Gästföreläsning - protokollskrivning

Per Johansson - IT-forensiker. IT-brott grupp 3.

Protokollskrivning

Undersökningens syfte

1. Klargöra om ett brott begåtts och i så fall hur det har genomförts
2. Klargöra för hur gärningsmannen har agerat
3. Klargöra om det finns spår som talar mot en bestämd gärningsman
    1. Dammsug tidslinjen
4. Klargöra om det finns spår som kan binda en gärningsman till brottet

Objektivitet

Det är inte en forensikers jobb att belägga kuld. En undersökning ska ta med allt som talar för och mot en misstänkt. Skyddat i grundlagen.

Mottagaranpassning

"Film" innebär att videon är garanterat komplett. Använd därför "videoklipp".

En ny installation Windows 10 är 10.9 GB. "Vanliga dödliga" förstår inte det. De förstår däremot 2725000 A4-sidor skrivna i Word.

Nämndemän består av förtroendevalda politiker - inte specialister. De måste förstå.

Tänk på:

- Vilka förkunskaper har läsaren / mottagaren?
- Vem ska läsa protokollet / rapporten?
    - Åklagare
    - Advokater
    - Domstolar (tingsrätt, hovrätt, högsta domstolen),
    - Målsägare,
    - Misstänkta,
    - Journalister,
    - Forskare,
    - Kunden

Vad ska rapporten innehålla?

Fetstilt är viktigt, kursivt mindre viktigt.

Det är ingen "C-uppsats" - det är kort och sammanfattande.

- **Inledande uppgifter**
  - Kan vara i punktform
  - Undersökning behärd av
  - Anledning till undersökningen
  - Handläggare / medundersökare
  - Plats och tider för undersökningen
  - Övrig information
- **Sammanfattning**
  - En tredjedel av en A4 att sammanfatta en hel undersökning, men kan vara så kort som "vid undersökningstillfället har ingen lagrad information påträffats som anses vara av intresse för aktuell utredning" eller liknande
- *Innehållsförteckning*
- *Bakgrundsuppgifter*
- **Beskrivning av material**
  - Vad är det som undersöks, en stationär dator, vilken (serienummer etc.)?
  - Vissa bevis förstörs då de saknar koppling till fallet
  - Kan vara bilder på datorn (med serienummer)
- **Iakttagelser och undersökningar**
  - Enda stället man kan vara teknisk. Förklara IT-termer (kan göras med fotnot)
  - "hash" har olika betydelser beroende på åhörare - MD5 eller gräs - ett digitalt fingeravtryck
  - EXIF-data säger inte mycket - en karta kan hjälpa visualisera
  - "Rå information"
  - Kan innehålla skärmdumpar. Markera viktiga delar
  - Historik etc. kan komma i appendix
  - "**Användaren** av datorn gjorde A" - inte misstänkt
- **Analys och slutsats**
  - Innehåller inte särskilt mycket. Forensiker kan komma att bli tillfrågade att presentera allt som hittats och då kommer ytterligare presentationer ändå
  - Sy ihop undersökningen, använd specialistkompetens, använd värdeord (se nedan)
  - Fanns inget av intresse - ta inte med denna punkt - finns istället i sammfattningen
- Materialförteckning
  - Vad har undersökts?
  - Materialmärkning (internt nummer), beslagsnummer, benämning (mobiltelefon, dator), datum och tid för beslag, vem som tog objektet i beslag
  - I Sverige attackeras inte Chain of Custody, men i andra länder förekommer det. Men det är viktigt att tänka på ändå
  - Måste vara noggrant
- *"Undersökningsmetoder"*
  - Metoden ska förklaras, men allt måste inte förklaras. Ibland vill man "inte utbilda kriminella" för hur man gör saker

    - Bevissäkring av hårddisk och hashning ska vara med
    - Kan beskriva hur materialet handskats

Värdeord

- ...visar att...
- ...ger starkt stöd för...
- ...ger stöd för...
- ...talar varken för eller emot...
- ...anses kunna vara av intresse...

Det är svårt att vara hundraprocentig. Om du skriver antal måste det stämma exakt. Var försiktig med exakta siffror.

Undersökningsmetoder

- Det kan vara enklare att göra en undersökning själv - helhetsbilden i huvudet hela tiden
- Torrentfiler som finns kvar
- Länkfiler
- Thumbnails
- Ser datorn ny ut? Används den ofta?
- Är det SMS som skickats? Fokusera på SMS, men bilder kan finnas innehållande saker så som skärmdumpar
- Kommunikation är mycket viktigt - vad ska göras?
- Dokumentera hur bevis hanterats och lagrats
- Rapportskrivning påbörjas den dag undersökningen är klar
- För en dagbok om du inte har den unika förmågan att hålla allt i huvudet över tid
- I USA, exempelvis begärs "case notes" ut. Hur forensikern jobbat - dagbok och kommandon som körts
- Anteckna i dagboken vilka frågetecken som kvarstår
- Skriv med olika färger beroende på vikt (för att kunna sålla vid ett senare tillfälle)
- Hittar du något intressant? Vad hände före och efter, i närhet? Inloggning på mejl, nätbank etc.
- Lösenordsskyddat och inte automatisk inloggning? Då stärker det misstanken att det är en viss person. Är det inget lösenord eller automatisk inloggning så kan det vara fler som använt datorn.