QUIZ FORENSICS Preparation instructions

General

As with all the quizzes in this course you have to answer 7 out 10 questions in order to pass the test. When preparing yourself read the slide sets Lect 7, study the Altheide video, and the

- Altheide Video The death of computer forensics
- Forensics of mobile phone internal memory: by Svein Y. Willassen. Norwegian University of Science and Technology

There are a lot of (new) terms so it is good that you read through the slides so you know where in the lecture slides things can be found. Below we walk through the different parts material above. In particular, you find items and questions that are useful to study. Numbers to the Altheide video give are time indicators of a relevant sequence in the video.

A good trick is to go through these items and questions with a colleague and ask him/her for explanations and check each other's answers.

general:

Computer vs data forensics: same or not?

Computer/data forensics results are used by?

Computer/data forensics is about?

Which are the 4 main steps in data forensics?

Data forensics is not?

Use of hashes to detect changes of seized data, why?

Types of data forensics?

What is CERT? CERT in Sweden.

Incident handling:

Incident handling terms (4)

Incident Handling is a process

Even correlation, what is it?

Chain of custody

"If it is on, leave it on – if it is off, leave it off." Why?

Analyzing documents/pictures:

Importance of metadata

Analyzing memories

Volatile and non-volatile memories.

Cooling down of RAM, why?

Slack and wasted space of non-volatile storage

Where can data be found: allocated space, slack space, or both?

File allocation: basic, deletion, slack space: (see Altheide video 23:50-26:50)

Allocation in Flash (SSD). Pages, : (see Altheide video 27:50-32:40)

Problems with flash: wear leveling (28:50), deletion(30:00)

Forensics of devices/phones (see Altheide video 51:40-57:00)

Cloud systems and computers/devices: storage is in cloud. Consequence for forensics, cloud forensics (see Altheide video 57:00-1:15:00)

Mobile phone memory analysis

Storage data on SIM vs storage on device own memory (sec 2.1, 2.2)

How to prevent memory contamination?

How to obtain an image: desoldering, jtag reading

What is jtag (Google , for example http://www.corelis.com/education/JTAG_Tutorial.htm or first pages of http://www2.lauterbach.com/pdf/training_jtag.pdf)

Data hiding

Steganography: meaning?

Use of encryption as part of hiding.

Watermarking: meaning?

Use of spread spectrum technology.

Data hiding terms: embedding, robustness

Magic triangle: tradeoffs

Detecting of hidden data vs extraction of hidden data: why is extraction not possible even if it is detected?