Computer Forensics

ISACA – London

26 June 2003

Ian R Henderson CISA FCA

Managing Director
Advanced Forensics Limited

Telephone: 020 7226 0303
Facsimile: 020 7226 0307
Mobile: 07940 540 399

Email: irh@advancedforensics.com

Ian R Henderson CISA FCA

Ian Henderson is the Managing Director of Advanced Forensics Limited who provide Forensic Accounting and Forensic Computer services to law-firms and a wide range of corporate clients.

Mr Henderson qualified as a Chartered Accountant in 1984. He specialised in investigations and computer audit at an early stage and worked on a number of Government and Department of Trade and Industry investigations. He is also a Certified Information Systems Auditor. Mr Henderson joined the regulatory division of Lloyd's of London in 1986 and was subsequently appointed manager of Lloyd's Investigations Department, where he was responsible for investigating suspected fraud or misconduct world-wide.

In 1996 Mr Henderson was appointed Head of Investigations at the Personal Investment Authority, the U.K.'s leading Financial Services regulator. He was responsible for many high profile investigations covering such diverse areas as pensions mis-selling, money laundering, mortgage fraud and theft of client funds. He was appointed by the Bank of England as a full member of FFIN, the Financial Fraud Information Network and had regular contact with senior officials at the Treasury, the DTI, the SFO and other Financial Services regulators.

In 1998 Mr Henderson moved into the private sector and was appointed Investigations Director of a company specialising in the prevention, detection and investigation of corporate fraud.

In January 2001, Mr Henderson was appointed Special Advisor to the Criminal Cases Review Commission, where he continues to provide professional advice on high profile fraud cases.

A particular professional interest is the recovery, analysis and presentation of digital evidence. Mr Henderson has developed a number of innovative techniques in this area, which are particularly appropriate in cases involving the theft or transfer of intellectual property, the loss of confidential information or when conducting due diligence enquiries.

Contact details

Ian R Henderson CISA FCA
Managing Director
Advanced Forensics
One Aberdeen House
22 – 24 Highbury Grove
London
N5 2EA

Telephone: 020 7226 0303
Facsimile: 020 7226 0307

Mobile: 07940 540 399

Email: irh@advancedforensics.com

Computer Forensics

Advanced Forensics

ISACA – London
26 June 2003

Ian R Henderson CISA FCA

Advanced Forensics Limited

Client Focused Solutions

Background

Advanced Forensics

- ***Advanced Forensics*** **specialise in fraud investigations**
- **One of the most effective (and cost effective) techniques is the use of Computer Forensics**
- **Can be used to clear the innocent, or identify the guilty**

Client Focused Solutions

We live in a digital world

Advanced Forensics

- Traces of what we do are everywhere (Locard's Principle - "Every contact leaves a trace")
- Even if steps are taken to hide the evidence
- Windows OS is particularly good at "covertly" recording the activities of users
- As are many external sources of data e.g. Network Server logs

Client Focused Solutions

A working definition

Advanced Forensics

Computer Forensics is the recovery, analysis and presentation of digital information in support of an investigation – to full legal standards of evidence, if necessary.

Can be used as either INTELLIGENCE or EVIDENCE

Client Focused Solutions

A digital paradox

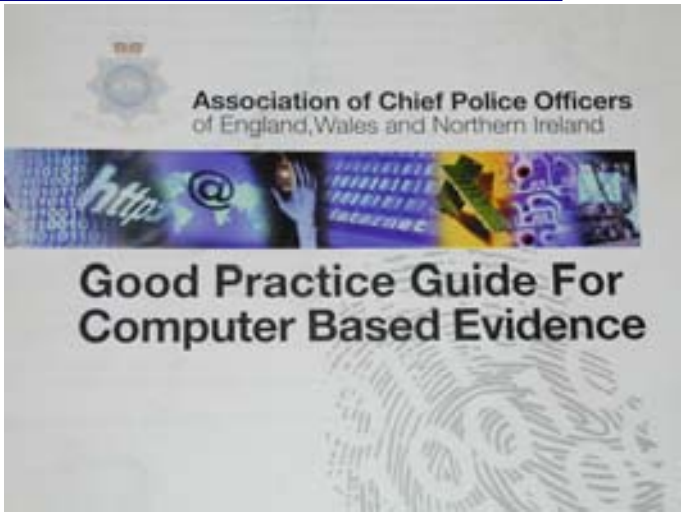
Advanced Forensics

- Digital evidence is extremely fragile, and
- Surprisingly resilient!
- But, it needs very careful handling

Client Focused Solutions

Best Practice Guide

Advanced Forensics



Client Focused Solutions

The main principles

Advanced Forensics

- DO NO HARM – ensure the original evidence is not altered in any way (Especially MAC time stamps)
- Always work from a copy, or a forensic image (Will usually require a DOS based acquisition)
- Establish an evidential AUDIT TRAIL
- REPLICABILTY - ensure any conclusions can be reproduced by the other side

Client Focused Solutions

Standard Operating Procedures

Advanced Forensics

- Consider a covert acquisition
- Remove network & dial-up connections
- DO NOT turn on
- If on, remove all power sources (DO NOT POWER DOWN)
- Only use accredited forensic tools
- DO NOT use a DIY approach

Client Focused Solutions

Why use Computer Forensics?

Advanced Forensics

- As part of the overall "evidence gathering"
- To eliminate the innocent
- To identify the guilty
- Usually part of an initial covert investigation, or
- To establish corroboration

Client Focused Solutions

Advanced Forensics

Some examples where Computer Forensics may have been used:

Client Focused Solutions

Tuesday, October 30, 2001 METRO 9

Barclays 'faced £25m blackmail'

BY DAVID FICKLING

A FORMER Barclays Bank employee threatened to compromise the security of millions of credit and debit cards in a £25million blackmail bid, the Old Bailey heard yesterday.

Graham Browne, 56, headed a security encryption team at one of the bank's computer centres.

The job gave him access to the credit card numbers of all the bank's customers and the encryption codes used on the cards' magnetic strips.

If they became public, the bank's entire security system would have been compromised – forcing it to spend millions of pounds to change its customers' details. Browne was disillusioned with his job and what he saw as the lack of resources Barclays was putting into card security.

In January last year he resigned, thinking his bosses would plead with him to stay. When they accepted his decision, he became resentful.

He began sending letters in which he demanded the bank set up a 'super security team' of 14 experts, including himself, each paid £1.7million.

Otherwise, he warned, he would publicise the bank's lack of security and the codes. The police were called and identified Browne as the culprit.

Browne said the demands he made in a series of four letters to the bank's chief executive were a 'huge joke'.

Sally Bennett-Jenkins, prosecuting, told the jury: 'You may think his allegations of bad security have merit. But that's not the issue. The question is whether he is guilty of blackmail.'

She said if Browne had released any information it would have been 'highly embarrassing' for Barclays.

Browne, of Knutsford, Cheshire, denies blackmail between March and September 2000. The case continues.

Wednesday, October 31, 2001 METRO 9

E-mail scam to hijack company

BY FINIAN DAVERN

AN ACCOUNTANT hatched an e-mail plot with a US businessman to kidnap two rivals and hijack their company, a court heard yesterday.

Peter Rapaport, 55, hired two thugs – one of whom used to guard the Queen – to snatch Philip Mason and Anne-Marie Moore at knifepoint.

They were ordered to sign resignation letters and documents handing ownership of their corporate hospitality business to David Reiss, who masterminded the scheme from his home in Texas.

The victims were handed a list of rules and told their families would suffer if they did not obey them. The couple were then released but, despite the threats, went straight to police.

The next day, officers raided the Affinity Group in Twickenham, Middlesex, and found new 'owner' Reiss already making himself at home.

Middlesex Guildhall Crown Court was told Mr Mason met Reiss more than ten years ago and became friends.

They had an arrangement whereby the American was paid commission for any deals he helped to set up.

But the relationship soured when Reiss demanded £35,000 he had not earned. Mr Mason had no contact with him for months – but Reiss was secretly plotting revenge with help from Rapaport.

Among evidence retrieved from the accountant's home was a string of incriminating e-mails he sent to Reiss.

Rapaport, of Maida Vale, West London, was convicted of conspiracy to rob and falsely imprison and remanded in custody until November 16, with a warning he faces jail.

Reiss, 48, of Dallas, Texas, pleaded guilty at an earlier hearing and has also yet to be sentenced.

THE DAILY TELEGRAPH Saturday, November 10, 2001

Four years for banker who took £1·5m from till

By Richard Savill

A BANK executive who admitted stealing £1·7 million from her firm to fund a life of luxury was jailed for four years yesterday.

Beryl Rowlands, 58, former head of private banking division of Dunbar Bank, a subsidiary of Zurich Financial Services, based in Swindon, Wilts, lavished expensive gifts on friends, her children and grandchildren and treated herself to Rolex watches and exotic holidays.

Swindon Crown Court was told that Rowlands, who took £1·5 million in cash "from the

Beryl Rowlands: luxuries

offered to help the company to identify weaknesses in their system to prevent any possible repetition.'

He added that Rowlands had sought to "bolster her self-esteem" by giving "extravagant gifts" and had found admitting her guilt "cathartic".

