Information Technology Audit & Forensic Techniques

CMA Amit Kumar

Amit Kumar & Co.

(Cost Accountants)

A perfect blend of Tax, Audit & Advisory services

Information Technology Audit & Forensic Techniques

B-73/B, Sainik Nagar, Nawada, New Delhi-110059. T- 91 9999803612 & 011-2533 0030
E-mail :: akcadvisors@gmail.com

Presentation Focus

- Importance of IT Forensic Techniques to Organizations
- Importance of IT Forensic Techniques to Auditors
- Audit Goals of Forensic Investigation
- Digital Crime Scene Investigation
- Illustration of Forensic Tools
- A Forensic Protocol

Forensic Computing Defined

Forensic Computing is the process of identifying, preserving, analyzing, and presenting digital evidence in a manner that is legally acceptable in a court of law

Our interest is in …

- Identifying and preserving evidence,
- "post-mortem" system analysis to determine extent and nature of attack, and
- the forensic framework

Importance of IT Forensic Techniques to Organizations

Corporate Fraud Losses in 2004

- Cost companies an average loss of assets over $ 1.7 million
- A 50% increase over 2003
- Over one third of these frauds were discovered by accident, making "chance" the most common fraud detection tool.
  - PriceWaterhouseCoopers, Global Economic Crime Survey 2005

The New Corporate Environment

- Sarbanes-Oxley 2002
- COSO and COBIT
- ISO 9000 and ISO 17799
- Gramm-Leach-Bliley Act
- US Foreign Corrupt Practices Act
- Companies Act 2013

…all of these have altered the corporate environment and made forensic techniques a necessity!

Intellectual Property Losses

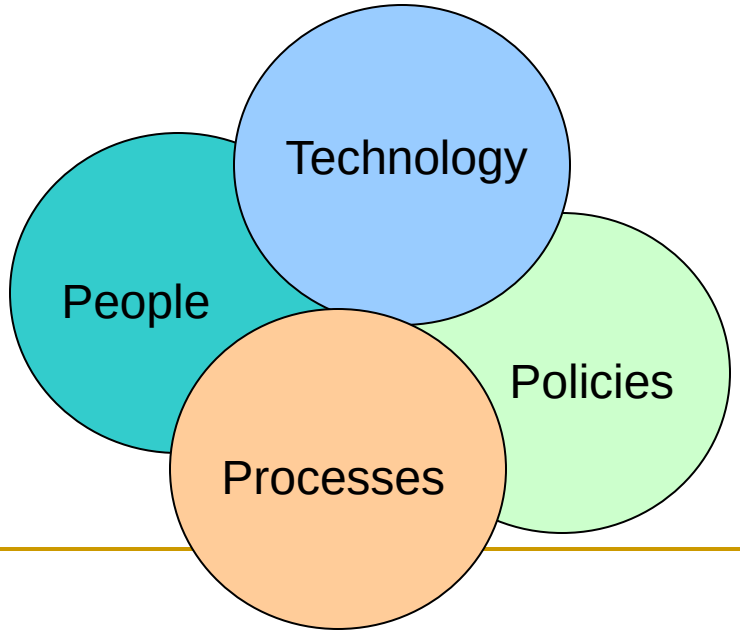
- Rapid increase in theft of IP – 323% over five year period 1999-2004
- 75% of estimated annual losses were to an employee, supplier or contractor
- Digital IP is more susceptible to theft
- Employees may not view it as theft

Network Fraud

- Companies now highly reliant on networks
- Networks increasingly vulnerable to attacks
- Viruses, Trojans, Rootkits can add backdoors
- Social Engineering including Phishing and Pharming
- Confidential and proprietary information can be compromised
- Can create a corporate liability

Security Challenges

- Technology expanding and becoming more sophisticated
- Processes evolving and integrating with technologies
- People under trained
- Policies outdated
- Organizations at risk



Importance of IT Forensic Techniques to Auditors

- Majority of fraud is uncovered by chance
- Auditors often do not look for fraud
- Prosecution requires evidence
- Value of IT assets growing

Treadway Commission Study …

- Undetected fraud was a factor in one-half of the 450 lawsuits against independent auditors.

Auditor's Knowledge, Skills, Abilities

- Accounting
- Auditing
- IT (weak)

Needed …

- Increased IT knowledge
- Fraud and forensic accounting knowledge
- Forensic investigative and analytical skills and abilities

Knowledge, Skills, Abilities: Needs

Auditor's need KSAs to …

- Build a digital audit trail
- Collect "usable" courtroom electronic evidence
- Trace an unauthorized system user
- Recommend or review security policies
- Understand computer fraud techniques
- Analyze and valuate incurred losses

KSA Needs (cont.)

- Understand information collected from various computer logs
- Be familiar with the Internet, web servers, firewalls, attack methodology, security procedures & penetration testing
- Understand organizational and legal protocols for incident handling
- Establish relationships with IT, risk management, security, law enforcement

Rules of Evidence

- Complete
- Authentic
- Admissible
- Reliable
- Believable

Requirements for Evidence

Computer logs …

- Must not be modifiable
- Must be complete
- Appropriate retention rules

Problems with Digital Investigation

- Timing essential – electronic evidence volatile
- Auditor may violate rules of evidence
- NEVER work directly on the evidence
- Skills needed to recover deleted data or encrypted data

Extract, process, interpret

- Work on the imaged data or “safe copy”
- Data extracted may be in binary form
- Process data to convert it to understandable form
  - Reverse-engineer to extract disk partition information, file systems, directories, files, etc
  - Software available for this purpose
- Interpret the data – search for key words, phrases, etc.

Technology

- Magnetic disks contain data after deletion
- Overwritten data may still be salvaged
- Memory still contains data after switch-off
- Swap files and temporary files store data
- Most OS's perform extensive logging (so do network routers)

Order of Volatility

- Preserve most volatile evidence first
  - Registers, caches, peripheral memory
  - Memory (kernel, physical)
  - Network state
  - Running processes
  - Disk
  - Floppies, backup media
  - CD-ROMs, printouts

Digital Forensic Investigation

A process that uses science and technology to examine digital objects and that develops and tests theories, which can be entered into a court of law, to answer questions about events that occurred.

IT Forensic Techniques are used to capture and analyze electronic data and develop theories.

