# 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 1, and study

- Altheide Video The death of computer forensics
- Forensics of mobile phone internal memory: by Svein Y. Willassen. Norwegian University of Science and Technology
- A Hierarchical, Objectives-Based Framework for the Digital Investigations Process, Nicole Beebe, Jan Clark, DFRWS 2004

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 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 Digital forensics: same or not?

Computer/Digital forensics results are used by?

Computer/Digital forensics is about?

Which are the 4 main steps in Digital forensics?

Digital forensics is not?

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

Which types of Digital 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, what is it?

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

**File systems**

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

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

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

Basics of how FAT is organized, sectors, heads, cluster, FAT table,

Analyzing Volatile and non-volatile memories.

Cooling down of RAM, why?

Slack and wasted space of non-volatile storage?

Three ways to organize memory blocks, reason about pros and cons, and which approach uses FAT.

**Analyzing documents/pictures:**

Importance of metadata.

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

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**

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

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

How to prevent memory contamination?

IMEI and IMSI, what is it?

Why is IMEI useful when prepaid SIM cards are used?

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 )

What is boundary scan?

**Data hiding**

Steganography: meaning?

Use of encryption as part of hiding.

Watermarking: meaning?

Use of spread spectrum technology.

EITN50-Quiz 1 preparation instructions Ben Smeets, 2021-09-03

Data hiding terms: embedding, robustness

Magic triangle: tradeoffs involved when constructing information hiding schemes.

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