Forenzní analýzy šifrovaných dat

Bc. Miroslav Smejkal

Diplomová práce
2015

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2014/2015

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Miroslav Smejkal**
Osobní číslo:	**A13412**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Forenzní analýzy šifrovaných dat**
Téma anglicky:	**A Forensic Analysis of Encrypted Data**

Zásady pro vypracování:

1. **Specifikujte dnešní možnosti šifrování dat na osobních počítačích dle konkrétních vlastností jednotlivých šifrovacích softwarů.**
2. **Analytzujte možnosti získání informací k zašifrovaným datům za pomoci zálohy a následné analýzy paměti RAM.**
3. **Specifikujte postupy nalezení zašifrovaných dat na digitálních stopách a následné získání informací z těchto dat.**
4. **Proveďte srovnání výkonnosti a nabízených funkcí u dostunych SW nástrojů (Elcomsoft, Passware, Extreme GPU Bruteforcer, hashcat) využitelných na získání informací ze zašifrovaných dat.**
5. **Vytvořte metodiku pro bezpečné zašifrování dat na osobních počítačích, stanovte parametry hesla a nastavení daného operačního systému.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **BAUER, Craig P. Secret history: the story of cryptology. Boca Raton: Taylor, 2013, xxv, 594 s. Discrete mathematics and its applications. ISBN 978-1-4665-6186-1.**
2. **LIGH, Michael Hale. The art of memory forensics: detecting malware and threats in windows, linux, and mac memory. pages cm. ISBN 11-188-2509-8.**
3. **STALLINGS, William. Cryptography and network security: principles and practice. Seventh edition. xix, 731 pages. ISBN 01-333-5469-5.**
4. **SWENSON, Christopher. Modern cryptanalysis: techniques for advanced code breaking. Indianapolis, IN: Wiley Pub., c2008, xxviii, 236 p. ISBN 04-701-3593-X.**
5. **STALLINGS, William a Lawrie BROWN. Computer security: principles and practice. Third edition. xix, 820 pages. ISBN 01-337-7392-2.**
6. **PAAR, Christof. Understanding cryptography: a textbook for students and practitioners. Heidelberg: Springer, c2010, xviii, 372 s. ISBN 978-3-642-04100-6.**

Vedoucí diplomové práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **12. ledna 2015**

Termín odevzdání diplomové práce: **15. května 2015**

Ve Zlíně dne 6. února 2015

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně .....

podpis diplomanta

ABSTRAKT

Ochrana citlivých elektronických dat a na druhé straně nutnost získávat informace z právě těchto zašifrovaných dat jako stěžejní kriminalistický důkaz při vyšetřování závažných zločinů. Tato dvě palčivá témata jsou hlavními body této práce. Jsou zde uvedeny důležité informace pro maximalizaci ochrany počítače. V práci je dále vysvětlena nenahraditelnost vytvoření bitové kopie paměti RAM při zajišťování digitálních stop a její následná forenzní analýza.

Klíčová slova: počítačová bezpečnost, ochrana elektronických dat, forenzní analýza počítačů, analýza dat, analýza paměti RAM, šifrování, šifrovací klíče, soudní znalec, šifrovací programy, dešifrovací software, FPGA.

ABSTRACT

Increased protection of sensitive electronic data and the need to obtain information from the same encrypted data as the key forensic evidence in the investigation of serious crimes. These two burning issues are the main points of this work. It contains important information for maximizing the protection of your computer. The paper also explain irreplaceability of imaged RAM in providing digital tracks and its subsequent forensic analysis.

Keywords: computer security, the protection of electronic data, computer forensic analysis, data analysis, analysis of RAM, encryption, encryption keys, forensic expert, encryption programs, decryption software, FPGA.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Proč svá data šifrovat?

Jeden z hlavních důvodů, proč šifrovat svá důležitá elektronická data je, odcizení či ztráta počítače (notebooku). Dalším důvodem může být možnost zabezpečit data při přenosu na jiné médium nebo při přenosu po síti internet. A neméně důležitým důvodem může také být ochrana dat před nežádoucím přístupem neautorizovaných osob (obchodní konkurent, šéf, manželka, policie…).

Šifrování je proces převodu nezabezpečených elektronických dat na data šifrovaná neboli zabezpečená, tzn. data čitelná pouze pro uživatele se znalostí dešifrovacího klíče (hesla).

