Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Obnova a mazání dat na úložných typech pamětí

Jindřich Vachata

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Vachata Jindřich

Informatika

Název práce

Obnova a mazání dat na úložných typech pamětí.

Anglický název

Recovering and erasing data from memory storage devices

Cíle práce

V diplomové práci je zkoumána problematika uložení a odstranění dat na různých paměťových mediích. Hlavní cíl DP je zhodnotit a navrhnout možnosti obnovení nechtěně smazaných dat a navrhnout bezpečné a trvalé odstranění citlivých dat.

Metodika

Teoretické i praktické seznámení s problematikou počítačových pamětí a rozbor jednotlivých typů. Analýza a technické posouzení ukládání dat. Syntéza teoretický a praktických poznatků a jejich vyhodnocení.

Harmonogram zpracování

1. Příprava spojená se studiem odborných informačních ztrojů a upřesnění cílů práce: 05/2013 - 06/2012
2. Zpracování přehledu řešené problematiky dle dostupných informačních zdrojů: 07/2013 - 09/2012
3. Analýza zkoumané technologie: 10/2013 - 11/2013
4. Zpracování a zhodnocení výsledků analýz řešené problematiky: 11/2013 - 12/2013
5. Vytvoření návrhu řešení problematických míst zkoumané technologie: 12/2013
6. Tvorba finálního dokumentu diplomové práce: 01/2014 - 02/2014
7. Odevzdání diplomové práce 03/2014

Rozsah textové části
60-80 stran

Klíčová slova
obnova dat, odstranění dat, paměť, paměťové médium, uložení dat

Doporučené zdroje informací

DEMBOWSKI, Klaus. Mistrovství v hardware. Brno: Computer Press, 2009. 712 s. ISBN 978-80-251-2310-2.

HORÁK, Jaroslav. Hardware učebnice pro pokročilé. Brno: Computer Press, 2007. 360 s. ISBN 978-80-251-1741-5.

TIŠKOVSKÝ, Pavel. Technologie flash pamětí a způsoby jejich využití. Root [online]. 2008 Dostupný na World Wide Web: <http://www.root.cz/clanky/technologie-flash-pameti-a-zpusoby-jejich-vyuziti/>

HOK, Aleš. Kouzla s pevným diskem v programech True Image a Disk Director. Brno: Computer Press, 2006. 248 s. ISBN: 80-251-1040-0.

HORÁK, Jaroslav. Havárie počítače. Brno: Computer Press, 2007. 208 s. ISBN: 80-251-1451-1.

Vedoucí práce
Brechlerová Dagmar, RNDr., Ph.D.

Termín odevzdání
březen 2014

doc. Ing. Zdeněk Havlíček, CSc.
Vedoucí katedry

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE
Provozně ekonomická fakulta

prof. Ing. Jan Hron, DrSc., dr. h. c.
Děkan fakulty

V Praze dne 30.10.2013

Čestné prohlášení

Prohlašuji, že svou diplomovou práci " Obnova a mazání dat na úložných typech pamětí" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 31. 3. 2014 _____

Jindřich Vachata

Poděkování

Rád bych touto cestou poděkoval vedoucí mé diplomové práce paní RNDr. Dagmar Brechlerové Ph.D. za její odborné vedení a rady při zpracovávání diplomové práce.

Obnova a mazání dat na úložných typech pamětí

Recovering and erasing data from memory storage devices

Souhrn

Diplomová práce je zaměřena na problematiku obnovy a bezpečného mazání dat na datových médiích. Problematika je v práci teoreticky popsána od samotného principu ukládání, čtení, mazání dat na jednotlivých typech pamětí. Uvedena jsou základní rizika hrozící datům, způsoby a možnosti bezpečného odstranění dat, po možnosti obnovy nechtěně smazaných dat.

Ve vlastní části práce je zkoumáno obecné povědomí o této problematice. Experimentem na získaných médiích jsou dokazována rizika nedostatečného odstranění dat. Zjišťovány jsou také možnosti softwarové obnovy nezálohovaných dat, při simulovaných situacích neúmyslného smazání.

Summary

The thesis is based on problems with recovery and safe data erasing on data media. The issue at work is theoretically described by the principle of storing, reading and deleting data on various memory types. Listed are the basic risks for data, methods, options for safe data erasing and the recovery possibilities of accidentally deleted data.

In the inherent part of the thesis general awareness of this issue is explored. Risks of insufficient data removal were demonstrated by Experiments on acquired media. Also possibilities of software backup data recovery at simulated situations when unmeant deletions are detected.

Klíčová slova: obnova dat, bezpečné mazání dat, paměť, paměťové médium, uložení dat

Keywords: data recovery, safe data erasing, memory, storage media, data storage

OBSAH

1 ÚVOD 9

2 CÍLE PRÁCE A METODIKA 11

2.1 CÍLE PRÁCE 11

2.2 METODIKA 11

3 TEORETICKÁ VÝCHODISKA 12

3.1 PAMĚŤOVÁ MÉDIA 12

3.1.1 Magnetická 12

3.1.2 Optická 17

3.1.3 Polovodičové paměti (média) 24

3.1.4 Nevolatilní polovodičové paměti 25

3.1.5 Magneto optická 32

3.1.6 Souborové systémy 34

3.2 RIZIKA 37

3.2.1 Neúmyslná 37

3.2.2 Úmyslná 38

3.2.3 Snížení rizika šifrováním 38

3.3 MAZÁNÍ DAT 39

3.3.1 Operační systém 39

3.3.2 Metody založené na softwarových řešeních 41

3.3.3 Sanitace 43

3.3.4 Nedestruktivní strojová zařízení 44

3.3.5 Destrukce (Destruktivní strojová zařízení) 45

3.3.6 Zákony a legislativní opatření 47

3.4 OBNOVA 48

3.4.1 Obnova dat za použití zálohy 48

3.4.2 Obnova dat bez použití zálohy 51

4 VLASTNÍ PRÁCE 54

4.1 ANKETA - DOTAZNÍKOVÝ PRŮZKUM 54

4.1.1 Základní údaje o provedené anketě. 54

4.1.2 Zdroj respondentů. 55

4.1.3 Souhrnné výsledky dotazníku 55

4.2 EXPERIMENTY 61

5 ZHODNOCENÍ VÝSLEDKŮ A DOPORUČENÍ 72

6 ZÁVĚR 75

7 BIBLIOGRAFIE 76

8 SEZNAM POUŽITÝCH OBRÁZKŮ, GRAFŮ TABULEK 80

9 PŘÍLOHY 82

9.1 PŘÍLOHA Č. 1: STRUKTUROVÁNÍ DOTAZNÍKU 82

9.2 PŘÍLOHA Č. 2 KOMPLETNÍ VÝSLEDKY DOTAZNÍKOVÉHO ŠETŘENÍ 86

1 Úvod

V dnešní době, razantně narůstá objem různých dat, která jsou ukládána a archivována. Většina těchto dat v komerční i soukromé sféře je pro dané subjekty velmi důležitá a citlivá. S tím souvisí i potřeba možnosti obnovy nechtěně smazaných dat a trvalého bezpečného odstranění citlivých dat.

Ztratit data nechtěným smazáním nebo poškozením je podstatně snazší než následné získání dat zpět, u některých dat může být opětovné získání velmi časově a finančně nákladné. Proto je důležité zaměřit se již na prevenci a data chránit před možnými hrozbami ať úmyslnými či neúmyslnými.

Nejsnáze a nejúčinněji lze taková data chránit promyšleným pravidelným způsobem zálohováním, umožňujícím následnou rychlou a přesnou obnovu poškozených nebo smazaných dat. A to jak u soukromého zálohování na běžně dostupná úložná média, nejčastěji na pevné nebo optické disky, nebo u komerčního zálohování za použití speciálního softwaru a hardwaru, kde jsou velmi často využívána disková pole, případně pásková média atd. Tato řešení jsou samozřejmě finančně náročná a výše potřebné investice silně závisí od charakteru dat, organizace a velikosti objemu dat.

Stejně důležitá jako potřeba bezchybné a rychlé obnovy dat je i potřeba bezpečného a trvalého odstranění citlivých dat, aby se zamezilo jejich úniku a zneužití a tím následným finančním či jiným ztrátám.

Je až s podivem, jak malá je informovanost v soukromé sféře o bezpečném smazání dat, které by znemožnilo jejich obnovu. Proto velká skupina soukromých osob nakládá lehkovážně s daty na paměťových mediích, což umožňuje velmi snadné zneužití. Nejčastěji se tak děje při prodeji, půjčení, či likvidaci paměťového média v domnění, že na něm již nejsou žádná citlivá data.

Oproti tomu v komerční sféře je toto téma hojně diskutované, zvláště u finančních institucí, či institucí/firem uchovávajících citlivé osobní údaje, kde musí být dodržovány i zákonem stanovené podmínky, vyplývající například ze zákonů o ochraně osobních údajů 101/2000 Sb., o utajovaných informacích 412/2005Sb. a dalších.

Na problém bezpečného mazání dat se ovšem nelze dívat jen z pohledu typu dat, ale také z pohledu, jak a kde jsou data uložena. Především nesmíme opomenout faktory, které jsou například: technologie zápisu dat, forma zápisu, souborový systém. V neposlední řadě musíme zohlednit i obecně platné standardy pro mazání dat, zaručující jejich bezpečnou likvidaci.

2 Cíle práce a metodika

2.1 Cíle práce

V diplomové práci bude prozkoumána problematika ukládání a odstranění dat na různých paměťových médiích.

Hlavním cílem je zhodnocení a návrh možnosti obnovení nechtěně smazaných dat a navrhnout bezpečné a trvalé odstranění dat.

2.2 Metodika

Vypracování práce předchází studium odborné literatury a dalších zdrojů pocházejících převážné z odborných webů a studií.

Ze získaných znalostí bude vycházet zpracování teoretických východisek o ukládání dat na datových médiích, bezpečného mazání a obnovy dat.

Na základě tohoto zpracování bude realizován průzkum a experimenty ověřující tato teoretická východiska za pomocí softwarových nástrojů Recuva a ActiveBootDisk.

Závěry budou vytvořeny na základě syntézy získaných teoretických a praktických poznatků.

3 Teoretická východiska

Problematika mazání a obnovy dat velmi úzce souvisí s principem a technickým provedením uložení dat na příslušné paměťové medium a uchování těchto dat. Bez znalosti, jak jsou data fyzicky na paměťovém médiu uložena, nelze plně pochopit a aplikovat jak obnovu, tak mazání. A pokud víme, jak jsou data uložena a jak funguje jejich obnova, jsme schopni mazat citlivé informace tak, aby je už nikdy nikdo nedokázal přečíst.

3.1 Paměťová média

Tato kapitola se zabývá technickými aspekty, principy ukládání, uchovávání a mazání dat na jednotlivých médiích.

Základně si paměťová média můžeme rozdělit do tří skupin podle typu záznamu na magnetické, optické a polovodičové (elektronické).

3.1.1 Magnetická

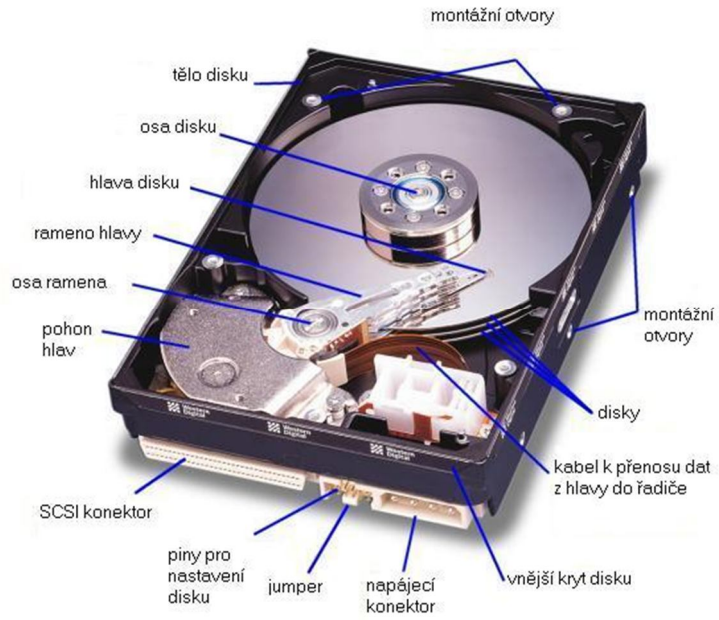
Dnes se používají pro největší množství uchovávaných dat, se kterými aktuálně nepracuje procesor, magnetická média uchovávající informace i po odpojení od elektrického proudu. Hlavní tři typy magnetických médií jsou pevné disky, diskety a magnetické pásky. U magnetických médií se využívá principu magnetické hystereze jejich datové vrstvy. Magnetický materiál datové vrstvy si díky ní „pamatuje“ intenzitu magnetického pole i poté, co na něj toto pole přestalo působit, protože se změní prostorová orientace magnetických dipólů materiálu. (1)

3.1.1.1 Pevné disky

Pevný disk je nejpoužívanější médium pro ukládání dat, proto je zde jeho detailnější rozbor. Je používán zejména pro svou velkou kapacitu, která v současné době dosahuje u pevných disků až 4Tb a náhodný přístup k datům (Random Access Memory). Pevný disk se skládá z mechanických a elektronických komponent viz obr 1.

Aby bylo možné zaznamenat data na disk v magnetické podobě, musí být povrchová vrstva „ploten“ magnetická. Dnes se jako materiál „ploten“ používají hlavně slitiny hliníku, pro jejich pevnost a mechanickou stabilitu (novinkou jsou plotny

ze speciálního skla). Na hliníkový nosič je nanesena magnetická vrstva „datové médium“ tato vrstva musí být magneticky tvrdá, aby bylo dosaženo velké bitové hustoty. Nanášení je prováděno galvanizováním nebo naprašováním, vrstva má tloušťku 0,05 až 0,2 µm. Nakonec je nanesena tenká tvrdá vrstva například grafitu, aby chránila povrch média před mechanickým poškozením při havarijním dotyku čtecích nebo zapisovacích hlav. (2 str. 895)



Obrázek 1 Pevný disk (2)

Samotná schopnost čtení a uložení je postavena u všech médií na určitém principu zjištění informace na základě změny. Při ukládání dat nejde jen o uložení nějaké skupiny dat, na povrch média, ale je třeba určit, kde bit končí a kde začíná. K tomu jsou používány různé metody.

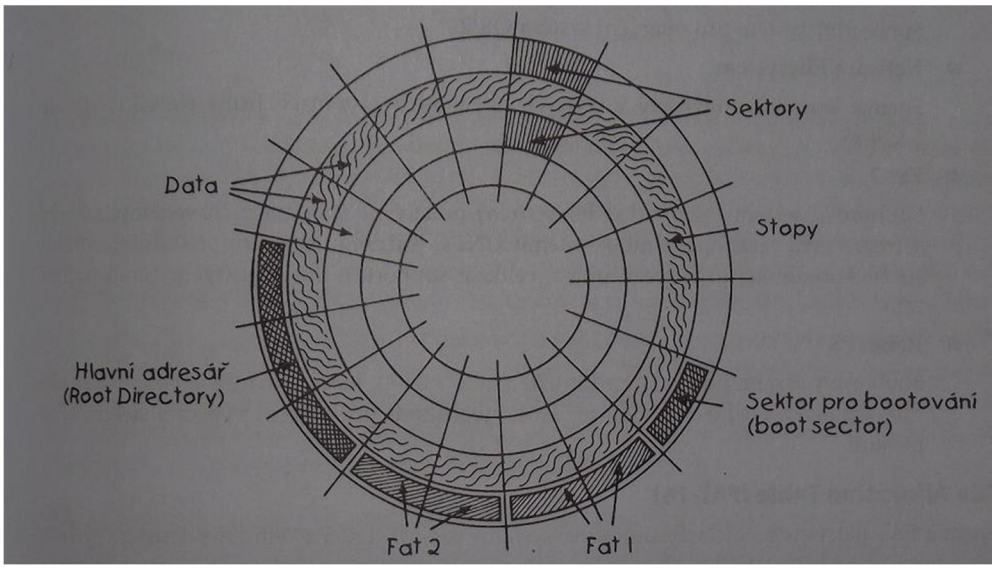
Pro objasnění například metoda FM (Frequency Modulation), tato metoda pracuje na principu změny magnetického toku. Magnetický tok se mění pouze při hodnotě 1 při hodnotě nula zůstává konstantní, pro zápis jedničky je nutno změnit velikost magnetického toku celkem dvakrát, pro záznam nuly pouze jednou, aby bylo možné zjistit, kde končí nebo začíná bit, v případě řady jedniček či nul vysílá se před každým datovým bitem speciální synchronizační impuls, dnes se již tato metoda nepoužívá, nebyla optimálně

využita kapacita disku, zde je uvedena, protože je její princip nejsnáze pochopitelný, tuto metodu nahradily následující, MFM (Modified Frequency Modulation),RLL (Run Length Limited), ARLL (Advanced Run Length Limited) a další. (4 str. 165)

Pevný disk obsahuje více „ploten“, jak je vidět na Obr. 1 a má data zapsána z obou stran v soustředných stopách, rozdělených do sektorů. Čtecí/zapisovací hlavičky jsou pevně spojeny, čtení/zapisování probíhá tudíž na stejně položených stopách a sektorech nad sebou, (sektory nad sebou jsou označovány jako cylindry).

Povrch disku je rozsáhlý prostor s obrovskou hustotou zapsaných dat. Pokud tedy operační systém požaduje od disku data, musí je na jeho povrchu vyhledat řadič disku. Ten potřebuje znát přesnou adresu (geometrickou polohu) dat. Proto je povrch disku rozdělen právě na stopy a sektory, které jsou adresovány. Do příslušné polohy dle adresy stopy a sektoru jsou hlavičky přesunuty dnes již výhradně pomocí vystavovací cívky.(5 str. 132)

Stopy a sektory jsou vyznačeny nízko úrovňovým formátováním. Dnes jsou všechny pevné disky nízko úrovňově naformátovány výrobcem. A neodborné nízko úrovňové formátování je může poškodit či zničit, to ovšem nemusí být hned patrné. U disků IDE, lze většinou najít na stránkách výrobců i speciální program na nízko úrovňové formátování daného disku bez rizika poškození. Toto formátování by se ovšem mělo provádět jen v závažných situacích například poruch. (2 str. 910)



Obrázek 2 Znázornění uspořádání pevného disku souborový systém Fat (3 str. 171)

Oproti tomu vysokoúrovňové formátování provádí běžně sami uživatelé pomocí příkazu formát. Při tomto formátování se vytváří pouze logická struktura příslušného diskového oddílu (souborový systém). To zahrnuje také vytvoření bootovacího sektoru a pro příklad u souborového systému FAT32 2x tabulku FAT a kmenový adresář. Všechny záznamy v tabulce FAT jsou primárně nastaveny na hodnotu 00h, indikující prázdný oddíl (volný prostor pro ukládání informací). Více v podkapitole „Souborový systém".

Příkaz vysokoúrovňového formátování provádí jen formátování určeného logického oddílu, pokud jich je na disku více, ne však celého disku. Chceme-li disk rozdělit na více logických oddílů, musíme je nejprve (po nízkoúrovňovém formátování), nastavit pomocí speciálního programu např. FDISK, ten vytvoří příslušné oddíly a tabulku oddílů. Až tyto oddíly můžeme naformátovat (vytvořit v nich určitý souborový systém). (4 str. 171)

Důležité z pohledu této práce je, že při vysokoúrovňovém formátování pevného disku je přemazána jen logická struktura, fyzicky jsou data i nadále k dispozici. Mnohé programy pak mohou, opět obnovit zformátovaný oddíl ve velmi krátkém čase. "*Při zničení více než jednoho souboru adresářů, je obnovení původní struktury adresářů a souborů mnohem složitější. .... U původně fragmentovaných adresářů a souborů jsou takové programy téměř bez šancí. Proto existují rezidentní programy, které se „zařadí" do všech operací pevného disku a navíc v rezervovaných sektorech uloží logickou strukturu pevného disku. Příslušný obnovovací program zná rezervované sektory, a protože vysokoúrovňovým formátováním se zničila jen logická struktura pevného disku, nikoliv však data samotná, může být informací uložených v rezervovaných sektorech obnovena logická struktura pevného disku."* (2 str. 910)

3.1.1.2 Diskety

Kvůli velkým nákladům a nízké kapacitě disket, je postupně nahradily CD-R/RW, DVD-R/RW/RAM, flash USB disky a další paměťová média. Dnes se již prakticky nepoužívají. Proto jsou jen stručně zmíněny.

Diskety jsou paměťová média skládající se z plastového obalu a vnitřního disku s magnetickou vrstvou, tento disk je na rozdíl od pevného disku ohebný. Vnitřek plastového obalu tvoří vystýlka chránící magnetickou vrstvu před poškrábáním. Princip

uložení dat je obdobný jako u pevného disku. Liší se ovšem formátování, při formátování diskety dochází k přepsání i datového prostoru. (2 str. 894) (1)

Nevýhodou disket, jak již bylo zmíněno, je jejich nízká paměťová kapacita 1,44 MB u nejčastějšího typu 3,5" palce a tím způsobená vysoká cena za GB paměti, i když se na trhu objevily v polovině 90 let i diskety s kapacitou až 750Mb (Iomega ZIP). Tyto diskety se díky své vyšší ceně, ale příliš na trhu neprosadily.

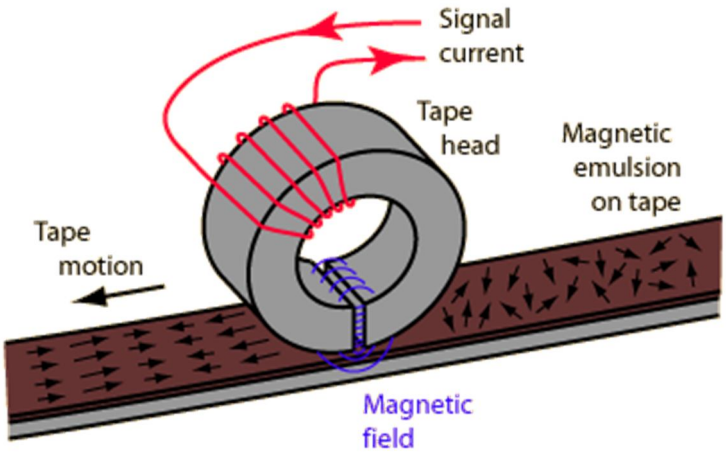
3.1.1.3 Magnetické pásky

Magnetická páska je jedním z nejstarších typů paměťového média, které se používá dodnes pro zálohy/archivaci obrovského množství dat. Na trh byla první uvedena již více než před 60 lety. (6)

Materiálem pásky bývá polyesterová fólie, případně materiál s obdobnými vlastnostmi, na kterou je z jedné, ale častěji z obou stran nanesena magnetická vrstva, tvořená práškem oxidu železitého rozpuštěného v epoxidové pryskyřici. Tato vrstva je stejně jako u pevných disků široká v řádu mikrometrů. Délka některých pásek přesahuje i 1 km a rekordní kapacita pásky uvedené firmou Oracle na trh v roce 2013 dosahuje 8,5 TB. (7) (1)

„Páska se při čtení či zápisu dat pohybuje konstantní rychlostí pod čtecí a zápisovou hlavou (může se jednat i o kombinovanou čtecí/zápisovou hlavu), která je na pásku pod určitým tlakem přitisknuta. Zápis probíhá tak, že se podélně či příčně zmagnetizuje malá část pásky pomocí zápisové hlavy, která obsahuje cívku s jádrem přerušeným úzkou mezerou. Mezera se nachází přesně nad páskou, tj. magnetické pole se v tomto místě z jádra rozšiřuje i přes pásku, jejíž magnetické dipóly jsou tímto polem natáčeny žádoucím směrem a díky tomu, že oxid železitý je feromagnetická látka, je orientace dipólů zachována i po posunu dotčeného místa pásky mimo dosah zápisové hlavy (takový záznam může v ideálních podmínkách vydržet i několik desítek let, mnozí majitelé osmibitových počítačů i dnes dokáží načíst původní data stará více než dvacet let). Čtení zapsaných dat je založeno na tom, že pohybující se páska vybudí ve čtecí hlavě napěťový impuls, z jehož polarity je možné zjistit, zda na pásku byla zapsána bitová hodnota 0 či 1. Pásky určené pro profesionální počítače (mainframy apod.) měly typicky devět datových stop a tím pádem i čtecí/zápisové hlavy obsahovaly stejný počet vinutí a čtecích zesilovačů

(osm stop bylo určeno pro záznam dat, devátá stopa například pro záznam paritního bitu).“ (1)



Obrázek 3 Znázornění zápisu na magnetickou pásku (zde magnetická páska stero kazety) (4)

Nevýhodou magnetických pásek je sekvenční přístup, s čímž souvisí dlouhá přístupová doba k datům.

