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
IT Forensic Techniques for Auditors

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
Importance of IT Forensic Techniques to Organizations

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
Importance of IT Forensic Techniques to Organizations

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
Importance of IT Forensic Techniques to Organizations

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- Policies outdated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.
Importance of IT Forensic Techniques to 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
Importance of IT Forensic Techniques to Auditors

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
Importance of IT Forensic Techniques to Auditors

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
Audit Goals of a Forensic Investigation

Rules of Evidence

- Complete
- Authentic
- Admissible
- Reliable
- Believable
Audit Goals of a Forensic Investigation

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
Digital Crime Scene Investigation

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.
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)
Digital Crime Scene Investigation

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 Crime Scene Investigation

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
Data Integrity

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
Data Integrity

MD5 Using HashCalc
Data Integrity

Private Disk
Data Monitoring

Tracking Log Files

Ok, now you will probably notice that 80% of the report is dedicated to one or two daemons. You can either re-configure them (i.e. reconfigure smartd to ignore Temperature and Raw Error Rate), or get logcheck to ignore them. Here are some examples:

Security Example

Security Events

May 29 06:42:51 imago smartd[8521]: Device: /dev/hda, SMART Prefailure Attribute: 1 Raw_Read_Error_Rate changed from 66 to 66
May 29 13:37:30 imago dhclient: receive_packet failed on eth0: Network is down
May 29 17:01:07 imago kernel: device eth0 entered promiscuous mode
May 29 17:01:08 imago kernel: bridge-eth0: enabled promiscuous mode
May 29 17:12:51 imago smartd[8521]: Device: /dev/hda, SMART Prefailure Attribute: 1 Raw_Read_Error_Rate changed from 65 to 65
May 29 17:27:34 imago kernel: device eth0 left promiscuous mode
May 29 20:56:50 imago sshd[28732]: (pam_unix) authentication failure: logname= uid=0 euid=0 tty=ssh ruser= host=castle.o
May 29 20:56:52 imago sshd[28732]: error: PAM: Authentication failure for stefanor from castle.owlsbarn.rivera.sa.net
May 29 22:12:51 imago smartd[8521]: Device: /dev/hda, SMART Prefailure Attribute: 1 Raw_Read_Error_Rate changed from 66 to 66

OK, I reconfigured smartd to forget about read error rates. I was messing around with networking, and I often do, so I'll ignore the promiscuous lines.

The Debian Logcheck package maintains the files in the ignore directories. It is good practice to put your own ignores into local-daemon-name files, so it won't touch them.

```
# vi ignore.d.server/local-networking

\^[0-9]+ \^[\(][0-9]+[..][^\)[,]+ \^[0-9]+ \^[\(][0-9]+[..][^\)[,]++ dhclient: receive_packet failed on eth\^[0-9]+ \^[\(][0-9]+[..][^\)[,]+: Network is down

# cp ignore.d.server/local-networking violations.ignore.d
```
Data Monitoring

PC System Log
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
Forensic Tools

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
Select Platform

- **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.
Command: STATISTICS ON Revenues__Last_yr TO SCREEN NUMBER 5
Table: compfirm

<table>
<thead>
<tr>
<th></th>
<th>Number</th>
<th>Total</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range</td>
<td>-</td>
<td>256,329.00</td>
<td>-</td>
</tr>
<tr>
<td>Positive</td>
<td>5,346</td>
<td>11,196,638.80</td>
<td>2,094.40</td>
</tr>
<tr>
<td>Negative</td>
<td>0</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Zeros</td>
<td>1,646</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Totals</td>
<td>6,992</td>
<td>11,196,638.80</td>
<td>1,601.35</td>
</tr>
<tr>
<td>Abs Value</td>
<td>-</td>
<td>11,196,638.80</td>
<td>-</td>
</tr>
</tbody>
</table>

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

6,992 Records
Command: STRATIFY ON Revenues__Last_yr INTERVALS 10 TO SCREEN
Table: compfirm

