Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Bezpečná likvidace datových médií a mazání dat

Diplomová práce

Autor: Bc. Jiří Klouda
Studijní obor: Aplikovaná informatika

Vedoucí práce: Mgr. Josef Horálek Ph.D.

Hradec Králové duben 2023

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a s použitím uvedené literatury.

vlastnoruční podpis

V Hradci Králové dne 3.4.2023 Jméno a Příjmení

Poděkování:

Děkuji vedoucímu bakalářské práce Mgr. Josefu Horálkovi Ph.D. za metodické vedení práce.

Anotace

Tato diplomová práce se zabývá problematikou bezpečného mazání dat z datových nosičů, zejména pak z pevných disků a SSD. V teoretické části jsou popsány druhy nosičů dat, jejich fyzická a logická struktura a způsob uložení dat. Dále jsou zde uvedeny možnosti likvidace dat pomocí definovaných algoritmů a metod a také fyzická likvidace datových nosičů. Závěr teoretické části je věnován platným právním předpisům a normám, zejména ze zemí Severní Ameriky a Evropské Unie.
V praktické části je realizováno mazání dat z pevných disků různými metodami. Je zkoumána jejich efektivita a časová náročnost. Poté je podle výsledků definována sada doporučení, kterými by se měl uživatel řídit v případě, kdy chce bezpečně odstranit svá data.

Annotation

Title: Secure data media disposal and data erasure

This thesis deals with the issue of secure deletion of data from data carriers, especially from hard disks and SSDs. The theoretical part describes the types of data carriers, their physical and logical structure and the way of data storage. Furthermore, the possibilities of data disposal using defined algorithms and methods as well as physical disposal of data carriers are presented. The theoretical part concludes with the current legislation and standards, especially from North American and European Union countries.
In the practical part, the deletion of data from hard disks is implemented using various methods. Their effectiveness and time consumption are examined. Then, according to the results, a set of recommendations is defined that the users should follow in case they want to safely delete their data.

Obsah

Obsah

1 Úvod

V dnešní době jsou na paměťová média ukládána velká množství citlivých dat. Firmy mají ve formě elektronických dat smlouvy, obchodní informace, data zákazníků nebo marketingové podklady. Na osobních počítačích uživatelů lze najít bankovní informace nebo soukromé fotografie. Uživatel si mnohy bohužel neuvědomuje, že se na disku takováto data stále nachází nebo dříve nacházela a že smazání těchto dat neznamená jejich faktické zničení. Ve většině případů lze smazaná data bez problémů obnovit a díky volně dostupným nástrojům nemusí být proces obnovení pouze práce pro odborníka z laboratoře. Úspěšnou obnovu může provést i útočník, který následně citlivá data zneužije.

Aby se zabránilo zneužití soukromých nebo firemních dat, je nutné je spolehlivě zlikvidovat. To lze provést mechanickým zničením datového nosiče, nebo využít speciální software, který uložená data nenávratně zlikviduje.

Uživatelé by si měli být těchto skutečností vědomi a před likvidací nebo prodejem datového nosiče provést důkladnou sanitaci celého zařízení. Mohou se tak vyhnout nechtěnému úniku dat, který v některých případech může skončit vysokou pokutou případně mít jiné nepříjemné následky.

2 Cíl práce

Teoretická část

Teoretická část práce si klade za cíl popsat možnosti bezpečné likvidace dat a datových médií. Dílčími cíli jsou popis fyzické a logické struktury pevných disků HDD a polovodičových disků SSD, vysvětlení způsobu uložení dat a rozbor algoritmů pro jednoduchý i vícenásobný přepis, způsoby destrukce digitálních i analogových dat a ekologická likvidace datových nosičů. Závěrem je uvedena platná legislativa a normy zabývající se touto problematikou.

Praktická část

Cílem praktické části je realizace konkrétních metod pro bezpečné mazání cvičné sady dat z mechanických disků a z disků s polovodičovou pamětí. Po smazání disku jsou data získávána zpět pomocí standardního softwaru pro jejich obnovu. U jednotlivých metod je zkoumána úspěšnost a čas potřebný pro smazání celého disku. Závěrečná analýza výsledků porovnává jednotlivé metody a na základě získaných informací je pro uživatele vytvořen soubor doporučení pro bezpečnou likvidaci dat.

3 Související práce

Problematikou bezpečného mazání dat z magnetických a polovodičových pamětí se ve své práci [47] z roku 1996 zabýval již Peter Gutmann. Analyzoval metody pro bezpečné mazání dat a zkoumal obnovu dat z takto smazaných disků na tu dobu velmi pokročilými technikami. Ve své práci zjišťuje zejména to, kolik přepisů je potřeba, aby se z datového média nedala obnovit žádná data a zkoumá možnosti využití magnetického pole pro likvidaci záznamu na magnetických médiích. Jako média jsou, vzhledem k roku publikace, uvedeny také diskety a magnetické pásky. Dále se zabývá problémem mazání dat z paměti typu Random-Access Memory (RAM), kde, vzhledem k tehdy použitých technologiím, shledává takovou obnovu dat jako velmi problematickou. Závěrem zmiňuje, že i když je magnetické médium několikrát přepsáno, lze z něj pokročilými metodami obnovit smazaná data nebo alespoň jejich část. V rámci této práce také navrhuje Peter Gutmann společně s Colinem Plumbem takzvanou Gutmannovu metodu, která přepisuje magnetický disk pomocí 35 průchodů.

Práce Petera Gutmanna částečně inspirovala studenty indické PES Univerzity, kteří pod vedením profesora Prasada Honnavalliho představili na Mezinárodní konferenci o kybernetické bezpečnosti začátkem roku 2021 práci, řešící problematiku mazání dat ze soukromých zařízení zaměstnanců firem [48]. V ní jsou popsány situace, kdy je potřeba z uživatelského zařízení smazat pouze firemní data bez toho, aniž by byla zasažena také data uživatele. Pro tento účel jsou zde navrženy algoritmy pro dva různé přístupy. Prvním je přepsání místa na disku, kde se nachází soubor. Druhým pak šifrování citlivých dat. Obě navržená řešení přináší uspokojivé výsledky a jsou autory označeny jako bezpečné metody pro mazání dat. Závěrem je zmíněno, že pro bezpečné smazání souboru pomocí přepisu cílového místa je plně dostačující pouze jeden průchod algoritmu.

4 Metodika zpracování

Teoretická část je zpracována analýzou odborné literatury a její následnou syntézou. Pro podporu literární rešerše jsou využity informace z odborných článků a internetových zdrojů. Praktická část vychází z teoretických poznatků a jsou zde demonstrovány ukázky mazání dat. Závěrem jsou shrnuty jednotlivé metody a je doporučen nejlepší postup.

5 Likvidace datových nosičů a mazání dat

Pod pojmem datový nosič si lze představit zařízení, které používá určitou formu záznamu pro uložení dat. Data mohou být uložena ve formě magnetického, optického nebo elektronického záznamu.

5.1 Pevný disk

Pevný disk (anglicky Hard Disk Drive neboli HDD) je jedním z nejčastěji používaných paměťových médií. Nabízí široké uplatnění napříč celou škálou moderních technologií. [1]

Primární funkcí pevného disku je zálohování dat. Mezi nejdůležitější parametry pevných disků proto patří kapacita, dále přístupová doba, přenosová rychlost, rychlost otáčení a cache neboli vyrovnávací paměť. [1]

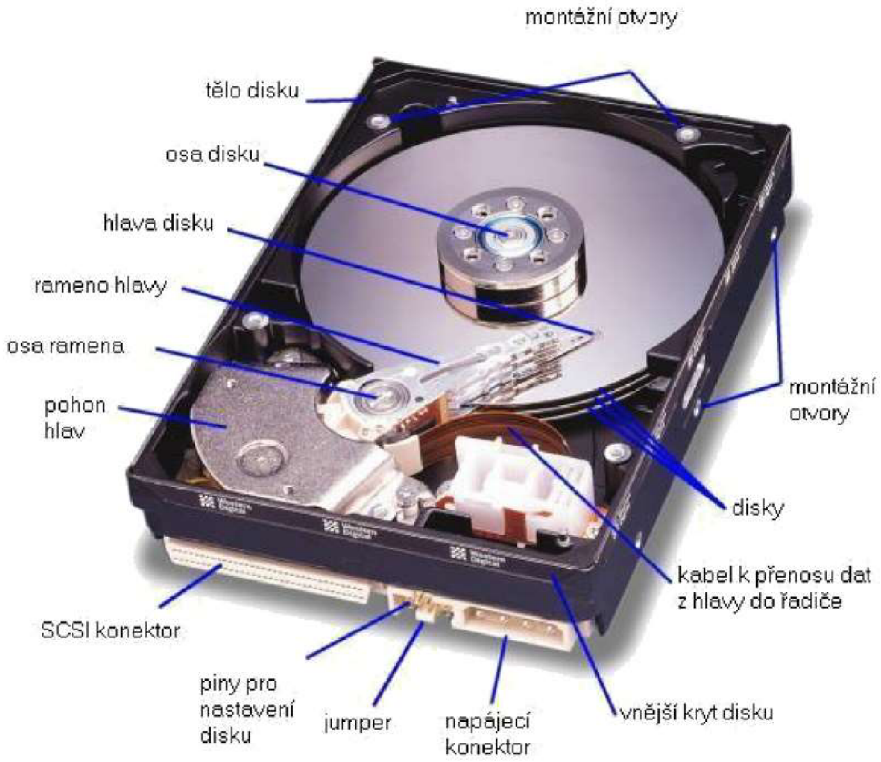
5.2 Fyzická struktura pevného disku

Datové médium pevného disku je složeno z tuhých kotoučů tzv. ploten, umístěných v několika patrech nad sebou. [2]

Plotny se vyrábí především z hliníku nebo legovaného hliníku. Novinkou jsou pak plotny vyráběné ze speciálního skla, na něž se oboustranným naprašováním nanáší zmagnetizovatelná vrstva oxidu železnatého nebo železitého. Je to vrstva, do níž se ukládají data. [3]

Pro čtení a zápis dat slouží elektromagnetická součástka s názvem hlava. Hlavy se nepohybují po povrchu disku, ale vznášejí se nad ním. To zajišťuje aerodynamický vztlak vznikající nad roztočeným diskem. Protože hlavy plují nad diskem, nedochází ke tření mezi hlavou a diskem. [2]

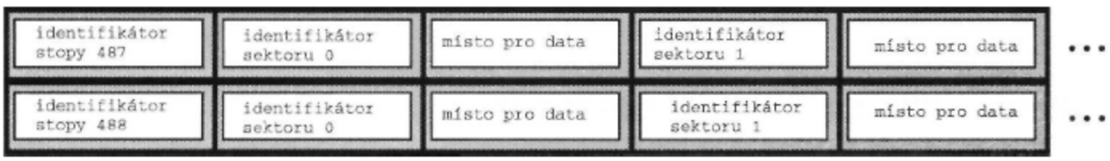
Plotny se v pevném disku otáčí neustále, ne jen když se s ním pracuje. Rychlost otáčení se pohybuje v intervalu mezi 3 600-15 000 otáčkami za minutu, magnetická hlavička se nachází asi 0,3-0,5 mikrometrů nad povrchem disku. Neustálé snižování výšky hlavičky nad povrchem disku je prostředkem pro zvyšování hustoty záznamu. Dají se takto lépe rozpoznávat čím dál slabší signály pocházející ze stále menších paměťových oblastí. V současnosti se již dá dosáhnout výšky v jednotkách nanometrů. [3]



Obrázek 1: Pevný disk (převzato z [4])

5.2.1 Fyzické formátování

Pokud operační systém požaduje od disku data, musí je na jeho povrchu vyhledat řadič. Jedná se o elektronickou řídící jednotku, která má na starost činnosti všech částí počítače. Ten tedy potřebuje znát přesnou geometrickou polohu zapsaných dat. Proto si povrch disku rozdělí na stopy (soustředné kružnice), do kterých si údaje zapisuje. Každá stopa je navíc příčně rozdělena na sektory. [2]



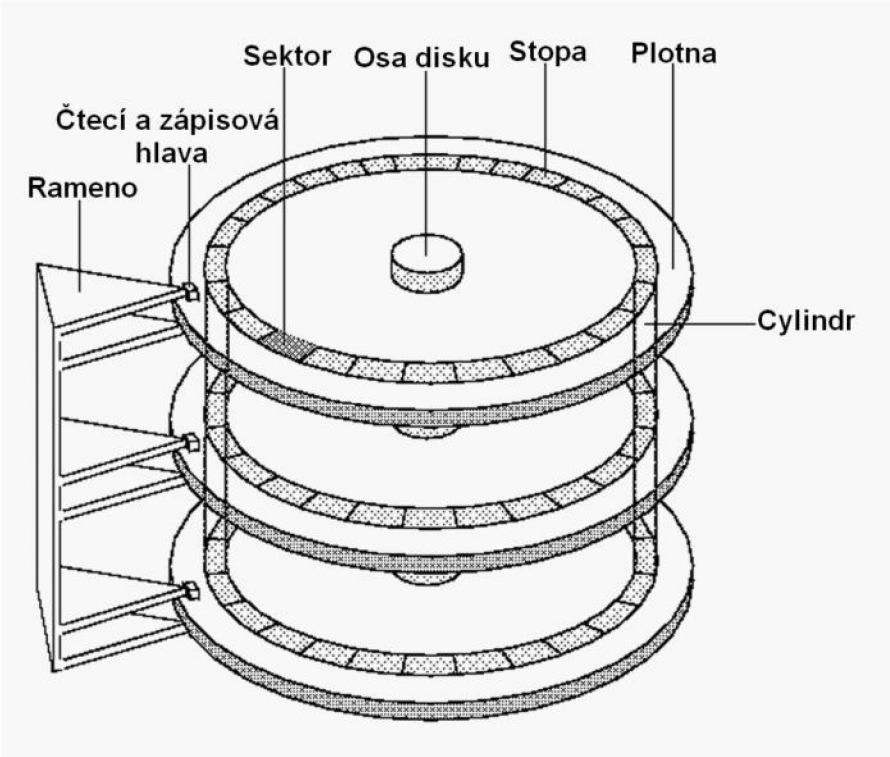
Obrázek 2: Fyzické formátování (převzato z [2])

Vzhledem k tomu, že pevný disk zpravidla obsahuje několik kotoučů a následně několik hlaviček pro čtení a zápis, používá pro označení stop ležících na jednotlivých discích navzájem pod sebou pojem cylindr. Data se pak ukládají

nikoliv tak, aby se nejprve zaplnil jeden kotouč a následně další, ale daty se nejprve obsazují jednotlivé cylindry. Tento způsob pak vede k rychlejší práci disku, protože rameno hlavičky pro čtení a zápis nemusí při ukládání měnit svou polohu. [3]

5.2.2 Hlavy a cylindry

Zápis a čtení dat mají na starosti magnetické hlavičky. Jsou to cívky navinuté na jádrech a na ramenech se vznášejí těsně nad povrchem ploten. [5]
Má-li pevný disk 5 kotoučů, může mít až 10 hlav, protože každý kotouč má 2 povrchy. Hlav však může být i méně, protože krajní kotouče nemusí mít nutně povrchy z obou stran. Všechny hlavy jsou umístěny na společném rameni. Pokud řadič posune hlavu číslo 3 (patřící třetímu povrchu) nad stopu 134, posunou se i hlavy nad ostatními kotouči nad stopu 134 „svého" povrchu. Díky společnému rameni se tedy hlavy vždy vznášejí nad stejnou stopou všech povrchů tedy cylindrem. [2]



Obrázek 3: Vizualizace fyzické struktury disku (převzato z [5])

Pokud cívkou prochází elektrický proud, dojde k vytvoření magnetického toku, který se uzavírá ve štěrbině mezi hlavičkou a plotnou a tím ovlivňuje i záznamovou vrstvu pevného disku. V závislosti na směru toku proudu při této operaci dochází k zmagnetizování daného místa určitým směrem. Mezi dvěma zmagnetizovanými místy vznikají tzv. magnetické reverzace. Jedná se o místa, v nichž se mění směr magnetizace, a právě ona jsou zodpovědná za vlastní funkčnost této metody zápisu. [5]

Čtení dat probíhá opačným způsobem nežli zápis. Během pohybu hlaviček nad povrchem plotny reagují cívky právě na magnetické reverzace a ty následně vyvolávají magnetický tok, který je zpracováván na elektrický impuls a dále řídící elektronikou disku. Dnes se používá technika kolmého zápisu dat, kdy orientace magnetického pole je kolmá vůči povrchu plotny. Tato technologie využívá pro záznam magneticky tvrdší materiály společně s magneticky měkkou spodní vrstvou, která pomáhá hlavičce v zápisu dat. Výhodou je vysoká hustota zápisu. [5]

5.2.3 Přístupová doba

Přístupová doba disku je doba, která udává, za jak dlouho se získá první datový znak po zahájení požadavku. Zahrnuje dobu přesunu čtecí/zapisovací hlavy na stopu (seek time) a dobu otáčení plotny na sektor (latence). Přístupová doba disku se vždy udává jako průměr, protože doba vyhledávání a latence se liší v závislosti na aktuální poloze hlavy a plotny. [6]

5.2.4 Doba čekání

I když hlava „doletí" nad správnou stopu (je vystavena), nemůže ještě začít se čtením. Musí počkat, až se pod ní dotočí sektor, v němž se má se čtením dat začít. Doba čekání záleží na náhodě, ale jako technická hodnota
se uvažuje jedna polovina otáčky disku. [2]

Tabulka 1: Vliv otáček na přístupovou dobu

Otáčky	Doba jedné otáčky
3 600 ot/min	16,66 ms
3 800 ot/min	15,79 ms
4 000 ot/min	15,00 ms
4 200 ot/min	14,26 ms
4 500 ot/min	13,33 ms
4 900 ot/min	12,25 ms
5 400 ot/min	11,11 ms
7 200 ot/min	8,33 ms
10 000 ot/min	6,00 ms
15 000 ot/min	4,00 ms

Zdroj: Převzato z [2]

Z tabulky vyplývá, že doba čekání se snižuje se zvyšujícími se otáčkami disku. Zároveň mají otáčky přímou souvislost s produkcí tak vznikajícího nežádoucího tepla. Čím vyšší jsou otáčky disku, tím víc se disk zahřívá a při velmi vysokých otáčkách je nutné využít přídavný chladič. [2]

5.2.5 Paměť cache

Stejně jako mikroprocesory, i pevné disky využívají paměť cache. Do této paměti se načítají data z disku a odtud se následně přenášejí na sběrnici. Využití vyrovnávací paměti výrazně zrychluje práci pevného disku. [2] Velikost vyrovnávací paměti v dnešních discích se pohybuje od 16MB do 512MB. Obecně platí, že čím víc paměti, tím lépe.

5.2.6 Kapacita disku

Kapacita je nejdůležitějším kritériem disku. Velikost disku byla dříve řádově v desítkách MB, dnešní disky již standardně disponují kapacitou v jednotkách až desítkách TB.