3.1.1.4 Specifika bezpečného mazání a obnovy vyplývající z fyzického principu magnetických médií.

Na bezpečné smazání dat a obnovu hlavně za použití speciálních strojů má specifický vliv u magnetických médií koercivita což je schopnost odolat demagnetizaci externím nebo vlastním magnetickým polem, také teplota, při níž je zápis proveden. Při vyšší teplotě dochází k hlubšímu zmagnetizování. Proto se v praxi používají zařízení zařazená do skupiny degauser. Toto zařízení vytváří dostatečně velké magnetické pole, aby bezpečně demagnetizovalo a tím smazalo veškerá magnetická média. Jinak je vždy teoretická možnost magnetické médiu přečíst například metodou MFM a data obnovit. Více v kapitolách „Mazání“ a „Obnova“.

3.1.2 Optická

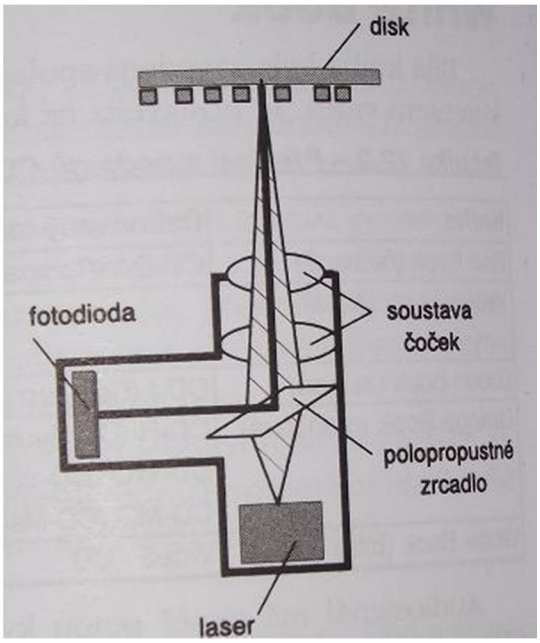
Optická média jsou dnes významně používána pro ukládání množství dat (video, audio, datové soubory atd.). Tyto média jsou, dobře známé optické disky CD (Compact Disc), DVD (Digital Versatile Disc), Blue-ray (BD) a jejich varianty, bližší specifika jsou u jednotlivých médií a jejich variant uvedena v této kapitole.

3.1.2.1 Základní technické parametry/princip

Optické paměti (disky) fungují na principu snímání odrazu laserového paprsku, který prochází datovou vrstvou na médiu. Standardní optické médiu je disk, který má průměr 120mm (80mm) s otvorem 15mm uprostřed a tloušťkou 1,2 mm. Oproti pevným diskům, jež mají data uložená v soustředných kruhových stopách a sektorech, jsou u optických médií uložena data v souvislé spirálové stopě o délce několika km, která je rozdělena na stejně velké sektory neboli bloky.

Nejmenší adresovatelnou jednotkou optického disku je právě jeden sektor, jehož vnitřní struktura se liší v závislosti na použitém režimu a podle toho je také doplněna datová část různými hlavičkovými a paritními bity.

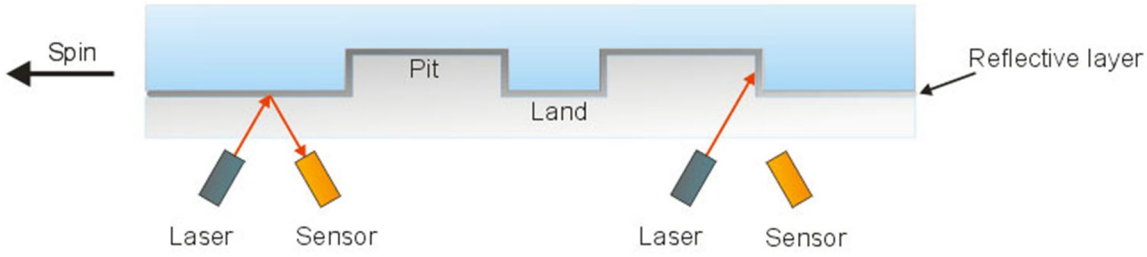
Informace jsou v sektorech uloženy principiálně ve formě malých prohlubní (dále je používán anglický název pit) a výstupků (land) nestejné délky. Laserový paprsek se při čtení média pohybuje po spirálové stopě, proto je nutno měnit rychlost otáčení disku v závislosti na poloze čtecí hlavy. To zajistí, aby se jednotlivé pity a landy četly konstantní nastavenou rychlostí. (5 str. 206)



Obrázek 4 Princip čtení u optických disků (5 str. 206)

Přechod z pitu na land (z prohlubně na výstupek) je interpretován jako 1, nastane-li úsek bez přechodu, je interpretován jako nula (např. každých 300 nm u CD). Paprsek vycházející z laserové diody se zaostří přes čočku na disk, a dopadne-li na pit (jak je

znázorněno na obr. 5), je rozptýlen, pokud na land, odrazí se zpět na senzor, tuto změnu zaznamená fotobuňka, kde vznikne elektrický impulz dále zpracovávaný řadičem a vyhodnotí se jako 1.

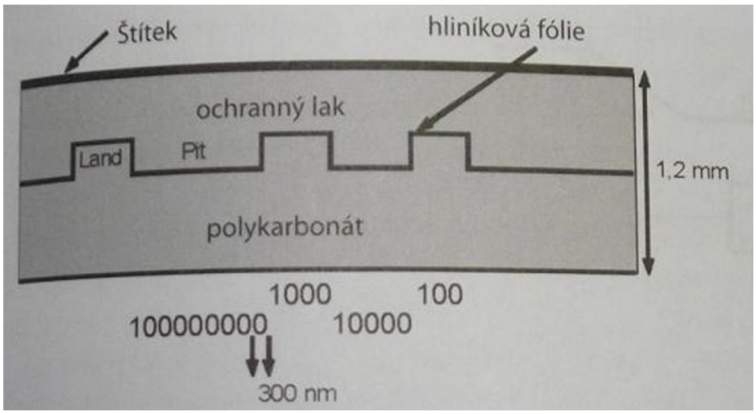


Obrázek 5 Přechod z pitu a land (6)

Při otáčení disku dochází k snímání jeho povrchu a tím je vytvářen digitální obraz disku. Není ovšem možné zaznamenat dvě jedničky vedle sebe, proto je nutné provést převod bitů (metoda EFM), data se tak převádí z 8 bitového kódování na 14 bitové (Channel Bits) (4 str. 280)

3.1.2.2 CD - ROM / R

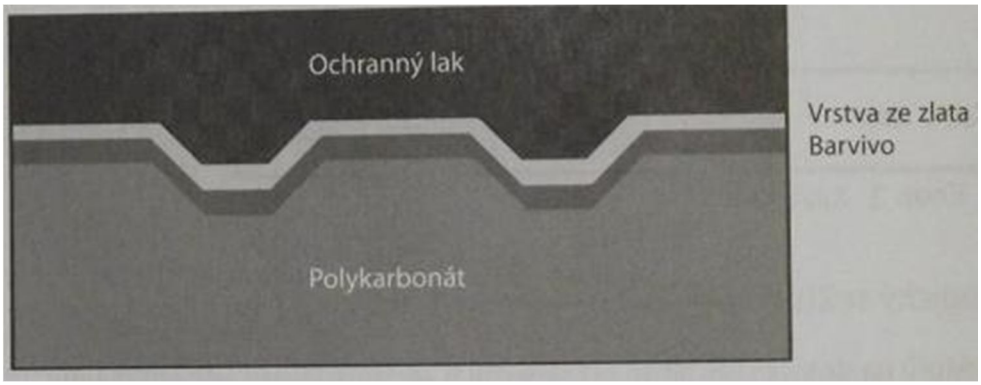
Médium označované jako CD-ROM se vyrábí lisováním, kdy se roztavená hmota tvaruje pomocí matrice. Tato matrice obtiskne do hmoty pity a landy. Takto vyrobený optický disk je ovšem průhledný a nebylo by možné ho číst. Je na něj tedy nanesena tenká reflexní fólie (nejčastěji hliník). Následně vrstva ochranného laku a nakonec je pomocí sítotisku na disk nanesen štítek. Tento disk, již z principu své výroby, obsahuje nesmazatelně data. (4 str. 280) Životnost disků je udávána firmou Verbatim až 100 let.



Obrázek 6 Struktura disku CD-ROM a znázornění uložení dat (3 str. 281)

Podstata média CD-R je velmi podobná CD-ROM, také se vyrábí z polykarbonátu a data jsou čtena stejným způsobem. Zápis i vrstvy se ovšem liší, na rozdíl od CD-ROM kde jsou data (pity a landy) vylisovány přímo při výrobě, jsou zde vypalovány zapisovacím laserem, který pro vypalování používá řádově vyšší energii než pro čtení dat. Toto médium je taktéž nepřepisovatelné, protože zápis nevratně mění zapisovací vrstvu, na celé médium lze na rozdíl od CD-ROM přidávat data postupně než dojde k jeho plnému zaplnění, pokud není médium při vypalování uzavřeno. (7)

Nové médium tohoto typu obsahuje stopu, sloužící k vedení zapisovacího paprsku a informace o čase sloužící, k určení lokace místa, ve kterém se právě paprsek nachází. Tato stopa je překryta vrstvou obsahující organické barvivo, sloužící pro ukládání dat. Za vrstvou barviva se nachází vrstva tvořená nejčastěji zlatem nebo stříbrem sloužící k odrazu paprsku. Tato vrstva je překryta opět vrstvou ochranného laku. (7)



Obrázek 7 Znázornění vrstev CD-R (3 str. 284)

Při vypalování (zaznamenávání dat) se nejedná o fyzické vypálení pitů, silný laserový paprsek pouze změní optické vlastnosti vrstvy barviva. Vrstva barviva je částečně průsvitná na místech, kde nejsou vytvořeny pity, v místě kde je vypalovacím laserem vytvořen pit dojde ke změně odrazivosti a snímač je schopen tento rozdíl zachytit. Změnu a rozsah zaplněné plochy disku jsme, schopni rozeznat částečně i pouhým okem, pokud není disk zcela zaplněn je na něm z dolní strany, zřetelně vidět zaplněná část jako tmavší. (1) (2)

Médium CD-R je ovšem díky použití vrstvy barviva citlivější. Nesmí se proto vystavovat vysokým teplotám a dlouhodobému působení přímého slunce. Také je náchylnější na fyzické poškození (poškrábání atd.). Životnost tohoto média je odhadována na desítky let. (2)

3.1.2.3 CD-RW (ReWritable)

CD-RW se od předešlých optických disků liší především tím, že umožňují opakovaný zápis na disk. K tomu využívají technologii fázových změn. Jejich nosná vrstva je složená opět z polykarbonátu, obsahují také reflexní a ochranné vrstvy jako u předešlých médií. Podstatný rozdíl je ovšem v datové vrstvě, materiál pro tuto vrstvu obsahuje řadu látek (selen, germinium atd.). To umožňuje, že při zahřívání dokáže malá oblast vrstvy přecházet z krystalické (pravidelné struktury) do amorfní (nepravidelné). Zahřívání (vypalování) je realizováno zapisovacím laserem, dvěma teplotami. Při nižší teplotě zahřátí následně vzniká při ochlazování krystalická struktura a při vyšší amorfní. Amorfní vrstva propouští méně záření (má menší odrazivost) než krystalická a díky tomu dokáže snímač číst stopu obdobně jako u CD-R/ROM ovšem musí být daleko citlivější, protože odrazivost je nižší. (2) (1) (10)

Schopnost zapisovat na tyto média opakovaně jim dává právě přechod mezi amorfní a krystalickou fází. Pro vymazání nosiče se jednoduše amorfní oblasti vystaví nižší teplotě a tím přejdou opět na krystalickou. Není proto nutné provádět jiné operace k odstranění dat (změna struktury umožní právě nový zápis na disk). Na udržení možnosti opakovaného zápisu dat a uchování informací má podstatný vliv chemické složení datové vrstvy, ale také vrstvy ochrany dat viz obr. 8. Ty ovlivňují rychlost chladnutí a vylepšují optické čtení. Životnost těchto disků se odhaduje na 30 let a až 1000 přepsání. (7)

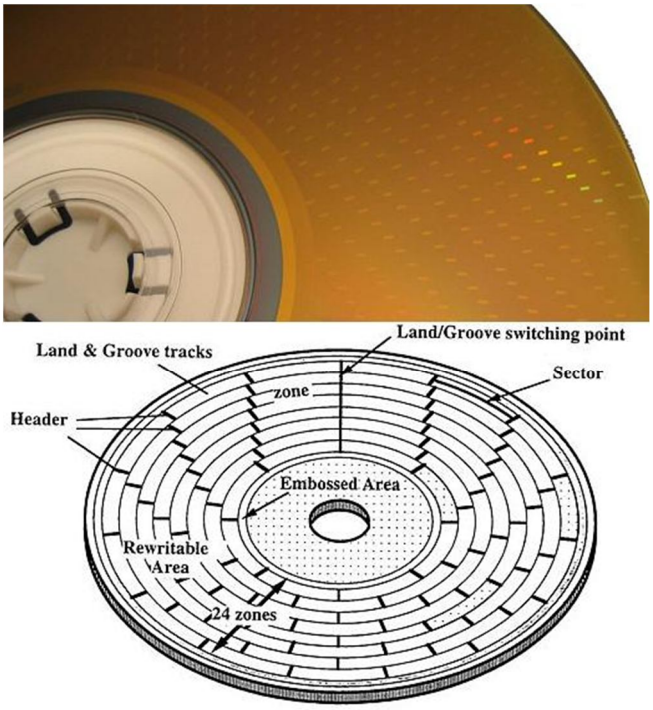
Obrázek 8 Znázornění vrstev CD-RW (3 str. 286)

3.1.2.4 DVD R/RW

Princip zápisu a čtení je stejný jako u CD R/RW, disk má i stejné rozměry. Rozdíl je, že došlo ke zvýšení hustoty zápisu dat. Toho bylo docíleno přesnějším laserem, zaostřením a jeho vlnovou délkou. Toto médium může být také dvojvrstvé, to znamená, že obsahuje dvě datové vrstvy. Při čtení je paprsek vždy zaostřen na jednu vrstvu. Na trhu jsou i oboustranná média, tato média jsou jakoby dvě slepená DVD horní stranou k sobě. Čtení je možné, ale pouze z jedné strany, proto je nutné médium při čtení druhé strany otočit. (5 str. 225)

3.1.2.5 DVD-RAM

Je optické médium (někdy je mylně považováno za optomagnetické). Od ostatních typů optických médií se ovšem odlišuje. Především uspořádáním dat, jsou-li data uspořádána do stop, majících kruhovou podobu se společným středem. Tyto stopy jsou dále děleny na jednotlivé sektory (podobně jako na pevném disku). Jednotlivé stopy a sektory jsou patrné pouhým okem, viz obr. 9. (8)



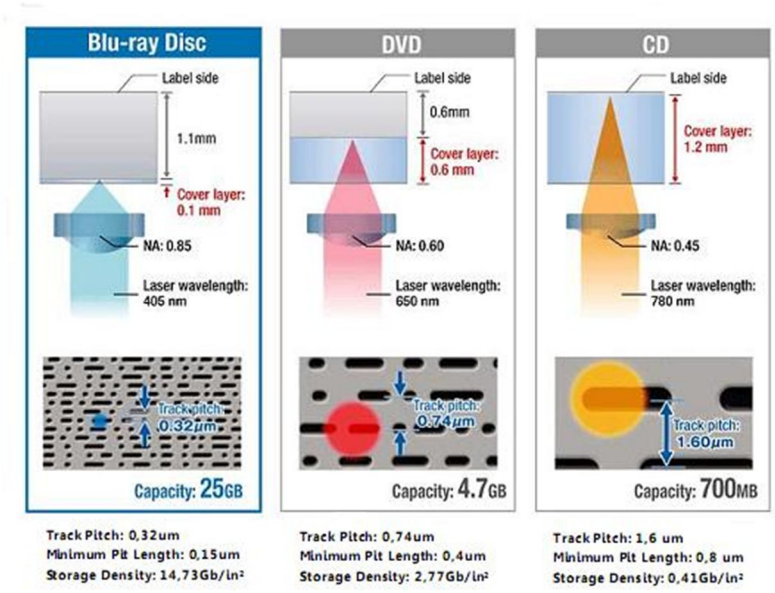
Obrázek 9Reálný pohled a schéma média DVD-RAM (8)

Nejdůležitější vlastností tohoto média je schopnost zapisování paketů hardwarově. Mechaniku s vloženým DVD-RAM diskem lze používat jako klasický pevný disk, tento disk lze naformátovat dle požadavků (např. FAT32, Ext2FS, UDF atd.). (12)

Nevýhodou tohoto média je ovšem ve většině případu nutnost speciální mechaniky podporující tento formát. Na trhu jsou k dostání dva typy klasický disk, cena se dnes (2014) pohybuje okolo 50Kč a disk s ochranným rámečkem, výhoda druhého provedení je zvýšená ochrana a prodloužení životnosti média, je bohužel vždy nutná speciální mechanika, další nevýhodou je horší dostupnost těchto médií a mechanik. Výhodami tohoto média naopak jsou možnost přepsání až 100 000 krát, práce jako s pevným diskem a životnost až 30let. Tyto disky jsou výhodné jako archivační média díky snadné práci, přepisovatelnosti a dlouhé životnosti. (11) (12)

3.1.2.6 Blu-ray

Je poslední typ optického paměťového média uvedený na trh. Princip zápisu vrstev a technické parametry disku jsou obdobné jako předem popsaných CD a DVD. Proto zde nebudou do hloubky rozebírány. Zásadní rozdíl je, že byl použit laser s výrazně kratší vlnovou dálkou než u CD a DVD. Tím bylo dosaženo zmenšení pitů a landů a zhuštění záznamové stopy. Kapacita média se u Blu-ray zvětšila na 25 GB u jednovrstvého a na 50GB u dvouvrstvého média.



Obrázek 10 Znázornění všech rozdílů u jednotlivých optických médií (9)

Při zhuštění stopy a zmenšení pitů, vyvstal problém s disperzí úzkého paprsku. Odstraněn byl zmenšením tloušťky polykarbonátové vrstvy na čtecí straně média (jak je vidět na obrázku). To má ovšem za následek horší a menší odolnost dat uložených na médiu proti poškrábání. Naproti tomu, že je datová vrstva díky blízkosti k povrchu zranitelnější, je možné kombinovat Blu-ray se záznamem kompatibilním s DVD. (9)

3.1.2.7 Specifika bezpečného mazání a obnovy vyplývající z povahy optických médií.

U nepřepisovatelných optických médií především u médií lisovaných nelze záznam nijak bezpečně nedestruktivně odstranit. To je způsobeno fyzickou povahou dat zapsaných na médiu. U poškozeného média, (není-li zcela zničena datová vrstva) lze data, i když je médium například rozlomené, pomocí speciální techniky přečíst a restaurovat. Zejména neefektivní je poškrábání média z dolní strany což sice vede k nežádoucím lomům čtecího paprsku, ale pokud není poškozena i datová vrstva, data lze obnovit. U přepisovatelných médií lze tato média přepsat několikrát dle speciálního algoritmu (popsaných v kapitole mazání) a tím dosáhnout neobnovitelnosti dat.

3.1.3 Polovodičové paměti (média)

V zásadě si polovodičová média a paměti lze rozdělit na volatilní a nevolatilní (závislé na napájecím napětí a nezávislé na napájecím napětí). Volatilní paměti nejsou příliš důležité z pohledu práce z důvodu, že dlouhodobě neuchovávají data, proto je jen krátce zmíním.

3.1.3.1 Volatilní polovodičové paměti

Volatilní polovodičové paměti se vyznačují, především vysokou rychlostí (nízkou přístupovou dobou), v porovnání s ostatními typy pamětí a médií. Další společnou vlastností je, že pokud dojde k přerušení napájecího napětí, jsou data ztracena. Jejich použití je u:

Registrů procesoru

Velmi malá, ale velmi rychlá paměť nacházející se v mikroprocesoru. Registry slouží zejména k dočasnému uložení operandů, se kterými se v procesoru provádějí např. aritmetické a logické operace. Velikost registrů proto bývá zpravidla stejná jako velikost

slova procesoru nebo jeho násobku. Tyto paměti jsou statické a tvořeny klopnými obvody zabudovanými přímo v procesoru. (7)

Cache

Jsou používány jako vyrovnávací paměti mezi dvěma subsystémy s různými rychlostmi. Jejich hlavní účel je urychlit přístup k často používaným datům uložených na pomalejších pamětích. Tyto paměti jsou kapacitně v řádech KB až MB a jsou typu SRAM. (2)

Operační paměť

Je rychlá paměť mezi procesorem a zbytkem PC komponent (hlavně pevným diskem) sloužící k udržení neustále používaných dat (operační systém) nebo aktuálních dat zpracovávaných procesorem. Operační paměť je dynamická, na rozdíl od registrů procesoru typu a je to také paměť s náhodným přístupem. Tyto paměti jsou označovány (DDRčíslo SDRAM a typ SIMM, DIMM, RIMM v dnešní době se převážně používají paměti DDR2 a 3 SDRAM DIMM). Dnes jsou velikosti těchto pamětí v řádu gigabytů u serverů až ve stovkách gigabytů. (2)

3.1.3.2 Specifika bezpečného mazání a obnovy vyplývající z povahy volatilních pamětí.

Jak je patrné již ze samé podstaty těchto pamětí, informace se bez přívodu elektrického napětí ztrácí. Důležité je si uvědomit, že tato ztráta není okamžitá, ale dochází k ní v řádech milisekund až sekund. Tato data se v řádech minut stávají rovněž prakticky neobnovitelná. V extrémních a laboratorních prostředích je možné data uchovat i v řádu hodin.

