University of Oslo
INF3510 Information Security
Spring 2018
Workshop Questions and Answers

Lecture 07: Digital Forensics and Incident Response

Question 1

a. How can somebody working in a company know what to do when he/she discovers a security incident ?
b. What are the main elements of an IR Policy (Incident Response Policy) ?
c. Describe the 3 main types of IR teams.

Answer

a. A security policy / IR policy defines what staff should do when they discover a security incident.
b. The IR policy should (at least) include the following elements:
   - Contact points for reporting incidents
   - Responsibility
     - Who makes the decisions about courses of action when responding to an incident?
   - Asset Priority
     - Which systems can be taken offline?
     - Which systems can absolutely not be taken offline?
   - Outside Experts and Agencies
     - Who you gonna call?
     - At what point is Law Enforcement involved?
c. The three main IR team types are:
   - Permanent IR team: A group of people working 100% on IR
   - Virtual IR team: IR team members normally do other jobs, but step in to do IR in case of incidents.
   - Hybrid IR team: Some IR team members are permanent, and other step in when needed.

   All team types can be combined with assistance from external experts/consultants.

Question 2

The following are steps of the incident response process. Briefly explain each concept and provide a Norwegian translation. The steps can often be executed in parallel.

a) Triage
b) Investigation
c) Containment
d) Analysis
e) Tracking
f) Recovery

Answer

a) Triage:
   Triage is the initial assessment of an incident to determine its severity, to prioritise resources and to set the direction for further action.
   Norwegian: Sortering og prioritering
b) Investigation
   Detect and collect evidence. Apply principle of OOV (Order of Volatility) to collect most volatile evidence first. Follow principles for chain of costody to allow the evidence to be admissible in court, in case that is needed.
   Norwegian: Undersøkelse, innhenting og sikring av bevis
c) Containment:
   Stop the attack from propagating to limit further damage. Use judgement to determine whether servers, applications and systems should be shut down and disocnnected, or be left running. It might be necessary to keep some systems running to support important business applications.
   Norwegian: Skadebegrensing
d) Analysis:
   Determine source and nature of incident. Answer: who, how, when and why. Police should be called when the incident has characteristics of serious crime. Consider the consequence of calling the police, e.g. loss of control and seisure of equipment.
   Norwegian: Analyse.
e) Tracking:
   Discovering the original source and cause of the incident when that is not immediately evident. This might involve collecting evidence from across networks and across the Internet. Collaboration with other organisations might be needed.
   Norwegian: Sporing
f) Recovery:
   Clean infected systems, patch servers, restore from backups, reconfigure perimeter security, remove vulnerable services, train staff, and implement any other control necessary for avoding similar incidents in the future. Learn from the incident and improve incident response process.
   Norwegian: Gjenoppretting

Question 3

Briefly explain and provide a Norwegian translation for the following terms:

a) Forensics
b) Digital Forensics
c) Computer Forensics
d) Network Forensics
e) Electronic data discovery
f) Cyber Forensics
g) Computational Forensics

Answer

a) Forensics:
   Application of a broad spectrum of sciences to answer questions of interest to a legal system. This may be in relation to a crime or a civil action. “Forensic” Comes from the Latin “forēnsis”, meaning “before the forum”, i.e. presented to a forum of judges.
   Norwegian: Etterforskning, Kriminaltekniske metoder
b) Digital Forensics:
   Recovery and investigation of material and legal evidence found in digital devices, often, but not necessarily, related to computer crime.
   Norwegian: Digital etterforskning, Digitale kriminaltekniske metoder
c) Computer Forensics:
   Recovery and investigation of material and legal evidence found in computers and digital storage media used with computers.
   Norwegian: Etterforskning på datamaskiner
d) Network Forensics:
   Monitoring and analysis of computer network traffic for the purposes of gathering legal evidence and information about events, or for intrusion detection. Unlike other areas of digital forensics, network forensics deals with volatile and dynamic information. Network traffic is transmitted and then lost, so network forensics is often a pro-active investigation.
   Norwegian: Etterforskning i datanett.
e) Electronic data discovery:
   eDiscovery refers to any process in which electronic data is sought, located, secured and searched with the intent of using it as evidence in a civil or criminal legal case. Electronic data includes emails, images, calender files, spreadsheets and audio files.
   Norwegian: Etterforskning av elektronisk dokumenter
f) Cyber Forensics:
   Cyber forensics is a general term covering the more specific topics of computer forensics and network forensics. It can be interpreted equivalent to digital forensics, but puts more focus on global aspects of forensics. The term is often used to describe courses, training programs and certifications.
   Norwegian: Cyberetterforskning, Etterforskning i cyberrommet
g) Forensic computing, or Computational Forensics:
   Quantitative approach to the methodology of the forensic sciences. It involves computer-based modeling, computer simulation, analysis, and recognition in studying and solving problems posed in various forensic disciplines. CF integrates expertise from computational science and forensic sciences.
   Norwegian: Digitale etterforskningsmetoder, Computerstøttet etterforskning