Illustration of Forensic Tools

Forensic Software Tools are used for …

- Data imaging
- Data recovery
- Data integrity
- Data extraction
- Forensic Analysis
- Monitoring

Data Imaging

- Reduces internal investigation
- Automated analysis saves time
- Supports electronic records audit
- Creates logical evidence files — eliminating need to capture entire hard drives

- **Previews computers over the network to determine whether relevant evidence exists:**
  - Unallocated/allocated space
  - Deleted files
  - File slack
  - Volume slack
  - File system attributes
  - CD ROMs/DVDs
  - Mounted FireWire and USB devices
  - Mounted encrypted volumes
  - Mounted thumb drives

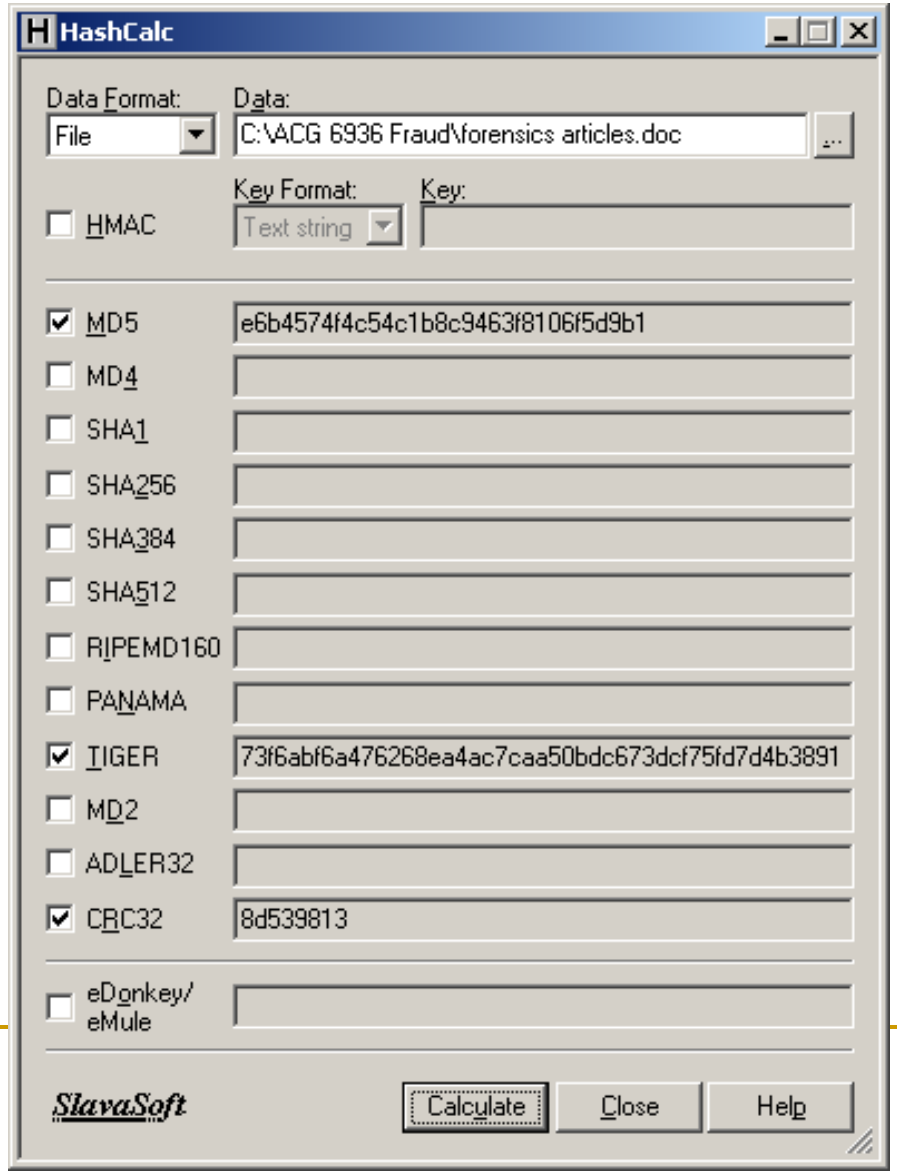
MD5

- Message Digest – a hashing algorithm used to generate a checksum
- Available online as freeware
- Any changes to file will change the checksum

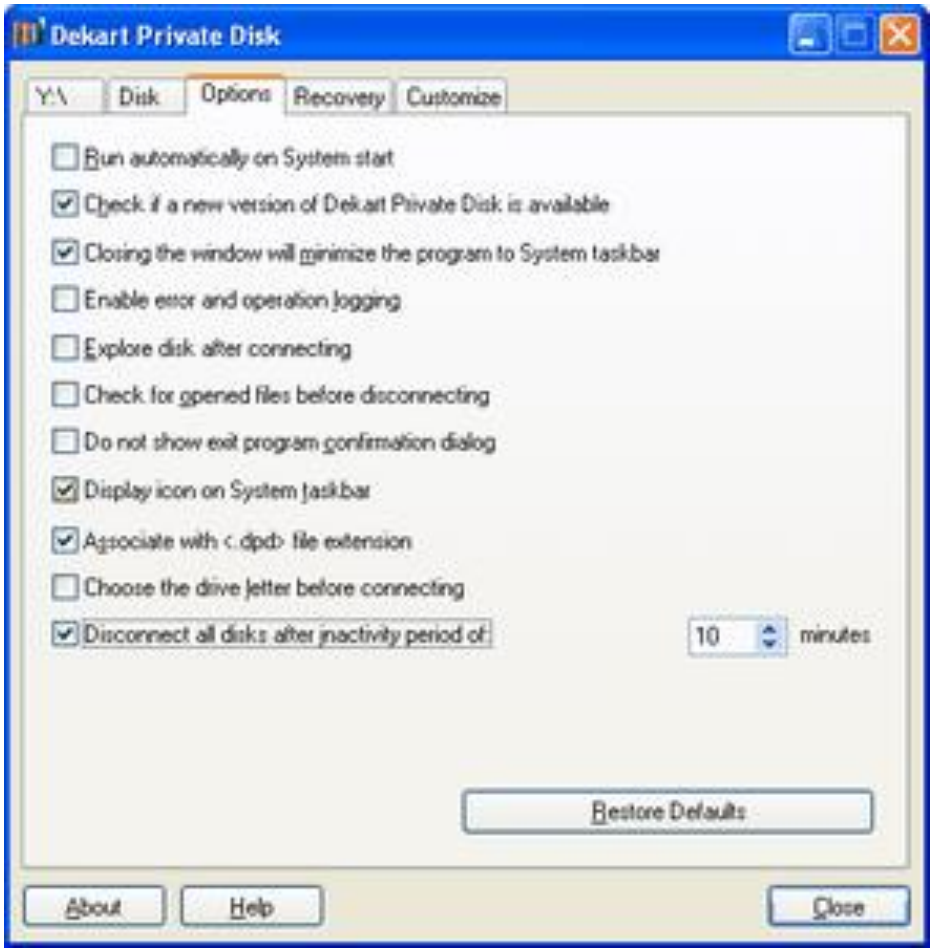
Use:

