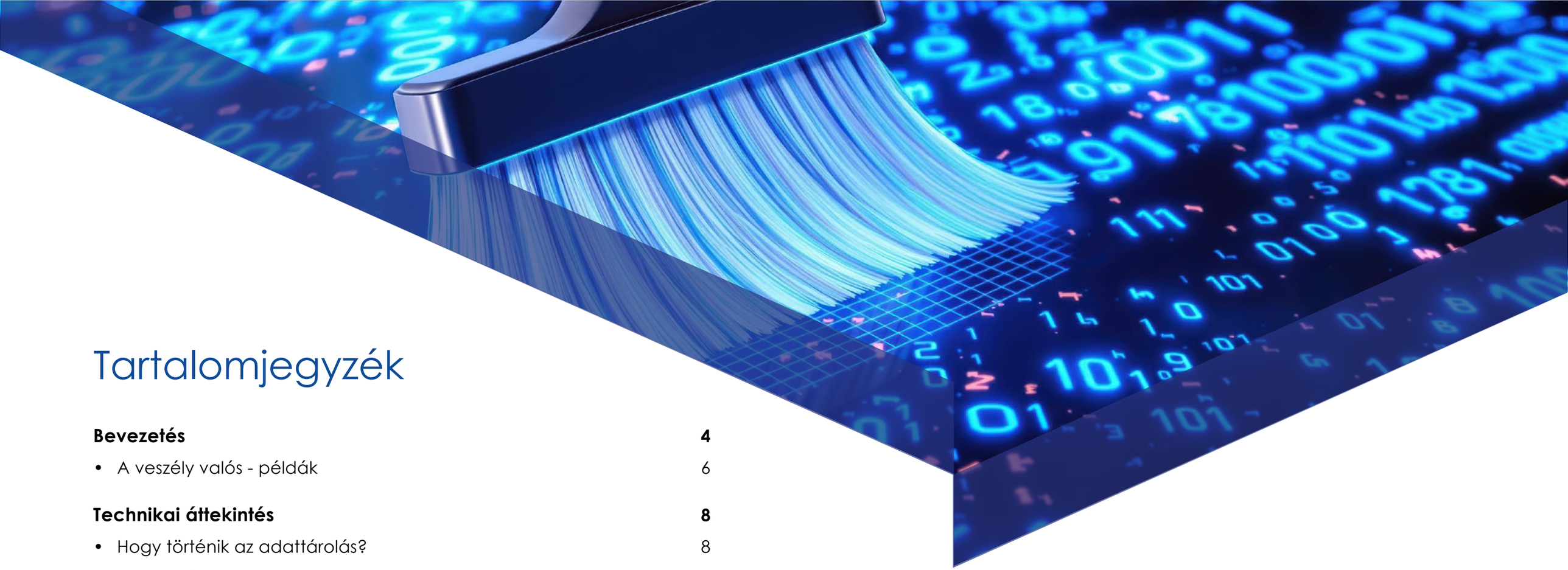
CTI Jelentés

Végleges adattörlés IT eszközökön

NEMZETI KIBERVÉDELMI INTÉZET



Tartalomjegyzék

Bevezetés

Ennek a jelentésnek a célja, hogy rávilágítson a már nem használt IT eszközök – okostelefonok, laptopok, tabletek, asztali számítógépek HDD vagy SSD meghajtói, pendrive-ok, memóriakártyák, stb. – selejtezést követő végleges adattörlésének kritikus fontosságára. Digitális eszközeinken számos érzékeny adatot tárolunk, gondoljunk csak a privát fotóinkra, videóinkra, dokumentumainkra, így ezekkel visszaélve komoly kárt okozhatnak nekünk. Amennyiben az adattárolásra alkalmas eszközeinket már nem használjuk (például csere miatt), akkor érdemes gondoskodunk a megfelelő adattörlésről.

Jelenlegi tapasztalatok alapján aggasztóan alacsony mértékű a tudatosság az adattörlési protokollok betartása tekintetében a szélesebb közönség körében. Sajnos elenyészően kevesen gondoskodnak egy új okostelefon megvásárlását követően a régi készülékük megfelelő végleges adattörléséről. Az a legfőbb tendencia a lakossági felhasználók körében - ha már elavult, alacsony értekkel rendelkező készülékről van szó -, hogy egy fiók mélyén landol az eszköz vagy éppen a család gyermekeinek adják „játszós" telefonnak. Rosszabb esetben a készülék minden további adattörlés nélkül kerül értékesítésre, vagy csak egész egyszerűen a szemétben végzi, mely természetesen környezetvédelmi aggályokat is felvet.

Az eszközeinken jelentős számú adat halmozódhat fel az évek során, így elsődleges célunk, hogy elejét vegyük annak, hogy ismeretlen személyek birtokába kerülhessenek ezen adatok. Tisztában kell lennünk azzal is, hogy amennyiben a tárolt adatok nem megfelelően kerülnek törlésre, azok különösebb informatikai szaktudás nélkül is visszaállíthatók maradhatnak, így olyan módszerekre van szükségünk, mellyel végleges adattörlést tudunk végrehajtani.

Végleges törlésnek azt tekinthetjük, amikor az adathordozón tárolt adatok nem helyreállíthatók, még speciális eszközökkel sem. Jelen útmutatóban ezt a témát járjuk körül alaposan.

A veszély valós – példák

Az esetek többségében az adatok nem megfelelő törlésének veszélye nem puszta hipotézis, hanem a valóságban is kézzel fogható – sok esetben anyagi - károkat tud okozni. Nem tekinthető evidenciának, hogy minden egyes adathordozó tökéletesen, visszaállíthatatlanul törlésre kerül, mielőtt az a másodlagos piacra kerül. Az interneten böngészve számos információbiztonsági incidensről szóló hírt lehet találni, melyek arról számolnak be, hogy a káresemények efféle mulasztások okán következtek be.

Egy példa a sok közül: New Jersey egyik online hírportálja számolt be egy olyan esetről, amikor a Pequannock-i Chilton Medical Center egyik volt alkalmazottja adott el online 2017-ben egy olyan korábban kórházi tulajdonban lévő merevlemezt, mely ***az összes 2008 és 2017 között ellátott beteg adatát tartalmazta****.*

Ugyancsak jó példa a 2021-ben szintén az Amerikai Egyesült Államokban nyilvánosságra került incidens, mely a HealthReach nevű Egészségügyi Központhoz kapcsolódott. Az incidensben mintegy 100000 Maine állambéli lakos volt érintett, ugyanis az egészségügyi intézmény által korábban használt merevlemezeket a használatból való kivonást követően nem megfelelő módszerrel törölték. A veszélybe került adatok között voltak olyan szenzitív adatok, mint a ***betegek nevei, SSN-ek*** *(amerikai társadalombiztosítási szám),* ***születési dátumok, számlaszámok, laboratóriumi/vizsgálati eredmények, biztosítási adatok, jelszavak, biztonsági kódok és PIN-kódok****.*

Lényeges felismerni, hogy a fenti incidensek sajnos nem egyediek, csak ritkán kerülnek nyilvánosságra, mivel az érintett cégek gyakran nem hozzák nyilvánosságra ezeket az eseteket reputációjuk védelme érdekében. A HIPAA Journal jelentése szerint 2020-ban 16 alkalommal jelentettek elektronikai eszközök nem megfelelő ártalmatlanítására vonatkozó incidenseket.

Ezen felül természetesen számos egyéb incidens híre is fellelhető az interneten, ahol az illetéktelenül megszerzett adatok felhasználásra is kerültek különféle csalásokhoz, például hiteligénylésekhez vagy egészségügyi szolgáltatások jogosulatlan igénybevételéhez.

Felmerülhet a kérdés, hogy milyen arányú mulasztásról van szó, mennyire bevett gyakorlat az, hogy megfelelően „fertőtlenítik" az adathordozókat: 2003 februárjában publikálásra került a témában egy tanulmány, melyet a neves Massachusetts Institue of Technology (MIT) egy végzett, és egy végzős hallgatója készített, melyben 158 darab általuk különféle forrásból vásárolt, használt merevlemezt vizsgáltak abból a szempontból, hogy megfelelően törlésre kerültek-e. A publikációban megállapították, hogy megfelelő módszertant rendkívül kevés esetben alkalmazták.

A kísérlet további részleteit jelen CTI jelentés Esettanulmány című fejezetében fejtjük ki.

