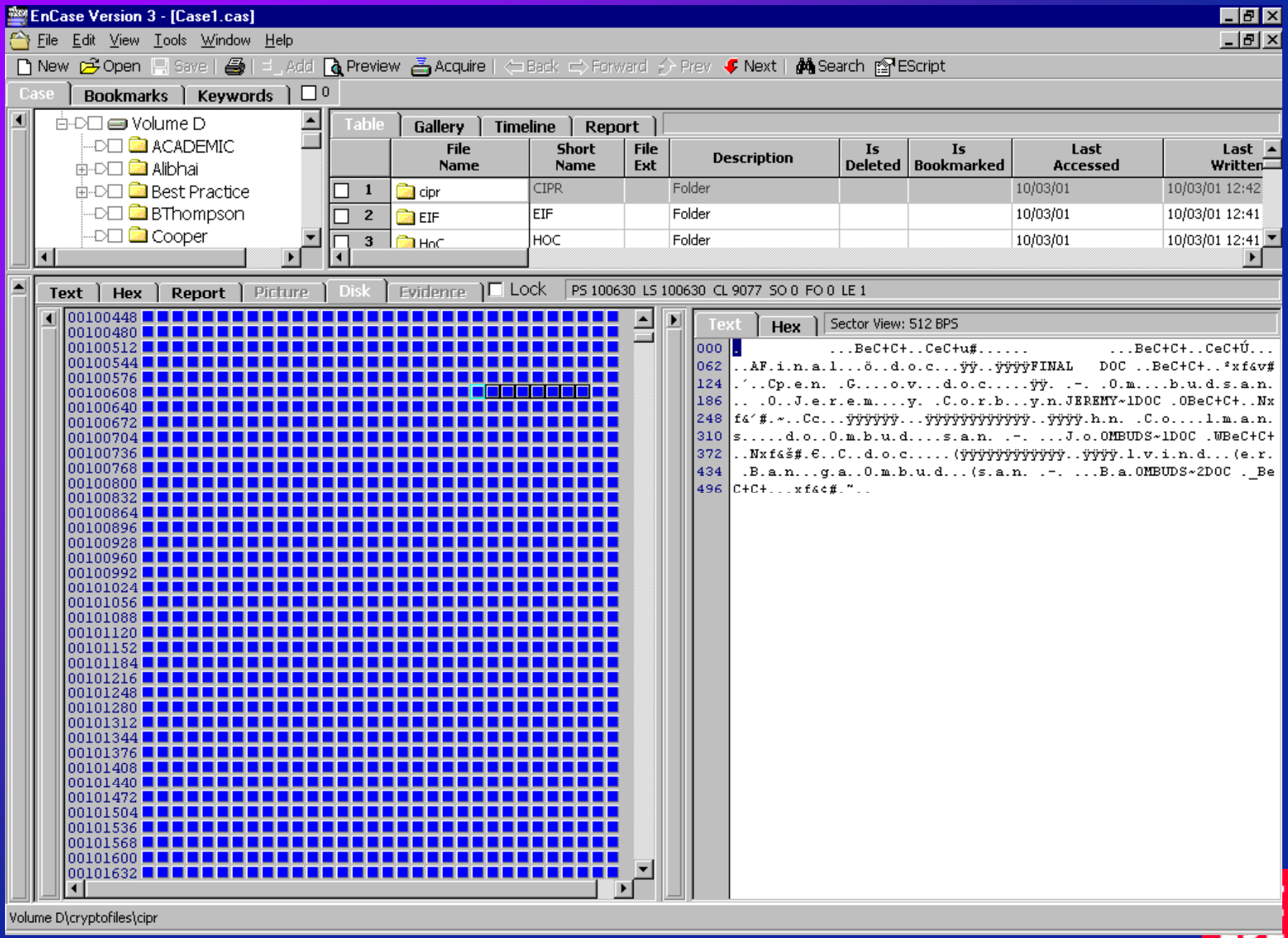
- **PCs**
  - → Make reliable complete copy ("forensic image") and analyse
    - Obvious, visible records, emails, Internet activity
    - Recovery of deleted date
    - Chronologies of activities
  - → Now standard procedures, products, training
  - → Imaging can be done covertly over night

