

Datautvinning från digitala lagringsmedia DT2002

25:e maj 2011

1400-1800

IDE, Högskolan i Halmstad

Kontaktperson: Mattias Weckstén, ankn. 7396

Betyg: Del 1, 32 p => 3
 Del 2, 30 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 = 40 p
 Del 3 = G

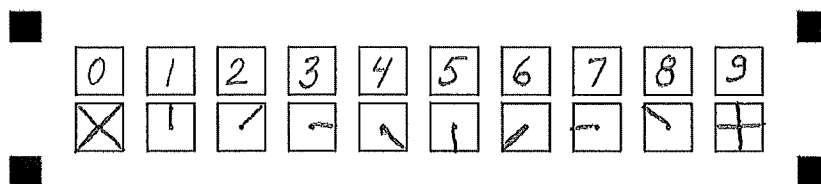
Hjälpmedel:

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:

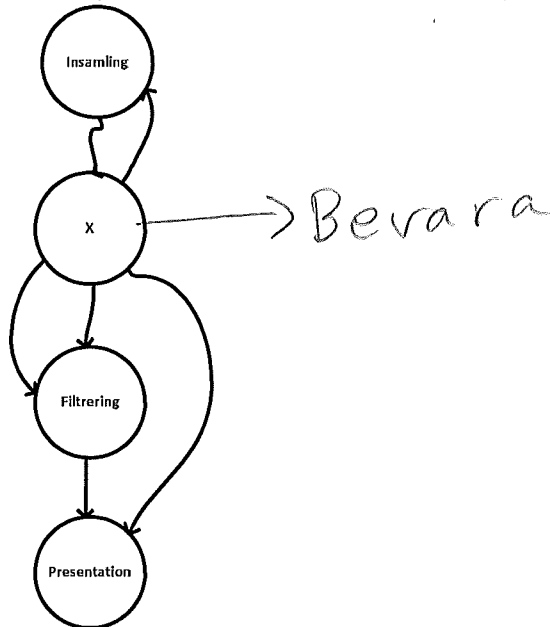
Anteckna svaren i provhäftet. När du är klar för du över svaren till svarsformuläret.
Svarsformuläret samt svar på lösa blad lämnas in. Provhäftet behålls eller kastas.
Skriv (och koda på blad 1) personnummer på varje blad. Även tomma blad som lämnas in.
Ansvarig för tentamen besöker tentasalen ca 1 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.
(Godkända kunskapsprov ger upp till 32 p bonus. Varje helt godkänt prov ~3p.)

1. Nedan syns en översikt av den forensiska processen enligt boken. Är x "analys"?



- A. Ja. B. Nej.
2. Är filer på en hårddisk att anse som volatila data?
A. Ja. B. Nej.
3. Måste två filer med samma MD5-summa ha exakt samma innehåll?
A. Ja. B. Nej.
4. Kan en RAID-5 array ha sämre skrivprestanda än de enskilda ingående diskarna?
 A. Ja. B. Nej.
5. Är det lämpligt att börja intervjua de som är mest misstänkta?
A. Ja. B. Nej.
6. Efter det att en incident detekterats så ska en checklista fyllas i. Första delen av checklisten 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/ Kvalificerad forensisk kopia" får komprimera tomma sektorer.

A. Ja.

B. Nej.

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

A. Ja

B. Nej

10. Kommandot netcat kan användas för att exportera data från en dator via nätverket:

A. Ja.

B. Nej.

11. Är det mest sannolikt att en dd-avbild blir strikt större än källan?

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, eftersom detta inte lämnar några spår på målsystemet."

A. Ja.

B. Nej.

17. En kollega hävdar att man ska köra målsystemets egen kommando-prompt vid live-utvinning. Stämmer det?

A. Ja.

B. Nej.

18. Ska verktygslådan (the toolkit) hanteras som ett bevis med tag och label efter att den använts 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

append

A. Ja

B. Nej.

20. Kommandot dd kan användas för att montera enheter.

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 som gått sedan senaste omstart.

A. Ja

B. Nej.

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

A. Ja

B. Nej.

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

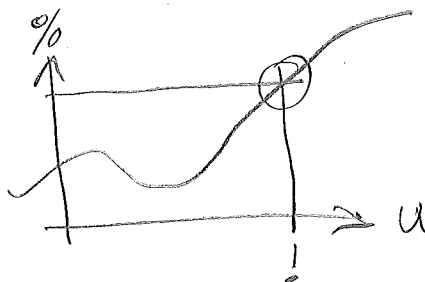
A. Ja.

B. Nej.

25.

A. Ja

B. Nej.



*Men frågan är
ganska svår.*

26. När du ska stänga av ett "hemma"-system (ej server) efter liveutvinning är det mest lämpligt att dra ur strömkabeln ur datorchassit.

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.

