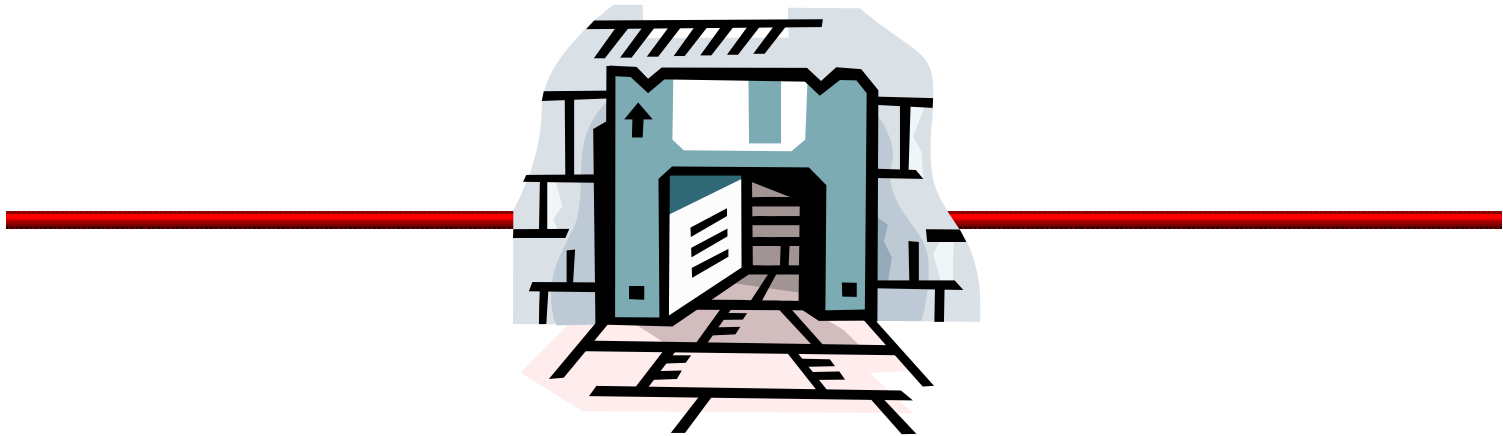


Brott och digitala bevis

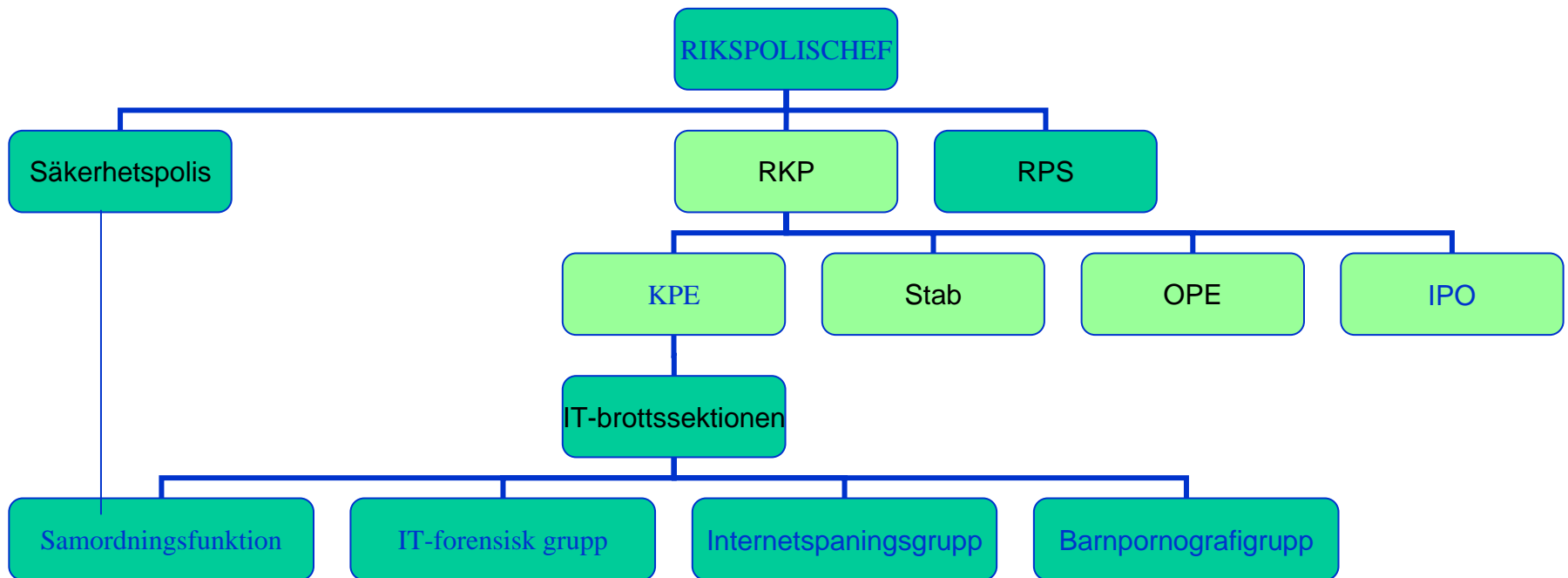


Stefan Kronqvist
e-Stockholm '08
2008-11-18



RKP:s IT-brottssektion

Var finns vi i organisationen?



Verksamhet

- Biträda polismyndigheterna operativt
- Internationell verksamhet
- Utbildning, teknikutveckling, metod d:o
- 24/7-beredskap
- Internetspaning
- Näringslivssamverkan
- IT-brottsforum
- Samordning polismyndigheter och andra myndigheter avseende ärenden, underrättelser och brottsförebyggande åtgärder



Operativ verksamhet

- Vanligaste brotten 1998 - 2007:

Grova narkotikabrott, vålds- och fridsbrott, barnpornografibrott



Statistik

- IT-brott vad är det? Två brott – dataintrång och datorbedrägeri. Veldig många andra brott kräver dock särskild kompetens för att utreda
- Statistik har hittills saknats i egentlig mening – ingen särskild kodning har använts. Undantag: dataintrång Brb 4:9 c §
- Datorbedrägeri Brb 9:1 § 2 st. samredovisades med automatmissbruk i statistiken
Fr.o.m. 2006 har BRÅ infört särskild kodning av Internetbedrägerier och internetrelaterade barnpornografibrott. Inte fullt genomslag ännu.



Utbildning

- Numera finns en särskild PHS-utbildning för s.k. IT-brottsspecialister
- Utbildningslinje totalt 20 veckor fr.o.m. 2007
- Fortbildningskurser arrangeras även av PHS
- Fristående kurser nationellt och internationellt



Brotten

- Alla traditionella brott som våldsbrott, narkotikabrott och förmögenhetsbrott där särskild utredningskompetens erfordras
- Ekobrott
- Barnpornografibrott
- Nätrelaterade bedrägerier (kort, affärer)
- Intrång etc (dataintrång, systemsabotage)
- Företagsspioneri/trolöshet mot huvudman