Technikai áttekintés

Hogy történik az adattárolás?

Működési elvük szerint 3 fő csoportra oszthatók a háttértárak:

- **optikai adattárolók** (pl.: DVD-RW),
- **mágneses adattárolás** (pl.: floppy, merevlemez) és az
- **elektronikus adattárolás** (a szilárd félvezető áramkörre épülő tárak).

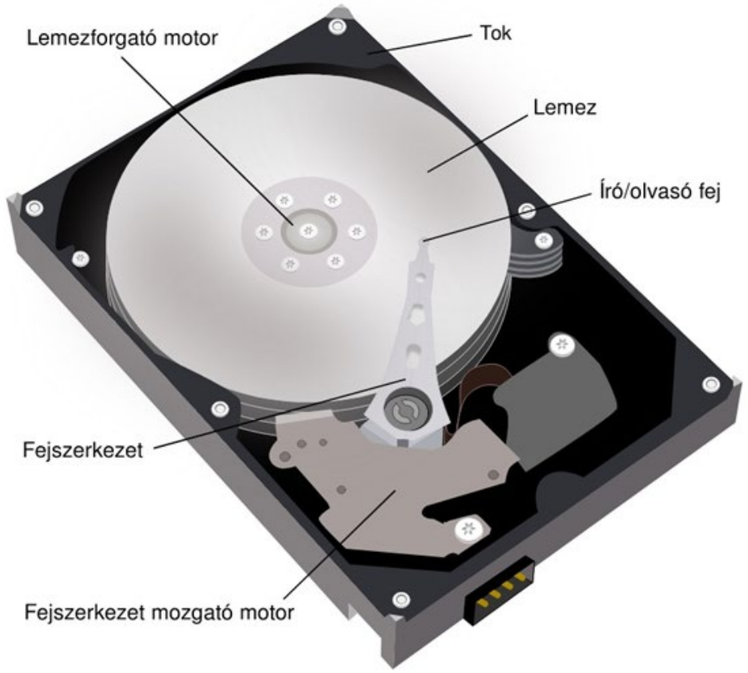
Jelen elemzésben az optikai háttértárakkal nem kívánunk foglalkozni, hanem a másik két kategóriára kívánunk fókuszálni, mivel azok adattartalmának a végleges – lehetőség szerint fizikai roncsolástól mentes – adattörlése igényelhet speciális ismereteket.

A mágneses adattárolás legelterjedtebb formája a merevlemez, amely egy vagy több mágneses anyaggal bevont merev, gyorsan forgó korong/tálca/lemez segítségével valósul meg. A lemezek együtt működnek a mágneses író-olvasó fejekkel, amelyek általában egy mozgó működtető karon helyezkednek el. A mágnesezett felületen az egyes blokkok és az adatok bármilyen sorrendben lehívhatók. A HDD-k tartós tárolók, amelyek a tárolt adatokat még kikapcsolt állapotban is megtartják.

A rögzítés elméleti alapja, hogy a digitális adatokat, azaz a jel és a jel hiányát egy adathordozó megmágnesezett felületén tulajdonképpen fizikai/analóg jellé alakítjuk olyan formában, hogy azt gépi feldolgozással a lehető leggyorsabb írási és olvasási lehetőséggel megbízhatóan tárolhassuk. Fizikai valóságában a megmágnesezhető anyag fölötti elektromágneses tekercsek mozognak (vagy az adathordozó mozog a megmágnesezhető anyag alatt, vagy mindkettő mozog a másikhoz képest), és a tekercsekben elektromos impulzusok hatására keletkező mágneses tér fizikai nyomot hagy az anyagban, amely később újra kinyerhető – visszaolvasható. A felülethez közel író- és olvasófej működik. Az olvasófejben a mágnesezett felületnél elektromos áram keletkezik a tekercsben és az információ meghatározható a visszaolvasott jel polarizációjából.

Egyszerűbben: az eszköz lelke maga a lemez vagy lemezek, ami egy mágnesezhető réteggel bevont forgó korong, erre írja az adatokat, tehát a biteket kettes számrendszerben az író-olvasó fej. Ez azt jelenti, hogy a lemez felett átsuhanó fej érzékeli, hogy 1-es vagy 0 felett haladt el éppen. Ebből áll össze minden számítógépes adat.

A rögzítés elve az alábbi: az adatokat a lemez felszínén koncentrikus körök (sávok = track-ek) mentén rögzítik. Az adatokat sávokon belül szektorokban tárolják. A tárolás logikai egysége a klaszter, ami a rendszerektől függően eltérő számú szektorból állhat.



1. ábra
A merevlemez felépítése
Forrás: Horváth Gábor: Számítógép Architektúrák 88.old. 6.7.ábra (BME, 2011)

A másik technológia az elektronikus adattárolás, jelen esetben a félvezető memória, ami félvezető alapú integrált áramkör (integrated circuit IC) chipeket használ az információk tárolására. Mivel a HDD-kkel szemben az SSD-k nem tartalmaznak mozgó alkatrészt, így a mechanikai behatásokra, ütésekre, vibrációra ellenállóbbak és működésük sem jár zajjal. Az adatokat általában fém-oxid-félvezető (metal-oxide-semiconductor – MOS) memória cellákban tárolják.

A félvezető memória chip több millió memóriacellát tartalmazhat, apró MOS mezőhatású tranzisztorokból és/vagy MOS kondenzátorokból állva. A flash memória (solid-state drives – SSD) már egyre nagyobb teret hódít magának, így egyre több gyártó kezdte el alapértelmezetten használni az asztali számítógépekben vagy laptopokban is a hagyományos HDD mellett vagy helyett. Ugyanilyen elektronikus elven működnek a mobiltelefonokban lévő háttértárolók is, de ne feledkezzünk el az esetlegesen kiegészítésképpen benne tárolt memóriakártyákról sem.

Egyszerűbben: a félvezető technológián alapuló háttértárak cellákban tárolnak töltéseket, egészen pontosan az ún. lebegő gate-es tranzisztorokban lévő elektronok jelenléte határozza meg, hogy a tranzisztor által reprezentált kapcsoló nyitott vagy zárt állapotban van, vagyis itt is megfigyelhető a bináris elv az adattárolásban. A kulcs az, hogy a tranzisztor lebegő gate nevű része úgy viselkedik, mint egy ketrec, amibe bele lehet kényszeríteni az elektronokat, és ezek a bezárt elektronok mindenfajta tápellátás nélkül, hosszú távon – akár évtizedekig – ott is maradnak. Ebben az esetben az adatok így kerülnek reprezentálásra: egy tranzisztor egy bitet tárol, ha a lebegő gate fel van töltve elektronokkal, az 0-s bitet, ha nincs, az 1-es bitet jelent.

2. ábra
SSD felépítése

Érdekességként érdemes kitekinteni a jövőbe, és megemlíteni a kvantumszámítógépeket is az adattárolás szempontjából. A kvantumszámítógép egy olyan számítógép, amely a kvantummechanika elveit használja a számítások elvégzésére. Ez alapvetően különbözik a hagyományos, klasszikus számítógépektől, amelyek biteken (0 és 1) alapuló műveleteket végeznek. A kvantumszámítógépek ezzel szemben **qubiteket** használnak, amelyek egyszerre lehetnek 0 és 1 szuperpozíciójában. Ez azt jelenti, hogy egy qubit párhuzamosan több állapotban is lehet. Két vagy több qubit összefonódhat, vagyis kvantummechanikai módon összekapcsolódhatnak, így az egyik qubit állapota automatikusan meghatározza a másikét, függetlenül attól, hogy milyen távol vannak egymástól. Ez lehetővé teszi a rendkívül gyors információfeldolgozást.

Természetesen erre nem a mindennapi feladatok során lehet szükség, hanem olyan speciális problémák megoldására lehet kiváló, mint például a titkosítások feltörése vagy a molekuláris szimuláció. Kiemelendő, hogy a kvantumszámítógépek még fejlesztés alatt állnak, és egyelőre kevés igazán praktikus alkalmazási lehetőségük van. Maga a technológia is még kiforratlan, így számos problémát kell még megoldani. Ilyen problémakör még éppen az adattárolás kérdésköre, ugyanis a fenti említett qubitek rendkívül érzékenyek és különleges környezetet igényelnek.

