Avancerade
IT-Forensiska Verktyg I

15:e mars 2012

1400-1800

IDE, Högskolan i Halmstad

Kontaktperson: Mattias Weckstén, ankn. 7396

Betyg:	Del 1, 75% => 3
	Del 2, 75% => 4
	Del 3, G => 5

För betyg 4 krävs även godkänt för betyg 3,
för betyg 5 både 3 och 4.

Max:	Del 1 = 40 p
	Del 2 = 40 p
	Del 3 = G

Hjälpmedel:
Blyertspenna och radergummi.

Ange svar för del I på avsedd blankett.
Svar för del II och III lämnas på lösblad.

Lycka till!

Del I

Varje rätt svar ger 1 p. Om flera av svarsalternativen är korrekta ska du välja det som är mest korrekt.

1. Den minsta datamängd du kan skriva till en hårddisk är _____. Den minsta datamängd en fil kan skrivas till är _____.

A. En bit / en byte.
B. En sektor/ ett kluster.
C. En volym/ en disk.
D. En partition/ en MFT.

2. Vilka slutsatser kan du dra om en hårddisk är byglad i läge "CS"?

A. Det är en PATA-drive.
B. Det är en SATA-drive.
C. Det är en SCSI-drive.
D. Ingen av ovanstående.

3. Vad hittar du på en hårddisks Cylinder 0, Huvud 0, Sektor 1?

A. MBR
B. MFT
C. VBR
D. VBS

4. Vad kallas den första sektorn på en hårddisk?

A. FAT
B. VBR
C. MBR
D. VBD

5. Vad skiljer mellan USB 1.1 och Firewire?

A. Kontakten.
B. Arkitekturen.
C. Överföringshastigheten.
D. A+B+C

6. Vad åstadkommer RAID 1?

A. Ökad läs och skrivprestanda.
B. Ökad läsprestanda.
C. Ökad redundans och läsprestanda.
D. Ökad redundans.

7. FAT organiserar _____ och folderposten (directory entry) håller ordning på _____.

A. Filnamn/ storlek.
B. Filernas startkluster/ slutkluster.
C. Filernas slutkluster/ startkluster.
D. Filstorlek/ fragmentering.

8. En fils logiska storlek visas som:

A. Antalet sektorer som den logiska filen ockuperar.
B. Antalet kluster som den logiska filen ockuperar.
C. Antalet byte som den logiska filen ockuperar.
D. Antalet bitar som den logiska filen ockuperar.

9. En fils fysiska storlek är:

A. Alltid större än den logiska storleken.
B. Antalet byte i den logiska filen plus antalet byte slack från filens slut till klustrets slut.
C. A+B
D. Varken A eller B.

10. Hur återskapar EnCase en raderad fil?

A. Den läser filens namn från FAT och identifierar filen utifrån dess startkluster och logiska storlek.
B. Den läser filens namn från folderposten och letar reda på motsvarande filnamn i det oallokerade utrymmet.
C. Den identifierar filen genom att hämta filens startkluster och storlek från folderposten.
D. Den identifierar filen genom att hämta filens startkluster och storlek från FAT.

11. När man ska stänga ner ett stationärt system genom att koppla från strömmen är det lämpligast att:

A. Dra ur kontakten ur vägguttaget.
B. Dra ur kontakten ur nätdelen.
C. A eller B.
D. Varken A eller B.

12. Folderposten (directory entry) i ett FAT-filsystem har den fysiska storleken:

A. 0 byte.
B. 8 byte.
C. 16 byte.
D. 32 byte.

13. Hur stänger man generellt sett ner en dator i samband med datautvinning, som kör DOS?

A. Använder funktionen exit i kommandotolken.
B. Genom att dra ur strömkabeln från datorn.
C. Genom att dra ur strömkabeln från vägguttaget.
D. Genom att dra ur strömkabeln från hårddisken.

14. Hur stänger man generellt sett ner en dator i samband med datautvinning, som kör Windows 2000 Server?

A. Använder funktionen "Shut down" i startmenyn.
B. Genom att dra ur strömkabeln från datorn.
C. Genom att dra ur strömkabeln från vägguttaget.
D. Genom att dra ur strömkabeln från hårddisken.

15. Om en körande Linux-dators terminalfönster visar tecknet _ i prompten kan man gissa att den har root access:

A. ?
B. $
C. #
D. &

16. Vilket av följande material är mest lämpligt ur ESD-synpunkt att förvara en hårddisk i?

A. Papperspåse.
B. Plastpåse.
C. Aluminumfolie.
D. Wellpapp.

17. Ur forensisk synvinkel, varför är det lämpligt att köra wipe på en hårddisk innan du använder den i ett fall?

A. Beviskedjan.
B. Korskontaminering.
C. För att kunna använda olika filsystem.
D. Det finns inget behov av att köra en wipe.

18. Vilken systemfil ändras då man skapar en bootdisk från EnCase?

A. IO.SYS
B. COMMAND.COM
C. DRVSPACE.BIN
D. A+B+C

19. I Linux, vad innebär att en hårddisk har benämningen hdc?

A. Primär master.
B. Primär slav.
C. Sekundär master.
D. Sekundär slav.

20. EnCase bevisfil kan bäst beskrivas som:

A. En spegling av källan, till en andra hårddisk.
B. En sektorvis avbildning av en hårddisk, skriven till motsvarande sektorer på en andra hårdisk.
C. En bitströmsavbild av källdata, skriven till motsvarande sektorer på en andra hårddisk.
D. En bitströmsavbild av källdata, skriven till en eller flera filer på en andra hårddisk.