Pokud se jedná o dnešní možnosti šifrování, tak se nacházíme v době, kdy je šifrování technologicky prozkoušené, a dalo by se říci, relativně bezpečné. Dnes využívané šifry jsou vysoce odolné proti standardním možnostem matematického prolomení, nebo proti útokům tzv. hrubou silou. Avšak stejně jako u většiny zabezpečení, je i u šifrování největší slabina lidský prvek. Jedná se nejčastěji o problém velice slabého hesla (krátké heslo, žádné speciální znaky, heslo nalezitelné pomocí tzv. "slovníkového útoku", stejné heslo použité v jiném programu…), a pak také o problém nezabezpečeného počítače jako celku, ke kterému může mít útočník, jak fyzický přístup (automatické zamykání PC v nečinnosti, zablokována možnost přístupu pomocí DMA…), tak i vzdálený přístup (neaktuální operační systém, žádný nebo slabý firewall …).

Teoreticky lze prolomit (dostat se k informacím ze zašifrovaných dat) téměř každé šifrování za pomoci metod jako jsou útok na operační paměť (bitová kopie, podchlazení RAM, DMA), obnovení hesel u ostatních aplikací (použitá stejná hesla), útok pomocí vysokého výpočetního výkonu (grafické karty, FPGA …) a další. Ale prakticky to není tak jednoduché a rozhodně né vždy jsou tyto „útoky" realizovatelné.

Obecně platí, že náklady na dešifrování by měly být nižší, než předpokládaný výnos z dešifrovaných dat.

I. TEORETICKÁ ČÁST

1 MOŽNOSTI ŠIFROVÁNÍ ELEKTRONICKÝ DAT

Existují dvě hlavní možnosti šifrování dat na osobních počítačích:

- šifrování celého disku – FDE (full disk encryption)
- šifrování konkrétních dat – FES (file encryption)

Obě tyto možnosti mají samozřejmě své výhody, nevýhody a také svá specifika.

1.1 FDE – šifrování celého disku

Tato možnost je také v některých publikacích nazývána WDE (whole disk encryption). Jedná se o způsob šifrování, kdy jsou veškerá data na disku šifrována (včetně zaváděcího oddílu, MBR, systémových souborů…).

U tohoto typu šifrování se nemusí uživatel starat o to, jaká data mají být šifrována, a tak je tento způsob ochrany jednodušší na používání i pro méně zkušené uživatele tak pro uživatele, kteří nemají jasno, jaká přesně data mají být chráněna.

Nevýhodou je, že šifrování více zatěžuje počítač a tím navyšuje časy přístupů na disk a také je samozřejmě zpomalena jakákoli disková operace (spuštění programu…) bez ohledu na její prioritu. Tuto nevýhodu dokážou dnešní rychlé SSD disky částečně eliminovat. Další nevýhodou oproti ochraně konkrétních souborů je, že při přenosu jednotlivých dat na jiný disk nebo pomocí internetu nejsou tato data šifrována (chráněna).

Výhody FDE:

- Může využívat pro zabezpečení jak software, tak hardware.
- Každý bit na disku je šifrován.
- Možnosti využití TPM.

Nevýhody FDE:

- Navýšení časů přístupů na disk.
- Nechrání data při přenosu po síti.

1.2 FES – šifrování konkrétních dat

Nejdůležitější u této varianty zabezpečení je správně vymezit oblast dat, na které se má tato ochrana vztahovat. Je tudíž o něco složitější na používání pro méně zkušené uživatele. Výhodou je, že nezpomaluje diskové úlohy do té doby, než se uživatel rozhodne pracovat se šifrovanými daty. Jedná se o šifrování nejen jednotlivých souborů, ale také složek nebo částí disku.

Jedním takovým příkladem je šifrování souborů (složek) pomocí archivátorů. Takto vytvořený soubor, který může být vytvořen, jako samo-spustitelný a není pak závislý na konkrétním osobním počítači a jeho softwarovém vybavením.

Výhody FES:

- Nezpomaluje diskové operace do doby používání šifrovaných dat.
- Možnost vymezení oblasti šifrování.
- Ochrana dat po síti.

Nevýhody FES:

- Nejsou chráněna veškerá data na disku.
- Složitější pro koncové (méně zkoušené) uživatele.