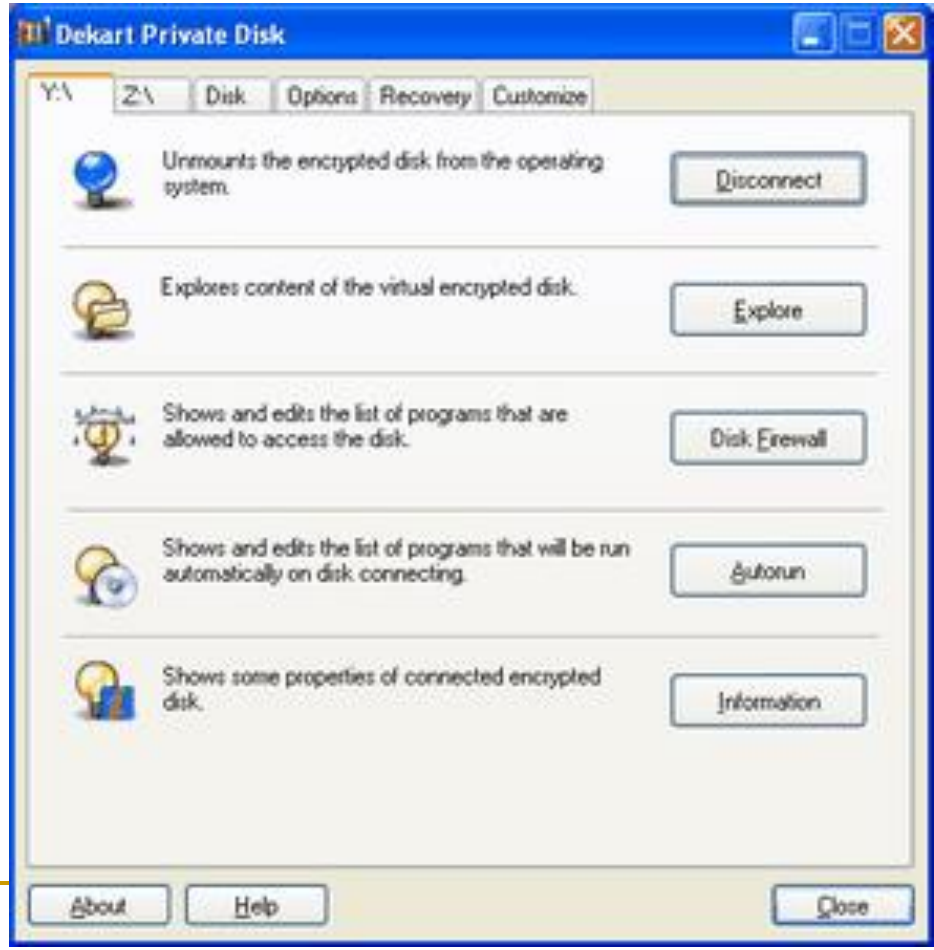
- Generate MD5 of system or critical files regularly
- Keep checksums in a secure place to compare against later if integrity is questioned

