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. Hva er forholdet mellom dataetterforskning og IT-sikkerhet?

2. Forklar begrepet *datarekonstruksjon*. Hva er forskjellen på dette og dataetterforskning?

3. Beskriv hva som bør gjøres for å forberede ransaking og beslag i datamiljø.

4. Hva er utfordringene med å sikre bevis fra et RAID-sett? Forklar minst to ulike måter å sikre bevis fra et RAID-sett.

5. Hva er en *digital hash* og hvorfor er dette nyttig i dataetterforskning? Angi minst to ulike hash-algoritmer.

6. Forklar hva som menes med slakkområder. Angi to forskjellige typer slakkområder og forklar hvor disse er plassert på en harddisk.

7. Hva er en skriveblokker, og hvorfor er dette nyttig i dataetterforskning?

8. Hva er forskjellen på et *teknisk vitne* og et *sakkyndig vitne*?

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. **Sleuth Kit** er
    a. et bevislager
    b. et system for å sikre bevis fra mobiltelefoner
    c. et dataetterforskningsprogram for Linux
    d. en arbeidsstasjon for dataetterforskning
    e. et rootkit

2. **dcfldd** er
    a. et verktøy for å analyse datadumper
    b. DC Forensic Laboratory Digital Detektiv
    c. Et verktøy for å analysere slakkområder
    d. dataetterforskningsversjonen av verktøyet dd
    e. en organisasjon for dataetterforskere

3. **ex-culpa bevis** er
    a. bevis for siktedes uskyld
    b. inkriminerende bevis
    c. bevis som presenteres utenom retten ("*ex culpa*")
    d. ulovlig anskaffede bevis
    e. lovlig anskaffede bevis

4. I NTFS, er en **ikke-resident fil**
    a. en fil som er lagret på et ikke-NTFS filsystem
    b. en fil hvor datainnholdet er lagret utenfor primærpartisjonen
    c. a fil hvor datainnholdet er lagret på primærpartisjonen
    d. a fil hvor datainnholder er lagret utenfor MFT
    e. a fil hvor datainnholdet er lagret i MFT

5. Et **dataløp** i NTFS er
    a. del av fil som er lagret i påfølgende clustre
    b. en kjørbar fil
    c. den del av MFT filentry som inneholder datainnhold
    d. del av filsystemet som ikke opptas av MFT
    e. metadata lagret i MFT filentry

6. Følgende er *ikke* et eksisterende dataetterforskningsverktøy
    a. EnCase
    b. AccessData Forensic Toolkit
    c. X-Ways Forensics
    d. ProDiscover
    e. Daubert Digital Investigator

7. Prosjektet **Computer Forensic Tool Testing (CFTT)** utføres av
    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. MFT i NTFS inneholder *ikke*
    a. filinnhold
    b. tidsstempler på filer
    c. Master Boot Record
    d. filnavn
    e. innhold i kataloger

9. **MD5-hasher** kan brukes til å
    a. identifisere ulovlige bilder på en beslaglagt harddisk
    b. verifisere integriteten til en speilfil
    c. identifisere kjente filer, feks filer fra operativsystemet
    d. teste tapsfri kompresjon
    e. alle alternativene over

10. Følgende kan ikke føres som bevis i Norge
    a. notater skrevet av en ingeniør
    b. legejournaler
    c. en politirapport
    d. rettsdokumenter
    e. e-post

11. **Ransaking** kan i Norge gjennomføres dersom
    a. Siktede med skjellig grunn kan mistenkes for en straffbar handling som kan resultere i mer enn 6 måneders frihetsstraff.
    b. Siktede med skjellig grunn kan mistenkes for en straffbar handling som kan resultere i frihetsstraff.
    c. Siktede med skjellig grunn kan mistenkes for en straffbar handling som kan resultere i mer enn ett års frihetsstraff.
    d. Det er grunn til å tro at siktede har utført en straffbar handling som kan resultere i mer enn 6 måneders frihetsstraff.
    e. Det er mulig at siktede har utført en straffbar handling som kan resultere i mer enn 6 måneders frihetsstraff.

12. **Kommunikasjonskontroll** kan *ikke* gå ut på
    a. å ta opp telefonsamtaler
    b. å fange opp epost
    c. å lagre besøkte nettsteder
    d. å lagre tastetrykk på en datamaskin
    e. å lagre trafikk i fildelingsnettverk

13. Databevis fremskaffet av norsk politi uten rettslig beslutning kan sendes til politiet i et annet land
    a. direkte
    b. kun gjennom rettsanmodning
    c. kun dersom det blir tillatt av retten
    d. kun gjennom Interpol
    e. kun med godkjenning fra justisdepartementet

14. Hovedregelen i straffeprosessloven §197 sier at
    a. politiet må ha en beslutning fra retten for å foreta ransaking

b. ransaking kan besluttes av påtalemyndigheten
c. ransaking kan besluttes av en polititjenestemann
d. ransaking kan besluttes av datatilsynet
e. ransaking kan besluttes av justisdepartementet

15. Kommunikasjonskontroll kan gjennomføres som del av etterforskningen av
    a. enhver straffbar handling
    b. straffbar handling som kan medføre mer enn 3 års frihetsstraff
    c. straffbar handling som kan medføre mer enn 6 års frihetsstraff
    d. straffbar handling som kan medføre mer enn 10 års frihetsstraff
    e. straffbar handling som kan medføre mer enn 10 års frihetsstraff, samt enkelte andre straffbare handlinger

16. Siktedes forsvarer har rett til å motta
    a. kopi av alt etterforskningsmateriale, også digitalt materiale
    b. kopi av etterforskningsdokumentene, men ikke digitalt materiale
    c. kun kopi av avhør og enkelte andre dokumenter
    d. kun kopi av bevis som skal presenters i retten
    e. kun materiale som politiet ønsker å utlevere

17. Informasjon om hvilken bruker som har brukt en IP-adresse kan utleveres til
    a. politiet, kun ved beslutning fra retten
    b. politiet, kun ved belutning fra påtalemyndigheten
    c. politiet, ved skriftlig begjæring
    d. datatilsynet
    e. den norske dataforening

18. Med **datalagring**, menes i rettslig sammenheng først og fremst
    a. krav til motparten i en sivil sak om lagre data
    b. krav til politiet om å lagre beslaglagte filer
    c. krav til lagringsleverandører om å lagre data i en bestemt tidsperiode av bevishensyn
    d. krav til kommunikasjonsleverandører om å lagre data i en bestemt tidsperiode av bevishensyn
    e. krav til forsvarer om å ta vare på lagrede data

19. Vedlikehold av en profesjonell CV er nyttig for dataetterforskere fordi

a. det kan være kjekt å ha når man skal søke jobb
b. det kan brukes for å dokumentere erfaring ved sakkyndig vitneførsel
c. den bør vedlegges enhver etterforskningsrapport
d. den trengs for å få en beslutning fra retten
e. den trengs for å bli registrert som sakkyndig vitne hos justisdepartementet

20. I forbindelse med en etterforskning, bør en dataetterforsker
a. ha jevnlig kontakt med media
b. bare oversende de viktigste bevisene til media
c. unngå kontakt med media
d. kun sende skriftlige uttalelser til media
e. kun uttale seg muntlig til media