Parul® University

Cyber Security and Forensics - I
05201296

Prof. Dipak L. Agrawal, Assistant Professor
Faculty of IT & Computer Science

Parul®
University

DIGITAL LEARNING CONTENT

CHAPTER-5

Understanding Cyber Forensics

Topics

- Computer forensics
- Cyber forensics and Digital evidence
- Rules of evidence, Forensics analysis of e-mail- RFC282
- Digital forensics life cycle
- Chain of custody concept, Network forensics, Setting up a computer forensics laboratory
- Computer forensics and steganography, Rootkits, Information hiding, Relevance of the OSI layer model to computer forensics,
- Forensics and social networking sites - security, privacy, threats.

What is Computer Forensics?

- "The process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable." (McKemmish, 1999)
- "Gathering and analyzing data in a manner as freedom distortion or bias as possible to reconstruct data or what has happened in the past on a system." (Farmer & Vennema,1999)
- Computer forensics is the application of computer investigation and analysis techniques in the interests of determining potential legal evidence.
- Forensic Computing, also known as Evidential Computing and even sometimes Data Recovery, is the specialist process of imaging and processing computer data which is reliable enough to be used as evidence in court

What will Computer Forensics do?

- Computer forensics, innovators of image copying technology, defined the principles of the science of computer forensics and formalized an approved and accepted methodology to COLLECT, ANALYSE and PRESENT suspect data to a Court of Law.
- Computer forensics evidence is frequently sought in a wide range of computer crime or misuse, including but not limited to theft of trade secrets, theft of or destruction of intellectual property, and fraud.
- Computer forensics specialists draw on an array of methods for discovering data that resides in a computer system.
- Experts in forensics computing can frequently recover files that have been deleted, encrypted, or damaged, sometimes as long as years earlier. Evidence gathered by computer forensics experts is useful and often necessary during discovery, depositions, and actual litigation.

Some areas of Computer Forensics

- Image Capture - The Imaging process is fundamental to any computer investigation.
- Image Processing - The processing software consists of two modules, GenX and GenText, running automatically to index and extract text from all areas of the target image.
- Investigation - Once the processing has taken place full searches of all areas of the disk takes only seconds.

Case study of Computer Forensics

(what does computer forensics look like?)

- Hacker, Human resources
- Money on disk, Hidden bits
- Disk swap, Tapes rarely lie...
- Narcotics, Fraud
- Theft, Corporate or University internal investigation
- FBI or (unlikely) Sheriff investigation
- Computer Security Research
- Post Mortem or Damage Assessment
- Child Pornography
- Espionage & Treason
- Corporate or University Policy Violation

The broad tests for evidence

(from Sherlock Holmes to current forensic scientist)Money on disk, Hidden bits

- authenticity - does the material come from where it purports?
- reliability - can the substance of the story the material tells be believed and is it consistent? In the case of computer-derived material are there reasons for doubting the correct working of the computer?
- completeness - is the story that the material purports to tell complete? Are there other stories which the material also tells which might have a bearing on the legal dispute or hearing?
- conformity with common law and legislative rules - acceptable levels of freedom from interference and contamination as a result of forensic investigation and other post-event handling

Elements of Computer Forensics

well-defined procedures to address the various tasks

- an anticipation of likely criticism of each methodology on the grounds of failure to demonstrate authenticity, reliability, completeness and possible contamination as a result of the forensic investigation
- the possibility for repeat tests to be carried out, if necessary by experts hired by the other side
- check-lists to support each methodology
- an anticipation of any problems in formal legal tests of admissibility
- the acceptance that any methods now described would almost certainly be subject to later modification

Divergences from conventional forensic investigation

- the main reason is the rate of change of computer technology
- a key feature of computer forensics is the examination of data media
- computer architectures have show profound change in the same short period, computer peripherals keep on changing as well
- wide area telecoms methods are being used more and more.
- the growth of e-mail
- the growth of client / server applications, the software outcome of the more complex hardware architectures.
- the greater use of EDI and other forms of computer-based orders, bills of lading, payment authorizations, etc.
- computer graphics, the greater use of computer-controlled procedures
- the methods of writing and developing software have changed also

Computer Forensics Situations

- documents - to prove authenticity; alternatively to demonstrate a forgery, reports, computer generated from human input.
- real evidence - machine readable measurements, etc.
- electronic transactions - to prove that a transaction took place - or to demonstrate that a presumption that it had taken place was incorrect.
- conclusions reached by "search“- programs which have searched documents, reports, etc.
- event reconstruction- to show a sequence of events or transactions passing through a complex computer system.
- liability in situations where CAD designs have relied on auto-completion or filling in by a program conclusions of computer "experts" - the results of expert systems.

Some litigations

- Civil Matters
- Breach of Contract
- Asset recovery
- Tort, including negligence
- Breach of Confidence
- Defamation
- Breach of securities industry legislation and regulation and /or Companies Acts, Employee disputes
- Copyright and other intellectual property disputes
- Consumer Protection law obligations (and other examples of no-fault liability)
- Data Protection law legislation

Criminal Matters

- Theft Acts, including deception
- Criminal Damage
- Demanding money with menaces
- Companies Law, Securities Industry and banking offences
- Criminal offences concerned with copyright and intellectual property
- Drug offences
- Trading standards offences
- Official Secrets
- Computer Misuse Act offences

Computer Forensics Methods (1)

- safe seizure of computer systems and files, to avoid contamination and/ or interference
- safe collection of data and software
- safe and non-contaminating copying of disks and other data media
- reviewing and reporting on data media
- sourcing and reviewing of back-up and archived files
- recovery / reconstruction of deleted files - logical methods
- recovery of material from "swap" and "cache" files
- recovery of deleted / damaged files - physical methods

Computer Forensics Methods (2)

- core-dump: collecting an image of the contents of the active memory of a computer at a particular time
- estimating if files have been used to generate forged output
- reviewing of single computers for "proper" working during relevant period, including service logs, fault records, etc.
- proving / testing of reports produced by complex client / server applications
- reviewing of complex computer systems and networks for "proper" working during relevant period, including service logs, fault records, etc.
- review of system / program documentation for: design methods, testing, audit, revisions, operations management.

Computer Forensics Methods (3)

- reviewing of applications programs for "proper" working during relevant period, including service logs, fault records, etc.
- identification and examination of audit trails
- identification and review of monitoring logs
- telecoms call path tracing (PTTs and telecoms utilities companies only)
- reviewing of access control services - quality and resilience of facilities (hardware and software, identification / authentication services)
- reviewing and assessment of access control services - quality of security management
- reviewing and assessment of encryption methods - resilience and implementation

Computer Forensics Methods (4)

- setting up of pro-active monitoring in order to detect unauthorised or suspect activity
- monitoring of e-mail
- use of special "alarm" or "trace" programs
- use of "honey pots"
- inter-action with third parties, e.g. suppliers, emergency response teams, law enforcement agencies
- reviewing and assessment of measuring devices, etc. and other sources of real evidence, including service logs, fault records, etc.
- use of routine search programs to examine the contents of a file
- use of purpose-written search programs to examine the contents of a file

Computer Forensics Methods (5)

- reconciliation of multi-source files
- examination of telecoms devices, location of associated activity logs and other records perhaps held by third parties
- event reconstruction
- complex computer intrusion
- complex fraud
- system failure
- disaster affecting computer driven machinery or process
- review of "expert" or rule-based systems
- reverse compilation of suspect code
- use of computer programs which purport to provide simulations or animations of events: review of accuracy, reliability and quality

Chain of custody (CoC)

- Chain of custody (CoC), in legal contexts, refers to the chronological documentation or paper trail, showing the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence.
- Importance of chain of custody
- Evidence admissibility in court is predicated upon an unbroken chain of custody. It is important to demonstrate that the evidence introduced at trial is the same evidence collected at the crime scene, and that access was controlled and documented.

Steganography

- Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. The word steganography combines the Greek words steganos (στεγανός), meaning "covered, concealed, or protected", and graphein (γράφειν) meaning "writing".
- The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny.
- For example, a sender might start with an innocuous image file and adjust the colour of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

Rootkit

- A rootkit is a type of malicious software that is activated each time your system boots up. Rootkits are difficult to detect because they are activated before your system's Operating System has completely booted up.
- Rootkit installation can be automated, or an attacker can install it once they've obtained root or Administrator access. Obtaining this access is a result of direct attack on a system (i.e.), exploiting a known vulnerability (such as privilege escalation) or a password (obtained by cracking or social engineering). Once installed, it becomes possible to hide the intrusion as well as to maintain privileged access.

Social Network Data Pool

- While social networks vary in features and architecture, we identify the following generic data sources to be of interest in forensic examinations on social networks:
- The social footprint: What is the social graph of the user, with whom is he or she connected (“friend”)?
- Communications pattern: How is the network used for communicating, what method is used, and with whom is the user communicating?
- Pictures and videos: What pictures and videos were uploaded by the user, on which other peoples pictures is he or she tagged?
- Times of activity: When is a specific user connected to the social network, when exactly did a specific activity of interest took place?
- Apps: What apps is the user using, what is their purpose, and what information can be inferred in the social context.

Relevance of the OSI layer model to computer forensics:

- Physical Layer is used for defining the technical qualifications of the data connectivity. Since the security in this layer is critical, so in case of any cyber danger (DoS attack), it is recommended to unplug the cable from the primary system.
- Safeguarding this layer needs bio-metric security, camera-based surveillance, key cards, and other physical monitoring.
- Data Link Layer comprises of data packets transported from the physical layer. Any malfunctioning in this layer or data breach can impede the working of the network layer. Vulnerabilities that can be used and attacks that can be made in this layer are MAC address spoofing and virtual-LAN circumvention.

Relevance of the OSI layer model to computer forensics:

- So for protecting your system, common security mechanisms are MAC address filtering, assessment of wireless applications, checking of proper data encryption standards.
- Network Layer is the last of the media layer and has an association with the real world. It deals with the addressing and routing of packets. IP address spoofing is one of the common attack of this phase. Strengthening this layer needs the techniques of firm anti-spoofing, proper implementation of firewalls and routing filters, and secure routing protocols.

The subsequent four layers are host layers:

- Transport Layer - comes under the logical layer, which helps in transferring variable-length data sequence. The reliability of this layer can be achieved by ensuring the segmentation and de-segmentation mechanism and error control. For security purposes, this layer needs an appropriate firewall, restrictive admission of transmission protocols, and appropriate port number.
- Session Layer - essentially manages the inter-system communication and sessions. The handling of local and remote application's interaction is done in this layer. In case of weak authentication methods, it can help attackers to perform a brute force. So the effective way of securing this layer is by ensuring appropriate encrypted key exchange, along with the restriction of unsuccessful session attempts using timing methods.

The subsequent four layers are host layers:

- Presentation Layer - is used to standardize data with the help of various conversion schemes. But if there is poor conduct of malicious input, it can help cybercriminals exploit the system or even crash a system. Separate sanitized input and proper input validation can help protect the system from attackers.
- Application Layer - contain the UI and the closest of all layers for the user-end. The widest range of cyber-attacks and security breaches is possible in this layer. It can lead to shutting down the network, stealing data, crashing the application, manipulating the information sent from source to destination, and many more.

Forensics and social networking sites - security, privacy, threats

- There are a wide variety of threats stated below:
- A. Baits: In this mechanism keywords are used to make links and on this basis ranking of sites are done. Maximum social networks permit people to see what is stylish and hot at the moment. For example, Twitter lists the top trending topics on its home page which makes it easily available for attackers, who automatically take hot keywords and include them in their spam messages to get a better listing.
- B. Follower scams: With the rapid growth of importance of social networks people are more stressed to get people as more friends or followers as possible. In some social groups, acceptance of any person as a member of that group generally depends on his or her number of social connections. Generally school going students and college students are fascinated about it

Forensics and social networking sites - security, privacy, threats

- C. Impersonation of celebrities and friends: Many times, fake profiles of celebrities are seen on various social networks. Unfortunately there is no policy for stopping someone from registering a new account under the name of a celebrity or any one and similarly there are no policies for using a publicly available photo as a profile picture. In fact there are not real authentication that links a virtual profile to a real-life identity.
- D. Koobface: The W32.Koobface worm has been one of the first large malware attacks, targeting social networks for years, and it is still wide-spread and active today. It is very successful as it uses clever social engineering attacks and counts on the link-opening behaviour of social media users.

DIGITAL LEARNING CONTENT

Parul® University

www.paruluniversity.ac.in