Datautvinning från digitala lagringsmedia
DT2002

-= FACIT =-

26:e maj 2010

0900-1300

IDE, Högskolan i Halmstad

Kontaktperson: Mattias Weckstén, ankn. 7396

Betyg:	Del 1, 32 p => 3
	Del 2, 22 p => 4
	Del 3, G => 5

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

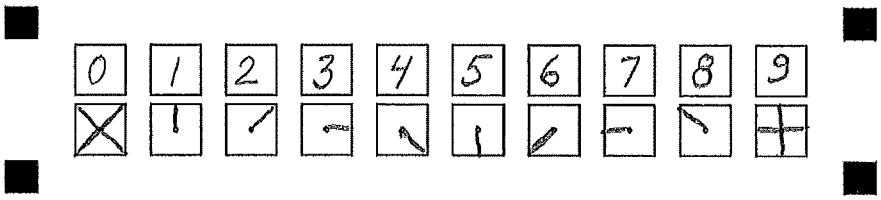
Max:	Del 1 = 40 p
	Del 2 = 30 p
	Del 3 = G

Hjälpmedel:
Blyertspenna och radergummi.

Viktigt! Läs noga instruktionerna på nästa sida innan du börjar!

INSTRUKTIONER

Val markeras med kryss i vald ruta, från hörn till hörn. Felaktig markering suddas ut. Siffror i personnummer och siffersvar kodas på följande vis:



Observera:

Anteckna svaren i provhäftet. När du är klar för du över svaren till svarsformulären.
Samtliga svarsformulär ska lämnas in. Provhäftet behålls eller kastas.
Skriv och koda personnummer på varje blad. Även tomma blad.
Glöm inte att koda siffersvar. Tomma rutor i siffersvar fylls ut med nollor.
Exempel på ifyllda svarsformulär finns hos tentavakten om något är oklart.
Ansvarig för tentamen besöker tentasalen ca 1 timma in i skrivningen.

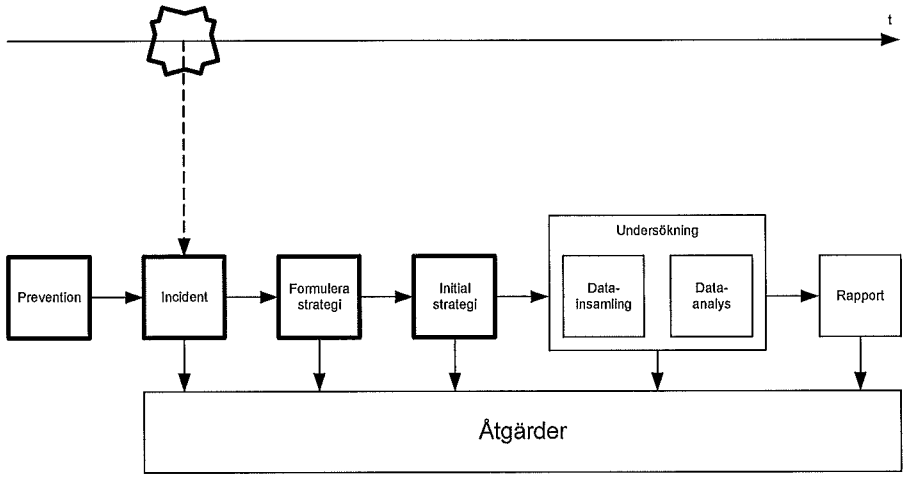
Lycka till!

Del I

Varje rätt svar ger 1 p. Om båda svaren är korrekta ska du välja det som är mest korrekt.

(Varje godkänt kunskapsprov ger 3 bonuspoäng, upp till max 36 bonuspoäng.)

1. Nedan syns en översikt av incidenthanteringsprocessen. Är momenten "Prevention" till och med "Formulera strategi" i rätt ordning (markerade med tjocka ramar)?



A. Ja. B. Nej.

2. Är filer på en hårddisk att anse som volatila data?

A. Ja. B. Nej.

3. Kan två filer med olika MD5-summa ha exakt samma innehåll?

A. Ja. B. Nej.

4. CSIRT (Computer Security Incident Response Team) är en grupp sammansatt av ett antal datortekniska experter.

A. Ja. B. Nej.

5. Är intervjuer med ledning och chefer del av initial respons?

A. Ja. B. Nej.

6. Efter det att en incident detekterats så ska en checklista fyllas i. Första delen av checklistan är för inhämtning av information från "the first responder". Vem är "the first responder"?

A. En slutanvändare av systemet. B. En systemadministratör.

7. Så snart som incidenten övergått i en utredning är det lämpligt att informera alla i organisationen att en utredning pågår.