3.1.4 Nevolatilní polovodičové paměti

Po zapnutí počítače nejsou ve volatilních pamětech uloženy žádné relevantní informace, ani instrukce, které by mohl mikroprocesor začít zpracovávat. Z tohoto důvodu obsahují všechny moderní počítače kromě volatilních pamětí i nevolatilních pamětí, jejichž obsah není spolu s přerušením napájecího napětí ztracen. (10)

ROM

Technologicky již ne příliš používaná paměť, nahradily ji dále zmíněné paměti. Data do této paměti byla zapisována při výrobě. Kde hodnota jedna, byla konstrukčně realizovaná tranzistorem, který byl na vodivé cestě otevřen a nula tranzistorem, který byl uzavřen. (13)

PROM

PROM je elektronicky jednou programovatelná paměť. Obsahuje tranzistory, nebo diody a rezistory. Programování se provádí ve speciálním přístroji, je založeno na destruktivním přerušení spojů v těch místech, kde má být zapsána logická nula za pomocí napětí (20V). Její opětovný přepis není možný. (10)

EPROM

Je polovodičová paměť, jejíž čip si zachovává data i po odpojení elektřiny do té doby, než je paměť vystavena skrze okénko na horní straně čipu silnému UV záření (např. použitím světla z UV lampy), což paměť zcela vymaže. Tuto paměť tvoří řada plovoucích-bran tranzistorů programovatelných elektronicky za pomocí napětí, které je vyšší než běžně používané v obvodech (12V nebo 25V). (13)

EEPROM

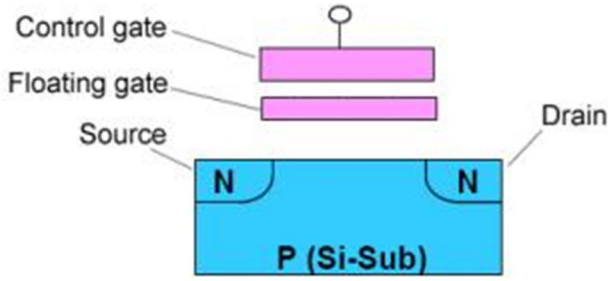
Polovodičová paměť, která je již elektronicky mazatelná. Tato paměť má díky své konstrukci ovšem omezený počet přepsání, daleko nižší než následující FlashPROM. Při výrobě se používá speciálních tranzistorů vyrobených technologií MNOS (Tranzistory, mají na řídící elektrodě nanesenou vrstvu nitridu křemíku a pod ní je umístěna tenká vrstva oxidu křemičitého.) Paměťová buňka pracuje následně na principu vkládání elektrického náboje na přechod. Zápis dat je proveden tak, že se na příslušný vodič přivede záporné napětí -U a datový vodič buněk, do nichž se má zaznamenat hodnota 1, se uzemní. Tranzistor se tím otevře a vznikne v něm náboj, to vede k velkému prahovému napětí. Při čtení přijde na adresový vodič záporný impuls. Ten zapříčiní, že tranzistor s malým prahovým napětím se otevře a umožní vedení proudu do datového vodiče, zatímco tranzistor s velkým prahovým napětím zůstane uzavřen.

Využití této paměti bylo dříve především pro ukládání firmwaru, dnes její funkci většinově přebrala FlashPROM. Jedním z důvodů byla i nutnost před novým programováním paměť celou vymazat. (13)

FlashPROM

Většinou se používá označení pouze Flash paměť. Představuje nástupce elektricky programovatelných pamětí typu EEPROM. Paměti typu Flash jsou dnes hojně používány v různých formách a médiích (paměťové karty, Flash disky, SSD disky, interní paměti) především v přenosných zařízeních (telefony, tablety, fotoaparáty, digitální kamery), protože paměti neobsahují žádné pohyblivé části, u kterých by vlivem otřesu mohlo dojít k havárii nebo vychýlení zapisovací/čtecí hlavy atd. Výhodou flash je i menší velikost médií, nižší energetická náročnost a rychlost, ta je ovšem ovlivněna celkovou konstrukcí paměťového média a použitou výrobní technologií. Paměť je navíc vnitřně organizována po blocích, to umožňuje programovat a přepisovat každý blok samostatně bez nutnosti smazání celé paměti. (10) (11)

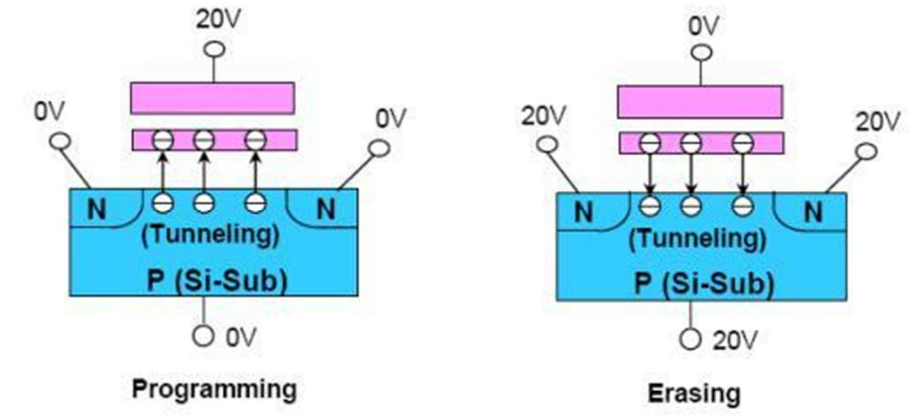
Paměť funguje na principu ukládání dat v poli unipolárních tranzistorů s plovoucími hradly viz obr. 11.



Obrázek 11 Konstrukce paměťové buňky (11)

Jedno hradlo je ovládací (značení CG „control gate) a druhé plovoucí (FG „floating gate“) izolované vrstvou oxidu. Protože FG je izolované, všechny elektrony na něj přivedené jsou zastaveny (uvězněny/uloženy) a tím je uložena informace. To zapříčiní částečné rušení elektrického pole z CG čímž je ovlivněno prahové napětí buňky, které ovlivňuje průchod proudu a tím je zjištěno, jestli je uložena 0 nebo 1. Buňky paměti jsou v základu nastaveny všechny na hodnotu 1. Vymazání uložených informací spočívá v

nastavení hodnoty hradla opět na 1 a je realizováno velkým záporným napětím přivedeným na CG a nebo napětím na zdroj „source“, to odvede uložené elektrony pryč kvantovým tunelem (vzniká takzvané tunelování znázorněno na následujícím obr.). Tak to lze ovšem vymazat pouze celé bloky, nebo sektory paměti. (15)



Obrázek 12 Programování a vymazání flash paměti typu NAND (11)

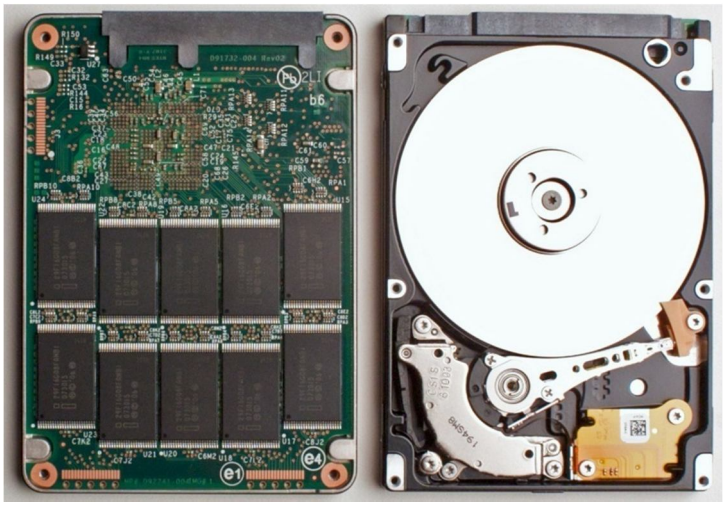
U těchto pamětí ovšem nastává problém s degradací buněk. Opakovaným přepisem se postupně opotřebovávají (množství přepisu závisí na technologii NOR 100 000 a NAND 1 000 000 cyklů), což vede na konec až ke ztrátě dat. Jedna vadná buňka navíc znemožňuje čtení ostatních zapojených do série. Proto je použito několik prvků ochrany dat. Například „Mass storage controller“, hlídající počet zápisů do buňky a vyřazující automaticky vadné bloky, dále ověřuje, jestli po každém vymazání jsou všude nastaveny 1 a po zápisu se ověřují zapsané 0. Dalším prvkem je „Flash Translation Layer“ sloužící k rovnoměrnému rozkládání zápisu na celé paměťové médium (defragmentaci), kdyby tento prvek neexistoval, paměť by zapisovala opakovaně do stejného místa (vždy například na začátek zatímco ostatní buňky by nebyly používány), tím by docházelo k degradacím a k postupnému poklesu kapacity až znehodnocení celé paměti. (14) (13)

Jak již bylo na začátku řečeno Flash paměti se vyskytují, v různých médiích. Nejdůležitější média a jejich parametry jsou SSD disky, Flashdisky a paměťové karty.

SSD disky

SSD disky se začínají značně rozšiřovat, vliv na to má zejména snížení ceny kapacity GB/Kč, kterou tlačí dolů jak vyšší objem výroby, tak konkurence dvou technologií SLC

(Single Level Cell) a MLC (Multi Level Cell). Zvětšení úložné kapacity (dnes běžně 256GB až 7,42 TB serverové s vnitřním raidem) a jejich rychlost (dnes běžně 550MB/s čtení a 520 MB/s zápis) oproti klasickým magnetickým pevným diskům. To vede k jejich začleňování i do složitých diskových polí a systémů (zde však dosahuje zápis a čtení násobných hodnot). Dále se již poměrně běžně vyskytují v noteboocích a především ultraboocích.



Obrázek 13 Rozdíl vnitřní konstrukce SSD a pevného disku (HDD)

Zdroj: (12)

Rozdíl mezi technologiemi SLC a MLC je v tom, kolika bitovou informaci je jejich paměťová buňka schopná uchovat a životností buňky. Velikost SLC paměťové buňky je 1 bit (0 / 1), zatímco velikost MLC paměťové buňky jsou 2 bity (00 / 01 / 10 / 11). To je způsobeno tím, že FG uchovává paměťovou (bitovou) informaci ve formě elektrického náboje (počtem elektronů). Čím více různých hodnot elektrických nábojů v FG jsme schopni naprogramovat (operace zápis) a následně detekovat (operace čtení), tím více informací můžeme do jedné paměťové buňky uložit. (15)

MLC je tedy technologie s vyšší, resp. dvojnásobnou hustotou zápisu vůči SLC. Toho je dosaženo tím, že vzdálenost ΔU mezi napěťovou hodnotou reprezentující logickou 0 a 1 je u SLC větší (tisíce elektronů) a u MLC (stovky elektronů). Velikost ΔU ovšem přímo úměrně souvisí se životností SSD buňky, takže větší ΔU znamená delší životnost. Je to dáno tím, že ne všechny elektrony při programování a mazání se přesouvají, jak mají. Některé elektrony neproniknout do FG nebo dokonce uváznout navěky v izolační vrstvě

oddělující FG. To vede k postupnému splynutí elektrických hodnot reprezentujících logické úrovně, a tím pádem ke zničení paměťové buňky. Proto mají MLC disky kratší životnost v porovnání s SLC. To neznamená, ale že u nich hrozí větší riziko ztráty dat. Tomu je zabráněno důkladnějšími opravnými algoritmy s větší režií, což nepatrně zpomaluje zápis na disk. (15)

Flashdisky

Je paměťové médium používané převážně jako náhrada za diskety, CD a DVD. Rozměrově se podobá klíčence nebo zapalovači a jejich výhodou oproti výše zmíněným médiím je odolnost proti magnetickému poli a zejména poškrábání vlivem častého přenášení. Samotné médiu se skládá z malé desky s plošnými spoji, na kterých jsou integrované obvody, které jsou chráněny obalem z plastu, kovu nebo pogumovaného. USB flash disk je napájen z USB portu. Data se na tento disk zapisují přes USB (2.0, 3.0) rozhraní. USB flash disky používají pro ukládání dat standard „USB Mass Storage“, který podporují všechny běžně používané operační systémy, jako je Linux, OS X, Windows a další systémy. Komerčně se začaly rozšiřovat od roku 2000, kdy je na trh uvedla společnost IBM s kapacitou 8MB, dnes (2014) jsou dostupné modely s kapacitu až 1TB. Způsob uložení a uchování dat je principiálně stejný, jak již bylo popsáno výše. Nerovnoměrnému opotřebení zabraňuje opět mezivrstva FTL rozkládající postupně data po celém médiu (defragmentovaně). (4 str. 353)

Paměťové karty

Paměťové karty slouží jako paměťová média v přenosných zařízeních (telefony, tablety, digitální fotoaparáty) díky výše obecně popsaným vlastnostem u polovodičových pamětí. Jejich prudký rozvoj souvisel především s rozvojem moderních telefonů a fotoaparátů, které potřebovaly odolné paměťové médium schopné uchovávat velké množství dat při malých rozměrech.

Existuje množství druhů paměťových karet např. Secure Digital High Capacity (SDHC), Multi Media Card (MMC) atd. Jednotlivé druhy paměťových karet se odlišují především velikostí, počtem pinů, kapacitou a rychlostí. U paměťových karet bývá přímo implementována i ochrana autorských práv DRM (Digital Rights management) jež omezuje například přehrávání hudby. Dnes jsou nejčastěji používány karty SD

a odvozené/vylepšené/zmenšené“ verze (SDHC, SDXC, microSD, microSDHC, miniSD atd.). (4 str. 353)

Obrázek 14 Znázornění množství typů paměťových karet

(Zdroj: http://www.infobarrel.com/media/image/58094.jpg)

Zajímavost

Velmi zajímavá je výroba ať již samotného čipu tak celé karty, nebo USB. Zrychlený náhled výroby lze nalézt na videu „*A Behind the Scenes Look: How We Make Our Products*“, zachycující výrobu ve firmě Lexar z USA.

www.youtube.com/user/LexarMediaInc

3.1.4.1 Specifika bezpečného mazání a obnovy vyplývající z povahy nevolatilního paměťového média

Polovodičové paměti ROM, PROM, kde jsou data zapsána bez možnosti přepisu, neumožňují jiný než destruktivní princip jejich bezpečného smazání. Zde je nutné vzít v potaz, že většina těchto pamětí neobsahuje tajné a citlivé informace (vyjma vojenských zařízeních jejichž jsou součástí). U pamětí typu EPROM je před opětovným zápisem nutnost paměti smazat z hlediska konstrukce, toto smazání prakticky znemožní jakoukoliv

obnovu dat, navíc paměti bývají pevnou součástí zařízení a opět vyjma vojenské a speciální techniky neobsahují citlivá data, u této techniky jsou čipy při odstranění fyzicky rozemlety. Obnova dat je u poškozených paměťových čipů složitá leč možná, ale z jejich povahy se neprovádí.

Složitější je situace u médií založených na Flash paměťových modulech (flashdisk, SSD disk, paměťové karty). Mazání probíhá plně elektronicky, jak bylo popsáno výše a vyvstává zde právě problém, že díky konstrukci a omezené životnosti dochází k postupnému obsazování paměťových buněk (FLT). To způsobuje, že jsou v paměti skrytě ukryta zbylá data, která je možné obnovit. Navíc studie „*Reliably Erasing Data From Flash-Based Solid State Drives*“ testy prokázala, že na SSD discích je zároveň několik kopií stejného souboru a protože je fyzická adresace souborů řízena přímo firmwarem, nelze s jistotou smazat jen jednotlivý soubor a všechny paměťové bloky ve kterých byl uložen. Ale musí být smazáno celé médium a ani to nezaručuje kompletní bezpečné smazání. (17)

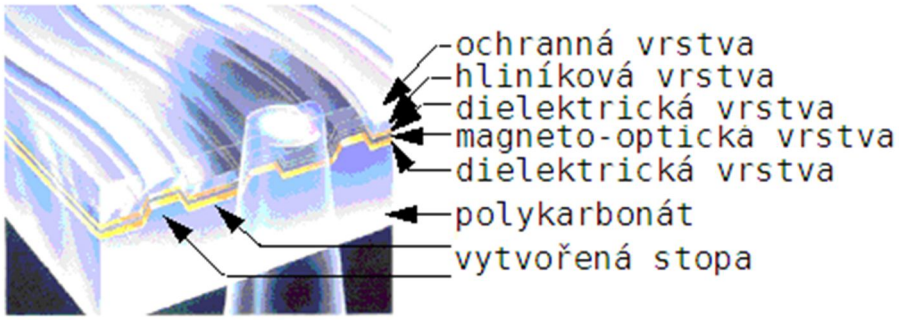
Částečně jiná je situace u moderních SSD disků ve spolupráci s moderním operačním systémem (například od WIN 7). Podporující funkci TRIM což je inteligentní mazání. „*Když ve Windows smažeme nějaký soubor, tak se fyzicky nesmažou odpovídající sektory, ale pouze se označí jako nepoužívané, takže je možno je přepsat. To je proto, aby mazání bylo rychlé, a pro klasický disk není rozdíl v zápisu nebo přepisu. Trim řeší to, aby se sektory označené jako nepoužívané smazaly“ (garbage collection)*.“ (18)

3.1.5 Magneto optická

V závěru této kapitoly by bylo vhodné zmínit magneto optická média. Tato média se v současné době nepoužívají příliš často, jejich funkci převážně nahradila jiná řešení a média, pro dlouhodobou úschovu cenných dat. Stále jsou ovšem využívána v některých finančních a vládních institucích díky velké odolnosti.

Magneto optická média využívají pro uložení dat princip změny magnetizace, ale pro zápis nebo čtení je použit laserový paprsek. Tím tyto disky kombinují přednosti magnetických (nedestruktivní, rychlí zápis po blocích) a optických (vysoká hustota dat, odolnost proti vnějším vlivům, bezdotykové čtení, jednoduchost mechanik atd.).

Magnetooptické disky mají stejné rozměry jako CD a jejich základ je tvořen polykarbonátovým diskem. Jím prochází laserový paprsek a dostává se na vrstvu o šířce 100nm tvořenou dielektrickým materiálem, následuje vrstva feromagnetického materiálu o tloušťce 30nm, dielektrická vrstva, odrazová vrstva tvořená hliníkem, překrytá ochrannou vrstvou laku. Materiály pro feromagnetickou vrstvu se liší dle výrobce. V polykarbonátové vrstvě jsou drážky pro vedení laseru. Drážky přispívají k rozkladu světla na magnetooptických discích, na nichž jsou viditelné i začátky jednotlivých sektorů, vytvořené mechanicky, rýhou kolmou na směr záznamu jako u DVD- RAM. (17)



Obrázek 15 Znázornění drážky a jednotlivých vrstev optomagnetického disku (13)

Zápis je oproti jiným technologiím specifický v tom, že „*je prováděn pomocí zapisovací magnetické hlavy a laserového paprsku. Feromagnetická vrstva na magnetooptickém disku je totiž vytvořena z materiálu, který je za běžných pokojových teplot možné zmagnetizovat pouze působením velmi silného pole, který zapisovací hlava nemůže vyvinout. Pokud se však teplota feromagnetické vrstvy zvýší nad takzvanou Curierovu teplotu, překoná náhodný pohyb atomů vnitřní síly působící spontánní magnetizaci a z feromagnetické látky se stává látka paramagnetická, na níž už relativně slabé magnetické pole zapisovací hlavy může působit. Teplota feromagnetické vrstvy je zvyšována laserovým paprskem, který je velmi přesně zaostřen právě na tuto vrstvu a dokáže zvýšit teplotu zápisového místa (to má velmi malou plochu) na cca 180 °C. Tento způsob záznamu umožňuje, aby byla zapisovací hlava umístěna v poměrně značné vzdálenosti od disku, protože případný rozptyl magnetického pole neovlivní okolní bity – na ně totiž laserový paprsek nesvítí, tudíž nemají dostatečnou teplotu.*“ (13)

Čtení dat je realizováno slabším polarizovaným laserovým paprskem (magnetická hlava se pro čtení vůbec nepoužívá), který je vlivem magnetizace materiálu pootočen.

Pro vyhodnocení je použit dvojlomný hranol, sestavený ze dvou krystalů opticky spojených pod úhlem 45°, z něhož dopadají paprsky na dvě fotodiody (detektory). Rozdíl oproti optickým médiím je v tom že u nich se indikuje útlum odraženého paprsku kdežto u magnetooptických úhel odražení, při přechodu mezi pity a lendy. (13)

Magnetooptické disky mají mnoho výhod, hlavní je vysoká odolnost dat i nosiče proti. Zničení dat nastává až při velké magnetizaci daleko větší než u čistě magnetických médií (zejména magnetické pásky). Nosič je sám o sobě chráněn pevným rámečkem před poškrábáním a dalším neduhům optických médií. Nevýhoda je ovšem vysoká cena technologie a horší dostupnost.

3.1.5.1 Specifika bezpečného mazání a obnovy vyplívající z povahy magnetooptických médií.

Tato média byla speciálně navržena pro uchování dat. Demagnetizace média je díky jeho velké odolnosti obtížná. Lze zde ovšem použít, algoritmy a metody pro pevné disky, které ve spolupráci se speciálním programem dokážou znečitelnit změny po předešlých datech a tím médium bezpečně vyčistit. Obnova dat z poškozeného média je proveditelná podobným způsobem jako u optického disku, vychází ze stejného principu čtení média.

3.1.6 Souborové systémy

Na obnovu a bezpečné mazání dat má vliv nejen fyzické uložení informace tedy 1 nebo 0, ale i samotné logické uložení dat. To do značné míry ovlivňuje, souborový systém což je nutné brát v potaz především při používání nástrojů pro obnovu dat nebo nástrojů pro destrukci dat pouze určených souborů (bezpečném mazání celého média nehraje souborový systém takovou roly).

Souborový systém určuje způsob ukládání dat na médium, nejčastěji je toto médium pevný disky, SSD disk, Flashdisk. Podle souborového systému se data organizují do souboru a následně do adresářové struktury. Dnes se běžně můžeme setkat s různými souborovými systémy, nejčastěji používané jsou NTFS, FAT32, FAT, exFAT, EXT (1,2.3), HFR. Dále jsou popsány základy třech běžně používaných souborových systémů.

3.1.6.1 Souborový systém FAT, FAT32

Tyto souborové systémy požívají adresáře s položkami obsahující bitmapu volných bloků, nazývané „File Allocation Table“ zjednodušeně FAT tabulky. Zde se jedná o seznam všech bloků, kde každá položka obsahuje informaci o následujícím bloku, hodnotu označující konec souboru, prázdný blok, vyřazený blok.

FAT32 se od FAT odlišuje velikostí adresovatelného prostoru a uloženého souboru. Kde u FAT je velikost adresovaného prostoru max. 4GB a souboru 2GB. U FAT32 je maximální velikost adresovatelného prostoru až 2TB a velikost souboru až 4GB.

Princip smazání souboru je realizován pouhým odstraněním záznamu o jeho existenci z FAT tabulky. Tento záznam i celý soubor je softwarově snadné obnovit.