- Upphovsrättsbrott/varumärkesintrång
- Näthandel med illegala tjänster/produkter (koppleri, droger)



Vad är digital bevisning?

- Per definition: Med digitala eller elektroniska bevis avses information eller data som lagras i eller förmedlas av en elektronisk utrustning.
- Digitala sammanställningar (Power Point-presentationer etc.) eller bearbetningar av annat än ursprungligen datalagrad bevisning är inte digitala bevis enligt denna definition
- Bygger på internationella definitioner



Internetbevisning

- Inhämtning av bevisning från Internet består egentligen av två saker :
- Identifieringsbevisning (spårning)
- Informationsbevisning (säkring av information om brottet eller om informationen utgör brottet)
- Särskilda förhållanden gäller ifråga om bevis från Internet. “Allting är inte som det verkar!”
- Uttrycket “någon annan har kört via min dator” kan inte avfärdas utan vidare.



Digital bevisning i samband med ~~husrannsakan och beslag~~

- Datorer och andra IT-hjälpmiddel finns i alla brottsutredningar
- Man bör vara beredd på detta i utredningsupplägget
- Digital bevisning är numera ett vanligt inslag även i "traditionella" utredningar



Husrannskan och beslag - metoder

- Tre operativa huvudfaser:
- Före – under – efter åtgärden

- Fyra huvudsakliga hanteringsfaser:
- Insamling – undersökning - analys - dokumentation



När beslut fattats...forts

- Tänka igenom om åtgärden innebär driftstörningar eller integritetsstörningar för personer/företag som inte har med utredningen att göra.
- Förbereda teknik som kan underlätta vid ingrepp i ett företag; t.ex. utrustning för kopiering av stora datavolymer.