   A. Ja. B. Nej.

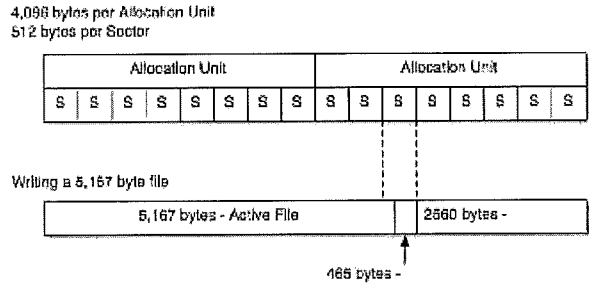
8. En "Qualified Forensic Duplicate" får komprimera tomma sektorer.

   A. Ja. B. Nej.

9. Kan autopsy användas för att skapa en "Forensic Duplicate"?

   A. Ja B. Nej

10. Pilen i figuren pekar på:



   A. File slack. B. RAM slack

11. Loopback används för att montera avbilder (images) i filsystemet.

   A. Ja. B. Nej.

12. Det går att återställa raderade filer på en Windowspartition även om man jobbar i Linux.

   A. Ja. B. Nej.

13. Kan en kopia (tex. en avbild) vara bästa bevis?

   A. Ja. B. Nej.

14. Kan man använda MD5 för att validera avbilder?

   A. Ja. B. Nej.

15. Är fotografering en lämplig metod vid bevishantering?

   A. Ja . B. Nej.

16. Följande påstående är korrekt: "Du ska genomföra initial respons på ett Windows-system. Du väljer att ansluta en usb-disk för att lagra data på, efterssom detta inte lämnar några spår på målsystemet."

A. Ja. B. Nej.

17. En kollega hävdar att man inte ska köra målsystemets egen kommando-prompt vid live-utvinning utan att man ska ha med sig en egen kommandoprompt på tex. CD. Stämmer det?

A. Ja. B. Nej.

18. Ska verktygslådan (the toolkit) hanteras som ett bevis med tag och label efter att den användts även om den inte innehåller utvunnen data? (tex. du har ditt toolkit på en cd)

A. Ja. B. Nej.

19. Följande kommando tömmer en befintlig fil logg.txt och lagrar sedan utdatat från fport i denna fil.

fport >> logg.txt

A. Ja B. Nej.

20. Kommandot lsof listar systemets öppna filer.

A. Ja. B. Nej.

21. Routrar innehåller icke-volatila data precis som ett datorsystem

A. Ja. B. Nej.

22. En routers "uptime" syftar på den tid det tar att skicka ett paket uppåt i hierarkin.

A. Ja . B. Nej.

23. Att kapa strömförsörjningen till en router kan anses vara en DDoS attack.

A. Ja B. Nej.

24. Swap-utrymmet i Windows består av en fil i filsystemet.

A. Ja. B. Nej.

25. I en standardinstallation av Windows; när du raderar en fil i terminalen med "del filnamn" så raderas filen inte utan den flyttas endast till papperskorgen.

A. Ja. B. Nej.

26. En död länk uppstår när en länk pekar på en målfil och länken därefter raderas.

A. Ja B. Nej.

27. I Linux börjar filnamnet på dolda filer med . (tex. .dold_fil).

A. Ja. B. Nej.

28. "Event monitoring" innebär att man spelar in all trafik, dvs. headers och data, från en given länk.

A. Ja. B. Nej.

29. Avlyssning syftar i huvudsak till att undvika attacker.

A. Ja. B. Nej.

30. Din kollega hävdar att "en switch med SPAN underlättar avlyssning". Stämmer detta uttalande?

A. Ja. B. Nej.

31. Du använder en Linux-server för avlyssning och lagring av dessa data. När du kontrollerar diskutrymmet ser du följande:

df –h

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/hda2	28G	23G	5G	82%	/
/dev/hda1	464M	37M	403M	9%	/boot

Du vet att du ska avlyssna ytterligare 24 timmar och räknar fram att mängden data som ska loggas kommer inte att vara mer än 250 Mbyte per timma. Kommer diskutrymmet att räcka?

A. Ja B. Nej.

32. Ett så kallat "SYN-paket" indikerar början på en session.

A. Ja. B. Nej.

33. Du analyserar en tcp-dump men får inte den att stämma. Din kollega hävdar då att du måste ta hänsyn till att paketen kanske inte kommer i rätt ordning, så kallad "out-of-order delivery". Stämmer det?

A. Ja. B. Nej.

34. Du har precis genomfört en live-repons. Du har dokumenterat systemets all volatil data till en loggfil. Det sista du gör är att du sparar undan vilka kommandon och vilka inställningar du använt. Därefter är du klar med inhämtningen och kan åka tillbaka till labbet.

A. Ja. B. Nej.

35. Din kollega säger att då strömförsörjningen bryts så försvinner all data ur RAMet (volatilt minne). Du å din sida hävdar att det tar ganska lång tid innan all data försvunnit; betydligt längre tid än vad det skulle ta att tex. ta ur och sätta i en laptops batteri. Vem har rätt?

