EKSAMEN
TTM2 – Informasjonssikkerhet, videregående

Hjelpemidler: Ingen
Varighet: 0900 – 1200 (3 timer)
Kontaktperson: Svein Willassen, tlf. 92449678

Del 1

Denne delen består av 8 spørsmål. Hvert spørsmål kan gi opp til 8 poeng. Maksimalt antall poeng som kan oppnås på denne delen er 64. Anslått tid for arbeid med denne delen: 120 minutter.

1. Forklar hva som menes med å *opprettholde en profesjonell framferd* i forbindelse med dataetterforskning.

2. Forklar hva som menes med en *bitstrømkopi.* (*bit stream copy*) Nevn minst tre ulike verktøy som kan benyttes til å lage en bitstrømkopi.

3. Beskriv egenskapene ved ulike fil format for speilfiler. Hva er *Advanced Forensic File Format*?

4. Forklar hva *dcfldd* er. Hva heter standardversjonen av dette verktøyet og hvordan er de to utgavene forskjellige?

5. Hva menes med *validering av sikrede data*? Nevn minst to ulike algoritmer som kan brukes til å validere sikrede data.

6. Hva er *nøkkelordsøk (keyword search)* og *datautskjæring (data carving)*? Gi eksempler på sakstyper hvor disse teknikkene kan være nyttige.

7. Forklar hva som menes med *slakkområder*. Nevn to ulike typer slakkområder og forklar hvor de befinner seg på en harddisk.

8. Hva er en *virtuell maskin* og hvilken rolle kan den spille i dataetterforskning?

Del 2

Denne delen består av 20 spørsmål. For hvert spørsmål er det gitt 5 alternative svar. Kun ett av disse er korrekt. Korrekt svar gir 1.8 poeng. Feil svar gir -0.4 poeng. Hvis du velger å ikke svare blir det 0 poeng på det spørsmålet. Maksimalt antall poeng som kan oppnås på denne delen er 36. Anslått tid for arbeid med denne delen: 60 minutter.

1. **Encrypting File System (EFS)** er en funksjon i
    a. FAT-filsystemet
    b. NTFS-filsystemet
    c. EXT3-filsystemet
    d. REISERFS-filsystemet
    e. UFS-filsystemet

2. **FAT** er en forkortelse for
    a. File Address Table
    b. Files And Tables
    c. File Acronym Table
    e. File Allocation Table
    f. File Attribute Table

3. Forskjellen melleom **FAT16** og **FAT32** er
    a. FAT16 kan bare installeres på disketter
    b. FAT16 kan bare installeres på flash-disker
    c. FAT16 kan bare installeres på små harddisker
    d. størrelsen på sektoradressen
    e. størrelsen på cluster-adressen

4. Etter å ha slettet en fil i FAT-filsystemet
    a. blir det første tegnet i filnavnet overskrevet men resten kan rekonstrueres
    b. er hverken filnavn eller innhold mulig å rekonstruere
    c. er innhold mulig å rekonstruere men ikke filnavn
    d. er filnavn mulig å rekonstruere men ikke innhold
    e. er det mulig å rekonstruere alt, men bare ved magnetisk analyse av disken

5. Tidsstempler i NTFS finnes i
    a. filens innslag i Master File Table
    b. filens innslag i FAT
    c. filens inode
    d. $Logfile
    e. filens ikke-residente dataløp

6. I NTFS er datainnhold for en **resident fil** lagret
    a. i flere dataløp på disken
    b. i filens innslag i MFT
    c. inni filsystemets metadata
    d. inni filens inode
    e. hvor som helst i filsystemet

7. Etterforskning og påtale av straffbare handlinger er i Norge regulert i
    a. straffeloven
    b. lov om etterforskning og påtale
    c. tvisteloven
    d. straffeprosessloven
    e. personopplysningsloven

8. En skriftlig ransakingsbeslutning kan utstedes av
    a. enhver
    b. politiet
    c. påtalemyndigheten
    d. retten
    e. retten og i noen tilfeller påtalemyndigheten

9. **Kommunikasjonskontroll** kan innebære
    a. å analysere en beslaglagt mobiltelefon
    b. å lese epost og chat-logger fra en beslaglagt datamaskin
    c. å kontrollere innhold på skjermen ved å se gjennom vinduet
    d. avlytting av telefonsamtaler og datakommunikasjon
    e. kontroll av talende prosessfullmektig ved å legge inn en protest

