Chapter 7. Digital forensics

Marta Fernández Diego

Index

- What is digital forensics?
- Sub-branches
- Computer experts
- Who uses computer forensics?
- Forensic methodology
- Expert report
- Types of cases
- Digital evidence
- Case study

What is digital forensics?

- The term forensics can be defined as the application of science to a matter of law.
- A branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime
- Originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data
- Wikipedia

What is digital forensics?

- Computer forensics involves the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis
- Information collected assists in arrests, prosecution, termination of employment, and preventing future illegal activity

How does the digital forensics process work?

- http://www.youtube.com/watch?v=nYrLwbBI_sE&feature=related

Sub-branches

- Relating to the type of digital devices involved:
  - Computer forensics
  - Database forensics
  - Mobile device forensics
  - Network forensics
  - Forensic video
  - Forensic audio

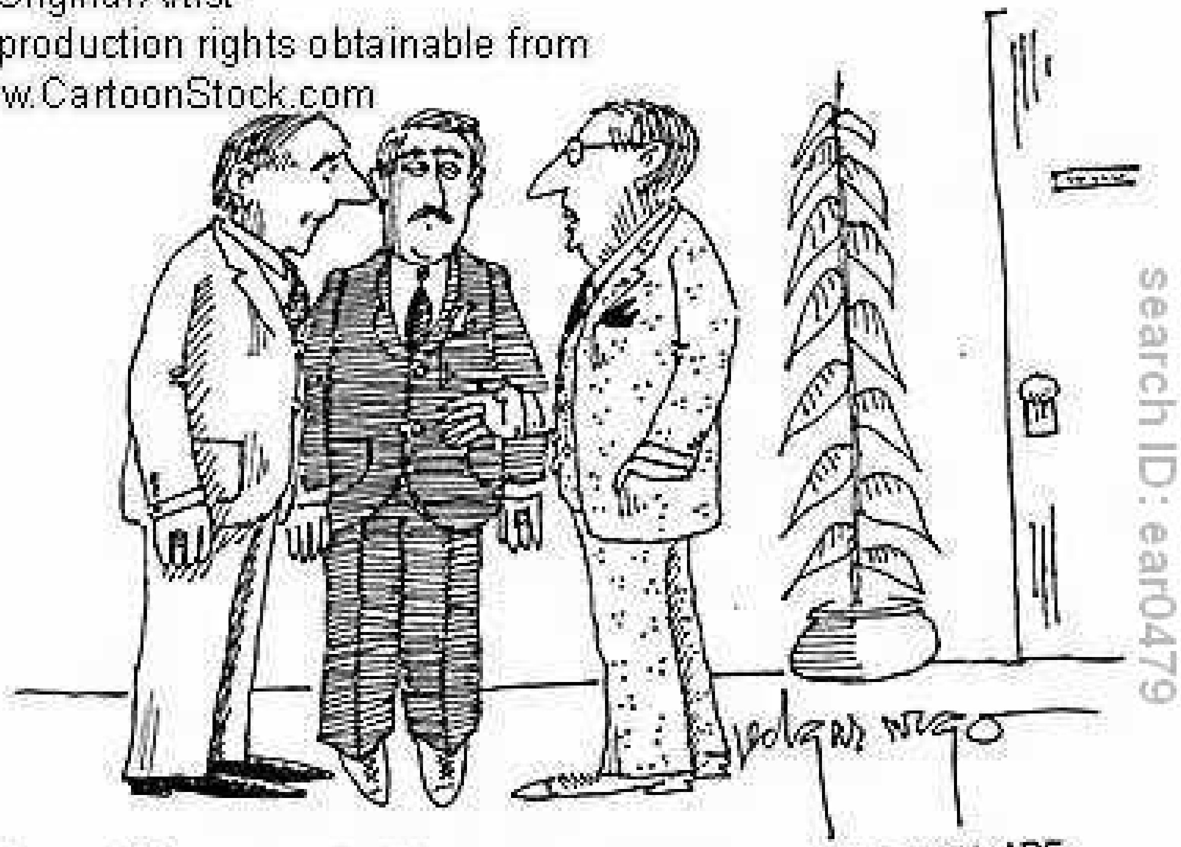
Basic approach

- Process to answer questions about digital states and events
  - Process of searching and analyzing
- Examples
  - An employee is suspected of violating a company's Internet-usage policy.
  - A hard disk is found in the house of a suspected terrorist.
  - Abnormal logs are observed on a server – a security breach is suspected.

Digital evidence management

- http://www.youtube.com/watch?v=y_BLtefQv40&feature=related

Computer experts



"TOO MANY PEOPLE ARE TRYING TO CONVINCE ME THAT THEY ARE COMPUTER EXPERTS WHEN THEY SHOULD BE CONVINCING THE COMPUTER."

How to become a computer expert?

- Take a computer course
- Make sure you have a computer
- Be prepared to fix
  - Every time your computer goes wrong, resign yourself to fixing it yourself.
- Don't be afraid of your computer!
- When fixing other people's computers, be sure to bring a flash drive with the software you will possibly need
- Read tech support forums to recognize the symptoms of well known problems
- http://www.wikihow.com/Become-a-Computer-Expert

Computer experts
Warnings

- Being a Computer Expert is a life long process. If you are genuinely not interested in Computer, don't try to be. It will cause more loss than profit.
- Go for it if and only if, Computer is your passion and Love.
- Make sure you're not going to make any computer problem worse by having some knowledge of it before you fix your neighbors PC.
- Don't fiddle with settings on a perfectly working family computer. Have an old 128mb RAM basic tower that your friends scrapped years ago to do that with! Then mess around until your heart is content!
- http://www.wikihow.com/Become-a-Computer-Expert

Computer forensic tools

- http://www.youtube.com/watch?v=zO4xeQvStQs&feature=related

Applications

- To support or refute a hypothesis before criminal or civil (as part of the electronic discovery process) courts
- In the private sector, such as during internal corporate investigations or intrusion investigation
- Wikipedia

Who uses computer forensics?

