

Loggar som bevisning

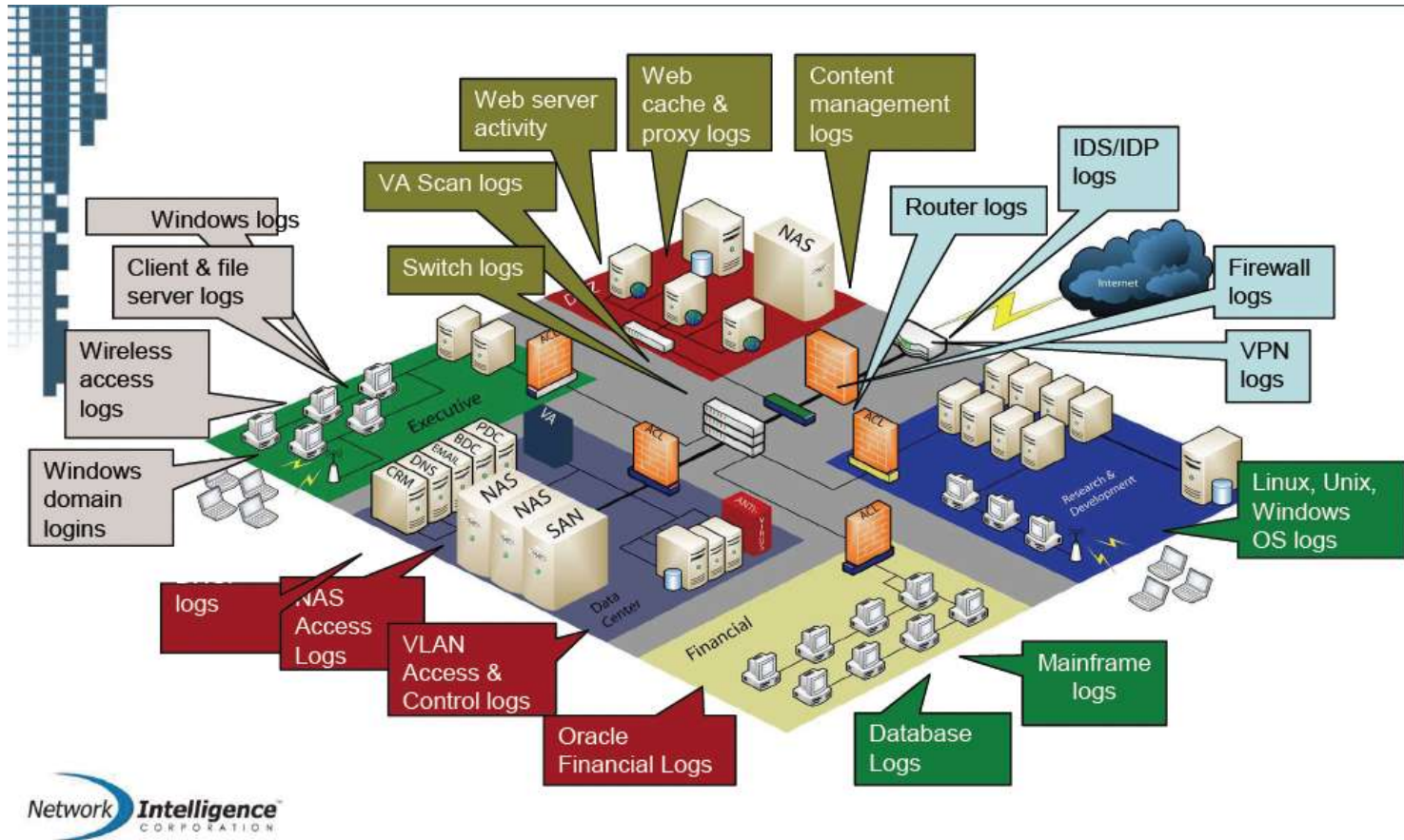


Roger Lindblom

roger@alinda.se

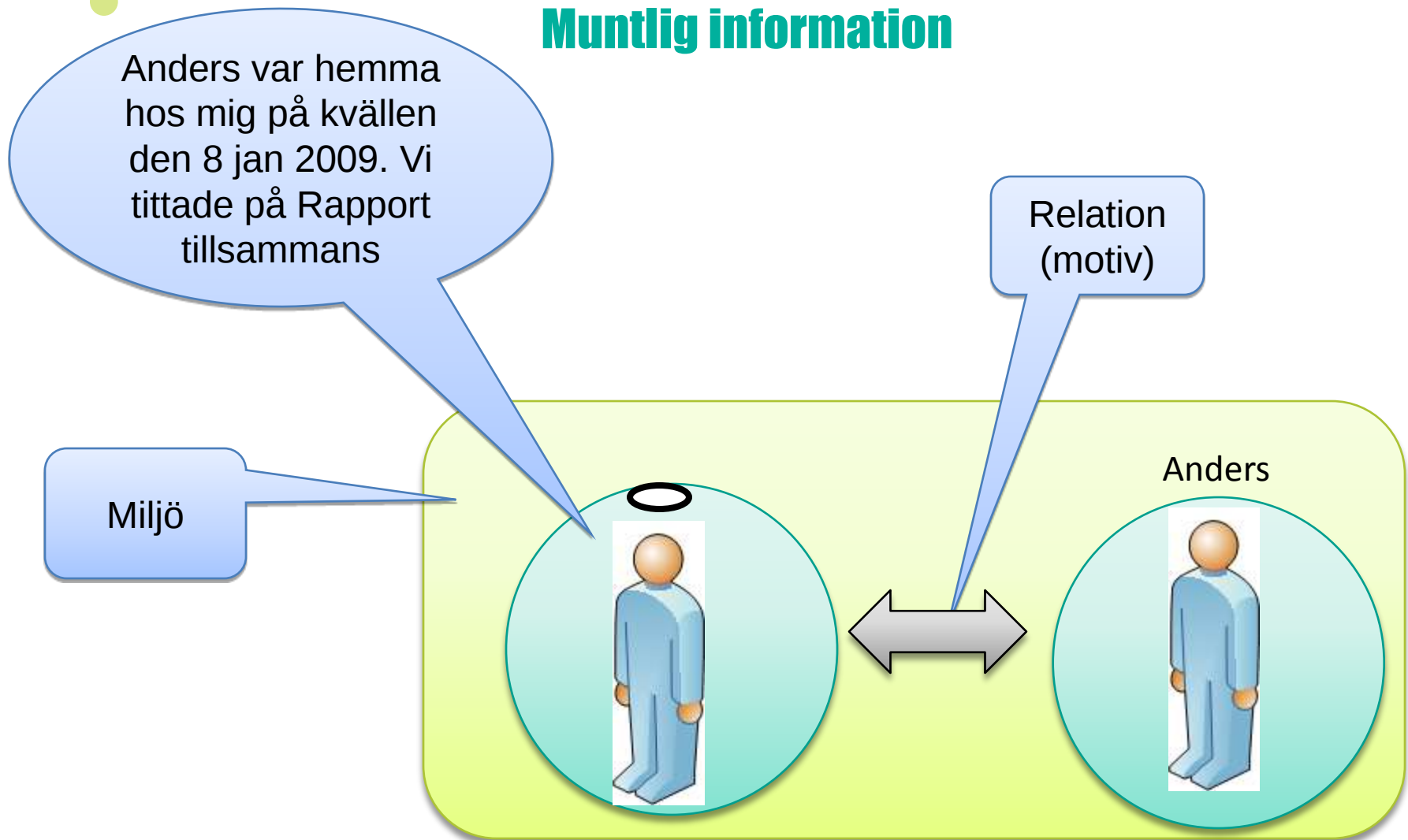
Tel: 070-206 10 26

Loggar som bevisning



Bevisvärdering

Muntlig information





Bevisvärdering

Skriftlig information

Riktighet:

Att
handlingens
innehåll inte
har förändrats

Anders var
hemma hos mig
den 8 dec 2009.
Vi tittade på
rapport
tillsammans

Jonas Jensen

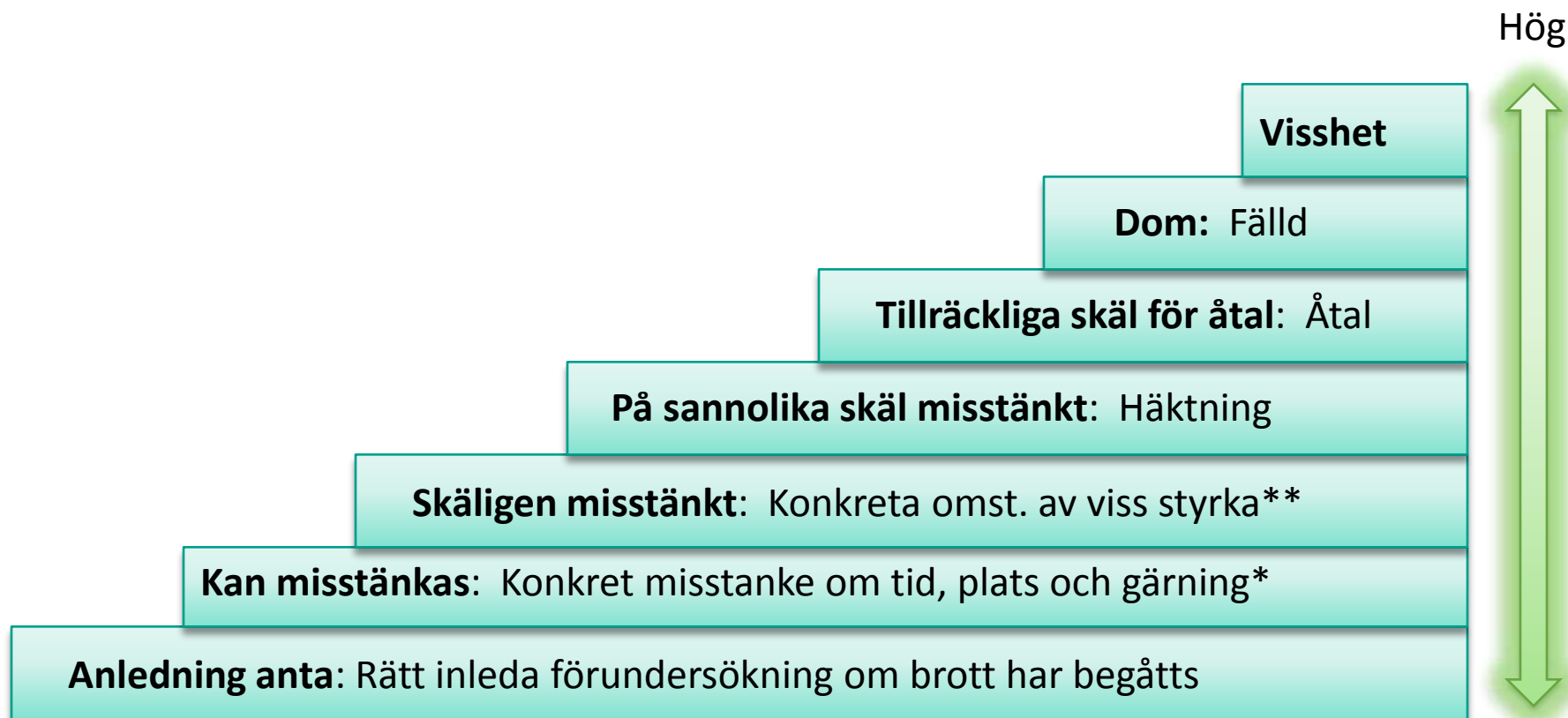
Autenticitet:

Verifiering av
handlingens
upphovsman,
framställningstid och
tillkomstförhållanden



Bevistrappan i RB

Graden av sannolikhet inom rättsväsendet



- *HÄFÖ, ögonundersökning (narkotika) som kan leda till skälig misstanke
- **Gripa, husrannsakan, kroppsbesiktning, häktning kortare tid



Bevisvärdering

Applikationslogg

•2009-10-21T14:48:25.781+0200|200908110001|||kvr|172.31.10.52||vm225639|Läsa|1|0|PersonDTO|193704260000|Personnummer|||

•2009-10-21T14:47:41.507+0200|200908110001|||kvr|172.31.10.52||vm225639|Läsa|1|1|PersonDTO|196001250000|Personnummer|||

•2009-10-21T14:47:25.803+0200|200908110001|||kvr|172.31.10.52||vm225639|Läsa|1|1|PersonDTO|196001250000|Personnummer|||

•2009-10-21T14:45:14.449+0200|200908110001|||kvr|172.31.10.52||vm225639|Läsa|1|0|PersonDTO|195506300000|Personnummer|||

•2009-10-21T14:44:54.694+0200|200908110001|||kvr|172.31.10.52||vm225639|Läsa|1|0|PersonDTO|196305090000|Personnummer|||