She was suspended in May last year when a junior staff member stumbled across the fraud when Rowlands was seen inputting financial data without documentation.

Ian Lovett, chief executive of Dunbar Bank, said yesterday: "This was a serious fraud

What can we expect to see using Computer Forensics?

Advanced Forensics

- Activity involving deception
- True picture of lifestyle / pattern of use
- Internet or server activity
- Copying of documents
- Documents / emails that have been "deleted"

Client Focused Solutions

Computer Forensics is particularly useful in cases involving

Advanced Forensics

- Collusion
- Theft of Intellectual Property or Confidential Information
- Receipt of bribes / backhanders
- Forgery of documents / signatures
- EFT fraud
- Blackmail / intimidation / harassment

Client Focused Solutions

"Hidden" sources of information

Advanced Forensics

- Windows Swap File
- File Slack
- Unallocated File Space
- Windows Registry
- Cookies
- "Recent" Links and Internet History
- Access and other logs
- Microsoft Metadata

Client Focused Solutions

Windows Swap File

Advanced Forensics

- Can be dynamic or static
- Often up to 200 Mbytes in size
- The Windows "dustbin" – particularly relating to recent activity – up to 3 or 4 months old
- Will usually hold images of printed documents

Client Focused Solutions

File Slack

Advanced Forensics

- The space between the end of a physical file and a logical cluster
- Very difficult to hide or destroy
- Can be used to "date" the hidden evidence

Windows File	Original Data to end of Cluster

Client Focused Solutions

2 x 16 KB clusters

Advanced Forensics

12 Kb of "original" data in slack space

Each cluster is between 8 Kb and 32 Kb

Client Focused Solutions

Unallocated File Space

Advanced Forensics

- **"Deleted" documents are not really deleted**
- **The area on the disk is just marked as available for re-use**
- **Specialist tools can recover "deleted" files or examine fragments of those files**

Client Focused Solutions

Windows Registry

Advanced Forensics

- A "gold mine" if used correctly
- Will contain passwords, internet search terms, applications used or installed, email programs (including Hotmail and Yahoo), details of "secure" log-ins
- Protected Data Areas can be decrypted

Client Focused Solutions

Cookies

Advanced Forensics

- Can be used to track and time stamp internet activity
- In combination with URL searches can establish a detailed profile of internet activity

Client Focused Solutions

"Recent" Links and Internet History

Advanced Forensics

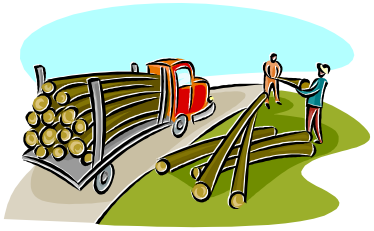
- Shows the most recent activity, including files accessed and copied
- Very useful if floppy disks are being used to "hide" suspicious activity
- Internet History tracks internet usage on a site by site basis – but can be deleted

Client Focused Solutions

Access and Other Logs

Advanced Forensics

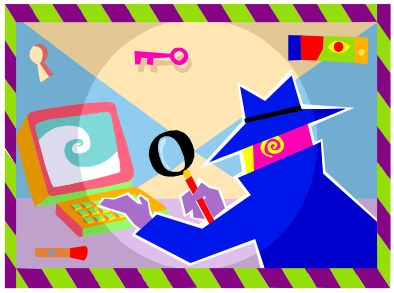
- Not just on the desktop / laptop
- Can be used to "re-create" a detailed record of previous activity, with date and time stamps



Client Focused Solutions

Advanced Forensics

Let's look at theft of IP by 2 ex-employee's



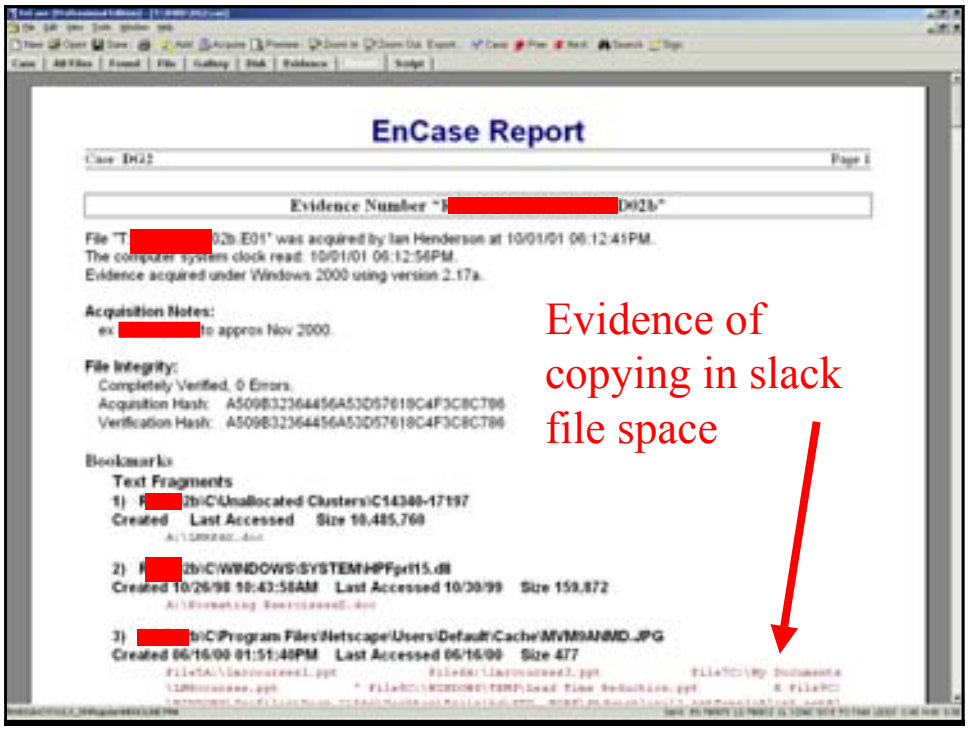
Client Focused Solutions

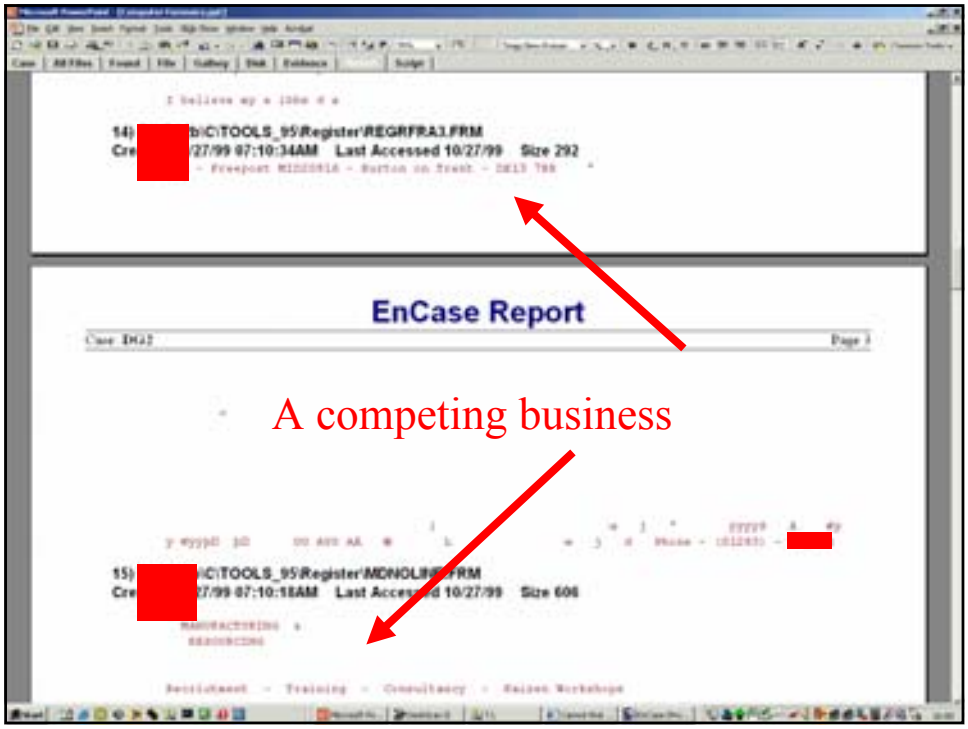
Company had suspicions and launched an investigation

