EXAM
TTM2 – Information security, advanced

Technical Tools/Aid: None
Duration: 0900 – 1200 (3 hours)
Contact person: Svein Willassen, ph. 92449678

Part 1

This part consists of 8 questions. Each question can give up to 8 points. Maximal number of points in this part of the exam is 64. Time for work on this part of the exam: ~120 minutes.

1. Explain what is understood with *Maintaining Professional Conduct* in the context of Computer Investigation and Forensic Analysis.

2. Explain what is meant with a *bit stream copy*. Name at least three different tools that can be used to make a bit stream copy.

3. Describe the properties of different forensic file formats. What is the *Advanced Forensic File Format*?

4. Explain what *dcfldd* is. What is the name of the standard version of this tool and how do these versions differ?

5. What is meant with *validating acquired data*? Name at least two different algorithms that can be used for validation of acquired data.

6. What is *keyword search* and *data carving*? Give examples of case types where these techniques may be useful.

7. Explain what is meant with *slack space*. Name two different kinds of slack space and explain where they occur on a hard disk.

8. What is a *virtual machine* and which role can it play in Digital Forensics?

Part 2

This part consists of 20 questions. For every question 5 alternative answers are given, of which ONLY ONE is correct. If you chose the correct answer you will earn 1.8 points, otherwise you will loose 0.4 points (i.e. the penalty is -0.4 points). If you not choose any answer - then you will not get any points (i.e. the earned points are 0). Maximal number of points in this part of the exam is 36. Time for work on this test: ~60 minutes.

1. **Encrypting File System (EFS)** is a feature in
    a. the FAT file system
    b. the NTFS file system
    c. the EXT3 file system
    d. the REISERFS file system
    e. the UFS file system

2. **FAT** is an acronym for
    a. File Address Table
    b. Files And Tables
    c. File Acronym Table
    e. File Allocation Table
    f. File Attribute Table

3. The difference between **FAT16** and **FAT32** is
    a. FAT16 can only be installed on floppy disks
    b. FAT16 can only be installed on flash drives
    c. FAT16 can only be installed on small hard disks
    d. the size of the sector address
    e. the size of the cluster address

4. When a file is deleted in the FAT file system
    a. the first character in the file name is overwritten but the rest is recoverable
    b. neither file name and file content is recoverable
    c. file content may be recoverable but not the file name
    d. the file name may be recoverable but not the file content
    e. anything can be recovered, but only by magnetic analysis of the disk

5. File timestamps in NTFS are contained in
    a. the file entry in the Master File Table
    b. the file entry in the FAT
    c. the file Inode entry
    d. $Logfile
    e. the file nonresident data run

6. In NTFS, data content for a **resident file** is stored
    a. in multiple data runs on the disk
    b. in the file entry in the MFT
    c. inside the file system metadata
    d. within the file inode entry
    e. anywhere inside the file system

7. Criminal Investigation and Prosecution in Norway is regulated in
    a. the Penal Code
    b. the Investigation and Prosecution Act
    c. the Disputes Act
    d. the Criminal Procedure Act
    e. the Personal Data Act

8. A written search order can be issued by
    a. anyone
    b. the police
    c. the Prosecution Authority
    d. the court
    e. the court and in some cases the Prosecution Authority

9. **Lawful interception** may involve
    a. analyzing a seized mobile phone
    b. reading email and chat logs on a seized computer
    c. intercepting screen content by looking through the suspect's window
    d. wiretapping of phone conversations and data communication
    e. intercepting the currently talking lawyer by expressing an objection

10. Information about who used an IP-address at a specific time can be obtained by
    a. anyone by request to the ISP
    b. the police by court order only
    c. the police by request to the ISP
    d. any lawyer by request to the ISP
    e. the Data Inspectorate by request to the ISP

11. An expert in digital forensics appearing in court in Norway must qualify
    a. requirements set forth in the Disputes Act
    b. requirements set forth by the Justice Department
    c. requirements set forth by the Data Inspectorate
    d. requirements set forth by the Norwegian Computer Association
    e. There are no formal qualification requirements to appear as expert in Norwegian courts.

12. Pursuant to the CPA Section 199a Norwegian police can during a search instruct
    a. the system administrator of the computer system to assist but no one else
    b. anyone who has knowledge of the computer system to assist, including the suspect
    c. anyone who has knowledge of the computer system to assist, excluding the suspect
    d. any individual approved by the Data Inspectorate to assist
    e. any individual approved by the court to assist

13. The police can obtain CDR records from telecommunication networks
    a. by obtaining a court order ordering handover of communication records
    b. by installing a covert wiretap without informing the provider
    c. by extracting the records from the National CDR register
    d. only after the EU Data Retention Directive has been implemented in Norway
    e. only by obtaining a search order ordering a search of the provider's office

14. Attaching to a suspect's ADSL connection and storing passing data constitutes
    a. search
    b. seizure
    c. prosecution
    d. lawful interception
    e. not possible in a legal way

15. The following email can be classified as **exculpatory evidence**:
    a. an email that has been obtained by computer intrusion
    b. an email that indicates that the suspect is innocent
    c. an email that indicates that the suspect is guilty
    d. an email from the suspect to his lawyer
    e. an email where the suspect writes that he knew he was being investigated

16. The following email is exempt from being presented as evidence in Norwegian courts:
    a. a secret email from a perpetrator to his accomplices
    b. an email from a perpetrator to his wife
    c. an email from a perpetrator to his mistress
    d. an email from a perpetrator to his attourney
    e. an email from a perpetrator to his boss

17. The EU Data Retention Directive

    a. is currently not supported by Norwegian legislation at all and there is no plan to support it.

    b. is supported by the Electronic Communications Act, but no regulations have yet been given that details its implementation.

    c. is implemented in the Electronic Communications Act and detailed in the Electronic Communications regulation

    d. is currently not supported by Norwegian legislation at all, but there are plans to introduce it.

    e. is not relevant for Norway under the EEA agreement

18. In criminal matters, the burden of proof standard applied when deciding on guilt is

    a. weighted probability

    b. probable cause

    c. reason to believe

    d. general preponderance of the evidence

    e. beyond reasonable doubt

19. **Opinion shopping** involves

    a. an attourney obtaining opinions from witnesses in court

    b. taking of evidence in a pre-trial court hearing

    c. a police officer looking for the best opinions to match his preconceptions

    d. an attourney looking for an expert to testify on an opinion supporting his case

    e. a forensic examiner looking for differing opinions on a technical problem

20. An **expert witness** is different from a **technical witness** in that

    a. an expert witness has at least a Master's degree in Digital Forensics

    b. an expert witness is allowed to decide the case in cooperation with the judge

    c. an expert witness is allowed to render an opinion based on education, training and experience

    d. an expert witness is allowed to testify on technical details

    e. an expert witness is allowed to appear in both criminal and civil cases