•2009-10-21T14:44:39.520+0200|200908110001|||kvr|172.31.10.52||vm225639|Läsa|1|0|PersonDTO|196305090000|Personnummer|||

•2009-10-21T14:44:17.053+0200|200908110001|||kvr|172.31.10.52||vm225639|Läsa|1|0|PersonDTO|196305090000|Personnummer|||

•2009-10-12T13:54:02.503+0200|407402010032|||KVR-L|172.31.10.60||vm2256396|Söka|1|1|PersonDTO|||postnr=;brottKlartext=;anstalt=AnstaltDTO[id=1;namn=ASPTUNA;];brottLagrum=Alla Samtliga lagstiftningar SFS: ;over4Ar=0;||

•2009-10-12T13:53:41.530+0200|407402010032|||KVR-L|172.31.10.60||vm2256396|Söka|1|1|PersonDTO|||postnr=;brottKlartext=;anstalt=AnstaltDTO[id=7;namn=GRUVBERGET;];brottLagrum=Alla Samtliga lagstiftningar SFS: ;over4Ar=0;||



Autentiseringslogg

03/08/06 09:57:43 boks-replika3.appl.se - RsaAuth from 193.234.24.194: Authentication success using virtual card kalors
03/08/06 09:57:53 boks-replika3.appl.se - RsaAuth from 193.234.24.194: Authentication success using virtual card stejon
03/08/06 09:58:07 boks-replika3.appl.se - RsaAuth from 193.234.24.154: Authentication success using virtual card roglin
03/08/06 09:58:43 boks-replika3.appl.se - RsaAuth from 193.234.24.122: Authentication success using virtual card andlin
03/08/06 09:59:13 boks-replika3.appl.se - RsaAuth from 193.234.24.168: Authentication success using virtual card roldju
03/08/06 09:59:27 boks-replika3.appl.se - RsaAuth from 193.234.24.99: Authentication success using virtual card P4559
03/08/06 09:59:43 boks-replika3.appl.se - RsaAuth from 193.234.24.23: Authentication success using virtual card P3441
03/08/06 09:59:53 boks-replika3.appl.se - RsaAuth from 193.234.24.138: Authentication success using virtual card K1346
03/08/06 10:00:07 boks-replika3.appl.se - RsaAuth from 193.234.24.143: Authentication success using virtual card olljon
03/08/06 10:00:43 boks-replika3.appl.se - RsaAuth from 193.234.24.84: Authentication success using virtual card svennis
03/08/06 10:01:13 boks-replika3.appl.se - RsaAuth from 193.234.24.103: Authentication success using virtual card torgus

Hur värderar vi bevisvärdet av dessa loggposter?



Bevisvärdering av en loggpost

Loggpostens sak- och sanningsinnehåll

- En loggpost kan vara sann till sitt sakinnehåll men samtidigt falsk till sitt sanningsinnehåll.
- Detta sker om jag loggar in i ett IT-system med din användaridentitet.
- Loggposten pekar felaktigt ut dig som ansvarig för operationerna i IT-systemet och inte mig.



Exempel på deduktion

- **Premiss 1.** Alla människor är odödliga.
- **Premiss 2.** Sokrates är en människa.
- **Slutsats.** Sokrates är odödlig.
- För att slutsatsen skall vara sann måste samtliga premisser vara sanna.



Deducering av en logg

- **Premiss 1.** Loggen visar att **roglin** har loggat in i lönesystemet och höjt sin lön från x till y kronor
- **Premiss 2.** **roglin** = Den fysiska personen Roger Lindblom
- **Slutsats.** Roger Lindblom har höjt sin egen lön i lönesystemet från x till y kronor