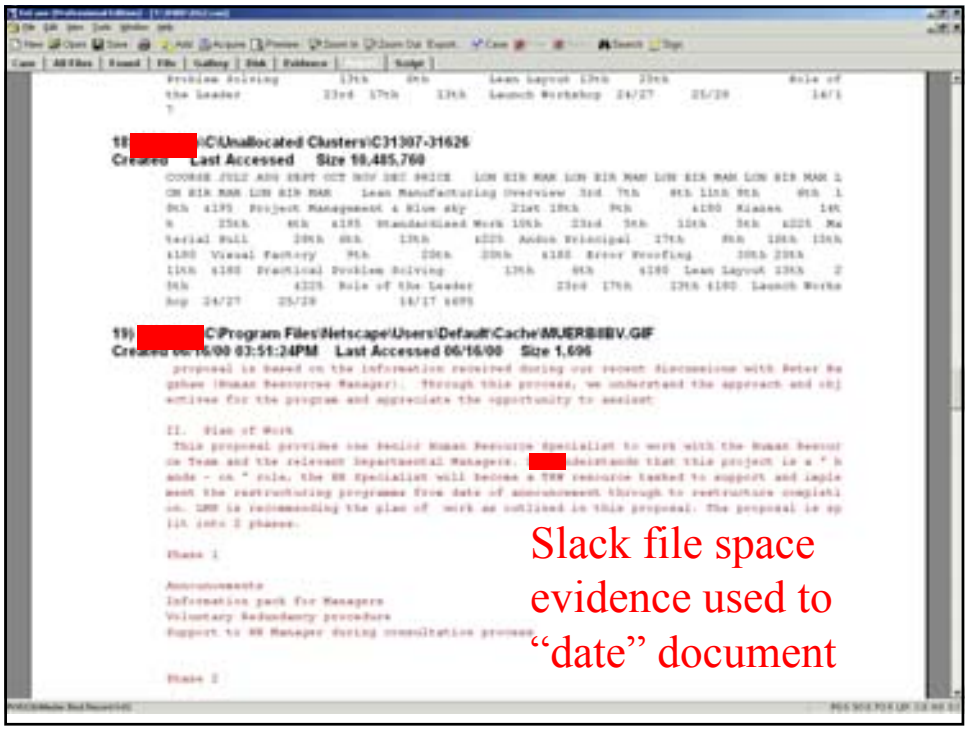
Advanced Forensics

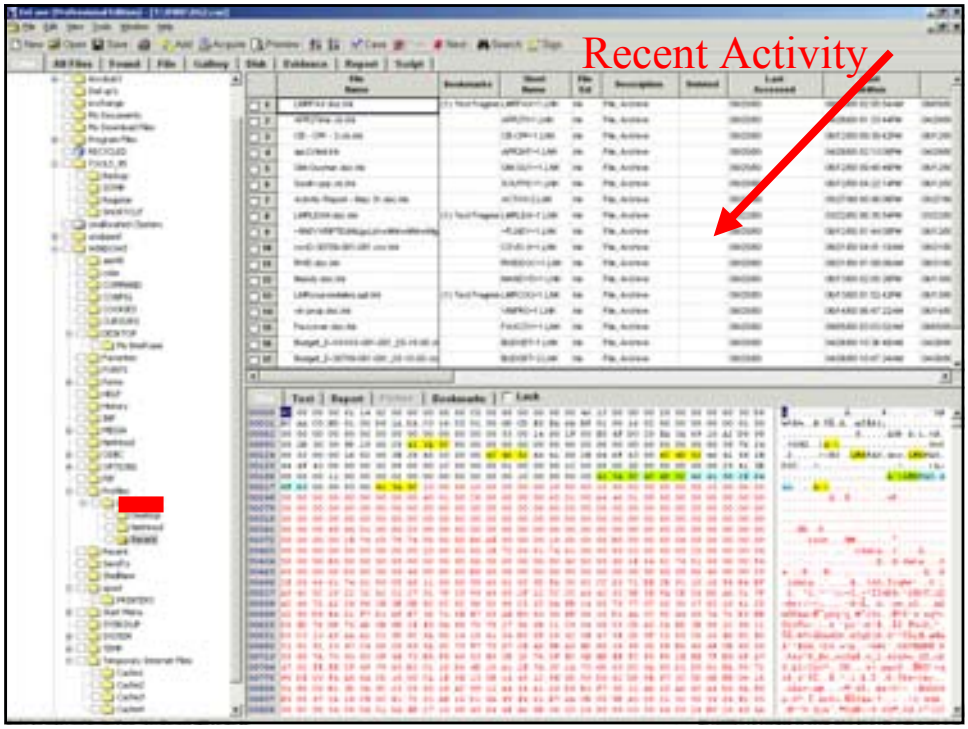
- Review of laptops used 6 months earlier
- Review of e-mails
- Telephone call logs
- Other covert activity

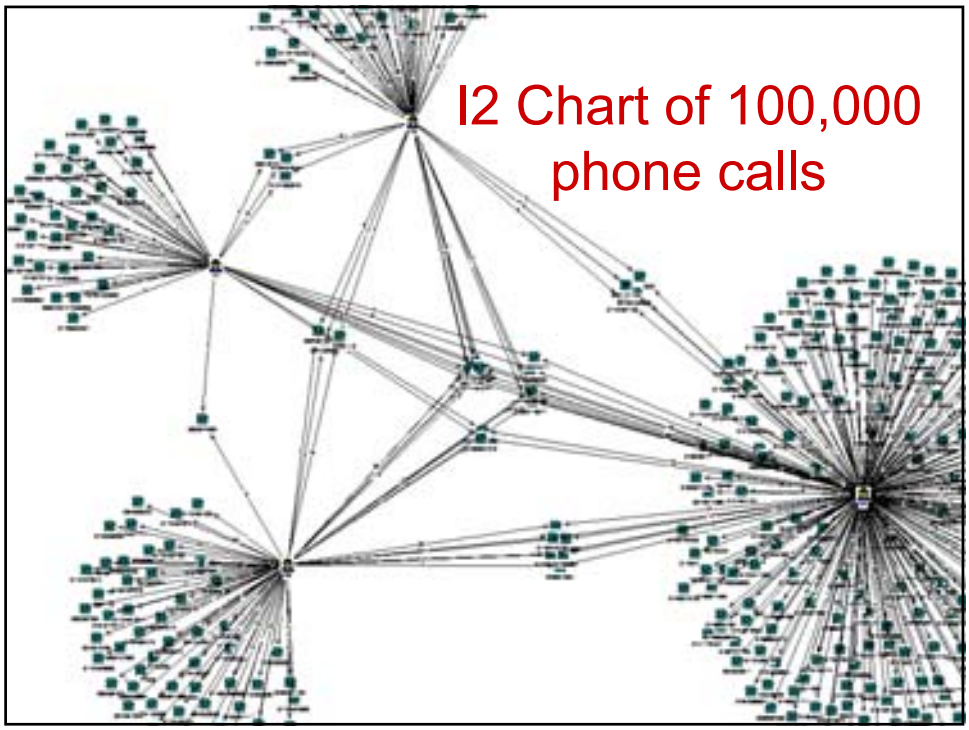
Client Focused Solutions

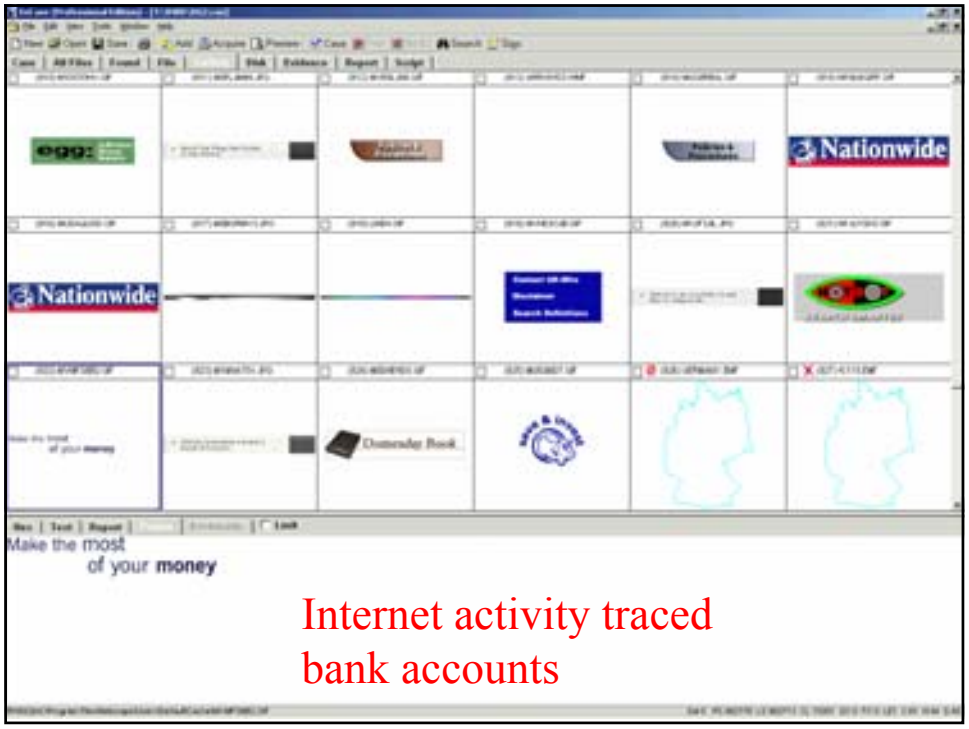












Lets look at an EFT fraud

Advanced Forensics

- Bank reported suspicious funds transfer over the weekend to its customer
- Customer established it was unauthorised
- Implemented Security Incident Response Plan

