DT2005-ALL

1. Tillåter EnCase att användaren skriver data till ev inhämtad bevis-fil?

A. Ja, för att lägga till noteringar och kommentarer.
B. Ja, för att lägga till sökresultat.
C. Både A och B.
D. Nej, data kan inte läggas till bevisfilen efter slutförd inhämtning.

2. Om du tömmer papperskorgen och därefter raderar filen D:\Filer\PC.doc genom att lägga den i papperskorgen så har den internt i papperskorgen följande namn:
A. DC1.doc
B. DD1.doc
C. PD1.doc
D. PC1.doc

3. Om man kodar 8-bitars ASCII som 7-bitars ASCII så använder du följande algoritm:
A. PGP
B. ROT-13
C. BASE-64
D. Ingen av alternativen.

4. Vilket/ vilka beroenden är korrekta?

A. CRC ändras då blockstorleken ändras.
B. MD5 ändras då segmentstorleken ändras.
C. A + B
D. Varken A eller B.

5. 

Vad anger den blå triangeln?
A. Att samtliga filer är markerade.
B. Att vi jobbar med en avbild.
C. Att vi jobbar med en fysisk enhet.
D. Att samtliga items (filer, foldrar etc.) är markerade.

6. Hittar EnCase ord eller fraser som är fragmenterade över icke konsekutiva kluster?
A. Ja, men endast om man valt att söka i "file slack".
B. Ja. EnCase gör både logisk och fysisk sökning.
C. Nej, efterssom de är i icke-konsekutiva kluster.
D. Nej, EnCase gör endast fysisk sökning.

7. Vad krävs av en hårddisk innan du lagrar avbilder på den?
A. En wipe.
B. En FAT32-partition.
C. En NTFS-partition.
D. En formatering.

8. Om man kodar C:\Program Files till P:\Cebtenz Svyrf så använder du följande algoritm:
A. PGP
B. BASE-64
C. ROT-13
D. Ingen av alternativen.

9. Vart hittar man en dators swapfil?
A. pagefile.sys
B. swapfile.sys
C. hiberfil.sys
D. Inte som en fil i filsystemet.

10. När en fil öppnas i Windows skapas en länk i vilken folder?
A. Recent
B. Shortcut
C. History
D. Temp

11. Vilket påstående är rätt?
A. Den fysiska storleken kan inte vara mindre än den logiska storleken.
B. Begreppen logisk och fysisk storlek saknar relevans när det gäller filer.
C. Den logiska och fysiska storleken är alltid samma.
D. Den logiska storleken kan inte vara mindre än den fysiska storleken.

12. Vart hamnar resultatet vid en copy/unerase?
A. Temp
B. Evidence
C. Export
D. Ingen av alternativen är korrekt.

13. Datorers talsystem som består av siffrorna 0 och 1 benämns:
A. Hexadecimalt
B. ASCII
C. Binärt
D. FAT

14. Vart hittar man spår efter web-mail som tex. Hotmail och Gmail?
A. Temporary Internet Files.
B. Pagefile.sys.
C. Både A och B.
D. Varken A eller B.

15. Kommer en .jpg-fil som döpts om till .txt visas i table-pane under gallery-view?
A. Ja, efter signaturanalys.
B. Ja, efter hashgenerering.
C. Ja, utan vidare.
D. Nej.

16. Vad kan leda till problem för att kunna återskapa raderade filer?
A. Fragmentering.
B. Överskrivning.
C. A+B.
D. Varken A eller B.

17. Data du väljer i en panel visas mer detaljerat i nästa osv. Vilken beskrivning är korrekt?
A. Data från Tree-pane visas i Table-pane, där vald data i sin tur visas i View-pane.
B. Data från Tree-pane visas i Filter-pane, där vald data i sin tur visas i View-pane.
C. Data från View-pane visas i Table-pane, där vald data i sin tur visas i Tree-pane.
D. Data från Filter-pane visas i View-pane, där vald data i sin tur visas i Table-pane.

18. Vart lagras filernas tidsstämplar?
A. I folder-tabellen.
B. I fil-tabellen.
C. I datum-tabellen.
D. I FAT.

19. Hur många primära partitioner finns maximalt i MBR?
A. 1
B. 2
C. 4
D. 6

20. Vart lagras sökuttryck i EnCase 6?
A. I case-filerna (.case och .cbak)
B. I KEYWORDS.INI-filen.
C. A+B
D. Varken A eller B.