Identifierade premisser

Loggpostens metainformation

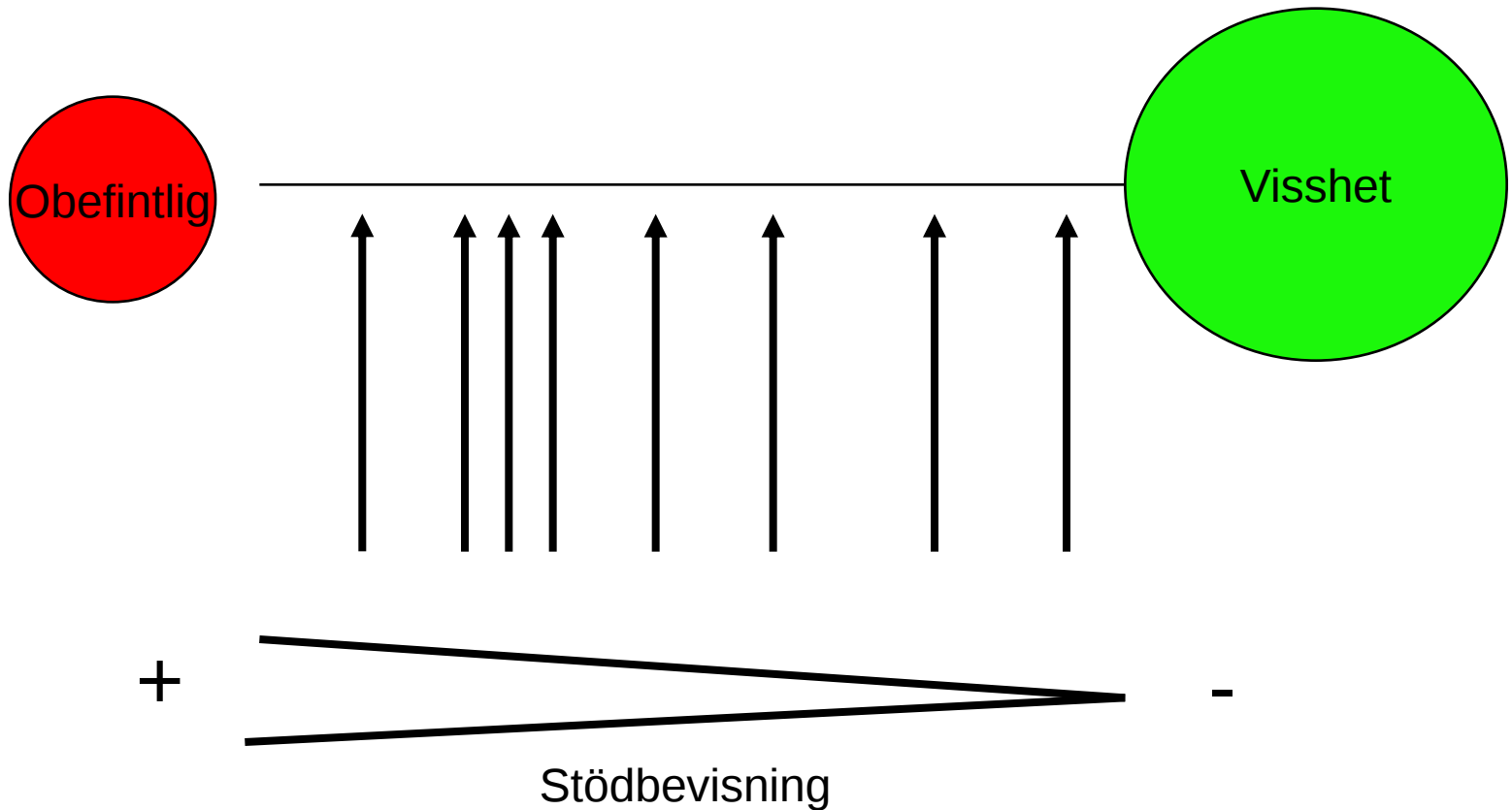
Den fysiska, tekniska och administrativa miljön

- Premiss 1:** Autentisering (graden av bindning mellan logisk och fysisk person)
- Premiss 2:** Överföringsprotokoll (Klartext eller krypterad)
- Premiss 3:** Nätverk (hubbade eller switchade)
- Premiss 4:** Administratörer på servrar
 - Autentisering
 - Loggning
- Premiss 5:** Skyddsfunktioner på klienterna
- Premiss 6:** Eget rum eller kontorslandskap (shoulder sniffing)

...



Loggpostens bevisvärde





Fri bevisvärdering

Hur påverkar det vår logghantering

Vår logghantering kan vara hur noggrann som helst, fri bevisvärdering gäller vid svenska domstolar, och det är alltid domstolens sak att bedöma bevisvärdet av en upptagning. Detta gäller oavsett om de loggarna utgör original eller om de utgörs av kopior.

Objektivitetsprincipen RB 23 Kap 4 §

- Vid förundersökningen ska ej blott de omständigheter, som tala emot den misstänkte, utan även de som äro gynnsamma för honom beaktas och bevis, som är till hans förmån, tillvaratagas.

Tack!

roger@alinda.se

070-206 10 26