2 DNEŠNÍ MOŽNOSTI ŠIFROVÁNÍ DAT

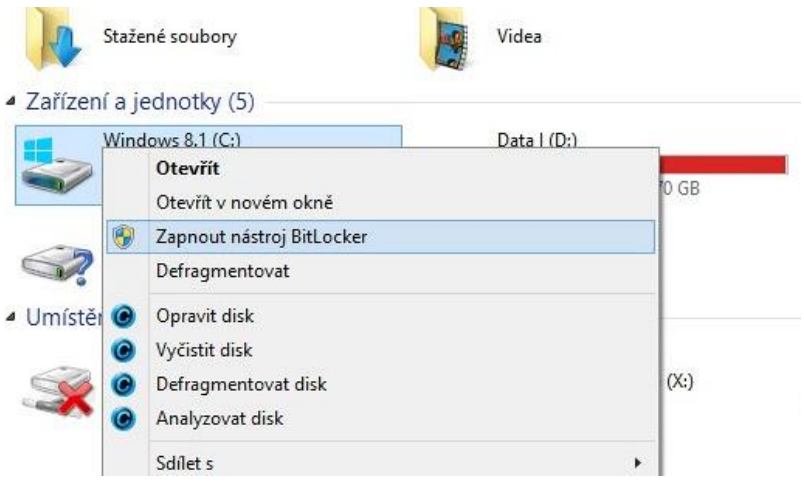
Na následujících řádcích budou popsány vlastnosti a možnosti nejpoužívanějších softwarů pro šifrování dat dnešní doby (pro operační systém Microsoft Windows). Budou zde popsány informace u softwarů využívající obě možnosti šifrování (FDE a FES).

2.1 BitLocker

Jedná se o šifrovací software vyvinutý firmou Microsoft, který je zdarma jako součást operačního systému Windows Vista a Windows 7 (verze Ultimate a Enterprise) a Windows 8 a Windows 8.1 (verze Pro a Enterprise) a serverové verze Windows Server 2008 a novější. Využívá možnosti šifrování FDE.

2.1.1 Obecné informace

Pro plnohodnotné využití tohoto softwaru je zapotřebí mít na disku nejméně dva diskové oddíly (aktuální verze vytváří tyto oddíly automaticky) a podporu TPM. Diskové oddíly vytvořené tímto softwarem mají souborový systém typu NTFS a jsou to: bootovací oddíl (který obsahuje soubory potřebné ke spuštění počítače, tento oddíl není zašifrován) a oddíl s operačním systémem (který obsahuje soubory systému Windows a ostatní uživatelská data). Oddíl s operačním systémem bude zašifrován a bootovací oddíl zůstane nezašifrovaný, aby bylo možné počítač spustit.[1]



Obrázek 1: Aktivování šifrovacího softwaru BitLocker.

[1] **Microsoft.** *Ochrana souborů nástrojem BitLocker Drive Encryption.* [Online] http://windows.microsoft.com/cs-cz/windows/protect-files-bitlocker-drive-encryption#1TC=windows-7.

Detekci toho, jestli náš počítač a systém, splňuje veškeré požadavky pro úspěšné nasazení tohoto typu šifrování, provádí software automaticky.

Kód Bitlockeru je zavřený, což znamená, že není možné modifikovat ani prohlížet jeho zdrojový kód. To představuje určitý problém, protože nelze ověřit, jestli nejsou přidány do softwaru tzv. zadní vrátka.

Pokud zašifrujete jednotku operačního systému, nástroj BitLocker během spouštění počítače zkontroluje, zda není ohroženo jeho zabezpečení (například kvůli změně systému BIOS nebo změně spouštěcích souborů). Pokud se zjistí možné riziko narušení zabezpečení, nástroj BitLocker zamkne jednotku operačního systému a bude k jejímu odemknutí požadovat speciální obnovovací klíč nástroje BitLocker. Tento obnovovací klíč je nutné vytvořit při prvním zapnutí nástroje BitLocker. V opačném případě byste mohli trvale ztratit přístup k souborům. Pokud počítač obsahuje čip TPM (Trusted Platform Module), nástroj BitLocker jej použije k zapečetění klíčů, které se používají k odemknutí zašifrované jednotky operačního systému. Po spuštění počítače nástroj BitLocker vyžádá od čipu TPM klíče k jednotce a odemkne ji.[2]

2.1.2 Přídavné možnosti zabezpečení

Pokud máme počítač, který podporuje TPM verze 1.2 nebo vyšší umožňuje BitLocker využít tento čip k lepšímu zabezpečení. Je zde možnost uzamčení bootovacího procesu, dokud uživatel nezadá tzv. osobní identifikační kód (PIN) nebo nevloží USB zařízení (flashdisk), který obsahuje spouštěcí klíč. Také lze tyto možnosti ověření zkombinovat:

- pouze PIN
- pouze TPM
- TPM + PIN
- TPM + PIN + USB klíč
- TPM + USB klíč
- USB klíč

Tato přídavná bezpečnostní opatření také zajišťují, že se počítač nepustí z režimu spánku nebo z režimu hibernace dokud nedojde k ověření uživatele.