MD5 Using HashCalc



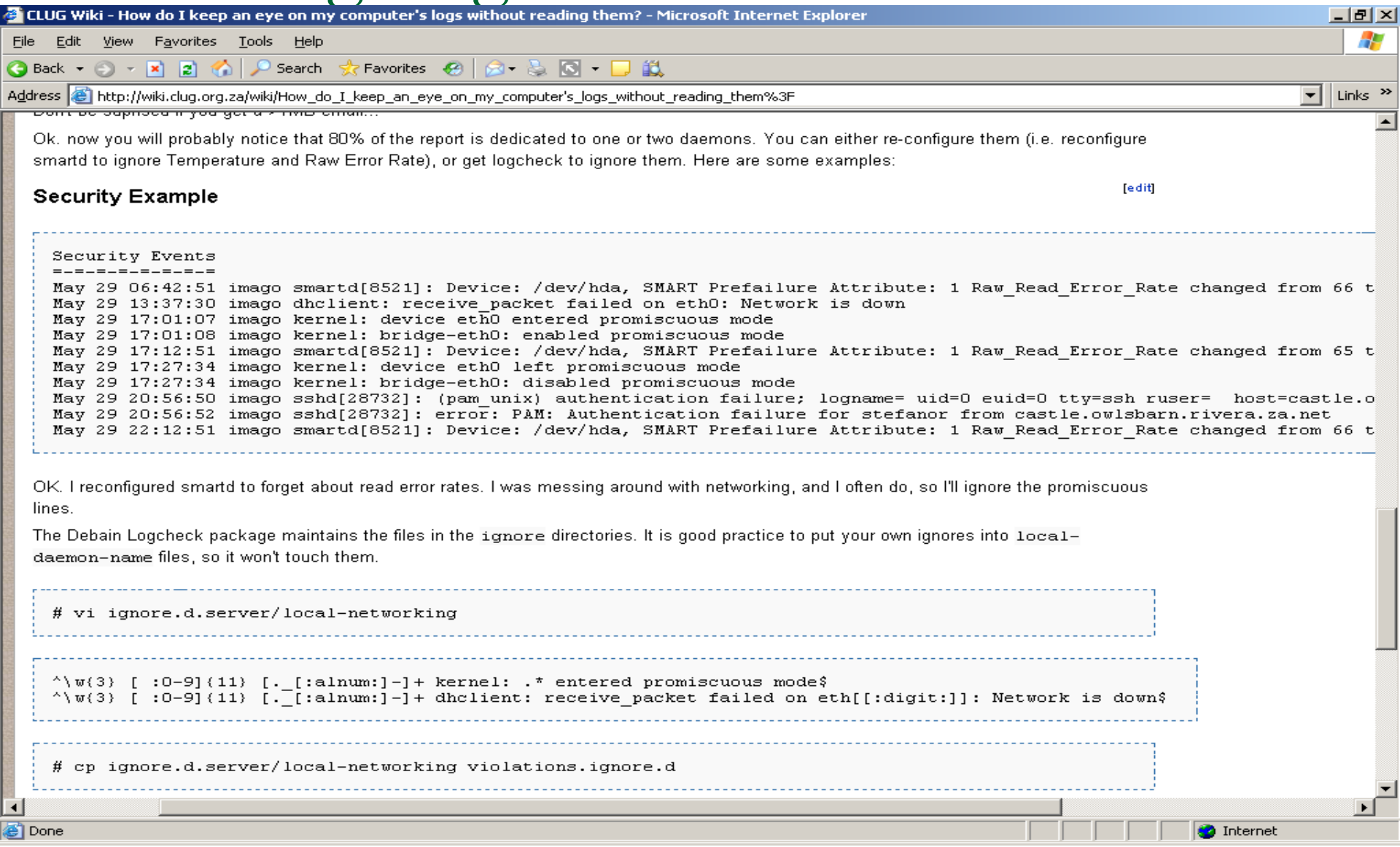
Private Disk



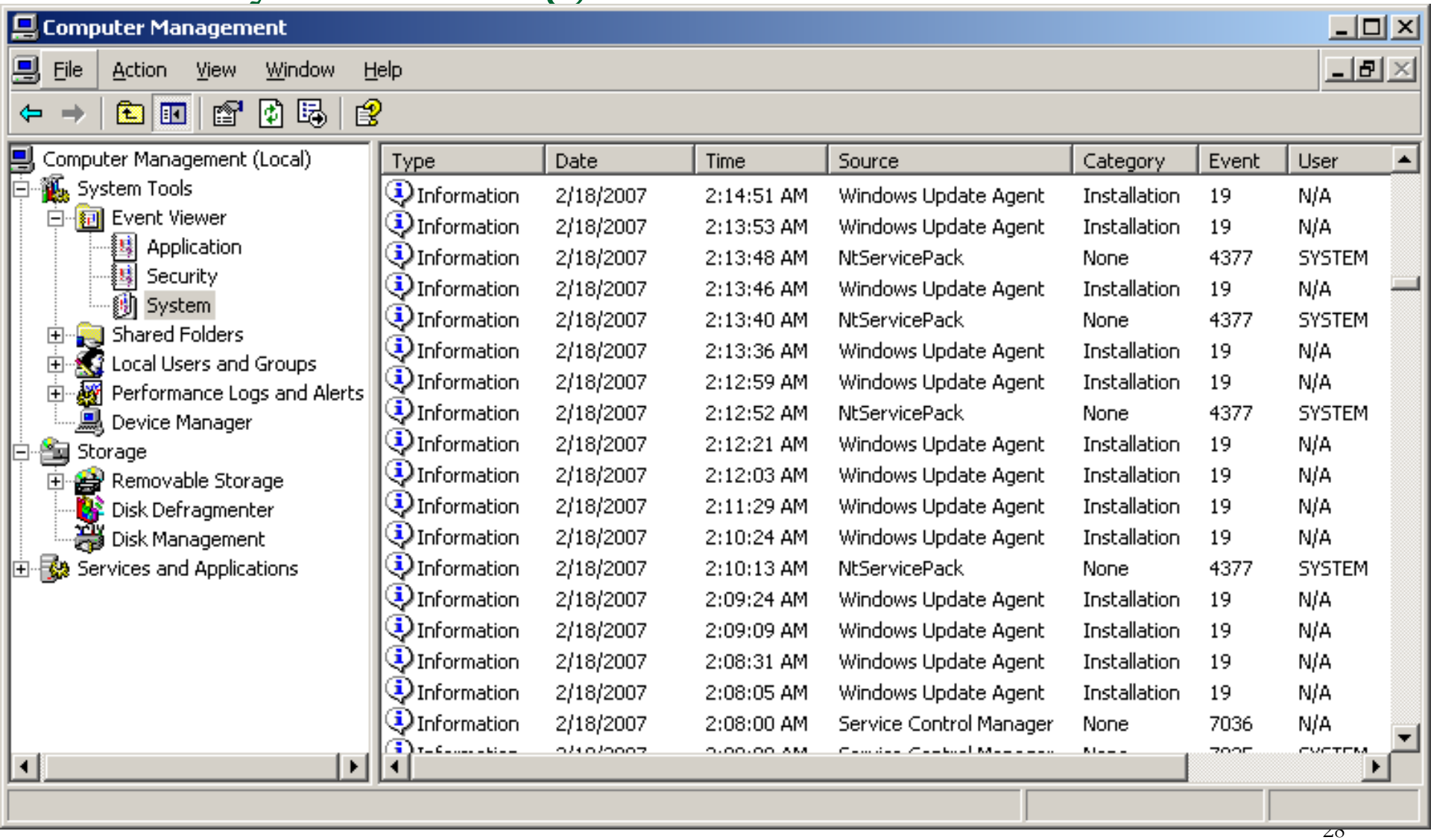


Data Monitoring

Tracking Log Files



PC System Log



Type	Date	Time	Source	Category	Event	User
Information	2/18/2007	2:14:51 AM	Windows Update Agent	Installation	19	N/A
Information	2/18/2007	2:13:53 AM	Windows Update Agent	Installation	19	N/A
Information	2/18/2007	2:13:48 AM	NtServicePack	None	4377	SYSTEM
Information	2/18/2007	2:13:46 AM	Windows Update Agent	Installation	19	N/A
Information	2/18/2007	2:13:40 AM	NtServicePack	None	4377	SYSTEM
Information	2/18/2007	2:13:36 AM	Windows Update Agent	Installation	19	N/A
Information	2/18/2007	2:12:59 AM	Windows Update Agent	Installation	19	N/A
Information	2/18/2007	2:12:52 AM	NtServicePack	None	4377	SYSTEM
Information	2/18/2007	2:12:21 AM	Windows Update Agent	Installation	19	N/A
Information	2/18/2007	2:12:03 AM	Windows Update Agent	Installation	19	N/A
Information	2/18/2007	2:11:29 AM	Windows Update Agent	Installation	19	N/A
Information	2/18/2007	2:10:24 AM	Windows Update Agent	Installation	19	N/A
Information	2/18/2007	2:10:13 AM	NtServicePack	None	4377	SYSTEM
Information	2/18/2007	2:09:24 AM	Windows Update Agent	Installation	19	N/A
Information	2/18/2007	2:09:09 AM	Windows Update Agent	Installation	19	N/A
Information	2/18/2007	2:08:31 AM	Windows Update Agent	Installation	19	N/A
Information	2/18/2007	2:08:05 AM	Windows Update Agent	Installation	19	N/A
Information	2/18/2007	2:08:00 AM	Service Control Manager	None	7036	N/A

Audit Command Language (ACL)

- ACL is the market leader in computer-assisted audit technology and is an established forensics tool.