Question 4

Evidence integrity is essential in order for digital evidence to be admissible in court and to carry weight as evidence.

a. What is CoC (Chain of Custody) and why is it important for evidence integrity?
b. Assuming that a forensic team follows the right steps for preserving evidence integrity and for keeping an unbroken CoC, what must they do in order to convince the court that they have done so?
c. What is OOV (order of volatility), and how does it influence decisions regarding which evidence should be preserved first?
d. List various data storage media as a function of their OOV.

Answer

d. Chain of custody (CoC) refers to the chronological documentation or paper trail, showing the seizure, custody, control, transfer, analysis, and disposition of evidence, physical or electronic. Because evidence can be used in court to convict persons of crimes, it must be handled in a scrupulously careful manner to avoid later allegations of tampering or misconduct which can compromise the case of the prosecution toward acquittal or to overturning a guilty verdict upon appeal.
e. Document it.
f. Data stored on media can be modified or erased due to various factors. The volatility expresses the rapidity and ease with which such factors can modify or erase data. The OOV expresses the relative ranking of media according to volatility.
g. OOV of various media: Microprocessor registers, microprocessor cache, RAM, HD cache, HD, peripheral memory (R/W), Write once media.

Question 5

a. Explain the difference between “live acquisition” and “post mortem acquisition”.
b. What are the advantages and disadvantages of live and post mortem acquisition?
c. Give an example when “live acquisition” is necessary.

Answer

a. In case of live acquisition, the evidence is collected from a system where the microprocessor is running. In case of post mortem acquisition, the evidence is collected from storage media of a system that is shut down.
b. Post mortem provides better integrity preservation and does not influence the data. However, volatile data can be lost in the process of shutting down a system. Live acquisition enables the collection of volatile data, but also influences the data.
c. In case the HD is encrypted, it is better to collect the data from the HD while it is running.

Question 6

Explain the basic steps of the forensic investigation process.

Answer

1. **Identification**
   Discovering the incident
   «My computer is acting weird»
   «Someone just posted our entire database on wikileaks»
2. **Preservation**
   Make sure that the evidence is not destroyed - «Do not turn that off»
3. **Collection**
   Gathering all the potential evidence in a forensic manner - Volatile data first - RAM, then disks - Use write blockers, create multiple images, one image is kept as «master»
4. **Examination**
   Find and extract hidden and deleted files and partitions
5. **Analysis**
   Use two tools to verify results – the steps MUST be repeatable
   Create timelines of events
6. **Presentation**
   Presenting the evidence to the court

Question 7

Explain the basic scientific principles for the forensic investigation process.

Answer

1. **Best evidence**
   Obtain the best possible evidence. Preferably, the original, if not, then a clone and so on.
2. **Minimal Intrusion**
   Only seize what is necessary, only keep for as long as necessary
3. **Minimal Force**
   Do not use excessive force to gain access to the evidence
4. **Minimal Interruption**
   Do not interrupt the business unnecessarily
5. **Transparency**
   All the evidence is revealed to the court, no steps taken are secret
6. **Chain of Custody**
   Document how the evidence was kept and who had access to the evidence
7. **Primacy of the Mission**
   Focus on the mission, despite interesting sidetracks. Note them and move back if necessary
8. **Impartiality**
   Do not evaluate evidence with the focus of proving one or the other. Let it speak for itself
9. **Documentation**
   Document everything. When, what, why. Both to provide to the court, and to remember. Often a long time between operation and trial.