Az adattárolás különböző fizikai rendszereken alapulhat, például:

- **Szupravezető hurkokon**: A legtöbb jelenlegi kvantumszámítógép (pl. IBM, Google) szupravezető qubiteket használ, amelyeket rendkívül alacsony hőmérsékleten (-273 °C) tartanak, hogy minimalizálják a zavaró hatásokat.
- **Ioncsapdákon**: Egyes kvantumszámítógépek ionizált atomokat (ionokat) használnak, amelyek lézerek segítségével stabilizálhatók és manipulálhatók.

Tekintve, hogy a kvantumállapotok rendkívül érzékenyek a külső hatásokra, például hőmérsékletre, elektromágneses zajra vagy mechanikai rezgésekre, emiatt jelenleg még a kvantumszámítógépek esetén inkább az jelenti a kihívást, hogy hogyan lehet fenntartani az adattároláshoz szükséges optimális állapotot, nem pedig az, hogy hogyan lehet a tárolt adatokat megsemmisíteni. Jelenleg ugyanis az adattárolás azonnal sérül az optimális körülmények változása esetén. Az, hogy a későbbiekben milyen adattörlési metodikát kell alkalmaznunk, attól függ majd, hogy milyen technikai megoldással sikerül megoldani a kvantuminformációk hosszú távú tárolását.

Adattörlés

Azt fontos kihangsúlyozni, hogy lényeges különbség van adatok törlése és a végleges (helyreállíthatatlan) törlése között. A lényeg az, hogy az „egyszerű" törlés során (pl.: mikor a Windows operációs rendszert használva belehúzzuk a lomtárba a törlendő állományt és utána kiürítjük a lomtárt) nem törlődnek véglegesen az adatok, csak a felhasználó számára vállnak elérhetetlenné. Viszont ez az adat még törlés után is visszahozható bizonyos módszerekkel.

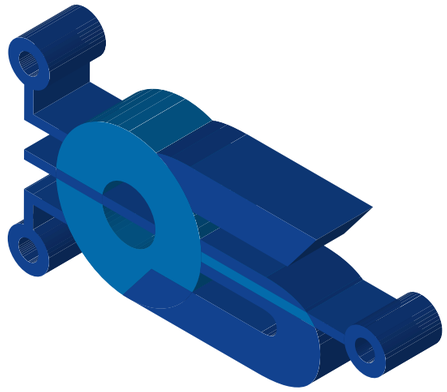
Felmerülhet a kérdés, hogy ha egy adatot kitöröltünk, akkor az, „hogy lehet mégis ott"? Magyarázatképpen egy analógiát fogunk alkalmazni: legtöbb esetben, ha egy adat kitörlésre kerül, az olyan mintha egy könyvből a tartalomjegyzékből kihúznánk az adott sort, ami az adott fejezetre utal. A fejezet ekkor még ott van, viszont már a tartalomjegyzékben nem látjuk. Mikor egy monitort nézünk, ahol ikonok, könyvtárak és fájlok vannak, akkor gyakorlatilag egy tartalomjegyzéket nézünk.

Így tehát az esetek többségében a törlés nem egy teljes értékű törlés, hanem csak az adott bejegyzés törlése, ami arra a területre mutatott. Az eszköz későbbi használata közben új adatok íródhatnak a felszabadult memória területre (mivel azt szabadnak jelölte meg az operációs rendszer), így az ott tárolt korábbi adatok ténylegesen elérhetetlenné válnak. Nagyon fontos konklúzió az adattörlésről a merevlemezek esetében: **az adat felülírás esetén elérhetetlenné válik, törlés esetén pedig elképzelhető, hogy még visszaállítható**.

Mi történik az adatok törlésekor az operációs rendszerben?

Ezidáig főként arról beszéltünk, hogy milyen folyamatok mennek végbe a fizikai háttértárolókon, és csak általánosságban beszéltünk az adattörlés folyamatáról az operációs rendszer szintjén. Érdemes azonban ez utóbbi folyamatokat részletesebben is kifejteni. Azt a fentiek alapján már tisztáztuk, hogy amikor adattörlést hajtunk végre az operációs rendszerben, akkor az általában nem azonnali fizikai törlést jelent a háttértárolókról. Ehelyett az operációs rendszer különböző mechanizmusokat használ, hogy az adatokat „töröltnek" jelölje. Ezek a mechanizmusok platformonként és fájlrendszerenként eltérőek lehetnek, azonban általános közös vonások is felfedezhetők a különféle folyamatokban.

Mint fentebb említettük operációs rendszertől és fájlrendszertől függ, hogy pontosan mi az adattörlési metodika.



A leggyakrabban használt operációs rendszer, a Windows például NTFS, FAT32 vagy egyéb fájlrendszert használ. A törlési metodika megegyezik a fenti, általános leírással, azzal a kiegészítéssel, hogy a Windows még egy lépcsőt beépített ebbe a folyamatba, gondolunk itt a mindenki által ismert lomtárra és annak ürítésére. A Linux – vagy Linux alapú operációs rendszerek – leginkább az ext4 fájlrendszert használják, ami az inode nevű táblázatot alkalmazza indextáblaként, így a törlés az inode-ból való eltávolítást jelenti. Hasonló elven működnek a macOS-t és az Android-ot használó eszközök is. Közös vonás tehát szinte az összes fent említett operációs rendszerben, hogy a fájlok tényleges adatblokkjai nem kerülnek azonnal törlésre. Amíg azokat új adatok nem írják felül, addig speciális adat-helyreállító szoftverekkel a törölt fájlok visszaállíthatók.

A végleges törléshez – shredding - olyan módszerek szükségesek, amelyek többször felülírják az adatblokkokat véletlenszerű adatokkal, hogy biztosan ne lehessen őket visszaállítani.

*A **fájlrendszerek** az operációs rendszerek alapvető komponensei, amelyek **lehetővé teszik az adatok szervezését, tárolását, kezelését és visszakeresését a háttértárolókon**, például merevlemezeken, SSD-ken és USB-meghajtókon. A fájlrendszerek különböző struktúrákat és módszereket használnak az adatok kezelésére, és számos típusuk létezik, amelyek különböző operációs rendszereken érhetők el.*

TUDTAD?

Mikor válnak véglegesen töröltté az adatok?

A **shredding** egy olyan folyamat, amely az adatok felülírása révén biztosítja, hogy az adatok véglegesen és visszaállíthatatlanul törlésre kerüljenek a háttértárolóról. Ez különösen fontos a bizalmas adatok védelme szempontjából. Számos eszköz áll rendelkezésre a folyamatot különböző operációs rendszereken történő végrehajtására, de az OS-ek többnyire rendelkeznek is saját beépített programokkal.

Az adatok bináris módon, vagyis 0 és 1-es formátumba vannak eltárolva, így értelemszerűen a felülíráshoz ezt az elvet kell követni. Elviekben az is megoldás lehetne, ha a merevlemezre folyamatosan újabb és újabb irreleváns adatokat másolnánk, így elérve a tökéletesen felülírt állapotot. Belátható, hogy ez a módszer jelentős erőforrást kívánna meg, így olyan programokhoz tudunk ehelyett fordulni, amelyek ezt a felülíró tevékenységet **elvégzik helyettünk**.

Az SSD meghajtók adattörlése másképp működik, mint a hagyományos merevlemezeké. Az adatokat többnyire blokkokban tárolják. Amikor törölni szeretnénk valamit a meghajtóról, az operációs rendszer jelzi, hogy az adott blokk figyelmen kívül hagyandó adattárolás szempontjából. Az SSD meghajtó ezután jelöli ezt a blokkot „üresnek", így új adatokat lehet rá írni. A tényleges adattörlés ennél azonban bonyolultabb lehet: az SSD-kben az adatok írási teljesítményének optimalizálása érdekében az operációs rendszer nem mindig írja felül azonnal a törölt adatokat, ehelyett gyakran csak megjelöli ezeket a blokkokat újraírhatóként, és az adatokat csak akkor törli, amikor ténylegesen szükség van az adott blokkra.

Az adatok teljes törlése érdekében az SSD-k rendelkeznek egy **TRIM** nevű funkcióval, amely segít az adatok végleges törlésében és a meghajtó teljesítményének optimalizálásában. A TRIM egy szabványos SATA utasítás, ami jelzi a vezérlő felé, hogy az adott adat valóban törölhető. Ha az SSD vezérlője tudja, hogy az adat törölhető, akkor felszabadíthatja a TRIM nélkül csak felülírhatóként megjelölt területeket, ennek következtében pedig az új SSD sebességével folytatódhat az írás. Tulajdonképpen ez a TRIM funkció indítható el a windows-ban a „meghajtók optimalizálása" menüpontban.