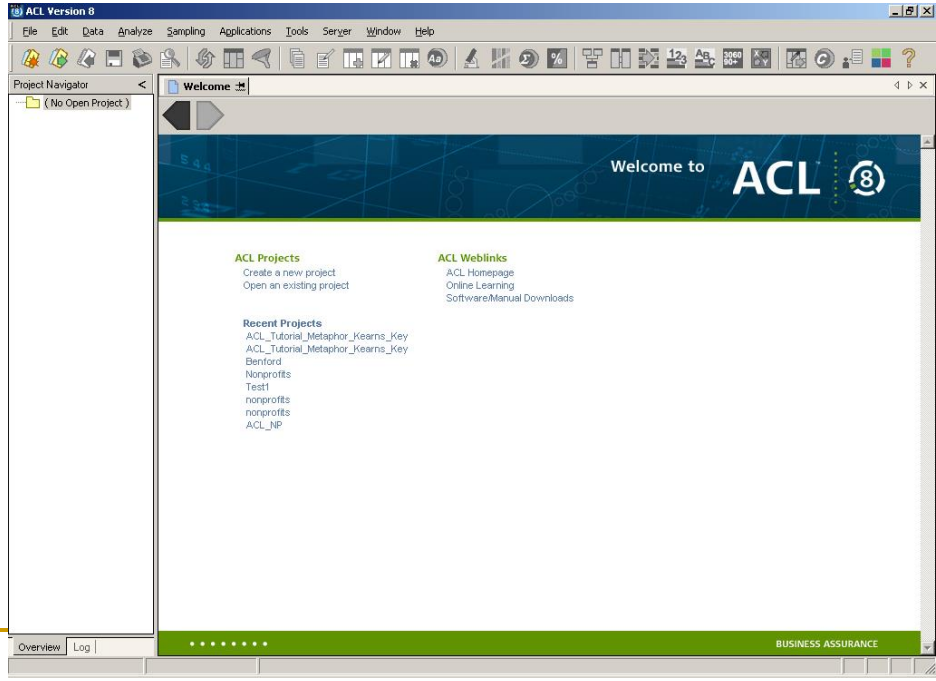
Clientele includes …

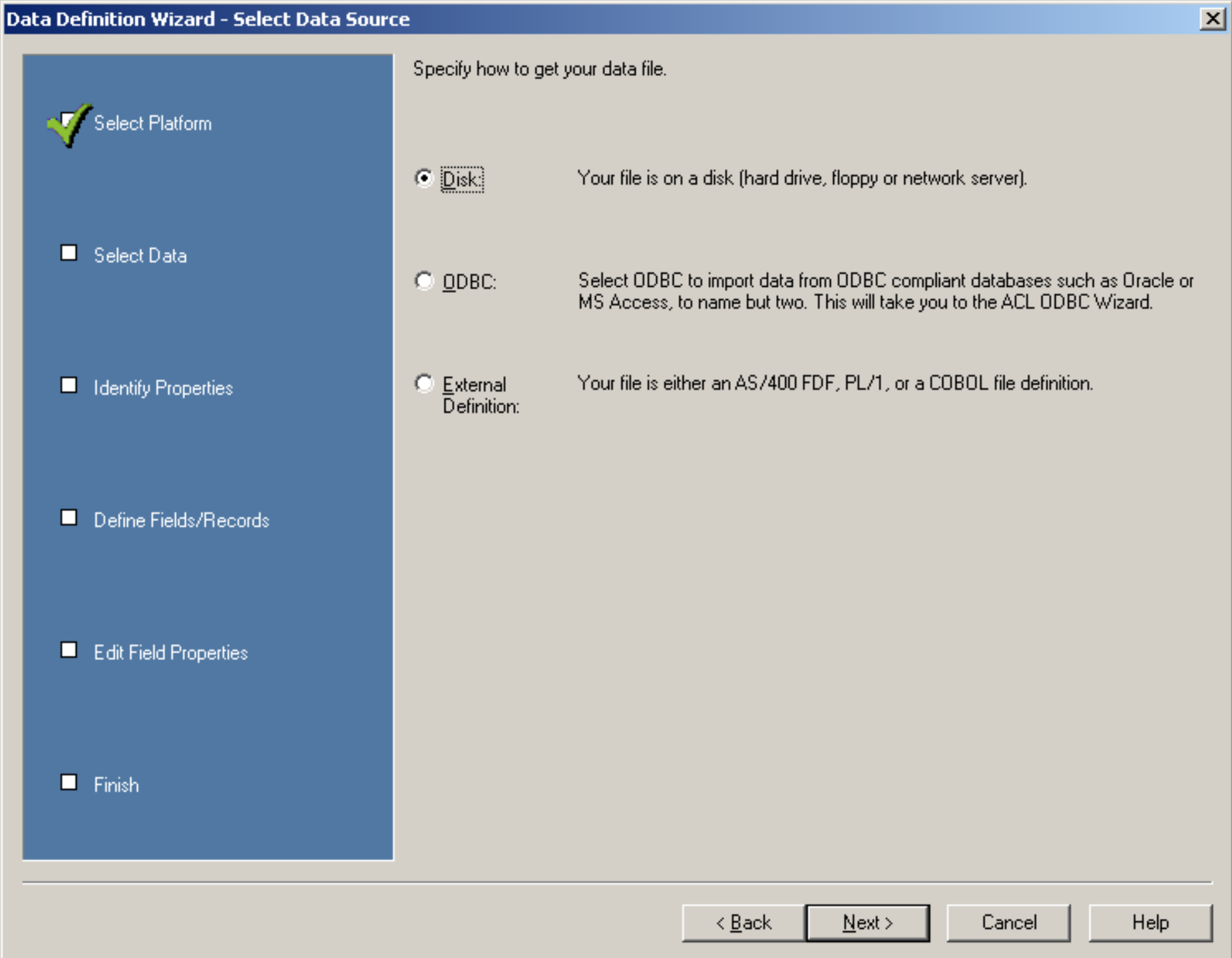
- 70 percent of the Fortune 500 companies
- over two-thirds of the Global 500
- the Big Four public accounting firms

Audit Command Language

ACL is a computer data extraction and analytical audit tool with audit capabilities …

- Statistics
- Duplicates and Gaps
- Stratify and Classify
- Sampling
- Benford Analysis




Data Definition Wizard - Select Data Source
Select Platform
Select Data
Identify Properties
Define Fields/Records
Edit Field Properties
Finish
Specify how to get your data file.
Disk:
Your file is on a disk (hard drive, floppy or network server).
ODBC:
Select ODBC to import data from ODBC compliant databases such as Oracle or MS Access, to name but two. This will take you to the ACL ODBC Wizard.
External Definition:
Your file is either an AS/400 FDF, PL/1, or a COBOL file definition.
< Back
Next >
Cancel
Help

File Edit Data Analyze Sampling Applications Tools Server Window Help

Proje... >

Foren
co
Fo

Welcome | compfirm | Statistics

Command: STATISTICS ON Revenues__Last_yr TO SCREEN NUMBER 5
Table: compfirm

Revenues__Last_yr

	Number	Total	Average
Range	-	256,329.00	-
Positive	5,346	11,196,638.80	2,094.40
Negative	0	0.00	0.00
Zeros	1,646	-	-
Totals	6,992	11,196,638.80	1,601.35
Abs Value	-	11,196,638.80	-

Highest	Lowest
256,329.00	0.00
232,571.00	0.00
210,959.00	0.00
201,932.00	0.00
201,932.00	0.00

Text

O.. L...

compfirm 6,992 Records

Forensics Project.ACL - ACL Version 8

File Edit Data Analyze Sampling Applications Tools Server Window Help

Project Navigator

Forensics Proje
compfirm
Forensics_Pro

Welcome | compfirm | Stratify

Command: STRATIFY ON Revenues__Last_yr INTERVALS 10 TO SCREEN
Table: compfirm

Minimum encountered was 0.00
Maximum encountered was 256,329.00

Revenues__Last_yr	Count	Percent of Count	Percent of Field	Revenues__Last_yr
0.00 - 25,632.89	6,909	98.81%	52.85%	5,917,853.10
25,632.90 - 51,265.79	54	0.77%	17.08%	1,912,781.90
51,265.80 - 76,898.69	12	0.17%	6.95%	778,569.20
76,898.70 - 102,531.59	4	0.06%	2.94%	329,632.70
102,531.60 - 128,164.49	3	0.04%	2.98%	333,794.10
128,164.50 - 153,797.39	1	0.01%	1.2%	134,187.00
153,797.40 - 179,430.29	3	0.04%	4.47%	500,573.80
179,430.30 - 205,063.19	3	0.04%	5.26%	589,388.00
205,063.20 - 230,696.09	1	0.01%	1.88%	210,959.00
230,696.10 - 256,329.00	2	0.03%	4.37%	488,900.00
Totals	6,992	100%	100%	11,196,638.80

Text | Graph

Overview | Log

ompfirm | 6,992 Records

Welcome | compfirm | Classify

Command: CLASSIFY ON Industry SUBTOTAL Capital_Expenditures Growth_in_Revenue__last_year ROE TO SCREEN
Table: compfirm

Industry	Count	Percent of Count	Percent of Field	Capital_Expenditures	Growth_in_Revenue__last_year	ROE
«34 spaces»	1,647	23.56%	0%	0.00	0.0000	0.0000000000
Advertising	28	0.4%	0.11%	729.80	2.8691	-17.7430691224
Aerospace/Defense	65	0.93%	0.56%	3,627.60	9.2737	-0.7091448840
Air Transport	42	0.6%	1.71%	10,985.50	4.1704	-26.7134943353
Apparel	61	0.87%	0.13%	814.20	4.1098	-15.1080127024
Auto & Truck	22	0.31%	7.05%	45,354.00	1.5342	-3.2817630075
Auto Parts	57	0.82%	1.05%	6,767.30	3.9520	8.6820586961
Bank	1	0.01%	0%	1.00	-0.2735	0.1362530414
Beverage (Alcoholic)	18	0.26%	0.23%	1,493.30	0.9024	-2.1822496885
Beverage (Soft Drink)	16	0.23%	0.73%	4,725.60	3.3217	-1.4602867980
Biotechnology	65	0.93%	0.33%	2,096.20	9.4486	-35.1767875676
Building Materials	44	0.63%	0.2%	1,267.90	2.5131	1.7837356860
Cable TV	19	0.27%	2.03%	13,082.80	2.3795	-0.4403124585

