Fråga 1 4p

Förklara vad som menas med "DIGITAL FORENSICS?

Fråga 2 4p + 4p

A) Förklara: vad är orsaken till att man gör en "forensic image"?

B) Det finns 2 huvudtyper av "forensic image"; så kallade "E0" resp "raw/iso/dd". Förklara skillnader samt fördelar och nackdelar.

Fråga 3 5p

Förklara hur man återskapar en fil som blivit raderad i MS-Windows-dator och kopplar filen till dess ägare.

Fråga 4 ***2+2p***

Hur kan man veta att ett speciellt USB minne varit inkopplat i en MS-Windows-dator?

Fråga 5 (4+4p)

När man exporterar ut filer från en foresic image så behöver du koppla filen till en ägare, hur görs detta?

A) för MS-Win NTFS

B) för linux Ext3

Fråga 6 (5p)

Redogör för de digitala bevis som kan hittas i en modern "smart phone" samt tillhörande metadata och på vilket sätt den informationen kan användas för att förbättra utredingen.

Fråga 7 (2+2+2+2+2+2+2+2=16p)

Diskutera och redogör för var och en av nedanstående punkter.
(Vad menas med X , X resulterar i, X används till)

A) Timeanalys 2p
B) Harvesting 2p
C) Reconstruction 2p
D) Reduction 2p
E) Carving 2p
F) Preservation 2p
G) Recovery 2p

H) Sätt alla ovan i rätt ordning. ***Motivera ordningsföljden*** 2p

Fråga 8 (2+2+2p)

Beskriv följande termer, redogör för fördelar/ nackdelar och förväntad nytta/resultat ,

A static forensics
B live forensics
C network forensics

Fråga 9 (5p)

För att digitala bevis skall vara användbara krävs att bevisen uppyller tre krav,
Vilka ? Samt motivera svaren

Fråga 10 (3 p)

MO är ett begrepp inom " Kriminologi".

Vad menas med MO, och på vilket sätt kan MO vara till hjälp vid en undersökning?