Att tänka på vid brottsplatsundersökning

- En dator kan innehålla bevisning och betydelsefulla uppgifter om brottet; tidpunkter, mail m.m.
- Stäng aldrig av en påslagen dator utan att ha rådgjort med en expert (om du inte själv är en sådan).
- Slå aldrig på en dator utan att ha rådgjort med....(se ovan)



Brottsplats forts....

- Genomför aldrig bearbetningar eller "raca runt" i en dator som har betydelse eller kan ha betydelse i en brottsutredning



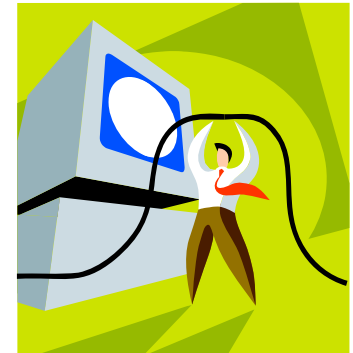
Varför?

- Kryptering eller låsning av systemet kan ske
- Systemet skriver på disk vid uppstart och avstängning
- Tidsstämpling och omfattning av filer kan förändras
- Originaldata kan förändras
- Trovärdighetsproblem i en process



Vid analysen

- Polisen jobbar i princip aldrig i originalet utan i en kopia. Kan vara en ren datakopia som tas med backup-program eller en mirror image(spegling) som görs med särskild utrustning.



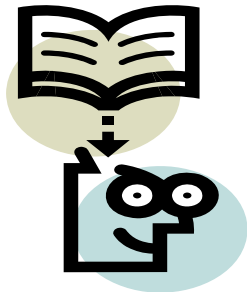
Polisens analysprogram

- EnCase är f.n. det dominerande. Utvecklat av ett amerikanskt dataföretag (Guidance Software) och är allmänt använt inom europeiska polisorganisationer.
- Andra liknande program finns; t.ex. ILook (används av bl.a. FBI) och Forensic Toolkit Programvarorna används vid spegling och analys av hårddiskar; kan även läsa raderade filer m.m.
- SKL studerar fortlöpande dessa mjukvaruverktyg.



Under och efter analysen, forts

- Dokumentation över vad som gjorts
- Redogörelse för genomförda bearbetningar, t.ex. rapporter från en databas eller d:o från bokföringsprogram, bildbehandling m.m.
- Användning av lathund om det finns tillgång till sådan.



Övrigt

- Mobiltelefoner, faxar, (vissa) personsökare och PDA:er är också datorer! En dator kännetecknas av att den innehåller en processor och ett lagringsmedium.
- Raderat utrymme kan ofta återvinnas. Gäller även "normalt" formaterade diskar. Överskriven data kan antagligen inte återställas. "sju lager" är tyvärr en myt.



Mobiltelefon- problematiken

- Utvecklingen har exploderat, både vad avser teknik och förekomsten av telefoner i brottsutredningar.
- Den strategi som finns, när det gäller kompetenshöjande åtgärder avseende undersökning datorer i brottsutredningar och bekämpning av Internetbrott har saknats på mobiltelesidan
- Utbildning finns numera
- "Lathund" har sänts ut till samtliga pmynd och finns även på IT-brottsforum



Hur får vi tillgång till information i Cyberrymden?

- Öppna källor – information som i princip är tillgänglig för alla.
- Abonentuppgifter och historiska trafikuppgifter – lag 2003:389 om elektronisk kommunikation (6 kap. 20, 22 §§)
- Innehåll i elektroniskt meddelande från/till skäligen misstänkt persons teleadress – HTA/HTÖ



Anmälningar

- En anmälan kan givetvis göras vid vilken polisstation som helst, men i vissa ärenden kan ett möte med målsägaren rekommenderas
- Vid komplicerade fall ta hjälp av en IT-brottsspecialist. Se till att målsägaren tar med dokumentation som är begriplig
- Företag bör förberedas på viss egen insats, t.ex. utse kontaktperson, "uthållighet", arbetsinsatser