21. Hur många entries kan man ha i rootfoldern i FAT32?
A. 2048
B. 512
C. 4096
D. Det finns ingen begränsning.

22. En byte består av ___ bitar.
A. 2
B. 4
C. 8
D. 16

23. Du utvinner en bevsfil från en hel hårddisk X. Vilket påstående är korrekt?

A. MD5-hashen för bevisfilen och datat på disken X är samma.
B. MD5-hashen i bevisfilen och datat på disken X är samma.
C. A + B
D. Varken A eller B.

24. Vilken algoritm är mest resurskrävande?

A. CRC
B. MD5
C. De är lika resurskrävande.
D. Det går inte att jämföra.

25. Vilket är det minsta element en fil kan uppta?
A. En sektor.
B. En byte.
C. En volym.
D. Ett kluster.

26. En fil ockuperar tre kluster på en hårddisk. Klustren är fyra sektorer långa och sektorerna är av standardstorlek. Hur stor är filens fysiska storlek?
A. ca 3 kB
B. ca 6 kB
C. ca 12 kB
D. Det går inte att avgöra.

27. Får man samma resultat om man tittar på registry-filerna i EnCase som om man göra en registry-dump i ett körande system?
A. Ja, alltid.
B. Ja, men endast om man stänger av systemet med hjälp av "Start->Shutdown" innan man gör diskutvinning.
C. Ja, men endast om man stänger av systemet genom att dra ur strömkabeln innan man gör diskutvinning.
D. Nej.

28. Exakt position för markerad data i bevisfilen kan alltid ses genom att titta vart?
A. Statusraden längst ner i fönstret.
B. Dixon-boxen i avdelaren mellan table och view.
C. I view under hex-view.
D. I table under disk-view.

29. Vad är korrekt för GREP?
A. GREP matchar endast data.
B. GREP matchar endast mönster.
C. GREP matchar mönster och data.
D. Ingen av alternativen.

30. När du skapar ett nytt case så ska du ange en "Index Folder". Vad är dess syfte?
A. Organisera bevisfiler.
B. Indexera rapporten.
C. Snabba upp sökningar.
D. Lagra temporära filer.

31. Vart kan man se en fils fysiska position?
A. GPS
B. DVF
C. Man måste genomföra en positionssökning.
D. Det finns inget stöd för detta i EnCase.

32. Om en bevisfil är delad i fem segment och varje segment sedan skrivits till CD; går det då att verifiera ett segment medans den fortfarande ligger på CDn?
A. Nej, det behövs data från andra segment också.
B. Nej, det går inte att göra direkt från en CD.
C. Ja, men endast om det handlar om det sista segmentet.
D. Ja, det går för alla segment.

33. Du har monterat en disk från EnCase. När du tittar på diskens innehåll i utforskaren ser du en fil med oallokerade kluster och du ser även filer som varit raderade. Vilken metod användes för att montera?
A. VFS
B. PDE
C. VFS eller PDE, går ej att särskilja
D. Varken VFS eller PDE, de har inte de beskrivna funktionerna.

34. Vart lagrar Windows en dators tidszon?
A. I BIOS.
B. I INFO2-filen.
C. I registryn.
D. I MFT.

DT2005-ALL Key

1. *(p. 179)* Tillåter EnCase att användaren skriver data till ev inhämtad bevis-fil?

A. Ja, för att lägga till noteringar och kommentarer.
B. Ja, för att lägga till sökresultat.
C. Både A och B.
D. Nej, data kan inte läggas till bevisfilen efter slutförd inhämtning.

DT2005 ch.... #4

2. *(p. 392)* Om du tömmer papperskorgen och därefter raderar filen D:\Filer\PC.doc genom att lägga den i papperskorgen så har den internt i papperskorgen följande namn:
A. DC1.doc
B. DD1.doc
C. PD1.doc
D. PC1.doc

DT2005 OS... #5

3. *(p. 524)* Om man kodar 8-bitars ASCII som 7-bitars ASCII så använder du följande algoritm:
A. PGP
B. ROT-13
C. BASE-64
D. Ingen av alternativen.