3.1.6.2 Souborový systém NTFS

Dnes nejčastěji používaný lokální souborový systém, který nahradil FAT32 především kvůli zvýšení bezpečnosti. Tento souborový systém zaznamenává všechny změny na logické jednotce (jako meta data) a je postaven na řídících atributech souborů. I obsah souborů je jeho atributem. Většina datové struktury toho systému je reprezentována pomocí souborů. Samotný zaváděcí sektor disku je reprezentován jako soubor v seznamu souborů. Všechny soubory NTFS jsou udržovány v seznamu souborů ($MFT), tento soubor udržuje obdobně jako FAT informace o všech souborech, adresářích a metadatech. Jeho kopie je na rozdíl od FAT umístěna veprostřed logického prostoru a nikoliv na začátku (tato kopie ovšem neobsahuje kompletní záznamy, ale pouze prvních 16). Atributy souborů lze najít v seznamu souborů nebo pomocí odkazů uložených v jiných místech. Tento systém byl vytvářen pro Windows NT, ale ten nedokázal plně využít jeho potenciálu. Toho dosáhly až následující systémy s podporou NTFS. Maximální velikost souborového systému je 256TB a souboru 16TB. (14)

I přes zásadní odlišnosti je mazání a možná obnova dat velmi podobná jako u systému FAT a FAT32. To znamená, že v případě smazání souboru dojde v MFT k označení souboru jako smazaného, zápis ovšem nadále existuje. Clustry v metasouboru $Btimap jsou označeny jako volné/prázdné. Zde je ještě snadnější softwarově obnovit smazaná data, jelikož je k dispozici i záznam o smazaných souborech. (14)

3.1.6.3 Souborový systém EXT

Jedná se o Unixový souborový systém, jehož základem jsou i-uzly, každá položka v adresáři je svázaná s tímto uzlem. Tento systém využívá abstraktní vrstvu nad fyzickými soubory. Tato datová struktura obsahuje metadata – práva, vlastník… a seznamy, popisující umístění souboru na disku. V těchto seznamech se vyskytují adresy bloků jednotlivých souborů, čehož je využíváno i při mazání. Kdy se při akci smazat soubor v příslušném i-uzlu sníží počet hardlinků o jeden (když soubor neodkazuje nikam je počet hardlinků roven 0) a obsah i-uzlu se vynuluje. Toto vynulování „adresy“ způsobuje, že softwarová obnova dat musí pracovat se složitějšími, algoritmy, jelikož se musí určit poloha dat na disku (analýza žurnálovacích souborů). (15)

Adresáře jsou v této struktuře ve své podstatě soubory osahující seznam jmen souborů a čísla jejich i-uzlů. Vyhledávání souborů lze provést pomocí vyhledávacího stromu, hašovací tabulky, nebo přečtením všech položek adresáře.

Poslední verze tohoto souborového systému s označením ext4 byla představena v roce 2008. Umožňuje uložit soubor o velikosti až 16TB a adresovat prostor 1EB pro celý svazek. Fyzicky je disk opět rozdělen do bloků a ty jsou soustředěny do větších skupin bloků obsahujících mapu i-uzlů, tabulku i-uzlů a datové bloky. (15)

3.2 Rizika

K pochopení nutnosti bezpečného odstranění dat a potřeby možnosti obnovy dat, musíme znát i rizika hrozící datům a médiím. Ať už je to riziko úmyslné nebo častěji neúmyslné vedoucí ke smazání (ztrátě) dat.

3.2.1 Neúmyslná

Lidský faktor

Je jedním z největších rizik, způsobujících ztrátu dat. Za hlavní příčinu lze obvykle označit nepozornost, neznalost a nedbalost při nakládání s daty. Charakteristickým projevem je neúmyslné smazání vlastních nebo cizích souborů a složek při mazání vícero souborů a složek. Přepsání již existujících souborů novými, případně ztráta celého datového média. Do této kategorie patří i špatné použití programového vybavení, kdy špatně provedený příkaz (např. SQL) naruší databázi dat. Z hlediska bezpečnosti je to pak neodborná manipulace při likvidaci citlivých údajů a médií nesoucí tyto data.

Hardware a software

Porucha hardwaru je dalším běžným způsobem nechtěné ztráty dat. Nejčastěji se jedná o poruchy úložných datových médií (pevný disk, poškrábaný optický disk atd.) Tato porucha může nastat přímo u samotného média nebo může být způsobena následkem jiné poruchy (přepětí v elektrické síti atd.).

Porucha softwaru je méně časté riziko, jeho nebezpečnost je, že následky nemusejí být hned zjevné, to zhoršuje šance na případnou obnovu dat.

Příroda a technické nedostatky

Přírodní katastrofy mají za následek většinou kompletní ztrátu dat vlivem poškození paměťového média (zemětřesení a zřícení budovy, záplava, úder blesku, požár). Mezi technické nedostatky způsobující ztrátu neuložených dat, poškození editovaných dat a v některých případech poškození paměťových médií patří zejména výpadek elektrického proudu, při absenci záložního nouzového napájení.

3.2.2 Úmyslná

Ztráta a smazání dat nemusí být a často ani není způsobena pouze neúmyslně. U rizik spojených se zneužitím citlivých dat, je tento záměr evidentní. Tyto rizika se dají rozdělit na vnitřní a vnější.

Vnitřní

Ke smazání dat může dojít, z vnitřního pohledu například tak, že nespokojený zaměstnanec po ukončení pracovního poměru poškodí, smaže firemní data nebo poškodí datové médium. Případně se díky absenci bezpečného smazání dat dostane k citlivým údajům například výplatním záznamům, které obnoví na datovém médiu.

Vnější

Mezi vnější rizika můžeme jednoznačně zařadit viry modifikující, mazající či jinak softwarově destruující data. Hackerské útoky mající za cíl poškození organizace způsobené ztrátou důležitých dat, nebo naopak snaha o získání takových dat proniknutím do systému, případně obnovením smazaných dat ze systému a vyřazených paměťových médií.

Jedno z největších rizik je samotné odcizení média, ze kterého je bez použití sofistikované ochrany možno data přímo získat a smazaná obnovit.

3.2.3 Snížení rizika šifrováním

Snížit riziko při ztrátě a nakládání s médii uchovávajícími data lze pomocí šifrování. Šifrování je také vhodný doplňkem k bezpečnému mazání a zálohování. Šifrování je zjednodušeně proces, kdy se data pomocí algoritmu a klíče překódují tak, že nelze běžně rozeznat, o jaká data se jedná, kde určitý soubor končí a kde začíná. To zamezuje prakticky jakémukoliv obnovení dat po smazání bez použití šifrovacího klíče, protože nelze rozpoznat, co která informace je, takže i když data fyzicky nejsou přepsána, jejich pouhé přečtení bez prolomení kódu je k ničemu. Šifrovat se dají jednotlivé soubory, oddíly disku i celé disky. (16)

„Hlavním důvodem šifrování je samozřejmě ochrana soukromí. Je jedno, zda na svém notebooku používáte heslo v operačním systému, heslo disku (ATA Password), nebo máte zaheslovaný BIOS (User/Supervisor Password). Pokud nemáte data šifrovaná, útočník se k nim snadno dostane. Pevný disk stačí vyjmout a připojit ho k jinému počítači.

Zaheslování elektroniky běžného disku je jen iluze bezpečnosti, neboť přes různé ATA terminály můžete heslo snadno vyčíst a zrušit. Nastavená práva čtení/zápisu v OS jsou po připojení do jiného počítače také jen otázkou několika kliknutí (případně chmod/chown).“ (16)

3.3 Mazání dat

3.3.1 Operační systém

Všechny operační systémy umožňují smazání souborů a dat i zde ovšem existují rozdíly. Základně je třeba říci rozdíl mezi smazáním dat a smazáním souboru. Tento rozdíl spočívá v tom, že při prostém smazání souboru dojde pouze k označení paměťového místa, kde byl jako volného místa pro zápis dat samotná data, ale na místě zůstávají, jen nejsou běžně viditelná. Oproti tomu, když dojde ke smazání dat, jsou data alespoň jednou náhodně přepsána nebo je místo nastaveno na samé 0/1.

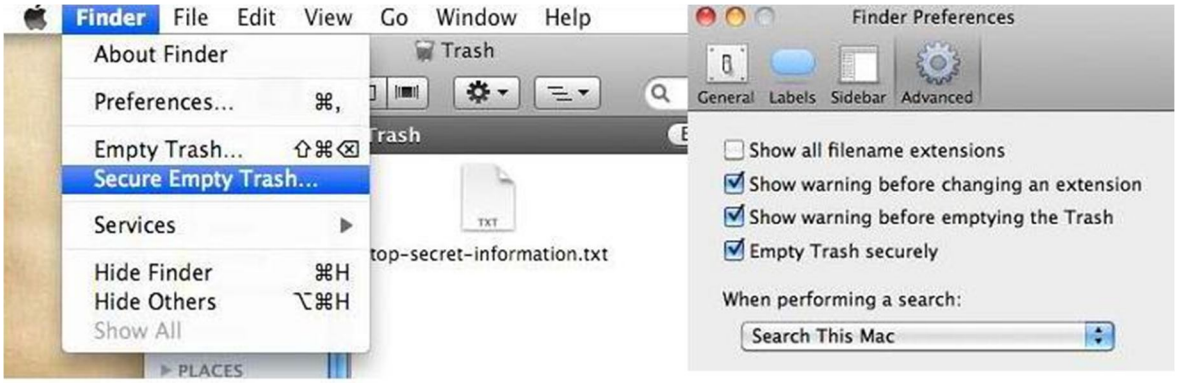
3.3.1.1 Windows

Většina dnes používaných počítačů pracuje s operačním systémem Windows (dle různých statistik a šetření přes 91%). Proto logicky i nejvíce operací odstraňující citlivá data probíhá zde. Všechny operační systémy Windows disponují funkcí odstranit „Delete“, která přesune zvolené soubory/složky do koše. V této fázi nejsou data nijak odstraněna jen je skryt ukazatel na soubor. V samotném koši jsou data stále viditelná a funkcí obnovit se jen odkryje znovu ukazatel na ně (data se v podstatě neobnovují, protože nikdy nebyla smazána). Při použití funkce vysypat implementovanou do koše dojde ke smazání ukazatele na data (dle souborového systému buď ve FAT tabulce, nebo označení v MFT jako smazaný soubor a označením místa jako volného atd.). Stejná situace nastává při použití klávesové zkratky Shift + Delete zde je rovnou mazán ukazatel na příslušná data

3.3.1.2 MAC OS (OS X)

Tento systém je rozšířen především na noteboocích a obdobných zařízeních od firmy Apple od roku 2012 se pro něj začal používat název pouze OS. Zatím poslední verzí vydanou 22. Října 2013 je OS X 10.9 Mavericks. Při smazání volbou „Delete“ dojde opět pouze k přesunutí do koše a jeho vysypáním pouze k uvolnění místa pro zápis, dříve

zabíraného souborem. Tento OS má ovšem v koši implementovánu i možnost bezpečného odstranění „bezpečně vysypat koš“ viz obr. 16.



Obrázek 16 Kde najít a nastavit bezpečné vymazání (17)

Tato funkce přepíše místo uloženého souboru 1x samými nulami. Tuto funkci lze nastavit, aby byla automaticky u všech souborů, nebo lze jí spouštět výběrově. Lze jí také nastavit, pokud je použito šifrování disku, aby automaticky přepisovala soubory na něm. (17)

3.3.1.3 UBUNTU

Tato linuxová distribuce má v sobě přímo nástroj na bezpečné mazání dat. Tento nástroj má název „Shred“. Jeho použití je omezeno, souborový systém nesmí být v „JOUTNAL Mode“. Pro bezpečné odstranění je třeba spustit terminál „man shred“, který je součástí mnoho verzí Ubuntu. (18)

V terminálu lze použít následující příkazy (bude mazán soubor data.txt obsahující například uložená hesla) (18):

- shred ~/data.txt (znečitelní soubor)
- shred -u ~/data.txt (znečitelní + smaže soubor)
- shred -u -x ~/data.txt (-x nakonec přepíše soubor nulami)
- shred -u -v -n 45 ~/data.txt (smaže; vypíše co dělá; -n číslo = nastavitelný počet přepisů)

3.3.2 Metody založené na softwarových řešeních

3.3.2.1 Algoritmy/Metody/Standardy

Pro bezpečné mazání bylo v průběhu let navrženo mnoho algoritmů, metod a standardů vycházejících zejména z armádního a vládního použití. Mazací algoritmy a metody jsou určeny především pro data uložená na magnetických médiích, aby se nedalo forenzními metodami a superpočítači zrestaurovat přepsaná data pomocí zbytkového magnetizmu i po přepsání. Základ těchto metod a algoritmů tvoří přepis paměťového místa vhodně stanovenými náhodnými nebo určenými vzory jedniček a nul.

Běžně je prezentováno, že proti útočníkovi používající běžné metody obnovy převážně softwarové je nutný alespoň 3 přepisy a proti laboratorním pokusům používající analogové útoky, mikroskopy (metoda MFM) a superpočítače nemusí stačit ani 30 přepisovacích cyklů pokud je zvolen nevhodný vzor.

S tímto názorem je ovšem v přímém rozporu studie s názvem „*Overwriting Hard Drive Data: The Great Wiping Controversy*“ vydaná odborníkem na forenzní analýzu Craigem Wrightem a jeho kolegy. (19) Ti provedli sérii analýz a pokusů s rekonstrukcí dat pomocí MFM a došli k závěru, že stačí přepsat dnešní velkokapacitní magnetické disky jakýmikoliv daty a data jsou nenávratně ztracena. Důvod této ztráty je neuvěřitelná hustota stop vedle sebe. Tím pádem ani pomocí MFM nelze rekonstruovat magnetickou stopu s dostatečnou přesností. Po pouhém jednom přepisu byla přesnost rekonstrukce čtení bitu pouze 56% po opakovaném čtení. Pravděpodobnost správného výsledku obnovy byla následně pouhých 0,97%.

Rychlé metody

Metody používající právě jeden přepis dat (výše zmíněný) jsou nazývány rychlé metody z důvodu krátkého času potřebného k provedení přepsání dat. Základní dvě metody pracují tak, že přepisují data 0 nebo používající náhodné hodnoty. Ještě rychlejší jsou metody, které nepřepisují celý datový prostor, ale náhodně řetězec hodnot, čímž zcela poškodí čitelnost původních dat.

Pokročilé metody/algoritmy

Metod mazání a algoritmů bylo a je v praxi využíváno mnoho druhů. Zde jsou popsány některé z nich. Nejčastěji jsou používány první dvě.

Gutmann

Metoda vyvinutá Peterem Gutmannem na univerzitě v Aucklendu na Novém Zélandu. Metoda používá nejvíce přepsání až 35 různých sérií a je díky tomu považována za nejbezpečnější. První a poslední čtyři série přepisu obsahují náhodně stanovená data, 27 vnitřních sérií má určený přesný vzorec, ale je náhodně seřazeno. Sestavené algoritmy byly navrženy, aby byla zajištěna co největší míra bezpečnosti i bez nutné znalosti příslušného kódování disku. Velkou nevýhodou této metody je dlouhé provedení samotného přepisu. Pouhý jeden GB se i při dnešních rychlostech disků maže průměrně déle než hodinu. (20)

U. S. DoD 5220.22-M

Byla vyvinuta ministerstvem obrany USA. Tato metoda používá pro smazání/přepsání disku 3 série. Při prvním průchodu je disk přepsán nulami a tento přepis je následně ověřen, Následuje přepis jedničkami opět, je zde provedena kontrola. Třetí přepis je proveden náhodně vygenerovaným vzorcem znaků. Postup zaručuje dle poznatků stoprocentní odolnost proti všem pokusům o obnovu pomocí softwarových nástrojů. Pro obnovení, alespoň části dat by proto byl nutný hardwarový způsob obnovy. (21)

VSITR standard

Tento standard pochází z Německa a byl stanoven Německým spolkovým úřadem pro bezpečnost v informačních technologiích. Algoritmus používá 7 sérií přepisu, kdy se v prvních šesti střídají pouze sekvence 01010101 a v posledním se zapíší náhodné znaky.

Russian GOST

Metoda vycházející ze souboru norem známých pod označením GOST, používaných často v zemích bývalého Sovětského svazu. Používající 2 série přepisu, v první se přepisuje pouze nulou a ve druhé jsou data přepsána náhodnými znaky.

Další standardy

Standardů je ve světě velké množství většinou byly vytvářeny na základě vládních a armádních požadavků nebo na základě firemních požadavků vyjmenování a popsání všech není ovšem tak zásadní protože pracují na stejných principech a předpokladech jako již popsané, jako další běžně používané můžeme jmenovat například (20):

- HMG Infosec Standart 5
- Schnier
- US Air Force 5020
- US Army Ar380-19

3.3.3 Sanitace

Protože pouhá softwarová metoda bezpečného mazání založená na algoritmech není použitelná u všech typů pamětí a zejména u polovodičových z principu jejich konstrukce značně selhává, byly vyvinuty metody, které zajišťují téměř 100% neobnovitelnost dat. Tyto metody jsou označovány jako „sanitace“. Samotnou sanitaci lze dělit do několika úrovní, dle již zmíněné studie „*Reliably Erasing Data From Flash-Based Solid State Drives“* (22) z níž vychází tato část, je dělení následující.

Logická

Tato sanitace je založena na výše popsaných metodách/algoritmech, takže se data nedají obnovit přes softwarové nástroje. Je ovšem omezená možností provést tyto metody, což například poškozené médium (nefunkční pevný disk, nebo chybné bloky na disku) neumožňují. U polovodičových pamětí typu flash je nelze bezpečně použít pro mazání pouze některých souborů, jelikož selhávají z hlediska konstrukčních prvků.

Digitální

Tato následující úroveň sanitace zajišťuje, nemožnost obnovy dat i za použití neznámých ovládacích příkazů nebo speciálně vytvořených verzí firmwaru. Je zde ovšem opět problém se sanitací poškozených médií a paměťových bloků označených jako nefunkční a vyřazených z požívání. U SSD a flash pamětí je digitální sanitace ještě více komplikovaná.

Analogová

Je založena na degradování analogových signálů, takže z nich nebude možné sestavit data. Rekonstrukce těchto signálů navíc taktéž není možná i za použití nejmodernější laboratorní techniky. (Analogové signály u čtení využívají magnetická a optická média.)

Kryptografická

Alternativou k přepisování či jinému mazání bitů je kryptografická dezinfekce skladovaných informací. Zde je používán kryptografický klíč, ke kódování příchozích a odchozích dat. K samotné sanitaci pak postačuje bezpečně odstranit šifrovací klíč čímž se uložená data stanou absolutně nečitelnými, pokud nedojde k prolomení tohoto šifrování, což má za následek přímý přístup k informacím.

3.3.4 Nedestruktivní strojová zařízení

Na trhu existují i speciální hardwarové zařízení využívající postupy logické a digitální sanitace, splňující požadavky příslušných norem např. NSA, DoD5220.00-M. Funkce je založena na již zmíněných algoritmech a několika násobném přepisu celého pevného disku. Výhody těchto zařízení je podstatně vyšší rychlost provedení bezpečné sanitace. A možnost znovu použití pevného disku oproti destruktivním řešením. Tyto zařízení navíc bývají více účelová, umožňují testování, mazání, replikaci i obnovu dat.

Příkladem takového zařízení může být KESENDER 2 podporující disky s rozhraním IDE a SATA.

Obrázek 17 KESENDER 2

Zdroj: http://www.kk-yec.com/products/closed/kesender2

3.3.5 Destrukce (Destruktivní strojová zařízení)

Fyzická likvidace datového média přináší stoprocentní jistotu zničení dat, ale pouze v případě, je-li správně a odborně provedena. To je často podceňováno, v praxi jsem se setkals tím, že ve většině firem se k destrukci paměťových médií využívá kladiva, nebo aku vrtačky k provrtání disků a jejich ploten. U SSD disků je tento problém ještě zhoršen tím, že k úplné bezpečné likvidaci musí být nenávratně poškozeny všechny interní paměťové čipy. Na trhu je řada přístrojů zajišťující spolehlivou destrukci dle bezpečnostních norem.

Demagnetizace (degrausing)

Tato zařízení jsou určená k trvalému bezpečnému odstranění dat z magnetických nosičů. Svým výkonem překonávají problém s koercivitou. Jejich výhodou je možnost odstranění dat i z nefunkčních magnetických nosičů (fyzicky poškozený například pohon pevného disku znemožňující logickou a digitální sanitaci). Data z datových pásek, typu LTO, apod., pevných disků jsou po demagnetizaci nenávratně smazána a média již nejsou použitelná. Následně lze tyto nosiče ekologicky zlikvidovat, případně navrátit dle smluvních podmínek výrobci atd. bez rizika zneužití dat.

Příkladem je Degausser ProDevice ASM120 schopný vytvořit magnetické pole o intenzitě 11 000 Gaussů. Datová média se vkládají do zásuvné přihrádky. Následně jsou spuštěny dva silné elektromagnety demagnetizující médium. Mazání trvá dle výrobce přibližně 30s. Přístroj umožňuje i nastavení počtu povolených mazacích cyklů (umožnění pronajmutí přístroje dle množstevní licence na počet mazaných médií přímo zákazníkovi). (23)

Destruktéry

Tyto přístroje se zaměřují na fyzickou destrukci paměťových médií. Patří do nich skartovačky na optická média, lamače přístroje na fyzické ničení pouze magnetických pevných disků, kdy je pevný disk a plotny zcela rozlomen a tím nenávratně poškozen příkladem může být:

Garner PD-4 fyzicky ničící pevné disky ohýbáním, lámání a mandlování pevný disk i jeho vnitřní komponenty, včetně datových ploten. Datové plotny jsou ohnuté a odděleny od náboje, pevný disk i obal pevného disku je rozlomen, řadič je zničen a čtecí / zapisovací hlavy jsou rozbité. Tento přístroj ničí až dva disky naráz za 28s.

Obrázek 18 Garner PD-4 (24)

Drtiče

Dalším typem jsou drtiče, tyto přístroje jsou daleko dražší. Použití drtiče je univerzální, rozemele jakékoliv datové médium na miniaturní částice, neumožňující jakoukoliv obnovu dat. Tento typ stroje je zejména vhodný pro likvidaci SSD a flash disků. Většina drtičů produkuje části o maximální velikosti 20x30-50mm na trhu jsou i varianty produkující ještě menší částice původních zařízení.

Pro nejpřísněji střežená data a provozy existují dezintegrátory/granulátory, tyto přístroje jsou nejbezpečnější a umožňují nastavení velikosti částic pomocí obrazovky. Ovšem čím menší částice stroj musí produkovat, tím se zvyšuje doba potřebná na provedení operace. Princip destrukce je následující po vložení například SSD disku do řezací komory, jsou spuštěny řezací nože proti dvěma stacionárním a disk je rozřezán na předem velikostně stanovené části. (24)

3.3.6 Zákony a legislativní opatření

V České republice a ve světě se mnohé zákony a legislativní opatření týkají nakládání s daty a jejich bezpečnou likvidaci. Řada těchto opatření má i sankční klauzuli při jejich nedodržování. V ČR řeší problematiku citlivých dat a informací shromažďovaných a uchovávaných na datových nosičích především podle směrnice 95/46/ES Zákon č. 89/2012 Sb., občanský zákoník, Zákon č. 101/2000 Sb., Zákon o ochraně osobních údajů a Zákon č. 40/2009 Sb., trestní zákoník. Podle něj může být případný únik osobních/citlivých dat i z nedbalosti posuzován jako závažný trestný čin s trestní sazbou a dle provinění 1 – 8 let. Nebo ho může postihovat Úřad pro ochranu osobních údajů, kde jsou sankce pro právnické osoby až do výše 5 000 000 Kč dle provinění.