Kapacitu disku lze snadno spočítat podle následujícího vzorce:

Kapacita = počet cylindrů * počet hlaviček * počet sektorů na stopu * počet bajtů na sektor

Při výpočtu kapacity je vhodné použít přepočet 1KB = 1024B a nikoliv 1KB = 1000B, jak nesprávně používají někteří výrobci. Díky tomu je velmi obtížné porovnat kapacity jednotlivých disků, protože nelze určit, jaký přepočet mezi jednotkami byl použit. [3]

5.2.7 Hustota záznamu

Každý bit je reprezentován miniaturním dipólem zapsaným do magnetického povrchu. Cílem je tedy miniaturizovat dipóly a vytvářet stále jemnější magnetické struktury s možností vyšší hustoty zápisu dat. Dříve používaná technologie, kdy se na povrch kotoučů nanášela vrstva oxidů, byla nahrazena vrstvou tenkého filmu z magnetického materiálu. Dokonalejší povrch filmu umožňuje menší výšku letu hlavy nad diskem, což znamená potřebu menšího magnetického pole. To dovoluje použití menších dipólů a větší hustotu stop. [2]

5.2.8 Kódování dat

Při čtení se dipóly pohybují pod magnetickou hlavou, což v ní vyvolává elektrické napětí. Podle induktivního zákona je napětí vyvoláno jen změnami magnetického toku. Pokud ovšem následuje několik stejných bitů, například 1000111, hned po sobě, stojí řadič před problémem, jak od sebe jednotlivé bity oddělit. Každý bit by se dal oddělit speciálním impulsem, tím by ale výrazně vzrostl počet dipólů potřebných k zápisu jednoho bajtu a tím by klesla i kapacita disku. Proto se používají speciální algoritmy úspornějšího zápisu na disk. [2]

Nejstarší metoda, která se používala v prvních typech disků je Frequency Modulation (FM). Tato metoda funguje na principu, kdy je za každý bit přidána

rozlišovací značka. [7] Modified Frequency Modulation (MFM) vychází z předchozí metody a vymezuje datovému signálu přesnou délku. Podle času trvání stejného magnetického toku řadič rozpozná počet shodných bitů. Dříve byla tato metoda využívána hlavně u disket. Další často používanou metodou je Run Length Limited (RLL). Řadič si přepočítá ukládanou posloupnost na novou kombinaci 0 a 1. Ukládané číslo je přeměněno tak, že se v něm nevyskytnou „nečitelné" sledy 0 a 1. V porovnání s MFM potřebuje RLL pro uložení stejné informace jen asi jednu třetinu kapacity disku. Další zvýšení kapacity pak přináší metoda Partial Response Maximum Likelihood (PRML). Čtené impulsy se zpracovávají digitálním signálovým procesorem - DSP. Ten přesně ví, jak má vypadat sled signálů vyvolaný hustě ležícími dipóly, dokonce dokáže dopočítat i chybějící údaj. Výsledné resumé je jasné - PRML rozezná více dipólů na malé ploše, což vede ke zvýšení kapacity disku. [2]

5.2.9 Prekompenzace

Při pohledu na geometrii disku je zřejmé, že vnější stopy jsou delší než vnitřní stopy. Sektor stopy 0, první vnější stopy, je delší, než sektor poslední stopy ležící u středu, přesto nesou stejné množství dat. [2]

Díky větší hustotě dipólů blíže středu se zvyšuje pravděpodobnost magnetické interakce. Dipóly, v nichž jsou data uložena, jsou v podstatě malými magnety, které mají jako každý jiný magnet své póly, severní a jižní. Stejné póly se odpuzují, opačné přitahují. Na vnitřních stopách, kde jsou tyto „magnety" blízko u sebe, hrozí nebezpečí, že při jisté kombinaci kladných a záporných impulsů, např. 1100..., mohou v důsledku přitažlivých a odpudivých sil „vniknout" bity (magnety) do sebe, čímž se informace naruší a data budou nečitelná. [2]

Pro omezení tohoto efektu je nutné předkompenzovat zápis určitých bitů v bitových jednotkách, aby byly na disk zapsány o něco dříve nebo o něco později. Nejvzdálenější číslo válce, od kterého se má tato úprava časování použít, se označuje jako počáteční válec předkompenzování zápisu. [8]

5.2.10 Zone bit recording

Zone bit recording (ZBR) úzce souvisí s problémem popsaným v kapitole 4.1.9. Díky této funkci je povrch disku rozdělen do několika zón. Nejméně sektorů se nachází blíže ke středu disku, naopak nejvíce sektorů je ve vnější oblasti. Hustota záznamu zůstává na celém disku přibližně stejná. Při použití této metody se kapacita disku zvýší asi o 30 procent, zároveň se pak odlehčí přenos dat z vnitřní části kotouče. Zároveň se však při použití této metody zvyšují požadavky na elektroniku disku, protože se elektronika, zajišťující čtení a zápis dat musí nastavit v každé zóně jinak. [3]

5.2.11 Střední doba mezi chybami

Střední doba mezi chybami je jedním z parametrů poruchovosti disku. Je to odhadovaná doba, za kterou dojde k poruše zařízení. V závislosti na tom, která společnost vyrábí produkt, existuje několik různých způsobů výpočtu. Ve své podstatě je výpočet jednoduchým procesem analýzy doby provozu pevného disku, SSD nebo jiného produktu a zprůměrování této doby s počtem selhání. Tím lze získat střední dobu mezi poruchami. [9]

Střední doba mezi chybami je jistě důležitým indikátorem spolehlivosti, ale je nutné si uvědomit její statistickou podstatu. Pokud bychom měli hodnotu tohoto parametru 117 let, není zaručeno, že se disk 117 let nerozbije. Může se rozbít v prvním měsíci provozu, ale pak se s velkou pravděpodobností porouchá až za 117 let. [2]

5.2.12 SMART

SMART je zkratka anglického Self Monitoring And Reporting Technology a ve volném překladu by název mohl znít: technologie monitorující a posuzující stav disku. SMART má za úkol detekovat a zaznamenávat veškeré anomálie a chyby v práci disku a z nich vyvozovat nejen kondici disku, ale i předpovídat, kdy může dojít k jeho selhání. [10]

Řadič disku, který vlastnosti disku sleduje, uloží zprávu o pravděpodobném vzniku chyby do paměti EEPROM. Odtud údaje přečte a vyhodnotí speciální software. V tabulce SMART jsou výrobcem uložené mezní hodnoty a stropní či aktuální

hodnoty jednotlivých ukazatelů. Doplňkovými informacemi jsou počet startů disku, doba provozu disku, aktuální teplota apod. V široké škále hodnot SMART se sledují drobné chyby funkčnosti pevného disku. Jde o chyby opravené ECC korekcí, nutné relokace chybných bloků, chyby polohování hlaviček a podobně. Většiny chyb si uživatel vůbec nevšimne, ale jejich nadměrný výskyt znamená, že pevný disk je na pokraji zhroucení. [2]

Tabulka 2: Příklady atributů SMART

Atribut	ID	Popis
Raw Read Error Rate	1	Počet chyb čtení včetně korigovaných (ty jsou v průběhu činnosti HDD běžné). Aktuální hodnota by neměla klesnout pod prahovou hodnotu.
Spin Up Time	3	Čas potřebný k roztočení ploten. Rozhodující není samotný čas, ale to, zda se tato doba neprodlužuje.
Start/Stop Count	4	Počet start/stop cyklů jednotky.
Reallocated Sector Count	5	Označuje množství vadných sektorů přemapovaných do záložní části disku. Hodnota 100 značí, že k dispozici je 100 % záložních sektorů (nedošlo tedy k žádnému přemapování). Práh je 36 %.
Seek Error Rate	7	Indikuje počet nepřesností v pozicování hlaviček na danou stopu. Aktuální hodnota by neměla klesnout pod prahovou hodnotu.
Power On Hours Count	9	Měří, kolik hodin provozu má disk za sebou.
Spin Retry Count	OA	Počet případů kdy se plotny neroztočily po inicializaci disku.
Power Cycle Count	OC	Počet zapnutí disku.
Drive Temperature	C2	Aktuální teplota disku (°C). Vysoká interní teplota společně s mechanickými otřesy a vibracemi zkracuje životnost disku ze všeho nejvíce.
Current Pending Sector	C5	Počet podezřelých sektorů.
Uncorrectable Sector	C6	Neopravitelné sektory
Ultra ATACRC Error Rate	C7	Chyby přenosu rozhraní Ultra ATA

Write Error Rate	C8	Počet chyb při zápisu dat

Zdroj: Převzato z [2]

Sledované atributy mají pro spolehlivost disku různý význam. Některé atributy mají doplňující údaj T.E.C. (Threshold Exceeded Condition). Ten se snaží předpovědět datum, kdy by mohlo dojít k překročení prahové meze. Hodnota T.E.C, je prognózou selhání disku a jako každá prognóza není úplně stoprocentní. V každém případě nás však upozorní na možné problémy s diskem. [2]

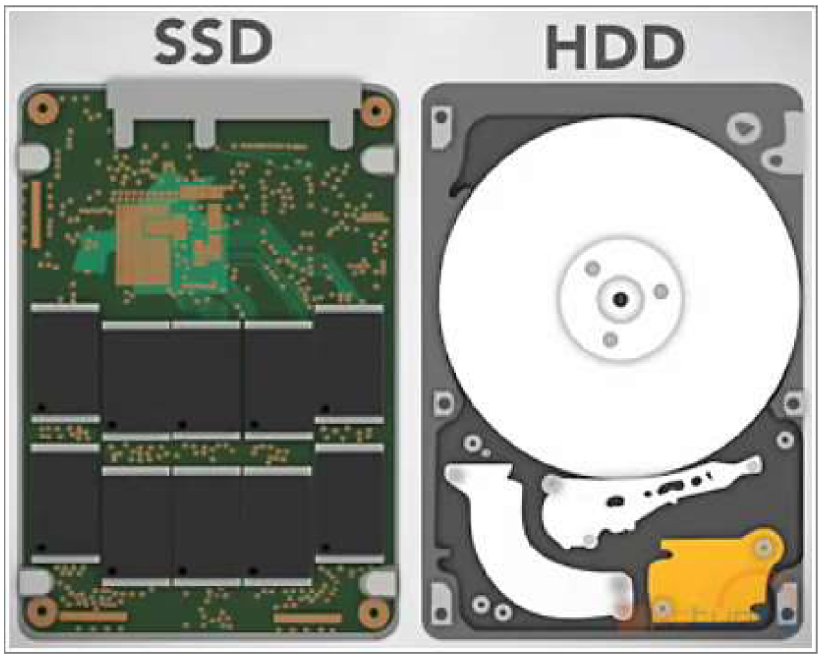
5.3 Solid state drive

Solid state drive, neboli SSD, je typ úložného zařízení, které ukládá trvalá data do polovodičové flash paměti. SSD plní stejnou funkci jako mechanické disky, v porovnání s nimi jsou však rychlejší. [49]

SSD nemá narozdíl od mechanických disků žádné pohyblivé části. Klíčovými částmi jsou řadič a paměťové čipy. Tato konfigurace je aby poskytovala vysoký výkon čtení a zápisu. [49]

5.4 Fyzická struktura SSD

Průměrná přístupová doba disků rotujících 7 200 otáčkami za minutu se pohybuje mezi 10-12 ms. Doba jde zkrátit zvýšením rychlosti otáčení na 10 000 nebo 15 000 otáček. Nevýhodou je mnohem vyšší hlučnost, ale také vyšší náročnost provedení, která je vykoupena vyšší cenou. A přes to všechno není možné snížit přístup na zanedbatelnou hodnotu, pouze na nějakých 5 ms. [11]

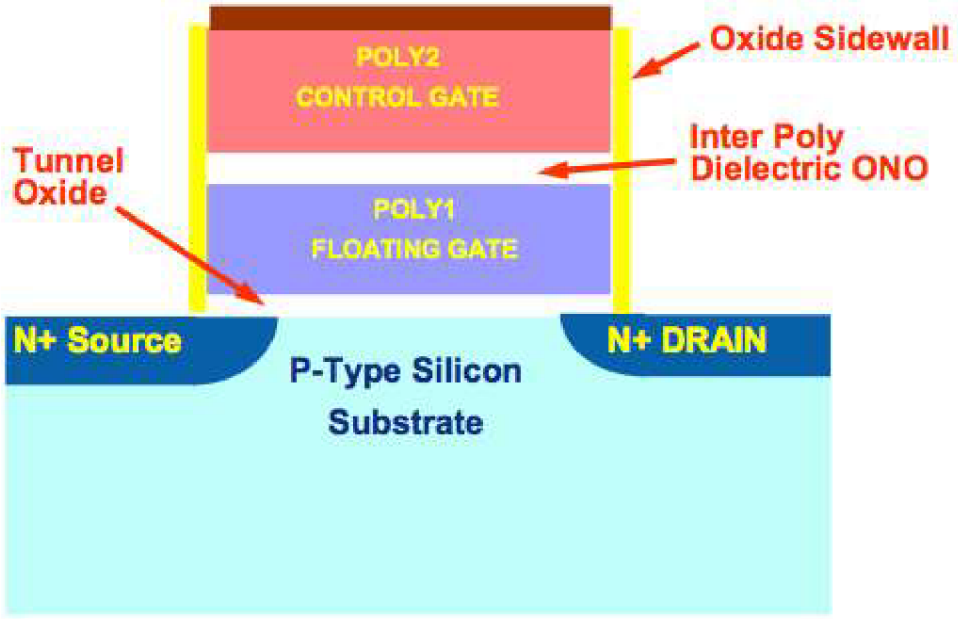


Obrázek 4: Porovnání struktury SSD a HDD (převzato z [11])

Mnohem lepší je však aplikovat Random Access Memory, což znamená paměť s přístupem na libovolné místo v paměti ve stejný čas, i do problematiky pevných disků. Nejlepší cestou se staly NAND flash paměti. Rychlost zápisu se původně pohybovala okolo 10 MB/s, v roce 2006 se ale na trh dostal první komerční disk na bázi NAND flash čipu s rychlostí sekvenčního čtení 53 MB/s a rychlostí zápisu 28 MB/s. [11]

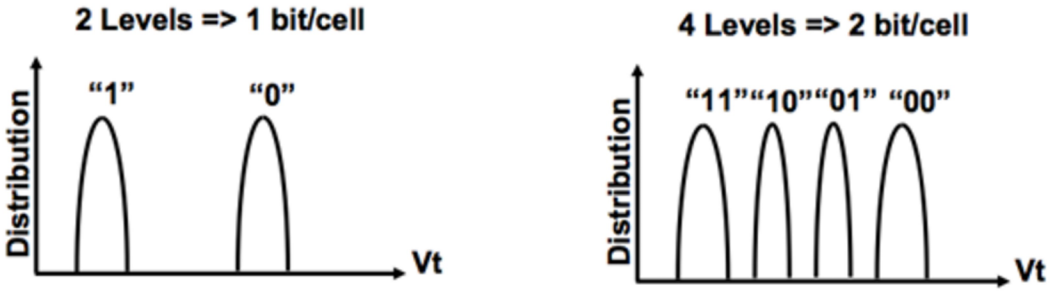
5.4.1 Počet přepisů

Jedním z nedostatků je omezený počet zápisů do buňky uvnitř jednotlivých čipů. Buňky se skládají z MOS tranzistorů s plovoucími hradly a jsou vzájemně odděleny vrstvou nevodivého oxidu. Při změně jednotlivých napěťových úrovní, kterým odpovídají logická 1 nebo logická 0, dochází k opotřebení materiálu a změně vodivosti. S tím je spojen posun napěťové logické úrovně, kterou řídící elektronika chápe jako logickou 0 nebo 1. [11]

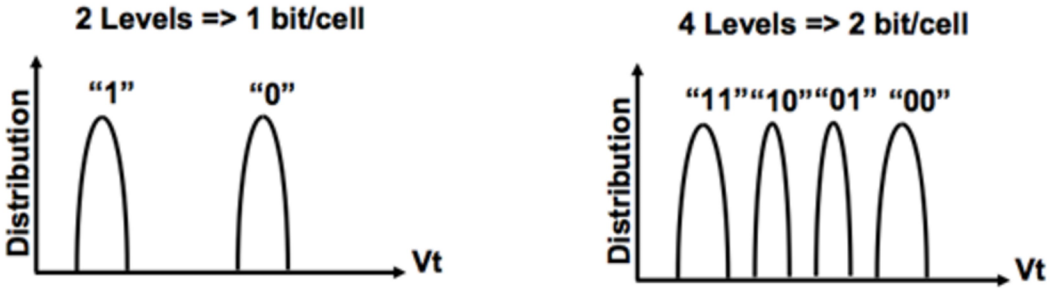


Obrázek 5: Průřez Single Level Cell buňkou (převzato z [12])

Jedna buňka NAND flash paměti může ukládat buďto jeden, nebo 2 bity. Pokud uchovává pouze jeden bit, nazýváme ji Single Level Cell, zkráceně SLC. Pokud uchovává 2 bity, nazývá se Multi Level Cell, zkráceně MLC. Oba typy jsou fyzicky vyrobeny stejným způsobem a neexistuje nic, co by SLC a MLC odlišovalo. Rozdíl mezi těmito buňkami je jen v tom, jak jsou v nich data uložena a čtena. [12]



Obrázek 6: Porovnání SLC (vlevo) a MLC (vpravo) (převzato z [12])



Obrázek 7: Porovnání SLC (vlevo) a MLC (vpravo) (převzato z [12])

Aby se předcházelo nadměrnému opotřebení, obsahují moderní SSD disky algoritmy pro automatickou správu paměti, takzvaný Garbage collection. S využitím dostatečně velké vyrovnávací paměti je možné provádět Write amplification, wear leveling nebo automatický příkaz trim. [11]

5.4.2 Write amplification

Pokud se řadič snaží zapsat určité množství dat, může díky velkému množství reorganizace, kterou je třeba provést nakonec zapsat více dat, než bylo původně plánováno. Poměr toho, kolik dat je zapsáno a kolik bylo potřeba zapsat, se nazývá write amplification. Toto číslo by mělo být v ideální případě 1, v závislosti na kvalitě SSD, ale může se pohybovat až v řádu nižších desítek. [13]

Write amplification je způsoben nedokonalostí souborového systému. Disk umí data zapisovat po celých stránkách, kde stránka má velikost 512kB a pokud dostane k dispozici méně dat, stránku obsadí a vznikne nevyužitý prostor. Díky využití kompresních algoritmů, cache paměti a optimalizacím zapisují moderní disky do buněk nepatrně více dat, než jim odeslal systém. Nejlepší poměry se pohybují od 1,1 do 0,5. [11]

$$\frac{data\ zapsaná\ do\ paměti}{původní\ velikost\ dat} = write\ amplification$$

Obrázek 8: Výpočet hodnoty write amplification

5.4.3 Wear leveling

Wear leveling umožňuje rozložit zápis dat mezi jednotlivé buňky a tím zajišťuje jejich rovnoměrné opotřebení. Jedná se o algoritmus, pomocí kterého řadič přemapovává logické adresy bloků na různé fyzické adresy. [14]

U wear levelingu rozlišujeme dva druhy. Dynamický střídá zápis pouze u neobsazeného prostoru, statický počítá celkový zápis do všech buněk a přesouvá na disku všechna data. [11]

5.4.4 Příkaz trim

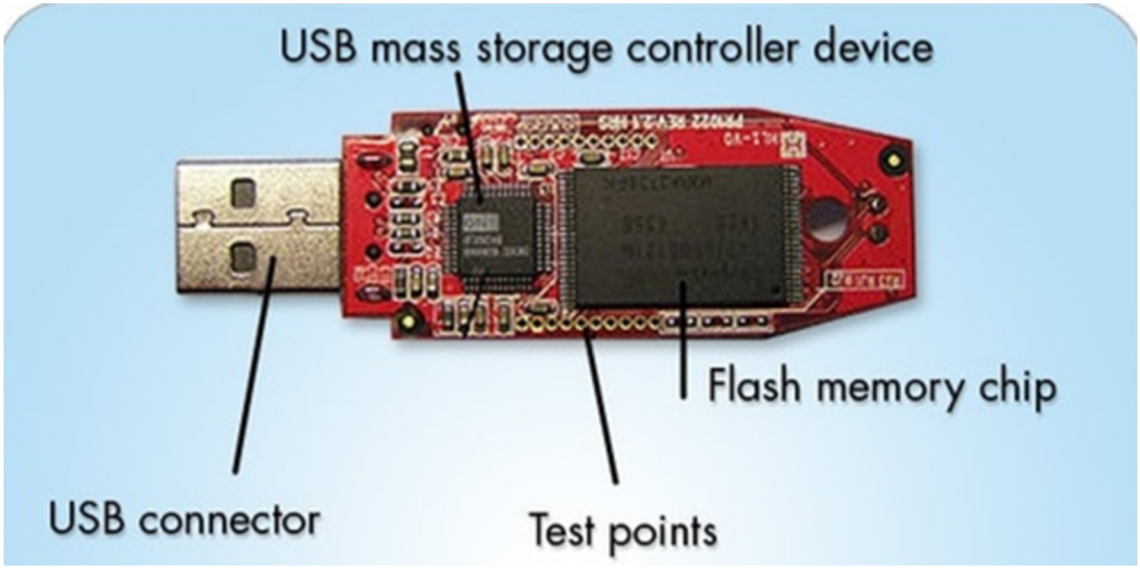
Při mazání dat z SSD nedojde k fyzickému smazání dat, ale řadič uloží do tabulky informaci o tom, že oblast byla smazaná. Data však v buňce zůstávají a tak při dalším zápisu musí řadič buňku smazat. Tím dochází ke zpomalení zápisu. Pokud je disk nečinný, příkaz trim prochází všechny buňky z tabulky, které jsou označeny jako smazané a nuluje je.