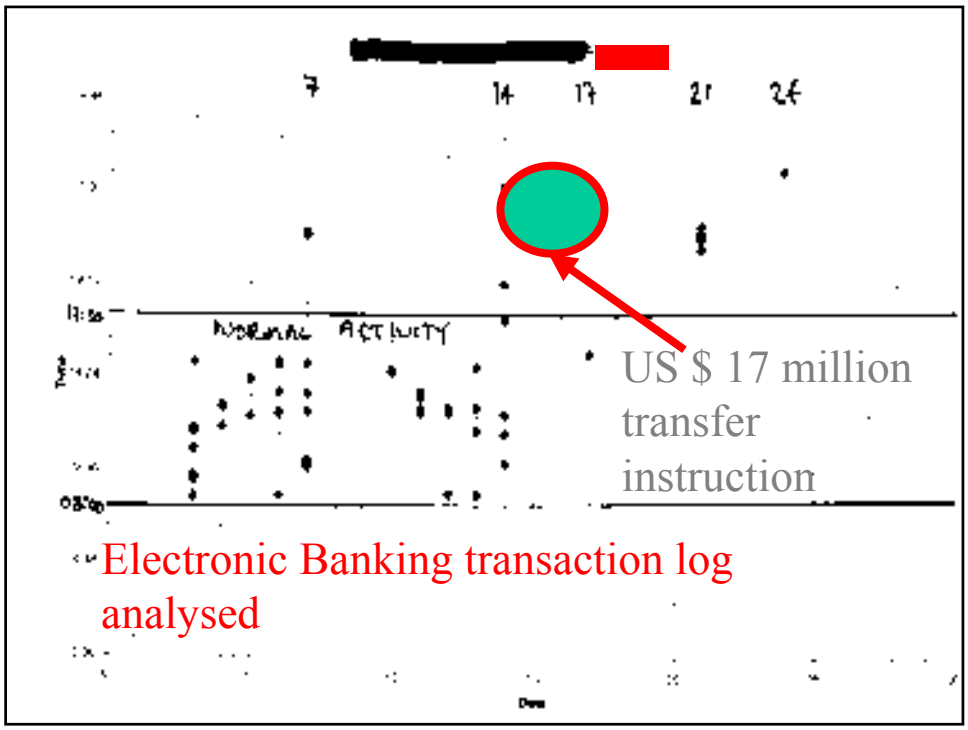
Client Focused Solutions

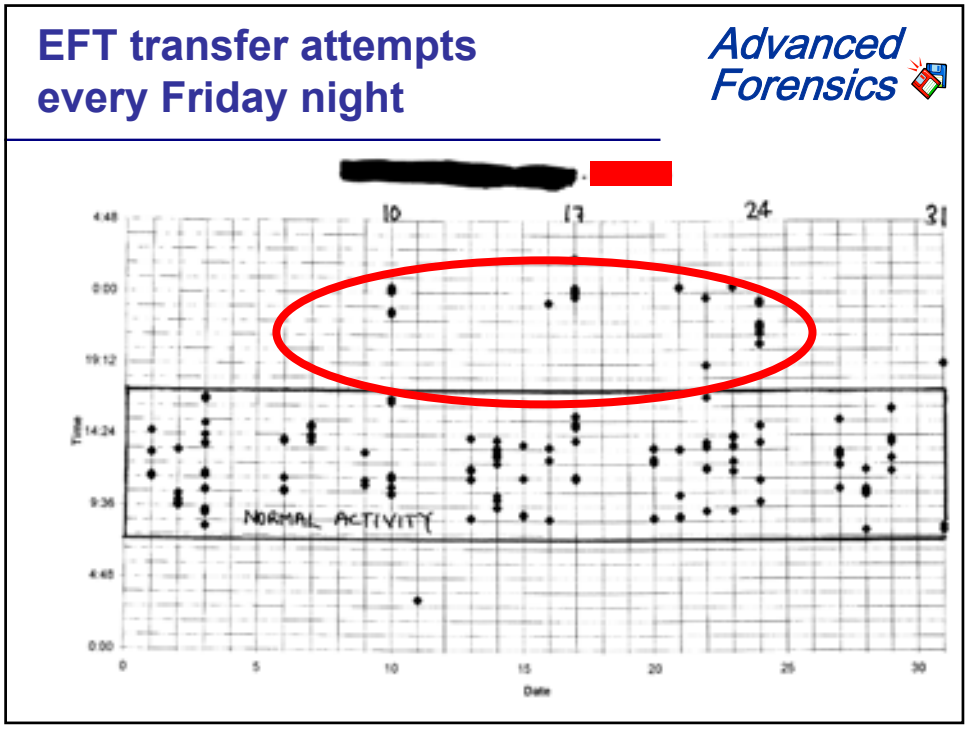
Immediate Action Drills

Advanced Forensics

- Suspend EFT facility
- Trace and freeze funds
- Preserve evidence
- Start hard hitting investigation

Client Focused Solutions





What we found

Advanced Forensics

- Targeted by organised crime
- IT expert infiltrated into company
- Used automated hacking tools – without success
- Trial and error approach – over 6 months
- Audit logs not fully on or monitored

Client Focused Solutions

Eventual outcome

Advanced Forensics

- 100% funds recovery
- Method of attack identified
- Perpetrators arrested and now in Jail
- Lessons learnt and improved security
- All of this in 3 weeks – based 90% on computer forensics

Client Focused Solutions

Investigative techniques

Advanced Forensics

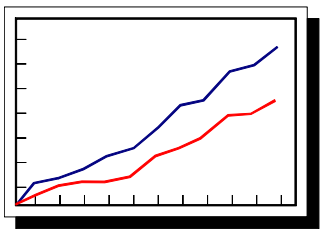
- Computer Forensics
- Digital Analysis
- Data mining

Client Focused Solutions

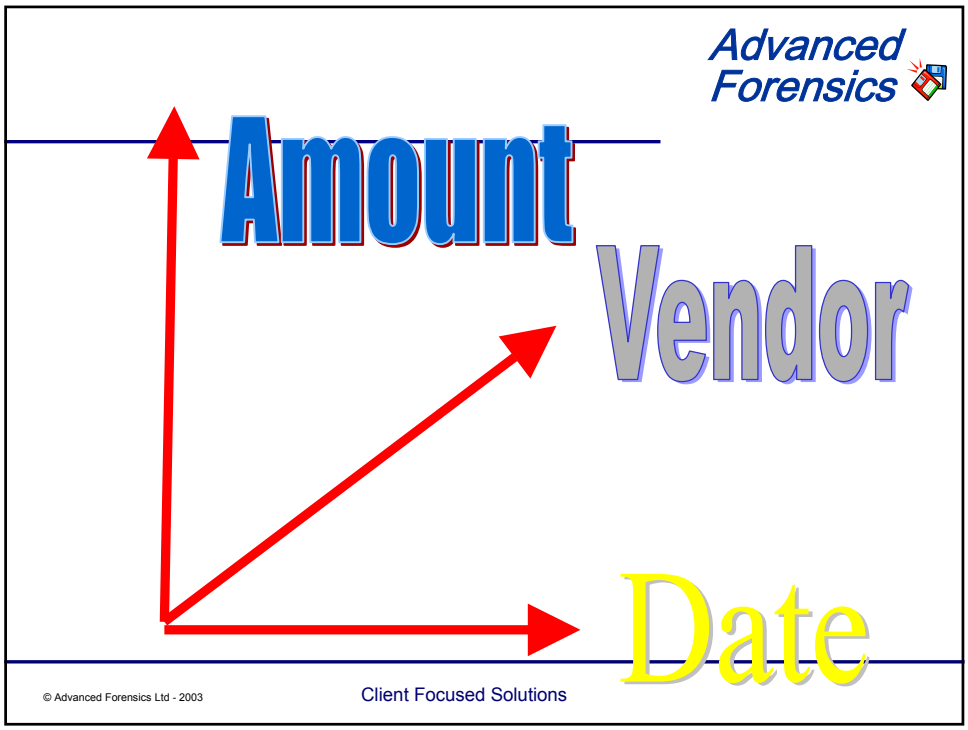
Types of Digital Analysis

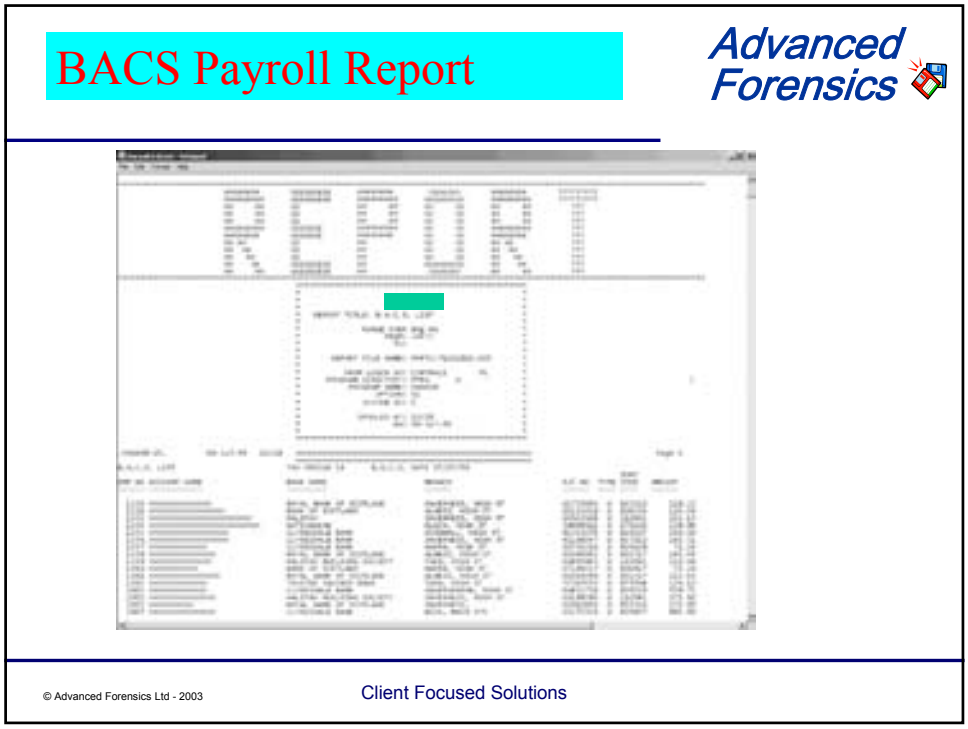
Advanced Forensics

- Relative Size Factor
- Duplicate Payments
- Round Numbers & last 2 digits
- Number Frequency Factor
- Digital Fingerprints