Text | Graph

compfirm | ?/6,992 | Global Filter: (Industry = " ")

Benford Analysis

- States that the leading digit in some numerical series is follows an exponential rather than normal distribution
- Applies to a wide variety of figures: financial results, electricity bills, street addresses, stock prices, population numbers, death rates, lengths of rivers

Leading Digit	Probability
1	30.1 %
2	17.6 %
3	12.5 %
4	9.7 %
5	7.9 %
6	6.7 %
7	5.8 %
8	5.1 %
9	4.6 %

As of: 03/31/2007 10:52:28

Command: BENFORD ON Growth_in_Revenue__last_year LEADING 1 TO SCREEN
Table: compfirm

2030 zero amounts bypassed

Leading Digits	Actual Count	Expected Count	Zstat Ratio
1	1519	1494	0.767
2	894	874	0.736
3	619	620	0.019
4	457	481	1.121
5	415	393	1.136
6	343	332	0.586
7	248	288	2.384
8	246	254	0.472
9	221	227	0.377

Employee Internet Activity

Spector captures employee web activity including keystrokes, email, and snapshots to answer questions like:

- Which employees are spending the most time surfing web sites?
- Which employees chat the most?
- Who is sending the most emails with attachments?
- Who is arriving to work late and leaving early?
- What are my employees searching for on the Internet?

*Data Monitoring : **Spector***

Recorded Email

http://www.spectorcne.com - Spector CNE - View Recorded Email - Microsoft Internet Explorer

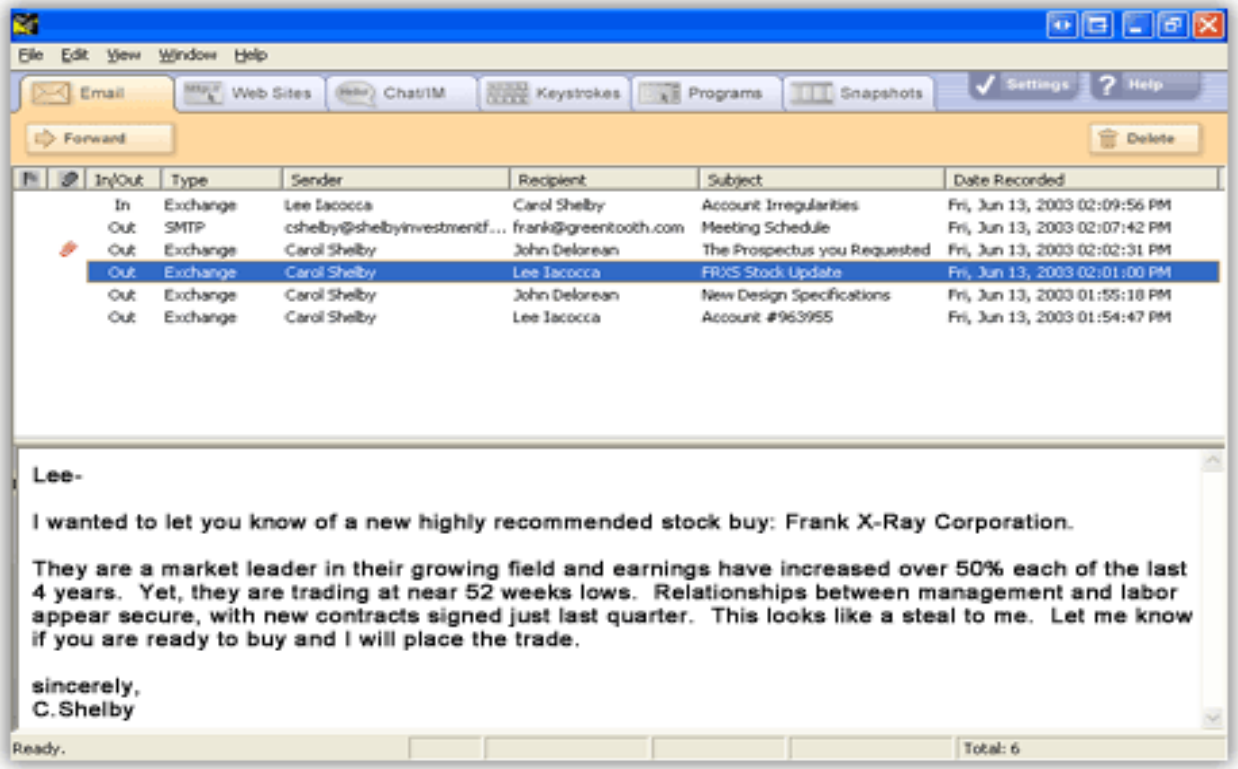
Spector CNE Viewer - Recorded Email

Close Window

Spector CNE can record in detail all incoming and outgoing company email, as well as the employee's personal Internet email service, such as Hotmail, Yahoo or AOL, meeting regulations for compliance.

Whenever email is sent or received, Spector CNE creates an invisible duplicate, including file attachments that contain transaction data, and stores for later view. Even if an employee later deletes the email, Spector CNE will have saved an exact copy.

>>> Click here to see the features of the Email Recorder.



Internet

*Data Monitoring : **Spector***

Recorded Web Surfing

http://www.spectorcne.com - Spector CNE - View Recorded Web Surfing - Microsoft Internet Explorer

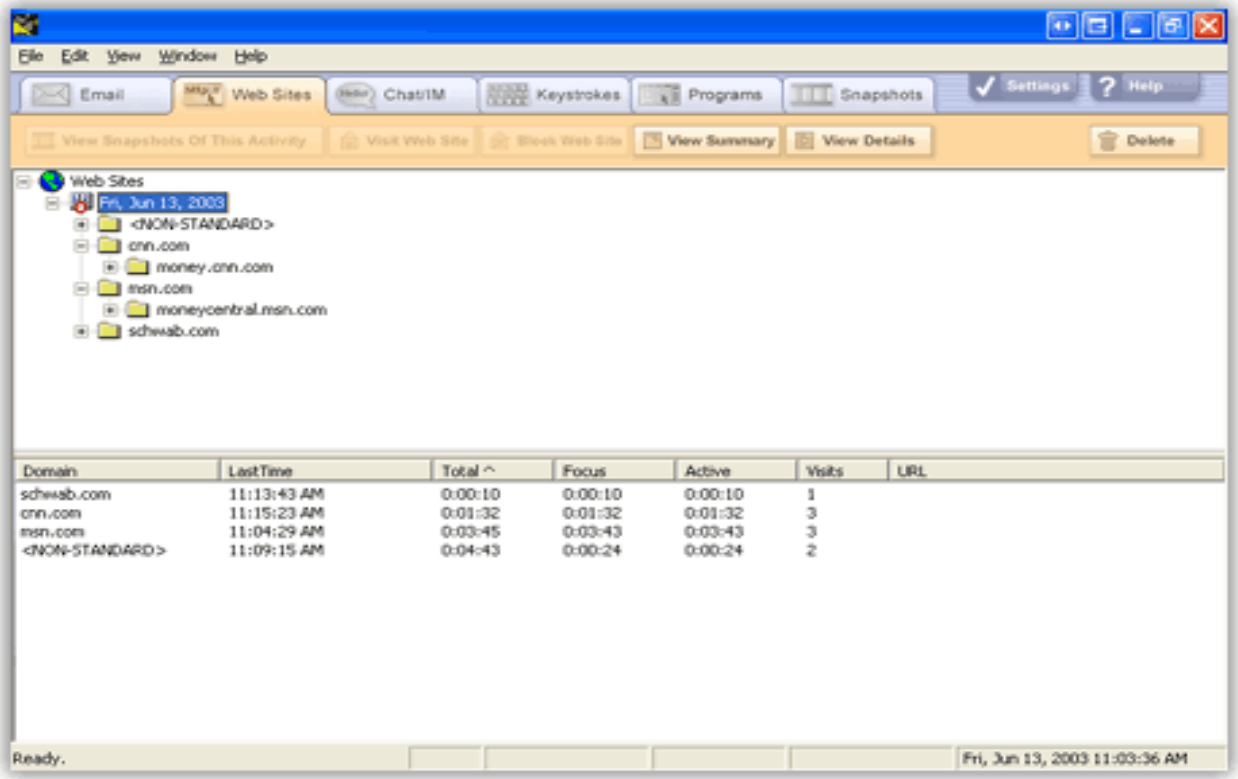
Spector CNE Viewer - Recorded Web Surfing