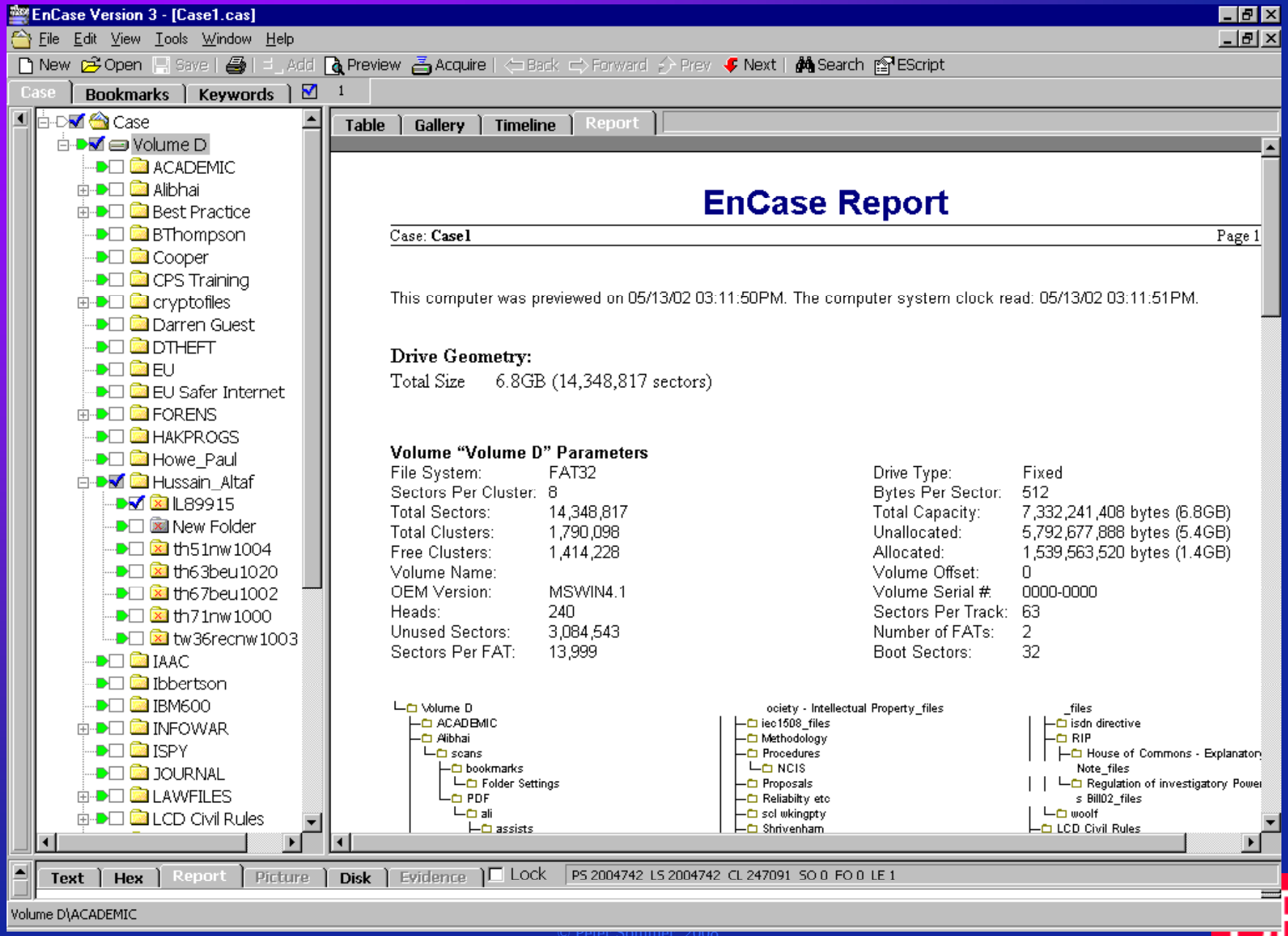
LSE

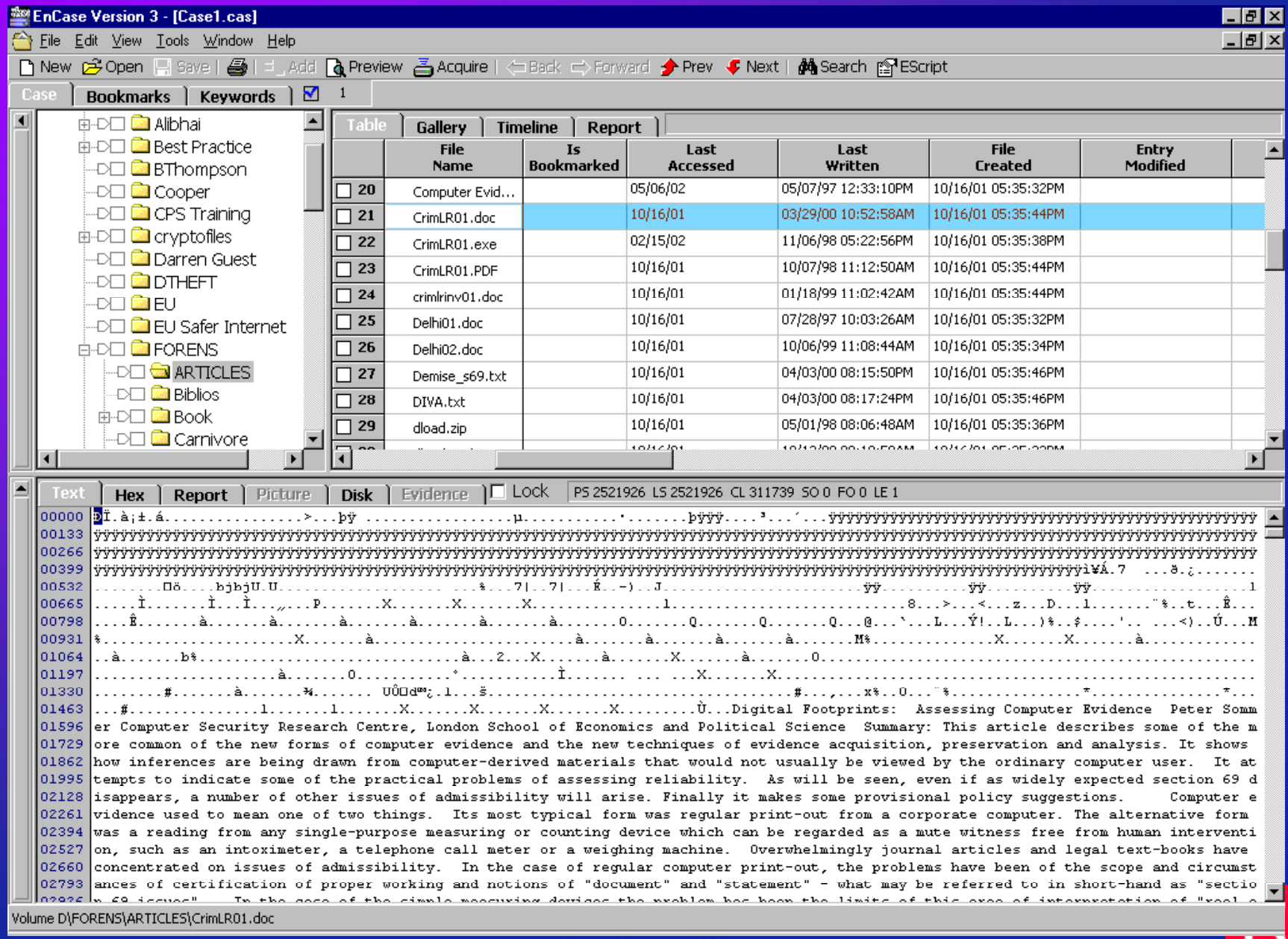


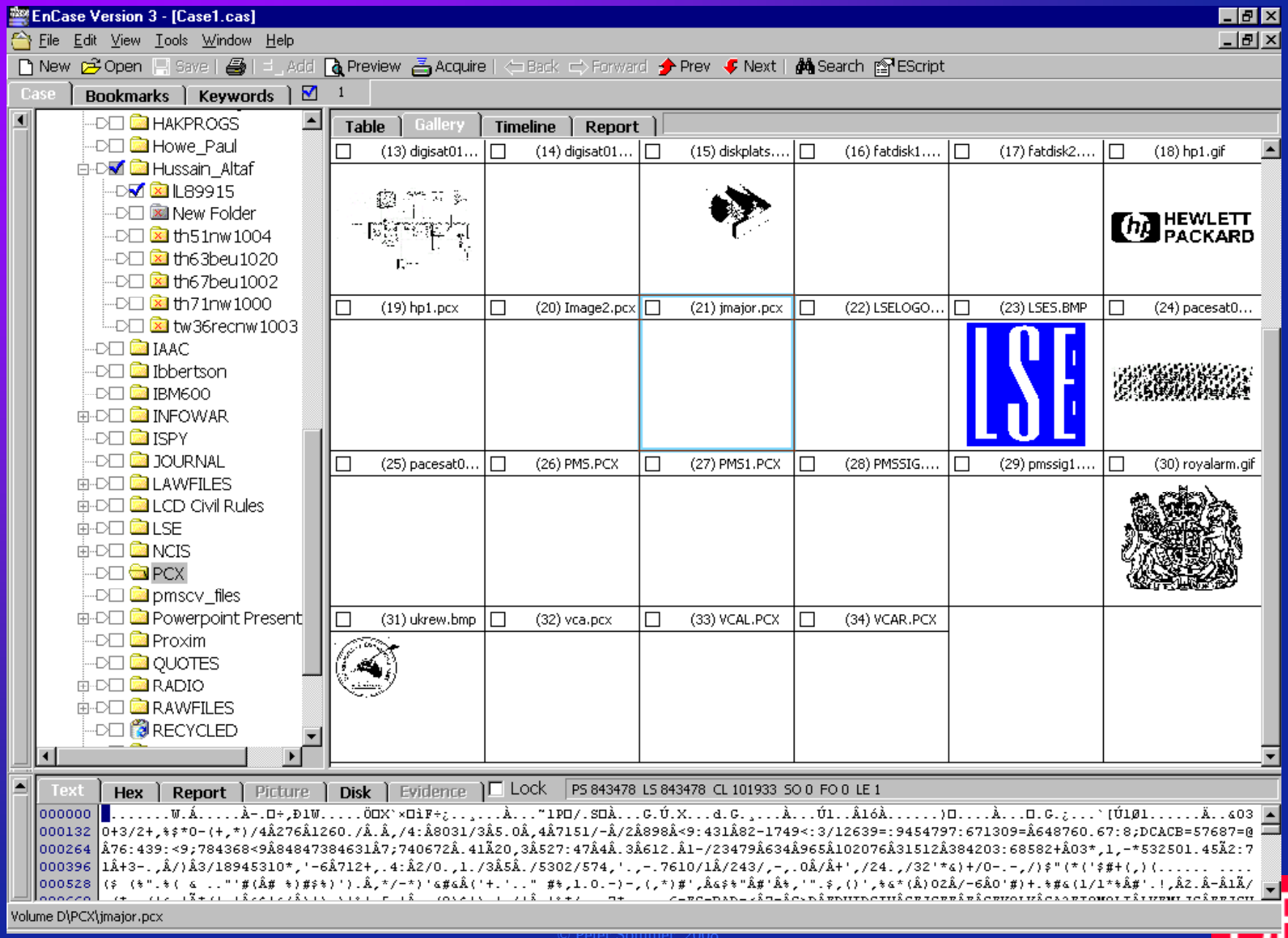

EnCase Version 3 - [Case1.cas]
File Edit View Tools Window Help
New Open Save Add Preview Acquire Back Forward Prev Next Search EScript
Case Bookmarks Keywords 0
Volume D
ACADEMIC
Alibhai
Best Practice
BThompson
Cooper
CPS Training
cryptofiles
Darren Guest
DTHEFT
EU
EU Safer Internet
FORENS
HAKPROGS
Howe_Paul
Hussain_Altaf
IAAC
Ibbertson
IBM600
INFOWAR
ISPY
JOURNAL
LAWFILES
LCD Civil Rules
LSE
Table Gallery Timeline Report
File Name
Short Name
File Ext
Description
Is Deleted
Is Bookmarked
Last Accessed
Last Written
1
Volume D
Volume, Sector 0-14348817
Text Hex Report Picture Disk Evidence Lock
PS 28030 LS 28030 CL 2 SO 0 FO 0 LE 1
Volume D