Ve světě zejména v USA jsou tyto postihy ještě daleko přísnější a vztahují se i na finanční data, kde je postih až 20 let odnětí svobody. Komplexní přehled o zákonných a legislativních opatřeních týkajících se datové bezpečnosti obsahuje studie „Data Protection Laws of the world“ rozebírající tuto problematiku řešenou ve státech celého světa. (25)

Z hlediska práce je zde uvedena právní kvalifikace termínů „Osobní údaje“ a „Citlivé osobní údaje“ jež jsou v práci často zmiňovány.

Osobní údaje

Jsou kvalifikovány podle zde uvedených zákonů jakákoli informace týkající se určeného nebo určitelného subjektu údajů. Údaje předmět se považuje za určitelný, jestliže je možné identifikovat subjekt údajů zejména na základě čísla, kódu nebo jednoho či více specifických faktorů, přímo či nepřímo na jeho / její fyzické, fyziologické, psychické, ekonomické, kulturní nebo sociální identity. (25)

Citlivé osobní údaje

Citlivé jsou kvalifikovány, jako osobní údaje odhalující národnost, rasový nebo etnický původ, politické postojů, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný akt, zdravotní stav a sexuální život subjektu údajů, jakož i veškeré genetické či biometrické údaje. (25)

3.4 Obnova

Data, která jsou často omylem smazaná nebo ztracená, lze ve většině případů obnovit. V některých případech velmi snadno se zanedbatelnými náklady, jak finančními tak časovými. Běžně ale nastávají případy, kdy je nutno k obnovení dat vyvinout zvýšené úsilí a samotná obnova, rekonstrukce dat trvá hodiny až dny.

Zde už je třeba zvážit, jakou cenu ztracená data mají, a jak se dají nahradit. Jestli jde o data poměrně nedůležitá (část dat nainstalované aplikace, které lze znovu vytvořit její reinstalací). Pracně nahraditelná výsledky dlouhodobé práce, dlouhodobý sběr měření/informací, jejichž ztráta představuje významný problém a jejich nahrazení/ opětovné vytvoření by představovalo velké finanční nebo časové prostředky. Nebo data nenahraditelná (lékařské záznamy, ale i například staré rodinné digitální fotografie) jejichž opětovné vytvoření již není možné.

Obnovu ztracených, náhodně smazaných, nebo poškozených dat lze základně rozdělit na dvě metody. Na obnovu dat s využitím zálohy a na datovou remanenci. Obnova dat za použití zálohy je vždy rychlejší a dle ceny dat, při jejich případné ztrátě a velké náročnosti na obnovení v některých případech i nemožnosti rozhodně ekonomicky výhodnější.

3.4.1 Obnova dat za použití zálohy

Je zřejmé, že zálohování úplně všech dat je zbytečné. Takové zálohování by bylo finančně i časově dle objemu dat velmi náročné. Proto by se měly zálohovat pouze důležité soubory vytvořené vlastní prací uživatele nebo získané a běžně nenahraditelné. Do této kategorie mohou spadat i důležitá nastavení, náročná na obnovu po případné havárii. (5 str. 188)

3.4.1.1 Kritéria na zálohovací médium a skladování

Kapacita média je jedním z důležitých kritérií, měla by být dostatečná, aby pokryla pravidelně opakující se zálohy a tím i zvětšující se objem dat.

Cena za prostor je nejčastěji definována jako GB prostoru média / cena média. Je nutné vzít v potaz, ale také náklady spojené s využitím příslušné technologie.

Bezpečnost médium by mělo být schopné data bezpečně uložit a uchovat po potřebnou dobu. Z tohoto důvodu se nedoporučuje používat pro zálohování již jednou

média poškozená (například havarovaný disk, který byl vyřazen jako primární, ale následně byl v rámci snížení nákladů použit pro zálohování).

Fyzické uložení a nepřístupnost média. Médium se zálohou dat by nemělo být uloženo na stejném místě jako primární data. Z důvodů popsaných v kapitole „Rizika“ a mělo by být zabezpečeno proti krádeži/cizímu přístupu. (5 str. 188)

3.4.1.2 Metody zálohování

Zálohování je možné provádět několika způsoby a jejich kombinacemi. Důležitou vlastností je schopnost, aby byla záloha prováděna zcela automaticky a zamezilo se tak riziku opomenutí a snížila se nestrojová časová náročnost na tuto úlohu. Je také důležité, aby bylo možné vybrat, určitá data nebo prostor, který se má pravidelně dle určené metody zálohovat. Nejběžnější metody zálohování, které jsou již běžně součástí programového vybavení operačních systémů (například Windows) jsou (5):

Normální zálohování

Kopíruje všechny vybrané soubory. Pro následnou obnovu je zapotřebí pouze poslední takto vytvořená kopie. Normální zálohování provádí opakovaně ručně nejčastěji sami uživatelé, což je neefektivní (přílišná časová i prostorová náročnost). Obvykle se proto provádí jen při zakládání datového skladu a následně je použitá některá z dále jmenovaných metod.

Denní zálohování

Zkopíruje/zálohuje všechny zvolené soubory (označené pro zálohování), změněné v den, kdy bylo denní zálohování provedeno.

Rozdílové zálohování

Zálohuje soubory vytvořené, nebo změněné od posledního normálního nebo přírůstkového zálohování. Pokud je provedeno rozdílové zálohování, je k obnově za potřebí poslední normální a rozdílové zálohování.

Přírůstkové zálohování

Zálohuje pouze soubory vytvořené, nebo změněné od posledního přírůstkového zálohování. Při použití kombinace normálního a přírůstkového zálohování je pro obnovu nezbytné mít datový sklad normálního zálohování a všechny datové sklady přírůstkového zálohování.

Kombinace normálního a přírůstkového zálohování je nejméně prostorově náročná a nejrychlejší. Obnova je ovšem časově pomalejší a vyžaduje všechny datové sklady ve správné chronologii (pokud jsou uloženy na více médiích). Oproti tomu to kombinace normálního a rozdílového zálohování je časově náročnější, zejména když dochází k častým změnám dat, ale obnova je rychlejší, záloha existuje v menším množství souborů. Po provedení zálohy by měla nastat verifikace dat. Zvyšuje sice časovou náročnost, ale i bezchybnost zálohy. Běžně se následně provádí komprimace záložních dat (úspora prostoru média). (5 str. 189)

3.4.1.3 Pokročilé způsoby zálohování a ochrany dat

Při uchovávání a zálohování důležitých dat nebo velkých objemů dat jsou používány dnes systémy/metody/technologie ukládání a zálohování dat spojené se síťovím přístupem a diskovými poli s RAID technologií. Ty lze základně rozlišit podle toho, jestli je disk napojen přímo na aplikační server, pak je tento způsob označován jako DAS. Nebo jestli se jedná o oddělené úložiště propojené pouze sítí, zde se pak hovoří o SAN a NAS. Tyto systémy jsou také často rozšířené o páskovými mechanikami pro dlouhodobou zálohu a archivaci dat. (26)

NAS je označení pro síťové úložné zařízení, dostupné přes síťové propojení PC stanicím atd. Toto zařízení je schopno pracovat samostatně, obsahuje n počet disků (pracujících v diskovém poli s technologií RAID) a vlastní řadič s přístupem na síť. Úložná kapacita jednoho takového zařízení je dnes běžně od několika TB až po desítky PB (26)

SAN zde jsou přímo disková pole propojena vlastní sítí a vlastním protokolem. Následně jsou připojeny přes speciální karty k řídicímu systému, ten následně poskytuje data uživatelům. (26)

DAS je diskové pole připojené přímo k serveru. Slouží převážně ke zvýšení úložné kapacity a jeho výhodou je nižší pořizovací cena. (26)

RAID technologie

Je metoda zabezpečující data proti riziku selhání disku. Zabezpečení zajišťuje specifické ukládání/rozkládání dat na disky v poli. Data jsou zachována i při poruše některého z disků míra bezpečnosti je dána typem RAID označovaného číslem. RAID sám o sobě by neměl nahrazovat ovšem zálohování. Nejčastěji je používán RAID0, RAID1, RAID10, RAID5, RAID6.

3.4.2 Obnova dat bez použití zálohy

Obnova dat bez použití zálohy je téměř vždy složitější a nemůže zaručit 100% navrácení všech ztracených dat. Její nákladnost se odvíjí od míry poškození datového média a jeho typu. (Někdy na ní má i výrazný vliv výběr specializované firmy zabývající se záchranou dat.)

U této obnovy můžeme rozlišovat dva způsoby prostou softwarovou obnovu a laboratorní obnovu. Tyto metody jsou založeny na „remanenci dat“, jde o znovu rekonstruování zbytkové reprezentace dat ze zbylých dat v datových sektorech, které zde zbyly po prostém smazání/formátování/havárii (např. smazáním záznamu o datech z tabulky FAT atd.).

Pro obnovu dat má velký význam i samotný typ paměťového média a způsob poškození nebo zapříčinění ztráty dat. U pevných disků bývá ztráta dat nejčastěji způsobena logicky smazáním/znedostupněním nebo hardwarovou poruchou. USB flash pamětí jsou to nejčastěji poničené USB konektory nebo řadiče, případně plošný spoj okolo čipu. U optických médií je to nejčastěji poškrábání atd. Toto poškození vede nejčastěji pouze ke ztrátě některých dat, zbytek dat lze obnovit.

Softwarové metody

Předpokladem softwarových metod je základní funkčnost datového média (funkční pevný disk, neroztříštěný optický disk atd.). Jinak je nejdříve nutné použít laboratorní metodu a až následně je možné použít softwarovou.

Softwarová obnova je vhodná především u nechtěně smazaných dat na logické bázi (vyspání koše, zformátování, zrušení diskového oddílu atd.), kdy nedochází k fyzickému přepsání/odstranění dat, ale pouze ke smazání záznamu s odkazem na data v příslušné tabulce souborového systému. Nebo jsou tyto data ztracena poruchou souborového systému. (2)

Pokud dojde k samotnému přepsání dat, je softwarová metoda obnovy u pevného disku prakticky nemožná. Takové přepsání dat může nastat prakticky kdykoliv za běhu pevného disku a nejenom vlivem nahrání nových souborů. Operační systém totiž běžně při svém chodu zapisuje data. A v případě pravidelně prováděné defragmentace je riziko ještě větší. Zde se dá tvrdit, že čím větší objem dat byl, smazán a čím větší doba od smazání za provozu uběhla, tím se snižuje šance na obnovení dat. (19)

U médií používající paměťové moduly typu Flash, jak již bylo řečeno, se díky konstrukci a realizaci postupného ukládání/zaplňování disku dají obnovit. Algoritmus prohledá celý datový prostor média a rekonstruuje a obnoví všechna dosud v paměti uložená data. To platí i u disků na technologii SSD zde má na obnovu vliv ovšem již dříve popsaná funkce TRIM vymazávající fyzicky prostor, který je označen jako volný. (27)

Komerční programy zabývající se obnovou dat využívají speciální algoritmy, které jsou různě výkonné pro rekonstrukci a obnovení dat. Těchto programů existuje na trhu velké množství. Správný program pro datovou obnovu by měl dodržovat jednoduché pravidlo, že nesmí při své činnosti zapisovat cokoliv na analyzované médium, zejména pevný disk. Měl by také umožňovat hloubkovou analýzu po jednotlivých sektorech a né pouze obnovu alokačních tabulek.

Laboratorní postupy/metody

Jsou téměř vždy nutné při fyzickém poškození média. Zde jsou dodržovány přesné postupy oprav a obnov těchto médií ve správných podmínkách (bezprašná komora atd.) za použití speciálního vybavení umožňujícího přístup k diskům v režimu výrobce a dokážou tak nejen diagnostikovat chybové stavy disku ale i zasahovat do výrobní servisní stopy a měnit tak důležité parametry disku. Při záchraně dat z poškozených flash disků (USB, paměťové karty) používají zařízení umožňující přímý přístup k paměťovému čipu a následnou rekonstrukci dat, aby nedošlo k dalšímu poškození dat.

Metoda MFM

Mezi laboratorní postupy patří již dříve zmiňovaná metoda MFM (Magnetic force microscope) v kapitole „Mazání“. Tato technologie je založena na principu snímání magnetických sil pomocí ostrého magnetického hrotu upevněného na raménku a plujícího těsně nad povrchem magnetického média. Vlivem magnetických interakcí mezi hrotem a magnetickou stopou dochází k detekovatelným pohybům hrotu. Tyto interakce jsou zachycovány a na jejich základě probíhá vyhodnocování. Takto lze zcela bez problémů přečíst celý magnetický povrch a zjistit všechna data. Navíc je zde i možnost zjistit data, která byla již dříve zapsána. To je zapříčiněno tím, že při zápisu (přepisu) je změněna polarita pouze u některých domén. Následně tedy dojde ke zvýšení původní hodnoty magnetického pole zhruba o 5% (zápis stejné hodnoty např. 1), nebo ke snížení té nové (zápis rozdílné hodnoty od předešlé). Tento stav není schopná běžná čtecí hlava zaznamenat, protože pracuje s daleko větší tolerancí při určení, zda se jedná o informaci 0 či 1.

Tato metoda se dnes běžně používá pro rekonstrukci záznamu datových pásek.

4 Vlastní práce

4.1 Anketa - dotazníkový průzkum

Úvodem vlastní práce byla provedena anketa, jak jsou lidé obeznámeni s problematikou bezpečného mazání a obnovy dat. Řeší-li „bezpečné“ mazání citlivých údajů, znají-li možnost obnovy dat a případně jakým způsobem. Dále bylo sledováno, nakládání s médii a daty na nich v souvislosti s touto problematikou. Získaná data z ankety posloužila i k ověření, zda mají znalosti IT/ICT prokazatelnou souvislost s používáním bezpečného mazání dat.

Příloha č. 1: struktura dotazníku a otázek

Příloha č. 2: kompletní výsledky dotazníkového šetření

4.1.1 Základní údaje o provedené anketě

Typ dotazování:	elektronické
Počet respondentů:	184
Počet otázek:	16
Použité ochrany:	unikátní ip adresy
Zobrazení otázek:	celý dotazník najednou
Typy otázek:	výběrové, rozdělující, výběrové/polouzavřené
Návratnost dotazníků:	80 %
Průměrná doba vyplňování:	00.04:14
Dotazník vytvořen na serveru:	vyplnto.cz

Tabulka 1 Základní údaje o provedené anketě

Zdroj dat: http://www.vyplnto.cz/moje-pruzkumy/?did=37767

4.1.2 Zdroj respondentů.

Odkaz na dotazník byl rozšiřován prostřednictvím e-mailové komunikace, sociálních sítí a serveru vyplnto.cz. Zjištěné zdroje uživatelů, weby ze kterých přicházely, dle serveru vyplnto.cz :

nezjištěno	(53,2 %)
facebook.com	(30,7 %)
vyplnto.cz	(6,1 %)
google.cz	(5,4 %)
m.facebook.com	(3,2 %)

Tabulka 2 Zdroje respondentů

Zdroj dat: http://www.vyplnto.cz/moje-pruzkumy/?did=37767

4.1.3 Souhrnné výsledky dotazníku

Zde jsou uvedeny pouze identifikační a nejdůležitější výsledky a poznatky dotazníkového šetření. Celkové výsledky jsou k nalezení v „Příloze č. 2“. Grafy byly vytvořeny na podkladě získaných dat.

Mezi respondenty převládali respondenti ve věku 16-30 (144/80%) a respondenti se středním vzděláním a maturitou (78/43%), vysokoškolským vzděláním, (92/51%) zajímavé bylo, že zde byla velká skupina respondentů, která označila své znalosti práce s počítačem pouze za základní znalosti (78/43%). Souhrn grafů znázorňujících charakterizující údaje o složení respondentů z otázek 14,15,16 viz Grafy 1.

Grafy 1 Souhrn charakterizujících údajů o složení respondentů z otázek 14,15,16

Zdroj: Autor

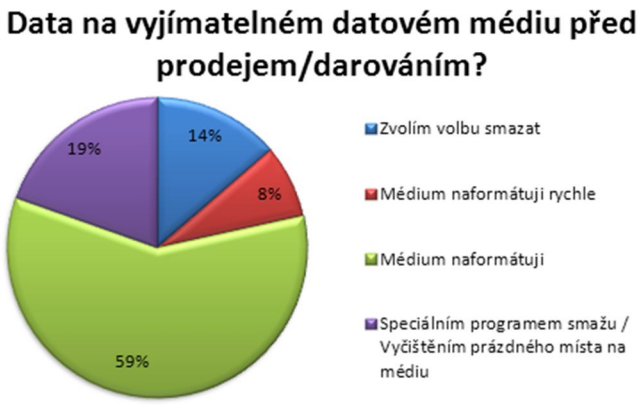
Základní úvodní otázka byla zvolena: „*Myslíte si, že soubory vysypané z koše (např. ve Windows) jsou nenávratně ztraceny?*“ Výsledek potvrdil, očekávání, že zhruba každý desátý respondent si neuvědomuje možnost obnovy dat a souborů po pouhém jednoduchém smazání. Ze 17 respondentů, kteří si myslí, že jsou data nenávratně ztracena, patřilo 14 do skupiny označující své znalosti pouze jako základní. Ve skupině práce/studium v oboru IT/ICT se nenašel žádný, kdo by nevěděl, že takto smazané soubory lze obnovit.

Na otázku č. 2 zaměřující se na bezpečné mazání citlivých dat: „*Jak běžně odstraňujete citlivá data (soukromé fotografie, finanční záznamy, privátní archivovanou korespondenci atd.) na pevném disku nebo jiném přepisovatelném médiu, které denně používáte?“* Byly výsledky překvapivé z toho důvodu, že většina respondentů neřešila, jaká data odstraňuje a postupovala jako u běžných dat. Toto zjištění je z hlediska práce velmi podstatné. Bylo nutné ověřit, jestli tuto skutečnost nezkresluje složení respondentů vzhledem k jejich znalostem (viz kapitola 4.1.3.1.), kdy se v anketě vyskytovalo nadprůměrné množství respondentů studujících nebo pracujících v IT/ICT (27%).

Graf 2 Výsledek otázky č. 2

Zdroj: Autor

Ještě hůře z pohledu bezpečného mazání dat dopadly odpovědi na otázku číslo 4, kdy byli respondenti tázáni, odstraňují-li data na vyjímatelném datovém médiu z elektroniky při jejím prodeji nebo darování Graf 3, kde pouze 19,61% odpovědělo, že použijí speciální program. Zbytek používal z pohledu bezpečnosti zcela nedostačující řešení.



Graf 3 Výsledek otázky č. 4

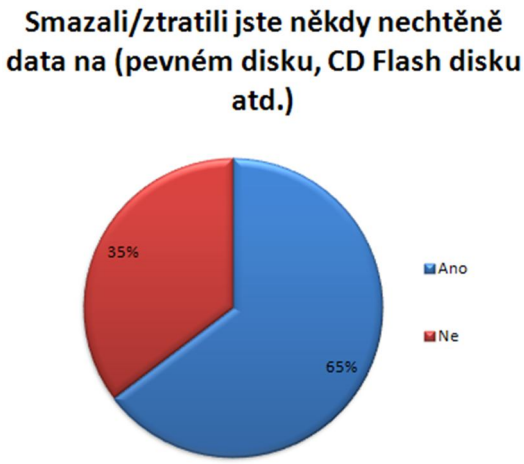
Zdroj: Autor

U podobné otázky zabývající se interní pamětí, kde nebylo uvedeno přímo bezpečné řešení mezi nabízenými, ale byla záměrně možnost vlastní odpovědi (správné), tak to učinili, pouze 4 respondenti. Zbytek zvolil nabízené nedostačující odpovědi, nebo vlastní odpověď neposkytovala jistotu neobnovitelnosti citlivých dat.

Otázka týkající se likvidací poškozených médií prokázala u značného množství respondentů nedostačující postup a např. 34% respondentů médium prostě vyhodilo.

Zarážející ovšem bylo, že 7% respondentů při výměně nebo upgradu médium prostě vyhodí (nesnažili se ho nijak poškodit ani smazat/ bezpečně smazat).

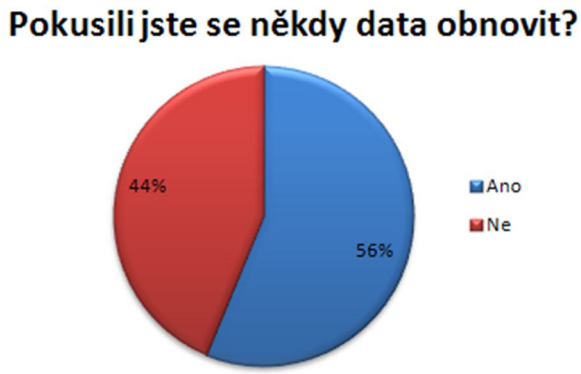
Ze získaných dat vyplynulo, že většina respondentů nějakou formou zálohuje svá data, pouze 24 odpovědělo, že ne. Z těchto 24 přesná polovina přiznává, že si již někdy omylem smazala data.



Graf 4 Výsledek otázky č. 10

Zdroj: Autor

Obnovit svá data po ztrátě nebo nechtěném smazání se již pokusila nadpoloviční většina respondentů, kteří vědí, že data lze obnovit a to jak za použití zálohy, nebo speciálního programu, jak je vidět na následujícím grafu.



Graf 5 Výsledek otázky č. 12

Zdroj: Autor

Zajímavou skutečností vyplývající z dat následující otázky bylo, že 14 respondentů popisujících své znalosti pouze jako základní se již pokusilo obnovit data pomocí speciálního programu. Celkově se pomocí speciálního programu pokusilo obnovit data 66 respondentů. To ještě umocňuje riziko zneužití nesprávně smazaných dat na datovém médiu. Protože povědomí o obnově dat je, jak prokázal dotazník rozšířené, a i někteří uživatelé pouze se základními znalostmi se již pokusili smazaná data obnovit (zde je třeba připustit, že se jednalo o obnovu vlastních náhodně smazaných dat). Od toho je však již jen

krok k pokusu o obnovení dat například na nalezeném flash disku a zneužití nesprávně smazaných citlivých dat.

4.1.3.1 Vliv znalostí na mazání citlivých dat

Otázka č. 4 ukázala, že většina respondentů maže citlivá data stejně jako běžná data. Toto zjištění je z hlediska práce velmi podstatné. Složení respondentů vykazuje velké početní rozdíly mezi jednotlivými skupinami dle znalostí IT/ICT, mezi respondenty se vyskytuje i velká část respondentů pouze se základními znalostmi, to by mohlo mít značný vliv na výsledek. Možnou závislost bylo nutné proto ověřit za použití statistických nástrojů výzkumu (testů závislosti kvalitativních znaků) na získaných datech.

Hypotézy byly stanoveny takto:

H_0 – Nebude existovat prokazatelná závislost mezi znalostmi IT/ICT respondentů a způsobem mazání citlivých dat.

H_1 – Bude existovat prokazatelná závislost mezi znalostmi IT/ICT respondentů a způsobem mazání citlivých dat.

K výpočtu hypotézy bylo nutné použít testování nezávislosti znaků v kontingenční tabulce o rozměrech k x m. Z důvodu, že u této hypotézy byla použita data z druhé otázky, na kterou odpovědělo pouze 167 respondentů a odpovědi nebyly pouze ano a ne. Data pro tuto tabulku byla získána extrahováním z celkových výsledků pomocí funkce suma s vloženými vnitřními podmínkami v aplikaci Excel. Následný výpočet probíhal v aplikaci Excel za použití statistických vzorců a pravidel pro výpočty závislosti kvalitativních znaků (χ2-test nezávislosti).