10. Informasjon om hvem som har brukt en IP-adresse på et bestemt tidspunkt kan utleveres
    a. til enhver ved forespørsel til leverandøren
    b. til politiet ved beslutning fra retten
    c. til politiet ved forespørsel til leverandøren
    d. til enhver advokat ved forespørsel til leverandøren
    e. til datatilsynet ved forespørsel til leverandøren

11. En sakkyndig i dataetterforskning som opptrer i norsk rett må tilfredsstille
    a. kvalifikasjonskrav gitt i tvisteloven
    b. kvalifikasjonskrav gitt av justisdepartementet
    c. kvalifikasjonskrav gitt av datatilsynet
    d. kvalifikasjonskrav gitt av den norske dataforening
    e. Det er ingen formelle kvalifikasjonskrav for å opptre som sakkyndig i norsk rett.

12. I henhold til straffeprosessloven §199a, kan politiet under ransaking pålegge
    a. systemansvarlig til å assistere, og bare denne
    b. enhver som kjenner datasystemet til å assistere, inkludert siktede
    c. enhver som kjenner datasystemet til å assistere, men ikke siktede
    d. enhver som er godkjent av datatilsynet til å assistere
    e. enhver som er godkjent av retten til å assistere

13. Politiet kan innhente CDR-data fra telekommunikasjonsnett
    a. ved å skaffe et utleveringspålegg fra retten
    b. ved å installere en hemmelig avlyttingsmekanisme uten å informere leverandør
    c. ved å hente ut data fra det nasjonale CDR-registeret
    d. bare etter datalagringsdirektivet er implementert i Norge
    e. bare ved å skaffe en beslutning om ransaking hos leverandøren

14. Å koble seg til siktedes ADSL-forbindelse og lagre data som passerer på denne er
    a. ransaking
    b. beslag
    c. påtale
    d. kommunikasjonskontroll
    e. ikke mulig å gjøre på en lovlig måte

15. Følgende epost kan karakteriseres som **ex-culpa-bevis**:
    a. en epost fremskaffet ved datainnbrudd
    b. en epost som indikerer at siktede er uskyldig
    c. en epost som indikerer at siktede er skyldig
    d. en epost fra siktede til hans advokat
    e. en epost hvor siktede skriver at han visste han var under etterforskning

16. Følgende epost er unntatt som bevis i norsk rett:
    a. en hemmelig epost fra gjerningsmannen til hans medsammensvorne
    b. en epost fra gjerningsmannen til hans kone
    c. en epost fra gjerningsmannen til hans elskerinne
    d. en epost fra gjerningsmannen til hans advokat
    e. en epost fra gjerningsmannen til sjefen

17. Datalagringsdirektivet
    a. er ikke gjort gjeldende i norsk lovgivning og det er ingen plan for å gjøre det
    b. støttes av ekomloven men det er ikke gitt noen forskrift som beskriver hvordan det skal implementeres
    c. er implementert i ekomloven og detaljert i ekomforskriften
    d. er overhodet ikke støttet av norsk lovgivning, men det er planer om å innføre det
    e. er ikke relevant for Norge under EØS-avtalen

18. I strafferetten anvendes følgende bevisbyrdestandard for avgjørelse av skyldspørsmålet
    a. vektet sannsynlighet
    b. skjellig grunn til mistanke
    c. grunn til å tro
    d. sannsynlighetsovervekt
    e. hinsides enhver rimelig tvil

19. **Shopping av vurderinger** involverer
    a. en advokat som innhenter vurderinger fra vitner i retten
    b. bevisopptak før hovedforhandling
    c. en politimann som ser etter vurderinger som passer hans forhåndsmistanke
    d. en advokat som ser etter en ekspert som kan gi en vurdering som passer med hans sak
    e. en dataetterforsker som ser etter avvikende vurderinger av et teknisk problem

20. Et **sakkyndig vitne** er forskjellig fra et **teknisk vitne** ved at
    a. et sakkyndig vitne har minst en mastergrad i dataetterforskning.
    b. et sakkyndig vitne har lov å bestemme sakens utfall sammen med dommeren
    c. et sakkyndig vitne kan gi sine egne vurderinger basert på utdannelse, kursing og erfaring
    d. et sakkyndig vitne kan forklare seg om tekniske detaljer
    e. et sakkyndig vitne kan forklare seg i både straffesaker og sivile saker