21. I Windows hittar du swap-utrymmet:

A. på en egen partition på bootdisken.
B. på en egen partition på valfri disk i systemet.
C. i en fil i filsystemet.
D. i RAM.

22. MD5-algoritmen skapar en summa på _____ bitar.

A. 32
B. 64
C. 128
D. 256

23. En bevisfil har arkiverats till fem CD. Segment 3 ligger på CD 3. Kan man verifiera datat i segment 3 separat medans det fortfarande ligger på CD?

A. Ja. Med hjälp av CRC.
B. Ja. Med hjälp av MD5.
C. Nej. Alla segmenten krävs för att sedan verifiera med hjälp av CRC.
D. Nej. Alla segmenten krävs för att sedan verifiera med hjälp av MD5.

24. Kommer EnCase "Gallery-view" att visa en .jpeg-fil om den döpts om till .txt?

A. Ja, "Gallery-view" tar bara hänsyn till filsignaturen.
B. Ja, men endast om filsignaturanalys genomförts.
C. Ja, men endast efter hashanalys genomförts.
D. Nej, "Gallery-view" kommer att hantera filen som en textfil.

25. I EnCase kan man alltid se den exakta positionen för markerat data i bevisfilen genom att titta på:

A. Statusraden.
B. Dixonboxen.
C. Diskvyn.
D. Hexvyn.

26. Filer i temp-foldern tas bort när:

A. Vyn som genererade filen stängs.
B. Det aktuella caset stängs.
C. EnCase stängs.
D. Filen använts färdigt.

27. Om 1 bit kan representera två olika utfall, hur många utfall kan 7 bitar representera?

A. 8
B. 16
C. 128
D. 256

28. Om tecknet B visas som värdet *101010b* så kallas denna representation:

A. ASCII
B. Hexadecimal
C. Decimal
D. Binär.

29. Vilken av följande texter ger inte en träff för följande GREP-uttryck:

```
\x50\x01\0x02[\0x04-\0x09]..
```

A. \0x50\0x01\0x02\0x03\0x04\0x05
B. \0x50\0x01\0x02\0x04\0x05\0x06
C. \0x50\0x01\0x02\0x05\0x06\0x07
D. \0x50\0x01\0x02\0x06\0x07\0x08

30. Vilken av följande texter ger en träff för följande GREP-uttryck:

```
al*drig
```

A. adrig
B. aldrig
C. A + B
D. Varken A eller B.

31. Vilken av följande texter ger inte en träff för följande GREP-uttryck:

```
035-?16[78]###
```

A. 035167123
B. 035-167333
C. 0351681464
D. 035-169208

32. Vart lagras sökuttrycken i EnCase?

A. I respektive case-fil.
B. I filen KEYWORDS.INI.
C. A+B.
D. Varken A eller B.

33. Kan vi vara säkra på att EnCase hitta ett ord eller en fras i en fil som är fragmenterad på hårddisken (dvs. inte ligger i konsekutiva kluster)?

A. Ja, EnCase klarar både fysisk och logisk sökning.
B. Ja, om man avmarkerar "File Slack" i sökdialogen.
C. Nej, endast om klustren är konsekutiva.
D. Nej, EnCase kan bara göra fysiska sökningar.

34. Vad är en fil-header?

A. Ett unikt set av tecken i början av filen som identifierar filens typ.
B. Ett 128-bitars värde som är unikt för en specifik fil, baserat på filens innehåll.
C. Rubriken i filnamnet.
D. Synonymt med filändelse.

35. Om en fils signatur är känd, men filändelsen stämmer inte med signaturen, kommer EnCase efter en signaturanalys att klassificera den som:

A. Alias (Signature Mismatch).
B. Unknown.
C. Match.
D. !Bad Signature.

36. Om en fils signatur är känd och filändelsen stämmer med signaturen, kommer EnCase efter en signaturanalys att klassificera den som:

A. Alias (Signature Mismatch).
B. Unknown.
C. Match.
D. !Bad Signature.

37. Om en fils signatur är okänd, men den har en känd filändelse, kommer EnCase efter en signaturanalys att klassificera den som:

A. Alias (Signature Mismatch).
B. Unknown.
C. Match.
D. !Bad Signature.

38. EnCase kan inte skapa hashvärden för:

A. Fysiska enheter.
B. Logiska volymer.
C. Tomma foldrar.
D. Varken A, B eller C.

39. Vilken del av bevisfilen analyserar EnCase under verifieringsprocessen för att få fram MD5-summan?

A. Avbildningsdatat.
B. Hela bevisfilen.
C. Casedatat.
D. Varken A, B eller C.

40. Filsystemet FAT lagrar datum och tid i _____, medans NTFS lagrar datum och tid i _____.

A. DOS-foldern/ lokal tid.
B. Zulu/ GMT.
C. Lokal tid/ GMT.
D. SYSTEM.DAT/ NTUSER:DAT.