Close Window

The Web site recording tool in Spector CNE will continually monitor every web page that is being accessed by the computers on your network and save a record of those URLs and Domain Names.

With CNE's advanced and intuitive Web Site recording, you're provided a quick, yet exact, picture of each individual's web surfing.

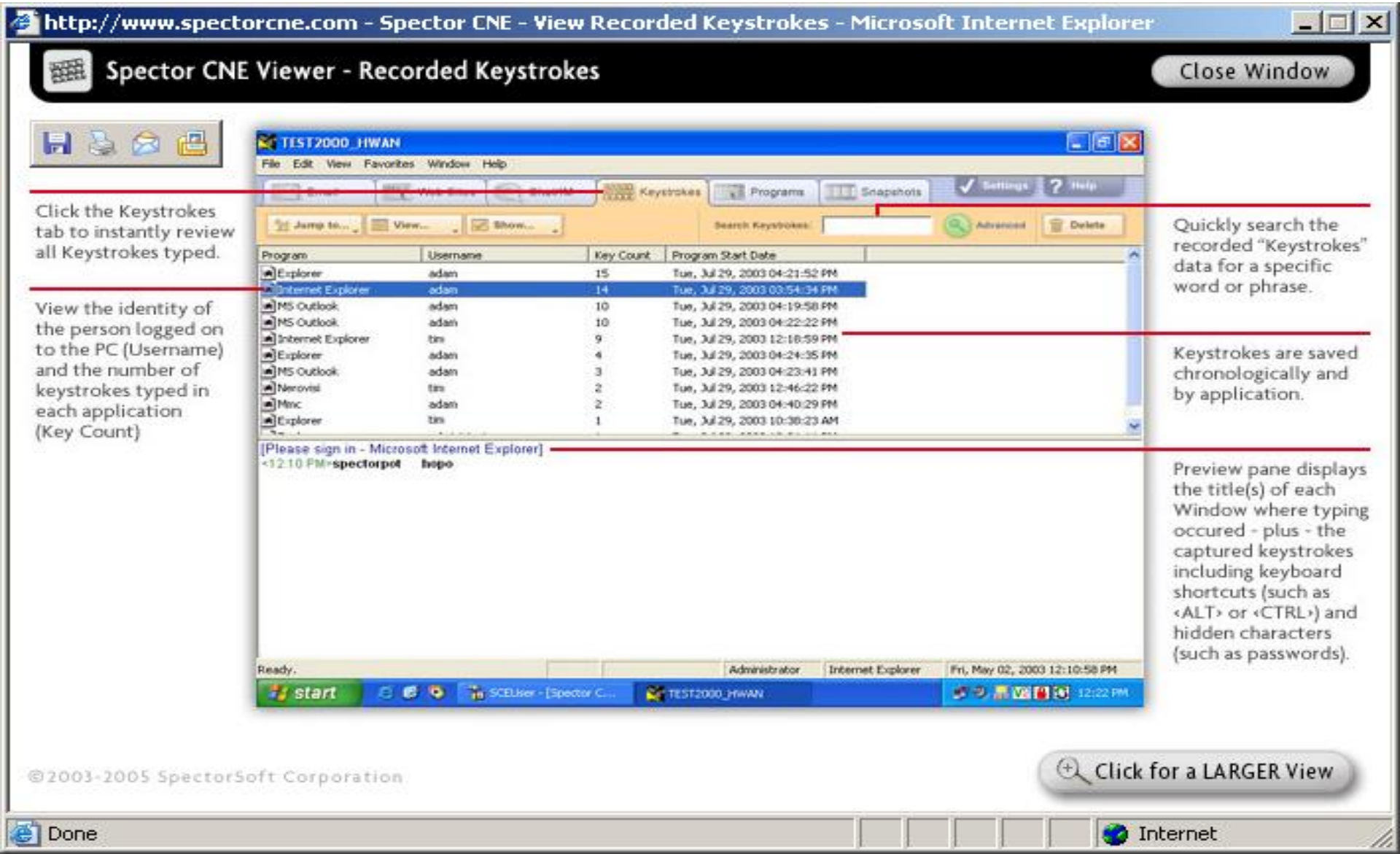
>>> Click here to see the features of the Web Site Recorder.