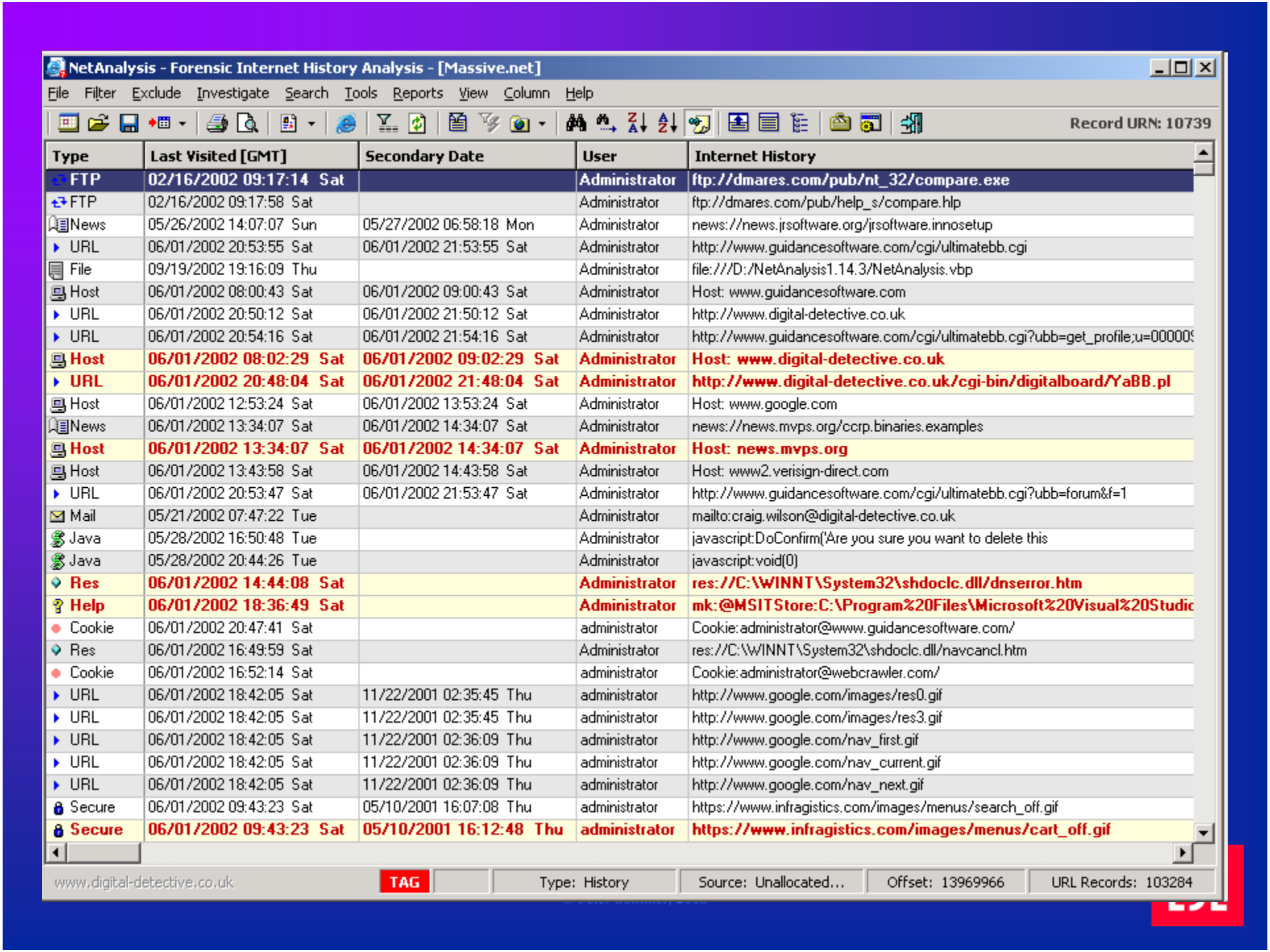

EnCase Version 3 - [Case1.cas]
File Edit View Tools Window Help
New Open Save Add Preview Acquire Back Forward Prev Next Search EScript
Case Bookmarks Keywords 0
Volume D
ACADEMIC
Alibhai
Best Practice
BThompson
Cooper
CPS Training
cryptofiles
Darren Guest
DTHEFT
EU
EU Safer Internet
FORENS
HAKPROGS
Howe_Paul
Hussain_Altaf
IAAC
Ibbertson
IBM600
INFOWAR
ISPY
JOURNAL
LAWFILES
LCD Civil Rules
LSE
Table Gallery Timeline Report
File Name | Short Name | File Ext | Description | Is Deleted | Is Bookmarked | Last Accessed | Last Written
1 cipr | CIPR | | Folder | | | 10/03/01 | 10/03/01 12:42
2 EIF | EIF | | Folder | | | 10/03/01 | 10/03/01 12:41
3 HoC | HOC | | Folder | | | 10/03/01 | 10/03/01 12:41
4 Pgutmann | PGUTMANN | | Folder | | | 10/03/01 | 10/03/01 12:45
5 2519(2)(b)(iv).txt | 2519(2~1.TXT | txt | File, Archive | | | 10/03/01 | 05/04/00 03:10
6 3-way.zip | 3-WAY.ZIP | zip | File, Archive | | | 10/03/01 | 01/05/95 11:57
7 3sec.html | 3SEC~1.HTM | html | File, Archive | | | 10/03/01 | 02/22/99 08:30
8 A Taxonomy fo... | ATAXON~1.HT | htm | File, Archive | | | 10/03/01 | 10/27/99 10:40
9 a5.zip | A5.ZIP | zip | File, Archive | | | 10/03/01 | 11/22/94 03:37
10 akedeniz.htm | AKEDENIZ.HTM | htm | File, Archive | | | 10/03/01 | 07/02/97 09:31
11 assorted.zip | ASSORTED.ZIP | zip | File, Archive | | | 10/03/01 | 11/25/93 06:21
12 austrc.txt | AUSTRC.TXT | txt | File, Archive | | | 10/03/01 | 07/11/97 07:50
13 bbc.zip | BBC.ZIP | zip | File, Archive | | | 10/03/01 | 09/28/93 09:14
14 bignum1.zip | BIGNUM1.ZIP | zip | File, Archive | | | 10/03/01 | 10/12/93 03:29
15 bignum2.zip | BIGNUM2.ZIP | zip | File, Archive | | | 10/03/01 | 01/06/95 12:00
16 blowfish.zip | BLOWFISH.ZIP | zip | File, Archive | | | 10/03/01 | 04/07/94 04:24
17 blowfsh2.zip | BLOWFSH2.ZIP | zip | File, Archive | | | 10/03/01 | 01/06/96 08:24
18 bohmsfs.html | BOHMSF~1.HT | html | File, Archive | | | 10/03/01 | 02/22/99 08:31
19 c143e.pdf | C143E.PDF | pdf | File, Archive | | | 10/03/01 | 10/12/98 12:27
Text Hex Report Picture Disk Evidence Lock
PS 100630 LS 100630 CL 9077 SO 0 FO 0 LE 1
Volume D\cryptofiles\cipr


EnCase Version 3 - [Case1.cas]
File Edit View Tools Window Help
New Open Save Add Preview Acquire Back Forward Prev Next Search EScript
Case Bookmarks Keywords 0
Volume D
ACADEMIC
Alibhai
Best Practice
BThompson
Cooper
Table Gallery Timeline Report
File Name | Short Name | File Ext | Description | Is Deleted | Is Bookmarked | Last Accessed | Last Written
1 cipr CIPR Folder 10/03/01 10/03/01 12:42
2 EIF EIF Folder 10/03/01 10/03/01 12:41
3 HoC HOC Folder 10/03/01 10/03/01 12:41
Text Hex Report Picture Disk Evidence Lock
PS 100630 LS 100630 CL 9077 SO 0 FO 0 LE 1
00100448
00100480
00100512
00100544
00100576
00100608
00100640
00100672
00100704
00100736
00100768
00100800
00100832
00100864
00100896
00100928
00100960
00100992
00101024
00101056
00101088
00101120
00101152
00101184
00101216
00101248
00101280
00101312
00101344
00101376
00101408
00101440
00101472
00101504
00101536
00101568
00101600
00101632
Text Hex Sector View: 512 BPS
000 ...BeC+C+..CeC+u#..... ...BeC+C+..CeC+Ú...
062 ..AF.i.n.a.l...ö..d.o.c...ÿÿ..ÿÿÿÿFINAL DOC ..BeC+C+..²xf&v#
124 .´..Cp.e.n. .G....o.v...d.o.c.....ÿÿ. .-. .O.m....b.u.d.s.a.n.
186 .. .O..J.e.r.e.m....y. .C.o.r.b...y.n.JEREMY~1DOC .OBeC+C+..Nx
248 f&´#.~..Cc...ÿÿÿÿÿÿ...ÿÿÿÿÿÿÿÿÿÿÿÿ..ÿÿÿÿ.h.n. .C.o....l.m.a.n.
310 s.....d.o..O.m.b.u.d....s.a.n. .-. ...J.o.OMBUDS~1DOC .WBeC+C+
372 ..Nxf&š#.€..C..d.o.c.....(ÿÿÿÿÿÿÿÿÿÿÿÿ..ÿÿÿÿ.l.v.i.n.d...(e.r.
434 .B.a.n...g.a..O.m.b.u.d...(s.a.n. .-. ...B.a.OMBUDS~2DOC ._Be
496 C+C+...xf&c#.˜..