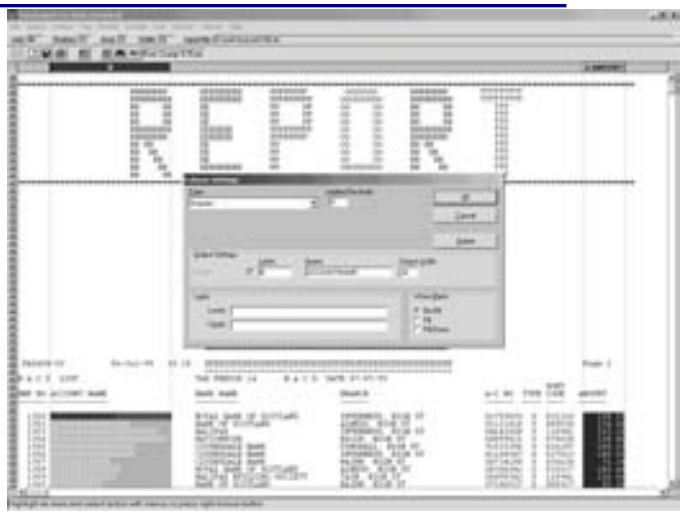
Client Focused Solutions


Advanced Forensics
Amount
Vendor
Date
© Advanced Forensics Ltd - 2003
Client Focused Solutions


BACS Payroll Report
Advanced Forensics
REPORT
© Advanced Forensics Ltd - 2003
Client Focused Solutions

BACS data import using IDEA™

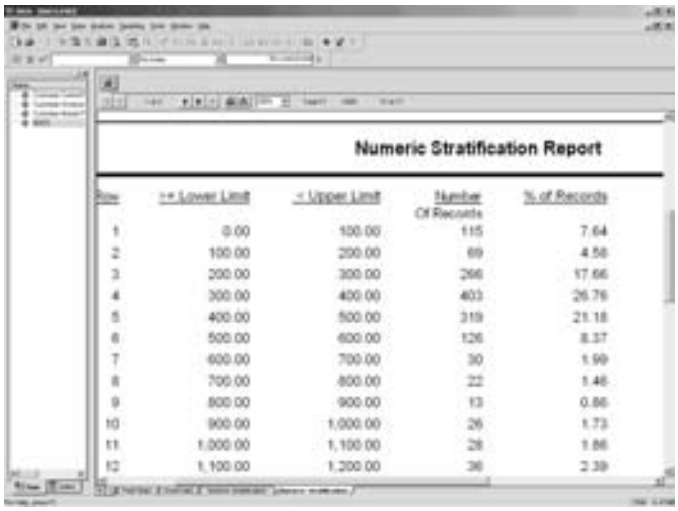
Advanced Forensics



Client Focused Solutions

Initial IDEA™ analysis

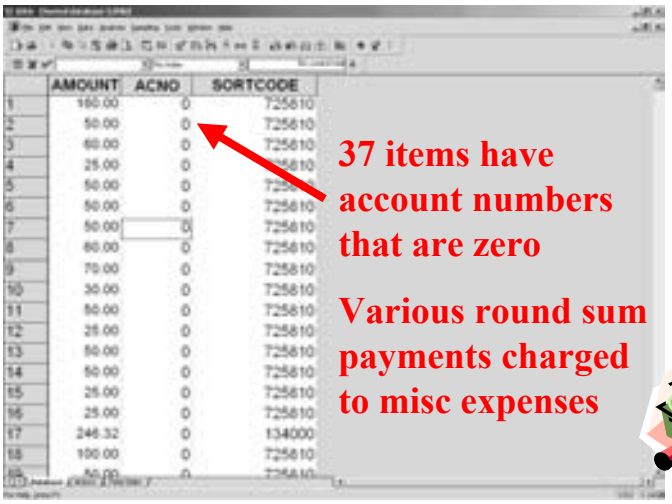
Advanced Forensics



Client Focused Solutions

Key finding

Advanced Forensics



	AMOUNT	ACNO	SORTCODE
1	150.00	0	725810
2	50.00	0	725810
3	60.00	0	725810
4	25.00	0	725810
5	50.00	0	725810
6	50.00	0	725810
7	50.00	0	725810
8	60.00	0	725810
9	70.00	0	725810
10	30.00	0	725810
11	50.00	0	725810
12	25.00	0	725810
13	50.00	0	725810
14	50.00	0	725810
15	25.00	0	725810
16	25.00	0	725810
17	246.32	0	134000
18	100.00	0	725810

37 items have account numbers that are zero

Various round sum payments charged to misc expenses

Client Focused Solutions

What have we found?

Advanced Forensics

- **Deliberate errors introduced into BACS run**
- **BACS run includes expense payments**
- **Error report results in cash payments**
- **Approx £2000 being taken each week and shared between 3 corrupt employees**

Client Focused Solutions

Relative Size Factor

Advanced Forensics

- Within a sub-set e.g. Vendor name
- Take largest item and second largest
- Calculate ratio
- Investigate anomalies
- Good at finding mis-postings and errors as well as fraud

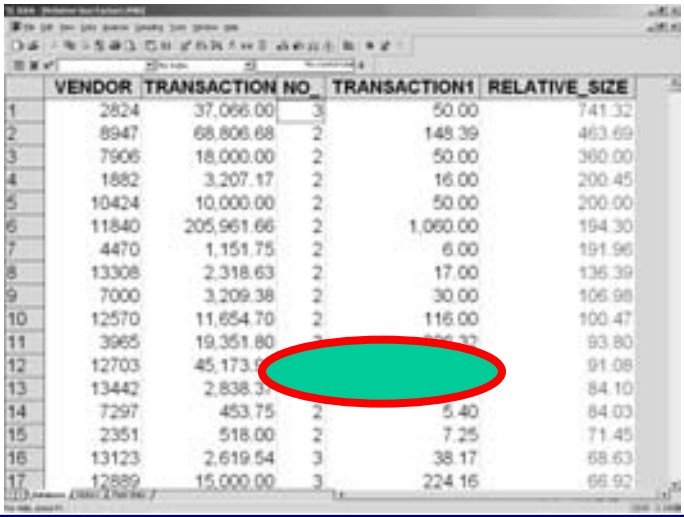
25,000.00

130.75

Client Focused Solutions

RSF analysis

Advanced Forensics



	VENDOR	TRANSACTION NO_	TRANSACTION1	RELATIVE_SIZE
1	2824	37,066.00	50.00	741.32
2	8947	68,806.68	148.39	463.69
3	7906	18,000.00	50.00	360.00
4	1882	3,207.17	16.00	200.45
5	10424	10,000.00	50.00	200.00
6	11840	205,961.66	1,060.00	194.30
7	4470	1,151.75	6.00	191.96
8	13308	2,318.63	17.00	136.39
9	7000	3,209.38	30.00	106.98
10	12570	11,654.70	116.00	100.47
11	3965	19,351.80		93.80
12	12703	45,173.6		91.08
13	13442	2,838.3		84.10
14	7297	453.75	5.40	84.03
15	2351	518.00	7.25	71.45
16	13123	2,619.54	38.17	68.63
17	12889	15,000.00	224.16	66.92

Client Focused Solutions

Cleaning Company

Advanced Forensics

- 10 regular monthly payments of £496
- Then the big one - £45,173.92
- Awarded maintenance contract in suspicious circumstances
- 3 man company
- Collusion and kickbacks

Client Focused Solutions

Link Analysis

Advanced Forensics

- Used to show relationships between, people transactions and events
- Often used in Court to explain complex information
- Leading Software is I2
- Recently used to submit evidence to the House of Commons Treasury Select Committee

