

Praktiskt prov DT2005

2010-03-10

Hjälpmedel: *Inga*

Tid till förfogande: *45 minuter*

Betygsskala: *U/G*

För betyget G krävs att alla uppgifter utförts korrekt.

Läs följande orientering:

Wendy Sanders har precis blivit befordrad och tänkte fira detta med en kort semesterresa till Thailand. Precis efter det att hon lämnat Sverige så får personalchefen ett mail från Wendys e-postadress där hon säger att hennes assistent kommer att jobba med förberedelser under veckan. På grund av trafikproblem i Amsterdam så valde Wendy att avbryta sin utresa och återgå till arbetet redan dagen efter. Under dagen blir hon tillfrågad om sin assistent. Hon söker något snopet upp mannen som poserat som hennes assistent varpå densamme snabbt avviker från platsen. Tack vare snabba insatser lyckas man identifiera att mannen bott på Grand Hôtel på företagets bekostnad där han lämnat en laptop efter sig. Datorn tas in som bevis och det genomförs en datautvinning från hårddisken.

Målet med detta praktiska prov är att du ska genomföra ett antal moment vilka leder till ett antal bokmärken. Dessa bokmärken ska redovisas genom att exportera en rapport i rtf-format.

Alla filer du behöver finns på hårddisk D:, där du även ska spara filer i den förberedda filstrukturen. Det är viktigt att du följer instruktionerna noga och inte söker mer än angivet då detta kan ta för lång tid. Om du lägger till bokmärken för bild-data så ska bilderna visas i rapporten.

VÄNTA!

Vänd blad på tentamensvaktens signal.

Dina uppgifter:

1. Skapa ett nytt case.
2. Lägg till filerna från foldern hash-set.
3. Skapa ett nytt hash-set baserat på filerna du just lagt till. Namnet ska vara "Kittens" och typen ska vara "Notable".
4. Lägg till bevisfilen PM_Fraud.E01 till ditt case.
5. En verifiering startar automatiskt (se nedre högra hörnet). Avbryt denna.
6. Gör en signaturanalys för alla filer på hårddisk C.
7. Skapa bokmärken för alla omdöpta filer där signaturen anger att det är en fil av JPG-typ.
8. Generera hashsummer för alla filer på hårddisk C.
9. Slå på och refresha ditt hash-set "Kittens".
10. Skapa bokmärken för alla filer som är av typen "Notable".
11. Sök igenom allt oallokerat utrymme på hårddisk C efter raderade filer av typen JPG.
12. Skapa bokmärken för alla sökträffar du kan verifiera som JPG-data och där motivet är levande varelser.
13. Sök igenom hela hårddisk C efter Wendys epost (wendy_san@live.com).
14. Skapa ett bokmärke som indikerar att någon använt Wendys mailkonto från den beslagtagna datorn.
15. Gå till bokmärkesvyn och organisera dina bokmärken. Slå på set-include för alla bokmärken. Visa dina bokmärken som en rapport. Kontrollera att alla bokmärken visas korrekt i rapporten. Exportera rapporten till foldern report och döp den till Dittförnamn.Dittefternamn.rtf . Öppna rapporten och kontrollera att den ser korrekt ut.
16. Spara ditt case.
17. Anmäl till tentamensvakten.