

A V A N C E R A D E  
F O R E N S I S K A  
V E R K T Y G

I

DT2005

2010-03-17

Kontakt: Mattias Weckstén  
Telefon: 7396

**Instruktioner:**

Tentamen består av 55 frågor. Varje fråga har ett korrekt svarsalternativ. Tycker du att det finns flera korrekta svar ska du gissa på det som verkar mest korrekt. Använd bifogat svarsformulär för att svara på frågorna. Markera rätt svar på formuläret med ett kryss. Om du markerat fel, sudda eller fyll den felaktiga rutan helt.

**Betygsgränser:**

0-39 rätt	U
40-45 rätt	3
46-50 rätt	4
51-55 rätt	5

LYCKA TILL!

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 IDE-drive.
- B. Det är en SATA-drive.
- C. Det är en SCSI-drive.
- D. A+B+C

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 volym?

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

5. Vad skiljer mellan USB 1.1 och USB 2?

- A. Kontakten.
- B. Spänningsnivåerna.
- C. Överföringshastigheten.
- D. A+B+C

6. Vad åstadkommer RAID 0?

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

7. FAT organiserar \_\_\_\_\_ och folderposten 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. Vilket filsystem har en övre gräns för filnamn på 64 tecken?

- A. ISO 9660 Level 1
- B. ISO 9660 Level 3
- C. Joliet
- D. UDF

12. Folderposten i ett FAT-filsystem har den logiska storleken:

- A. 0 byte.
- B. 8 byte.
- C. 16 byte.
- D. En sektor.

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

- 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.

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 dators terminalfönster visar tecknet \ i prompten kan man anta att den kör:

- A. Red Hat.
- B. Unix.
- C. En Linux-distribution med root inloggad.
- D. MS-DOS

16. Vilket av följande material är minst lämpligt för att förvara en hårddisk i?

- A. Papperspåse.
- B. Plastpåse.
- C. Aluminiumfolie.
- 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 hdb?

- 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 hårddisk.
- 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. Hur verifierar EnCase att bevisfilen innehåller en exakt kopia av källdatat?

- A. Genom att jämföra MD5-summan för källan och MD5-summan från bevisfilen.
- B. Genom att jämföra CRC-värdena för källan och CRC-värdena från bevisfilen.
- C. Genom att jämföra MD5-summan för källan och MD5-summan för hela bevisfilen.
- D. Genom att jämföra CRC-värdet för källan och CRC-värdet för hela bevisfilen.

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 8 bitar representera?

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

28. Om tecknet *A* visas som värdet *41h* 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:

`\x00\x01\xee[\x55-\xaa]..`

- A. `\x00\x01\xee\x55\x77\xaa`
- B. `\x00\x01\xee\x77\x77\xaa`
- C. `\x00\x01\xee\xaa\x77\xaa`
- D. `\x00\x01\xee\xcc\x77\xaa`

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

`1a juli, 2?0?10`

- A. 1a juli, 2010
- B. 1a juli, 210
- C. 1a juli, 10
- D. A+B+C.

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

`[#]ABC[ \-]45[ \-]DEFG[#]`

- A. 3ABC45DEFG6
- B. 3ABC 45-DEFG6
- C. 3ABC-45-DEFG6
- D. 3ABC 45 DEFG6

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 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.

36. 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.

37. 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.

38. EnCase kan skapa hashvärden för:

- A. Fysiska enheter.
- B. Logiska volymer.
- C. Filer eller set av filer.
- D. A+B+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.

41. Vart lagrar Windows tidszoninställningarna?

- A. BIOS.
- B. Registryn.
- C. INFO2.
- D. DOS-foldern eller MFT.

42. När en textfil på en WindowsXP-dator skickas till papperskorgen så ändras det korta filnamnet till DC0.txt. Vilken av följande påståenden om det korta filnamnet stämmer bäst?

- A. D=DOS, C=textfil, 0=index number, .txt=filens ursprungliga ändelse.
- B. D=Deleted, C=textfil, 0=index number, .txt=filens ursprungliga ändelse.
- C. D=Deleted, C=volymnamn, 0=index number, .txt=filens ursprungliga ändelse.
- D. D=DOS, C=volymnamn, 0=index number, .txt=filens ursprungliga ändelse.

43. När ett dokument öppnas i Windows skapas en länk med dokumentets filnamn i \_\_\_\_\_ foldern.

- A. Shortcut.
- B. Recent.
- C. Temp.
- D. History.

44. Eftersom denna Windowsfil består av innehållet i RAM när datorn stängs av, så kommer den att ha samma storlek som RAMet och ligga i rotfoldern.

- A. HIBERFIL.SYS
- B. WIN386.SWP
- C. PAGEFILE.SYS
- D. NTUSER.DAT

45. Hur många logiska partitioner tillåter partitionstabellen på master boot record för en fysisk disk, enligt IBM PC-standard?

- A. 1
- B. 2
- C. 4
- D. 8

46. Den första sektorn i en partition kallas:

- A. Fysisk sektor 0.
- B. Aktiv primärpartition.
- C. MBR.
- D. VBR.

47. I Windows 2000 finns information om en specifik användares inställningar i filen NTUSERS.DAT. Vart hittar vi denna fil?

- A. C:\
- B. C:\WINDOWS\
- C. C:\Documents and Settings\username
- D. C:\Documents and Settings\All Users\Application Data

48. Modulen för det virtuella filsystemet VFS monterar data som \_\_\_\_\_, medan modulen för fysisk diskemulering PDE monterar data som \_\_\_\_\_.

- A. Nätverksdisk/ Emulerad disk.
- B. Emulerad disk/ Nätverksdisk.
- C. Virtuellt volym/ Fysisk volym.
- D. Virtuellt fil/ Fysisk disk.

49. \_\_\_\_\_ är en substitutionskodning som används i registern. \_\_\_\_\_ används för att koda binära data som text.

- A. MD5/ ROT-13
- B. ROT-13/ BASE-64
- C. BASE-64/ ASCII
- D. ASCII/ MD5

50. Vad av följande gör det möjligt att identifiera MBR och VBR på en hårddisk?

- A. HBR i sektor -1.
- B. Genom att starta i första sektorn av FAT och gå ett steg bakåt.
- C. Genom signaturanalys.
- D. Varken A, B eller C.

51. \_\_\_\_\_ finns både i den lokala och globala vyn.

- A. Keywords.
- B. File Signatures.
- C. Hash Sets.
- D. Projects.

52. Vilket läge ska du ställa "debug logging" om du vill debugga men måste vara säker på att ingen information om ditt case läker ut?

- A. Off.
- B. Stack.
- C. Heap.
- D. EnCase har inte "debug logging".

53. En fil tar upp tre kluster om fyra sektorer vardera på hårddisken. I det sista klustret nyttjar filen endast 200 byte. Det outnyttjade utrymmet i den påbörjade sektorn i sista klustret kallas \_\_\_\_\_ och de outnyttjade sektorerna i sista klustret kallas \_\_\_\_\_.

- A. RAM-slack/ sektorslack.
- B. Sektorslack/ filslack.
- C. Filslack/ sektorslack.
- D. Filslack/ RAM-slack.

54. Vad innebär "Zoned-Bit Recording"?

- A. Antalet bitar som krävs för att representera en byte varierar.
- B. Antalet byte i en sektor varierar.
- C. Antalet sektorer på ett spår varierar.
- D. Antalet spår på en skiva varierar.

55. Vad anger den blå triangeln i bilden?



- A. Att enheten innehåller filer och foldrar.
- B. Att enheten är direktuppkopplad.
- C. Att avbildning pågår.
- D. Att sökning pågår.