---

[2] **Microsoft.** *Ochrana souborů nástrojem BitLocker Drive Encryption.* [Online] http://windows.microsoft.com/cs-cz/windows/protect-files-bitlocker-drive-encryption#1TC=windows-7.

2.1.3 Klíče a hesla

TPM vlastníkovo heslo (TPM owner password**)**

Před používáním TPM spolu s BitLockerem je zapotřebí inicializovat TPM čip. Inicializační proces vygeneruje tzv. heslo vlastníka čipu TPM. Pokud následně chceme TPM povolit nebo zakázat, musíme zadat toto heslo.

Obnovovací heslo a obnovovací klíč (Recovery password and recovery key)

Při nastavování šifrování pomocí programu BitLocker musíme vytvořit obnovovací heslo. A pak, jestliže se počítač dostane do obnovovacího stavu, bude potřeba právě toto heslo (obnovovací heslo nebo obnovovací klíč), pro odemčení zašifrovaných dat na disku. Obnovovací heslo může být uloženo v jednom z následujících formátů:

- Jako numerické heslo obsahující 48 číslic rozdělené do 8 skupin.
- Jako obnovovací klíč uložený v podobě souboru na USB úložišti.

PIN

Pro zvýšení levelu bezpečnosti můžeme nastavit PIN pro využití TPM. Tento PIN si může zvolit uživatel (musí obsahovat 4 až 20 číslic). Tento PIN se musí zadávat při každém zapnutí počítače nebo při obnovení z režimu hibernace.

Startovací klíč (Startup key)

Jedná se o další možnost zvýšení bezpečnosti. Startovací klíč je uložen na USB paměťovém médiu a musí být vložen do počítače pokaždé, když dochází ke spouštění daného operačního systému.

2.1.4 Metody šifrování

Data jsou šifrována pomocí klíče, který šifruje celý diskový oddíl. Většinou se jedná o tzv. diskový hlavní klíč (volume master key). Následující tabulka popisuje, jak může být tento hlavní klíč využit pro šifrování v program BitLocker.

Tabulka 1: Využití hlavního šifrovacího klíče v programu BitLocker.

Šifrovací metoda	Popis
TPM klíč + startovací klíč	RSA šifrování kombinované se startovacím klíčem hlavní klíč je šifrován jako 128 nebo 256

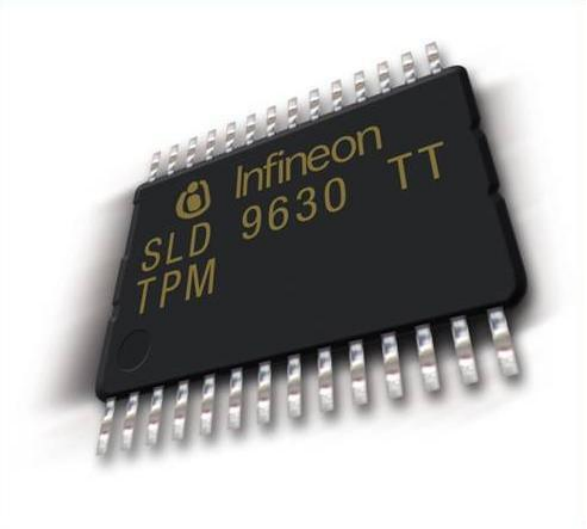
	bitový AES klíč
TPM klíč + PIN	šifrování hlavního klíče pomocí RSA
Pouze TPM klíč	šifrování hlavního klíče pomocí RSA
Pouze startovací klíč	šifrování hlavního klíče pomocí AES
Pouze obnovovací klíč	šifrování hlavního klíče pomocí AES
Obnovovací heslo + sůl (salt)	odvozený klíč je vytvořen za pomocí algoritmu náročného na matematický výpočet šifrování hlavního klíče pomocí AES
Čistý klíč	šifrování hlavního klíče pomocí AES, klíč AES je uložen nezašifrovaně a nezabezpečeně, když je BitLocker vypnut

Standardně BitLocker využívá šifru AES v CBC módu s defaultně nastavenou délkou klíče 128 bitů, ale tato délka lze nastavit na 256 bitů.