A. Din kollega. B. Du.

36. Statisk data i körbara program, som tex. vissa typer av lösenord går att hitta med hjälp av strängutvinning.

A. Ja. B. Nej.

37. En rapport måste alltid vara skriftlig.

A. Ja. B. Nej.

38. SAS och SCSI har samma fysiska gränssnitt.

A. Ja. B. Nej.

39. Signaturanalys kan användas för att identifiera huruvida en fils ändelse matchar filens innehåll (tex. fil.jpg faktiskt är en bild).

A. Ja. B. Nej.

40. Om man kan polisanmäla en incident ska man ändå göra en egen utredning?

A. Ja. B. Nej.

Del 2

Om inget annat anges ger varje rätt svar 1 p. (Varje inlämningsuppgift ger upp till 3 bonuspoäng, upp till max 12 bonuspoäng.)

1. 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

2. 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.

3. När ett dokument öppnas i Windows skapas en länk med dokumentets filnamn i _____ foldern.

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

4. Här ser du FAT-tabellen för en partition med endast tre filer. Alla kluster bortom kluster 10 är oallokerade. Hitta den största filen och markera med kryss i svarsformuläret vilka kluster den ockuperar. (3p)

FAT Table

Kluster	2	3	4	5	6	7	8	9	10
	X	X	7	X	EOF	8	EOF	EOF	0

5. Para ihop följande begrepp och benämningar två och två. Exempel: hänger 01 och 14 ihop anger du 01 – 14 i svarsformuläret. Glöm inte att koda svaret. Fel ger poängavdrag. (min 0 p, max 7 p)

01. Avbild
02. Brandvägg
03. Checksumma
04. dcfldd
05. dir /t:a
06. Filsystem
07. grep
08. Masslagrings-gränssnitt
09. MD5
10. Mönstermatchning
11. NTFS
12. IDE
13. Port
14. Tidsstämplar.

01-04
05-14
08-12
02-13
06-11
03-09
07-10

6. Para ihop de sex lagren i lagringsmodellen med rätt begrepp. Ange en siffra till varje bokstav i svarsformuläret. Exempel: hänger A och 5 ihop anger du A – 5 i svarsformuläret. (5 p)

A. Lagringshantering (storage space management)	1. Sektor.
B. Dataklassificering (data classification)	2. Mappning.
C. Fysiska (physical)	3. Kluster.
D. Allokeringsenheter (allocation units)	4. Filer och foldrar.
E. Informationsklassificering (information classification)	5. Partition.

A – 2
B – 5
C – 1
D – 3
E – 4

7. Du vill göra en total avlyssning av en switch med 16 stycken 100 Mbit/s portar. Switchen har en speciell avlyssningsport med prestandan 10 Gbit/s som kan kopplas in till din avlyssningsutrustning. Du har fått instruktioner om att under minst 20 timmar genomföra fullständig avlyssning. Hur stor hårddiskarray behöver du i värsta fallet för att lösa problemet? Ange svaret i hela Gigabyte rundat uppåt. Tomma rutor i svarsformuläret fylls ut med inledande nollor. (6p)

8. Du vill göra en total avlyssning av en switch med 20 stycken 100 Mbit/s portar. Du vet att belastningen per port i snitt på kort horisont kommer inte att vara högre än 50%. Switchen har en speciell avlyssningsport med prestandan 1 Gbit/s som kan kopplas in till din avlyssningsutrustning. Du har en liten hårddiskarray med 4.5 Terabyte ledigt utrymme. Hur kort tid kan du spela in trafik i värsta fallet? Ange svaret i hela timmar rundat nedåt. Tomma rutor i svarsformuläret fylls ut med inledande nollor. (6p)

7. $\frac{16 \cdot 100\ \text{Mbit/s}}{8\text{bit}} = 200\text{MByte/s} < 10\text{GBit/s}$

$20\text{h} = 3600\text{s} \cdot 20 = 72000\text{s}$

$72000\text{s} \cdot 200\ \text{MByte/s} = 14400000\text{MByte}$
$= 14400\ \text{GByte}$

8. $\frac{20 \cdot 100\text{M/s}}{2 \cdot 8} = \frac{1000\text{M/s}}{8} = 125\text{MB/s} \leq 1\text{GBit/s}$

$\frac{4500000\text{MB}}{125} = 36000\text{s} = 10\text{h}$

Del 3

Välj ett ämne av nedanstående. Detta är uppgiften för betyg 5, så du måste verkligen gå på djupet och visa din förståelse för att få godkänt. Betygskriteriet kräver att man kan *"analysera och argumentera runt givna situationer med utgångspunkt i grundläggande uttryck och begrepp"*. Det räcker med andra ord inte att endast skriva en beskrivning av det valda ämnet. Max en A4.

1. Beskriv hur man enkelt och billigt kan konfigurera en dator som inte lämnar några eller åtminstone väldigt få eller svårtydda digitala spår efter användaren.

2. Beskriv vad man måste tänka på när man bygger en forensisk hårdvaruplattform (dator).

3. Beskriv incidentkedjan och de ingående stegen.

4. Beskriv initial respons och de ingående stegen.