Client Focused Solutions

Automated data feed from Companies House

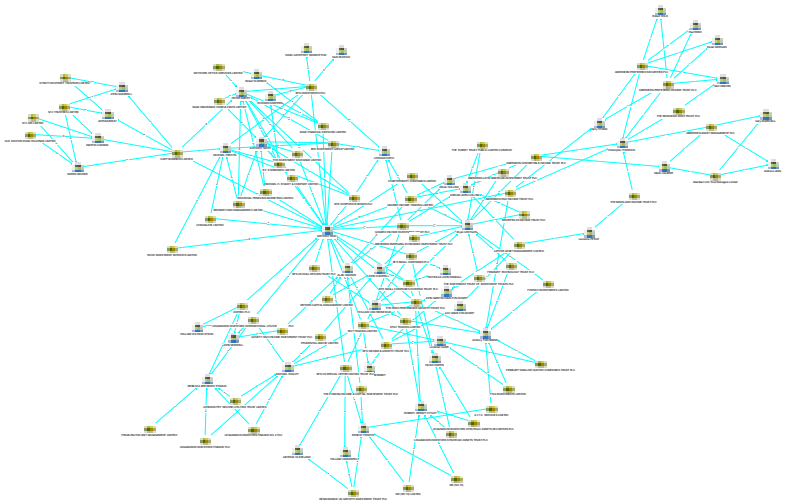
Advanced Forensics

NAME	DIR/S	APPOINTED	STATUS	DATE	POSITION	CO NO.
ANTHONY SMITH	DIR	01/04/1992			CHAIRMAN	1815509
ANTHONY SMITH	DIR	21/12/1992	Dissolved	25/01/2000	COMPANY CHAIRMAN	2650531
ANTHONY SMITH	DIR	15/04/1993			CHAIRMAN	2110493
ANTHONY SMITH	DIR	28/07/1993	Dissolved	15/01/2002	COMPANY CHAIRMAN	2835443
ANTHONY SMITH	DIR	14/12/1993			INVESTMENT CONSULTANT	2761956
ANTHONY SMITH	DIR	01/10/1993	Dissolved	25/01/2000	CHAIRMAN FINANCIAL SERVICES	2628242
ANTHONY SMITH	DIR	16/09/1994	Dissolved	16/07/1996	BROKER FINANCIAL SERVICES PLC	1310243
ANTHONY SMITH	DIR	15/09/1994			DIRECTOR	2900056
ANTHONY SMITH	DIR	30/05/1997			CHAIRMAN	3320911
MARTIN CADMAN	DIR	pre 03/04/1992			COMPANY DIRECTOR	2352583
MARTIN CADMAN	DIR	13/02/1992	Dissolved	03/08/1993	PENSIONS CONSULTANT	2685523
MARTIN CADMAN	DIR	pre 31/12/1991			EMPLOYEE BENEFIT CONSULTANT	1179485
MARTIN CADMAN	DIR	pre 31/10/1991	Dissolved	12/05/1998	COMPANY DIRECTOR	2363663
MARTIN CADMAN	DIR	13/02/1992	Dissolved	22/03/1994	PENSIONS CONSULTANT	2680763
MARTIN CADMAN	DIR	10/07/1996	Dissolved	26/11/1999	PENSIONEER TRUSTEE	3212889
MARTIN CADMAN	DIR	04/09/1996			PENSION CONSULTANT	3198181
MARTIN CADMAN	DIR	21/10/1996			DIRECTOR	3239644
MARTIN CADMAN	DIR	25/01/1999			PENSIONER TRUSTEE	2931449
MARTIN CADMAN	DIR	11/10/1999			DIRECTOR	3856537
MARTIN CADMAN	DIR	15/06/2001			PROFESSIONAL TRUSTEE	4233986
MARTIN CADMAN	SEC	21/10/1996	Resigned:	04/08/2000	DIRECTOR	3239644
MARTIN CADMAN	DIR	pre 20/10/1991	Resigned:	19/08/1993	COMPANY DIRECTOR	2434536
MARTIN CADMAN	DIR	pre 30/04/1992	Resigned:	04/11/1996	COMPANY DIRECTOR	1866180
MARTIN CADMAN	DIR	pre 11/10/1991	Resigned:	04/11/1996	COMPANY DIRECTOR	1957940
ERNEST FENTON	SEC	pre 01/08/1991	Dissolved	11/12/2000		1750126
ERNEST FENTON	DIR	pre 01/08/1991	Dissolved	11/12/2000	COMPANY DIRECTOR	1750126
ERNEST FENTON	DIR	21/01/1992			COMPANY DIRECTOR	2679222
ERNEST FENTON	DIR	pre 15/07/1991	Dissolved	11/04/1995	ACCOUNTANT/DIRECTOR	1810496
ERNEST FENTON	DIR	01/06/1994			DIRECTOR GENERAL ASSOCIATION O	572840
ERNEST FENTON	DIR	03/05/1996			DIRECTOR	3150876
ERNEST FENTON	DIR	15/03/2001			DIRECTOR	4180516
ERNEST FENTON	DIR	pre 30/03/1992	Resigned:	23/09/1992	STOCKBROKER	1816512
ERNEST FENTON	DIR	01/07/1992	Resigned:	23/09/1992	STOCKBROKER	1604046
ERNEST FENTON	DIR	pre 30/03/1992	Resigned:	23/09/1992	STOCKBROKER	1844941
ERNEST FENTON	DIR	pre 30/03/1992	Resigned:	23/09/1992	STOCKBROKER	1958866
ERNEST FENTON	DIR	15/12/1995	Resigned:	31/12/1997	DIRECTOR	3138669
ERNEST FENTON	DIR	23/09/1994	Resigned:	21/01/1998	DIRECTOR	2883334
ERNEST FENTON	DIR	21/01/1998	Resigned:	28/09/1998	COMPANY DIRECTOR	3401611
ERNEST FENTON	DIR	01/04/1993	Resigned:	08/12/1997	DIRECTOR	1910539
GEORGE CLEVELAND	DIR	15/03/2001			INVESTMENT MANAGER	4180516
GEORGE CLEVELAND	DIR	24/04/1996			INVESTMENT MANAGER	3150876
JOHN MATATKO	DIR	pre 12/10/1992			UNIVERSITY LECTURER	2548099
JOHN MATATKO	DIR	pre 01/02/1993			UNIVERSITY LECTURER	2579300
JOHN MATATKO	DIR	15/09/1994			DIRECTOR	2900056
JOHN MATATKO	DIR	pre 10/11/1991			LECTURER	1815509

Client Focused Solutions

Automated link analysis

Advanced Forensics



Client Focused Solutions


ANALYSIS: SPLIT CAP TRUSTS

Revealed: the 'magic circle'