Volume D\cryptofiles\cipr








NetAnalysis - Forensic Internet History Analysis - [Massive.net]
File Filter Exclude Investigate Search Tools Reports View Column Help
Record URN: 10739
Type | Last Visited [GMT] | Secondary Date | User | Internet History
FTP | 02/16/2002 09:17:14 Sat | | Administrator | ftp://dmares.com/pub/nt_32/compare.exe
FTP | 02/16/2002 09:17:58 Sat | | Administrator | ftp://dmares.com/pub/help_s/compare.hlp
News | 05/26/2002 14:07:07 Sun | 05/27/2002 06:58:18 Mon | Administrator | news://news.jrsoftware.org/jrsoftware.innosetup
URL | 06/01/2002 20:53:55 Sat | 06/01/2002 21:53:55 Sat | Administrator | http://www.guidancesoftware.com/cgi/ultimatebb.cgi
File | 09/19/2002 19:16:09 Thu | | Administrator | file:///D:/NetAnalysis1.14.3/NetAnalysis.vbp
Host | 06/01/2002 08:00:43 Sat | 06/01/2002 09:00:43 Sat | Administrator | Host: www.guidancesoftware.com
URL | 06/01/2002 20:50:12 Sat | 06/01/2002 21:50:12 Sat | Administrator | http://www.digital-detective.co.uk
URL | 06/01/2002 20:54:16 Sat | 06/01/2002 21:54:16 Sat | Administrator | http://www.guidancesoftware.com/cgi/ultimatebb.cgi?ubb=get_profile;u=00000
Host | 06/01/2002 08:02:29 Sat | 06/01/2002 09:02:29 Sat | Administrator | Host: www.digital-detective.co.uk
URL | 06/01/2002 20:48:04 Sat | 06/01/2002 21:48:04 Sat | Administrator | http://www.digital-detective.co.uk/cgi-bin/digitalboard/YaBB.pl
Host | 06/01/2002 12:53:24 Sat | 06/01/2002 13:53:24 Sat | Administrator | Host: www.google.com
News | 06/01/2002 13:34:07 Sat | 06/01/2002 14:34:07 Sat | Administrator | news://news.mvps.org/ccrp.binaries.examples
Host | 06/01/2002 13:34:07 Sat | 06/01/2002 14:34:07 Sat | Administrator | Host: news.mvps.org
Host | 06/01/2002 13:43:58 Sat | 06/01/2002 14:43:58 Sat | Administrator | Host: www2.verisign-direct.com
URL | 06/01/2002 20:53:47 Sat | 06/01/2002 21:53:47 Sat | Administrator | http://www.guidancesoftware.com/cgi/ultimatebb.cgi?ubb=forum&f=1
Mail | 05/21/2002 07:47:22 Tue | | Administrator | mailto:craig.wilson@digital-detective.co.uk
Java | 05/28/2002 16:50:48 Tue | | Administrator | javascript:DoConfirm('Are you sure you want to delete this
Java | 05/28/2002 20:44:26 Tue | | Administrator | javascript:void(0)
Res | 06/01/2002 14:44:08 Sat | | Administrator | res://C:\WINNT\System32\shdoclc.dll/dnserror.htm
Help | 06/01/2002 18:36:49 Sat | | Administrator | mk:@MSITStore:C:\Program%20Files\Microsoft%20Visual%20Studic
Cookie | 06/01/2002 20:47:41 Sat | | administrator | Cookie:administrator@www.guidancesoftware.com/
Res | 06/01/2002 16:49:59 Sat | | Administrator | res://C:\WINNT\System32\shdoclc.dll/navcancl.htm
Cookie | 06/01/2002 16:52:14 Sat | | administrator | Cookie:administrator@webcrawler.com/
URL | 06/01/2002 18:42:05 Sat | 11/22/2001 02:35:45 Thu | administrator | http://www.google.com/images/res0.gif
URL | 06/01/2002 18:42:05 Sat | 11/22/2001 02:35:45 Thu | administrator | http://www.google.com/images/res3.gif
URL | 06/01/2002 18:42:05 Sat | 11/22/2001 02:36:09 Thu | administrator | http://www.google.com/nav_first.gif
URL | 06/01/2002 18:42:05 Sat | 11/22/2001 02:36:09 Thu | administrator | http://www.google.com/nav_current.gif
URL | 06/01/2002 18:42:05 Sat | 11/22/2001 02:36:09 Thu | administrator | http://www.google.com/nav_next.gif
Secure | 06/01/2002 09:43:23 Sat | 05/10/2001 16:07:08 Thu | administrator | https://www.infragistics.com/images/menus/search_off.gif
Secure | 06/01/2002 09:43:23 Sat | 05/10/2001 16:12:48 Thu | administrator | https://www.infragistics.com/images/menus/cart_off.gif
www.digital-detective.co.uk
TAG
Type: History
Source: Unallocated...
Offset: 13969966
URL Records: 103284