Meg kell említenünk még a **Secure Erase parancs** használatát. Ez arra utasítja az SSD vezérlőjét, hogy minden adatot töröljön és az összes cellát alaphelyzetbe állítsa. Ez a folyamat biztosítja, hogy minden adat visszaállíthatatlanul törlődjön az SSD-ről. A speciális – SSD-re optimalizált – adattörlő szoftverek ezeket az utasításokat hajtatják végre. Mindezek tükrében az SSD meghajtókon a végleges adattörlés nem felülírással történik, ugyanis ezzel az eszköz élettartama csökkenne.

Megjegyzendő, hogy a telefonokban lévő háttértárak is ugyanilyen elvek mentén működnek.

Kitekintés a jogszabályi háttérre

Felmerülhet a kérdés, hogy milyen kötelezettség vonatkozik egy átlagos felhasználóra. A saját adatai vonatkozásában természetesen mindenki szabadon rendelkezik, azonban a mindennapi életben számos olyan szituáció előfordul, amikor más emberek személyes adatai is a birtokunkba kerülnek (önéletrajz, személyes adatok, elérhetőségek stb.). Amikor megnyitjuk ezeket a dokumentumokat, legtöbbször letöltésre és eltárolásra is kerülnek eszközünkön, amivel egyidejűleg adatkezelővé is válunk, vagyis kötelezettségeink adódhatnak. A kötelezettség kikényszeríthetőségét nem célja megvitatni jelen értekezésnek, ezzel szemben néhány tanáccsal kívánunk szolgálni, hogy milyen módon kezelhetjük biztonságosan az adatokat törlés szempontjából.

Mivel ennek szükségessége már jogalkotók részéről is felmerül, a személyes adatok védelmében a **Nemzeti Média- és Hírközlési Hatóság (NMHH)** ingyenes adattörlést biztosít a fogyasztóknak, egészen pontosan ingyenes hozzáférést egy adattörlő alkalmazáshoz 2021. december 1-től kezdődően. Ez a szoftver a tartós adathordozó eszközök – például mobiltelefonok és laptopok – széles körénél teszi lehetővé a tárolt adatok biztonságos és visszavonhatatlan törlését. Az NMHH – a 2016-ban hatályba lépett Általános adatvédelmi rendelettel (GDPR) összhangban - az adatok végleges hozzáférhetetlenné tételét lehetővé tevő alkalmazás biztosításával kapcsolatos eljárási szabályok meghatározásáról szóló 726/2020. (XII. 31.) számú kormányrendelet alapján látja el az adattörlő alkalmazással kapcsolatos feladatokat. A gyakorlatban ez abban nyilvánul meg, hogy a kereskedőknek át kell adni valamilyen formában – például a vásárlási számlán vagy nyugtán rögzítve, vagy ettől eltérő egyéb módon – egy adattörlő kódot, mellyel a felhasználók jogosultságot kapnak egy készülék ingyenes adattörlésére a **Certus** nevű szoftver segítségével, melynek alkalmazása után egy tanúsítványt is kapnak a felhasználók a törlés sikerességéről.

Lehetséges megoldások

Adattörlő szoftverek

Általánosságban elmondható, hogy az adattörlő szoftverek olyan programok, amelyek biztosítják, hogy a fájlok és egyéb adatok véglegesen törlődjenek a háttértároló eszközről, oly módon, hogy azok visszaállítása semmilyen módon sem lehetséges. Ezek a szoftverek különböző módszereket alkalmaznak az adatok biztonságos törlésére, amelyek leggyakrabban a többszörös felülíráson alapulnak.

A szoftverek alkalmazása során ki kell választani a törölni kívánt fájlokat, mappákat, vagy akár egész meghajtókat. Ezután az adattörlő szoftverek többször felülírják az adatok helyét a lemezen véletlenszerű vagy meghatározott mintázatokkal. Érdekesség, hogy az adatok felülírásának is vannak különféle szabványai: például a DoD 5220.22-M szabvány szerint az ilyen szoftvereknek háromszoros felülírást kell alkalmazniuk: először nullákkal, másodszor egyesekkel, vagy pedig véletlenszerű adatokkal. Fontos kiemelni, hogy az adattörlő szoftverek nemcsak a fájlok tényleges tartalmát törlik, hanem a hozzájuk kapcsolódó metaadatokat is, úgymint fájlneveket, időbélyegeket és egyéb információkat, amelyek segíthetnek az adatok visszaállításában. Az adattörlő szoftverek nagy előnye, hogy képesek a háttértárolón található szabad területeket is felülírni. Ez különösen hasznos, ha korábban törölt fájlok maradványait szeretnénk eltávolítani, amelyek még mindig visszaállíthatók lehetnek.

Az adattörlő módszerek többnyire csak a felülírások számában, illetve a mintázatokban különböznek. Az egyszerű felülírás ugyan gyors, de nem feltétlenül biztosítja az adatok teljes megsemmisülését, így célszerűbb a kissé lassabb, de biztosabb többszörös felülírást választani.

Létezik másfajta módszer is: az úgynevezett kriptográfiai „törlés", mely azt jelenti, hogy a módszer titkosítja az adatokat, majd törli a titkosítási kulcsot, így az adatok visszaállítása kulcs nélkül gyakorlatilag lehetetlen. Itt nem valódi törlésről beszélünk, hanem inkább egy olyan módszerről mely biztosítja azt, hogy az adatok valódi tartalmát ne ismerhessük meg, csak valamilyen aránytalanul nagy erőforrásráfordítás árán.

Adattörlő kód

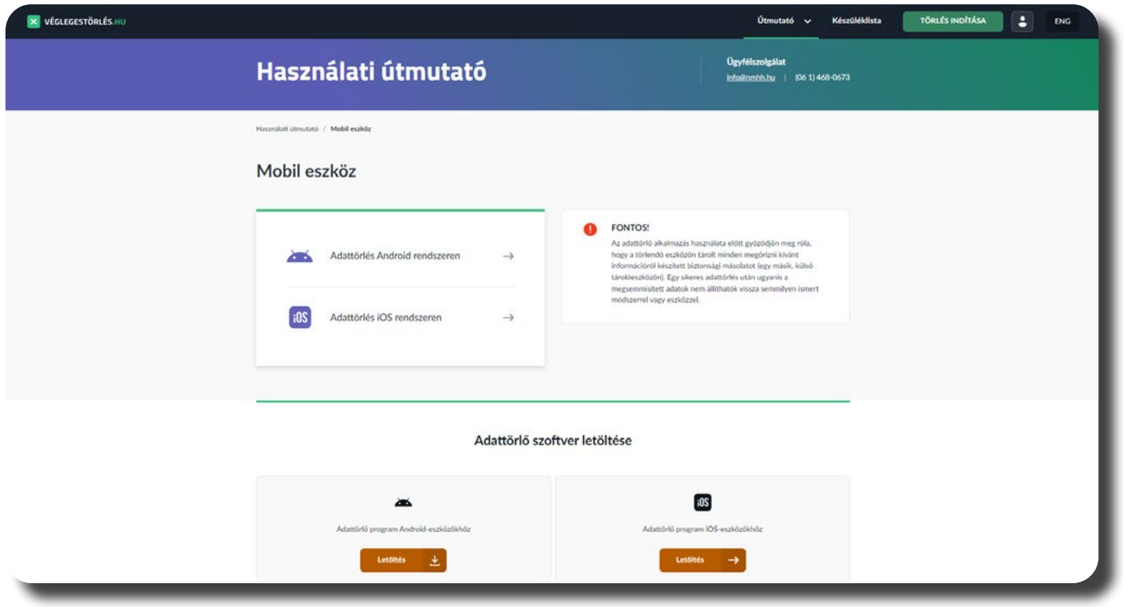
Ugyan számos adattörlő szoftver létezik, azonban érdemes használni az NMHH által biztosított adattörlő kódot (amennyiben rendelkezésre áll), mely a leginkább felhasználóbarát megoldás, hiszen nem nekünk kell ilyen speciális célszoftver biztosításáról gondoskodnunk. A 2021. december 1-től biztosított kódon felül egyéb korlátozás még, hogy vannak bizonyos eszközök, melyek nem törölhetők a biztosított szoftverrel, így például olyan SSD-k, amelyek OPAL titkosítással vannak ellátva vagy a 7.0-nál régebbi Android készülékek. A teljes lista a veglegestorles.hu weboldalon megtalálható.