DT2005 Advanced... #3

4. *(p. 179)* Vilket/ vilka beroenden är korrekta?

A. CRC ändras då blockstorleken ändras.
B. MD5 ändras då segmentstorleken ändras.
C. A + B
D. Varken A eller B.

DT2005 ch.... #2

5. *(p. 217)*
Vad anger den blå triangeln?

A. Att samtliga filer är markerade.
B. Att vi jobbar med en avbild.
C. Att vi jobbar med en fysisk enhet.
D. Att samtliga items (filer, foldrar etc.) är markerade.

DT2005 Environment... #2

6. *(p. 308)* Hittar EnCase ord eller fraser som är fragmenterade över icke konsekutiva kluster?

A. Ja, men endast om man valt att söka i "file slack".
B. Ja. EnCase gör både logisk och fysisk sökning.
C. Nej, efterssom de är i icke-konsekutiva kluster.
D. Nej, EnCase gör endast fysisk sökning.

DT2005 search... #4

7. *(p. 157)* Vad krävs av en hårddisk innan du lagrar avbilder på den?

A. En wipe.
B. En FAT32-partition.
C. En NTFS-partition.
D. En formatering.

DT2005 ch.... #1

8. *(p. 498)* Om man kodar C:\Program Files till P:\Cebtenz Svyrf så använder du följande algoritm:

A. PGP
B. BASE-64
C. ROT-13
D. Ingen av alternativen.

DT2005 Advanced... #2

9. *(p. 435)* Vart hittar man en dators swapfil?
A. pagefile.sys
B. swapfile.sys
C. hiberfil.sys
D. Inte som en fil i filsystemet.

DT2005 OS... #1

10. *(p. 416)* När en fil öppnas i Windows skapas en länk i vilken folder?
A. Recent
B. Shortcut
C. History
D. Temp

DT2005 OS... #2

11. *(p. 228)* Vilket påstående är rätt?
A. Den fysiska storleken kan inte vara mindre än den logiska storleken.
B. Begreppen logisk och fysisk storlek saknar relevans när det gäller filer.
C. Den logiska och fysiska storleken är alltid samma.
D. Den logiska storleken kan inte vara mindre än den fysiska storleken.

DT2005 Environment... #3

12. *(p. 212)* Vart hamnar resultatet vid en copy/unerase?
A. Temp
B. Evidence
C. Export
D. Ingen av alternativen är korrekt.

DT2005 ch.... #2

13. *(p. 275)* Datorers talsystem som består av siffrorna 0 och 1 benämns:
A. Hexadecimalt
B. ASCII
C. Binärt
D. FAT

DT2005 search... #1

14. *(p. 514)* Vart hittar man spår efter web-mail som tex. Hotmail och Gmail?
A. Temporary Internet Files.
B. Pagefile.sys.
C. Både A och B.
D. Varken A eller B.

DT2005 OS... #4

15. *(p. 231)* Kommer en .jpg-fil som döpts om till .txt visas i table-pane under gallery-view?
A. Ja, efter signaturanalys.
B. Ja, efter hashgenerering.
C. Ja, utan vidare.
D. Nej.

DT2005 ch.... #4

16. *(p. 64)* Vad kan leda till problem för att kunna återskapa raderade filer?
A. Fragmentering.
B. Överskrivning.
C. A+B.
D. Varken A eller B.

DT2005 File... #5

17. *(p. 210)* Data du väljer i en panel visas mer detaljerat i nästa osv. Vilken beskrivning är korrekt?
A. Data från Tree-pane visas i Table-pane, där vald data i sin tur visas i View-pane.
B. Data från Tree-pane visas i Filter-pane, där vald data i sin tur visas i View-pane.
C. Data från View-pane visas i Table-pane, där vald data i sin tur visas i Tree-pane.
D. Data från Filter-pane visas i View-pane, där vald data i sin tur visas i Table-pane.

DT2005 Environment... #1

18. *(p. 45)* Vart lagras filernas tidsstämplar?
A. I folder-tabellen.
B. I fil-tabellen.
C. I datum-tabellen.
D. I FAT.

DT2005 File... #4

19. *(p. 471)* Hur många primära partitioner finns maximalt i MBR?
A. 1
B. 2
C. 4
D. 6

DT2005 Advanced... #1

20. *(p. 197)* Vart lagras sökuttryck i EnCase 6?
A. I case-filerna (.case och .cbak)
B. I KEYWORDS.INI-filen.
C. A+B
D. Varken A eller B.