	IT/ICT znalosti				
Jak běžně odstraňujete citlivá dat	Základní	Dobré domácí	Velmi dobré	Práce/studium IT/ICT	SUMA
Odstraněním do koše a jeho vysypáním (jako běžná data)	49	23	4	30	106
Odstraněním a vyčištěním volného místa paměti v určitém časovém cyklu (týdně, měsíčně)	8	8	2	12	30
Odstraněním specialním programem	9	11	3	8	31
SUMA	66	42	9	50	167

Tabulka 3 Extrahovaná data pro ověření závislosti

Zdroj: Autor

Výsledky:

	IT/ICT znalosti				
Jak běžně odstraňujete citlivá dat	Základní	Dobré domácí	Velmi dobré	Práce/studium IT/ICT	SUMA
Odstraněním do koše a jeho vysypáním (jako běžná data)	1,206	0,502	0,513	0,095	2,317
Odstraněním a vyčištěním volného místa paměti v určitém časovém cyklu (týdně, měsíčně)	1,254	0,027	0,091	1,014	2,387
Odstraněním speciálním programem	0,863	1,316	1,058	0,177	3,414
SUMA	3,323	1,846	1,662	1,286	8,117

Tabulka 4 Výsledek výpočtu závislosti

Zdroj: Autor

Protože vypočtená hodnota testového kritéria 8,117 je nižší než 15,507 (kritická tabulková hodnota $\chi 2$ na hladině významnosti 0,05 a rozdělení pro 8 stupňů volnosti), přijímáme nulovou hypotézu.

Bylo potvrzeno, že neexistuje podstatná statistická závislost mezi znalostmi IT/ICT respondentů a způsobem mazání citlivých dat a výsledek otázky č. 4 není tímto ovlivněn.

4.1.3.2 Analýza zajímavých souvislostí (DZD)

Analýza proběhla prostřednictvím serveru vyplnto.cz a vyplynula z ní souvislost mezi odpověďmi respondentů na otázky 6 a 7.

U otázky *6. Pokud paměťové médium přestane fungovat (Disk, CD, atd. nemohu načíst data) tak?* Byla odpověď „Vyhodím, nic jiného nedělám“ 2,7x pravděpodobnější. Když byla zvolena u otázky odpověď *7. V případě, že paměťové médium (disk, flash disk) měním kvůli upgradu hardwaru (médium je stále běžně čitelné). Tak staré médium?* „jednoduše vyhodím do elektro odpadu“. (confidence zde vyšla 0,9231 a e-confidence 0,7174)

Z toho lze usoudit, že tito respondenti z 92,31% zacházejí obdobně při likvidaci nefunkčních i funkčních starých médií.

4.2 Experimenty

Na základě zjištění dotazníkového šetření a teoretických východisek byly provedeny experimenty se softwarovou obnovou dat za použití běžně dostupných programů. Experiment měl prokázat nebezpečnost nepoužívání nástrojů pro bezpečné mazání citlivých dat a s tím spojenou následnou možnost obnovy takových to dat na různých médiích.

Byly provedeny experimenty s možností obnovy nechtěně smazaných dat v předem připravených scénářích a kontrolovaných podmínkách. Prověřeny možnosti bezpečného smazání dat taktéž v předem připravených situacích a následná verifikace pokusem obnovit tato data.

K tomuto účelu byly zvoleny dva obnovovací programy a to Active Boot Disk 8.0.5.1 a Recuva 1.50.1036. Program Recuva byl zvolen na základě, krátkého dotazovacího šetření mezi 30 respondenty používajícími běžně obnovu dat (nejčastěji používán). Tento program je v této verzi volně šiřitelný a vyžaduje instalaci na disk s operačním systémem Windows. Active Boot Disk se spouští sám při startu počítače z externího média a jedná se o komerční program, jehož je autor vlastníkem (aby nebyla porušena licenční práva).

Experimenty byly prováděny prostřednictvím notebooku Lenovo G550. O hardwarových a softwarových parametrech

- CPU Intel Core 2 Duo T6500 2,1GHz
- RAM 2,96GB
- NVIDIA GeForce G 105M WD-WXE0A59N9701
- Pevný disk
- USB 2.0
- OS Windows XP Profesional SP3

4.2.1.1 *Experiment č. 1 Obnova dat ze získaných médií*

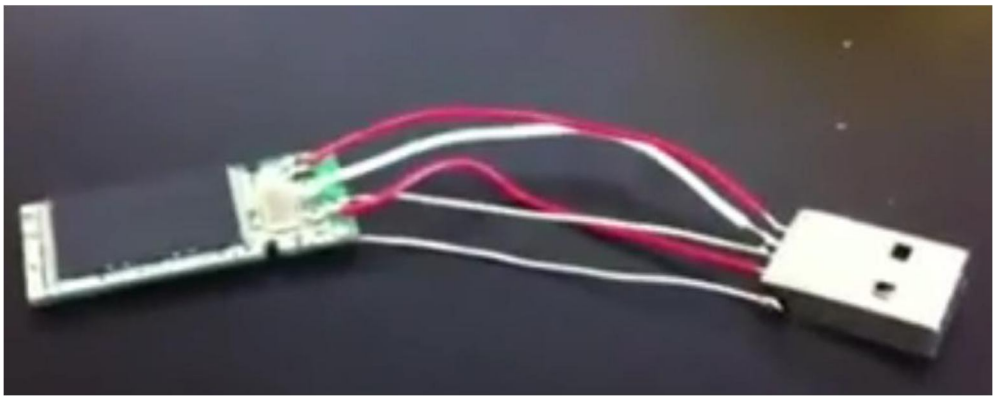
Pro experiment č. 1 byla zajištěna média, na která se v praxi nejvíce ukládají a zálohují citlivá data. Těchto médií bylo dohromady šest, 1x SD karta, 2x flash disk (1x ulomený konektor), 1x pevný disk a 1x externí pevný disk (domněle nefunkční). Skladba médií byla zvolena tak, aby obsáhla co nejširší spektrum běžných situací nakládání s médii. Jednak to byla média vyhozená po upgradu (pevný disk), poškozená média, která byla podle vlastníků nadobro zničená, tím pádem data neobnovitelná a určená k obyčejnému vyhození (flash disk a externí disk), médium běžně půjčované pro přenos dat flash disk a médium prodané spolu s elektronickým zařízením SD karta u digitálního fotoaparátu.

Zařízení	Výrobce	Udávaná kapacita GB	Typ paměťového média	Typ	Stav při získání
Externí disk	Hitachi	500	Magnetický disk	0S00232	Chyba ve vystavování hlav
Pevný disk	WD	320	Magnetický disk	WD3200EVT	Funkční
Flash disk	Kingston	8	Flash paměť		Ulomený USB konektor
Flash disk	Kingston	4	Flash paměť	DT160	Funkční
Paměťová karta	Pretec	2	Flash paměť	PCSD2GB	Funkční

Tabulka 5 Přehled médií pro experiment č.1

Zdroj: Autor

Na všech těchto médiích byla možná rekonstrukce dat. U poškozeného flash disku bylo nutné pomocí mikro pájky a drátků připájet konektor jak je vidět na obrázku č. 19. Poškozený externí disk, který hlásil i zvukově chybu vystavování hlav a byl na první pohled nečinný, stačilo otočit „na záda“ tím došlo vlivem gravitace ke vzdálení hlav od ploten do tolerované vzdálenosti a umožnilo čtení disku.



Obrázek 19 Připájení odlomeného USB konektoru falsh disku

Zdroj: Archiv autora

Skladba rekonstruovaných dat velmi závisela na předchozím používání. Částečné informace o médiích poskytli většinou sami původní majitelé, až na zakoupenou SD kartu, u které původní majitel nebyl před experimentem znám. SD karta obsahovala pouze fotografie, byly součástí fotoaparátu zakoupeného prostřednictvím online bazaru. Flash disky byly pro účely experimentu vypůjčeny se souhlasem majitelů a sloužily převážně pro potřeby přenášení a rychlého zálohování dat. Externí disk sloužil pro běžné zálohování materiálů, fotografií, ale i zálohu celých nainstalovaných her a filmů v HD rozlišení. Pevný disk nejdříve sloužil jako hlavní disk, na němž byl i operační systém a následně po formátu jako záložní pro ukládání filmů.

Všechna média byla podrobena softwarové obnově za použití výše zmíněných programů. Nebylo překvapením, že doba potřebná pro analyzování rostla s celkovou kapacitou média a průměrnou rychlostí čtení. Nejdelší dobu obnovy zabral pevný externí disk (velký vliv na časovou náročnost mělo i zvolení typu obnovy a upřesnění souborového systému pokud bylo známo), ale překvapující byla obnovená data z hlediska rizik bezpečnosti a to především z paměťové karty.

Bylo již zmíněno, že na všech médiích byla nalezena obnovitelná data, jejich množství úměrně rostlo s velikostí daného média a kvalita s množstvím přepsání části jejich prostoru, kde byla uložena. Vliv měl i výše zmíněný software, u analýzy médií byl rychlejší a celkové schopnosti obnovy dat byly lepší u komerčního ActiveBootDisk. Rekonstruování dat ovšem opět záviselo na typu a vlastnostech testovaného média. Na zvýšení rychlosti mělo i vliv spuštění tohoto programu bez nutnosti podpory

operačního systému a tím lepší využití výkonu. Pro znázornění rozdílů byl podrobněji popsán test s SD kartou.

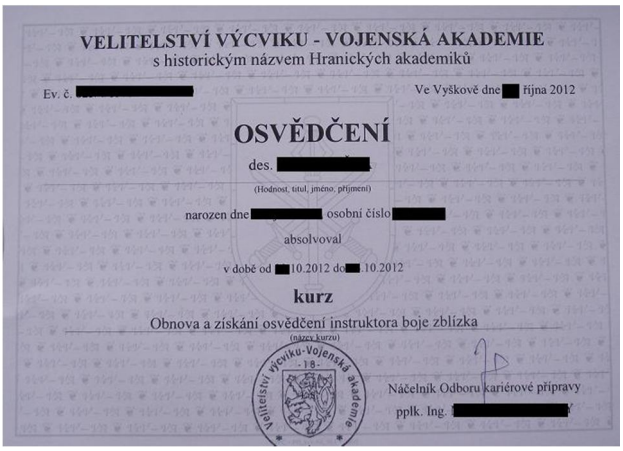
Stručný přehled výsledků experimentu

Testy s médii vyplynuly značně nelichotivě. Vyjma flash disku Kingston o kapacitě 4GB byly obnoveny pouze nezávadné dokumenty (školní projekty, poznámky, obrázky a videa), byla nalezena na všech určitá data, která se dají zařadit do kategorie citlivých informací (nejčastěji to byly fotografie, osobní dokumenty a záznamy). Na všech médiích byla obnovena data, jež obsahovala informace postačující k určení původního majitele. Nejčastěji to byly soubory Word s uvedeným jménem autora a informacemi o autorovi, které se podařilo obnovit. Nejvíce citlivých informací v poměru k množství obnovených dat bylo nalezeno na médiích využívajících flash paměti a to vzhledem k jejich používání i v již popsané metodice ukládání/mazání dat na těchto pamětích. Nejstarší data se podařilo obnovit na pevném disku, data smazaná z již neexistujících diskových oddílů, až z roku 2009, kdy začal být disk používán. Některé obnovené soubory obsahovaly data potenciálně nebezpečné i k vydírání nebo jiné trestné činnosti vůči původnímu majiteli. Blíže jsou zmíněny pouze dva experimenty, jelikož detailní rozbor a popsání všech, by zabral neúměrně mnoho prostoru, zde jsou uvedeny i konkrétní obnovená data.

Paměťová karta

U zakoupeného digitálního fotoaparátu byla přiložena SD karta o kapacitě 2GB. Na SD kartě bylo zjištěno, že pro odstranění dat bylo běžně používáno pouze prosté vymazání a před prodejem zvoleno rychlé formátování. Tento postup se ukázal vlivem jednoduchosti obnovy jako absolutně nedostatečný vzhledem k povaze části dat na SD kartě. Obnova trvala za použití Recuva skenování 717s, obnova souborů 497,34s, obnoveno bylo 332 souborů, z toho 257 úplně a 75 částečně. U programu ActiveBootDisk skenování 627s, obnova 1170s a bylo obnoveno 732 souborů (zde se povedlo obnovit i některé kopie, které byly na médiu vytvořeny). Z nich se dalo ještě několik částečně zrekonstruovat a přečíst pomocí speciálního programu na obnovu JPG souborů. Přibližně 6% dat se dalo považovat za velmi citlivá a skládala se z intimních fotografií a ofocených dokumentů včetně osobních dokladů. Pro příklad do diplomové práce byl zachován jeden dokument obsahující pouze identifikační údaje o původním majiteli SD

karty, který byl vzhledem k dodržování ochrany osobních údajů částečně začerněn. Byl zvláště nebezpečný pouze v kombinaci s intimními fotografiemi a zajímavý pouze z důvodu, poněvadž dokládal, že majitel byl členem armády, kde je zvláště dbáno na zacházení s citlivými daty viz Obr. 24.


VELITELSTVÍ VÝCVIKU - VOJENSKÁ AKADEMIE
s historickým názvem Hranických akademiků

Ev. č. [redacted] Ve Vyškově dne [redacted] října 2012

OSVĚDČENÍ

des. [redacted]

(Hodnost, titul, jméno, příjmení)

narozen dne [redacted] osobní číslo [redacted]

absolvoval

v době od [redacted].10.2012 do [redacted].10.2012

kurz

Obnova a získání osvědčení instruktora boje zblízka

(název kurzu)

Velitelství výcviku-Vojenská akademie - 18 -

Náčelník Odboru kariérové přípravy

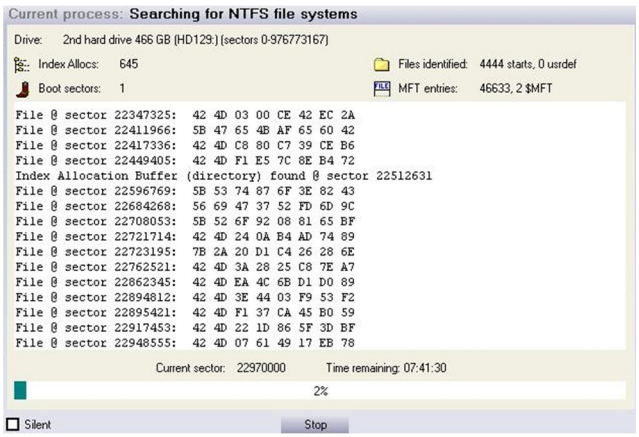
pplk. Ing. [redacted]

Obrázek 20 Příklad citlivých dat, která měla být bezpečně smazána

Zdroj: Archiv autora

Pevný externí disk

Analýza dat z pevného externího disku byla časově nejnáročnější. Důkladná analýza trvala konkrétně 8:36:22 při použití softwaru Recuva a 7:45:22 u ActiveBootDisk. Počet částečně obnovených a zcela obnovených souborů se dostal u obou programů na číslo převyšující půl milionu, drtivá většina souborů byla součástí zálohovaných nainstalovaných her, nebo nešla blíže identifikovat.



Obrázek 21 Průběh obnovy externího disku ActiveBootDisk

Zdroj: Archiv autora

Tento disk sloužil podle struktury dat jako záložní, neobsahoval žádnou zálohu osobní komunikace. Většina obsahu byla více jak 99% obecného charakteru necitlivých dat (filmy, hudba, zálohy celých nainstalovaných her), díky tomu bylo velké množství složek a souborů. Zbylé necelé procento dat, která by se dala zařadit do kategorie citlivá, byly osobní fotografie, až na malý textový soubor s názvem banka.txt vytvořený 9. 7. 2013 o velikost 96 bajtů, který obsahoval klient.č, xxxxxxxxxxxx, heslo pro telebanking xxxxxxxx, bezpečnostní kód xxxxxxxxxx. Zde je jasně vidět, že i zdánlivě opomenutý malý textový dokument, obnovený přes naformátování disku může za určitých dalších okolností vést k velkým finančním ztrátám.

4.2.1.2 Experiment č. 2 Obnova omylem smazaných souborů

Předcházející experimenty probíhaly v předem neřízených situacích a poukazovaly spíše na nebezpečí plynoucí z nedokonalého smazání dat. Následující experimenty mají za úkol prověřit možnosti a náročnost obnovy nechtěně smazaných souborů při nejčastějších situacích.

Pro potřeby tohoto experimentu byl na pevném disku WD-WXE0A59N9701 vytvořen oddíl o velikosti 0,98 GB, NTFS, velikosti alokační jednotky 512 bajtů a použit flash disk o velikosti 4GB, FAT32. Pro pokus experimentu byla vytvořena i data o celkové velikosti 0,93GB skládající se z archivů 47%, fotografií ve formátu JEPG 33%, různých dokumentů Office 18% a ostatních drobných souborů TXT, PNF, GIF. Celkem 168 souborů různých velikostí a rozmístění. Simulované situace byly náhodné smazání dat bez možnosti návratu dat z koše, rychlé přeformátování diskového oddílu, přeformátování diskového oddílu, zrušení diskového oddílu. Po každém pokusu byl prostor kompletně vyčištěn pomocí programu Eraser, aby nebyl ovlivněn následující pokus.

Výsledky:

Náhodné smazání souborů

Soubory byly uloženy a následně přes volbu „delete“ a vysypání z koše smazány. Zde stačilo u pevného disku použít i rychlou analýzu diskového prostoru a veškerá smazaná data bylo možné navrátit, tato analýza trvala méně než 1s.

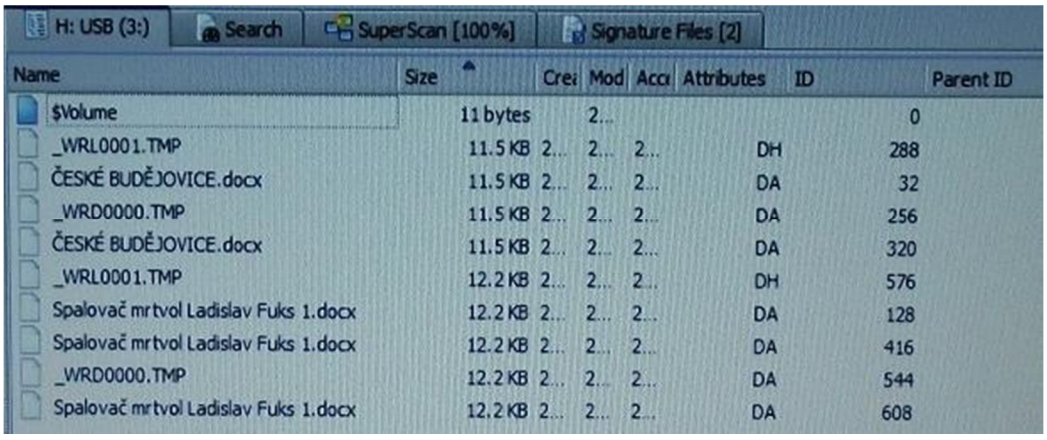
U flash disku rychlá analýza trvala pouze v řádu setin až desetiny vteřiny, při jednom z pokusů bylo po pouhém smazání zhruba 30% dat označeno jako nenávratně poškozená. Důvod neobnovitelnosti byl popsán tím, že daný soubor byl přepsán (vždy ovšem došlo k identifikaci jména souboru a původní velikosti). Situace nastala u reklamního flash disku neznámého výrobce.

Přepsání souborů

Přesný postup pokusu editace:

- nahrání dokumentu „ČESKÉ BUDĚJOVICE.docx“
- otevření
- editace a uložení
- odstranění dokumentu

- nahrání dokumentu „Spalovač mrtvol Ladislav Fuks 1.docx“
- okamžité odstranění
- znovu nahrání
- editace a uložení
- následovalo opět odstranění.



Name	Size	Cre	Mod	Acc	Attributes	ID	Parent ID
$Volume	11 bytes	2...				0	
_WRL0001.TMP	11.5 KB	2...	2...	2...	DH	288	
ČESKÉ BUDĚJOVICE.docx	11.5 KB	2...	2...	2...	DA	32	
_WRD0000.TMP	11.5 KB	2...	2...	2...	DA	256	
ČESKÉ BUDĚJOVICE.docx	11.5 KB	2...	2...	2...	DA	320	
_WRL0001.TMP	12.2 KB	2...	2...	2...	DH	576	
Spalovač mrtvol Ladislav Fuks 1.docx	12.2 KB	2...	2...	2...	DA	128	
Spalovač mrtvol Ladislav Fuks 1.docx	12.2 KB	2...	2...	2...	DA	416	
_WRD0000.TMP	12.2 KB	2...	2...	2...	DA	544	
Spalovač mrtvol Ladislav Fuks 1.docx	12.2 KB	2...	2...	2...	DA	608	

Obrázek 22 Všechny zjištěné soubory po krocích pokusu

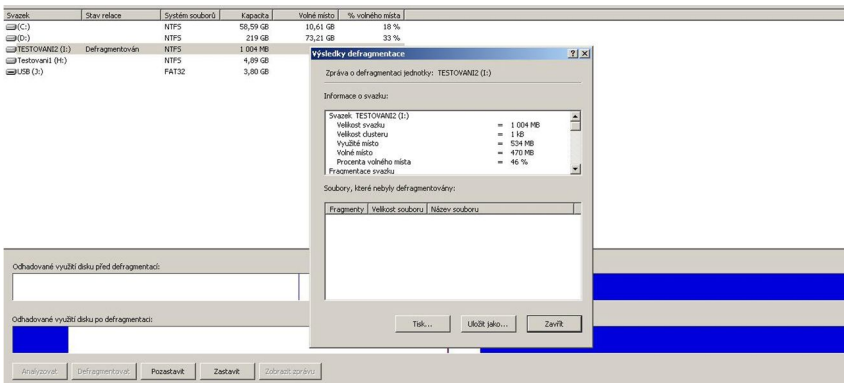
Zdroj: Archiv autora

Byla-li v souborech editována data, nebylo možné na pevném disku získat zpět původní data, pokud se nevytvořily stínové kopie, nebo záloha. Protože došlo k fyzickému přepsání paměťových oblastí původních dat.

Při editaci jednotlivých souborů (například Word dokumenty) přímo na flash disku byly zachovány předcházející verze před prostým uložením (přepsáním) dokumentu po editaci, stejně jako dočasné stínové zálohy pro případ pádu aplikace před uložením.

Náhodné smazání části souborů a defragmentace

Pokus se týkal pouze pevného disku, jelikož se defragmentace na flash discích se vzhledem k jiné konstrukci a ukládání dat neprovádí, není vhodná. Náhodně byla promazána polovina dat pouhým obyčejným smazáním a následně provedena defragmentace. Proběhlá defragmentace, jak je vidět na obrázku vlevo dole, přesunula část souborů.



Obrázek 23 Výsledek defragmentace

Zdroj: Archiv autora

To mělo za následek, že byla poškozena a nevratně zničena část souborů (přepsáním), které byly před tím uloženy v této oblasti. To je zřetelné na výpisu, po pokusu o obnovu v programu Recuva, na němž je jasně viděno místo, které bylo přesunutím zasaženo a soubory, které byly poškozeny. Z nezasažených míst šly soubory opět všechny obnovit.