Ez egy egyszerű megoldást nyújt a felhasználóknak a teljes és biztonságos végleges adattörlésre, legyen szó telefonról, tabletről vagy laptopról: amikor új készüléket vásárolunk, akkor kapunk hozzá egy ingyenes kódot, amivel a régi eszközön lévő adatokat véglegesen törölhetjük. Ezt a kódot be kell gépelni a veglegestorles.hu weboldalon, majd meg kell adni egy e-mail címet és az eszköz típusát, majd a kódaktiválás igénylése gomb lenyomása után követni kell a használati utasítást. A kód segítségével a készülék elvégzi minden adat végleges törlését, majd a folyamat végén egy igazoló e-mailt kapunk, hogy a készülékről minden adat helyreállíthatatlanul törölve lett. Ezután már nyugodt szívvel megválhatunk a készüléktől. Fontos kiemelni, hogy **vásárláskor az adattörlő kódot a kereskedő köteles átadni, így azt automatikusan és ingyenesen megkapjuk**.

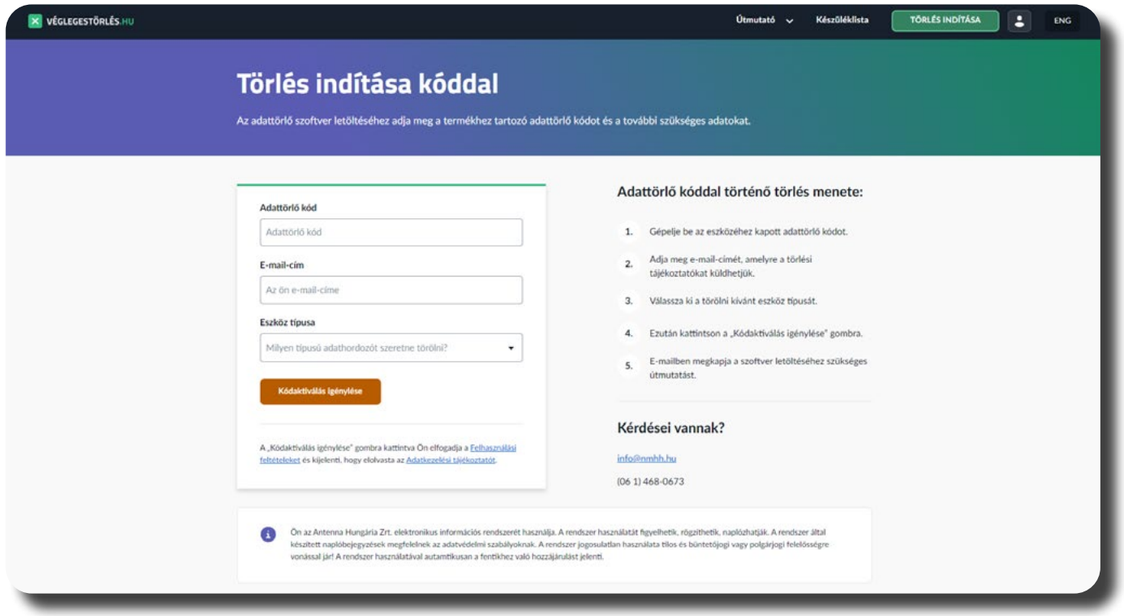
Ez többnyire a gyakorlatban úgy nyilvánul meg, a kereskedők az adattörlő kódot a számlán vagy nyugtán történő rögzítéssel, illetve ettől eltérő, egyéb módon (így különösen papír alapon) adják át a fogyasztók részére. Egy ilyen adattörlő kóddal egyetlen tartós adathordozó eszköz egyszeri törlésére nyílik lehetőség. Amennyiben nem kaptunk ilyen kódot a kereskedőtől, akkor az NMHH-tól is tudunk igényelni a vásárlásról szóló bizonylat bemutatásával.

Mit is csinál pontosan az NMHH által biztosított adattörlő kód?

Mobiltelefon adattörlése esetén gyakorlatilag egy applikáció kerül letöltésre a telefonunkra, ami elvégzi az adattörlést. A törlést követően a mobileszköz a vásárláskori alapállapotába kerül. Android rendszeren számos hozzáférést kell adni az adattörlő szoftvernek. Ezen részletesen a veglegestorles.hu által biztosított felhasználói kézikönyv vezet végig.



3. ábra
A véglegestörlés.hu weboldalának felülete (mobil eszközök)



4. ábra
A véglegestörlés.hu weboldalának felülete (PC felület)

PC esetében le kell tölteni egy programot, melyet szükséges ezután felmásolni egy pendrive-re, ami alkalmas boot-olásra. Egyúttal át kell állítani a PC-t pendrive-ról való boot-olásra a BIOS/UEFI rendszerben, majd innen fogja elvégezni a törlést a program. Ezután megkapjuk a tanúsítványt e-mailben, ha megfelelően jártunk el. A külső eszközről való indítást számos BIOS/UEFI beállítás akadályozhatja, emiatt érdemes részletesen áttanulmányozni a veglegestorles.hu által biztosított felhasználói kézikönyvet. Ezután egy bejelentkezési felületre jutunk, melynek egyszerű instrukcióit követve már végre tudjuk hajtani az adattörlést.

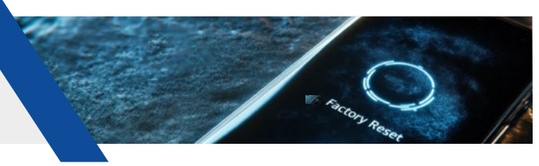
Titkosítás alkalmazása

Indokoltnak tűnik egy kis kitekintés a titkosítási eljárásokra is. Ez egy olyan folyamat, melynek során az adatokat átalakítják egy olyan formába, amely csak az arra jogosultak számára olvasható egy titkosítási kulcs segítségével. A gyakorlatban ez úgy néz ki, hogy az operációs rendszeren egy olyan speciális szoftvert használunk, amely az összes merevlemezen – vagy egyéb meghajtón – tárolt adatot egy titkosítási algoritmus segítségével átalakítja illetéktelenek számára olvashatatlan formátummá. Ezt követően az adatok egy titkosítási kulcs – például karakterlánc – segítségével könnyedén visszafejthetők. Ha nem áll rendelkezésre a kulcs, akkor gyakorlatilag – az alkalmazott algoritmustól függően – visszafejthetetlenek a titkosított adatok. A titkosítás és a végleges adattörlés két különböző biztonsági módszer, azonban jól kiegészítik egymást. A titkosítás erejét jól mutatja, hogy egyes vállalatok az eszközök selejtezése során csakis ilyen „kriptográfiai törlést" alkalmaznak, mivel ez a módszer kifejezetten gyors, míg a felülírással végzett adatmentesítés ennél jóval több időt vesz igénybe.

A fentiekre figyelemmel kifejezetten tanácsos titkosítást végző szoftvereket alkalmazni, melyet szerencsére minden népszerűbb operációs rendszer tartalmaz már beépített eszközként is.

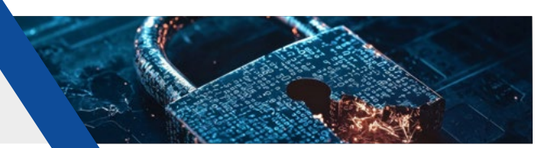
Ha szeretne többet megtudni a kriptográfia világáról, olvasásra ajánljuk A kriptográfia napjainkban című kiberbiztonsági elemzésünket.

Gyári visszaállítás



Gyakran hangzik el ellenérvként az adattörlő szoftverekkel szemben, hogy felesleges azok alkalmazása, ha gyári visszaállítást (angolul factory reset) eszközölünk a készülékünkön. **Ez sajnos nem jelent feltétlen garanciát, a gyári visszaállítással nem tudjuk szavatolni a végleges törlést**. A gyári visszaállítás egy olyan művelet, amely visszaállítja az informatikai eszközt az eredeti, gyári állapotába. Ez a művelet általában törli az összes felhasználói adatot, alkalmazást és beállítást, majd újratelepíti az operációs rendszert és az alapértelmezett alkalmazásokat, amelyek az eszköz első bekapcsolásakor jelen voltak, ugyanakkor az eszközben lévő háttértároló nem feltétlenül kerül teljesen „üres" állapotba. Ilyen esetben az eredeti problémakör áll fenn, annak ellenére, hogy ennek elvégzése még mindig jobb, mintha semmilyen adatvédelmi intézkedést nem tettünk volna.

