Tentamen I Digital Undersöknings teknik och digitala bevis

Ex . är Frågor där du förtydligar funktioner begrepp som har relevans för en forensisc undersökning :

Diskar: partionstabeller, Slack space, HPA

Filsystem: EXT 2,3,24NTFS/FAT/EXFAT/FAT32,

Filer: metadata, återskapa,

Operativsystem, med processer,

Nätverk, metatdata i nätverk, / kommunikation
ex hur kopplas en process ihop med en pågående/established socket

Hur kopplas en pågåående pårosess i ett Operativsystem med en användare

Beskriv följande, Vad är speciellt med :

A static forensics
B live forensics
C network forensics ?

För att Digitala Bevis skall vara användbara behöver de vara ,
Vilka?

- Fördel nackdel mellan static forensics / live forensics

- Beskriv kortfattat generella regler kring en forensisc rapport
  Rubriker – kortfattat om resp rubriuks innehåll

- Redogör vad som menas med MO Modus Operande
  och hur det kan hjälpa en undersökning.

Beskriv varför/hur en fil som raderats i ett ext2/3 filsystem kan återskapas.

Förklara vilka olika varianter/delar av en fil som kan återfinnas på en image/disk

Redogör för de digitalt bevis som kan hittas i en modern ”smart phone”
samt tillhörande Metadata, och på vilket sätt den informationen kan användas i en utredning för att fördjupa utredingen

A) Timeanalys
B) Harvesting
C) Reconstruction
D) Reduction
E) Carving
F) Preservation
G) Recovery
H) Report
I) Analyse

I definition av digitala bevis

Mallware Forensics / frågor koppklade till Memory / mallware forensics.

Vad är ett Rootkit:

Vilken fördel