DT2005 search... #3

21. *(p. 43)* Hur många entries kan man ha i rootfoldern i FAT32?
A. 2048
B. 512
C. 4096
D. Det finns ingen begränsning.

DT2005 File... #2

22. *(p. 279)* En byte består av ___ bitar.
A. 2
B. 4
C. 8
D. 16

DT2005 search... #2

23. *(p. 182)* Du utvinner en bevsfil från en hel hårddisk X. Vilket påstående är korrekt?

A. MD5-hashen för bevisfilen och datat på disken X är samma.
B. MD5-hashen i bevisfilen och datat på disken X är samma.
C. A + B
D. Varken A eller B.

DT2005 ch.... #5

24. *(p. 179)* Vilken algoritm är mest resurskrävande?

A. CRC
B. MD5
C. De är lika resurskrävande.
D. Det går inte att jämföra.

DT2005 ch.... #1

25. *(p. 41)* Vilket är det minsta element en fil kan uppta?
A. En sektor.
B. En byte.
C. En volym.
D. Ett kluster.

DT2005 File... #1

26. *(p. 41)* En fil ockuperar tre kluster på en hårddisk. Klustren är fyra sektorer långa och sektorerna är av standardstorlek. Hur stor är filens fysiska storlek?
A. ca 3 kB
B. ca 6 kB
C. ca 12 kB
D. Det går inte att avgöra.

DT2005 File... #3

27. *(p. 493)* Får man samma resultat om man tittar på registry-filerna i EnCase som om man göra en registry-dump i ett körande system?
A. Ja, alltid.
B. Ja, men endast om man stänger av systemet med hjälp av "Start->Shutdown" innan man gör diskutvinning.
C. Ja, men endast om man stänger av systemet genom att dra ur strömkabeln innan man gör diskutvinning.
D. Nej.

DT2005 Advanced... #4

28. *(p. 243)* Exakt position för markerad data i bevisfilen kan alltid ses genom att titta vart?
A. Statusraden längst ner i fönstret.
B. Dixon-boxen i avdelaren mellan table och view.
C. I view under hex-view.
D. I table under disk-view.

DT2005 ch.... #3

29. *(p. 297)* Vad är korrekt för GREP?
A. GREP matchar endast data.
B. GREP matchar endast mönster.
C. GREP matchar mönster och data.
D. Ingen av alternativen.

DT2005 search... #5

30. *(p. 213)* När du skapar ett nytt case så ska du ange en "Index Folder". Vad är dess syfte?
A. Organisera bevisfiler.
B. Indexera rapporten.
C. Snabba upp sökningar.
D. Lagra temporära filer.

DT2005 Environment... #5

31. *(p. 243)* Vart kan man se en fils fysiska position?
A. GPS
B. DVF
C. Man måste genomföra en positionssökning.
D. Det finns inget stöd för detta i EnCase.

DT2005 Environment... #4

32. *(p. 183)* Om en bevisfil är delad i fem segment och varje segment sedan skrivits till CD; går det då att verifiera ett segment medans den fortfarande ligger på CDn?
A. Nej, det behövs data från andra segment också.
B. Nej, det går inte att göra direkt från en CD.
C. Ja, men endast om det handlar om det sista segmentet.
D. Ja, det går för alla segment.

DT2005 ch.... #3

33. *(p. 535)* Du har monterat en disk från EnCase. När du tittar på diskens innehåll i utforskaren ser du en fil med oallokerade kluster och du ser även filer som varit raderade. Vilken metod användes för att montera?
A. VFS
B. PDE
C. VFS eller PDE, går ej att särskilja
D. Varken VFS eller PDE, de har inte de beskrivna funktionerna.

DT2005 Advanced... #5

34. *(p. 386)* Vart lagrar Windows en dators tidszon?
A. I BIOS.
B. I INFO2-filen.
C. I registryn.
D. I MFT.

DT2005 OS... #3

DT2005-ALL Summary

Category	*# of Questions*
DT2005 Advanced...	5
DT2005 ch....	9
DT2005 Environment...	5
DT2005 File...	5
DT2005 OS...	5
DT2005 search...	5