Fizikai megsemmisítés



A szoftveres adattörlés mellett egy másik kategória a fizikai megsemmisítés. Ennek az eljárásnak a lényege az, hogy az adathordozót **egy olyan eljárásnak teszik ki, amelynek eredményeképpen az eszközről** – legalábbis a technika mai állása szerint – **lehetetlen az adatok visszaállítása**.

A fizikai megsemmisítés gyakorlatilag a legbiztosabb módszernek tekinthető adatvédelmi szempontból, azonban ebben az esetben a költséghatékonysági szempontok teljes mértékben háttérbe szorulnak, mivel az eszközök további felhasználása, értékesítése már nem lehetséges. Mégis azonban vannak helyzetek, mikor érdemes ezt választani, mert az eszközön olyan szenzitív adatok vannak, melyeknél kritikus fontosságú az, hogy illetéktelen személy ne férjen hozzá. A fizikai megsemmisítési módszereknél szintén figyelembe kell venni azt, hogy pontosan milyen adathordozóról van szó (és annak mi a működési elve), azonban ezen túl már a kreativitásunk és a költségvetésünk szab határt.

A pendrive-ok és memórikártyák esetén jó módszer lehet a fizikai zúzás, égetés vagy darabolás. A HDD-k esetében más módszerek is szóba jönnek a sajátos felépítése miatt: a merevlemezek zúzása vagy éppen a lemeztányérok több helyen történő átfúrása.

Ezen felül, mivel mágneses elven működő eszközről van szó – a HDD-k esetében - egy erős mágneses mező alkalmazása – ún. degausser gép - éppúgy tönkreteszi a rajta lévő adatokat. A degausser működése viszonylag egyszerű: a készülék erős mágneses mezőt hoz létre, amely képes megzavarni a tárolóeszközökben lévő részecskék mágneses orientációját (vagy mágneses tartományát). A degaussing folyamat eredményeként az elektronikus eszközökben tárolt adatok teljes mértékben törlődnek, ezt követően az eszközök továbbadhatók például újrahasznosításra.

5. ábra
Degausser gép

Léteznek olyan, egyéb módon működő célgépek is, amelyek egész egyszerűen szétzúzzák az adathordozókat. Az ilyen eszközök használata is inkább vállalati környezetben lehet elérhető, illetve célszerű, ahol esetenként több száz ilyen eszköz megsemmisítéséről kell gondoskodni.

6. ábra
Zúzógép elektronikus adattárolókhoz

Érdekességként megemlíthető, hogy léteznek egyéb speciális mechanikai eszközök is, melyek kifejezetten a merevlemezek használhatatlanná tételére szolgálnak: ilyen például a merevlemez roppantó, amely gyakorlatilag egy hosszú erőkarral ellátott satuszerű eszköz, mely teljesen használhatatlanná teszi az eszközt.

7. ábra
Merevlemez roppantó

Iparági szakértők tanácsai

Ezen CTI jelentés írásakor célunk volt, hogy a lehető legtöbb aspektusból körbejárjuk a témát. Ennek részeként megkérdeztünk egy témában jártas iparági szakértőt is, hogy milyen tanácsai vannak a lakosági felhasználók részére. **Solymos Ákos**, a Quadron Kibervédelmi Szolgáltató Zrt. szakértője elsőként azt ajánlotta, hogy amennyiben mélyebb ismereteket szeretnénk szerezni az adathordozók végleges törlését illetően, akkor érdemes lehet áttanulmányozni a különféle iparági szabványokat.

Az első ilyen elterjedt szabvány az Amerikai Védelmi Minisztérium (Department of Defense, DoD) által létrehozott és korábban említett DoD 5220.22-M volt, amely különösen a digitális adathordozók végleges törlésére vonatkozott. Ez részletesen ismertette azokat a módszereket, amelyekkel az érzékeny információk biztonságosan eltávolíthatók voltak az adathordozókról oly módon, hogy azok visszaállítása ne legyen lehetséges. A legelterjedtebb eljárás a **felülírásos törlés**, amely során az adatokat többszörösen felülírják. A szabvány meghatározza, hogy az egyes adathordozókat hányszor szükséges felülírni a teljes törlés érdekében. A szakértő rámutatott, hogy a legnagyobb problémát az jelenti, hogy a felhasználók – a technológia mélyebb ismerete nélkül – **tévesen azt feltételezik, hogy ha egy fájlt törölnek, az végleg eltűnik**.

Nem feltétlenül tudják, hogy az adathordozókon – például a hagyományos merevelemezeken - van egy olyan rész elkülönítve, ahol azok az adatok foglalnak helyet, amelyek referenciaként mutatnak az egyes adatok az adathordozó különböző részein való fizikai elhelyezkedésére. A felhasználók pedig nincsenek azzal tisztában, hogy amikor törölnek valamit, akkor nem a tényleges adatok kerülnek törlésre – mivel ez technikailag időigényes – hanem csak az arra mutató, az un. fájl allokációs táblában tárolt hivatkozás. Emiatt a törölni szándékozott adat még megtalálható az adathordozón és majd csak később kerül felülírásra.

A különféle adatvisszaállító szoftverek pontosan ilyen elven működnek, hogy részletesen átnézik a merevlemezt ilyen adatállományok után kutatva, és ilyenkor sikeresen megtalálják ezeket a „törölt” állományokat. Ez a módszer elsősorban a hagyományos merevlemezekre igaz, azonban az újabb technológiák, például az SSD-k, eltérő működési elveket követnek. Az SSD-k esetében az adatok tárolásának módja és az úgynevezett garbage collection, illetve TRIM funkció miatt más törlési eljárásokat kell alkalmazni.

Az elmúlt években a DoD 5220.22-M szabvány elavulttá vált, ezért 2015-ben az NIST (National Institute of Standards and Technology) kiadta a NIST Special Publication 800-88 szabványt, amely “*Guidelines for Media Sanitization*” néven vált ismertté. Ez a szabvány újabb, hatékonyabb törlési módszereket ajánlott. Ezen felül 2022-ben megjelent az IEEE 2883-2022 szabvány, amely részletesen meghatározta, hogy az egyes adathordozótípusokat milyen módon érdemes megsemmisíteni – beleértve az adathordozók teljes fizikai megsemmisítését is. Bizonyos esetekben ez hatékonyabb megoldás lehet, mint a szoftveres törlési technikák alkalmazása.

A vállalati környezetben gyakran alkalmaznak fizikai megsemmisítési módszereket, például demagnetizálást vagy mechanikai aprítást. A demagnetizálás (degaussing) esetenként nehézkes, mivel a demagnetizáló eszközök nem mindig biztosítanak azonnali visszajelzést a törlés sikerességéről, így manuális ellenőrzést igényelhetnek, ami jelentős erőforrást emészt fel. A szakértő saját tapasztalatára hivatkozva elmondta, hogy egy korábbi munkahelyén közel 1000 merevlemez fizikai megsemmisítésére kényszerültek, mivel a használt degausser nem garantálta a teljes adatmegsemmisítést. Ezt végül ipari szemétégetőben hajtották végre, ahol az adathordozók olvadásig hevültek, biztosítva, hogy az adatok helyreállíthatatlanok legyenek.

A hangsúly itt az ipari kifejezésen van, ugyanis otthoni körülmények között – pl.: egy szalonnasütőben – nem lehet elégséges hőfokot elérni a megfelelő eredményhez. Példaként említette a Kürt Zrt. esettanulmányait, melyekben már több esetben publikáltak róla, hogy sikeresen tudtak adatokat visszaállítani megégett vagy egyéb módon súlyosan megrongálódott merevlemezekről is.

Megosztotta velünk saját tapasztalatát is az otthoni körülmények közötti megsemmisítésről is: a merevlemez megsemmisítése, bizony kemény munka. Az eszközben lévő fém korongok meghajlítása kifejezetten nagy erőkifejtést igényel.

Erről az alábbi linken lévő szakkcikkben bővebben is olvashatunk.