Minimum encountered was 0.00
Maximum encountered was 256,329.00

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

### Table
<table>
<thead>
<tr>
<th>Industry</th>
<th>Count</th>
<th>Percent of Count</th>
<th>Percent of Field</th>
<th>Capital_Expenditures</th>
<th>Growth_in_Revenue_last_year</th>
<th>ROE</th>
</tr>
</thead>
<tbody>
<tr>
<td>«34 spaces»</td>
<td>1,647</td>
<td>23.56%</td>
<td>0%</td>
<td>0.00</td>
<td></td>
<td>0.0000</td>
</tr>
<tr>
<td>Advertising</td>
<td>28</td>
<td>0.4%</td>
<td>0.11%</td>
<td>729.80</td>
<td></td>
<td>2.8691</td>
</tr>
<tr>
<td>Aerospace/Defense</td>
<td>65</td>
<td>0.93%</td>
<td>0.56%</td>
<td>3,627.60</td>
<td></td>
<td>9.2737</td>
</tr>
<tr>
<td>Air Transport</td>
<td>42</td>
<td>0.6%</td>
<td>1.71%</td>
<td>10,985.50</td>
<td></td>
<td>4.1704</td>
</tr>
<tr>
<td>Apparel</td>
<td>61</td>
<td>0.87%</td>
<td>0.13%</td>
<td>814.20</td>
<td></td>
<td>4.1098</td>
</tr>
<tr>
<td>Auto &amp; Truck</td>
<td>22</td>
<td>0.31%</td>
<td>7.05%</td>
<td>45,354.00</td>
<td></td>
<td>1.5342</td>
</tr>
<tr>
<td>Auto Parts</td>
<td>57</td>
<td>0.82%</td>
<td>1.05%</td>
<td>6,767.30</td>
<td></td>
<td>3.9520</td>
</tr>
<tr>
<td>Bank</td>
<td>1</td>
<td>0.01%</td>
<td>0%</td>
<td>1.00</td>
<td></td>
<td>-0.2735</td>
</tr>
<tr>
<td>Beverage (Alcoholic)</td>
<td>18</td>
<td>0.26%</td>
<td>0.23%</td>
<td>1,493.30</td>
<td></td>
<td>0.9024</td>
</tr>
<tr>
<td>Beverage (Soft Drink)</td>
<td>16</td>
<td>0.23%</td>
<td>0.73%</td>
<td>4,725.60</td>
<td></td>
<td>3.3217</td>
</tr>
<tr>
<td>Biotechnology</td>
<td>65</td>
<td>0.93%</td>
<td>0.33%</td>
<td>2,096.20</td>
<td></td>
<td>9.4486</td>
</tr>
<tr>
<td>Building Materials</td>
<td>44</td>
<td>0.63%</td>
<td>0.2%</td>
<td>1,267.90</td>
<td></td>
<td>2.5131</td>
</tr>
<tr>
<td>Cable TV</td>
<td>19</td>
<td>0.27%</td>
<td>2.03%</td>
<td>13,082.80</td>
<td></td>
<td>2.3795</td>
</tr>
</tbody>
</table>

compfirm  
[Image of the interface showing the classification results]
Forensic Tools: ACL

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

<table>
<thead>
<tr>
<th>Leading Digit</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>30.1 %</td>
</tr>
<tr>
<td>2</td>
<td>17.6 %</td>
</tr>
<tr>
<td>3</td>
<td>12.5 %</td>
</tr>
<tr>
<td>4</td>
<td>9.7 %</td>
</tr>
<tr>
<td>5</td>
<td>7.9 %</td>
</tr>
<tr>
<td>6</td>
<td>6.7 %</td>
</tr>
<tr>
<td>7</td>
<td>5.8 %</td>
</tr>
<tr>
<td>8</td>
<td>5.1 %</td>
</tr>
<tr>
<td>9</td>
<td>4.6 %</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Leading Digits</th>
<th>Actual Count</th>
<th>Expected Count</th>
<th>Zstat Ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1519</td>
<td>1494</td>
<td>0.767</td>
</tr>
<tr>
<td>2</td>
<td>894</td>
<td>874</td>
<td>0.736</td>
</tr>
<tr>
<td>3</td>
<td>619</td>
<td>620</td>
<td>0.019</td>
</tr>
<tr>
<td>4</td>
<td>457</td>
<td>481</td>
<td>1.121</td>
</tr>
<tr>
<td>5</td>
<td>415</td>
<td>393</td>
<td>1.136</td>
</tr>
<tr>
<td>6</td>
<td>343</td>
<td>332</td>
<td>0.586</td>
</tr>
<tr>
<td>7</td>
<td>248</td>
<td>288</td>
<td>2.384</td>
</tr>
<tr>
<td>8</td>
<td>246</td>
<td>254</td>
<td>0.472</td>
</tr>
<tr>
<td>9</td>
<td>221</td>
<td>227</td>
<td>0.377</td>
</tr>
</tbody>
</table>
Data Monitoring

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

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.
Data Monitoring: **Spector**

**Recorded Web Surfing**

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.](#)
Data Monitoring: **Spector**

**Recording Keystrokes**

- Click the Keystrokes tab to instantly review all keystrokes typed.
- View the identity of the person logged on to the PC (Username) and the number of keystrokes typed in each application (Key Count).

Quickly search the recorded “Keystrokes” data for a specific word or phrase.

Keystrokes are saved chronologically and by application.

Preview pane displays the title(s) of each Window where typing occurred - plus - the captured keystrokes including keyboard shortcuts (such as `ALT` or `CTRL`) and hidden characters (such as passwords).

©2003-2005 SpectorSoft Corporation
Data Monitoring: **Spector**

**Recorded Snapshots**

- Click the Snapshots tab to instantly review Snapshots of all PC and Internet activity.
- Easy-to-use VCR-like playback controls.
- Jump to a snapshot of any website visited.
- Tag critical snapshots that you wish to save, export or delete.
- A timeline slider lets you quickly move to a snapshot taken at a specific date and time.
- Record snapshots in full color or save disk space by recording in black and white.
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

www.lakeshoretechnology.com
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.
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
A Forensic Protocol

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
A Forensic Protocol

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
A Forensic Protocol

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
A Forensic Protocol

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
A Forensic Protocol

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?