5.4.5 Ostatní typy flash pamětí

Existuje několik druhů pamětí flash, které se liší velikostí a uspořádáním paměťových buněk, a také stavbou vnitřní struktury. Používané typy pamětí se označují jako NAND, AND, NOR a DINOR. Struktura paměťové buňky NAND a AND je menší než struktura buňky NOR, která také vyžaduje vyšší proud a napětí při programování. Paměť typu NOR je ale při přístupu do náhodné oblasti paměti rychlejší. Náklady na 1MB paměti u typu NAND je nižší než u paměti v provedení NOR. [3]

Tento typ paměti využívají například flash disky. Jedná se o spolehlivá, robustní zařízení, která jsou odolná vůči vibracím a otřesům. Pro ukládání dat nejsou použity žádné mechanické součásti a jsou odolná i vůči působení magnetického

pole a jeho výkyvům. Kapacita flash disků se dnes může pohybovat až v jednotkách TB. [3]



Obrázek 9: Vnitřní struktura flash disku (převzato z [22])

Pro ukládání a přenos dat v digitálních fotoaparátech nebo mobilních telefonech se používají paměťové flash karty. Princip ukládání je zde stejný jako u ostatních zařízení využívající technologii flash, jednotlivá zařízení a jejich rozhraní se od sebe však významně liší. [3]

Existuje několik standardů paměťových karet, k nejrozšířenějším patří typy SD, Micro SD a Micro SDHC či SHXC, což jsou moderní typy SD karet, které umožňují uložení většího množství dat a rychlejší datové přenosy. [23]

5.5 Logická struktura disku

Pomocí vysokoúrovňového formátování se vytváří logická struktura disku. Tato struktura slouží primárně k organizaci dat na disku a umožňuje fyzický disk rozdělit na více oddílů. Informace o oddílech a organizaci dat jsou uloženy v tabulkách, které tvoří souborový systém. [3]

5.5.1 Souborový systém

Souborový systém je pojem pro organizaci a hierarchické řazení dat do souborové a adresářové formy. Je založen na binární soustavě a ukazuje, kde jsou data fyzicky zapsána. Souborový systém lze najít kromě pevných disků také na optických

discích, jako jsou CD a DVD. Jeho primárním účelem je snadná přístupnost a orientace, čtení a ukládání dat, která jsou pro uživatele reprezentována právě ve formě adresářové struktury a souborových složek. [15]

Souborový systém zaznamenává informace o uložených datech. Těmto informacím říkáme metadata a mohou obsahovat například velikost souboru, čas poslední změny, vlastníka souboru nebo oprávnění uživatelů. [15]

Existuje několik souborových systémů, které určují, jakým způsobem jsou data na disku zpracovávána. Od použitého souborového systému se odvíjí i způsob vytváření oddílů a formátování. Mezi nejpoužívanější můžeme zařadit FAT, exFAT, NTFS a EXT2/3/4. [3]

5.5.2 File Allocation Table

File Allocation Table, neboli FAT, existuje ve dvou variantách a to FAT16 a FAT32. FAT16 mezi nejstarší souborové systémy pro operační systémy MS-DOS a Windows. Základní stavební jednotkou je cluster, který se skládá z několika sousedních sektorů, jejichž velikost je 512 bajtů. Pracuje se 16 bitovým adresováním, takže maximální počet sektorů, které může spravovat je 65 536. Při velikosti clusteru 2 KB je pak maximální velikost oddílu 128MB. [3]

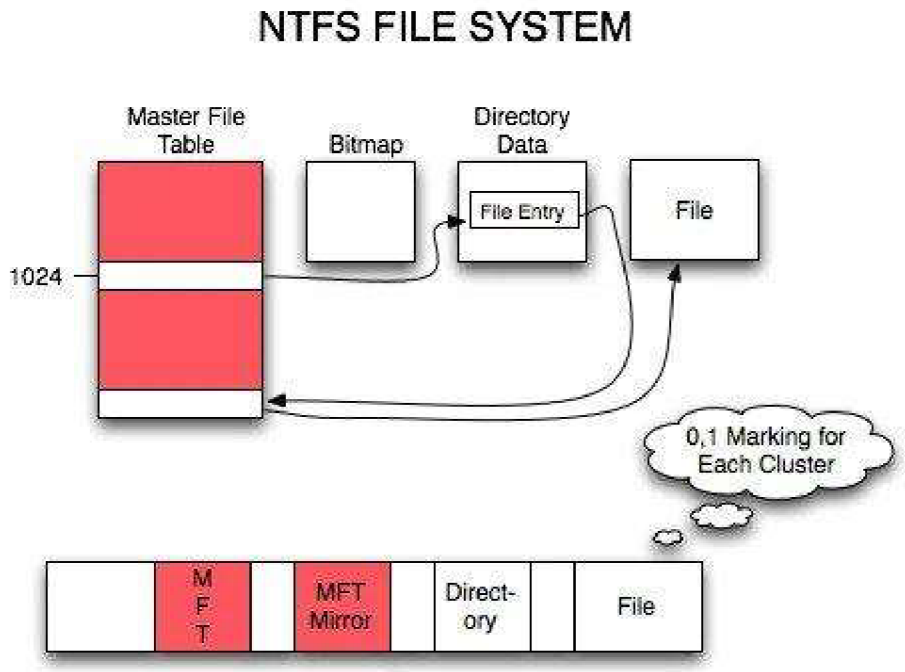
Se zvyšující se velikostí disku je potřeba zvětšovat i velikost clusteru a to až do maximální velikosti 32 KB. Maximální velikost diskového oddílu tak bude mít 2 GB. Vzhledem k tomu, že cluster je nejmenší jednotkou, i soubor o velikosti jednoho bajtu obsadí na disku prostor o velikosti jednoho clusteru. [3]

U formátu souborů FAT32 je maximální hranice diskového oddílu posunuta až na 2 TB, což odpovídá 2048 GB. Při posuzování velikosti využitého místa se ale velikosti clusterů zmenšují, takže vyplýtvaného místa je je méně, než u formátu FAT16. [3]

5.5.3 New Technology File System

New technology File System, pro který se používá zkratka NTFS, nabízí proti FAT vysokou úroveň spolehlivosti a zabezpečení. Každá změna v systému souborů je zapsána do speciálního souboru, ve kterém jsou uloženy údaje o všech správně provedených transakcích. Při výskytu chyby se po restartu provede kontrola

systému souborů CHKDSK a data v nekonzistentním stavu jsou opravena. V případě, že poškozená data nejdou opravit, nedojde vůbec k jejich načtení.[3]
Další komponentou je Master File table, v níž je uložen záznam o minimální velikosti 2 KB pro každý soubor uložený na disku. Operační systém pak vytváří několik kopií tohoto souboru. Toto zabezpečení však zabírá místo na pevném disku. [3]



Obrázek 10: Reprezentace NTFS (převzato z [16])

NTFS také uspořádává data do clusterů, jejichž velikosti jsou 512, 1024, 2048 či 4096 KB. Velikost clusteru se dá nastavit při formátování disku podle potřeby. Standardně se využívá dynamická velikost, která vychází z kapacity pevného disku. [3]
V novějších systémech pak lze použít diskové kvóty pro uživatele nebo skupiny. Další změnou je Mount Points, díky nimž je možné přiřazovat diskovým jednotkám různé svazky. Je zde také možnost šifrování, kterým lze data uživatelů chránit pomocí certifikátů. Od verze systému Windows Vista je implementována funkce pro provádění transakcí. Změny v souborech, jako je například přejmenování nebo odstranění, se provedou až po úspěšném provedení celé transakce. Tímto způsobem se dá zabránit vzniku neúplných či poškozených souborů. [3]

5.5.4 Extended File Allocation System

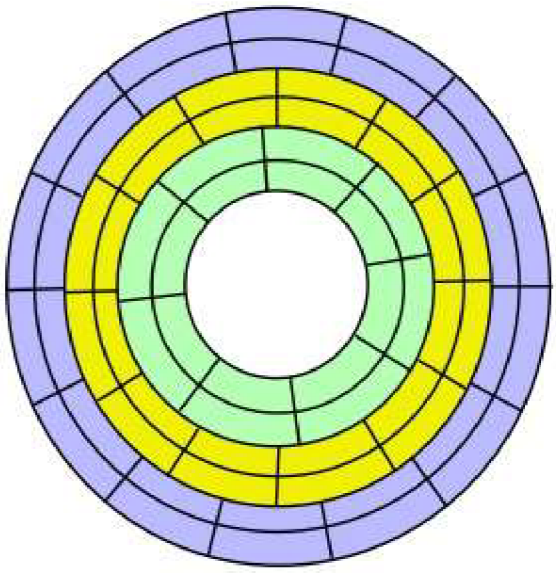
Extended File Allocation System neboli exFAT je vhodný souborový systém pro SD karty, flash disky a SSD. Proti FAT32 se velikost souboru zvětšila ze 4 GB až na 16 EB, což se rovná 16 miliardám GB. Jelikož některé šifrovací nástroje vytvářejí rozsáhlé soubory, usnadňuje exFAT šifrování na USB discích a SSD. [17]

Limit na počet souborů v adresáři, který byl přítomen u FAT16 je zde také zrušen. Celkový počet souborů v adresáři je tedy omezen pouze volným místem na paměťovém médiu. Velikost clusteru je u exFAT maximálně 32 MB, což výrazně zrychluje propustnost dat při práci s flash pamětí. [17]

Souborový systém exFAT také zajišťuje větší přenosovou rychlost. K tomu je využita funkce Free Space Bitmap, kde sysexFAT indexuje nejen použité clustery, ale i ty volné. Při přenášení souboru na paměťové médium tedy systém přesně ví, kde je dostupné volné místo. [17]

5.5.5 Zone Bit Recording

U pevných disků se na každou stopu ukládá stejně velké množství dat. To znamená, že počet sektorů na jednu stopu je stejný jak uvnitř kotouče, tak na okraji. Maximální počet sektorů ve stopě tedy definuje nejkratší stopa, která se nachází na vnitřní straně kotouče. Díky tomu zbývá na středních a vnějších stopách mnoho místa. [3]



Obrázek 11: Vizualizace Zone Bit Recording (převzato z [21])

Funkce Zone Bit Recording rozdělí povrch pevného disku do několika zón. Nejméně sektorů na stopu se vytvoří uvnitř disku, nejvíce sektorů naopak ve vnější oblasti. Díky tomu zůstává hustota záznamu na celém disku přibližně stejná. Při použití této metody se kapacita disku může zvýšit až o 30 procent. Vzrůstají však požadavky na elektroniku disku, protože se elektronika, zajišťující čtení a zápis, musí nastavit v každé zóně jinak. [3]

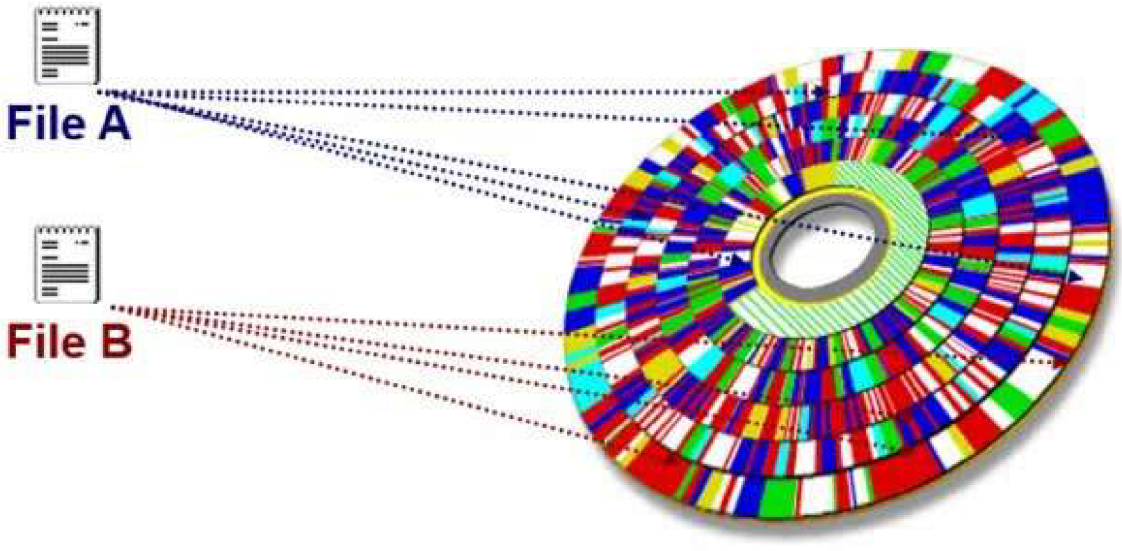
5.5.6 Master Boot Record

Master Boot Record, dále jen MBR, je informace v prvním sektoru pevného disku. Určuje, jak a kde je umístěn operační systém, aby mohl být zaveden do hlavního úložiště nebo paměti RAM. MBR obsahuje programy, které určují, jaký oddíl bude použit pro spuštění systému. Bez toho není možné systém spustit. [18]

MBR má velikost 512 bajtů. Jeho první sektor má specifickou adresu, Cylindr 0, Head 0 a Sektor 1. MBR se vytváří v systémech MS Windows při rozdělení pevného disku na oddíly. Není však umístěn v rámci oddílu, proto paměťové média bez oddílu, neobsahují MBR. MBR může fungovat jako řetězový zavaděč nezávisle na operačním systému [18]

5.5.7 Fragmentace disku

Fragmentace je důsledkem nespojitého ukládání, kdy různé části aplikace nebo souboru nejsou v úložném zařízení uloženy v sadě bloků jdoucích po sobě. Fragmentace disku se v průběhu času obvykle zvyšuje, protože v operačním systému neustále probíhají operace čtení a zápisu. Jelikož jsou soubory neustále přidávány a odebírány, zůstávají v úložišti nesouvislé bloky. [19]



Obrázek 12: Fragmentace disku (převzato z [20])

Důsledkem fragmentace se prodlužuje doba čtení z disku, protože je třeba najít různá místa, kde se daný soubor nachází. Operace zápisu je naopak rychlejší, protože systém může soubor zapsat na libovolný dostupný blok uložiště. [19]

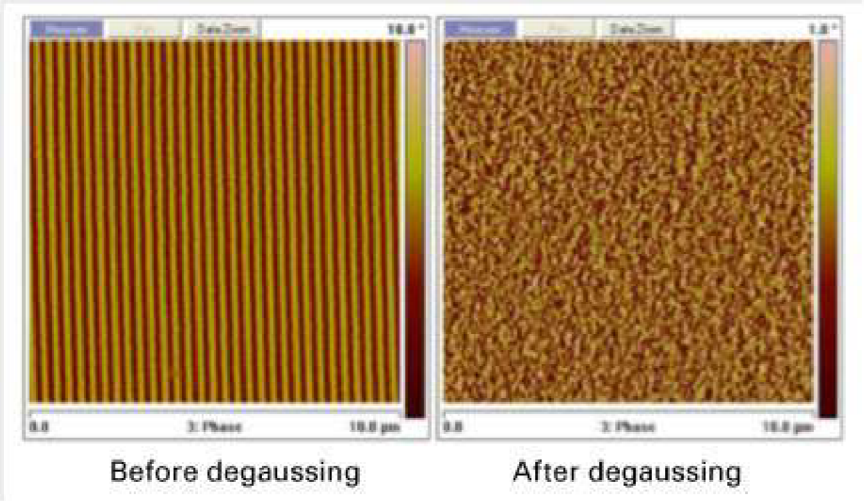
5.6 Likvidace dat

Likvidace dat je proces, při němž jsou data uložena na pevných discích nebo jiných datových médiích zničena tak, aby byla zcela nečitelná a nebylo možné k nim získat přístup. Po smazání nejsou data již přístupná operačnímu systému nebo aplikaci. K vymazání souboru je nutné přepisovat bloky náhodnými znaky, dokud nejsou data považována za nevratná. [24]

Data na magnetických paměťových médiích lze zničit pomocí degaussingu, což je změna magnetického pole. Další metodou likvidace dat je fyzické zničení datového nosiče, například skartováním nebo roztavením. [24]

5.6.1 Fyzická likvidace

Pokud je zařízení fyzicky zlikvidováno, stává se zcela nepoužitelným. Tento proces může obecně zahrnovat skartování pevných disků, mobilních telefonů a dalších paměťových médií na malé kousky pomocí velkých mechanických skartovaček. Fyzická likvidace může také zahrnovat změnu uspořádání magnetického pole na pevném disku HDD pomocí degausserů. [25]



Obrázek 13: Pevný disk před a po degaussingu (převzato z [26])

To, že bylo zařízení zničeno však nezaručuje, že se zničila i všechna data. Při demagnetizaci HDD je potřeba dodržet správné postupy a magnetické pole musí být dostatečně silné. Pokud je degaussing aplikován na nemagnetické disky, například SSD, data nejsou vůbec ovlivněna. [25]

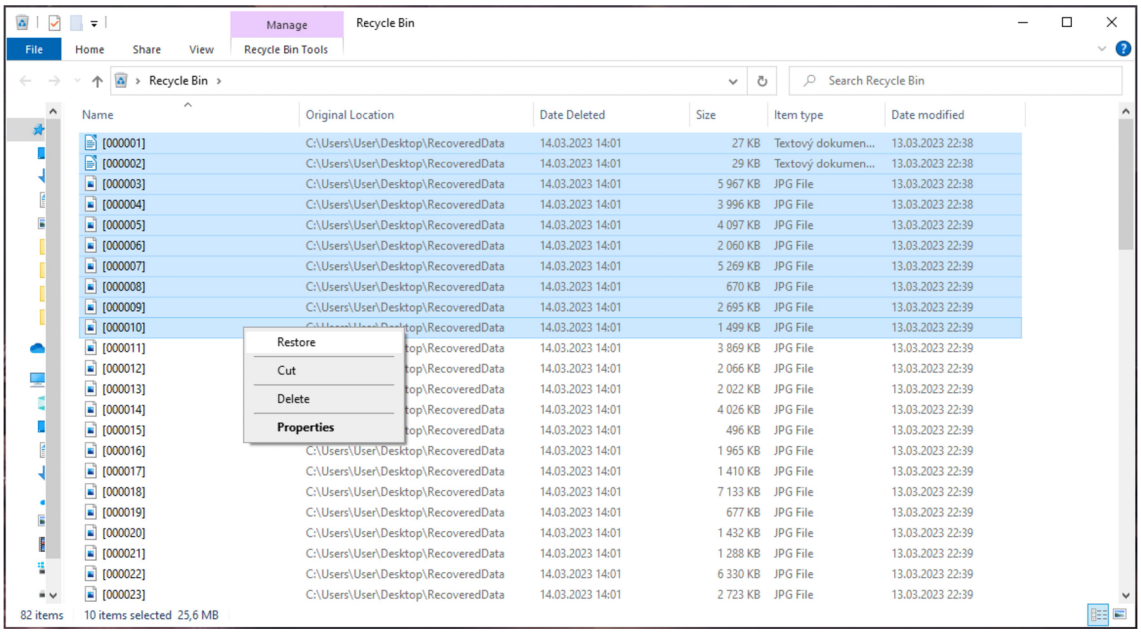
Skartování SSD pomocí skartovačky také nedokáže zaručit kompletní zničení dat. Běžné velikosti skartovacích strojů nedokáží úplně zničit paměťové čipy na SSD s vysokou hustotou, které mohou vyžadovat skartování na pouhé 2 milimetry. [27]

Další metodou likvidace pevných disků je jejich tavení. To spočívá v tom, že se disk ponoří do kyseliny, čímž se zcela zničí. Jedná se o jednu z nejúčinnějších metod zničení pevného disku, je ale také jedna z nejnebezpečnějších. Důvodem je použití kyseliny chlorovodíkové a dusičné, které jsou nebezpečné pro životní prostředí. Zároveň mají velmi špatný vliv na lidský organismus a je nutné použít vhodné ochranné pomůcky. [28]

5.6.2 Odstranění souboru

Pokud je soubor v operačním systému Windows smazaný, odstraní se z místa, kde je uložen. Pokud je tím místem pevný disk, je soubor přesunut do koše. Pokud je uložen na externím médiu, jako je flash disk, CD nebo síťové umístění, je soubor vymazán. [42]

Koš je v systému Windows složka nebo adresář, kam se dočasně ukládají smazané položky. Pokud nejsou soubory příliš velké, jsou po odstranění přesunuty do koše. Soubory v koši lze obnovit do původního umístění. Soubory v koši nelze používat. [43]



Obrázek 14: Reprezentace koše v prostředí Windows 10

Soubor nelze vymazat, pokud jej využívá jiný uživatel nebo proces. Pro smazání musí být soubor uzavřen a pokud se jedná o sdílený soubor, musí být odhlášen. [42]

Další možností je odstranění souboru pomocí příkazového řádku. Smazání souboru v příkazovém řádku odstraní možnost indexování, což způsobí, že soubor bude pro operační systém neviditelný. Při tomto způsobu odstranění nebude přítomen v koši, nebude ho tedy možné obnovit do původního umístění. [46]

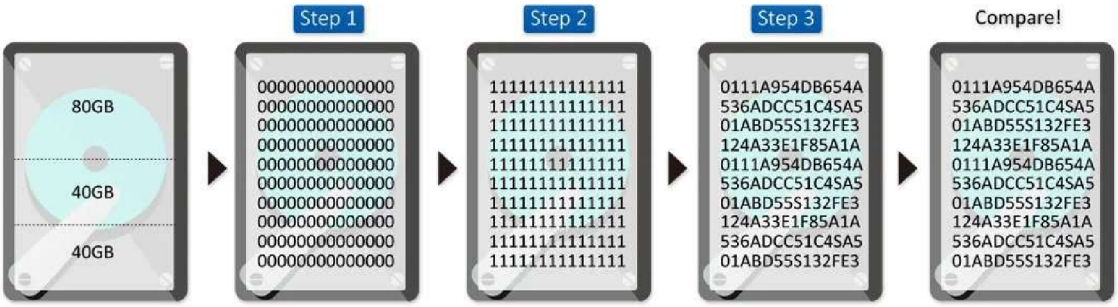
Pro smazání souboru je nutné pomocí příkazu cd otevřít složku, ve které jsou data uložena. Syntaxe pro smazání souboru je pak del "filename". Pro smazání souboru textovy_soubor.txt je tedy potřeba napsat příkaz del "textovy_soubor.txt". [46]
Pokud je soubor označen pouze pro čtení, při pokusu o smazání dojde k chybě. Smazání souboru však lze vynutit pomocí příkazu del /f "textovy_soubor.txt". [46]

5.6.3 Formátování disku

Formátování je proces, který vymaže všechna data na jednotce a nastaví nový souborový systém, který umožní operačnímu systému číst a zapisovat nová data.
Formátování disku se obvykle provádí za účelem přípravy nové jednotky na její první použití a připravuje dostupný prostor pro instalaci operačního systému. Při formátování disku lze provést změnu souborového systému. [44]
Formátování disku ale neodstraní všechna uložená data. Formátování není totéž jako bezpečná likvidace dat. Při formátování se pouze odstraní index, který umožňuje přístup k datům. Tyto indexy jsou uloženy v tabulce, která je formátováním odstraněna. [45]

5.6.4 Metoda DoD 5220.22-M

Algoritmus byl vyvinut bezpečnostní službou obrany jako řešení pro bezpečnou sanitaci dat. Jedná se o jeden z nejrozšířenějších a nejbezpečnějších standardů pro mazání dat a je implementován ve třech nebo sedmi průchodech s různou frekvencí ověřování. [29]
Tento algoritmus lze najít v několika verzích. Verze DoD 5220.22-M (ECE) přepíše data sedmkrát, verze DoD 5220.22-M (E) třikrát a verze DoD 5220.28-M -STD také sedmkrát. Rozdíl mezi nimi spočívá v tom, že každá verze používá různou frekvenci ověřování počtu průchodů. Pokud algoritmus provede pouze tři průchody, v prvním se zapíší a ověří nuly. V druhém průchodu pak jedničky a poslední průchod zapíše pseudonáhodná čísla. [29]



Obrázek 15: Vizualizace algoritmu DoD 5220.22-M (převzato z [30])

Při sedmi průchodech je dvakrát spuštěn DoD 5220.22-M a mezi nimi jednou proběhne DoD 5220.22-M (C) Standard. [29] Většina softwaru pro zničení dat tuto metodiku obsahuje.