The Investigator's Perspective

- **Main systems**
  - → Full imaging likely to be technically difficult
  - → Imaging is easier on a system taken off-line
    - But then the business is no longer functioning
  - → Partial copying runs risk that it shows an incomplete picture of events
  - → How far do existing back-up/archiving systems assist?
  - → How do I limit my examination so as not compromise the rights of third parties?
    - Employees, customers, clients

LSE

The Investigator's Perspective

- **Subsidiary systems**
  - ➔ Eg small specialist sub-systems
  - ➔ PDAs, laptops, cellphones, memory sticks, media players etc
  - ➔ Can we identify?
  - ➔ May be disputes over ownership, expectations of privacy
  - ➔ Some devices may be technically difficult to examine

LSE

The Investigator's Perspective

- **On-going suspicions: "live" investigations:**
  - → **Keyloggers**
  - → **Servlets**
  - → **Network monitoring**
  - → **CCTV**
  - → **Human surveillance**
  - → **Background investigations**
  - → **Physical searches**

LSE

Technical Support

- **Keyloggers**
  - ➔ **hardware**

completely invisible for computer operation (pure electronic device)
No software or drivers required
Huge 2MB flash memory disk, organized as a FAT file system
Installs as a flash drive for data retrieve (visible to system as additional disk)
Super fast data download (up to 100kB/s)
Quick and easy national layout support
Compatible with all Low-Speed USB keyboards (including Linux & Mac)

LSE

- k

Powered Keylogger 2.2 new

Invisibly records computer usage to the smallest detail.

- Automatically save the logs to USB Flash Drive new
- Records absolutely all keystrokes and passwords
- Keylogger invisibly sends logs via e-mail
- Fully supports the Unicode in contrast to many other keyloggers

Powered Keylogger is a driver-based software keylogger that secretly captures keystrokes, mouse clicks and passwords, tracks sent and received emails, monitors Internet activity and logs launched applications. Powered Keylogger is undetectable by a list of firewalls and antivirus software, even anti- spyware/anti- keyloggers won't locate it.

Download More info Purchase

Advanced Keylogger 2.0 new

Records every keystroke to encrypted easy-to-understand logs.

- Totally invisible to everyone but you
- Captures passwords and logins (even Winlogon passwords)
- Monitors e-mail clients and Internet activity

Advanced Keylogger records all computer activity and logs all information so that you can check later what's been done with the computer. You can also secretly receive logs of user's activity to your e-mail.

Download More info Purchase

LSE

With the Spector Pro Keylogger, you will be able to:

- Capture ev (including us
- Get the ex
- Capture &
- Read ever
- Review ev
- See everyt
- See every
- See every
- Quickly fin

Completely Invisible

Stealth Technology

The most advanced stealth technology available ensures that the Spector Pro keylogger is completely protected from everyone except those with authorized access.

Spector Pro does not appear in the Start Menu, Add/Remove Programs, Task Manager, Running Processes, System Tray, Registry, or on the Desktop – there aren't even any visible files.

"Spector Pro does the BEST job of hiding"
– PC Magazine

"EVERY word they type, EVERY link they click, SpectorSoft will be watching"
– InfoWorld Magazine

Instant Alerts

See What They Type and What They View

The Spector Pro keylogger will instantly inform you whenever they type – or even simply VIEW – any "alert words" or phrases that you specify.

Spector Pro continuously looks for alert words in EVERYTHING they type, EVERY web site they visit, ALL chats/Instant Messages and in EACH email sent or received.

EVERY time a keyword is detected, Spector Pro will immediately email you a detailed report of WHEN, WHERE and HOW the keyword was used.