2.1.5 Doporučené nastavení

Nejvíce bezpečné nastavení programu BitLocker, a tak nejhůře prolomitelné pro útočníka, je využití počítače s možností využití technologie TPM verze 1.2 spolu se startovacím klíčem. Tento startovací klíč, jak již bylo napsáno výše, obsahuje soubor, kde je uložen klíč, který musí být načten při startování počítače (jedná se o standardní zapnutí počítače, tak i probuzení ze stavu hibernace nebo z režimu spánku). [1]

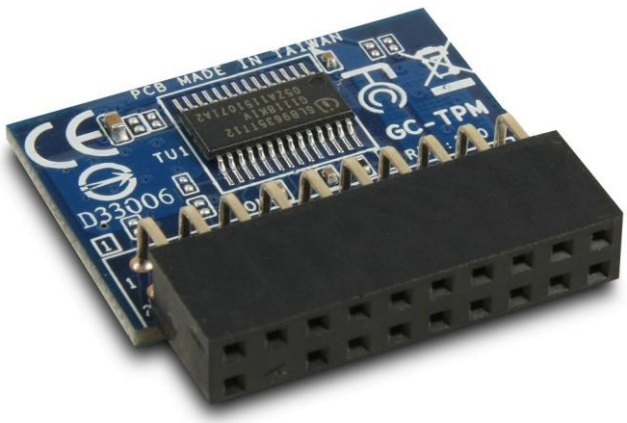
2.1.6 TPM - Trusted platform module



Obrázek 2: TPM čip.

Jedná se o mezinárodní standard (ISO/IEC 11889), který popisuje zabezpečený kryptoprocesor, který slouží k ukládání šifrovacích klíčů. Implementací specifikace je většinou myšlen TPM čip. Aktuální verze TPM specifikace je 2.0, která byla publikována 13. března 2014. Předchozí verze 1.2 byla zveřejněna 3. března 2011 a je stále využívána u stávajících počítačů (od této verze lze plnohodnotně využít všech vlastností například s šifrovacím programem BitLocker). Dále tento čip slouží k detekci hardwaru, softwaru a firmwaru našeho počítače. Pokud TPM detekuje nesoulad v uložených hodnotách, tak nedojde ke zpřístupnění dat uložených na disku.

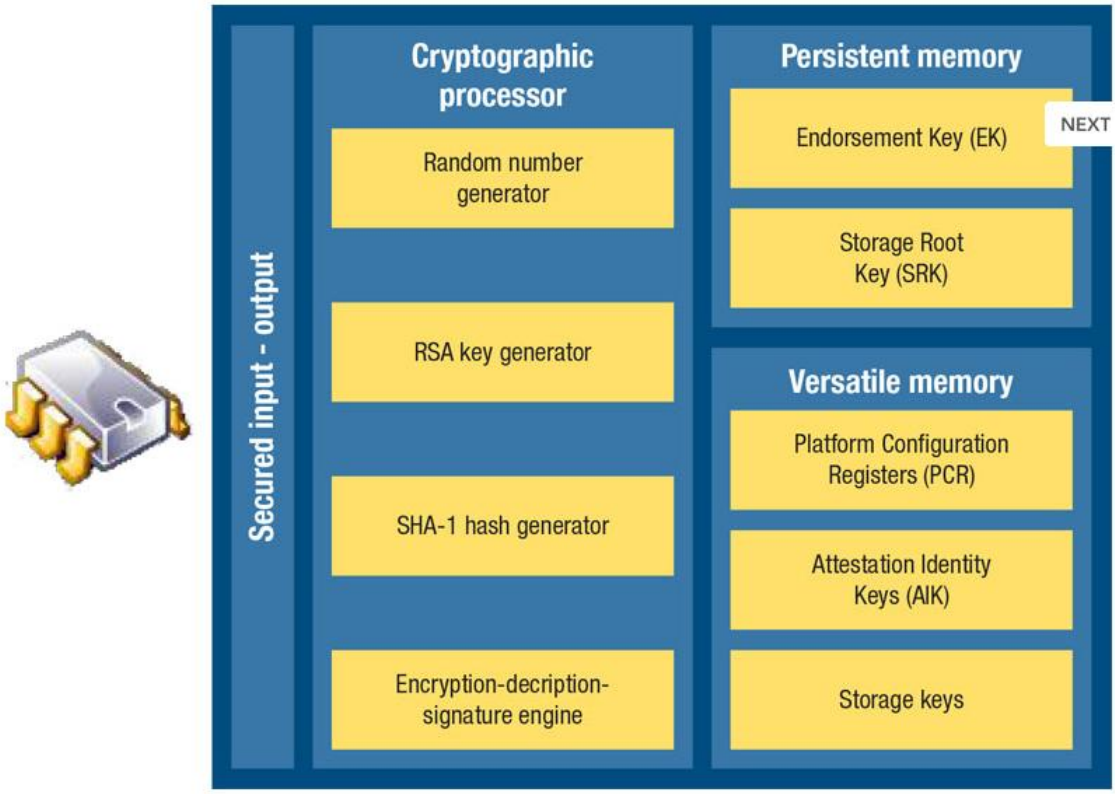
Tento čip obsahují dnešní moderní základní desky počítačů. Pokud tento čip neobsahuje základní deska, tak je možné koupit a instalovat externí TPM čip (Obrázek 3).