5.6.5 Metoda AR 380-19

Tato metoda mazání dat je definována a zveřejněna armádou USA v armádním předpisu 380-19. Tento algoritmus přepisuje data ve třech průchodech. První průchod zapíše náhodný znak. Druhý průchod zapíše specifický znak, například jedničku, a následně třetí průchod zapíše doplněk tohoto znaku a ověří přepsání. [29]

5.6.6 Metoda AFSSI-5020

Metoda byla definována letectvem Spojených států amerických v předpisu Air Force System Security Instruction 5020. Stejně jako v metodě DoD 5220.22-M i zde je nejprve cílová oblast přepsána konstantní hodnotou nula a následně jedničkou. Poslední průchod zapisuje pseudonáhodné číslo. [29]

5.6.7 Metoda RCMP TSSIT OPS-II

Algoritmus byl definován Královskou kanadskou jízdní policií. Používá průchodů doplňkových opakujících se hodnot a končí přepsáním pseudonáhodného znaku. Narozdíl od algoritmu DoD 5220.22-M, který po každém průchodu ověří přepis, je zde ověření pouze v sedmém průchodu. [29]

5.6.8 Metoda HMG IS5

Tento algoritmus lze najít ve dvou podobných verzích - HMG IS5 a HMG IS5 Enhanced. Základní algoritmus obsahuje pouze dva průchody, kdy při prvním průchodu zapíše nulu a při druhém pseudonáhodné číslo a ověří zápis. Enhanced verze algoritmu se skládá ze tří průchodů, kde v prvním zapíše nulu, ve druhém jedničku a ve třetím pseudonáhodné číslo a zápis ověří. Je tedy velmi podobná metodě DoD 5220.22-M, ověření ale probíhá až v posledním kroku. [31]

5.6.9 Gutmannova metoda

Základní princip spočívá v několikanásobném přepsání paměťového média určitou sekvencí dat. Originální metoda používá pro přepis dat 35 průchodů. V současné době je takovýto počet značně redundantní, proto se lze setkat s upravenou verzí označovanou jako Gutmann lite, která obsahuje pouze 10 průchodů. Jednotlivé sekvence průchodu jsou navrženy tak, aby eliminovaly zbytkový magnetismus z ploten disků a tím zabránily rekonstrukci dat. [32]

Tabulka 3: Gutmannova metoda

Průchod	Zapsaná hodnota binárně	Zapsaná hodnota hexadecimálně
1	Náhodné číslo	Náhodné číslo
2	Náhodné číslo	Náhodné číslo
3	Náhodné číslo	Náhodné číslo
4	Náhodné číslo	Náhodné číslo
5	01010101 01010101 01010101	555555
6	10101010 10101010 10101010	AAAAAA
7	10010010 01001001 00100100	924924
8	01001001 00100100 10010010	492492
9	00100100 10010010 01001001	249249
10	00000000 00000000 00000000	0
11	00010001 00010001 00010001	111111

12	00100010 00100010 00100010	222222
13	00110011 00110011 00110011	333333
14	01000100 01000100 01000100	444444
15	01010101 01010101 01010101	555555
16	01100110 01100110 01100110	666666
17	01110111 01110111 01110111	777777
18	10001000 10001000 10001000	888888
19	10011001 10011001 10011001	999999
20	10101010 10101010 10101010	AAAAAA
21	10111011 10111011 10111011	BBBBBB
22	11001100 11001100 11001100	CCCCCC
23	11011101 11011101 11011101	DDDDDD
24	11101110 11101110 11101110	EEEEEE
25	11111111 11111111 11111111	FFFFFF
26	10010010 01001001 00100100	924924
27	01001001 00100100 10010010	492492
28	00100100 10010010 01001001	249249
29	01101101 10110110 11011011	6DB6DB
30	10110110 11011011 01101101	B6DB6D
31	11011011 01101101 10110110	DB6DB6
32	Náhodné číslo	Náhodné číslo
33	Náhodné číslo	Náhodné číslo
34	Náhodné číslo	Náhodné číslo
35	Náhodné číslo	Náhodné číslo

Zdroj: vlastní zpracování

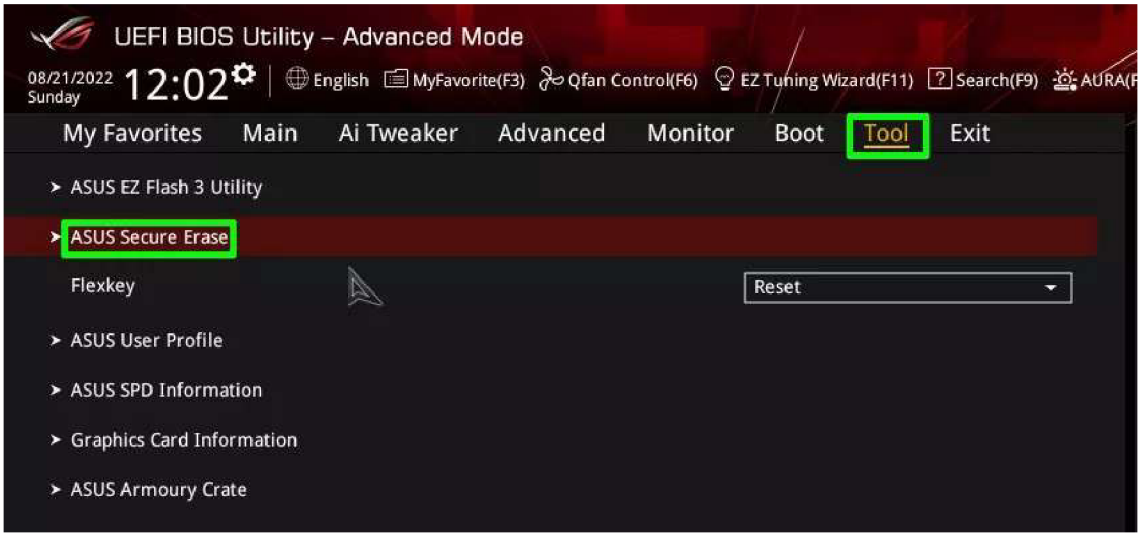
Náhodné číslo není dílem náhody, ale algoritmu, který zajišťuje, že se čísla nebudou po velmi dlouhou dobu opakovat. Tato pseudonáhodná čísla jsou

generována pomocí generátorů, které jako vstup používají seed, což je náhodné číslo nebo vektor a slouží pro inicializaci generátoru.. Ten může být určen například z aktuálního času nebo dalších zdrojů. [32]

5.7 Odstranění dat z SSD

Bezpečné odstranění dat z disku SSD se liší od stejného procesu u mechanického pevného disku, kde jsou všechny sektory několikrát přepisovány tak, že není již možné původní data zrekonstruovat. Tato metoda hrubého přepisu však nemusí u SSD fungovat stejně dobře. U těchto disků může být 5 až 10 procent bloků nedostupných pro operační systém. Přepsání celého disku by se vyloučených bloků tedy nedotklo. Jelikož jsou však tyto bloky zcela mimo, bylo by potřeba pro přístup k datům využít vysoce specializovaný software. [33]

Pro vymazání všech viditelných dat je potřeba využít vhodný nástroj. Některé systémy BIOS mají zabudovanou funkci na bezpečné mazání. [33]



Obrázek 16: Funkce Secure Erase na základních deskách ASUS (převzato z [33])

V závislosti na značce a modelu disku může mít výrobce k dispozici bezplatný nástroj, který umožní provést bezpečné vymazání. Pokud je však vymazávaný disk zároveň diskem spouštěcím, je potřeba použít nástroj, který umožňuje vytvořit flash disk s vlastním systémem. [33]

Pokud výrobce disku nenabízí bezplatný nástroj, nebo není možné využít funkce v systému BIOS, je možné využít placených nástrojů. Parted Magic nabízí spustitelné prostředí Linux s nástroji pro bezpečnou likvidaci dat. [33]

Obrázek 17: Prostředí nástroje Parted Magic (převzato z [33])

Další možností je využít integrovaného nástroje Diskpart v příkazovém řádku v systému Windows 10 nebo Windows 11. Tato metoda nevymaže nadbytečné bloky, ale vymaže mapu disku, která na ně ukazuje. [33]

5.8 Legislativa a normy

Existuje několik evropských norem, které se týkají problematiky mazání dat. Obecné nařízení o ochraně osobních údajů se zkratkou GDPR stanovuje zásady pro správu osobních údajů, včetně požadavku na mazání osobních údajů, pokud nejsou potřeba, nebo pokud subjekt odvolal souhlas s jejich zpracováním. [34]

Vláda USA vydala dokument s označením NIST SP 800-88, který obsahuje metodické pokyny pro vymazání dat z elektronických paměťových médií. [35]

Obdobná norma DIN 66399 je také vydána Evropskou komisí. V českém prostředí je bezpečnost dat definována zákonem o kybernetické bezpečnosti č. 181/2014 Sb.

5.8.1 General Data Protection Regulation

Obecné nařízení GDPR představuje jednotný právní rámec ochrany osobních údajů v zemích Evropské Unie, které od 25. května 2018 určuje pravidla pro zpracování osobních údajů. V českém právním prostředí nahradil zákon č. 101/2000 Sb., o ochraně osobních údajů, který byl novelizován. [36]

GDPR dává fyzickým osobám právo požádat o odstranění jejich osobních údajů a organizace mají povinnost tak učinit. Výjimka může nastat pouze v následujících případech. [37]

- osobní údaje, které společnost/organizace má, jsou nutné pro výkon práva na svobodu projevu
- existuje právní povinnost tyto údaje uchovat
- z důvodů veřejného zájmu

Osobní údaje shromážděné protiprávně nebo v případě, že jde o osobní údaje fyzické osoby shromážděné v době, kdy byla ještě nezletilá, musí být odstraněny. [37]

5.8.2 DIN 66399

Evropská norma DIN 66399 definuje sedm stupňů bezpečnosti dokumentů. Norma přesně stanovuje maximální velikost výsledných částí po skartaci. Dalším typem označení skartace je čeká norma NBÚ. Dne 13. ledna 2022 vyšla ve sbírce zákonů vyhláška č. 13/2022 Sb., kterou se mění vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků. Ustanovení řešící velikosti odpadních částic v kapitole 9. přílohy č. 1 nabývá účinnosti dnem 1. ledna 2023. [38]

Tato klasifikace rozlišuje šest druhů materiálu, na kterých jsou data uložena.

- Písemnosti (P) - data z papíru, výtisky, dopisy, formuláře
- Optické nosiče dat (O) - CD a DVD
- Magnetické nosiče dat (T) - diskety, ID karty s magnetický proužkem
- Elektronické nosiče dat (E) - USB disky, čipové karty, paměťové karty
- Data ve zmenšené podobě (F) - mikrofilmy, fólie
- Data na pevných discích (H)

Dále jsou definovány tři úrovně ochrany podle charakteru skartovaných údajů.

Tabulka 4: Úrovně ochrany dat podle DIN 66399

Úrovně ochrany	Stupeň bezpečnosti	Typ dat
úroveň ochrany 1	1, 2, 3	Běžná úroveň ochrany obchodních a vnitropodnikových dokumentů
úroveň ochrany 2	3, 4, 5	Vysoká úroveň ochrany vnitroponikových a obchodních dokumentů
úroveň ochrany 3	5, 6, 7	Velmi vysoká úroveň ochrany, důvěrné a tajné dokumenty

Stupně bezpečnosti jsou určeny pro každý z typů dat. Jak je znázorněno v tabulce 4, pro každý druh existuje 7 stupňů zabezpečení. Čím vyšší je stupeň zabezpečení, tím menší jsou výsledné částice po skartaci. Stupně se dělí na:

- stupeň 1: běžné dokumenty (katalogy, brožury)
- stupeň 2: vnitropodnikové dokumenty (směrnice, obchodní podmínky)
- stupeň 3: osobní a citlivá data (obchodní nabídky, obecné ceníky)
- stupeň 4: obzvlášť citlivá a osobní data (cenové nabídky, obchodní výsledky, zdravotní dokumentace)
- stupeň 5: důvěrná data (patenty, stavební dokumentace, ID)
- stupeň 6: tajné dokumenty vyžadující mimořádné opatření
- stupeň 7: přísně tajné dokumenty vyžadující mimořádné bezpečnostní opatření (armáda, tajné služby)

P	O	T	E	F	H
P-1 proužky max. 12mm	O-1 částice max. 2000 mm2	T-1 mechanické zničení	E-1 mechanické/ elektronické zničení	F-1 částice max. 160 mm2	H-1 mechanické/elektronické zničení
P-2 proužky max. 6 mm	O-2 částice max. 800 mm2	T-2 částice max. 2000 mm2	E-2 rozdělení	F-2 částice max. 30 mm2	H-2 poškození
P-3 částice max. 320 mm2	O-3 částice max. 160 mm2	T-3 částice max. 320 mm2	E-3 částice max. 160 mm2	F-3 částice max. 10 mm2	H-3 deformace
P-4 částice max. 160 mm2	O-4 částice max. 30 mm2	T-4 částice max. 160 mm2	E-4 částice max. 30 mm2	F-4 částice max. 2,5 mm2	H-4 rozdělení či deformace na částice max. 2000 mm2
P-5 částice max. 30 mm2	O-5 částice max. 10 mm2	T-5 částice max. 30 mm2	E-5 částice max. 10 mm2	F-5 částice max. 1 mm2	H-5 rozdělení či deformace na částice max. 320 mm2
P-6 částice max. 10 mm2	O-6 částice max. 5 mm2	T-6 částice max. 10 mm2	E-6 částice max. 1 mm2	F-6 částice max. 0,5 mm2	H-6 rozdělení či deformace na částice max. 10 mm2
P-7 částice max. 5 mm2	O-7 částice max. 0,2 mm2	T-7 částice max. 2,5 mm2	E-7 částice max. 0,5 mm2	F-7 částice max. 0,2 mm2	H-7 rozdělení či deformace na částice max. 5 mm2

Obrázek 18: Tabulka skartace podle druhu média a zabezpečení (převzato z [39])

5.8.3 NIST Special Publication 800-88

NIST Special Publication 800-88 je vládní dokument USA, který poskytuje metodické pokyny pro vymazání dat z elektronických paměťových médií. Cílem je účinně sanitovat média tak, aby všechna data byla po skončení životnosti dat nebo zařízení pro ukládání dat nevratná. [40]

Tuto normu lze použít pro magnetické, flashové i jiné technologie ukládání dat, jako jsou například USB disky nebo serverová úložiště. Ve skutečnosti nejsou tyto pokyny určeny pro konkrétní technologii. Naopak, zásady a pracovní postupy, které tento dokument popisuje, jsou určeny k univerzálnímu použití pro různé typy médií, včetně těch, která možná ještě nebyla vynalezena. [40]

Tento proces musí brát v úvahu likvidaci dat již od samého počátku plánování ukládání dat. To znamená posoudit média a pracovní postupy implementované v raných fázích budování informačního systému. Pochopení toho, jaké úrovně sanitizace jsou možné u komponent používaných k ukládání a zpracování dat, může usnadnit správnou implementaci sanitizace, když je to potřeba. [40]
NIST v podstatě doporučuje, aby uživatelé určili, jakou metodu sanitizace mají použít na základě:

- kategorie informace podle důvěrnosti
- povahy paměťového média
- rizika
- dalšího použití paměťového média

Jakmile jsou tato rozhodnutí učiněná, je možné rozhodnout, jakou metodu likvidace dat je potřeba zvolit. [40]

5.8.4 Zákon o kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti upravuje práva a povinnosti osob, jakož i pravomoc a působnost orgánů veřejné moci v oblasti kybernetické bezpečnosti. Zpracovává příslušné předpisy Evropské unie a upravuje zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů. [41]
Hlavním cílem zákona je:

- stanovit základní úroveň bezpečnostních opatření,
- zlepšit detekci kybernetických bezpečnostních incidentů,
- zavést hlášení kybernetických bezpečnostních incidentů,
- zavést systém opatření k reakci na kybernetické bezpečnostní incidenty,
- upravit činnost dohledových pracovišť.

V roce 2017 proběhly dvě obsahově významné novely zákona o kybernetické bezpečnosti, a to prostřednictvím zákona č. 104/2017 Sb. s účinností od 1. července a zákona č. 205/2017 Sb. s účinností od 1. srpna 2017. K aktuálnímu datu proběhly ještě následující novelizace tohoto zákona – novelizace zákonem č. 183/2017 Sb., zákonem 35/2018 Sb., zákonem č. 111/2019 Sb., č. 12/2020 Sb., zákonem č. 261/2021 Sb., a aktuálně poslední novelizace zákonem č. 226/2022 Sb. Aktuální znění zákona je účinné od 6. srpna 2022. [41]

5.8.5 Vyhláška o kybernetické bezpečnosti

Tato vyhláška zapracovává Směrnici NIS a pro informační systémy kritické informační infrastruktury, komunikační systémy kritické informační infrastruktury, významné informační systémy, informační systémy základní služby anebo informační systémy nebo sítě elektronických komunikací, které využívá poskytovatel digitálních služeb, upravuje:

- obsah a strukturu bezpečnostní dokumentace,
- obsah a rozsah bezpečnostních opatření,
- typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů,
- náležitosti a způsob hlášení kybernetického bezpečnostního incidentu,
- náležitosti oznámení o provedení reaktivního opatření a jeho výsledku,
- vzor oznámení kontaktních údajů a jeho formu,
- způsob likvidace dat, provozních údajů, informací a jejich kopií.

Nová vyhláška o kybernetické bezpečnosti byla zveřejněna ve Sbírce zákonů pod označením "Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)". [41]

5.8.6 Vnitřní politiky organizací

Organizace a firmy mohou mít své vlastní interní politiky týkající se mazání dat z pevných disků. Tyto politiky mohou být v souladu s výše uvedenými normami a doporučeními, ale mohou být také přizpůsobeny specifickým potřebám a bezpečnostním standardům organizace.