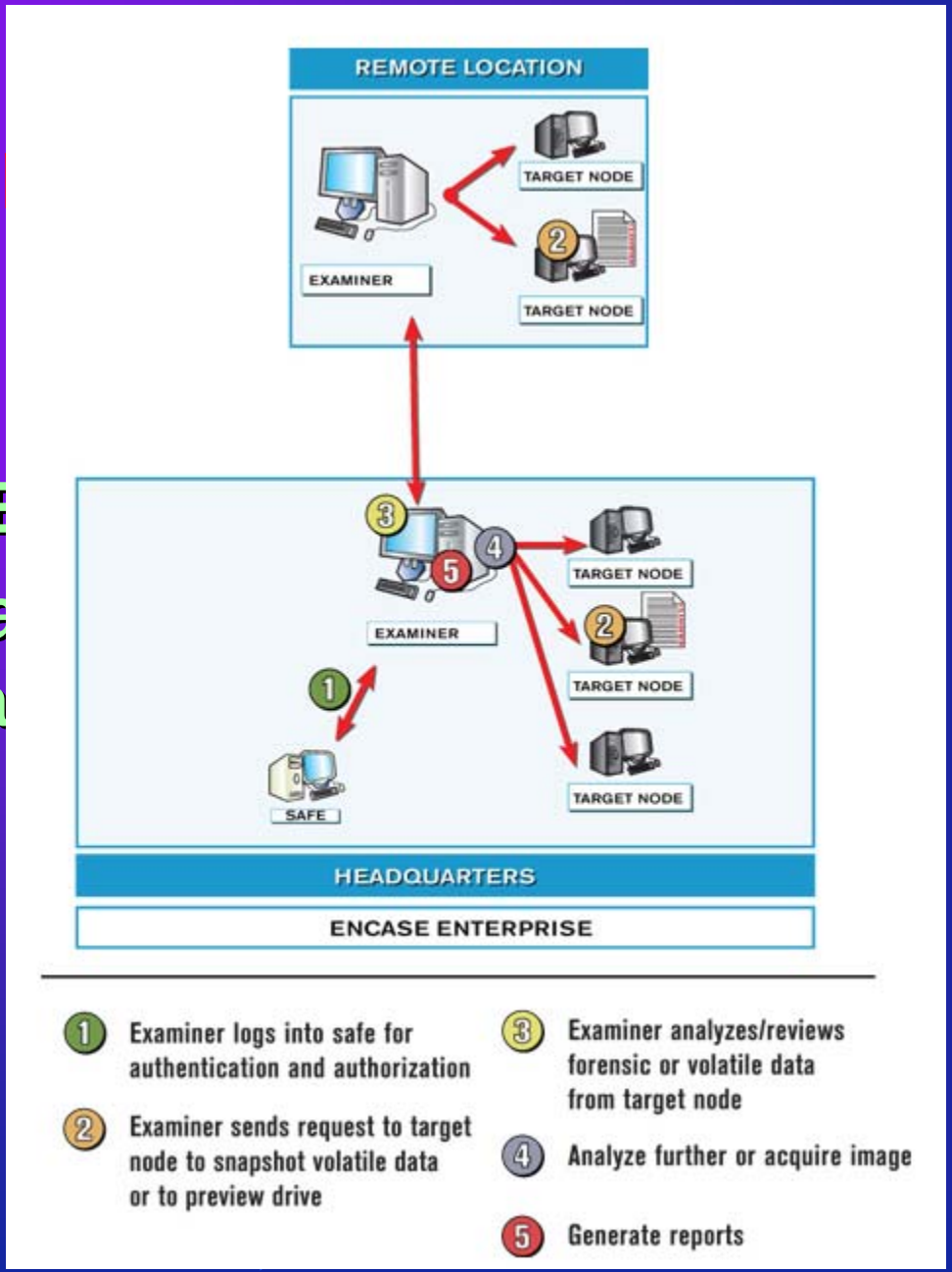
Alerts are sent to your office, home, cell phone or wherever you want!

"This is one slick piece of technology"
– US News & World Report

LSE

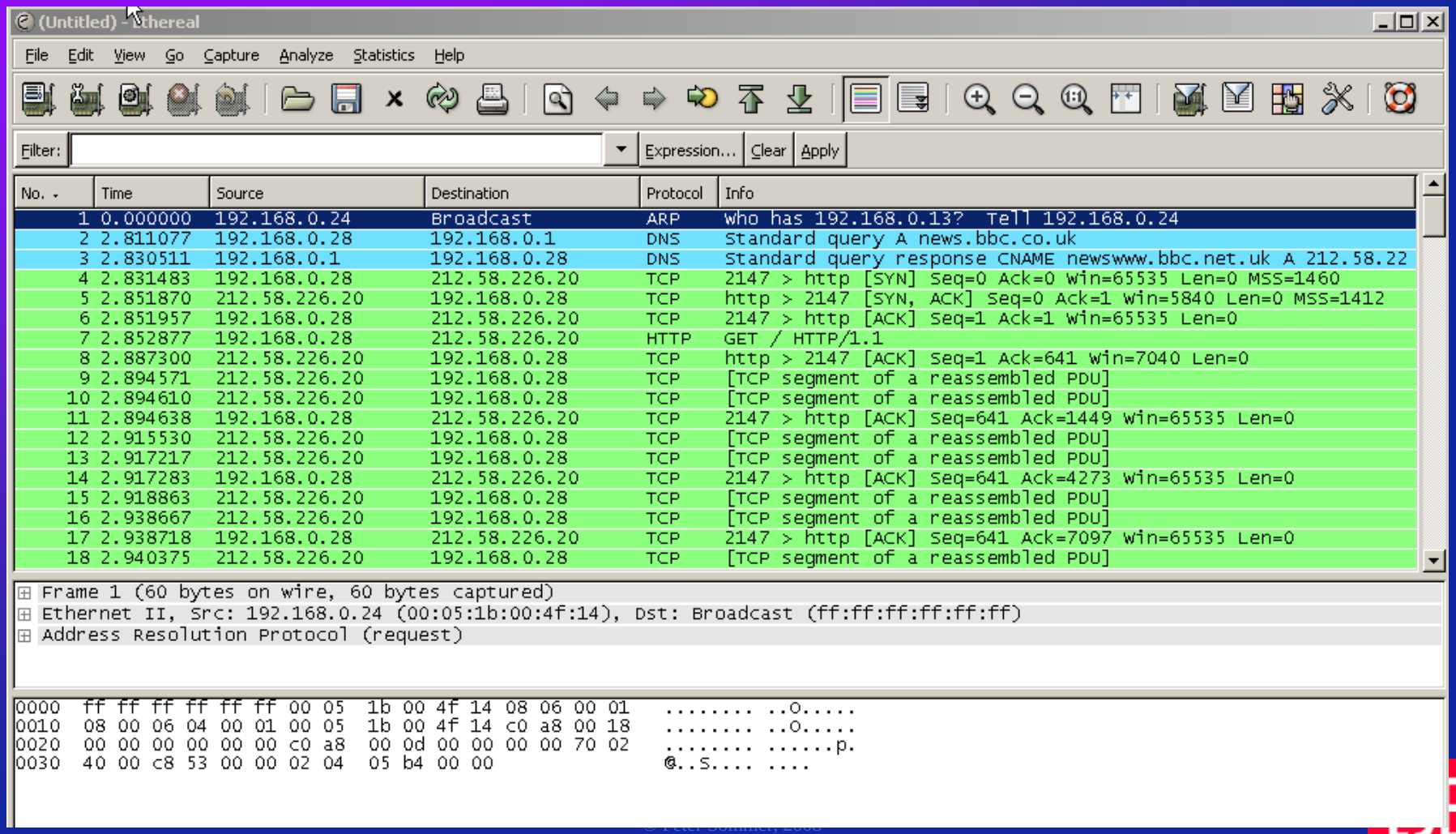
Tech

- **Servlets**
  - → Eg EnCase E
  - → Applied on a forensic exa



LSE

Network Surveillance



External Logs

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

Subject to DPA/ RIPA authorisation and/or consent!