A vizsgált merevlemez roncsolásos adatmegsemmisítése (kemény meló, a csavarhúzó is roncsolódott)

8. ábra

Merevlemez megsemmisítése házilag

A szabványok az adathordozók véletlen bitrátával történő többszörös felülírását javasolják. A szabványok szerint 7-8 ilyen felülírás már elegendő, ha biztos eredményt szeretnénk. Ennél viszont egyszerűbb és gyorsabb az un. purgálás, amikor az egész merevlemez teleírásra kerül titkosított adattal, majd a titkosító kulcsot töröljük. Ez a funkció megtalálható már a különféle adattörlő szoftverekben.

Kérdésként merült fel, hogy valóban indokolt-e a nyolcszoros felülírás vagy ez már csak egy túlbiztosítás. Erre válaszként kaptuk, hogy attól függ, hogy mennyire akarjuk az adatot védeni, milyen bizalmasságú adatunk van. Példának említette azt, hogy régebben rengeteg olyan csalás volt, mely arra épült, hogy Afrikából megvásároltak nagy mennyiségben Angliából származó, kiselejtezett merevlemezeket és visszaállították az adattartalmukat, és így tettek szert például bankkártya adatokra az elkövetői körök. Vagyis, **ha valóban olyan szenzitív adatokat tartalmazhat az adathordozó, akkor célszerű lehet ez a túlbiztosítás.** Itt azonban a szakértő szerette volna különválasztani azt, hogy magánszemélyekről vagy cégekről van-e szó. Ő magánszemélyeknek mindig azt szokta javasolni, hogy adathordozót ne adjanak el, például egy megunt laptoppal együtt. A mobiltelefonok esetében kicsit más a helyzet, mivel annak nem szerelhető ki a háttértárolója, így arra azt szokta javasolni, hogy legalább egy gyári visszaállítást mindenképpen alkalmazzunk.

Hozzáteszi ugyanakkor, hogy magánszemélyek esetében a háromszoros felülírás is jónak mondható, mert ha már nem lehetséges megállapítani, hogy kié volt korábban a merevlemez, akkor arról már jellemzően nem lehet adatokat visszanyerni érdemben. A céges környezetben – például egy banknál – mindenképpen érdemes az ilyen jellegű túlbiztosítás a védendő adatok jellege miatt.

Konklúzióként elmondta, hogy otthoni környezetben, ha lehet, akkor ne adjunk el adathordozót, vagy mindenképpen használjunk szoftveres felülírást, mivel a fizikai megsemmisítés komolyabb erőfeszítést igényel. A szoftveres felülíráshoz a gyakorlatban nagyon könnyen – esetenként ingyenesen – elérhetőek szoftverek.

A mobiltelefonok törlése, illetve továbbadása kapcsán pedig nem szabad elfelejtkezni az extra tárhelyként szolgáló memóriakártyáról sem, melyet vagy távolítsunk el, vagy gondoskodjuk annak a megfelelő törléséről is. Azonban a telefonok fizikai megsemmisítése is indokolt lehet esetenként.

Az alkalmazott intézkedések kiválasztásánál fontos vezérelv, hogy mindig érdemes megnézni egy támadó motivációját, hogy mennyi időt és pénzt érhet meg neki egy adathordozóról vagy telefonról adatokat visszanyerni. Így például egy lakossági felhasználású eszköznél, nem valószínű, hogy több millió forintot fognak költeni az adatvisszaállításra, vagyis valamilyen szintű arányosságot érdemes lehet tartani az alkalmazott intézkedések és a bekövetkező várható veszteséggel kapcsolatban.

Kihangsúlyozandó, hogy a különféle adatvisszaállító szoftverek felhasználása nem igényel speciális ismereteket. Mindez természetesen sérülésmentes, működőképes adathordozókra igaz, ugyanis a sérült adathordozók esetén már speciális szakismeretekre – és esetleg laboratóriumi körülményekre - lehet szükség. Ilyenkor az adatvisszaállítás sikeressége azon múlhat, hogy mennyi adatról van szó és mennyire sérült maga az adathordozó. Itt jótanácsként hangzott el, hogy a fontos adatokat mentsük rendszeresen legalább két külön helyre, egyiket akár a felhőbe, míg a másikat lehetőleg egy merevlemezre, mivel az SSD-vel szemben az biztonságosabb a hosszú adattárolás szempontjából.

Az adataink védelme érdekében javasolt még a különféle merevlemez titkosító szoftverek használata, mely nagy segítség lehet abban az esetben, ha az eszközünket eltulajdonítják vagy esetleg elhagyjuk.

Esettanulmány

Az „*Emlékezés az eltávozott adatokra: A lemeztörlési gyakorlatok vizsgálata*” című tudományos értekezés egy olyan kísérleten alapult, melynek során a két szerző – Simson L. Garfinkel és Abhi Shelat - 2000 novembere és 2002 augusztusa között **158 db merevlemezt vásárolt** a másodlagos piacon, majd azokat vizsgálatnak vetették alá.

A források különböztek: voltak használt árucikkekre szakosodott számítógépes boltok, használt eszközöket értékesítő kisvállalkozások vagy éppen online aukciósportálok. A vásárolt meghajtók gyártója, mérete, állapota, és sok egyéb paramétere eltérő volt, illetve több működésképtelen is volt. A meghajtókat megfelelő dokumentálást követően egy operációs rendszerhez csatlakoztatták, majd azok adattartalmát blokkról blokkra a Unix dd parancsával egy image-fájlba másolták. Ezután megpróbálták az egyes meghajtókat különféle fájlrendszerek segítségével csatlakoztatni, majd elemzés alá vonták az eszközöket többféle módszerrel. A szerzők hipotézise az volt, hogy sok kiselejtezett merevlemez tartalmaz bizalmas és helyreállítható információt. A vizsgálat célja az volt, hogy megállapítsák, hogy a merevlemezek pontosan milyen információkat tartalmaznak és a korábbi tulajdonosok milyen eszközökkel/módszerekkel tisztították meg a meghajtókat, mielőtt kidobták őket.

A kísérlet eredményeképpen **75 gigabájtnyi adat** került beszerzésre, mely ugyan nem tűnik soknak, de ismét kiemelnénk, hogy a kísérlet 2000 és 2002 között zajlott, amikor még az átlag merevlemezek 10 és 60 gigabájt közötti tárolókapacitással rendelkeztek (ráadásul a kísérletben még sokkal elavultabb merevlemezeket használhattak, ugyanis ekkor ezek már „leselejtezett" eszközök voltak). A kísérlet során megállapították, hogy a **129 db sikeresen lementett meghajtó** közül csak **12 db volt megfelelően törölve** a szektorok nullákkal történő felülírásával. Összeségében **28 db** olyan meghajtó volt, amely **aktív fájlrendszerrel rendelkezett még és dokumentumfájlokat tartalmazott**.

A szerzők aránylag kevésnek találták az ilyen módon fellelt dokumentumokat, így az a hipotézis alakult ki bennük, hogy ezekről a meghajtókról szándékosan törölték már a korábbi tulajdonosok az általuk relevánsnak ítélt fájlokat. Ennek alátámasztására írtak egy programot, mely lehetővé tette a FAT16 és FAT32 fájlrendszerekben a törölt állományok helyreállítását, majd átvizsgálták a meghajtókat olyan adatok után, amelyeket feltehetően a meghajtó eredeti tulajdonosa törölt, mielőtt a meghajtót kidobta volna. A hipotézisük igazolást nyert, ugyanis a **12 db szakszerűen törölt merevlemezt leszámítva az összes meghajtón jelentős mennyiségű helyreállítható fájl volt**. A keresés eredményeképpen több szenzitív adat került elő: személyzeti kérdésekkel kapcsolatos vállalati memorandumok, magánlevelezések.

Ezt követően további finomításként egy olyan programot írtak, amely olyan számsorokat keresett, amelyek hitelkártya számként voltak azonosíthatók. Ennek eredményeként **42** meghajtón találtak ilyen számadatokat, majd annak érdekében, hogy megállapítsák, hogy valóban hitelkártyaszámról van-e szó, megvizsgálták a számok kontextusát, melyből azt a következtetést vonták le, hogy **5** meghajtó tartalmazott pénzügyi stílusú naplófájlokat. Az egyik ilyen meghajtó **2868** számot tartalmazott napló formátumban. További vizsgálat során kiderült, hogy ezt a merevlemezt valószínűleg egy illinoisi bankautomatában használták és nem tettek különösebb erőfeszítéseket a meghajtó érzékeny adatainak eltávolítására.