Tangled web at heart of £100m class action

Business Comment

Savers' voices must be heard

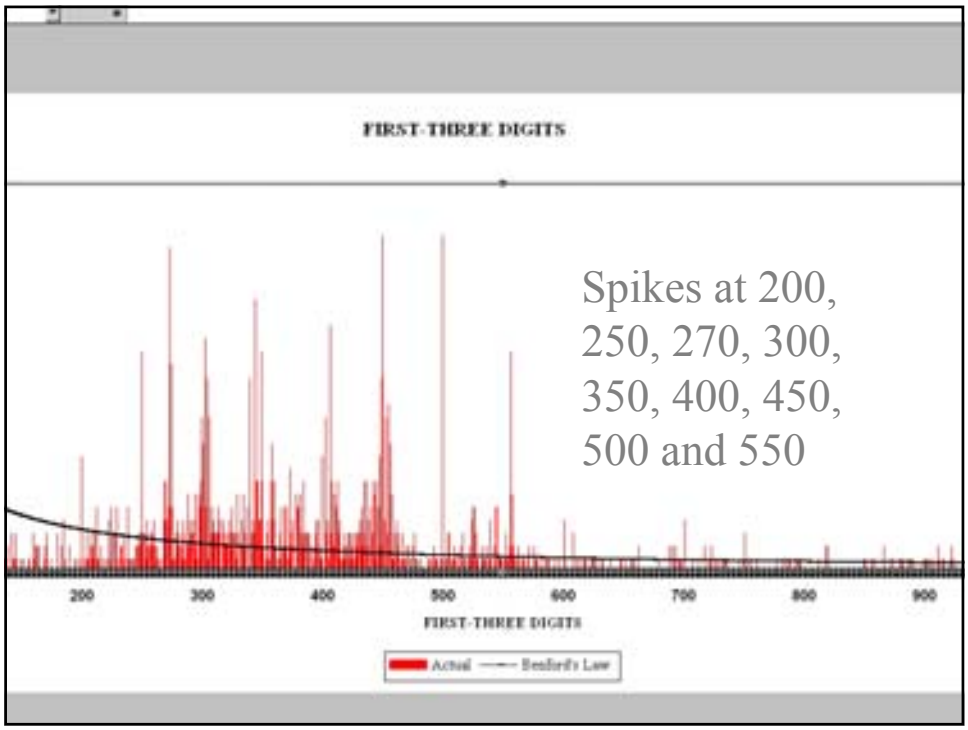
Digital Fingerprints

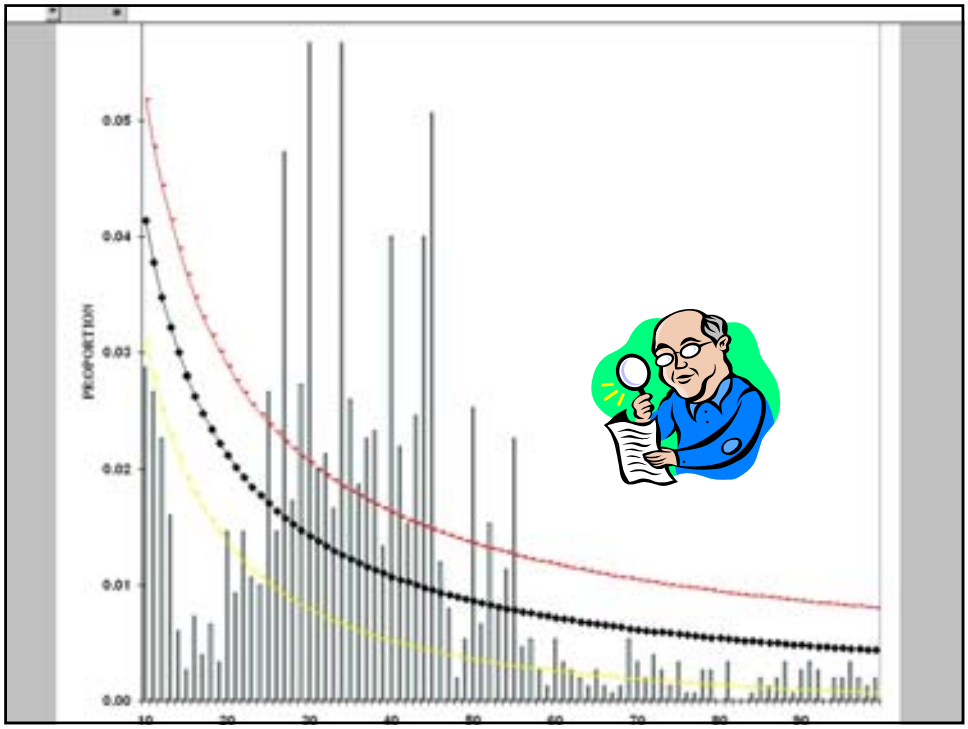
Advanced Forensics

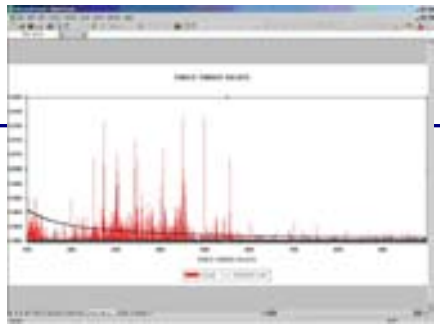
- Good for continuous audits
- Only just being developed
- Use DATAS™ to profile the data at a specific date
- Then compare it with the profile from a different date

© Advanced Forensics Ltd - 2003

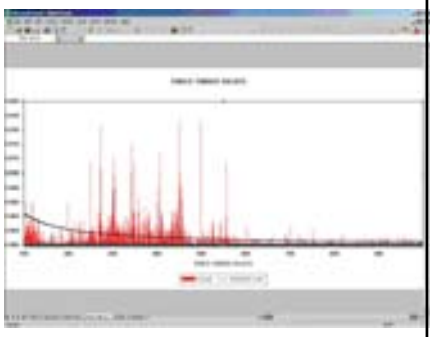
Client Focused Solutions


FIRST-THREE DIGITS
Spikes at 200, 250, 270, 300, 350, 400, 450, 500 and 550
200
300
400
500
600
700
800
900
FIRST-THREE DIGITS
Actual
Benford's Law


0.05
0.04
0.03
0.02
0.01
0.00



Advanced Forensics



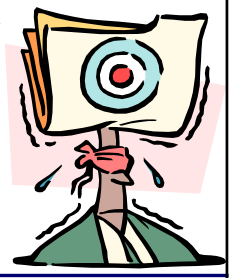
Has the profile changed?

Client Focused Solutions

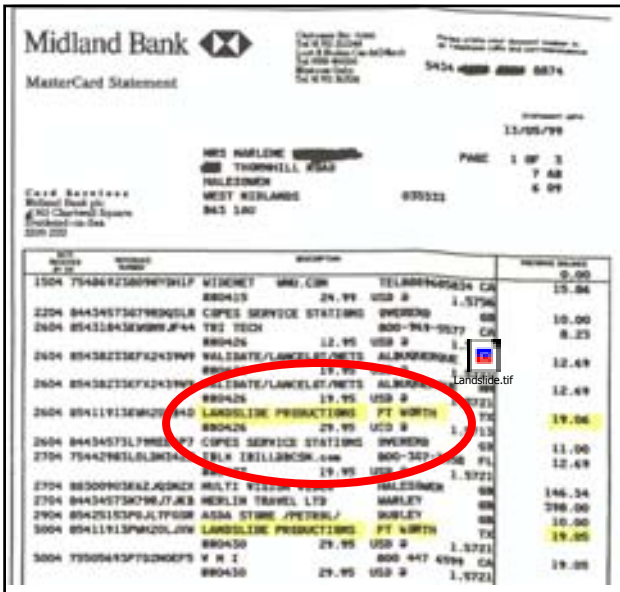
Operation Ore

Advanced Forensics

- The hunt for the UK's paedophiles
- It is a CRIMINAL OFFENCE to make, possess or distribute an indecent photograph of a child
- Includes pseudo photographs and videos
- Making, includes clicking on a URL link
- Most photographs are distributed via newsgroups or peer to peer software
- The corporate environment is at risk



Client Focused Solutions



Advanced Forensics

Prosecutions on this alone! – no photographs found

Client Focused Solutions

Peer to Peer Software

Advanced Forensics

- E.g. KaZaA
- Not stopped by many firewalls
- Not prevented by site/content filtering
- Uses Port 1214 (as default)
- File transfer by HTTP GET
- Make sure you filter headers with "X-KaZaA-"

Client Focused Solutions

Police Investigations

Advanced Forensics

- Thorough and aggressive, but
- Limited resources
- May prosecute on a single photograph (or caution) with 5 YEARS ON SEX OFFENDERS REGISTER
- Will be a career limiting incident
- Will use advanced forensic tools – including DBB fragments, HASH matching
- No Corporate prosecutions – so far …….

Client Focused Solutions

Bank Employee Fraud - April 2002

Advanced Forensics

Client Focused Solutions

Bank fraud – April 2002

Advanced Forensics

- Senior IT analyst "Mr fix-it"
- Had access to live data
- Lots of "red flags"
- Approx US$ 7 million stolen over 3 years
- Essential to use an IT based approach due to complexity of the fraud

Client Focused Solutions

Investigation priorities

Advanced Forensics

- Exposure verification – How big is the fraud?
- Asset identification & recovery – Get our money back
- Criminal prosecution – Punish the criminal
- Improvements and control – Stop it happening again
- Business continuity and integrity – keep trading

Client Focused Solutions

Problem areas

Advanced Forensics

- 3 separate systems
- Data dictionaries not up to date
- Very high volumes of data
- 20 Gb plus in system logs EACH DAY
- 400 staff with system access – 20 “super users”
- Liaison with National Clearing Bank
- Limited processing resources
- Much trial and error testing needed
- Safeboot protected laptop

Client Focused Solutions

Forensic evidence acquired locally

Advanced Forensics

- Forensic software and instructions e-mailed to the IT Security team in Prague
- Forensic Images saved to temporary hard drive and distributed on CD’s
- Safeboot successfully dealt with
- Analysis of Forensic Images conducted in London & Prague

Client Focused Solutions

The basic tools …..

Advanced Forensics

Client Focused Solutions

What did we expect to find?

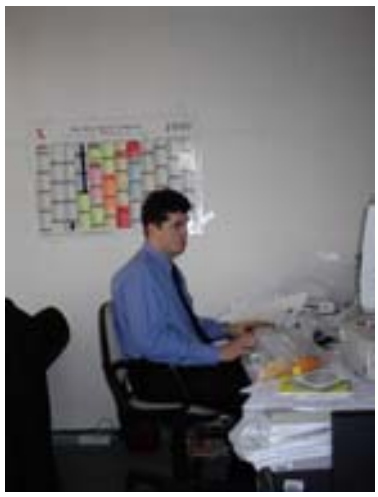
Advanced Forensics

- deleted or encrypted files
- internet activity
- lifestyle information
- traces of assets acquired
- direct evidence of the fraud

Client Focused Solutions

The fraudster!