6 Praktická část

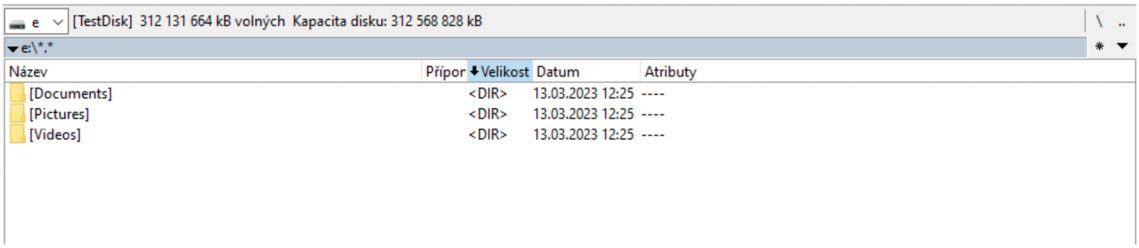
Cílem praktické části je aplikace a porovnání metod, kterými lze z pevných disků mazat data. Součástí praktické části je také návrh zásad a doporučení, kterými by se měl uživatel řídit, pokud chce spolehlivě odstranit data ze svého zařízení. Návrh vychází z poznatků nabitých v teoretické části a z výsledků získaných v praktické části.

6.1 Metodika

Pro každou demonstrovanou metodu je vytvořen stejný balíček testovacích dat. Jedná se o 50 fotografií ve vysokém rozlišení s celkovou velikostí 139MB. Nejmenší fotografie má velikost 494KB, největší pak 8,85MB.

Dalším typem dat jsou videa v rozlišení 1920x1080 s celkovou velikostí 184MB. Velikosti jednotlivých souborů se pohybují od 4,57MB do 61,6MB.

Poslední soubor testovacích dat obsahuje textové soubory ve formátu .odt. Jedná se o celkem tři soubory s celkovou velikostí 78,8KB.



Obrázek 19: Struktura testovacích dat

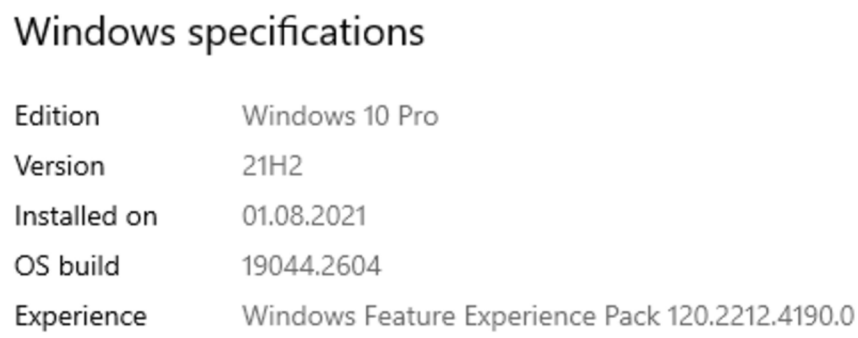
Aby byly výsledky testů relevantní a srovnatelné, je pro každou metodu použit stejný hardware a stejná verze softwaru.

Pro demonstraci mazání dat na magnetickém pevném disku je použit disk WD Scorpio Black BE s kapacitou 320GB. Jedná se o mobilní 2.5" disk s rychlostí otáček 7200/min, vyrovnávací pamětí 16MB a vyhledávací dobou 12 ms. Disk obsahuje rozhraní SATA 3Gb/s.

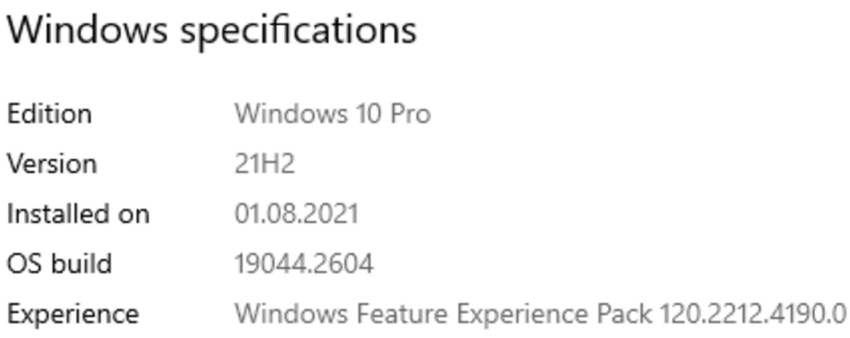
Pro demonstraci mazání dat na flash paměti je použit Samsung SSD 850 EVO s kapacitou 250GB. Pro flashovou paměť je použita technologie TLC. Formát disku

je také 2.5", rychlost čtení 540MB/s a rychlost zápisu 520MB/s. Disk obsahuje rozhraní SATA 6Gb/s.

Všechny ukázky jsou demonstrovány v prostředí Windows 10.



Obrázek 20: Specifikace Windows



Obrázek 21: Specifikace Windows

Pro mazání dat je použit software ERASER ve verzi 6.2.0.2993. Tento software obsahuje všechny standardně používané metody na přepsání dat na pevném disku. Na obnovu dat je použitý software Recuva ve verzi 1.53.2083 a software R-Studio verze 9.2.191126.

V rámci jednotlivých metod je zkoumána nejen kvalita mazání, ale také časová náročnost. Po testu každé metody je disk znovu přepsán pseudonáhodnými čísly a naformátován z prostředí Windows.

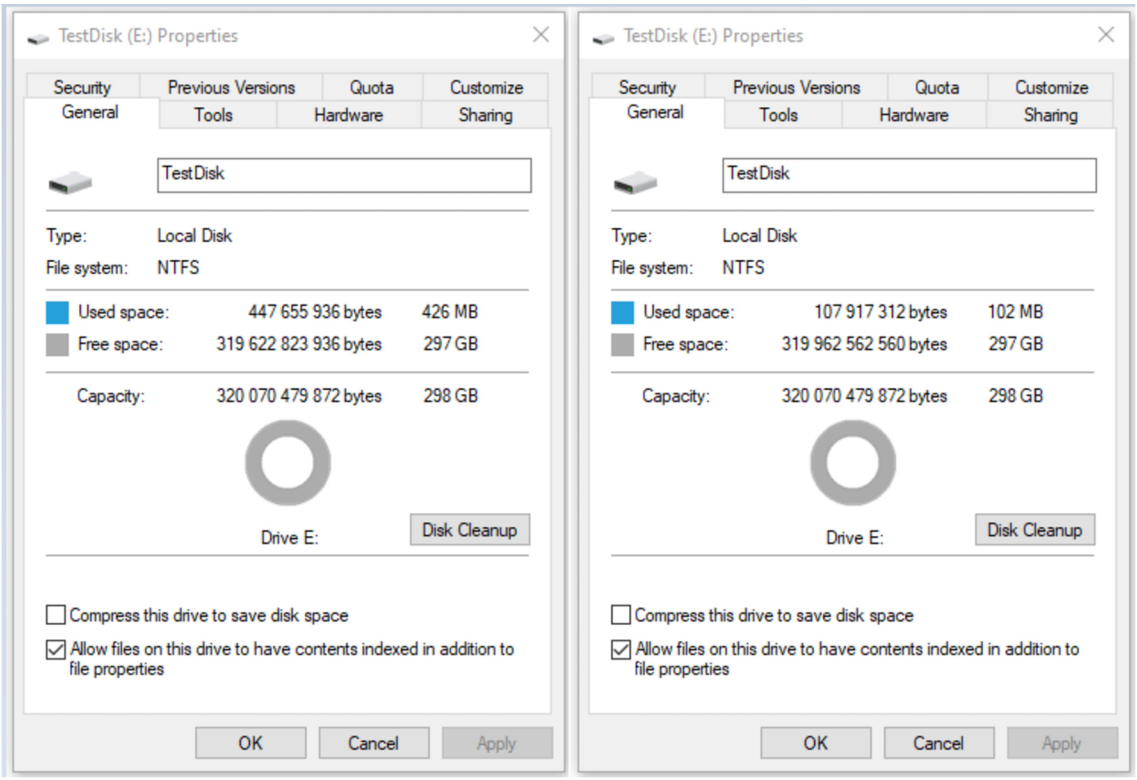
Pro mazání dat z disku typu SSD je využit software výrobce Samsung Magician ve verzi 10.0.19044. Pro obnovu dat pak software Disk Drill s verzí 5.1.808.0.

6.2 Likvidace dat na pevném disku

Nejlepší metodou pro odstranění dat z pevného disku je jeho několikanásobné přepsání. V závislosti na zvolené metodě je disk přepsán kombinací jedniček a nul, popřípadě pseudonáhodnými čísly. V následujících kapitolách je zkoumána efektivita jednotlivých metod a jejich časová náročnost.

6.2.1 Smazání dat z prostředí Windows

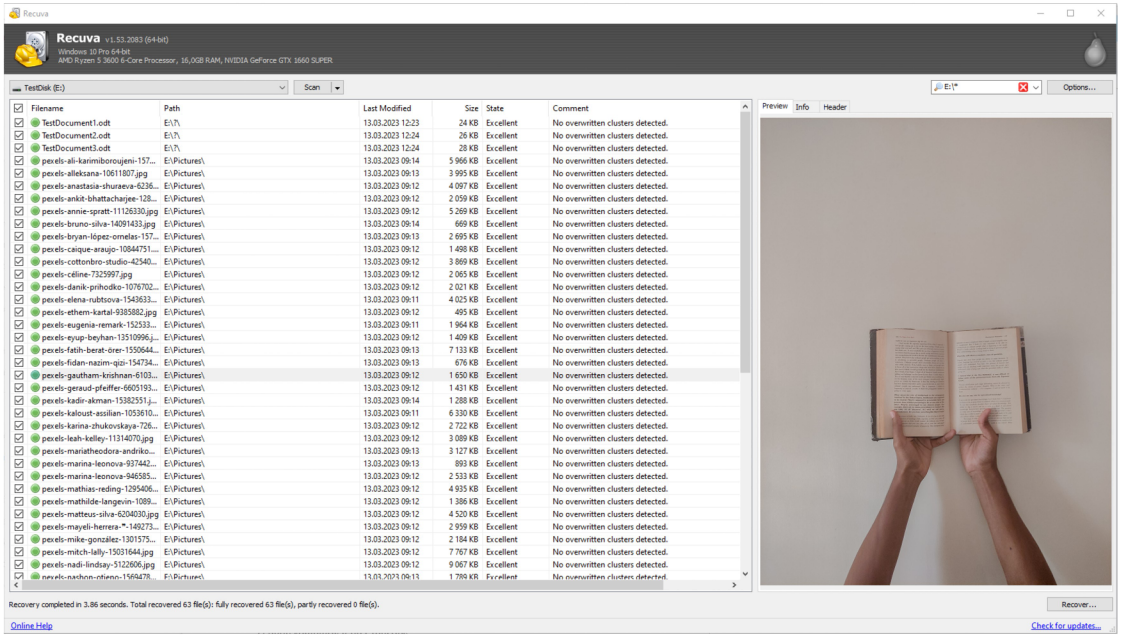
Nejběžnější a nejpoužívanější způsob mazání dat v prostředí Windows je jejich přesun do koše a jeho následné vysypání. Alternativně lze také využít klávesovou zkratku SHIFT + DELETE, kdy se soubory smažou rovnou bez nutnosti vysypat koš. Všechna testovací data jsou touto metodou smazána v řádech vteřin a není potřeba použít nástroj třetí strany.



Obrázek 22: Porovnání místa na disku před a po smazání souborů

Jak je patrné z obrázku 20., data smazaná touto metodou uvolní místo na disku a jsou dále pro uživatele nedostupná.

Již při rychlém naskenování disku softwarem Recuva lze najít smazané soubory a spustit jejich obnovu.

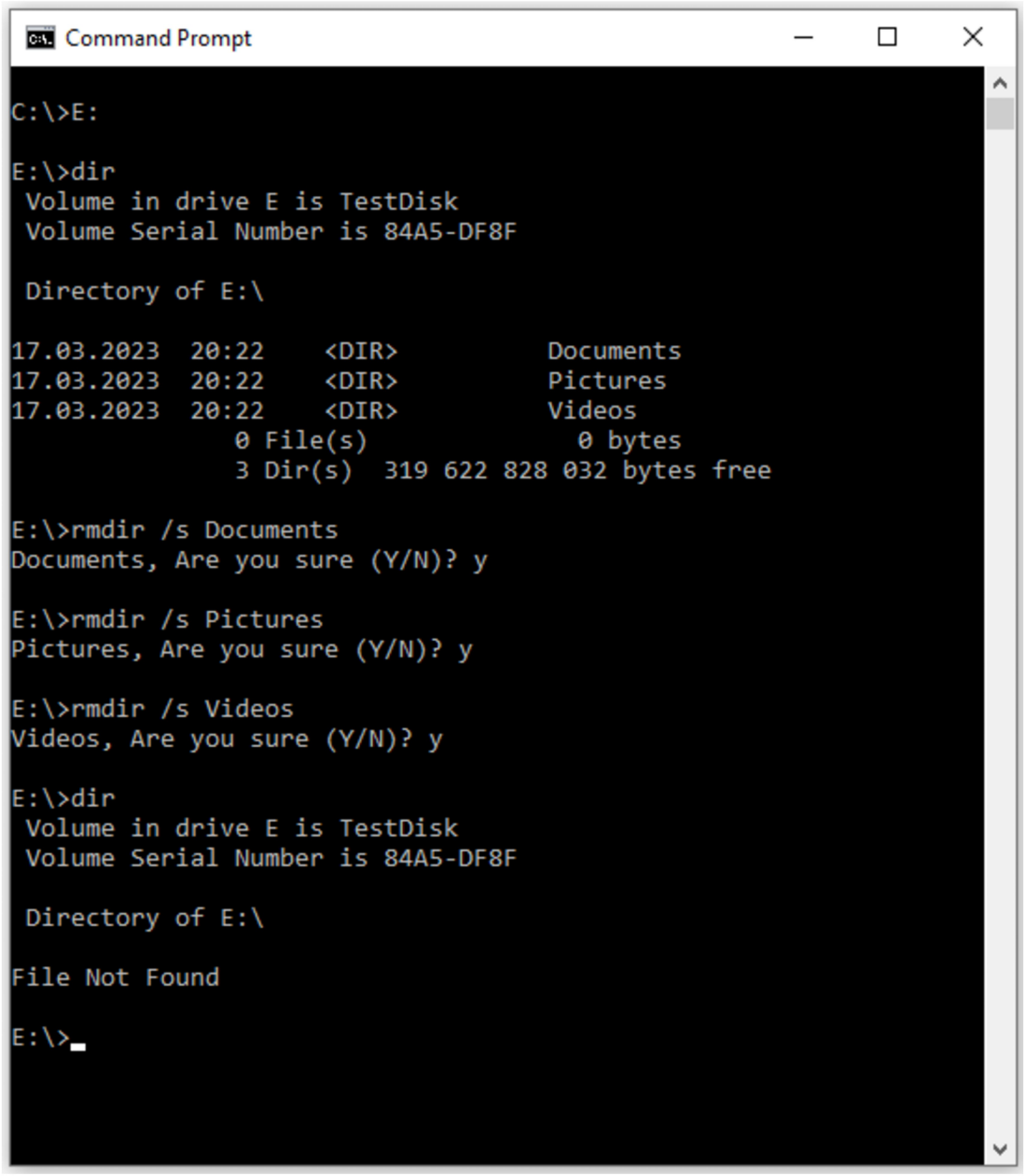


Obrázek 23: Smazaná data nalezena softwarem EaseUS

Všechna data smazaná z prostředí Windows jsou v pořádku obnovena a jsou čitelná. Obnova takto smazaných dat trvá pouhých 3,86 vteřiny.

Dalším způsobem, jak odstranit data z prostředí Windows, je využít příkazový řádek.Pokud data nejsou uložena na disku, kde je nainstalován systém, je potřeba v příkazovém řádku nejprve vybrat správné písmeno jednotky.

Následně je vhodné obsah disku zkontrolovat příkazem dir. Příkazem rmdir /s “nazev_slozky” lze vymazat adresář, který obsahuje podadresáře nebo soubory. Pro smazání je nutné volbu potvrdit.



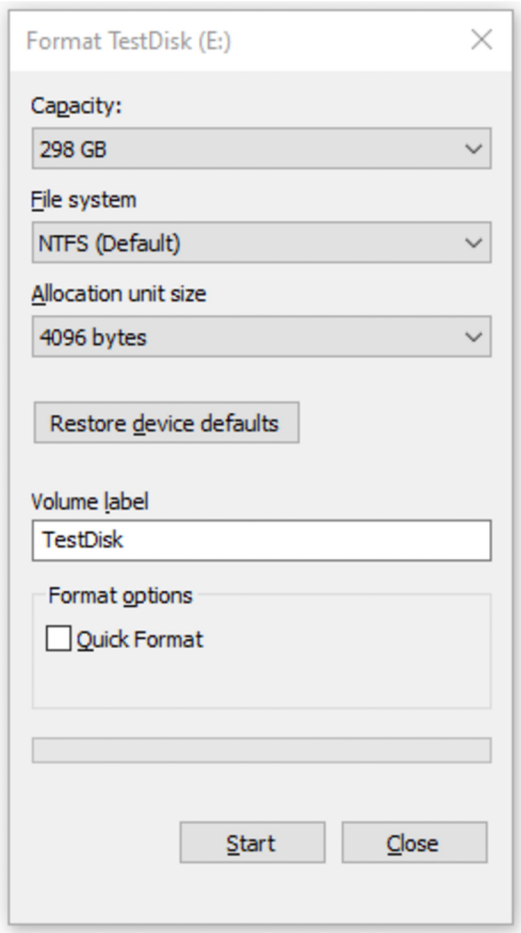
Obrázek 24: Posloupnost příkazů pro vymazání dat

Takto smazaná data nejsou přesunuta do koše, nelze je tedy jednoduše obnovit do původního umístění. Specializovaným softwarem však lze všechna samazaná data obnovit.

6.2.2 Formátování disku pomocí nástrojů prostředí Windows

Další metodou, kterou lze ke smazání souborů na disku využít, je aplikace nativní funkce operačního systému Windows na formátování. Tuto funkci lze spustit

z kontextového menu, které je možné vyvolat kliknutím pravého tlačítka myši na zvolený k formátování. V okně s nastavením lze pak vybrat vhodné parametry.

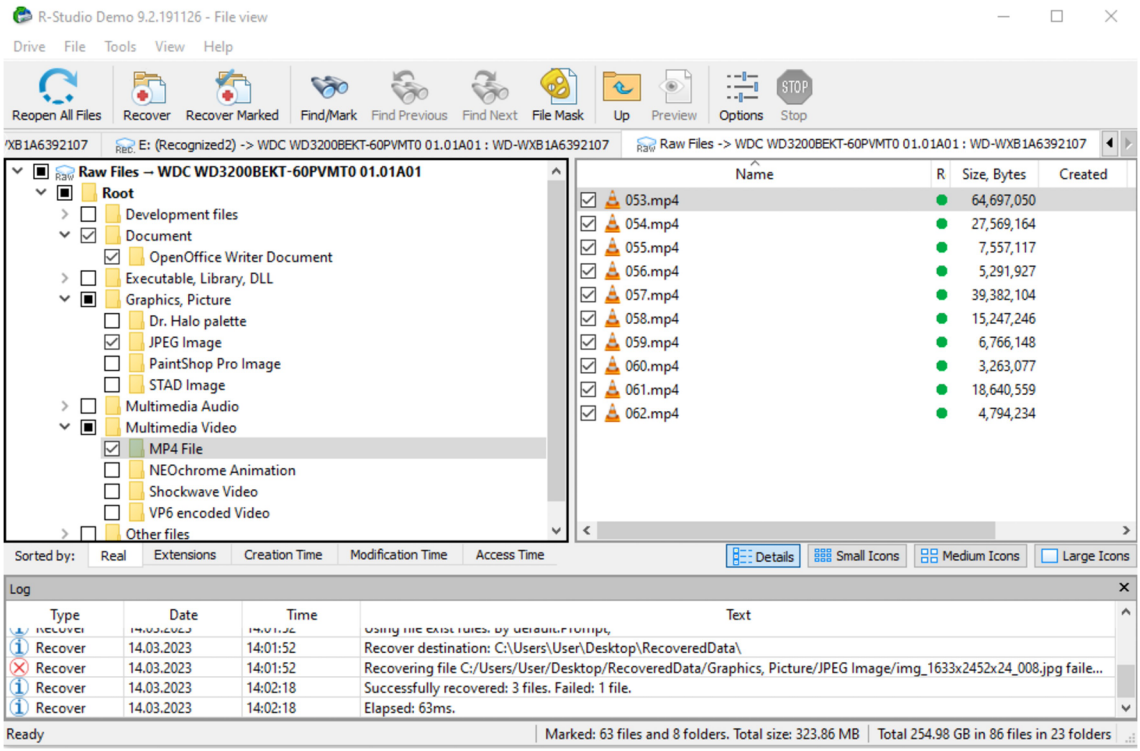


Obrázek 25: Funkce formátování v prostředí Windows

Pro účely demonstrace jsou všechny parametry nastaveny na výchozí hodnoty. Funkce Quick Format slouží k rychlému formátování. To data nevymaže, pouze je umožní přepsat. Disk se ale přesto tváří jako prázdný, podobně jako při odstranění dat v předchozí kapitole. Čas potřebný k rychlému formátování je několik vteřin.