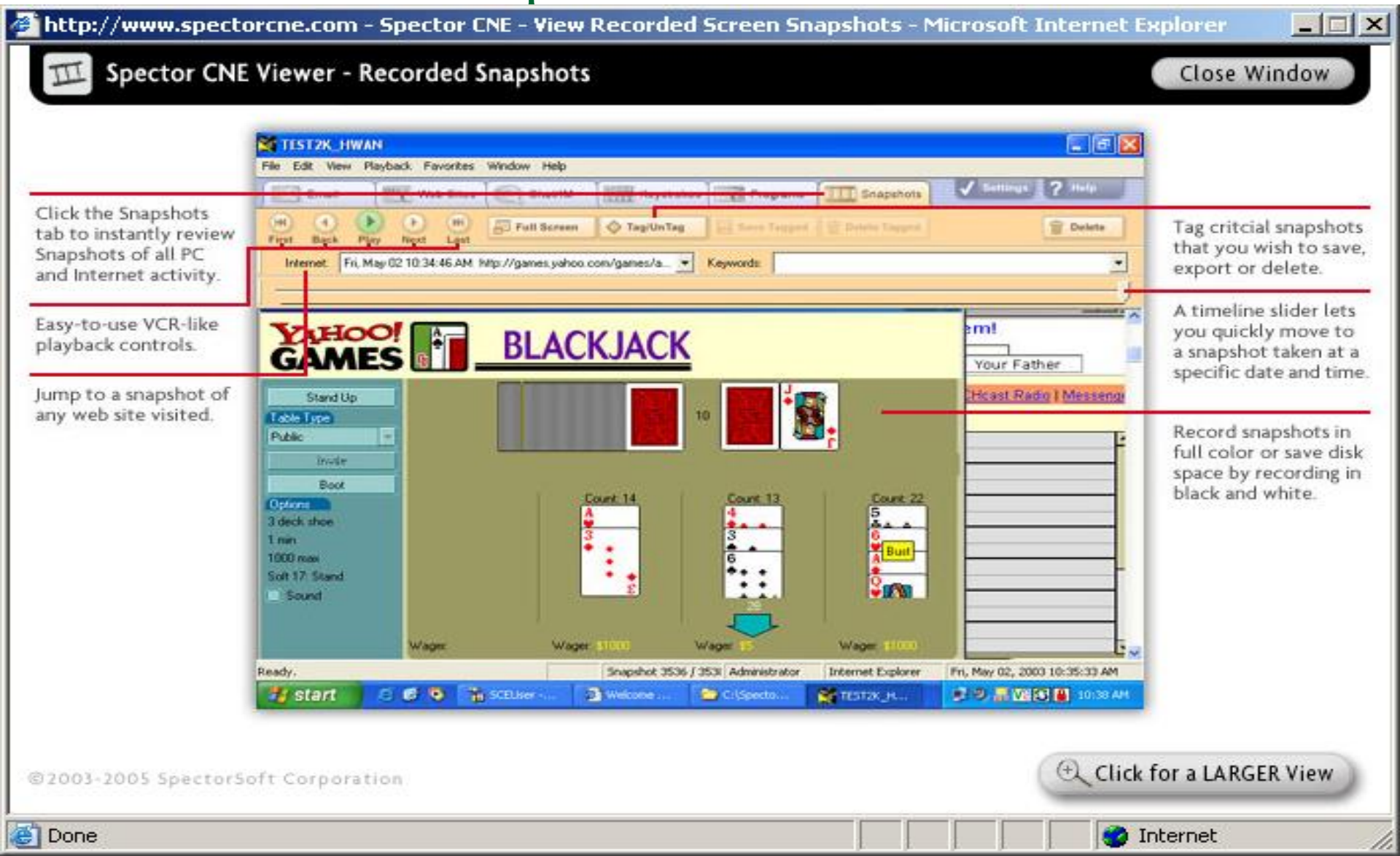
Done

Internet

Recording Keystrokes

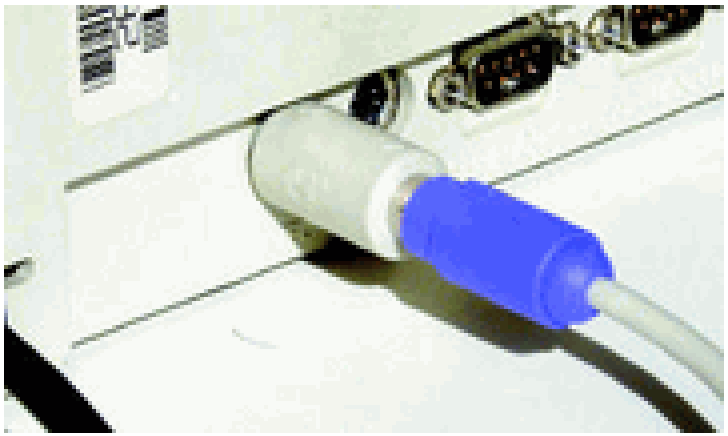


Recorded Snapshots



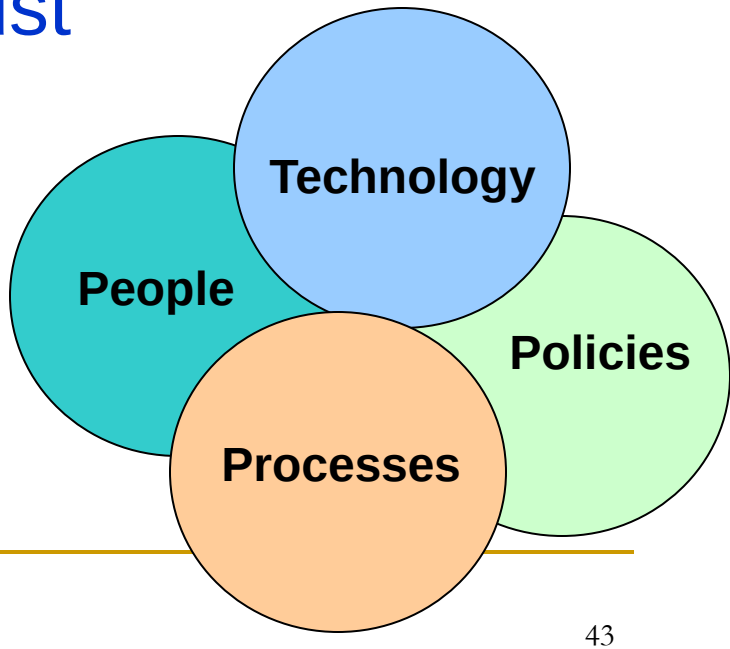
KeyKatcher

- Records chat, e-mail, internet & more
- Is easier to use than parental control software
- Identifies internet addresses
- Uses no system resources
- Works on all PC operating systems
- Undetectable by software



Developing a Forensic Protocol

- The response plan must include a coordinated effort that integrates a number of organizational areas and possibly external areas
- Response to fraud events must have top priority
- Key players must exist at all major organizational locations



End-to-End Forensic Analysis

First rule of end-to-end forensic digital analysis

- ***Primary evidence*** *must always be corroborated by at least one other piece of relevant primary evidence to be considered a valid part of the evidence chain. Evidence that does not fit this description, but does serve to corroborate some other piece of evidence without itself being corroborated, is considered to be* ***secondary evidence.***
- Exception: the first piece of evidence in the chain from the Identification layer

Security Exposures

Organizations may possess critical technology skills but …

- Skills are locked in towers – IT, Security, Accounting, Auditing
- Skills are centralized while fraud events can be decentralized
- Skills are absent – vacations, illnesses, etc

The Role of Policies

- They define the actions you can take
- They must be clear and simple to understand
- The employee must acknowledge that he or she read them, understands them and will comply with them
- They can't violate law

Forensic Response Control

Incident Response Planning …

- Identify needs and objectives
- Identify resources
- Create policies, procedures
- Create a forensic protocol
- Acquire needed skills
- Train
- Monitor

Documenting the Scene

- Note time, date, persons present
- Photograph and video the scene
- Draw a layout of the scene
- Search for notes (passwords) that might be useful
- If possible freeze the system such that the current memory, swap files, and even CPU registers are saved or documented

Forensic Protocol

- First responder triggers alert
- Team response
  - Freeze scene
  - Begin documentation
- Auditors begin analysis
  - Protect chain-of-custody
  - Reconstruct events and develop theories
  - Communicate results of analysis

Protocol Summary

- Ensure appropriate policies
- Preserve the crime scene (victim computer)
- Act immediately to identify and preserve logs on intermediate systems
- Conduct your investigation
- Obtain subpoenas or contact law enforcement if necessary

Key: Coordination between functional areas

Conclusion

IT Forensic Investigative Skills Can …

- Decrease occurrence of fraud
- Increase the difficulty of committing fraud
- Improve fraud detection methods
- Reduce total fraud losses

Auditors trained in these skills are more valuable to the organization!

Questions or Comments?