Advanced Forensics



Client Focused Solutions

On-line banking statement

Advanced Forensics

Client Focused Solutions

Assets purchased with the bank's money

Advanced Forensics

Client Focused Solutions

Diamonds from Amsterdam

Advanced Forensics

Client Focused Solutions

www.privateislandsonline.com

Advanced Forensics

Client Focused Solutions

Holidays and possible acquisitions

Advanced Forensics

Client Focused Solutions

His much loved Harley Davidson

Advanced Forensics

Client Focused Solutions

Property purchases

Advanced Forensics

Client Focused Solutions

Detailed maps and photographs of assets

Advanced Forensics

Client Focused Solutions

Some of the techniques used

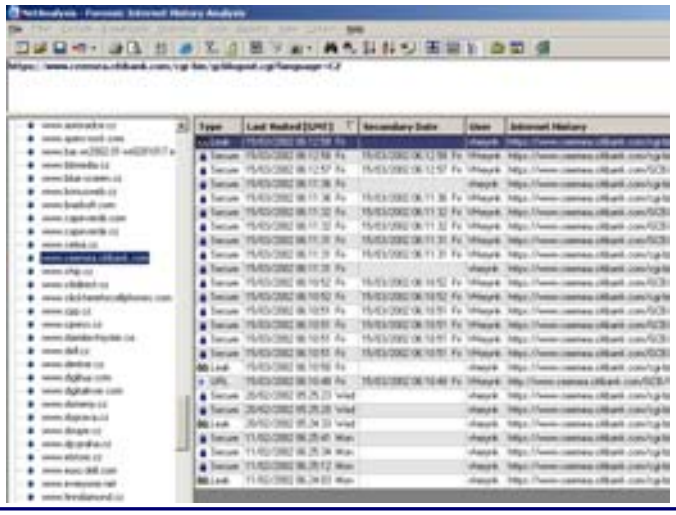
Advanced Forensics

- Analysis of Internet History Logs
- Recovery of deleted documents
- Analysis of financial data
- Analysis of System and other logs
- Data mining and text indexing

Client Focused Solutions

Analysis of internet history

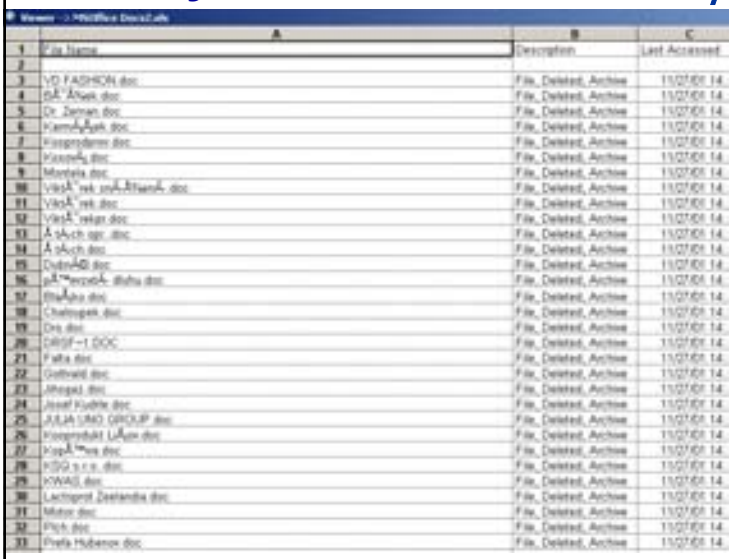
Advanced Forensics



Client Focused Solutions

Securely deleted documents

Advanced Forensics

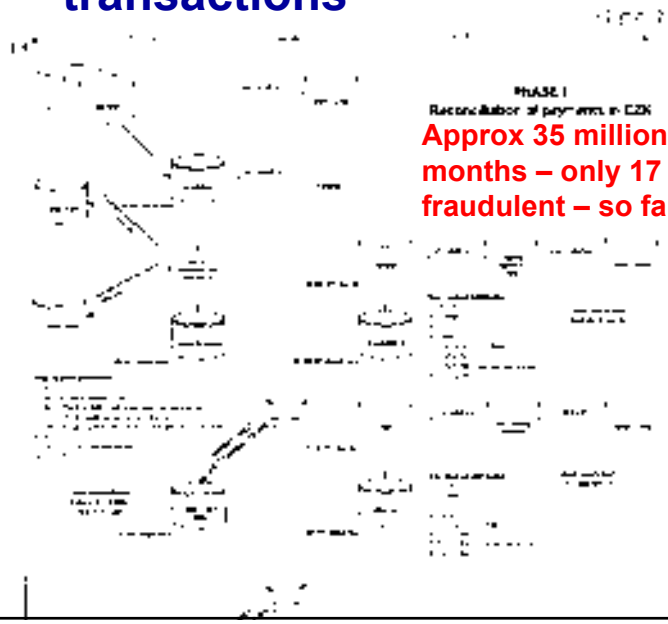


	A	B	C
1	File Name	Description	Last Accessed
2			
3	VD FASHION.doc	File, Deleted, Archive	11/27/01 14
4	BÂ´Ãšek.doc	File, Deleted, Archive	11/27/01 14
5	Dr. Zeman.doc	File, Deleted, Archive	11/27/01 14
6	KarmÃ¼nek.doc	File, Deleted, Archive	11/27/01 14
7	Kissingdamm.doc	File, Deleted, Archive	11/27/01 14
8	KissovÃ¡.doc	File, Deleted, Archive	11/27/01 14
9	Montaža.doc	File, Deleted, Archive	11/27/01 14
10	VlkÃ´rek snÃ-Ãšenka.doc	File, Deleted, Archive	11/27/01 14
11	VlkÃ´rek.doc	File, Deleted, Archive	11/27/01 14
12	VlkÃ´rekgr.doc	File, Deleted, Archive	11/27/01 14
13	Ã sAch gr .doc	File, Deleted, Archive	11/27/01 14
14	Ã sAch.doc	File, Deleted, Archive	11/27/01 14
15	DubnÃ©.doc	File, Deleted, Archive	11/27/01 14
16	pÃ™vodnÃ- dluhy.doc	File, Deleted, Archive	11/27/01 14
17	Øhaáka.doc	File, Deleted, Archive	11/27/01 14
18	Chaloupek.doc	File, Deleted, Archive	11/27/01 14
19	Dns.doc	File, Deleted, Archive	11/27/01 14
20	DRSF~1.DOC	File, Deleted, Archive	11/27/01 14
21	Falta.doc	File, Deleted, Archive	11/27/01 14
22	Gothard.doc	File, Deleted, Archive	11/27/01 14
23	Jihogal.doc	File, Deleted, Archive	11/27/01 14
24	Josef Kudrle.doc	File, Deleted, Archive	11/27/01 14
25	JULIA UNO GROUP.doc	File, Deleted, Archive	11/27/01 14
26	Kosprodukt LÃ¡zeň.doc	File, Deleted, Archive	11/27/01 14
27	KospÃ™va.doc	File, Deleted, Archive	11/27/01 14
28	KSG s.r.o..doc	File, Deleted, Archive	11/27/01 14
29	KWAS.doc	File, Deleted, Archive	11/27/01 14
30	Lachgrot Zeelandia.doc	File, Deleted, Archive	11/27/01 14
31	Motor.doc	File, Deleted, Archive	11/27/01 14
32	Pich.doc	File, Deleted, Archive	11/27/01 14
33	Prefa Hubenov.doc	File, Deleted, Archive	11/27/01 14

Client Focused Solutions

Analysis of ALL banking transactions

Advanced Forensics



Approx 35 million transactions in 3 months – only 17 identified as fraudulent – so far!

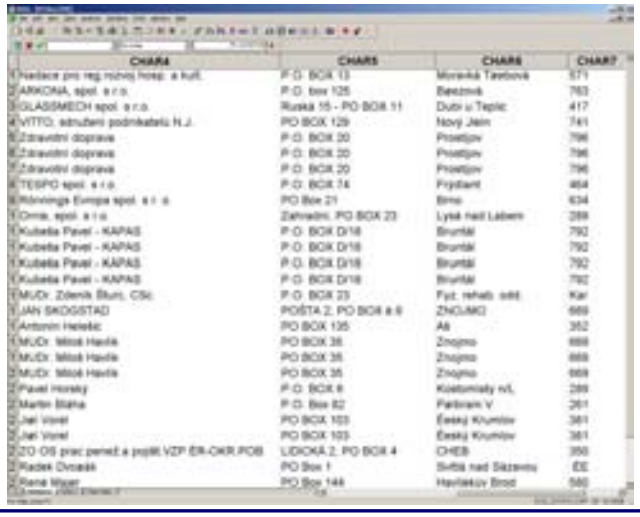
All data files indexed and searchable

Advanced Forensics

Client Focused Solutions

AS 400 data reviewed for leads

Advanced Forensics



Client Focused Solutions

Final result – April 2003

Advanced Forensics


MLADÁ FRONTA

DNES

ČTVRTEK 24. DUBNA 2003

Programátor dostal 7 let

Počítačový expert vyvedl z banky dvě stovky milionů

- 7 years in prison

- 95% of all funds recovered (US$ 6.5 million)

- improved systems

Client Focused Solutions

Other potential problem areas – to consider

Advanced Forensics

- Large hard disks
- Large amounts of data (including email)
- Encryption
- Size of audit logs
- Training for IT Audit (and IT Security)

Client Focused Solutions

Lessons for the future

Advanced Forensics

- Test data dictionaries
- Develop in-house data mining skills – possibly internal audit – look for the "killer" test
- Just one person can make the difference
- Aim for a 5:1 recovery rate
- Always use Computer Forensics

Client Focused Solutions

Key points …..

Advanced Forensics

- It's people, not systems, that commit fraud
  - Watch for Red Flags
- Don't underestimate the power of Forensic Evidence
  - Incorporate into contingency plans NOW
- Don't just design controls for compliant people
  - Crooks will ignore them
- Do involve the fraud specialists
  - at the design stage & when a fraud is suspected

Client Focused Solutions

Action Points

Advanced Forensics

- Actively consider how to use Computer Forensics
- Make use of the evidence you didn't know that you had!
- Set up contingency plans to capture forensic evidence

Client Focused Solutions

Where to go for further help

Advanced Forensics

Ian Henderson

irh@advancedforensics.com

Office: 020 7226 0303

Mobile: 07940 540 399

Client Focused Solutions