Při pokusu o obnovu pomocí softwaru Recuva není v rychlém módu detekován žádný soubor vhodný k obnovení. Při hloubkové kontrole disku jsou ale nalezena data, která lze obnovit. V nich však 4 soubory s příponou .jpg chybí. Všechna smazaná data tedy obnovit nelze.

Dalším pokusem je obnova pomocí softwaru R-Studio. Po naskenování celého disku se daří dohledat všechny smazané soubory a obnovit je.

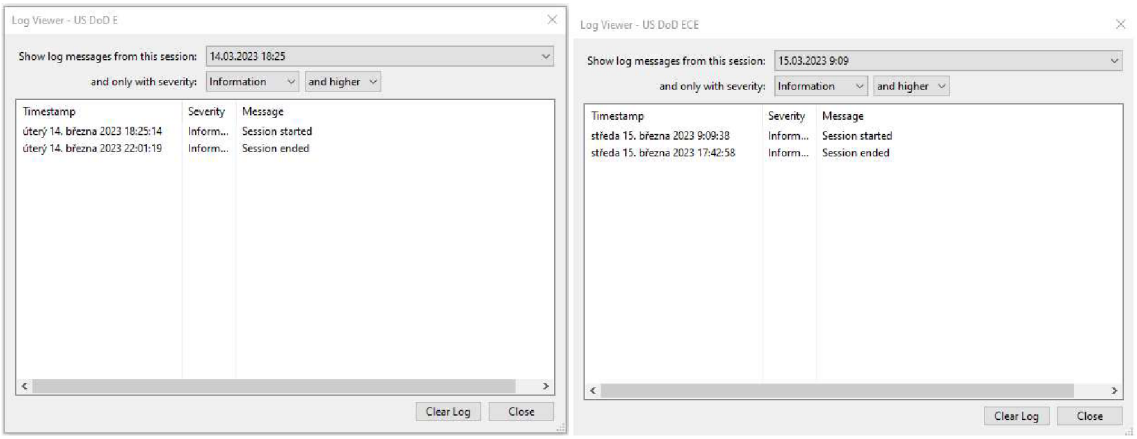


Obrázek 26: Obnovená data po rychlém formátování

Pokud není zvolena možnost rychlého formátování, časová náročnost stoupá z několika vteřin až na 120 minut. Pokus o obnovu však nevede k žádným výsledkům a data není možné obnovit ani pomocí softwaru Recuva, ani pomocí softwaru R-Studio.

6.2.3 Metoda DoD 5220.22-M

Tato metoda mazání není součástí standardní výbavy operačního systému Windows a je proto nutné využít software třetí strany. Software Eraser obsahuje obě verze metody DoD 5220.22-M. Jedná se o verzi 8-306./E, C, & E, která obsahuje 7 průchodů a o verzi 8-306./E, která obsahuje průchody tři. U této metody je sledována jak kvalita odstranění dat, tak časová náročnost.



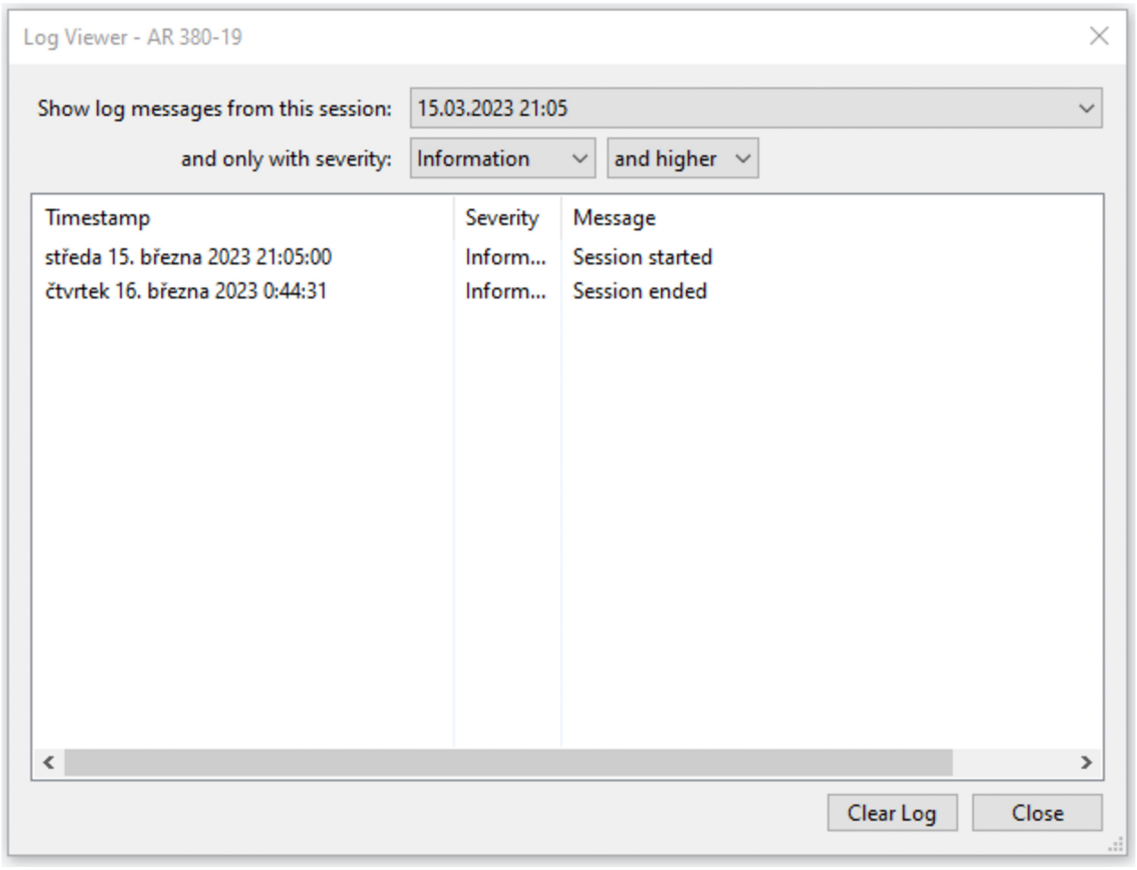
Obrázek 27: Porovnání časů běhů

Jak je patrné z logů na obrázku 25, tříprůchodový algoritmus projde celý disk za tři a půl hodiny. Varianta se sedmi průchody potřebuje pro přepis celého disku osm a půl hodiny.

Po smazání disku oběma variantami nelze najít žádná data vhodná k obnově ani pomocí softwaru Recuva, ani pomocí softwaru R-Studio. Nejpatrnější rozdíl mezi oběma variantami je tedy pouze čas potřebný k dokončení algoritmu.

6.2.4 Metoda AR 380-19

Metoda AR 380-19 nemá obdobně jako metoda DoD 5220.22-M nativní podporu v operačním systému Windows. Je tedy opět nutné využít software třetí strany. Software Eraser obsahuje podporu pro tento typ mazání dat.

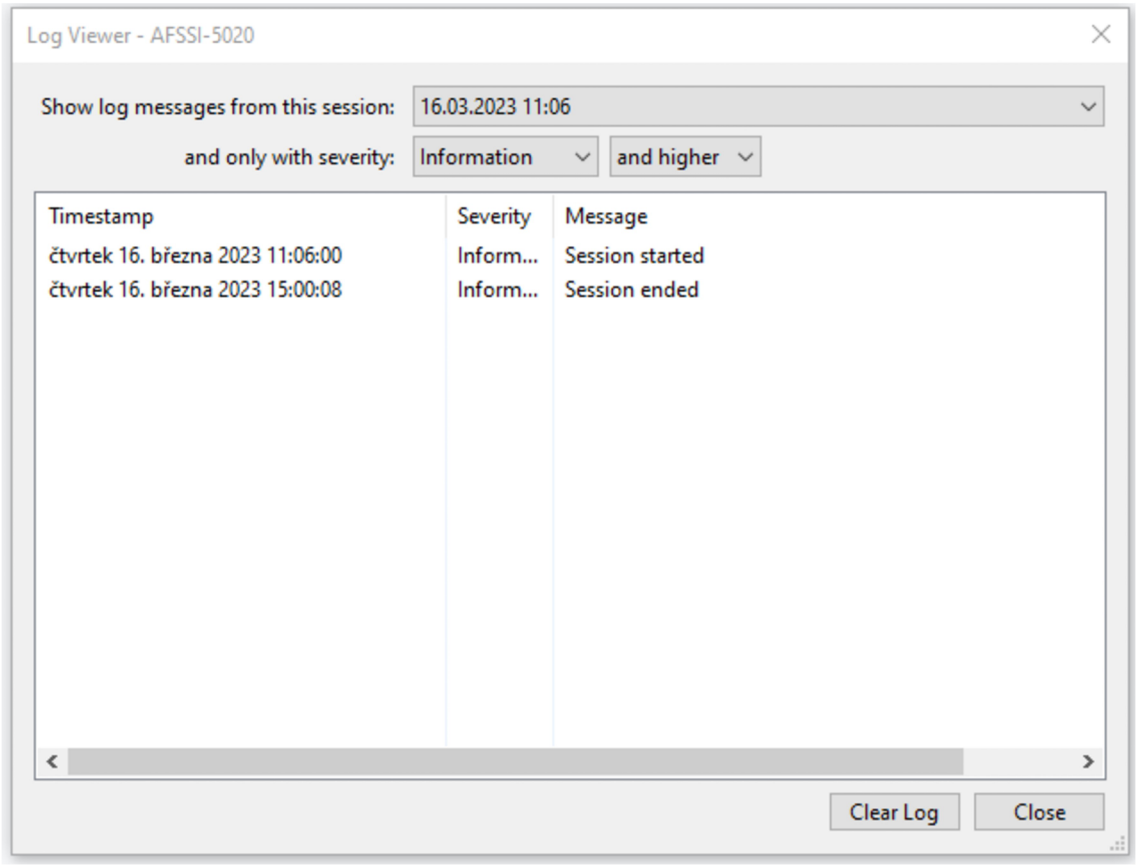


Obrázek 28: Záznam běhu metody AR 380-19

Průchod disku touto metodou trvá tři hodiny a 40 minut. Při pokusu o obnovení dat není možné dohledat žádná data.

6.2.5 Metoda AFSSI-5020

Další metodou pro bezpečné odstranění dat je AFSSI-5020. Jedná se o tříprůchodový algoritmus bez nativní podpory v prostředí operačního systému Windows. Pro jeho aplikaci je proto opět nutné použít nástroj třetí strany.

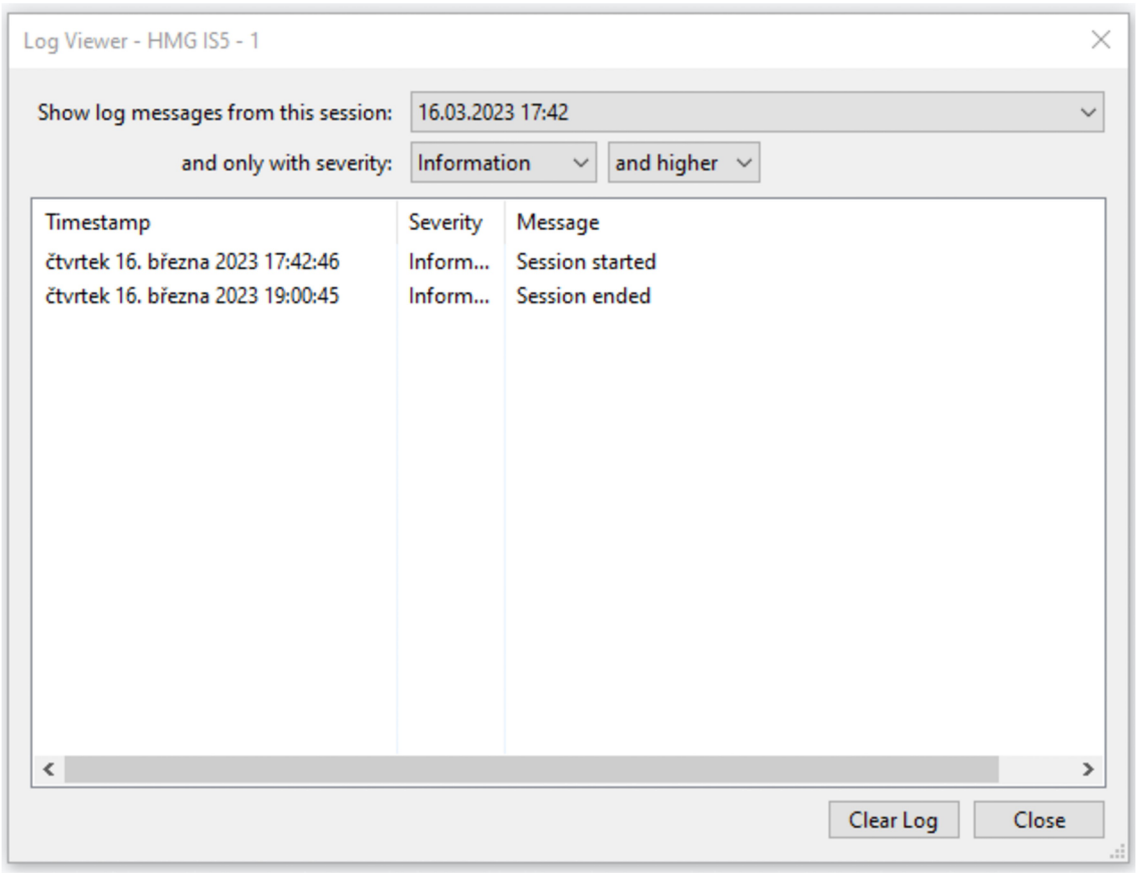


Obrázek 29: Záznam běhu metody AFSSI-5020

Doba potřebná pro vymazání celého disku metodou AFSSI-5020 je necelé 4 hodiny. Při pokusu o obnovu pomocí softwaru Recuva není možné obnovit žádná data. Stejný výsledek vykazuje také obnovení dat z disku pomocí softwaru R-Studio.

6.2.6 Metoda HMG IS5

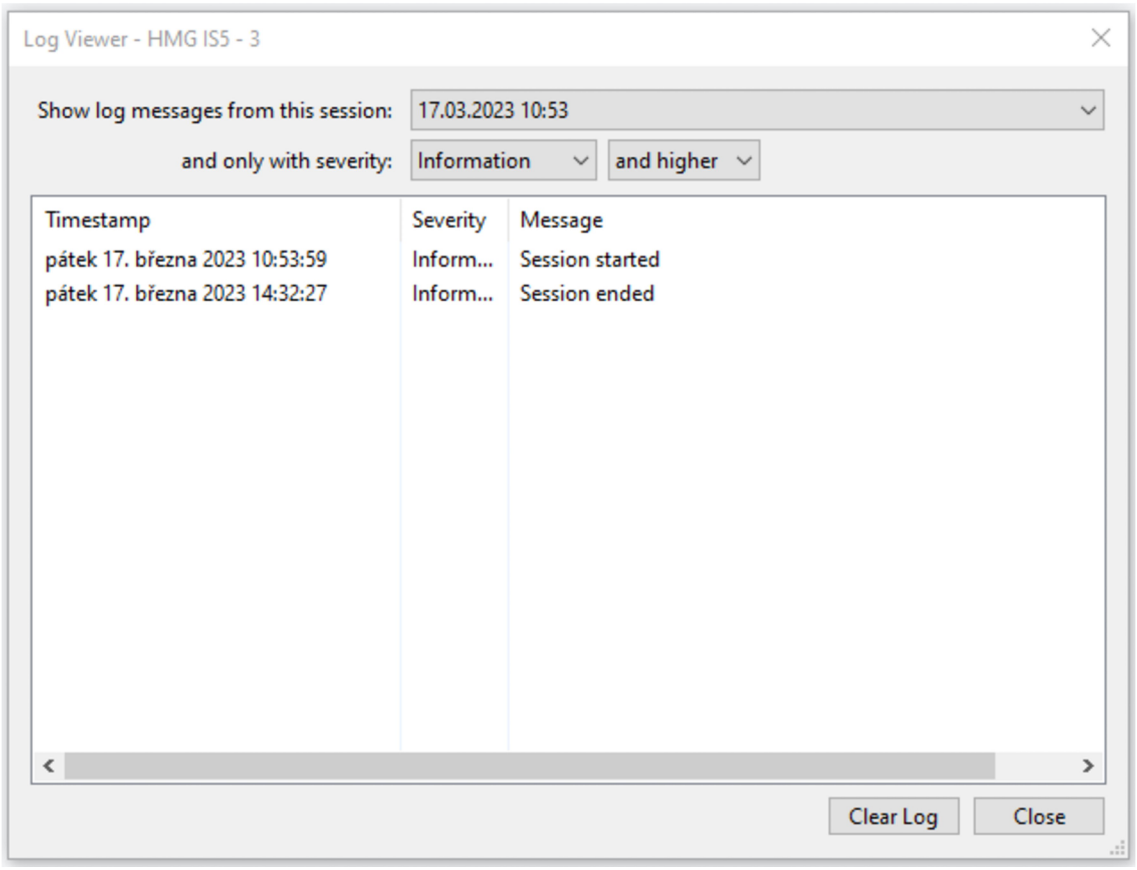
Algoritmus HMG IS5 lze spustit ve dvou verzích. První verze HMG IS5 baseline přepíše celý disk pouze nulami. Tato verze algoritmu přepíše disk pouze jednou, čas potřebný k přepsání je proto pouze 1 hodina a 18 minut. Baseline verze je součástí algoritmů, které obsahuje software Eraser.



Obrázek 30: Záznam běhu metody HMG IS5 Baseline

I přes to, že je pevný disk přepsán pouze jednou, nelze standardním softwarem obnovit žádná z dříve nahraných dat.

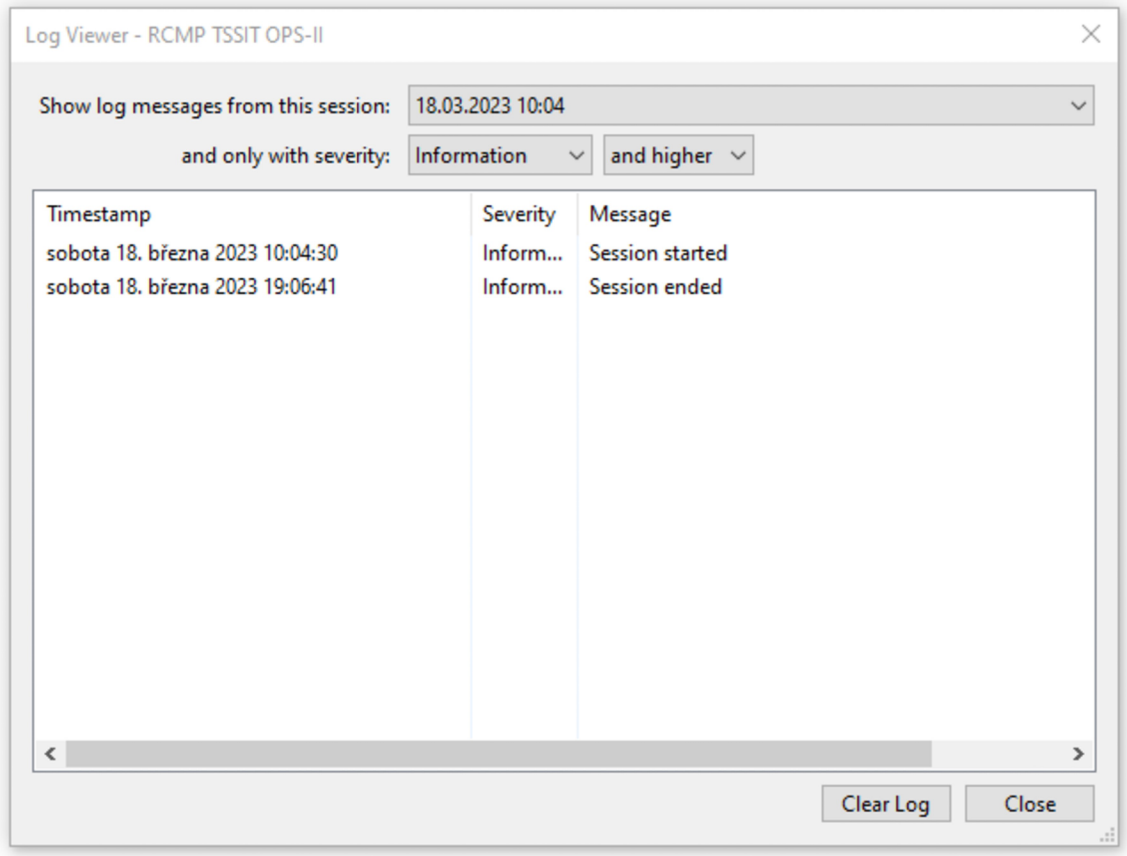
Další verze algoritmu, HMG IS5 Enhanced, prochází disk třikrát. První průchod zapisuje 1, druhý průchod 0, třetí průchod zapíše náhodně buď 1 nebo 0. Čas potřebný na průchod celého disku je v tomto případě 3 hodiny a 38 minut. Ani v tomto případě nelze obnovit odstraněná data.