— SPAN

30. Din kollega hävdar att "en switch med CPIS 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 6 timmar och räknar fram att mängden data som ska loggas kommer inte att vara mer än 750 MByte per timma. Kommer diskutrymmet att räcka?

$$6 \cdot \frac{3}{4} = 4.5$$

A. Ja

B. Nej.

32. Måste filernas tidsstämplar utvinnas vid live-utvinningen?

A. Ja .

B. Nej.

33. Om man av misstag kontaminerar disken ska man försöka "ångra" felet, dvs. återställa disken till läget före kontaminering.

A. Ja.

B. Nej.

NEJ 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.

Hash!

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. lösenord går alltid att hitta med hjälp av strängutvinning.

A. Ja.

B. Nej.

37. En rapport måste alltid vara skriftlig.

A. Ja.

B. Nej.

38. PATA 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 tänker 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. (Inlämningsuppgift PB ger upp till 15 p.)

1. Ur forensisk synvinkel, varför är det lämpligt att köra wipe på en hårddisk innan du använder den i ett fall? (3p)
2. Rita ett exempel på hur Network Attached Storage fungerar i ett segment av ett LAN. (3p)
3. Beskriv hur RAID 5 fungerar. (3p)
4. En kollega har gjort ett experiment där man avbildat en disk över eSATA och Gigabit Ethernet respektive. Experimentet visar att metoderna ger samma avbildningstid. Förklara detta utfall. Gör egna antaganden. (3p)
5. Här ser du FAT-tabellen för en partition med endast tre filer. Alla kluster bortom kluster 10 är oallokerade. Hitta den största filen och ange vilka kluster den ockuperar. (3p)

FAT Table

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

6. Para ihop följande begrepp och benämningar två och två. Exempel: hänger 01 och 14 ihop anger du 01 – 14. Fel ger -2p. (min 0 p, max 7 p)

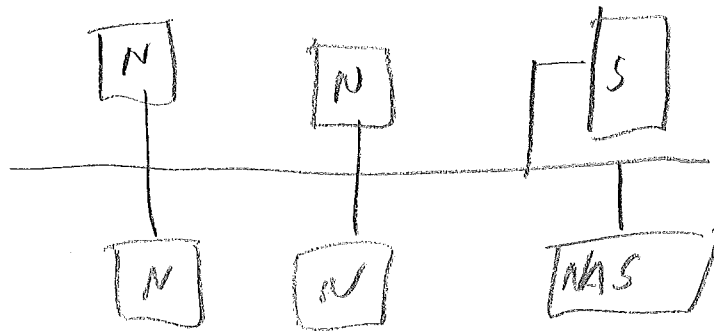
01. Avbild	06. Filsystem	10. Mönstermatchning
02. Brandvägg	07. grep	11. NTFS
03. Checksumma	08. Masslagrings- gränssnitt	12. IDE
04. defltd	09. MD5	13. Port
05. dir /t:a		14. Tidsstämpel.

7. Du vill göra en total avlyssning av en switch med 16 stycken 100 Mbit/s portar. Switchen har två speciella avlyssningsportar med prestandan 1 Gbit/s vardera 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. (6p)
8. Du har fått i uppdrag att göra avbilder av 30 stycken 500GB hårddiskar. Din enda avbildningsstation klarar av att kopiera diskar med en kapacitet av 60Mbyte/s. Hur lång tid i timmar måste du minst be om för att hinna klart med uppgiften? All utvinning sker seriellt. (6p)
9. Du har fått i uppdrag att under en arbetsdag (8h) göra avbilder av 10 stycken 750GB hårddiskar. Hårddiskarnas läskapacitet är 100Mbyte/s. Det är en ganska tight tidsplan, men du vill ju inte oroa gubbarna i onödan – så du tar en stund för dig själv och räknar lite på det där. Vilket minsta krav har du på din utrustning för att hinna med uppdraget? (6p)

Del 2

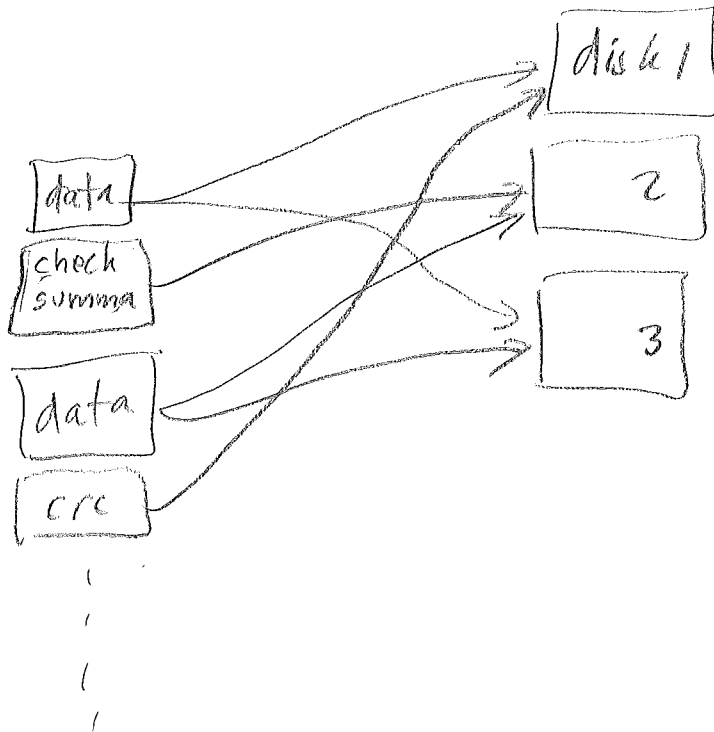
1. Kors kontaminering, best practice, du har koll.

