

# Case: Tyveri af data?

## Opklaring med Computer Forensics



*En mistanke om tyveri eller misbrug af data kan være vanskelig at få bekræftet. Med anvendelse af avanceret udstyr kan der imidlertid afdækkes mønstre og sikres spor, der kan dokumentere et it-misbrug. I følgende case belyses en opklarings sag.*

En virksomhed havde mistanke om, at en tidligere medarbejder havde taget kundedata med sig, da han forlod virksomheden til fordel for et job i en konkurrerende virksomhed.

Virksomhedens direktør kontaktede Forensic Technology Solutions (FTS), idet man gerne ville have vurderet, om det var muligt at finde beviser, der kunne underbygge mistanken.

På baggrund af en vurdering af bevismaterialet og tidsperspektivet vurderede FTS, at der var gode chancer for at finde elektroniske spor og anbefalede derfor at påbegynde en kortlægning af bevismateriale samt en indledende bevissikring.

### Den indledende bevissikring gav få resultater

Sammen med virksomhedens HR- og it-afdeling kortlagde FTS, hvilke it-systemer der kunne indeholde spor, der evt. kunne påvise, at den tidligere medarbejder havde kopieret eller sendt data.

Af relevante it-systemer blev fremdraget den tidligere medarbejders bærbare pc og PDA, som begge blev afleveret, da medarbejderen forlod virksomheden. Ingen af de to enheder havde været brugt, siden de var blevet afleveret – en afgørende fordel i forbindelse med opklaringsarbejdet.

Indledningsvis blev der "skrabet" i overfladen for at konstatere, om medarbejderen havde sendt data ud via sin firma-e-mail-konto, eller om der fandtes kopier eller gemte versioner af de berørte data på den bærbare pc eller PDA'en.

Den indledende undersøgelse gav ikke nogle endegyldige beviser, men udelukkede heller ikke et misbrug. Da virksomheden fortsat var overbevist om, at den tidligere medarbejder havde taget data med sig, besluttede man sig for at lade FTS foretage en dybdegående analyse.

### En dybdegående analyse gav afgørende spor

Næste skridt var at grave et spadestik dybere i systemerne, bl.a. med henblik på at finde spor og rester fra den mistænktets private e-mail-konto, som vedkommende havde tilgået via en internet-browser.

Der blev skåret datafragmenter ud af harddisken, som gav klare beviser for, at den tidligere medarbejder havde sendt kundedata fra sin bærbare pc via sin private web-mail.

Herefter bestod FTS' opgave blot i at rapportere de fundne beviser som dokumentation for, at håndteringen af bevismaterialet var korrekt.

FTS' rapport dannede grundlag for, at virksomhedens advokat kunne rejse erstatningskrav over for den tidligere medarbejder. Historien endte i sidste instans med et tilfredsstillende forlig for virksomheden.

fortsættes ...

... fortsat

## Ekspert er bør foretage den tekniske bevissikring

Det var netop muligt at finde de relevante beviser, fordi virksomheden ikke havde tændt udstyret og prøvet selv, men kontaktede en ekspert, som fik gennemført en korrekt bevissikring.

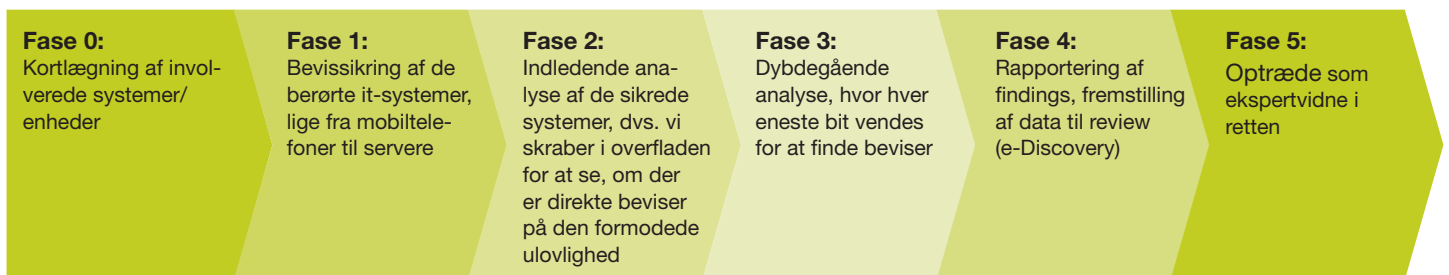
Hvis der er behov for at sikre bevismateriale, der om nødvendigt skal kunne fungere som dokumentation i en retssag, er det altafgørende, at bevissikringen sker efter særlige forholdsregler.

## Sådan arbejder FTS med it-bevissikring

FTS deler undersøgelsesforløbet op i seks afgrænsede faser, der supplerer hinanden, men også kan gennemføres enkeltvis uafhængigt af hinanden.

Alt efter hvor hurtigt der opnås resultater eller sikres beviser, vurderes i samråd med kunden efter hver afsluttet fase, om der skal fortsættes til næste fase.

De seks faser er:



### Case Facts:

Dato: Juli 2007  
Sag: Forensics analyse  
Kunde: Mellemstor dansk virksomhed

Kontakt FTS for yderligere information eller assistance.

PricewaterhouseCoopers  
Strandvejen 44  
2900 Hellerup  
www.pwc.dk

Per Leslie Jensen  
Tlf: +45 3945 3569  
Email: ple@pwc.dk