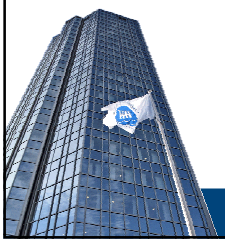
Bevishantering



Vad är bevishantering?

- Vad är bevis?
  - Data, information och bevis
- Bästa bevis?
- Original?
- Utmaningar
  - Dokumentation/ paper trail
- Autentisering
- Beviskedjan
- Validering

- (198-201)

Bevishantering - översikt

- Dokumentera information om miljön där mediet befunnit sig.
- Fotografera originalsystemet
- Förbered en etikett för varje original
- Märk upp alla original
- ”Bästa bevis” förvaras i ”kassaskåpet”
- Bevisförvaltaren loggar incheckningen av bevisen
- Utför undersökningen på arbetskopior (forensiska kopior av ”bästa bevis”)
- Förvaltaren tar backup på incheckat material
- Förvaltaren rensar ut enligt tidsangivelse från utredaren
- Förvaltaren utför validering av incheckat material
- (202)

Bevismiljön

- Vem befann sig i lokalen där beviset påträffades?
- Vem har haft tillgång till lokalen?
- Vilka har tillgång till systemet?
- Vart fanns systemet rent fysiskt?
- Var systemet på eller av? Fanns data på skärmen?
- Vilken tidsangivelse gav systemet jämfört med korrekt tid?
- Vilka nätverkskopplingar finns/ har funnits?
- Vilka var närvarande vid dupliceringen?
- Dokumentera serienummer, modellbeteckningar, varianter av hårddiskar och övriga systemkomponenter.
- Dokumentera övrig kringutrustning.
- (203)

Översikt - originalhantering

- (204)

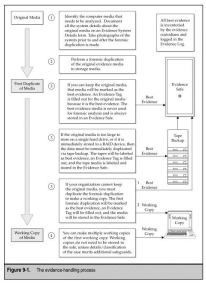


Figure 9-1. The evidence-handling process

Hur kan foto användas?

- Datorn ska ihop igen
- Dokumentera konfigurationer
- Dokumentera redan i bilden
- Undvika åverkan/ dokumentera
- Återställning vid dold undersökning
- Se exempel (p3)
- (204)

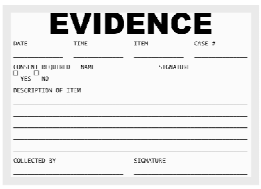
Bevisanvisning (tag)

- Se exempel.
- (205)

Bevismärkning (label)

- Se exempel.
- (207)

Tag


EVIDENCE

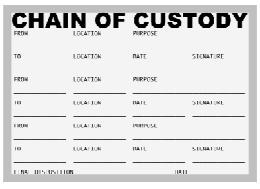
DATE TIME ITEM CASE #

FOUND BY NAME

☐ YES ☐ NO

DESCRIPTION OF ITEM

COLLECTED BY SIGNATURE


CHAIN OF CUSTODY

FROM LOCATION PURPOSE

TO LOCATION DATE SIGNATURE

FROM LOCATION PURPOSE

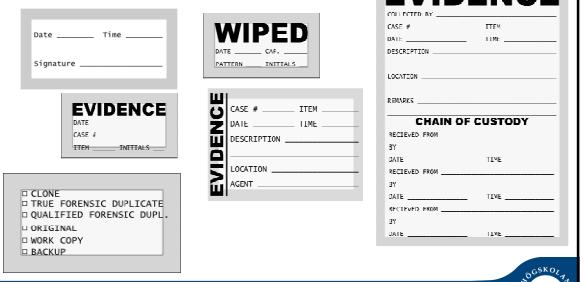
TO LOCATION DATE SIGNATURE

FROM LOCATION PURPOSE

TO LOCATION DATE SIGNATURE

FINAL DISPOSITION DATE

Labels



Förvaring och transport

- Förpackning
- Skydd
- Säkring
  - "Plastlås"
- (207-210)

Bevisloggen/ beviskedjan

- Se exempel (p4).
- (210)

Arbetskopia

- Inget egentligt säkerhets/ intrångskrav.
- Undantag: känslig information
- (211)

Beviskopiering

- Backup
- Storlek!!!
- Metod?
- (211)

Bevisgenomgång

- Rutiner
- Inventering
- Utrensning
- Backup
- Wipe
- (212)

Förbered

- Gruppuppgift

- Valfria fördjupningsuppgifter
- Läs fördjupning om AdWare
- Läs fördjupning om hur tcpdump fungerar
- Läs fördjupning om L0pth's Antisniff
- Läs fördjupning om FreeBSD