

Sikring av elektroniske spor

Av senior dataetterforsker Svein Yngvar Willassen, Ibas AS

Med dagens bruk av elektronikk sier det seg selv at elektronisk lagrede spor kan få betydning i nær sagt alle typer straffesaker. Frem til i dag er det mest telefonlogger og annen utlevert informasjon som er benyttet som bevis i de store sakene. Men hva med datamaskiner og annet utstyr som blir funnet på åstedet eller ved ransaking? Disse kan inneholde mye interessant informasjon, og kriminalteknikere bør derfor ha en grunnleggende forståelse for hvordan man sikrer disse så spor ikke går tapt.

Datamaskin

Datamaskiner inneholder svært viktige spor. All bruk av en datamaskin setter spor, og det er som regel mulig å rekonstruere når maskinen har vært brukt og hva den har vært brukt til langt tilbake i tid. Data som slettes på en datamaskin blir ikke borte. Isteden kan en identifisere hva som ble slettet, når og hvem som gjorde det.

Innholdet på datamaskiner er lagret på en eller flere harddisker som er montert inni maskinen. Dette innholdet sikres ved at det foretas en fullstendig kopiering av alle data over på en annen harddisk. Slik kopiering kalles speilkopiering og en vil da også få med all informasjon på harddisken som er slettet. Speilkopiering bør kun utføres av personell med utdanning i dataetterforskning, og utføres sikrest i laboratorium. Det er imidlertid svært viktig å være klar over at innholdet på harddisken er meget følsomt og vil bli endret ved hver minste bruk av maskinen, for eksempel ved oppstart. Det er derfor svært viktig at den som beslaglegger maskinen ikke faller for fristelsen å starte maskinen opp for å lete etter bevis, skrive beslagsrapport eller liknende. Harddisken er også meget følsom mekanisk. En må derfor behandle og transportere alle datamaskiner med forsiktighet. Å miste en maskin i gulvet er som regel nok til å ødelegge harddisken. Det er kun selve harddisken som inneholder lagret informasjon, så beslag av skjerm, tastatur og liknende er ikke nødvendig dersom det ikke gjøres for inndragningsformål.

Noen ganger kommer man over datamaskiner som står på. En bør da notere ned hvilke programmer som er i gang og hva man ellers ser på skjermen. Eventuelt kan skjermen fotograferes. Maskinen skruses deretter av ved å dra strømkontakten ut av veggen. Ikke bruk "Avslutt" i operativsystemet – dette kan medføre at informasjon forsvinner. Er det en bærbar PC er det i tillegg nødvendig å kople fra batteriet på undersiden av maskinen. En skal aldri la mistenkte få lov til å bruke datamaskiner som står på, uansett grunn. Det er svært lett for dem å slette filer, uten at politimannen nødvendigvis skjønner hva som foregår.

Ved ransaking i bedrifter eller andre steder der det forekommer datanettverk må spesialister i dataetterforskning medbringes.

Mobiltelefon

Mobiltelefoner inneholder spor som lagrede telefonnummer, sist oppringte og innkomne samtaler, tekstmeldinger (også slettede) og liknende. Siden så å si alle bruker mobiltelefoner, har disse ofte stor betydning som bevis i straffesaker.

GSM-systemet som brukes i dag kjennetegnes ved at telefonen inneholder et SIM-kort (smartkort) som identifiserer brukeren. Telefonen og SIM-kortet kan hver for seg inneholde interessant informasjon. SIM-kort er som regel beskyttet med en PIN- og PUK-koder. I tillegg kan også telefonen være beskyttet med kode. Dette er imidlertid lite brukt. PIN-koden er et tall på fire siffer som åpner SIM-kortet dersom riktig kode blir lagt inn. Dersom brukeren taster inn feil kode tre ganger sperres kortet, og en er nødt å legge inn PUK-koden (med mange flere siffer) for å få tilgang til kortet. Brukeren kan forandre PIN-koden, men ikke PUK-koden.

For å få tilgang til bevis lagret på SIM-kortet er det nødvendig med PIN eller PUK. En bør derfor spørre innehaver om PIN koden. Ved ransaking er det mulig å lete etter brev fra teleoperatøren, hvor PIN og PUK er oppgitt. Dersom man ikke har fått tak i noen av disse kodene må man få PUK-koden utlevert fra teleoperatøren gjennom fritak fra taushetsplikten/kjennelse fra retten.

Hva gjør man så med telefoner man kommer over? Regel nummer en er: Tenk! Hvis en telefon er av: Ikke skru den på! Hvis en telefon er på: Ikke skru den av! Årsaken til det siste er at det kan være mulig å tømme SIM-kortet for informasjon uten å oppgi PIN eller PUK, siden kortet allerede er åpnet. Dersom du har en sikker angivelse for PIN eller PUK kan du skru telefonen av. Hvis ikke, skaff en lader til telefonen snarest mulig, og sett den på lading for å hindre at den går tom for strøm.