DSC_0122.JPG	I:\?\	6 478 kB	Výborný	Nebyly nalezeny žádné přepsané clustery.
DSC_0123.JPG	I:\?\	5 716 kB	Výborný	Nebyly nalezeny žádné přepsané clustery.
DSC_0124.JPG	I:\?\	5 710 kB	Výborný	Nebyly nalezeny žádné přepsané clustery.
DSC_0125.JPG	I:\?\	5 926 kB	Výborný	Nebyly nalezeny žádné přepsané clustery.
DSC_0126.JPG	I:\?\	5 976 kB	Nelze obnovit	Soubor přepsán "I:\Sešit1.xlsx"
DSC_0127.JPG	I:\?\	6 042 kB	Nelze obnovit	Soubor přepsán "I:\$Extend\$RmMetadata\$TxfLog\$TxfLogContainer000000
DSC_0128.JPG	I:\?\	6 176 kB	Nelze obnovit	Soubor přepsán "I:\$Extend\$RmMetadata\$TxfLog\$TxfLogContainer000000
DSC_0129.JPG	I:\?\	5 595 kB	Nelze obnovit	Soubor přepsán "I:\$Extend\$RmMetadata\$TxfLog\$TxfLogContainer000000
DSC_0130.JPG	I:\?\	5 631 kB	Nelze obnovit	Soubor přepsán "I:\$Extend\$RmMetadata\$TxfLog\$TxfLogContainer000000
DSC_0131.JPG	I:\?\	5 759 kB	Nelze obnovit	Soubor přepsán "I:\Jive.mp4"
DSC_0132.JPG	I:\?\	5 561 kB	Nelze obnovit	Soubor přepsán "I:\Jive.mp4"
DSC_0133.JPG	I:\?\	5 605 kB	Nelze obnovit	Soubor přepsán "I:\Jive.mp4"
DSC_0134.JPG	I:\?\	5 721 kB	Nelze obnovit	Soubor přepsán "I:\Jive.mp4"
DSC_0136.JPG	I:\?\	6 072 kB	Nelze obnovit	Soubor přepsán "I:\Jive.mp4"
DSC_0137.JPG	I:\?\	6 106 kB	Nelze obnovit	Soubor přepsán "I:\Jive.mp4"
DSC_0138.JPG	I:\?\	5 597 kB	Špatný	Soubor přepsán "I:\Opportunity DNS_01_2014ffffffff.xlsx"
DSC_0139.JPG	I:\?\	6 003 kB	Výborný	Nebyly nalezeny žádné přepsané clustery.
DSC_0140.JPG	I:\?\	6 251 kB	Výborný	Nebyly nalezeny žádné přepsané clustery.

Obrázek 24 Přepis části dat způsobený defragmentací, výpis z programu Recuva

Zdroj: Archiv autora

Rychlé přeformátování

Rychlé formátování probíhalo ze souborového systému NTFS se zapsanými daty opět na NTFS. Tento postup používali cíleně pro odstranění dat i někteří respondenti.

V případě použití rychlého formátování se již situace oproti smazání souborů volbou „delete“ změnila. Rychlá analýza nenalezla žádná data, protože prohledává pouze alokační tabulky, které byly rychlým formátováním přepsány (znovu vytvořeny). Po hloubkové analýze bylo možné obnovit data, 4 soubory ze 168 byly poškozeny vlivem toho, že byly částečně přepsány tabulkami při rychlém formátování.

U flash disků došlo k zajímavému jevu, kdy po přeformátování bylo možné obnovit všechna data a žádná nebyla poškozená a to i u reklamního flash disku u něhož se stalo, že po prostém smazání nešla některá data obnovit.

Přeformátování

Formátování probíhalo ze souborového systému NTFS se zapsanými daty opět na NTFS. Po něm již byla pro obnovu nutná podrobná analýza prostoru (např. u Recuva trvala 72,41s a ActiveBootDisk 62,1s u 4GB reklamního flash disku). U pevného disku proběhlo opět přepsání 4 souborů na stejných místech tabulkami vytvářenými při formátování jako při rychlém formátování, jinak bylo možné data opět plně obnovit.

Na flash disku bylo možné obnovit všechna data, nedošlo k žádnému přepsání dat ani žádná data nebyla jinak poškozena.

Při zapnuté kompresi za běhu formátování se neprojevila žádná změna oproti předešlým zjištěním.

Změna souborového systému

Formátování měnící jeden souborový systém na jiný u pevného disku z NTFS na FAT32 a změně velikosti alokační jednotky nalezl program Recuva pouze 16 souborů (14JPEG a 2 dokumenty Word) analýza trvala 33s, program ActiveBootDisk obnovil 40 souborů různých typů, celková velikost byla pouze 14,4MB analýza trvala 47s, došlo k významnému poškození dat.

Při změně souborového systému na flash disku z FAT32 na exFAT se nepovedlo obnovit ani rekonstruovat použitému softwaru žádný soubor.

Zrušení oddílu na pevném disku

Při zrušení oddílu na pevném disku a přiřazením volného prostoru jinému existujícímu oddílu, nebo zrušením existujících oddílů a vytvořením jednoho společného se podařilo obnovit všechna původní data s výjimkou poškození několika souborů. Byl-li vytvořený oddíl naformátován stejným souborovým systémem jako předešlé, obnova trvala vzhledem k nutnosti projít celý disk pro rekonstrukci souborů 5:36:16 u programu ActiveBootDisk.

4.2.1.3 Experiment č. 3 Bezpečné smazání dat

Tento experiment měl za účel ověřit délku trvání odstranění dat na celém médiu (oddíl pevného disku o velikosti 0,98GB a Flash disku 4GB) a vybraných dat (168 různých souborů a typů o celkové velikosti 923MB) při použití různých metod/algoritmů a verifikovat, je-li možné data obnovit nebo identifikovat nějaké zbytky po smazání. K tomuto testu byl zvolen program Secure Eraser 4.201, protože poskytuje dostatečnou škálu metod odstranění a automaticky včleňuje možnosti bezpečného smazání do koše, navíc podává po odstranění přesný report o provedené činnosti.

Výsledek:

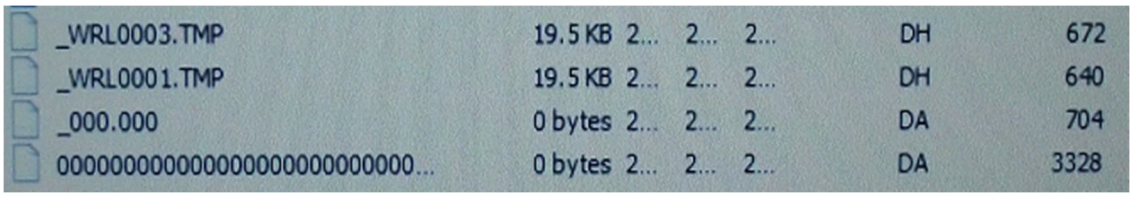
Jednotlivá zprůměrovaná časová náročnost zvolených metod z pěti měření je vidět v tabulce č. 6.

Metoda/ Algoritmus/ Norma	Počet cyklů	Doba mazání dat po jednotlivých datech HDD*	Celkové mazání diskového oddílu	Doba mazání dat po jednotlivých datech Flash disk*	Celkové smazání Flash disk
Random	1	0:03:23	0:00:32	0:04:52	0:19:44
US DoD 522.22-M E	3	0:10:13	0:01:22	0:12:11	0:42:12
German standart	7	0:22:11	0:01:45	0:23:33	0:52:59
US DoD 522.22-M ECE	7	0:25:14	0:03:31	0:27:14	1:53:07
Peter Gutmann standard	35	1:47:14	0:14:52	1:49:17	5:52:32

Tabulka 6 Přehled metod a průměrných dob 5x provedeného bezpečného mazání

Zdroj: Autor

Po přepsání celého oddílu a média, šla identifikovat pouze zvolená metoda podle specifických zbytků dat, nikoliv však počet ani jiné parametry předchozích dat. To samé platilo i u flash disku, u kterého byly dokonce odstraněny i předchozí kopie souborů při editaci. Jediné co zůstalo, byla data pro obnovu při náhlém selhání dokumentu Word, jak je patrné na obrázku.



Tabulka 7 Zbytek po bezpečném odstranění dvou souborů rychlou metodou

Zdroj: Archiv autora

5 Zhodnocení výsledků a doporučení

Zhodnocením výsledků ankety o problematice bezpečného mazání a obnovy dat vyplynulo, že povědomí o možnostech a rizicích je již rozšířené, ovšem neustále panuje mezi uživateli celá řada polopravd a omylů. Nejčastějším omylem je představa, že se formátováním odstraní data a následně je již nelze obnovit. Větší problém, jak se ukázalo, je běžné zacházení s citlivými daty, kde většina uživatelů nehledě na znalosti je maže jako běžná data. Zanedbávána je i likvidace citlivých dat na prodávaných, použitých a vyřazených médiích určených k vyhození. Podceňováno je tak riziko jejich zneužití k vydírání, bankovním podvodům a jiné trestné činnosti. To prokázaly i experimenty na několika získaných médiích, kde byla nalezena snadno zneužitelná citlivá data například intimní fotografie, zálohovaná osobní komunikace, hesla atd.

Výsledky experimentů se softwarovou obnovou při běžných situacích, kdy jsou smazány soubory, ukázaly, že tyto soubory lze ve většině případů jednoduše obnovit a časová náročnost této obnovy se převážně odvíjí od způsobu nechtěného smazání, celkové velikosti paměťového prostoru nutného analyzovat, rychlosti čtení a následně množství obnovovaných dat. Obnova proto může trvat sekundy nebo až desítky hodin. Soubory nelze plně obnovit pouze v tom případě, pokud jsou jejich paměťové sektory přepsány fyzicky jinými daty.

Z toho důvodu byla vytvořena následující navrhnutá doporučení, která mohou být implementována do směrnic bezpečnosti nebo mohou být použita jako návod pro běžného uživatele, zaručující bezpečné smazání dat, jistotu obnovy nechtěně smazaných dat a zvýšení zabezpečení dat.

První ze všeho by měla být ohodnocena jednotlivá data dle citlivosti a stejné ohodnocení musí dodržovat i datový nosič, na němž jsou tato data uložena, vždy podle nejvyšší citlivosti vyskytovaných dat. Rozdělí se na data a nosiče:

- veřejná: pro data volně šiřitelná
- důvěrná: data určená omezenému okruhu lidí (rodinné fotografie, údaje pro konkrétní osoby)

- osobní / interní: data pro vlastní potřebu (fotografie, poznámky, záloha telefonních kontaktů a komunikace atd.)
- tajná: v případě velmi důvěrných dokumentů (bankovní a přístupová hesla)

Za druhé nakládání s daty a médii během používání se musí řídit dle klasifikace dat a typu datového nosiče a doby skladování. Je nutné zabránit nepovolané osobě k přístupu k datům nebo k nosiči samotnému. U koncentrované zálohy neveřejných dat je vhodné použít dodatečné zabezpečení proti náhodnému úniku a to šifrováním informací nebo celého média.

Po expiraci dat kvalifikovaných jako důvěrná a výše, na nosiči, který je dále běžně používán musí být tato data bezpečně odstraněna speciálním programem (např. Secure Erase). V případě, že tato data byla na médiu s pamětí flash, musí být vyčištěn i volný prostor tohoto média. Pokud je běžný výskyt dat s klasifikací interní a důvěrná na SSD disku je nutné tento disk mít šifrovaný nebo zamezit přístupu nepovolané osobě.

Za třetí je důležité i správné nakládání s nosiči po vyřazení i při jejich nefunkčnosti. Po skončení životnosti nosiče dat, s ním musí být nakládáno dle dřívějšího obsahu a typu. Obsahuje-li pouze veřejná data, postačí prostá likvidace. V opačném případě jedná-li se o optické médium, musí být skartováno, funkční magnetické či flash médium bezpečně vymazáno některou z výše popsaných metod.

U nefunkčního optického média je nutná opět skartace, magnetické médium by mělo být demagnetizováno a mechanicky poškozeny datové vrstvy. U média či zařízení obsahující flash paměťové čipy musí být mechanicky zničeny všechny tyto čipy.

Za čtvrté pro obnovu dat, která poskytuje oprávněnou jistotu, že se povede obnovit všechna omylem smazaná data i po dlouhém časovém intervalu od smazání, až po zjištění ztráty (ať vinou uživatele nebo havárií zařízení) lze dosáhnout v běžných nekomerčních podmínkách pouze důsledným pravidelným automatickým rozdílovým/přírůstkovým zálohováním na dostatečně velké zálohovací médium, které by mělo umožňovat i přepis dat, aby se dalo opět použít po exspiraci zálohy.

Výběr média by měl odpovídat množství zálohovaných dat. Napovědět nejefektivnějšímu výběru by mohl průzkum ceny za jednotku prostoru (GB) na běžně dostupných přepisovatelných médiích. Z pohledu ceny za jednotku prostoru objemu zálohovaných dat a životnosti s přihlédnutím k rychlosti následné obnovy, ve většině případů vychází nejlépe externí pevný disk.

Médium	GB	Cena s DPH (czc.cz 24. 2. 2014)	cena/GB
Flash disk	32	395	12,34
Externí pevný disk	1000	1841	1,84
Externí SSD disk	128	2870	22,42
CD-RW	0,7	17.1	24,57
DVD-RW	4,7	29,9	6,36
Blu-ray-RW	25	49,2	1,97

Tabulka 8 Porovnání cena/GB u různých médií

Zdroj: Autor

Omylem smazaná data, jejichž smazání bylo záhy objeveno a hodnota dat je nízká, je navrhováno použití softwarového nástroje pro obnovu ActiveBootDisk, nebo obdobného softwaru, který se nemusí instalovat na dotčené médium a nikdy na něj nezapisuje žádná data.

6 Závěr

Počítačová gramotnost uživatelů v této oblasti je již dnes na poměrně uspokojivé úrovni, mnohá základní rizika si běžně uživatelé uvědomují. I přes veškeré publikované informace, odborné články a studie jim zůstávají mnohá nebezpečí neznámá. Zarážející je fakt, že i když tato rizika jsou části uživatelů známa, jsou ignorována, nebrána v potaz, nebo je volen nedostačující postup, zejména při odstraňování dat, přestože na trhu existuje mnoho prostředků na bezpečnou likvidaci jednotlivých dat i komponentů. Mnozí si neuvědomí závažnost možných důsledků svého jednání, pokud data a nosiče dat nesprávně likvidují. Rizika spojená s takovým chováním jsem se pokusil názorně ukázat na obnově citlivých dat ze získaných použitých médií. Potvrdilo se, že při nesprávně zvoleném postupu smazání dat může hrozit riziko vydírání nebo finanční ztráty způsobené cizí osobou za použití nalezených dat.

Naopak o obnovitelnosti zdánlivě ztracených dat, má většina běžných uživatelů základní povědomí. Část uživatelů je schopna svá data opět získat zpět pomocí různého volně dostupného softwaru, případně datových záloh. Zbytek se obrací na profesionály, kteří jim s touto problematikou pomohou.

Závěrem lze shrnout, že nezbývá než i nadále se snažit zvyšovat počítačovou gramotnost v této oblasti důkladnou osvětou, především mezi běžnými uživateli. Doufám, že i moje práce přispěje ke zlepšení povědomosti o nakládání s citlivými údaji.

7 Bibliografie

1. **Tišnovský, Pavel.** Magneticke pameti. *Root.cz.* [Online] Internet Info, s.r.o, 24. 7 2008. [Citace: 4. 11 2013.] http://www.root.cz/clanky/magneticke-pameti-pro-trvaly-zaznam-dat/. ISSN 1212-8309.

2. **ABAX SERVISNÍ CENTRUM s.r.o.** Záchrana a obnova dat. *ABAX.* [Online] ABAX SERVISNÍ CENTRUM s.r.o. [Citace: 9. 11 2013.] http://www.abax.cz/cz/zachrana-dat-a-obnova-dat/.

3. **Dembowski, Klaus.** *Mistrovství v Hardware.* 1. vydání. Brno : Computer Press, a.s., 2009. str. 712. ISBN 978-80-251-2310-2.

4. [Online] [Citace: 20. 11 2013.] http://hyperphysics.phy-astr.gsu.edu/hbase/audio/tape2.html.

5. **Horák, Jaroslav.** *Hardware učebnice pro pokročilé.* 3. vydání. Brno : CP Books, a.s., 2005. str. 344. ISBN 80-251-0647-0.

6. [Online] [Citace: 22. 11 2013.] http://www.primerpc.com/hardware/cdrom.htm.

7. **Messmer, Hans-Peter a Dembowski, Klaus.** *Velká kniha Hardware.* 1. vydání. Brno : CP Books, a.s., 2005. str. 1224. ISBN 80-251-0416-8.

8. **Krčmář, Petr.** DVD-RAM v linuxu. *ROOT.CZ.* [Online] Internet Info s.r.o., 22. 9 2005. [Citace: 6. 11 2013.] http://www.root.cz/clanky/dvd-ram-v-linuxu/. ISSN 1212-8309.

9. **Tišnovský, Pavel.** Vývoj optických pamětí. *Root.cz.* [Online] Internet Info, s.r.o., 11. 9 2008. [Citace: 6. 11 2013.] http://www.root.cz/clanky/vyvoj-optickych-pameti-od-dvd-k-blu-ray/#k06. ISSN 1212-8309.

10. —. Nevolatilní paměti. *Root.cz.* [Online] Internet Info, s.r.o., 18. 9 2008. [Citace: 7. 11 2013.] http://www.root.cz/clanky/nevolatilni-pameti/#ic=serial-box&icc=text-title. ISSN 1212-8309.

11. **Vondrášek, Martin.** Princip a vlastnosti USB flash paměti. *fallvonder.* [Online] 2009. [Citace: 20. 11 2013.] http://fallvonder.net/rest/flashtech/vondrm4-y31-eliflash.pdf.

12. **Vlček, Václav.** *PC TUNING.* [Online] EMPRESA MEDIA, a.s., 1. 12 2010. [Citace: 22. 11 3013.] http://pctuning.tyden.cz/hardware/disky-cd-dvd-br/19426-velka-vanocni-soutez-o-tri-ssd-disky-intel-druhe-generace. ISSN 1214-0201.

13. **Tišnovský, Pavel.** Magnetooptické disky. *Root.cz.* [Online] Internet Info, s.r.o, 14. 8 2008. [Citace: 6. 11 2013.] http://www.root.cz/clanky/magnetoopticke-disky/. ISSN 1212-8309.

14. **Hudson, Andrew.** NTFS: A File System with Integrity and Complexity. *OSnews.* [Online] OSNews Inc., 29. 11 2010. [Citace: 8. 12 2013.] http://www.osnews.com/story/24076/NTFS_A_File_System_with_Integrity_and_Complexity.

15. **Buse, Jarret W.** EXT File System. *Linux.org.* [Online] 31. 6 2013. [Citace: 15. 12 2013.] http://www.linux.org/threads/ext-file-system.4365/.

16. **Zima, Jiří.** *NOOTEBOKblog.* [Online] 27. 9 2011. [Citace: 5. 1 2014.] http://notebookblog.cz/technika/navody/zkusenosti-s-sifrovanim-disku-nastrojem-truecrypt/.

17. **support.apple.** OS X Mountain Lion: Prevent deleted files from being read. *Apple.* [Online] Apple Inc., 21. 8 2012. [Citace: 1. 12 2013.] http://support.apple.com/kb/PH11124?viewlocale=en_US.

18. **Windfinder.** Bezpečné smazání dat (Ubuntu). *Větrniště.* [Online] 1. 10 2007. [Citace: 19. 12 2013.] http://vetrnikplejs.blogspot.cz/2007/10/bezpen-smazn-dat-ubuntu.html.

19. **Wright, Craig, Kleiman, Dave a Shyaam, Sundhar.** *CERN Computer Security.* [Online] 2008. [Citace: 27. 12 2013.] https://security.web.cern.ch/security/rules/images/overwriting-hard-drive-data.pdf.

20. **Svojanovský, Petr.** Nepodceňujte skartaci dat. *Computerworld.* [Online] 18. 3 2011. [Citace: 28. 12 2013.] http://computerworld.cz/securityworld/nepodcenujte-skartaci-dat-48028.

21. **Fisher, Tim.** DoD 5220.22-M. *About.com PC Support.* [Online] [Citace: 28. 12 2013.] http://pcsupport.about.com/od/termsd/g/dod-5220-22-M.htm.

22. **Wie, Michael, a další, a další.** Reliably Erasing Data From Flash-Based Solid State Drives. *Usenix The advanced computing systems association.* [Online] [Citace: 5. 12 2013.] https://www.usenix.org/legacy/event/fast11/tech/full_papers/Wei.pdf. ISBN: 978-1-931971-82-9.

23. **Linkedin.** Degaussing - bezpečné mazání dat. [Online] [Citace: 29. 12 2013.] http://www.linkedin.com/company/diskus-spol-s-r-o-/degaussing-bezpe-n-maz-n-dat-1572946/product?trk=biz_product.

24. The Best Ways to Destroy a Hard Drive! *whitakerbrothers.* [Online] hubpages, 14. 3 2012. [Citace: 6. 1 2014.] http://whitakerbrothers.hubpages.com/hub/solid-state-hard-drive-destruction.

25. **Turle, Marcus a autorů, Kolektiv.** Data Protection Laws of the world. *dlapiperdataprotection.* [Online] 3 2013. [Citace: 14. 1 2014.] dlapiperdataprotection.com/. ISBN: 9780752005485.

26. **Černý, Jiří.** NAS vs. SAN - jak na správu dat? *svethardware.* [Online] 26. 8 2009. [Citace: 14. 1 2014.] http://www.svethardware.cz/nas-vs-san-jak-na-spravu-dat/27556.

27. **Bouška, Petr.** SSD disk a Windows 7. *Samuraj-cz.* [Online] 1. 11 2011. [Citace: 5. 12 2013.] http://www.samuraj-cz.com/clanek/ssd-disk-a-windows-7/.

28. **Chip, Redakce.** Trendy: Magnetická páska slaví 60. výročí. *Chip.cz.* [Online] BURDA Praha s.r.o., 21. 5 12. [Citace: 3. 11 2013.] http://www.chip.cz/trendy/magneticka-paska-slavi-60-vyroci/.

29. **Kolář, Pavel.** Oracle uvedl na trh magnetické pásky s kapacitou 8,5 TB. *itbiz.cz.* [Online] Argonit s.r.o., 13. 9 2013. [Citace: 3. 11 2013.] http://www.itbiz.cz/zpravicky/oracle-uvedl-na-trh-magneticke-pasky-s-kapacitou-8-5-tb. ISSN 1802-1581.

30. **Dedek, Jan.** Vše o DVD. *pctuning.* [Online] EMPRESA MEDIA, a.s., 25. 10 2004. [Citace: 6. 11 2013.]

http://pctuning.tyden.cz/index.php?option=com_content&id=4237&Itemid=46. ISSN 1214-0201.

31. **Petržela, Radim a Systems, Hitachi Data.** eMLC SSD – rozhodně ANO! . *Data v péči.* [Online] MHM computer a.s., 28. 3 2013. [Citace: 15. 1 2014.] http://www.datavpeci.cz/webdvp.nsf/articles/3AD9B646521603BAC1257B3C006A988B.