LSE

Squid Logs

```
1007949021.553     86 192.168.0.103 TCP_MEM_HIT/200 6947 GET http://us.a1.yimg.com/us.yimg.com/i/ww/m5v6.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/us.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/rib.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/us.yimg.com/i/us/pim/maillogin.gif graeme NONE/- image/gif
1007949032.324   3089 192.168.0.103 TCP_MISS/200 12044 GET http://mail.yahoo.com
:
```

```
    lwn.net/images/sp.gif
H   lwn.net/images/linuxpower2.png
    lwn.net/images/rarrow.png
    lwn.net/images/eklektixsm.png
    stats.lwn.net/1pixtrans.gif
    lwn.net/2002/0214/security.php3
    lwn.net/images/security.png
(96.03% to 100.00%) 60.00% Fri Feb 15 08:48 2002                    l h = help
```

LSE

Forensic Readiness Plan

Why have plan?

- To reduce costs and panic
- External consultants will have to “learn” the business
- Lawyers will have to identify admissibility and privilege issues on the spot
- Can also be used for other legal situations, eg internal disciplinary disputes, routine transaction disputes, to aid law enforcement

LSE

Forensic Readiness Programs

Essentially:

- **Based on threat analysis / scenario development**
- **Requires identification of potential evidence / disclosure requirements – and plan for their formal production**
- **Results in a proper Contingency Plan – which is tested and kept up-to-date**

LSE

7-step Forensic Readiness Plan

Identify:

- the main likely threats/ legal challenges faced by your organisation
- what sorts of evidence / disclosure you are likely to need if you have to proceed to civil or criminal litigation
- what you will need to do to meet various regulatory and compliance requirements
- how far you may have that material already
- what you will need to do to secure additional essential material

LSE

7-step Forensic Readiness Plan

- the management, skills and resources implications for your organisation
- turn the results into an action plan – which will need regular revision as the organisation and its ICT infrastructure develops.

LSE

7-step Forensic Readiness Plan

The Good News:

quite a bit of the work may already have been carried out elsewhere in the organisation….

…….Disaster Recovery / Business Contingency Plans

LSE

Business Contingency Plans

- **Preparation against disaster:**
  - → Fire
  - → Flood
  - → Terrorism
  - → Denial of access
  - → Computer failure
  - → Etc etc

LSE

Business Contingency Plans

- **Tells organisation what to do:**
  - ➔ Emergency Priorities
  - ➔ Team that will act / Reporting Responsibilities
  - ➔ Migrated offices, locations
  - ➔ Migrated people
  - ➔ Migrated ICT
  - ➔ PR for customers, clients, investors, bankers, public-at-large etc

LSE

Business Contingency Plans

Research, Design

- Business Analysis
  - → to determine priorities (it's too expensive to restore everything instantly)
- Relation of business processes to specific ICT resources, hardware, software, communications links; availability of back-up
- Detailed plan for who does what when
- Emergency Response Team
- Internally published Plan
- Frequent Testing and Revision

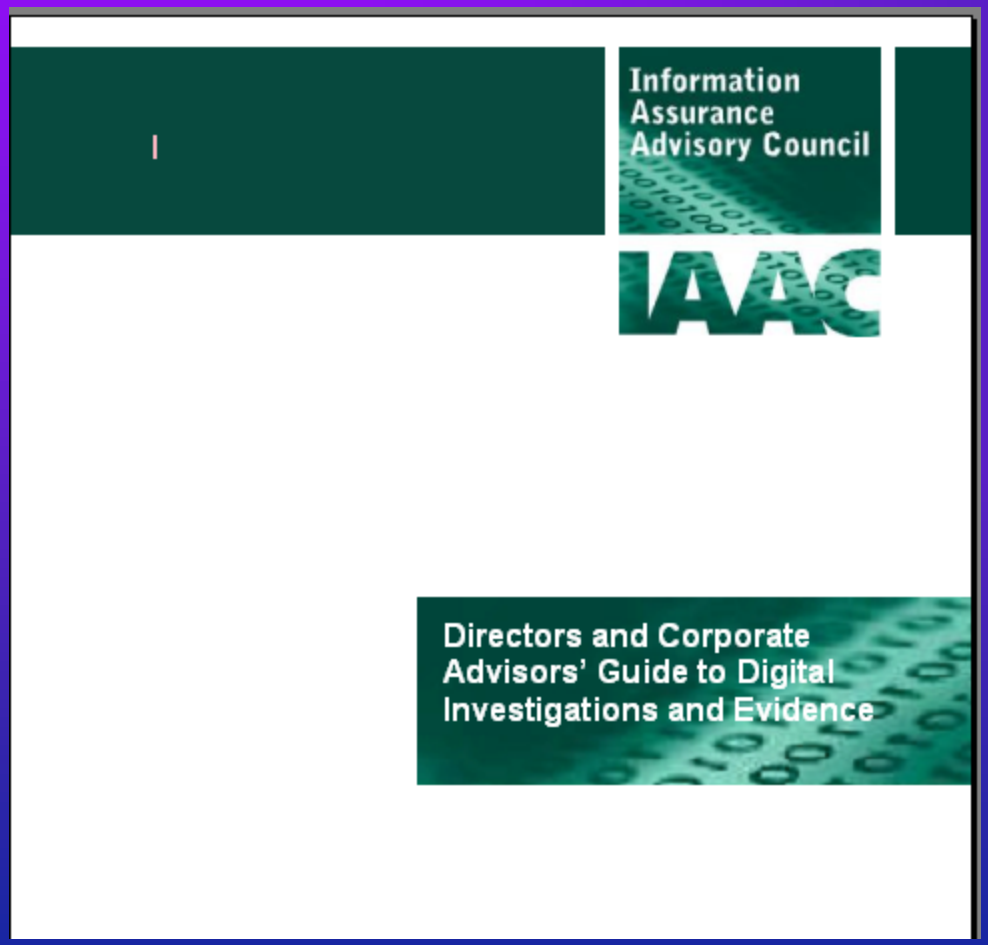
LSE

Forensic Readiness Plan: Additional Requirements

- Legal / Regulatory requirements
- Analysis of back-up plans
  - ➔ Incremental / complete
- Specific Data Retention / Destruction requirements
- Decisions about mode of disclosure
  - ➔ Electronic, print-out, extents, etc
- Witness to explain systems, material produced, testify to reliability and completeness

