IT-FORENSISKA UNDERSÖKNINGAR

Mattias Martinsson
Länskriminalpolisen Halland

mattias-c.martinsson@polisen.se

Introduktion

- Bakgrund.
- Att arbeta inom polisen.
- Andra arbetsgivare.
- Från beslag till protokoll.
- Presentation av projektarbete.

mattias-c.martinsson@polisen.se

Bakgrund

- Utbildningsbakgrund.
- Yrkesbakgrund.
- Vilka är kollegorna?

mattias-c.martinsson@polisen.se

Att arbeta inom polisen

- Ej en vanlig arbetsplats.
- Civil i en icke-civil värld.
- Alla dessa system…
- och alla dessa förkortningar!!

- En intressant arbetsplats där man gör en insats.

mattias-c.martinsson@polisen.se

Andra arbetsgivare

- Tullverket.
- Skattemyndigheten.
- Ekobrottsmyndigheten.
- Privata firmor:
  - Vanligt i t ex USA, kan förmodas bli vanligare även i Sverige. Arbetar med interna utredningar på företag eller som stöd åt försvarare i rätten.

mattias-c.martinsson@polisen.se

Vanliga arbetsuppgifter

- Teknisk undersökning av beslag.
- Konvertering av ljud- och bild:
  - T ex övervakningskameror
- Tekniskt stöd åt utredare.
- IT-juridiskt stöd åt utredare.

- Utbildning, utbildning och åter utbildning!

mattias-c.martinsson@polisen.se

IT-brott?!

- Tidigare använde man sig gärna av benämningen IT-brott, men förutom dataintrång sysslar vi sällan med renodlade sådana. Det mesta är ”vanliga” brott som:
  - Narkotikabrott
  - Bedrägerier
  - Våldsbrott
  - Barnpornografibrott
  - Stöldbrott

mattias-c.martinsson@polisen.se

Undersökningsprocessen

- Tvångsmedel
  - Husrannsakan
  - Beslag

- Teknisk undersökning
  - På plats ”Live Forensics”
  - I verkstad etc

mattias-c.martinsson@polisen.se

Live Forensics

- Samarbeta med kriminaltekniker och övriga!
- Ibland det enda vettiga alternativet
- T ex vid kryptering, ”fara i dröjsmål” eller känsliga datormiljöer som större företagsservrar.
- Avvägning intakta bevis kontra risken att missa viktig information.
- RAM-dump, selektiv kopiering, avfotografering, nätverksanslutningar m.m.

mattias-c.martinsson@polisen.se

Teknisk undersökning

- Undersökning av föremål i beslag
  - Demontering av hårddisk eller via nätverkskabel.
- ”Spegelkopiering” = skydda originaldata!
  - Skrivskyddat originalmedia.
  - Fysisk kopiering = allt tas med.
  - Undersökningsarbete sker mot kopian.
  - Kopian arkiveras, vanligen 5 år.

mattias-c.martinsson@polisen.se

Verktyg

- De vanligaste programvarorna är:
  - EnCase (Guidance Software).
  - Forensic Toolkit (Access Data).
  - ILook (US Department of the Treasury).
  - Smart for Linux (ASR Data).
  - Samt en hel del stödprogram för olika ändamål.

mattias-c.martinsson@polisen.se

Vad letar vi efter?

- I bästa fall får man tydliga undersöknings-direktiv av utredare eller förundersöknings-ledaren. Exempelvis ”sök efter dokument som innehåller ordet MORD”.
- Vanligare är tyvärr ”leta efter allt som kan ha med utredningen att göra”…
- Sökordslistor är inte så dumt.
- Vi använder också de polisiära systemen och registren för att söka information.

mattias-c.martinsson@polisen.se

Sånt som kan vara intressant

- Dokument av olika slag
- Bilder
- Chattloggar
- Epost
- Surfhistorik
  - (helst sökningar i stil med ”hur gömmer jag ett lik?”)
- Kontakter

mattias-c.martinsson@polisen.se

En bra början

- En första fråga man kan ställa sig är:
- ”Vem är egentligen den misstänkte?”
- Svaret kan finnas i datorn. Därför är det viktigt att skaffa sig en överblick av såväl personen som dennes datorkunnighet. Det är troligare att en ”hacker” har krypterade containers än att den som bara haft sin dator till att surfa med har det.
- Allt innehåll bör åtminstone skummas igenom.

mattias-c.martinsson@polisen.se

Söka information

- Två huvudsakliga söksätt:
  - Indexerad sökning, där man låter datorn skapa en databas över allt som inte är skräptecken. Tar lång tid att skapa, sedan går sökningarna snabbt. Hittar förstås endast det den indexerat.
  - ”Live sökning”, som görs på byte efter byte. Tar lång tid varje gång, men kan ta mer flexibla sökmetoder än indexerad sökning. Exempelvis GREP/reguljära uttryck för sökning efter telefonnr, kreditkort m.m.

mattias-c.martinsson@polisen.se

Oallokerat utrymme

- IT-forensikerns bäste vän.
- All data som inte skrivits över går att återskapa, även om man formaterat om och raderat partitioner.
- En analog jämförelse kan vara registret i en pärm. Även om man sliter ut det så finns sidorna i pärmen kvar, men man får leta manuellt för att hitta dessa.
- Viktigt att förstå filsystemets uppbyggnad.

mattias-c.martinsson@polisen.se

Oallokerat utrymme

- Vad hamnar i oallokerat utrymme?
  - Allt som raderas ”permanent”.
  - Tömning av papperskorgen.
  - RAM via swap-fil på hårddisken.
  - Webmail via cache.

mattias-c.martinsson@polisen.se

Kryptering

- Hot mot verksamheten, i stort sett omöjligt att med dagens datorer knäcka de mer avancerade krypteringsalgoritmerna.
- Ordliste eller ”brute force” –attacker mot lösenordet enda rimliga metoden.
- Exempel TrueCrypt med dolda containers samt dolt operativsystem!

mattias-c.martinsson@polisen.se

Protokoll

- Det vi finner ska presenteras på ett sätt som gör att inte fullt så datorvana utredare, åklagare och nämndemän förstår.
- Det är ingen gissningstävling.
- ”Troligen” är ett bra ord, precis som ”rimligen”.
- Ett protokoll ska vara neutralt, vår uppgift är lika mycket att fria som att fälla.

mattias-c.martinsson@polisen.se

Rättegång

- Protokollet kommer förmodligen att hamna i förundersökningsprotokollet, den s k ”Fuppen”, som utgör åklagarens material i rätten.
- Är något otydligt, ämnet svårbegripligt eller liknande kan man få vittna på sitt protokoll.
- Ta inte med komplicerade saker i onödan!

mattias-c.martinsson@polisen.se

Projektarbete

- Tre olika fall – tre olika förutsättningar
- Det primära är att lösa uppgiften på ett bra sätt, med stöd i föreläsningen samt övrigt material ni fått tillgång till.
- Ska läggas upp på studieportalen.
- Godkänd eller underkänd.

mattias-c.martinsson@polisen.se