Tømming av informasjon bør overlates til personell med utdanning i dataetterforskning. Telefoner tømmes ved å bruke kabel og programvare tilpasset hver enkelt telefontype. Den informasjonen som er lagret i selve telefonen kan en få ut uten å ha PIN/PUK. Dette gjør en ved å ta ut SIM-kortet, og sette inn et SIM-kort med kjent kode, og deretter bruke kabel/programvare. SIM-kort tømmes ved å benytte en smartkortleser og spesiell programvare. PIN/PUK er nødvendig. Dersom det haster, eller nødvendig utstyr mangler, kan en dokumentere informasjonen på telefonen ved å bla gjennom den manuelt. En kan da fotografere skjermen og/eller skrive rapport om innholdet på telefonen.

Telefonlogger kan utleveres fra operatøren relatert til telefonnummer eller telefon. En må da oppgi enten simkort-nummer, telefonnummer eller IMEI. IMEI er et nummer som unikt identifiserer selve telefonen. Dette finner en ved å taste *#06# mens telefonen er påslått. Nummeret står også på selve telefonen bak batteriet på de fleste telefontyper. Vær oppmerksom på at en telefon kan ha vært benyttet mot flere operatører! På SIM-kortet finner en simkortnummer og hvilken operatør kortet er tilknyttet. Telefonnummeret ligger lagret inni kortet. For å få utlevert logger kreves fritak fra taushetsplikt/kjennelse fra retten.

PDA

PDAer eller håndholdte datamaskiner som de ofte kalles har blitt mer vanlig de siste årene. Det finnes eksempler på at det er funnet lange lister over narkotikahandler på slike, så en bør være oppmerksom på betydningen slike bevis kan ha.

Eksempler på slike er Palm, HP Journada, Compaq Ipaq osv. De forskjellige typene har forskjellig programvare og tilkoblingsmuligheter. Som regel kreves det spesiell programvare og kabel for å få informasjon ut av dem, og det kan også være en utfordring å få ut

informasjonen uten å "forurens" den. Tømming av slike bør derfor overlates til personell med utdanning i dataetterforskning.

Når en kommer over en PDA bør en være klar over at dette er batteridrevne enheter som kan miste informasjon dersom de blir stående for lenge uten strøm (mer enn en uke). Derfor: Skru av enheten så raskt som mulig. (Informasjon går ikke tapt på disse når de skrur av.) Skaff deretter en lader, og sett enheten til lading. Hvis mulig, beslaglegg lader på samme sted som enheten selv.

PDA-er brukes ofte sammen med datamaskiner. Når enheten koples til synkroniseres dataene på datamaskinen med dataene på PDA-en. Når en mistenker at det finnes interessante spor på en PDA kan det derfor være en god ide å også beslaglegge datamaskinen. Siden slettede data ikke blir borte på datamaskinen, kan dette avsløre hva PDA-en har vært brukt til tidligere.

Disketter, CD-er

Disketter og CD-plater sikres og analyseres på samme måte som datamaskiner. I enkelte saker kan det være aktuelt å sikre fingeravtrykk på slike. Erfaringsmessig kan det oppstå skade på mediet ved sikring av fingeravtrykk. Det er derfor en fordel å speilkopiere innholdet før en foretar sikring av fingeravtrykk. Maskinlesing av mediet medfører ikke at kvaliteten på eventuelle fingeravtrykk forringes.

Integrert elektronikk – fremtiden for elektronisk sporsikring

Etter hvert som elektronikk integreres i stadig mer av hverdagen vår kan det bli aktuelt å foreta elektronisk sporsikring i mange sammenhenger. Eksempelvis kan det allerede i dag være av interesse å sikre spor fra bilnavigasjonssystemer, GPS-systemer i båt og datasystemer på fly. I fremtiden vil en nok kunne oppleve at alt fra kaffetraktere og vaskemaskiner til varmestyringssystemer i hus kan inneholde elektroniske spor av betydning. For å sikre at det finnes kompetanse for å utføre sikring av slike spor er det nødvendig at noen driver med forskning på elektronisk bevissikring.

Hvor kan man henvende seg?

- Politiets Datakrimsenter, ØKOKRIM er politiets sentrale bistandsorgan for sikring og analyse av datautstyr.

- Ibas AS utfører sikring og analyse av elektroniske spor på oppdrag fra private, politiet, kontrolltater og andre offentlige organer i Norge og hele verden.