

May 2006, IBSA Conference, Vienna

The Role of Digital Forensics within a Corporate Organization

Bruce J. Nikkel
IT Investigation & Forensics
Risk Control, UBS AG



Presentation Summary



- An overview of digital forensics
- The need for corporate forensics functionality
- Challenges in creating a forensics capability
- Questions, discussion, recommended resources

An Overview of Digital Forensics



- What is digital forensics?
- What is digital evidence?
- Who is using it?

What is Digital Forensics?



- The collection, preservation, analysis, and presentation of digital evidence
- Admissible in a court of law
- Usable for internal disciplinary hearings
- Supporting data for internal incident reports
- Assisting/furthering other investigations

Digital Evidence is Data Which:



- Helps reconstruct past events or activity (timelines)
- Shows possession/handling of digital data
- Show use/abuse of IT infrastructure & services
- Shows evidence of policy violation or illegal activity

The Main Areas of Digital Forensics



- Computer forensics (hard disk, removable media acquisition and analysis)
- Network forensics (network intrusions, abuse, .etc)
- Software forensics (examining malicious code, malware, etc.)
- Live system forensics (compromised hosts, system abuse, etc)

Organizations Using Digital Forensics Technology



- Law enforcement
- Military, government agencies
- Law firms (legal discovery)
- Data recovery firms
- Corporate organizations (relatively new)

Potential Sources of Digital Evidence



- Hard disks, tapes, external/removable media
- Network infrastructure logs (Firewall, IDS, proxy, etc.)
- Application, audit log files
- Email
- Other server content (Windows shares, web servers, databases, etc.)
- Captured network traffic

Difficulties of Digital Evidence



- Easy to destroy
 - starting a PC updates hundreds of timestamps and modifies many files
 - attaching a hard disk or USB stick will modify file system timestamps
 - volatile memory is lost when a machine is powered off
- Hard to get
 - network traffic only exists on the wire for milliseconds
 - intrusions and attacks may be cleverly devised
 - anti-forensic activity may prevent collection

Digital Forensics within a Corporate Organization



- What is driving the need for a digital forensics role within organizations?
- Driven by internal demand
- Driven by external factors
- Leveraging tools & skills

Driver: Legal and Regulatory Requirements



- Country/region specific laws
 - different countries have different laws and regulations
 - may require some form of forensic capability or readiness
 - example: Sarbanes Oxley Act Requires a Process for dealing with incidents requiring forensic analysis or investigation (SOX 012-s13)
- Regulated Industries
 - finance, Healthcare, Insurance, telecom, etc.
 - may have industry specific requirements
 - example: Swiss ISP log retention

Driver: Industry Best Practice



- ISO 17799 (2003)
 - international standard for Information security
 - recommends procedures for collecting evidence and analyzing incidents
- Information Assurance Advisory Council (IAAC)
 - guidelines for ensuring corporate forensic readiness
- Published, peer reviewed papers
 - Digital Investigation Journal, The International Journal of Digital Forensics & Incident Response (Elsevier)
 - International Journal of Digital Evidence (IJDE)

Driver: Internal Demand



- Legal departments
 - assisting corporate legal teams with discovery
 - ensuring compliance with local laws and regulations
- Corporate policies and standards compliance
 - company policies/standards may benefit from a forensic capability
 - audit requirements/recommendations

Driver: Internal Demand (cont.)



- HR
 - firing/termination
 - employee misconduct, disciplinary action
 - exceptional/extreme cases (death, suicide, kidnapping, etc.)
- Other corporate investigative bodies
 - many investigative roles may exist (fraud, crime, incident handling, disaster/emergency response, .etc)
 - need for assistance, central forensics competence center
 - risk management, risk control, crime risk control

Driver: Internal Demand (cont.)



- Intellectual Property (IP)
 - intellectual property abuse/infringement
 - brand/image reputation risk (investigating fraudulent websites, phishing attacks, etc.)
- IT
 - intrusion analysis
 - investigating IT policy violation
 - IT infrastructure abuse/misuse
 - logic bomb, virus/malware analysis, etc.
 - special services leveraging forensic team's tools and skills

Driver: Internal Demand (cont.)



- "Non-forensic forensics": Using forensic tools and skills for legitimate, but non-forensic purposes
 - verifying corporate disk wiping procedures
 - verifying disk/network encryption implementation
 - data recovery (crashed hard disks, old/obsolete media, etc.)
 - legitimate password recovery requests
 - assist with obscure troubleshooting
 - IT architecture and design (provide forensic readiness input/feedback)

Challenges in Creating a Forensics Capability



- What are some of the challenges in setting up a corporate forensics functionality?
- Basic needs/requirements of a digital forensics team
- Some key factors in implementing a digital forensics role in an organization

Organizational Challenges



- Team placement within the organization:
 - IT ?
 - IT security risk management ? IT security risk control ?
 - legal/compliance departments ?
 - part of CERT, CSIRT, SIRT, SOC ?
 - centralized? regional?
 - in-house or out-sourced ?
- Internal competition/diversity
 - very large organizations may have multiple investigation and/or forensic teams
 - varying degrees of responsibility/involvement (sometimes a lead role, sometimes an assisting role, sometimes a consulting role)

Forensic Readiness



- Investigative access policy
 - ensure authorized investigators are able to collect data
 - protect sensitive data
 - controlled/logged access (prevent abuse, reduce risk)
- IT data retention policy
 - legal/regulatory requirements
 - IT incident response requirements
 - forensic & investigative recovery requirements
- Establishing Forensics resources
 - a trained forensics team
 - a properly equipped forensics lab
 - outsourcing partners, external experts

Support and Awareness



- Management support
 - convincing management that a forensic team is needed/valuable to the organization
 - emphasis on readiness ("Fire Department" perspective)
 - makes things easier/cheaper for a number of internal groups
 - preventing a single high-cost court case alone could justify the expense of such a team
- Awareness in various areas of an organization
 - inclusion in work-flows and processes
 - having a point of escalation, additional support
 - knowing a forensics competence center exists

Establishing Formal Contact Channels



- To facilitate:
 - enabling others to efficiently contact the forensics team
 - enabling the forensics team to efficiently contact others
- Internal
 - contact to various IT areas for data collection and expertise
 - contact channel to the forensic team via shared mailbox, hotline, other departments, etc.
- External
 - peers in other organizations or in the digital forensics community
 - local/federal law enforcement
 - contact channel to the forensic team via abuse@company.com, hotlines, website contact forms

Forensic Team Skills and Tools



- Staff training and skills maintenance
 - knowledge of proper methods and procedures
 - allowing time to learn/understand new technologies
 - certified examiners (CISSP, Encase EnCE, etc.)
- Setting up a forensics lab & tools
 - forensics hardware (write blockers)
 - forensics software (commercial, Linux & open-source, custom in-house tools)
 - systems for performing acquisition, analysis, and testing
 - old media drives and technologies

Recommended Resources



- **Web resources**
 - www.e-evidence.info, a directory of digital forensics documentation and papers
 - www.forensicswiki.org, a Wikipedia style forensics website
 - www.forensicfocus.com, an online forensics community
- **Peer reviewed practitioner/research journals**
 - Elsevier's Digital Investigation Journal, The International Journal of Digital Forensics & Incident Response
 - International Journal of Digital Evidence (IJDE)
- **Software**
 - Commercial software: Encase, FTK, etc.
 - Opensource software: Linux, Sleuthkit, etc.

Questions or Comments?



- Questions or comments?
- Contact me at bruce.nikkel@ubs.com
- Slides available at www.digitalforensics.ch