Obrázek 31: Záznam běhu metody HMG IS5 Enhanced

6.2.7 Metoda RCMP TSSIT OPS-II

RCMP TSSIT OPS-II je sedmiprůchodový algoritmus, který v prvních šesti průchodech zapisuje střídavě 1 a 0. V posledním sedmém průchodu pak zapíše náhodný znak. Také tato metoda je součástí softwaru Eraser.

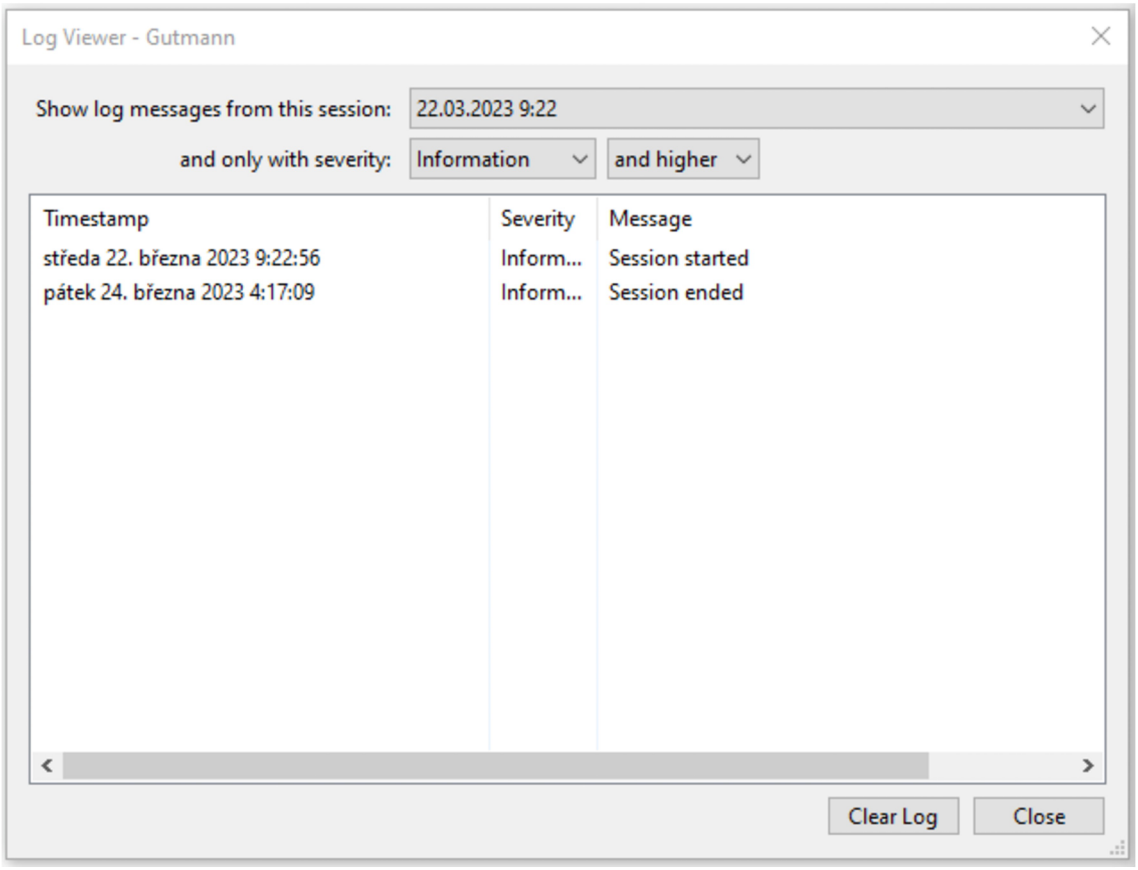


Obrázek 32: Záznam běhu metody HMG IS5 Enhanced

Celková doba potřebná na vymazání disku je 9 hodin. Data ani v tomto případě nelze standardním softwarem obnovit.

6.2.8 Gutmannova metoda

Gutmannova metoda provede celkem 35 průchodů, při kterých zapisuje náhodné číslo a předem definovaný řetězec znaků. Stejně jako ostatní, i tato metoda je součástí softwaru Eraser.



Obrázek 33: Záznam běhu Gutmannovi metody

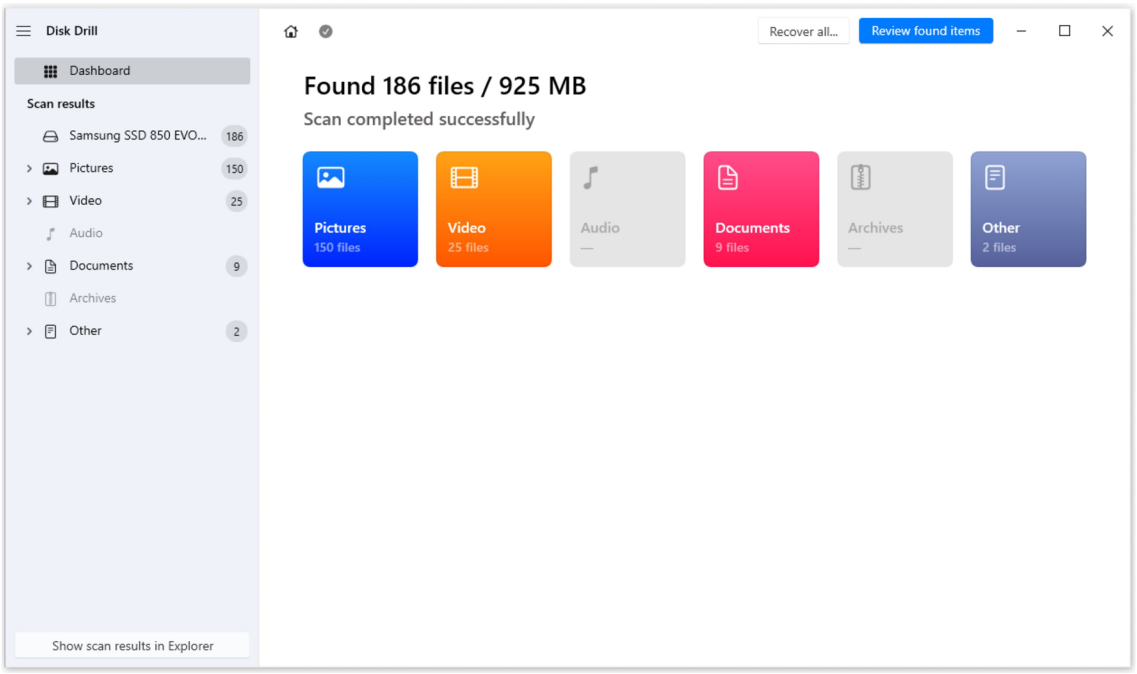
Tato metoda vyžaduje pro průchod celého disku necelých 43 hodin. Po sérii 35 zápisů nelze z disku obnovit žádná data.

6.3 Likvidace dat na SSD

Jelikož má každá paměťová buňka flash paměti, několikanásobným přepisováním celého disku by se mohla výrazně snížit jeho životnost. Je proto vhodné využít funkcí softwaru přímo od výrobce, které umožňují disk smazat bez výrazného snížení životnosti.

6.3.1 Smazání dat z prostředí Windows

Stejně jako u mechanického disku, i u SSD disku lze smazat data jejich přesunutím do koše a vysypáním, nebo kombinací kláves SHIFT + DELETE. Rychlost smazání dat závisí na jejich velikosti. Testovací data v určeném objemu jsou smazána v rámci vteřin.

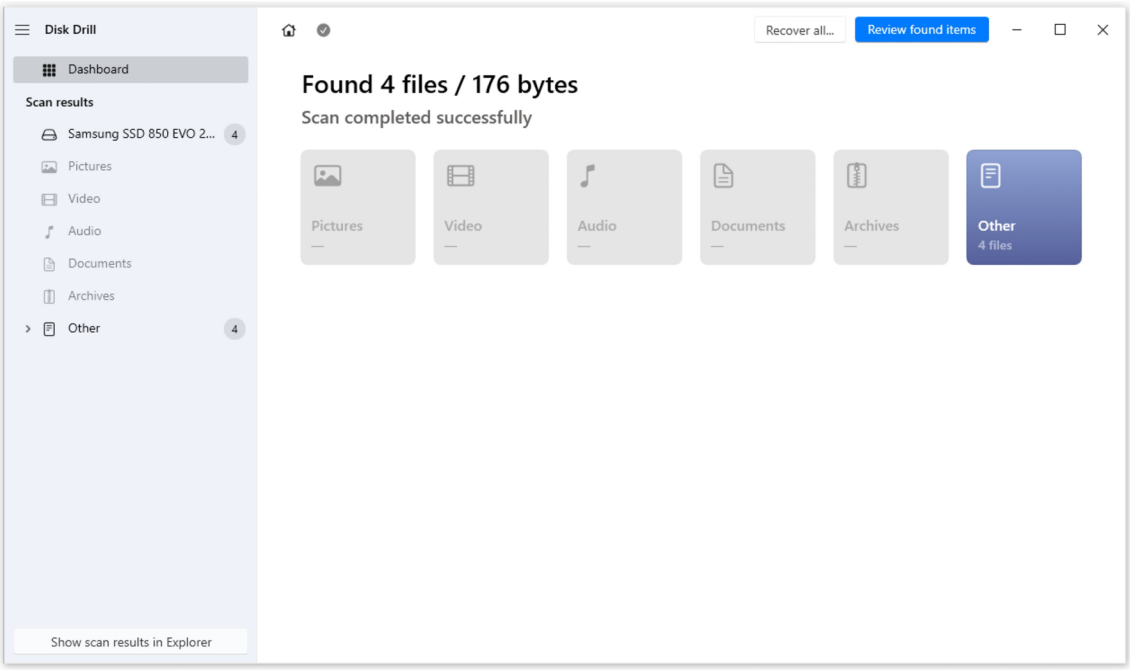


Obrázek 34: Obnovená data

Pomocí softwaru Disk Drill se lze obnovit všechna odstraněná data. Výsledný počet souborů je větší, než testovací soubor. Tato nesrovnalost je zapříčiněna tím, že se obnovovací SW pokusí nejen o obnovu souborů, ale také o jejich rekonstrukci. Ta probíhá na základě nalezených metadat a interní databáze.

6.3.2 Formátování disku pomocí nástrojů prostředí Windows

Nativní formátování prostředí Windows lze využít i na disky typu SSD. Tato funkce nabízí možnost rychlého formátování, které u mechanických disků není příliš spolehlivé. U SSD však ani po rychlém formátu nelze obnovit žádná data. Celý proces se u rychlého formátování odehrává v jednotkách vteřin, u pomalejší varianty se jedná o 16 minut.

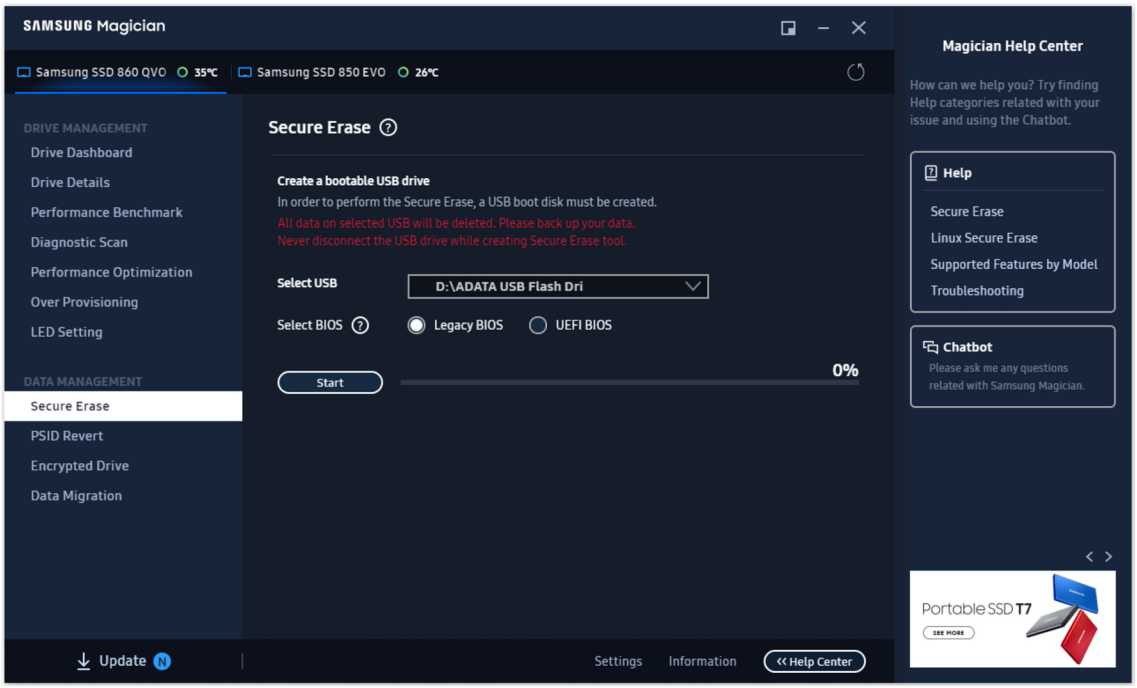


Obrázek 35: Výsledek obnovy dat po formátu disku z prostředí Windows

Data z disku nelze obnovit a to ani po formátování rychlou metodou. Na rozdíl od rychlého formátování mechanického pevného disku je takovýto postup u SSD spolehlivější.

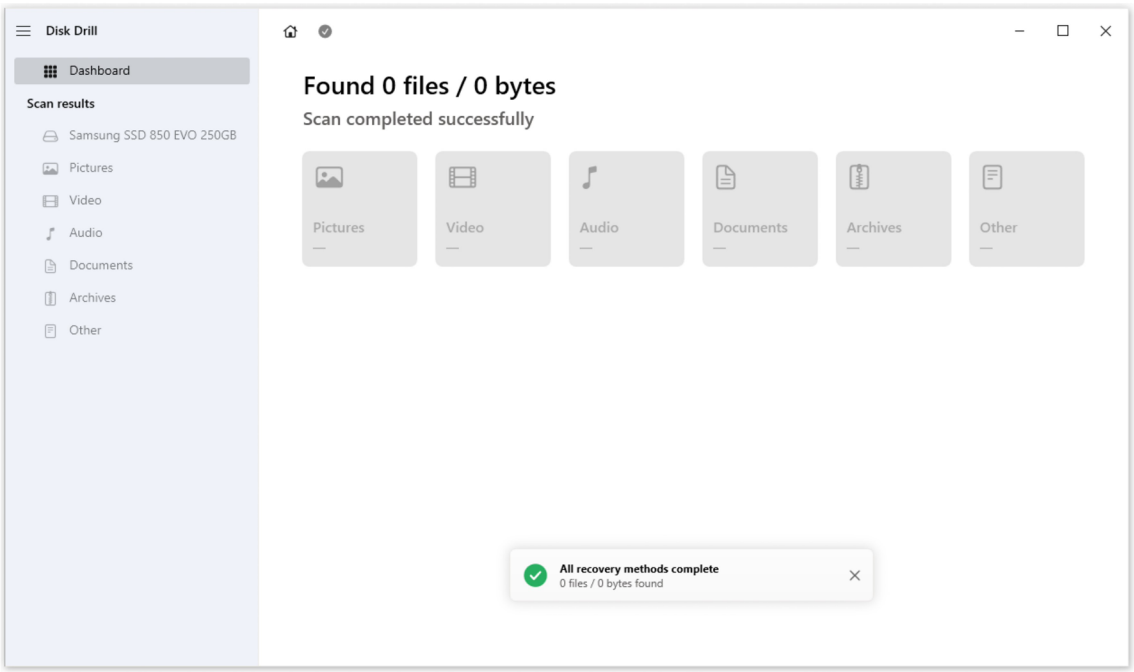
6.3.3 Odstranění dat nástroji od výrobce

Software Samsung Magician pro disky od výrobce Samsung nabízí mimo jiné nástroje také bezpečné mazání dat z SSD. V aplikaci lze využít funkci Secure Erase a vytvořit bootovatelný flash disk.



Obrázek 36: Vytvoření USB flash disku

Pro základní desky se starším systémem BIOS je možné vytvořit flash disk, který umožňuje bootovat v legacy módu. Pro novější je pak k dispozici i systém UEFI. Po vytvoření média je nutné restartovat systém a přes bootovací menu spustit systém vytvořený na flash disku. Zde už jen stačí vybrat správnou jednotku a potvrdit trvalé odstranění dat. Samotné odstranění dat z SSD zabere jen pár vteřin, vytvoření média, restart PC a správné nabootování ale může trvat i několik minut. Pro nezkušené uživatele pak tento proces může trvat mnohem déle. Při pokusu o obnovení nelze softwarem Disk Drill najít žádná zachovaná data.



Obrázek 37: Výsledek skenování disku po bezpečném smazání dat

6.4 Porovnání jednotlivých metod

V této kapitole je provedeno porovnání vzhledem k výsledkům získaným testováním jednotlivých metod.

Tabulka 5: Výsledky mazání z HDD podle jednotlivých metod

Metoda	Počet průchodů	Časová náročnost	Úspěšnost
Smazání souboru z prostředí Windows		< 1 min	0%
Smazání souboru přes příkazový řádek		< 1 min	0%
Formátování z prostředí Windows - rychlé		< 1 min	0% - 6,3%
Formátování z prostředí Windows		2h	100%
DoD 5220.22-M E	3	3h 36 min	100%
DoD 5220.22-M E.C.E	7	8h 33 min	100%
AR 380-19	3	3h 39 min	100%

AFSSI-5020	3	3h 54 min	100%
HMG IS5 Basic	1	1h 18 min	100%
HMG IS5 Enhanced	3	3h 38 min	100%
RCMP TSSIT OPS-II	7	9h 2 min	100%
Gutmannova metoda	35	42h 54 min	100%

Porovnání metod v tabulce 4 ukazuje, že všechny tříprůchodové algoritmy potřebují ke kompletnímu přepsání disku čas v rozmezí 3,5 hodiny až 4 hodiny. Úspěšnost smazání je u všech shodně 100%. To znamená, že nehledě na zvolenou metodu se podaří všechna data úspěšně smazat za stejný čas.

Metoda HMG IS5 Basic s jedním průchodem potřebuje pro kompletní smazání dat z disku 1 hodinu a 18 minut. I přes to, že je disk přepsaný pouze jednou, vykazuje tato metoda stejnou úspěšnost jako předchozí algoritmy. Lze tedy dosáhnout stejného výsledku za třetinu času.

Metody DoD 5220.22-M E.C.E a RCMP TSSIT OPS-II, které disk prochází sedmkrát mají také velmi podobnou časovou náročnost od 8 hodin 30 minut do 9 hodin. I tyto metody podle dosažených výsledků vykazují vysokou spolehlivost a ani u těchto metod nebylo možné obnovit žádná data.

Nejnáročnější Gutmannova metoda, která provede 35 průchodů je časově nejnáročnější. Smazání disku o kapacitě 320GB jí zabere necelých 43 hodin. Vzhledem k podobným výsledkům, kdy nebylo možné obnovit žádná smazaná data, se takovýto počet průchodů jeví jako redundantní a stejných výsledků se dá dosáhnout rychlejšími algoritmy.

U mechanickým pevných disků se jako neúčinné odstranění dat ukazuje prosté smazání z prostředí Windows. U tohoto typu odstranění dat bylo možné všechny soubory obnovit už rychlým skenováním disku, které trvá řádově minuty. Ani rychlé formátování pomocí nástrojů operačního systému nevede k uspokojivým výsledkům. Ačkoliv při rychlém prohledání disku některé soubory chyběly, hloubkový sken dokázal všechna data najít a obnovit. Formátování v pomalém režimu však dokázalo data odstranit trvale. Ačkoliv tato operace zabere

více času, je rychlejší než některé složitější metody a je možné docílit stejné úspěšnosti.

Tabulka 6: Výsledky mazání SSD podle jednotlivých metod

Metoda	Časová náročnost	Úspěšnost
Smazání souboru z prostředí Windows	< 1 min	0%
Formátování z prostředí Windows - rychlé	< 1 min	100%
Formátování z prostředí Windows	16 min	100%
Nástroje od výrobce	< 1 min	100%

Metody vhodné pro mechanické disky nelze aplikovat pro úložiště z flash pamětí. Díky omezenému počtu přepisů by mohlo dojít ke snížení životnosti disku. Pro bezpečné smazání dat je tedy potřeba použít software od výrobce, nebo využít nástroje operačního systému.

Z tabulky 5 je zřejmé, že všechny zvolené metody jsou časově efektivní. Při použití nástrojů od výrobce je ale nutné vytvořit bootovatelné médium a smazat disk přes takto vytvořený systém. To může odradit méně zkušené uživatele od použití tohoto nástroje. Narozdíl od rychlého formátování na mechanickém disku se u SSD nepodařilo obnovit žádná data. Obnovení dat bylo úspěšné pouze v případě smazání dat přesunutím do koše a následného vysypání.