2.



N = nod
S = server
NAS = disk

3.



4. eSata, max 3 Gbit/s

GB Ethernet, max 1 Gbit/s

källans läshastighet $\leq 1 \text{ Gbit/s}$ (ej troligt)

destinationens skrivhastighet $\leq 1 \text{ Gbit/s}$ (troligt)

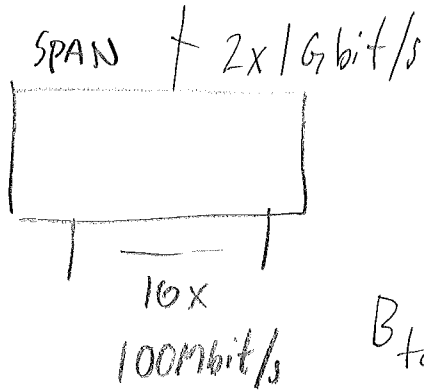
5.

2 → 3 → 5 → 9

6.

1-4 2-13 3-9 5-14
6-11 7-10 8-12

7.



$$B_{tot} = 1.6 \text{ Gbit/s} < B_{SPAN}$$
$$= 0.2 \text{ GByte/s} = 2 \cdot 10^8 \text{ Byte/s}$$

$$t = 20 \text{ h} = 20 \cdot 3600 \text{ s} = 72000 = 7.2 \cdot 10^4 \text{ s}$$

$$K = \frac{K}{B} \rightarrow K = t \cdot B$$

$$K = 7.2 \cdot 10^4 \cdot 2 \cdot 10^8 = 14.4 \cdot 10^{12} \approx \underline{15 \text{ TByte}}$$

8.



30 x 500 GB

B = 60 MB/s

$$t_s = \frac{K}{B}$$

$$K = 30 \times 500 \cdot 10^9 = 1,5 \cdot 10^{13} B$$

$$B = 6 \cdot 10^7 B/s$$

$$t_s = \frac{1,5 \cdot 10^{13} B}{6 \cdot 10^7 B/s} = \frac{3}{12} \cdot 10^6 = \frac{1}{4} \cdot 10^6 = 2,5 \cdot 10^5 s$$

i timmar: $t = \frac{2,5 \cdot 10^5 \cdot 10^2}{3,6 \cdot 10^3} = \frac{250}{3,6} \Rightarrow \underline{\underline{70 h}}$

69
 $\overline{2500} \overline{) 36}$
 - 216

 340
 - 324

 16 > 0

36
 $\overline{6} \overline{) 36}$
 216

 36
 9

 324

9. $t_p = 8 \text{ h}$

$K = 10 \cdot 750 \text{ GB} = 7500 \text{ GB} = 7.5 \text{ TB}$

$B = 100 \text{ MB/s} = 10^8 \text{ B/s}$

$t_s = \frac{7.5 \cdot 10^{12}}{10^8}$

i timmar $t = \frac{7.5 \cdot 10^4}{3.6 \cdot 10^3} \approx 20 \text{ h}$ | oj oj oj!

$t_s > t_p$! Hur många parallella spår måste vi göra?

$n = \left\lceil \frac{t_s}{t_p} \right\rceil$

$n = \left\lceil \frac{20}{8} \right\rceil = \left\lceil 2.5 \right\rceil = \underline{\underline{3}}$

$$\begin{array}{r} 2.5 \\ 20,0 \\ - 16 \\ \hline 40 \\ - 40 \\ \hline 0 \end{array}$$

Men 10 är inte delbart i 3!
 \Rightarrow Kolla att vi hinner rända

1	X	X	X	
2	X	X	X	
3	X	X	X	X

4 x 750 GB

$t_s = \frac{3 \cdot 10^{12}}{10^8} = 3 \cdot 10^4 \text{ s}$

i timmar:

$t = \frac{3 \cdot 10^4}{3.6 \cdot 10^3} = \frac{30}{3.6}$

$$\begin{array}{r} 8 \\ 30,0 \\ - 288 \\ \hline 120 \end{array}$$

Svar: 4 spår eller 3 spår och 9h.

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 korrekt beskrivning av det valda ämnet. Max en enkelsidig 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 vad man måste tänka på när man bygger ett forensiskt labb.
4. Beskriv hur man på lämpligt vis skulle kunna gå tillväga för vid anställning av en forensiker med specialisering på datautvinning.