

## Slettede data som bevis

*Svein Y. Willassen, dataetterforskningsjef, Ibas AS*

**De fleste vet at å kaste en fil i papirkurven på datamaskinen ikke er nok for at den skal slettes permanent. Færre er klar over at informasjonen filen inneholdt kan bli liggende på harddisken i lang tid, selv etter at papirkurven er tømt. Men slik er det, og informasjonen som finnes her kan ha betydning som bevis i straffesaker såvel som sivile saker.**

Filsystemet på de fleste moderne operativsystemer er organisert som en trestruktur av mapper, der hver mappe kan inneholde et vilkårlig antall mapper eller filer. En fil er en ansamling av informasjon som er organisert på en bestemt måte. Denne organiseringsformen bestemmes av programmet som lagrer filen. For eksempel vil Microsoft Word lagre dokumenter i et bestemt filformat som populært kalles doc-formatet. I tillegg til filenes innhold finnes det for hver fil en del metainformasjon, som for eksempel dato/tidspunkt filen ble opprettet, sist ble skrevet til og sist lest. Det finnes også en del metainformasjon i filsystemet. Dette omfatter blant annet en tabell over hvilke områder på harddisken som ikke er i bruk, samt lister over hvilke områder som hører til hvilken fil. De fleste filsystemer er organisert slik at metainformasjonen er plassert et annet sted på harddisken enn selve filinnholdet.

Når en tømmer papirkurven på datamaskinen utfører datamaskinen sletting av filene i filsystemet. Slettingen innebærer at området på disken som inneholder filen og området med tilhørende metainformasjon blir markert som ledig. Det blir ikke utført noen overskriving av nye data, slik at både filer og metainformasjon kan rekonstrueres komplett med spesielle verktøy. Etterhvert som nye filer blir lagret på systemet vil informasjonen bli overskrevet, og rekonstruksjon blir umulig. Imidlertid vil de fleste operativsystemer av driftshensyn prioritere å lagre nye filer på et stort ubrukt område fremfor små "hull" som oppstår som følge av at enkeltfiler blir slettet. Det er derfor svært ofte mulig å rekonstruere hele filer selv lang tid etter at de er slettet. Dersom systemet benytter "hull" som er oppstått vil det som regel være for å lagre mindre filer enn det som lå der fra før. I motsatt fall må systemet dele opp (fragmentere) filen, noe som er ineffektivt. Som et resultat av dette vil det som regel alltid ligge igjen ihvertfall deler (fragmenter) av filer som tidligere har eksistert på et system. Erfaringen viser at på de fleste filsystemer vil det ligge igjen fragmenter fra tidligere slettede filer fra hele maskinens levetid, med mindre det er tatt spesielle skritt for å overskrive hele harddisken med nye data.

Et tilleggsmoment som kan få betydning er at programvare på en datamaskin lagrer data på harddisken uten at brukeren er klar over dette. En kan for eksempel tenke seg en bruker som starter Microsoft Word, skriver et dokument, lagrer dette, skriver ut og deretter sletter dokumentet. Så langt brukeren kan se finnes dette dokumentet nå ikke lenger på datamaskinen. Imidlertid vil Word foreta autolagring på harddisken før brukeren lagrer dokumentet. Brukeren lagrer så dokumentet til en ny fil. Når brukeren skriver dokumentet ut blir det lagret en ny midlertidig skriverfil. Som et resultat ligger det aktuelle dokumentet etter denne operasjonen på tre ulike steder på harddisken, til tross for at brukeren tror det er fullstendig slettet.

Det er på det rene at det kan finnes mye informasjon på en harddisk som kan få betydning som bevis. Et problem med filer som er slettet fra filsystemet er at det i en del tilfeller er mulig å rekonstruere filene, men ikke deres metainformasjon. Dette medfører at man ikke kan si noe om når filene ble lagret på maskinen, når de sist ble lest eller deres plassering i filsystemet. Det kan for eksempel være vanskelig å konstatere hvilken bruker som har lagret filene på systemet, eller om lagringen i det hele tatt er et resultat av en bevisst handling fra brukerens side. Spørsmålet blir da om filenes innhold i seg selv er nok til å tjene som bevis.

Dataetterforskning er kunsten å finne informasjon relevant for rettslige prosesser i store datamengder, og sikre og dokumentere disse. Fagfeltet er i dag på et tidlig stadium. Det eksisterer mange nye muligheter for gjenfinning og tolkning av datainformasjon som enda ikke er utprøvd. Det er imidlertid på det rene at dataetterforskning som metode, korrekt utført, allerede i dag gir store muligheter for å frembringe nye momenter i en sak. Fremover vil vi se datainformasjon fremlagt som bevis i stadig nye saker, og tolkning av elektronisk lagret informasjon vil bli et viktig tema i rettssalene fremover.