LSE

Guide to Digital Investigations and Evidence

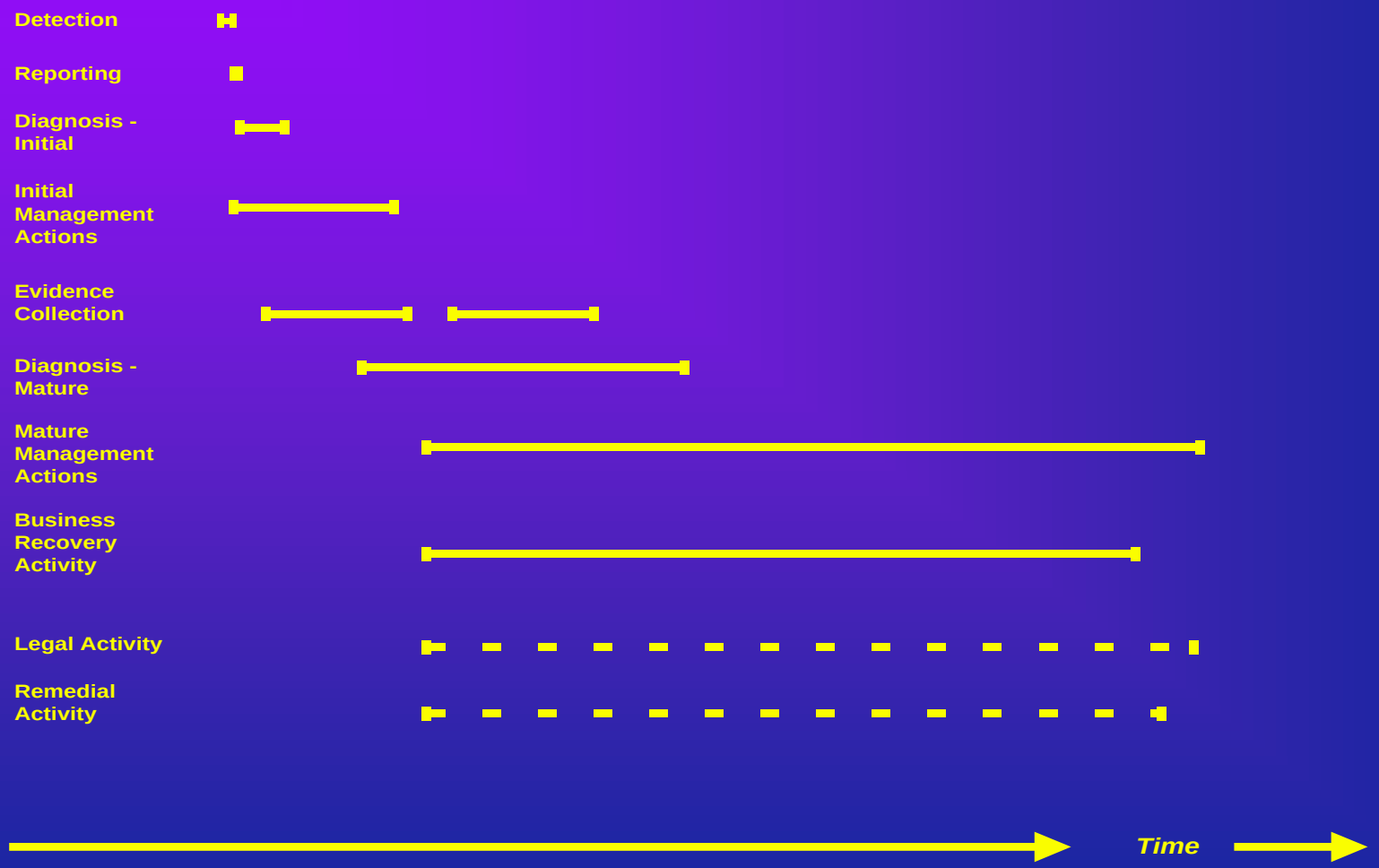


First published 2005; new edition due

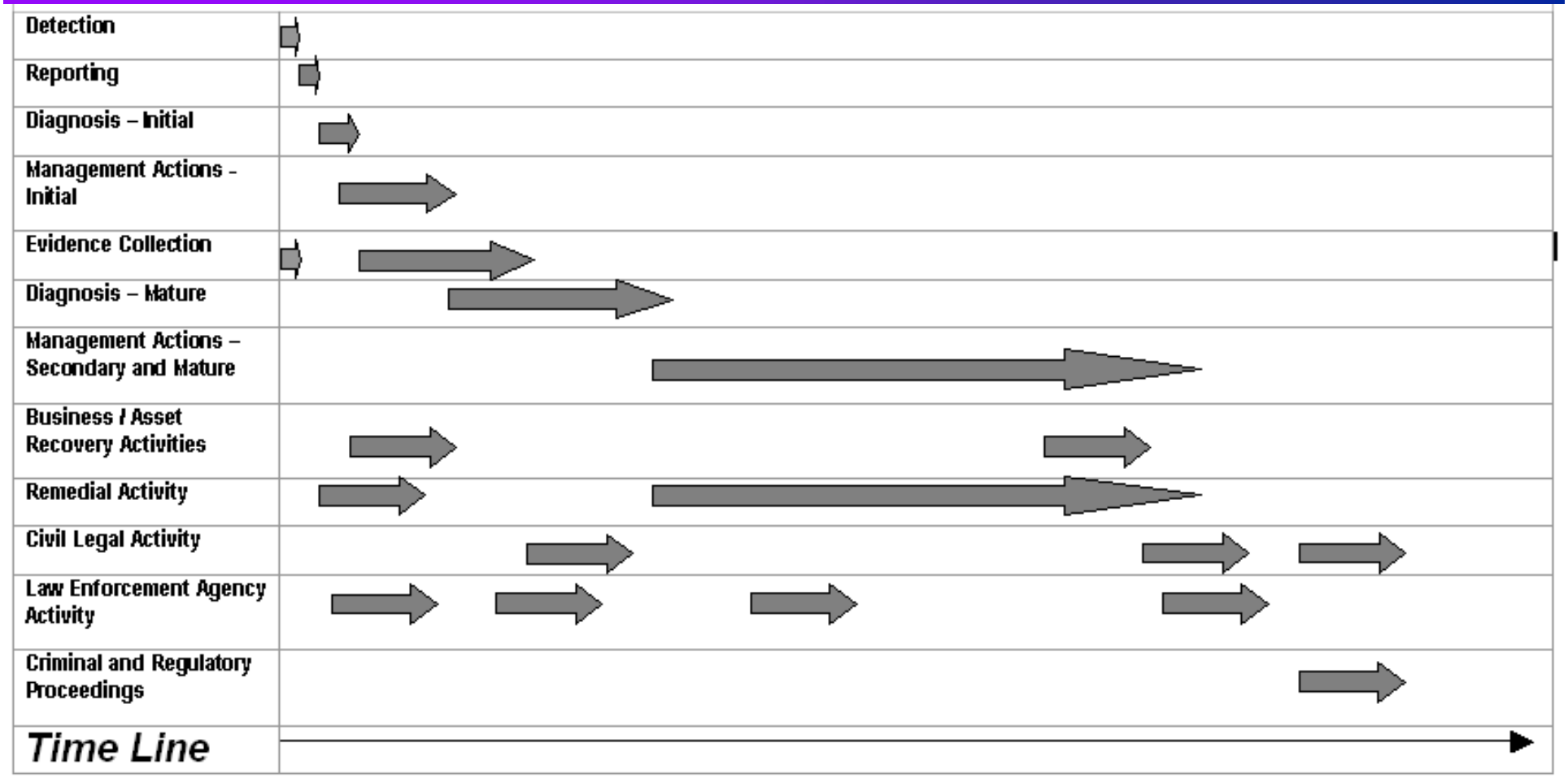
www.iaac.org

LSE

Life-cycle of incidents



Computer Incident Management
Life Cycle



Remedial Activity

- **The final "prize" from having a FRP:**
- **Closing the Loop / Learning the Lessons**

- ***Although the FRP is aimed at legal outcomes, after any event you will have a detailed explanation of what went wrong***
- ***Should lead to precise remedial actions***

LSE

The Malicious Exploitation of Information Systems:

Preventing the Rise of the Insider Threat

6-7 November 2008, UCL

Issues in the Technologies of Digital Investigation

Peter Sommer

London School of Economics, Open University

peter@pmsommer.com

p.m.sommer@lse.ac.uk

LSE