32. **Tanenbaum, Andrew S. a Wooldhull, Albert S.** *Operatings systems Design and Implementation.* 3. vydání. místo neznámé : Prentice Hall, 2006. str. 1080. Jazyk: Anglicky. ISBN 978-0131429383.

33. nutne-vybaveni-rizika-neprofesionalni-zachrany-dat. *Záchrana dat a obnova dat.* [Online] http://www.zachranadat-obnovadat.cz/nutne-vybaveni-rizika-neprofesionalni-zachrany-dat/.

8 Seznam použitých obrázků, grafů tabulek

Obrázek 1 Pevný disk (2) 13

Obrázek 2 Znázornění uspořádání pevného disku souborový systém Fat (3 str. 171) 14

Obrázek 3 Znázornění zápisu na magnetickou pásku (zde magnetická páska stero kazety) (4) 17

Obrázek 4 Princip čtení u optických disků (5 str. 206) 18

Obrázek 5 Přechod z pitu a land (6) 19

Obrázek 6 Struktura disku CD-ROM a znázornění uložení dat (3 str. 281) 19

Obrázek 7 Znázornění vrstev CD-R (3 str. 284) 20

Obrázek 8 Znázornění vrstev CD-RW (3 str. 286) 21

Obrázek 9Reálný pohled a schéma média DVD-RAM (8) 22

Obrázek 10 Znázornění všech rozdílů u jednotlivých optických médií (9) 23

Obrázek 11 Konstrukce paměťové buňky (11) 27

Obrázek 12 Programování a vymazání flash paměti typu NAND (11) 28

Obrázek 13 Rozdíl vnitřní konstrukce SSD a pevného disku (HDD) 29

Obrázek 14 Znázornění množství typů paměťových karet 31

Obrázek 15 Znázornění drážky a jednotlivých vrstev optomagnetického disku (13) 33

Obrázek 16 Kde najít a nastavit bezpečné vymazání (17) 40

Obrázek 17 KESENDER 2 44

Obrázek 18 Garner PD-4 (24) 46

Obrázek 19 Připájení odlomeného USB konektoru falsh disku 63

Obrázek 20 Příklad citlivých dat, která měla být bezpečně smazána 65

Obrázek 21 Průběh obnovy externího disku ActiveBootDisk 65

Obrázek 22 Všechny zjištěné soubory po krocích pokusu 67

Obrázek 23 Výsledek defragmentace 68

Obrázek 24 Přepis části dat způsobený defragmentací, výpis z programu Recuva 69

Grafy 1 Souhrn charakterizujících údajů o složení respondentů z otázek 14,15,16 55

Graf 2 Výsledek otázky č. 2 56

Graf 3 Výsledek otázky č. 4 57

Graf 4 Výsledek otázky č. 10 58

Graf 5 Výsledek otázky č. 12 58

TABULKA 1 ZÁKLADNÍ ÚDAJE O PROVEDENÉ ANKETĚ 54
TABULKA 2 ZDROJE RESPONDENTŮ 55
TABULKA 3 EXTRAHOVANÁ DATA PRO OVĚŘENÍ ZÁVISLOSTI 59
TABULKA 4 VÝSLEDEK VÝPOČTU ZÁVISLOSTI 60
TABULKA 5 PŘEHLED MÉDIÍ PRO EXPERIMENT Č.1 62
TABULKA 6 PŘEHLED METOD A PRŮMĚRNÝCH DOB 5X PROVEDENÉHO BEZPEČNÉHO MAZÁNÍ 71
TABULKA 7 ZBYTEK PO BEZPEČNÉM ODSTRANĚNÍ DVOU SOUBORŮ RYCHLOU METODOU 71
TABULKA 8 POROVNÁNÍ CENA/GB U RŮZNÝCH MÉDIÍ 74

9 Přílohy

9.1 Příloha č. 1: Strukturování dotazníku

1. Myslíte si, že soubory vysypané z koše (např. ve Windows) jsou nenávratně ztraceny?
Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí a podle toho se mu zobrazily další otázky [Ano → otázka č. 3, Ne → otázka č. 2].

Nabízené odpovědi: Ano; Ne

2. Jak běžně odstraňujete citlivá data (soukromé fotografie, finanční záznamy, privátní archivovanou korespondenci atd.) na pevném disku nebo jiném přepisovatelném médiu, které denně používáte?
Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí. Nehledě na volbu následuje otázka č. 3.

Nabízené odpovědi:

- Odstraněním do koše a jeho vysypáním (jako běžná data)
- Odstraněním a vyčištěním volného místa paměti v určitém časovém cyklu (týdně, měsíčně)
- Odstraněním speciálním programem

3. V případě prodeje/darování Vámi použité elektroniky (fotoaparát, telefon, tablet, počítač) prodáváte/darujete s vyjímatelnou paměťovou kartou/diskem)?
Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí a podle toho se mu zobrazily další otázky [Ano → otázka č. 4, Ne → otázka č. 5].

Nabízené odpovědi: Ano; Ne

4. Na tomto médiu data před prodejem/darováním?
Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí. Nehledě na volbu následuje otázka č. 5.

Nabízené odpovědi:

- Zvolím volbu smazat
- Médium naformátuji rychle
- Médium naformátuji

- Speciální program/ Vyčitění prázdného místa na médiu

5. Pokud tato elektronika má i vlastní integrovanou paměť tak data na ní před prodejem/darováním?
Povinná otázka, respondent musel zvolit alespoň některou z nabízených odpovědí nebo dopsat nějakou vlastní (min. 1). Nehledě na volbu následuje otázka č. 6.

Nabízené odpovědi:

- Obnovím tovární nastavení
- Data přes volbu smazat v menu odstraním
- Vlastní odpověď:

6. Pokud paměťové médium přestane fungovat (Disk, CD, atd. nemohu načíst data) tak?
Povinná otázka, respondent musel zvolit alespoň některou z nabízených odpovědí nebo dopsat nějakou vlastní (min. 1). Nehledě na volbu následuje otázka č. 7.

Nabízené odpovědi:

- Vyhodím, nic jiného nedělám
- Před vyhozením CD poškrábu
- CD skartuji kancelářskou skartovačkou
- Pevný disk, flash disk fyzicky poškodím
- Disk fyzicky poškodím a zmagnetizuji
- Zařízení obsahující interní paměť fyzicky poškodím
- Zařízení osahující interní paměť fyzicky a magneticky poškodím
- Vlastní odpověď:

7. V případě, že paměťové médium (disk, flash disk) měním kvůli upgradu hardwaru (médium je stále běžně čitelné). Tak staré médium?
Povinná otázka, respondent musel zvolit alespoň některou z nabízených odpovědí nebo dopsat nějakou vlastní (min. 1). Nehledě na volbu následuje otázka č. 8.

Nabízené odpovědi:

- Tuto situaci jsem ještě neřešil/a
- Jednoduše vyhodím do elktro odpadu
- Naformátuji a vyhodím
- Fyzicky poškodím a následně vyhodím
- Pevný disk zmagnetizuji, flash disk fyzicky zcela zničím

- Vlastní odpověď:

8. V případě, že likviduji paměťové médium (CD, DVD, Blu-ray). Tak staré médium?
Povinná otázka, respondent musel zvolit alespoň některou z nabízených odpovědí nebo dopsat nějakou vlastní (min. 1). Nehledě na volbu následuje otázka č. 9.

Nabízené odpovědi:

- Poškrábu ze zdola
- Poškrábu ze zhora
- Poškrábu z obou stran
- Rozlomím
- Skartuji ve skartovačce
- Vlastní odpověď:

9. Zálohujete Vaše data?
Povinná otázka, respondent musel zvolit alespoň některou z nabízených odpovědí nebo dopsat nějakou vlastní (min. 1). Nehledě na volbu následuje otázka č. 10.

Nabízené odpovědi:

- Ne
- Ano, mám je zkopírovaná na (CD, DVD, externím disku, flash disku)
- Ano, využívám cloudového vzdáleného úložiště (např. Dropbox)
- Ano, využívám diskového pole s RAID technologií na všechna data
- Vlastní odpověď:

10. Smazali/ztratili jste někdy nechtěně data na paměťovém médiu (pevný disk, CD, Flash disk atd.) tak, že nebyla viditelná ani v koši
Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí. Nehledě na volbu následuje otázka č. 11.

Nabízené odpovědi: Ano; Ne

11. Víte, že existuje možnost tato data obnovit.
Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí a podle toho se mu zobrazily další otázky [Ano → otázka č. 12, Ne → otázka č. 14].

Nabízené odpovědi: Ano; Ne

12. Pokusili jste se někdy data obnovit?

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí a podle toho se mu zobrazily další otázky [Ano → otázka č. 13, Ne → otázka č. 14].

Nabízené odpovědi: Ano; Ne

13. Obnovili jste tato data?

Povinná otázka, respondent musel zvolit alespoň některou z nabízených odpovědí nebo dopsat nějakou vlastní (min. 1). Nehledě na volbu následuje otázka č. 14.

Nabízené odpovědi:

- Neřešil/a jsem data nebyla podstatná
- Ano, data jsem měl zálohovaná
- Ano, za použití speciálního programu
- Ano, za použití odborné firmy
- Ne, nosič byl fyzicky poškozen a nepodařilo se data obnovit
- Vím, že je určitá možnost data obnovit, ale nevím jak (nebo se nepodařilo)
- Některá data jsem obnovil/obnovila, některá se nepodařilo
- Vlastní odpověď:

14. Váš věk?

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí. Nehledě na volbu následuje otázka č. 15.

Nabízené odpovědi:

- 0-15
- 16-30
- 46-60
- 60+

15. IT/ICT znalosti (používání počítače)

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí. Nehledě na volbu následuje otázka č. 16.

- Nabízené odpovědi:
- Pouze základní znalosti soukromé a běžné kancelářské používání
- Soukromé dobré znalosti IT/ICT
- Soukromé velmi dobré znalosti IT/ICT
- Práce/ studium v IT/ICT oboru

16. Nejvyšší dosažené vzdělání
Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí. Následuje konec dotazníku.
Nabízené odpovědi:

- Základní škola
- Střední škola bez maturiti a učiliště
- Střední škola s maturitou
- Vyšší odborná škola
- Vysokoškolské vzdělání

9.2 Příloha č. 2 Kompletní výsledky dotazníkového šetření

1. Myslíte si, že soubory vysypané z koše (např. ve Windows) jsou nenávratně ztraceny?

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí a podle toho se mu zobrazily další otázky [Ano → otázka č. 3, Ne → otázka č. 2].

Odpověď	Počet	Lokálně	Globálně
Ne	167	90,76%	90,76%
Ano	17	9,24%	9,24%

2. Jak běžně odstraňujete citlivá data (soukromé fotografie, finanční záznamy, privátní archivovanou korespondenci atd.) na pevném disku nebo jiném přepisovatelném médiu, které denně používáte?
Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí.

Odpověď	Počet	Lokálně	Globálně
Odstraněním do koše a jeho vysypáním (jako běžná data)	106	63,47%	57,61%
Odstraněním a vyčištěním volného místa paměti v určitém časovém cyklu (týdně, měsíčně)	31	18,56%	16,85%
Odstraněním speciálním programem	30	17,96%	16,30%

3. V případě prodeje/darování Vámi použité elektroniky (fotoaparát, telefon, tablet, počítač) prodáváte/darujete s vyjímatelnou paměťovou kartou/diskem)?

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí a podle toho se mu zobrazily další otázky [Ano → otázka č. 4, Ne → otázka č. 5].

Odpověď	Počet	Lokálně	Globálně
Ne	133	72,28%	72,28%
Ano	51	27,72%	27,72%

4. Na tomto médiu data před prodejem/darováním?

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí.

Odpověď	Počet	Lokálně	Globálně
Médium naformátuji	30	58,82%	16,30%
Speciální program/Vyčištění prázdného místa na médiu	10	19,61%	5,43%
Zvolím volbu smazat	7	13,73%	3,80%
Médium naformátuji rychle	4	7,84%	2,17%

5. Pokud tato elektronika má i vlastní integrovanou paměť tak data na ní před prodejem/darováním?

Povinná otázka, respondent musel zvolit alespoň některou z nabízených odpovědí nebo dopsat nějakou vlastní (min. 1).

Odpověď	Počet	Lokálně	Globálně
Obnovím tovární nastavení	114	61,96%	61,96%
Data přes volbu smazat v menu odstraním	84	45,65%	45,65%
formátuji	1	0,54%	0,54%
já bych poradila, protože to nepatří mezi můj obor	1	0,54%	0,54%
odstraním pomocí software	1	0,54%	0,54%
Použiji program na vymazání dané paměti.	1	0,54%	0,54%
elektroniku nedaruji	1	0,54%	0,54%
Smazat, prepsat jinymi (nedulezitymi) daty, opet smazat	1	0,54%	0,54%
jiný	1	0,54%	0,54%
nepředávám, ale v případě předání bych formátoval	1	0,54%	0,54%
zatím sem nemusela řešit	1	0,54%	0,54%
smazání + formátování	1	0,54%	0,54%
format	1	0,54%	0,54%

Nic neprodávám.	1	0,54%	0,54%
Speciální program	1	0,54%	0,54%
nafotím oblohu, nahraju "nic" nahraju obecný film apod.	1	0,54%	0,54%
preinstaluji system	1	0,54%	0,54%
mám všechny disky šifrované, tedy nic nepročišťuji, protože to není potřeba	1	0,54%	0,54%
jeste nikdy sem nedaroval ani neprodal a ani bych to neudelala	1	0,54%	0,54%
případně přeformátování speciálním programem	1	0,54%	0,54%
neřešila jsem	1	0,54%	0,54%
formátování	1	0,54%	0,54%

6. Pokud paměťové médium přestane fungovat (Disk,CD, atd. nemohu načíst data) tak?

Povinná otázka, respondent musel zvolit alespoň některou z nabízených odpovědí nebo dopsat nějakou vlastní (min. 1).

Odpověď	Počet	Lokálně	Globálně
Disk/flash disk fyzicky poškodím	68	36,96%	36,96%
Vyhodím nic jiného nedělám	63	34,24%	34,24%
Před vyhozením CD poškrábu	53	28,80%	28,80%
Zařízení obsahující interní paměť fyzicky poškodím	34	18,48%	18,48%
CD skartuji kancelářskou skartovačkou	29	15,76%	15,76%
Disk/flash disk fyzicky poškodím a zmagnetizuji	26	14,13%	14,13%
Zařízení obsahující interní paměť fyzicky a magneticky poškodím	24	13,04%	13,04%
zformátuji,pokud je to možné	1	0,54%	0,54%
rozeberu, rozlámu, atp.	1	0,54%	0,54%
CD/DVD rozstříhám na kusy.	1	0,54%	0,54%
flash disk jsem ještě nikdy nevyhazovala	1	0,54%	0,54%
Nevim	1	0,54%	0,54%
se pokusím o opravu	1	0,54%	0,54%
záleží jaká data jsou na nosiči	1	0,54%	0,54%
CD a DVD používám jako dekoraci.	1	0,54%	0,54%

většinou řeším brutální silou, kladivo, svěrák, apod.	1	0,54%	0,54%
Odnesu ho do servisu, aby zachránili data	1	0,54%	0,54%
tahle situace se mi jeste nestala	1	0,54%	0,54%
nechávám doma a nikam nevyhazuju	1	0,54%	0,54%
To bych udělala, ale neřešila jsem	1	0,54%	0,54%
crash - bum kladivem	1	0,54%	0,54%

7. V případě, že paměťové médium (disk, flash disk) měním kvůli upgrade hardwaru (médium je stále běžně čitelné). Tak staré médium?

Povinná otázka, respondent musel zvolit alespoň některou z nabízených odpovědí nebo dopsat nějakou vlastní (min. 1).

Odpověď	Počet	Lokálně	Globálně
Tuto situaci jsem ještě neřešil/a	102	55,43%	55,43%
Fyzicky poškodím a následně vyhodím	20	10,87%	10,87%
Naformátuji a vyhodím	18	9,78%	9,78%
Jednoduše vyhodím do elektro odpadu	13	7,07%	7,07%
Pevný disk z magnetizuji, fyzicky zcela zničím	9	4,89%	4,89%
Necham si ho	2	1,09%	1,09%
ponechám schovaný	1	0,54%	0,54%
zatím mám v šuplíku	1	0,54%	0,54%
naformátuji a daruji	1	0,54%	0,54%
bud vycistim data a daruji nebo si ho necham	1	0,54%	0,54%
schovám, může se někdy hodit	1	0,54%	0,54%
naformátuji a případně věnuji rodiným příslušníkům jako upgrade k jejich PC	1	0,54%	0,54%
Většinou zachovám pro možné pozdější využití jako záloha dat. Až po poškození a nemožnosti čtení vyhazuji.	1	0,54%	0,54%
Ponechám si ho, může se hodit	1	0,54%	0,54%
nechám si je, pokud fungují mohou je ještě hodit	1	0,54%	0,54%
Uložím jako zálohu dat	1	0,54%	0,54%
Použiji ho jako záložní	1	0,54%	0,54%
prepisu nekolikrat	1	0,54%	0,54%

ponechám si ho	1	0,54%	0,54%
Nechám si v trezoru.	1	0,54%	0,54%
prodám na aukru :)	1	0,54%	0,54%
dd if=/dev/urandom of=/dev/sdx	1	0,54%	0,54%
u HDD koupím box a vytvořím z něj externí disk	1	0,54%	0,54%
rána kladivem, vyhodit jako elektrotechnický odpad	1	0,54%	0,54%
schovám do šuplíku	1	0,54%	0,54%
Ponechám jako záložní médium.	1	0,54%	0,54%

8. V případě, že likviduji paměťové médium (CD, DVD, Blu-ray). Tak staré médium?

Povinná otázka, respondent musel zvolit alespoň některou z nabízených odpovědí nebo dopsat nějakou vlastní (min. 1).

Odpověď	Počet	Lokálně	Globálně
Rozlomím	113	61,41%	61,41%
Skartuji ve skartovačce	17	9,24%	9,24%
Poškrábu ze zdola	14	7,61%	7,61%
Poškrábu z obou stran	9	4,89%	4,89%
Poškrábu ze zhora	6	3,26%	3,26%
nic	3	1,63%	1,63%
vyhodím	3	1,63%	1,63%
spálím	2	1,09%	1,09%
vyhodim do koše	1	0,54%	0,54%
jen tak vyhodím	1	0,54%	0,54%
Vůbec s nim nic nedělám	1	0,54%	0,54%
Rozstřihnu - skartovačku nemám :-)	1	0,54%	0,54%
použiju na odhánění ptactva	1	0,54%	0,54%
Nelikviduji, archivuji. JInak ale záleží na obsahu.	1	0,54%	0,54%
Poškrábu z obou stran a rozlomím	1	0,54%	0,54%
jen vyhodím do odpadu	1	0,54%	0,54%
prostě vyhodím, nijak nepoškozuji	1	0,54%	0,54%
Používám jako dekoraci.	1	0,54%	0,54%

využiji k tvorbě	1	0,54%	0,54%
Rozsekám majzlíkem nebo rozřežu pilkou.	1	0,54%	0,54%
záleží co na něm je (film jen vyhodím) jinak rozlomím	1	0,54%	0,54%
jeste jsem neresila	1	0,54%	0,54%
Rozlámat i poškrábat, pokud je důležité chránit data, skartovačka je není vždy při ruce.	1	0,54%	0,54%
rozlámu, do odpadu	1	0,54%	0,54%
neřeším, neukládám citlivé informace na CD	1	0,54%	0,54%

9. Zálohujete Vaše data?

Povinná otázka, respondent musel zvolit alespoň některou z nabízených odpovědí nebo dopsat nějakou vlastní (min. 1).

Odpověď	Počet	Lokálně	Globálně
Ano, mám je zkopírovaná na (CD, DVD, externím disku, flash disku)	128	69,57%	69,57%
Ano, využívám cloudového vzdáleného úložiště (např. Dropbox)	44	23,91%	23,91%
Ano, mám je ve více složkách(nebo na C:a zároveň D: disku v pc)	36	19,57%	19,57%
Ne	24	13,04%	13,04%
Ano, využívám diskového pole s RAID technologií na všechna data	13	7,07%	7,07%
Jak kdy, jak která	1	0,54%	0,54%
Na e-mail	1	0,54%	0,54%
2,5 disk extr.	1	0,54%	0,54%
Mám na více médiích a někdy i počítačích	1	0,54%	0,54%
nahrávám na separátní HDD, který běžně nepoužívám, tento uschovávám mimo bydleště = u příbuzných. Totéž i s DVD, CD disky	1	0,54%	0,54%

10. Smazali/ztratili jste někdy nechtěně data na paměťovém médiu (pevný disk, CD, Flash disk atd.) tak, že nebyla viditelná ani v koši

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí.

Odpověď	Počet	Lokálně	Globálně
Ano	119	64,67%	64,67%
Ne	65	35,33%	35,33%

11. Víte že existuje možnost tato data obnovit.

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí a podle toho se mu zobrazily další otázky [Ano → otázka č. 12, Ne → otázka č. 14].

Odpověď	Počet	Lokálně	Globálně
Ano	152	82,61%	82,61%
Ne	32	17,39%	17,39%

12. Pokusili jste se někdy data obnovit?

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí a podle toho se mu zobrazily další otázky [Ano → otázka č. 13, Ne → otázka č. 14].

Odpověď	Počet	Lokálně	Globálně
Ano	86	56,21%	46,74%
Ne	67	43,79%	36,41%

13. Obnovili jste tato data?

Povinná otázka, respondent musel zvolit alespoň některou z nabízených odpovědí nebo dopsat nějakou vlastní (min. 1).

Odpověď	Počet	Lokálně	Globálně
Ano, za použití speciálního programu	66	76,74%	35,87%
Ano, data jsem měl zálohována	29	33,72%	15,76%
Ne, mnou zvolený program data neobnovil	10	11,63%	5,43%
Neřešil jsem data nebyla podstatná	8	9,30%	4,35%
Ano, za pomocí odborné firmy	7	8,14%	3,80%
Ne, nosič byl fyzicky poškozen a nepodařilo se mi data obnovit	4	4,65%	2,17%
Vím, že je určitá možnost data obnovit, ale nevím jak (nebo se nepodařilo)	2	2,33%	1,09%
Některá data jsem obnovil, některá se nepodařilo.	1	1,16%	0,54%
když je nejhůř, využívám lamaexpert.cz	1	1,16%	0,54%

14. Váš věk?

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí.

Odpověď	Počet	Lokálně	Globálně
16-30	147	79,89%	79,89%
31-45	20	10,87%	10,87%
46-60	14	7,61%	7,61%
60+	3	1,63%	1,63%

15. IT/ICT znalosti (používání počítače)

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí.

Odpověď	Počet	Lokálně	Globálně
Pouze základní znalosti soukromé a běžné kancelářské používání	79	42,93%	42,93%
Práce/studium v IT/ICT oboru	50	27,17%	27,17%
Soukromé dobré znalosti IT/ICT	45	24,46%	24,46%
Soukromé velmi dobré znalosti IT/ICT	10	5,43%	5,43%

16. Nejvyšší dosažené vzdělání

Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí.

Odpověď	Počet	Lokálně	Globálně
Vysokoškolské vzdělání	96	52,17%	52,17%
Střední škola s maturitou	79	42,93%	42,93%
Základní škola	4	2,17%	2,17%
Vyšší odborná škola	3	1,63%	1,63%
Střední škola bez maturity	2	1,09%	1,09%