A kísérlet egyik fontos konklúziója volt, hogy a felhasználók ugyan tesznek intézkedéseket a meghajtók törlésére, azonban nincsenek tisztában azzal, hogy **az egyszerű törlés, de még a meghajtó formázása sem elegendő az adatok végleges eltávolításához**. Az sajnos nem derült ki a kísérletből, hogy azokban az esetekben, amikor történt intézkedés az adattörlésre, akkor azt még az eredeti felhasználók hajtották végre, vagy már azon személyek, akik a merevlemezek további értékesítését végezték. A kísérlet további részletei az eredeti tanulmányban olvashatóak részletesebben.

Egyéb kísérletek

A fenti tanulmányt követően számos hasonló kísérletet végeztek, főként különféle egyetemeken, melyek közül további kettőt kiemelnénk:

Egy ausztrál szerzőpáros – az Edith Cowan Egyetemen kutató Craig Valli és Andrew Woodwad – 2004-től kezdve folytatott egy tanulmányt a másodlagos piacon vásárolt merevlemezeken megtalálható adatokról, és szinte évente publikálásra is kerültek a tapasztalataik. A 2008-as tanulmány alapjául szolgáló kísérletben összesen 48 meghajtót vizsgáltak meg, melyek többnyire árverések útján kerültek beszerzésre.

Megállapították, hogy megfigyelhető egyfajta javuló tendencia, mivel valamelyest nőtt a szakszerűen törölt merevlemezek száma, azonban még mindig **jelentős mennyiségű bizalmas és kereskedelmi adat volt megtalálható** a merevlemezeken. Ezen felül számos esetben találtak különleges személyes adatokat is, mint például egy idősotthon lakóinak egészségügyi információt.

2022-ben szintén megjelent egy tanulmány az egyik tudományos folyóiratban, mely az Egyesült Királyságban vizsgálta, hogy 100 db 2018 áprilisa és decembere között használtan vásárolt mobiltelefonon és táblagépen milyen mennyiségű és típusú információ maradt fennt. A kísérlet konklúziója az volt, hogy a készülékek adattörlése nem volt teljeskörű, összesen 72 eszköz adatmentése volt sikeres, melyből 53 készüléket visszaállítottak a gyári alapbeállításokra.

Az alábbi operációs rendszerek voltak azonosíthatók: 29 Android, 20 Apple IOS, 7 Blackberry OS, 8 Windows mobil és 8 egyéb. Fontos megjegyezni, hogy itt is csak olyan adatok helyreállítását tűzte ki a vizsgálat célul, amelyekhez bárki, aki az eszközt megvásárolta, speciális eszközök használata nélkül is – tehát igazságügyi célszoftverek nélkül - hozzáférhetett. A tanulmány bemutatja azt is tételesen – természetesen anonim formában -, hogy milyen adatokat sikerült kinyerni a készülékekről.

Végső konklúzió

Jelentésünkben részletesen megvizsgáltuk azokat az adattároló eszközöket, amelyekkel egy átlagos felhasználó találkozhat, és alapos ismereteket szereztünk a működési elvükről. Megértettük, hogy a digitális adatok törlése nem mindig jelenti azok végleges eltávolítását, ami különösen fontos adatvédelmi és biztonsági szempontból. A tanulmányunk során bebizonyosodott, hogy **a hagyományos törlési módszerek**, mint a fájlok egyszerű törlése vagy a „lomtár kiürítése" **nem elegendőek** az adatok helyreállíthatatlanságának biztosításához. Az adathordozók **fizikai megsemmisítése** vagy **speciális szoftverek** használata szükséges ahhoz, hogy a tárolt adatok ne kerülhessenek illetéktelen kezekbe.

Az adattörlési technikák, mint például a Degaussing, a Secure Erase vagy a kriptográfiai törlés, mind hatékony eszközök lehetnek a végleges adattörlésre. Ezek a módszerek biztosítják, hogy a törölt adatok még speciális helyreállítási eszközökkel se legyenek visszaállíthatók.

Javaslataink alapján **a lakossági felhasználóknak nagyobb figyelmet kell fordítaniuk az adatok megsemmisítésre**. A jelentésünk részletes útmutatót nyújt a megfelelő adattörlési technikák kiválasztásához és alkalmazásához. Tudatosítanunk kell magunkban, hogy az adatok biztonságos törlése nem csupán technikai kérdés, hanem felelősségünk is, hogy megvédjük magunkat és másokat az adatlopások és visszaélések ellen. Ezért fontos, hogy mind lakossági, mind vállalati szinten alkalmazzuk az itt bemutatott technikákat és eljárásokat, hogy garantáljuk az adatok végleges eltávolítását.

Végső soron a megfelelő adattörlési módszerek alkalmazása **kritikus lépés az adatbiztonság fenntartásában és a kibertámadások elleni védekezésben**. Ezzel a tudatossággal és felkészültséggel jelentősen csökkenthetjük a digitális adatokkal kapcsolatos kockázatokat és védhetjük személyes és üzleti információinkat a jövőben.

Források

- **Angelopoulou, O., Jones, A., Horsman, G. & Pourmoafi, S.** (2022) *A Study of the Data Remaining on Second-Hand Mobile Devices in the UK. Journal of Digital Forensics, Security and Law*, 17(2), Article 5. https://www.researchgate.net/publication/372670013_A_Study_of_the_Data_Remaining_on_Second-Hand_Mobile_Devices_in_the_UK (Letöltve: 2025. február 10.)
- **Balogh, Zs. Gy.** (2018) *Az informatikai biztonság szabályozása*. NKE Budapest.

- **ERI** (n.d.) *Improper Disposal of Hard Drives Leads to Large Healthcare Data Breach*. https://eridirect.com/news/2023/11/improper-disposal-of-hard-drives-leads-to-large-healthcare-data-breach/ (Letöltve: 2025. február 7.)
- **GUTMANN, P.** (1996) *Secure Deletion of Data from Magnetic and Solid-State Memory*. University of Auckland. https://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html (Letöltve: 2025. február 19.)
- **Horváth, G.** (2021) *Számítógép architektúrák*. BME jegyzet.
- **Kiber Blog.** (2021) *Adatok a szemétdombról: Több ezer egészségügyi és beteg adat végezte egy hulladék konténerben.* https://kiber.blog.hu/2021/02/26/adatok_a_szemetdombrol_tobbezer_egeszsegugyi_es_beteg_adat_vegezte_egy_hulladek_kontenerben (Letöltve: 2024. október 9.)
- **KÜRT Információbiztonsági és Adatmentő Zrt.** (2022) *Így működik az adatmentés*. https://kurt.hu/2022/08/03/igy-mukodik-az-adatmentes/ (Letöltve: 2025. február 19.)
- **MIT** (2003) *Remembrance of Data Passed: A Study of Disk Sanitization Practices*. https://www.mit.edu/people/ebh/www/disksanitization.pdf (Letöltve: 2025. február 19.)
- **MIT** (2003) *Remembrance of data passed: A study of disk sanitization practices.* https://www.mit.edu/people/ebh/www/disksanitization.pdf (Letöltve: 2025. február 19.)
- **Nagy, Z. A.** (é.n.) *Kibernyomozói kézikönyv*. Budapest, Ludovika. Egyetemi Kiadó.

- **News12** (n.d.) *Hard drive containing personal hospital records sold online*. https://longisland.news12.com/hard-drive-containing-personal-hospital-records-sold-online-37103529 (Letöltve: 2025. február 10.)
- **Nyakóné Dr. Juhász, K., Dr. Terdik, Gy., Biró, P., Dr. Kátai, Z.** (2011) *Bevezetés az informatikába*. Digitális Tankönyvtár.
- **PHISTON TECHNOLOGIES** (n.d.) *What is Degaussing, And How Is It Used for Data Destruction?* http://phiston.com/what-is-degaussing-and-how-is-it-used-for-data-destruction/ (Letöltve: 2024. június 4.)
- **PROHARDVER!** (é.n.) *TRIM (SSD)*. https://prohardver.hu/tudastar/trim_ssd.html (Letöltve: 2025. február 19.)
- **Solymos, Á.** (2024. október 1.) *Online interjú*. Személyes kommunikáció.
- **VALLI, C. és WOODWARD, A.** (2008) *The 2008 Australian Study of Remnant Data Contained on 2nd Hand Hard Disks: The Saga Continues.* https://www.researchgate.net/publication/230568499_The_2008_Australian_study_of_remnant_data_contained_on_2nd_hand_harddisks_the_saga_continues (Letöltve: 2025. február 10.)

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2025