6.5 Návrh zásad bezpečného mazání dat

V této kapitole jsou na základě poznatků z teoretické části a výsledků části praktické navrhnuty zásady bezpečné likvidace dat.

6.5.1 Nakládání s daty

Data je nutno chránit nejen po dobu jejich existence, ale i po jejich odstranění. V předchozích kapitolách je demonstrováno obnovení dat, která byla smazána nevhodným nebo nedostatečným způsobem.

Uživatel by si měl vždy uvědomit, jaký typ dat má a historicky měl uložený na svém zařízení a co by způsobilo jejich zneužití. V případě firem mohou být únikem těchto

dat také porušeny zákony nebo vyhlášky jako je například GDPR, což může vést k vysokým pokutám. Vždy je potřeba zvážit vhodnou likvidaci citlivých dat.

Důležité zásady při nakládání s daty:

- Mějte přehled o typech dat na vašem zařízení.
- Mějte na paměti následky v případě úniku citlivých dat.

6.5.2 Nakládání s datovým médiem

Nakládání s datovým médiem je pro bezpečnost dat stejně důležité jako jejich aktivní ochrana. Je nutné se zamyslet, co se stane s datovým úložištěm zařízení, které je určeno k vyřazení nebo prodeji.

Pokud je nepoužívané zařízení určeno k prodeji, je vhodné toto zařízení prodávat, pokud je to možné, bez pevného disku nebo jiného datového média. Pokud zařízení nejde prodat bez tohoto média, například mobilní telefon, nebo chce uživatel prodat samotné datové médium, je dobré si ověřit, že takovýto nosič neobsahuje data, která je možné zneužít. Obecně ale platí, že data mají ve většině případů větší cenu než zařízení, na kterých jsou uložena.

V případě likvidace zařízení obsahující pevný disk je vhodné vyjmout pevný disk a nechat ho zlikvidovat odbornou firmou. V tomto případě dojde k fyzické likvidaci média. Obnova dat z takto skartovaného média je velice náročná a nákladná.

Důležité zásady při nakládání s datovým nosičem:

- Zařízení likvidujte bez datových nosičů.
- Datový nosič neprodávejte.
- Datový nosič nechte zlikvidovat odbornou firmou.

6.5.3 Bezpečné mazání dat

Před vymazáním nežádoucích dat je nutné si rozmyslet, jakou metodou data vymazat, aby nemohla být později obnovena a zneužita. Jak je patrné z výsledků v praktické části, přesunutí souboru do koše a následné vysypání se ukazuje jako nedostatečné. Je proto vhodné zvolit alternativní metodu odstranění souboru vzhledem k jeho obsahu.

Ačkoliv je u jednotlivých algoritmů pro mazání dat vysoká časová náročnost, většina softwaru pro bezpečnou likvidaci dat nabízí možnost smazání konkrétního

souboru. Pro každý soubor lze zvolit vlastní metodu, a už jednoprůchodový algoritmus pro méně citlivé soubory může být účinný.

Důležité zásady pro bezpečné mazání dat:

- Pro mazání souborů používejte pokročilejší metody.
- Podle citlivosti dat zvolte vhodný algoritmus.

6.5.4 Předpisy a normy

Uživatel je zodpovědný za data, se kterými pracuje. Pokud dojde k jejich zneužití, může uživatel, nebo organizace, pro kterou pracuje, čelit právním následkům, jako je například vysoká pokuta.

Existuje několik předpisů a norem, které upravují, jak mají být citlivá data a nosiče zlikvidovány. Uživatel, který s takovými daty pracuje, by se měl seznámit s platnými právními předpisy a normami.

Je také vhodné se seznámit s vnitřní politikou a předpisy organizace, ve které uživatel pracuje. V případě, že není jasné, jak nakládat s citlivými daty a bezpečně je mazat, je nutné kontaktovat IT oddělení, popřípadě zaměstnance pověřeného touto agendou.

Důležité zásady pro dodržování předpisů a norem:

- Vždy se seznamte s platnými předpisy.
- Zjistěte, jaká vnitřní politika pro nakládání s daty existuje ve vaši společnosti.
- V případě, že si nejste jistí pravidly, kontaktujte pověřeného pracovníka.

7 Shrnutí výsledků

Výsledek práce ukazuje, že při zvolení nevhodné metody pro odstranění dat může útočník takováto data obnovit i za pomoci běžně dostupného softwaru. Pro získání citlivých dat, která neprošla sanitací, není potřeba použití zvláštních, drahých nástrojů.

Uživatel naštěstí může svá data bezpečně odstranit pomocí nástrojů a programů, které jsou v základních verzích často dostupné zdarma. Existují ale i komerční alternativy, které nabízejí rozšířené možnosti a funkcionality.

Při praktických pokusech na cvičných datech bylo zjištěno, že i nástroje, které nabízí operační systém, mohou být dostačující pro správnou likvidaci dat. Některé pokročilé metody se naopak ukázaly jako časově neefektivní. Jedná se zejména o víceprůchodové algoritmy, kde jsou některé průchody, vzhledem k úspěšnosti rychlejších metod, redundantní.

8 Závěry a doporučení

V současné době, kdy je většina citlivých dat ukládána v elektronické formě, by měli být uživatelé seznámeni se základními pravidly likvidace jak dat, tak datových médií.

Teoretická část práce se věnuje popisu datových úložišť, zejména pak magnetickým a polovodičovým diskům, jejich fyzické a logické struktuře a způsobu uložení dat. Je zde uvedena fyzická a logická struktura a způsob uložení dat.

Dále jsou zde popsány způsoby pro odstranění dat a to jak běžné metody jako odstranění souborů z prostředí Windows, tak i pokročilejší algoritmy. Důraz je kladen zejména na vícenásobné přepisy disku a u vybraných metod je detailně vysvětleno, jakým způsobem se sektory přepisují. Popsán je i způsob, jakým lze bezpečně smazat data z polovodičových disků typu SSD.

Závěr teoretické části se pak věnuje platným právním předpisům a normám, které se zabývají touto problematikou.

V praktické části jsou jednotlivé metody demonstrovány na sadě testovacích dat. U mechanických disků jsou exekuovány algoritmy pro vícenásobný přepis, je zkoumána jejich efektivita a časová náročnost. Jednotlivé metody jsou pak zhodnoceny a porovnány z hlediska úspěšnosti a časové náročnosti.

V závěru praktické části je navržena sada zásad a doporučení, kterými by se měl uživatel řídit v případě, že chce svá data bezpečně odstranit.

Diplomová práce tedy uživatelům nabízí jak teoretický základ, tak i praktické ukázky, ze kterých je patrné, jaká metoda pro odstranění dat je nejvhodnější.

9 Seznam obrázků a tabulek

Seznam obrázků

Seznam tabulek

10 Seznam použité literatury

[1] Co je to pevný disk? - Správa.sítě.eu. Správa sítě - slovník pojmů: správa sítě, zabezpečení sítě, outsourcing IT [online]. Copyright © [cit. 03.11.2022]. Dostupné z: https://www.sprava-site.eu/pevny-disk/

[2] HORÁK, Jaroslav. Hardware: učebnice pro pokročilé. 3., aktualiz. vyd. Brno: CP Books, 2005. ISBN 80-251-0647-0.

[3] DEMBOWSKI, Klaus. Mistrovství v hardware. Brno: Computer Press, 2009. ISBN 978-80-251-2310-2.

[4] Učebnice HW - HDD a Mechaniky. Základní škola Kadaň, ul. Chomutovská 1683 - [online]. Dostupné z: https://3zskadan.cz/hardware/ucebnice_hdd_a_mechaniky.html

[5] Jak pracují pevné disky - Cnews.cz. Cnews.cz – Píšeme o technologiích a internetu [online]. Copyright © 1997 [cit. 04.11.2022]. Dostupné z: https://www.cnews.cz/jak-pracuji-pevne-disky/

[6] Definition of access time | PCMag. The Latest Technology Product Reviews, News, Tips, and Deals | PCMag [online]. Copyright © 1996 [cit. 04.11.2022]. Dostupné z: https://www.pcmag.com/encyclopedia/term/access-time

[7] AdminXP.cz: HDD 3: Struktura uložení dat (geometrie disku), Metody kódování. AdminXP.cz: Průvodce pro začátečníky a administrátory. Tipy, triky, návody, odpovědi a odkazy. [online]. Copyright © 2000 [cit. 05.02.2023]. Dostupné z: https://www.adminxp.cz/hardware/index.php?aid=128

[8] Anthony Sammes; Brian Jenkinson (17 April 2013). Forensic Computing: A Practitioner's Guide. Springer Science & Business Media. pp. 108–. ISBN 978-1-4471-3661-3.

[9] What Is Mean Time Between Failures (MTBF) in Hard Drives? . How-To Geek - We Explain Technology [online]. Copyright © 2023 LifeSavvy Media. All Rights Reserved [cit. 05.02.2023]. Dostupné z: https://www.howtogeek.com/837903/what-is-mean-time-between-failures-mtbf-in-hard-drives/

[10] S.M.A.R.T - zjistěte jak je na tom Váš harddisk | Pctuning. Průvodce světem informačních technologií | Pctuning [online]. Copyright © 2002 [cit. 05.02.2023]. Dostupné z: https://pctuning.cz/article/s-m-a-r-t-zjistete-jak-je-na-tom-vas-harddisk

[11] Solidní budoucnost pevných disků – úvod k velkému testu SSD disků | Pctuning. Průvodce světem informačních technologií | Pctuning [online]. Copyright © 2002 [cit. 05.02.2023]. Dostupné z: https://pctuning.cz/article/solidni-budoucnost-pevnych-disku-uvod-k-velkemu-testu-ssd-disku

[12] The Anatomy of an SSD - The SSD Anthology: Understanding SSDs and New Drives from OCZ. AnandTech: Hardware News and Tech Reviews Since 1997 [online]. Copyright © 2023. All rights reserved. [cit. 05.02.2023]. Dostupné z: https://www.anandtech.com/show/2738/5

[13] The Secret Sauce: 0.5x Write Amplification - OCZ's Vertex 2 Pro Preview: The Fastest MLC SSD We've Ever Tested. AnandTech: Hardware News and Tech Reviews Since 1997 [online]. Copyright © 2023. All rights reserved. [cit. 05.02.2023]. Dostupné z: https://www.anandtech.com/show/2899/3

[14] Increasing Flash SSD Reliability. https://storagesearch.com/siliconsys-art1.html

[15] Co je souborový systém? - Správa.sítě.eu. Správa sítě - slovník pojmů: správa sítě, zabezpečení sítě, outsourcing IT [online]. Copyright © [cit. 07.02.2023]. Dostupné z: https://www.sprava-site.eu/souborovy-system/

[16] What is NTFS and how does it works? | Geekboots. Geekboots for programmer and tech enthusiast | Geekboots [online]. Copyright © 2023 [cit. 10.02.2023]. Dostupné z: https://www.geekboots.com/story/what-is-ntfs-and-how-does-it-works

[17] Souborový systém budoucnosti: exFAT | Chip.cz - recenze a testy. Informace, testy a novinky o hardware, software a internetu – CHIP.cz [online]. Copyright © 2003 [cit. 10.02.2023]. Dostupné z: https://www.chip.cz/casopis-chip/earchiv/rubriky/novinky-earchiv/souborovy-system-budoucnosti-exfat/

[18] What is the Master Boot Record (MBR)?. Purchase Intent Data for Enterprise Tech Sales and Marketing - TechTarget [online]. Dostupné z: https://www.techtarget.com/whatis/definition/Master-Boot-Record-MBR

[19] Enterprise Storage Forum | Data Storage News & Products [online]. Dostupné z: https://www.enterprisestorageforum.com/management/fragmentation/

[20] What is defragmentation: Why do I need it? | Diskeeper. Condusiv - Blazing Fast Windows Performance & Reliability Software [online]. Copyright

© [cit. 11.02.2023]. Dostupné z: https://condusiv.com/disk-defrag/defragmentation/

[21] The Evolution of Hard Disk Bit Recording. Bucaro Techelp [online]. Copyright ©2001 [cit. 11.02.2023]. Dostupné z: http://bucarotechelp.com/computers/architecture/80062801.asp

[22] https://www.edn.com/validate-usb-host-designs-with-a-bare-metal-driver/

[23] https://it-slovnik.cz/pojem/pametova-karta

[24] What is data destruction? | Definition from TechTarget. Purchase Intent Data for Enterprise Tech Sales and Marketing - TechTarget [online]. Dostupné z: https://www.techtarget.com/searchstorage/definition/data-destruction

[25] What is Data Destruction? For Data Protection, the Definition Matters - Blancco. Data Erasure Software | Secure Data Destruction — Blancco [online]. Copyright © 2022 Blancco Technology Group. All rights reserved. [cit. 16.02.2023]. Dostupné z: https://www.blancco.com/resources/article-data-destruction-definition/

[26] Why Use a Degausser and Degausser FAQs | Data Security, Inc.. Data Security, Inc. | Keeping Your Data Secure for Over 30 Years [online]. Copyright © Copyright 2021 Data Security, Inc. [cit. 16.02.2023]. Dostupné z: https://datasecurityinc.com/security/degausser.html

[27] SSD Erasure: What Enterprises Need to Know — Blancco. Data Erasure Software | Secure Data Destruction — Blancco [online]. Copyright © 2022 Blancco Technology Group. All rights reserved. [cit. 16.02.2023]. Dostupné z: https://www.blancco.com/resources/blog-what-do-you-really-know-about-ssd-erasure/

[28] Top 5 Hard Drive Destruction Methods That Actually Work. Hard Drive Shredding | Secure Paper Shredding | HDD Wiping [online]. Copyright © All Rights Reserved 2020. [cit. 16.02.2023]. Dostupné z: https://datadestruction.com/top-5-hard-drive-destruction-methods-actually-work/

[29] 8 Effective Algorithms to Wipe and Erase Data Permanently. Data Recovery, File Recovery and Email Recovery Software [online]. Copyright © 2001 [cit. 16.02.2023]. Dostupné z: https://www.datanumen.com/blogs/8-effective-algorithms-wipe-erase-data-permanently/

[30] Information on the DoD 5220.22-M Data Wipe Method. Data Destroyers EU, Data destruction equipment for destroying data carriers [online]. Copyright ©2001 [cit. 16.02.2023]. Dostupné z: https://www.datadestroyers.eu/technology/dod_5220.22-m_data_wipe_method.html

[31] ANON., no date. What is the HMG IS5 method?tipsmake.com [online] [accessed. 17. February 2023]. Dostupné z: https://tipsmake.com/what-is-the-hmg-is5-method

[32] Nepodceňujte skartaci dat - Computerworld. Computerworld [online]. Copyright © 2020 [cit. 17.02.2023]. Dostupné z: https://www.computerworld.cz/clanky/nepodcenujte-skartaci-dat/

[33] How to Securely Erase an SSD or HDD Before Selling It | Tom's Hardware. Tom's Hardware: For The Hardcore PC Enthusiast [online]. Copyright © [cit. 17.02.2023]. Dostupné z: https://www.tomshardware.com/how-to/secure-erase-ssd-or-hard-drive

[34] Data protection in the EU. Redirecting to /select-language?destination=/node/1 [online]. Dostupné z: https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en

[35] What is NIST 800-88, and What Does "Media Sanitization" Really Mean? — Blancco. Data Erasure Software | Secure Data Destruction — Blancco [online]. Copyright © 2022 Blancco Technology Group. All rights reserved. [cit. 21.02.2023]. Dostupné z: https://www.blancco.com/resources/blog-what-is-nist-800-88-media-sanitization/

[36] Stručný výklad GDPR - kdy, proč a jak | Největší katalog ICT řešení. Vylepšete své ICT řešení [online]. Copyright © Asociace za lepší ICT řešení, o.p.s. [cit. 21.02.2023]. Dostupné z: https://lepsi-reseni.cz/ochrana-osobnich-udaju-gdpr/vyklad-gdpr-proc-jak/

[37] Musíme osobní údaje odstranit vždy, když o to fyzická osoba požádá?. Redirecting to /select-language?destination=/node/1 [online]. Dostupné z: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/do-we-always-have-delete-personal-data-if-person-asks_cs

[38] Stupně bezpečnosti skartování | Skart.cz. Skartovačky papíru Fellowes a příslušenství [online]. Copyright © 2023 PALA, s. r. o. [cit. 21.02.2023]. Dostupné z: https://www.skart.cz/stupne-bezpecnosti-skartovani/

[39] https://www.univox.cz/nova-din-66399-nove-stupne-utajeni/t-189/

[40] What is NIST 800-88, and What Does "Media Sanitization" Really Mean? — Blancco. Data Erasure Software | Secure Data Destruction — Blancco [online]. Copyright © 2022 Blancco Technology Group. All rights reserved. [cit. 26.02.2023]. Dostupné z: https://www.blancco.com/resources/blog-what-is-nist-800-88-media-sanitization/

[41] Národní úřad pro kybernetickou a informační bezpečnost - Legislativa. Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka

[online]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

[42] Delete a file - Microsoft Support. [online]. Dostupné z: https://support.microsoft.com/en-us/office/delete-a-file-abaa4886-6a79-4d81-842d-46652e08c72a

[43] What Is the Recycle Bin? - Definition from Techopedia. Techopedia: Educating IT Professionals To Make Smarter Decisions [online]. Copyright © 2023 Techopedia Inc. [cit. 15.03.2023]. Dostupné z: https://www.techopedia.com/definition/4675/recycle-bin

[44] Disk formatting explained: When should I format my hard drive? - Safemode Computer Service. Same Day Computer Repairs. Rated Best 3 in Sydney 2022 [online]. Copyright © Copyright Safemode Computer Service [cit. 15.03.2023]. Dostupné z: https://safemode.com.au/disk-formatting-explained/

[45] What Does Format Disk Mean? Everything You Should Know - EaseUS. EaseUS Software | Data Recovery, Backup, Partition Manager, Data Transfer, Video Editor and Recorder. [online]. Copyright © [cit. 15.03.2023]. Dostupné z: https://www.easeus.com/computer-instruction/what-does-format-disk-mean.html

[46] [online]. Dostupné z: https://in.indeed.com/career-advice/career-development/how-to-delete-a-file-using-cmd

[47] USENIX | The Advanced Computing Systems Association [online]. Dostupné z: https://www.usenix.org/legacy/publications/library/proceedings/sec96/full_papers/gutmann/index.html

[48] Nuraqilah Haidah Ahmad Riduan, Cik Feresa Mohd Foozy, Isredza Rahmi A Hamid, Palaniappan Shamala, Nur Fadzilah Othman, "Data Wiping Tool: ByteEditor Technique", 2021 3rd International Cyber Resilience Conference (CRC), pp.1-6, 2021.

[49] What is an SSD (Solid-State Drive)?. Purchase Intent Data for Enterprise Tech Sales and Marketing - TechTarget [online]. Dostupné z: https://www.techtarget.com/searchstorage/definition/SSD-solid-state-drive

Oskenované zadání práce

UNIVERZITA HRADEC KRÁLOVÉ
Fakulta informatiky a managementu
Akademický rok: 2021/2022

Studijní program: Aplikovaná informatika
Forma studia: Kombinovaná
Obor/kombinace: Aplikovaná informatika (ai2-k)

Podklad pro zadání DIPLOMOVÉ práce studenta

Jméno a příjmení: **Bc. Jiří Klouda**
Osobní číslo: **I2100433**
Adresa: sidl. U Cukrovaru 1084, Kralupy nad Vltavou, 27801 Kralupy nad Vltavou 1, Česká republika

Téma práce: Bezpečná likvidace datových medií a mazání dat
Téma práce anglicky: Secure disposal of data media and data erasure
Jazyk práce: Čeština

Vedoucí práce: Mgr. Josef Horálek, Ph.D.
Katedra informačních technologií

Zásady pro vypracování:

Cílem diplomové práce je podrobně představit a popsat metody pro zajištění bezpečné likvidace datových médií a bezpečného mazání dat. V teoretické části autor zpracuje analýzu legislativních a normativních požadavků pro bezpečné likvidace datových médií a bezpečného mazání dat. Dále podrobně popíše systémy a algoritmy pro bezpečné mazání dat, jejich implementaci a navrhne postupy pro jejich realizaci. V praktické části autor provede komparativní analýzu vybraných dostupných softwarových řešení zaměřenou a efektivitu a výkon bezpečného mazání dat.

Seznam doporučené literatury:

SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.

BHUNIA, Swarup a Mark TEHRANIPOOR. Hardware Security : A Hands-on Learning Approach. Morgan Kaufmann Publishers In: Morgan Kaufmann Publishers In, 2018. ISBN 9780128124772.

Podpis studenta: Datum:

Podpis vedoucího práce: Datum: