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. What is the relationship between Computer Forensics and Digital Security?

2. Explain the term *Data Recovery*. How is it different from Computer Forensics?

3. Describe what steps should be taken to prepare for a computer search and seizure.

4. What are the challenges associated with acquiring evidence from a RAID array? Explain at least two different ways to perform data acquisition from a RAID array.

5. What is a *digital hash* and why is it useful in Computer Forensics? Name at least two common hashing algorithms.

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

7. What is a write-blocker and why is it useful in Computer Forensics?

8. What is the difference between a *technical witness* and an *expert witness*?

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. **Sleuth Kit** is
    a. an evidence locker
    b. a system for acquiring evidence from mobile phones
    c. a forensic analysis tool for Linux
    d. a forensic workstation
    e. a root kit

2. **dcfldd** is
    a. a tool for analysis of dumped data
    b. DC Forensic Laboratory Digital Detective
    c. a tool for analysis of slack space
    d. a forensic version of the tool dd.
    e. a professional organization for computer forensic investigators

3. **Exculpatory evidence** is
    a. evidence that might clear the suspect
    b. incriminating evidence
    c. evidence presented outside the courtroom ("*ex culpa*")
    d. illegally acquired evidence
    e. legally acquired evidence

4. In NTFS, a **nonresident file** is
    a. a file stored on a non-NTFS file system
    b. a file where the data content is stored outside the main partition
    c. a file where the data content is stored in the main partition
    d. a file where the data content is stored outside the MFT
    e. a file where the data content is stored in the MFT

5. In NTFS, a **data run** is
    a. a part of a file stored in consecutive clusters
    b. an executable file
    c. the part of the MFT file entry with actual data content
    d. part of the file system not occupied by the MFT
    e. metadata in the MFT entry

6. The following is *not* an existing tool for Digital Forensics
    a. EnCase
    b. AccessData Forensic Toolkit
    c. X-Ways Forensics
    d. ProDiscover
    e. Daubert Digital Investigator

7. The **Computer Forensic Tool Testing (CFTT)** project is sponsored by
    a. American Bar Association
    b. International Society of Forensic Computer Examiners
    c. Interpol European Working Party for IT Crime
    d. National Institute of Standards and Technology
    e. Guidance Software

8. The MFT in NTFS does *not* contain
    a. File content
    b. File timestamps
    c. the Master Boot Record
    d. File names
    e. Directory content

9. **MD5-hashes** might be used to
    a. Identify illegal images on a suspect drive
    b. Verify the integrity of an image file
    c. Identify known good files, i.e. Operating System files
    d. Testing lossless compression
    e. All of the above

10. The following is exempt from evidence in Norway

    a. An engineer's notes
    b. A physician's records
    c. A police report
    d. Court records
    e. E-mail

11. In Norway, **search** can be carried out if

    a. There is probable cause that the suspect committed an offence that might result in more than 6 months imprisonment.
    b. There is probable cause that the suspect committed an offence that might result in imprisonment.
    c. There is probable cause that the suspect committed an offence that might result in more than 1 year imprisonment.
    d. There is reason to believe that the suspect committed an offence that might result in more than 6 months imprisonment.
    e. It is possible that the suspect committed an offence that might result in more than 6 months imprisonment.

12. **Lawful interception** may not involve

    a. Recording phone calls
    b. Intercepting e-mail
    c. Storing visited web sites
    d. Recording keystrokes on a computer
    e. Recording peer-to-peer traffic

13. Digital evidence obtained by the Norwegian police without court order can be sent to the police in another country

    a. directly
    b. only through the letter rogatory procedure
    c. only after getting a court order allowing it
    d. through Interpol only
    e. only if the Justice Department approves

14. The main rule in the CPA section 197 states that

    a. the police must get a court order to conduct a search
    b. the prosecution authority can order a search

c. a police office can order a search

d. the Data Inspectorate can order a search

e. the Justice Department can order a search

15. Lawful interception may be implemented during investigation of
    a. any offence
    b. all offences that might result in more than 3 years imprisonment
    c. all offences that might result in more than 6 years imprisonment
    d. all offences that might result in more than 10 years imprisonment
    e. all offences that might result in more than 10 years imprisonment and certain other offences

16. The defence counsel is entitled to receive
    a. copies of all investigation material, including digital material
    b. copies of all investigation documents, but not digital material
    c. only copies of interviews and certain other documents
    d. only copies of evidence to be presented in court
    e. only material that the police want to hand over

17. Information about which user used an IP-address can be delivered to
    a. the police only if there is a court order
    b. the police only if there is an order from the prosecution authority
    c. the police, by written request
    d. The Data Inspectorate
    e. The Norwegian Computing Association

18. In a legal context, **Data Retention** primarily implies
    a. requiring the opposing party in a civil case to retain certain data
    b. requiring the police to retain seized files
    c. requiring storage providers to always store data for a certain time period for use as evidence
    d. requiring communication providers to always store data for a certain time period for use as evidence
    e. requiring defence counsel to retain stored files

19. Maintaining a professional CV is useful for forensic investigators because
    a. it is nice to have when applying for jobs

b. it can be used to qualify the experience at expert testimony
c. it should be attached to all forensic reports
d. it is necessary to obtain a court order
e. it is required to be registered as an expert witness by the Justice Department

20. During an investigation, a forensic investigator should
a. have regular contact with news media
b. provide only crucial evidence to news media
c. avoid contact with news media
d. only send written statements to news media
e. only deal with news media orally