- Criminal Prosecutors
- Civil Litigations
  - Fraud, divorce, harassment, or discrimination cases
- Insurance Companies
  - Fraud, worker’s compensation, arson
- Private Corporations
  - Harassment, fraud, and embezzlement cases
- Law Enforcement Officials
  - Backup search warrants and post-seizure handling
- Individual/Private Citizens
  - Claims of harassment, abuse, or wrongful termination from employment

Forensic methodology

- The three A's
  - Acquire
    - Do not alter or damage the original
    - Preserve the state of the computer (the crime scene)
  - Authenticate
    - Proof that your recovered evidence is the same as the original
  - Analyze
    - Inspect evidence without altering it
    - Use evidence to reconstruct events

Digital forensics process
http://www.ntcforensics.com/process.htm

- Gather as much information about the project as possible
  - What are the specific goals of this forensic examination?
  - Which devices or media are to be examined?
  - Will the imaging of the devices be performed in the lab or in the field?
  - Have the proper steps been taken to insure the legality of the examination?
  - What other information is known about the situation?
  - Who is authorized to receive the results of the examination?

Acquisition

- Acquisition of a forensically sound, verifiable image of each computer, drive, server or other device.
- This is done using hardware write blockers appropriate to the device, forensically sound software tools, and established acquisition procedures.

Analysis process

- Always performed on the image and not the device, attempts to gather information and answer the questions indicated when the goals of the project were defined.
- This step is where data is recovered, evidence of activity is collected, and pieces of the overall puzzle are put together.
- Analysis results are often used to refine the scope and goals of the overall project or stimulate and support further examination.

Post-analysis report

- Details the results of all the preceding steps
- May also include deposition or court testimony to support the results as part of a court proceeding

Presentation of evidence

- Presentation of evidence discovered in a manner which is understood by lawyers, non-technically staff/management, and suitable as evidence as determined by laws
- http://www.youtube.com/watch?v=J41w3y2AEwM&feature=related
  - The judges and the lawyers are not computer experts
  - Take this computer jargon and serve exploitative in plain English

Legal document

YOU DON'T CALL THIS A LEGAL DOCUMENT DO YOU?
I CAN UNDERSTAND EVERY WORD OF IT!!
search ID: mfln4301
© Original Artist
Reproduction rights obtainable from
www.CartoonStock.com

Factors influencing the results

- How soon we are called after the initial incident
- If any other recovery procedures have been attempted
- The condition of the hardware/software involved
- If someone has tried to hide or destroy evidence or data
- The amount of information that is provided before we start
- http://www.ntcforensics.com/process.htm

Expert report

- A study written by one or more experts that states findings and offers opinions
- In law, expert reports are generated by expert witnesses offering their opinions on points of controversy in a legal case, and are typically sponsored by one side or the other in a litigation in order to support that party's claims.
- The reports state facts, discuss details, explain reasoning, and justify the experts' conclusions and opinions.

Digital expert report

- One important aspect of Digital Forensics is reporting.
- The report may include something similar to:
  - An overview/case summary
  - Forensic acquisition & exam preparation
  - Findings and report (i.e., forensic analysis)
  - Conclusion
- http://computer-forensics.sans.org/blog/2010/08/25/intro-report-writing-digital-forensics/

Report template

- Executive Summary
- Objectives
- Computer Evidence Analyzed
- Relevant Findings
- Supporting Details
- Investigative Leads
- Additional Report Sections

Report template

- Executive Summary
  - Author, investigators, examiners
  - Why was the investigation undertaken?
  - List significant findings
  - Include signatures of examiners
- Objectives
  - Tasks of the investigation
- Computer Evidence Analyzed
  - Detailed description of evidence
  - Linked with evidence tags
  - If possible, with digital imagery of evidence

Types of cases

- Copyright infringement
- Industrial espionage
- Money laundering
- Piracy
- Sexual harassment
- Theft of intellectual property
- Unauthorized access to confidential information
- Blackmail
- http://www.expertlaw.com/library/forensic_evidence/computer_forensics_101.html

Types of cases

- Corruption
- Decryption
- Destruction of information
- Fraud
- Illegal duplication of software
- Unauthorized use of a computer
- Child pornography
- http://www.expertlaw.com/library/forensic_evidence/computer_forensics_101.html

Digital evidence

- Any information being subject to human intervention or not, that can be extracted from a computer
  - Must be in human-readable format or capable of being interpreted by a person with expertise in the subject
  - Might be required for a wide range of computer crimes and misuses
- What types of media hold digital evidence?
  - Hard disks, CD's, DVD's, floppies
  - PDA's, compact flash, zip disks, jazz disks
  - Backup tapes, copiers, printers, scanners, cell phones

Case study from Global Digital Forensics

- Scenario
  - Two employees and a manager left a large chemical manufacturing company with offices and facilities in New York, New Jersey, Texas, China and Argentina. The two employees and the manager had emailed a customer contact database, invoicing information, financial data and proprietary information to their home computer in an attempt to steal intellectual property. The employees believed they were untraceable since they emailed the information to their home computers and deleted the emails. The allegations were firmly denied. The company receiving the information denied having any knowledge of the transfer or the existence of the information acquired from the clients company.
- How would you defeat forensic analysis?