Obrázek 3: externí TPM čip.

Tento čip také umožňuje bezpečné generování kryptografických klíčů za pomoci například generátoru náhodných čísel. A dále tento čip má možnosti jako jsou vzdálené ověření nebo zapečetěné uložení:

- Vzdálené ověření (Remote attestation) – tato funkce vytváří velice těžce padělatelný klíč - hash , který obsahuje souhrn informací o hardwarové a softwarové konfiguraci daného počítače. Program využívaný na šifrování dat určuje rozsah těchto informací, a to poté umožňuje „třetí“ straně ověřit neměnnost těchto informací.
- Vázání (binding) – dochází k šifrováním dat za pomocí TPM potvrzovacího klíče, což je unikátní RSA klíč, který je pří výrobě přímo vypálen do čipu.
- Zapečetění (sealing) – jedná se o podobný způsob zabezpečení jako „vázání“, ale oproti vázání určuje stav, ve kterém musí být TPM v pořádku, aby mohla být data dešifrována (rozpečetěna).



Obrázek 4: TPM komponenty. [2]

2.2 TrueCrypt

Jedná se o bezplatný program s otevřeným zdrojovým kódem pro šifrování dat. Ochrannou známku TrueCrypt má od roku 2007 registrovanou David Tesařík, který ji poté převedl na asociaci TrueCrypt Developers Association se sídlem v americké Nevadě. Tuto asociaci, stejně jako vývojářská firma TrueCrypt Foundation, vede podle oficiálních záznamů Ondřej Tesařík.

Tento šifrovací program býval ještě před nedávnem nejpoužívanějším softwarem svého typu. Ale v květnu 2014 se na stránkách programu objevilo upozornění (Obrázek 5), že program již není bezpečný a byl doporučen přechod na software BitLocker od firmy Microsoft.


WARNING: Using TrueCrypt is not secure as it may contain unfixed security issues

This page exists only to help migrate existing data encrypted by TrueCrypt.

The development of TrueCrypt was ended in 5/2014 after Microsoft terminated support of Windows XP. Windows 8/7/Vista and later offer integrated support for encrypted disks and virtual disk images. Such integrated support is also available on other platforms (click here for more information). You should migrate any data encrypted by TrueCrypt to encrypted disks or virtual disk images supported on your platform.

Migrating from TrueCrypt to BitLocker:

Obrázek 5: Stránky projektu TrueCrypt a její záhadný obsah.

Tento náhlý konec tohoto projektu je opředen mnohými spekulacemi a zejména doporučení přechodu na konkurenční software a zejména BitLocker, u kterého není jasné, jestli neobsahuje zadní vrátka pro nějakou vládní agenturu (zde se nejvíce spekuluje o americké NSA nebo FBI) je více než podivný. Svět počítačů a šifrování již zažil nátlak ze strany americké agentury FBI o přidání zadních vrátek do komerčního softwaru a tudíž i u tohoto projektu je možné, že v tomto případě tvůrci odmítli, než aby zradili uživatele a svobodnou myšlenku, se kterou byl projekt zakládán. Pokud byl na ně uvalen příkaz mlčenlivosti (gag order) ve formě NSL (National Security Letter), vysvětluje to divné mlčení a nesmyslnou argumentaci na nově vytvořené stránce.

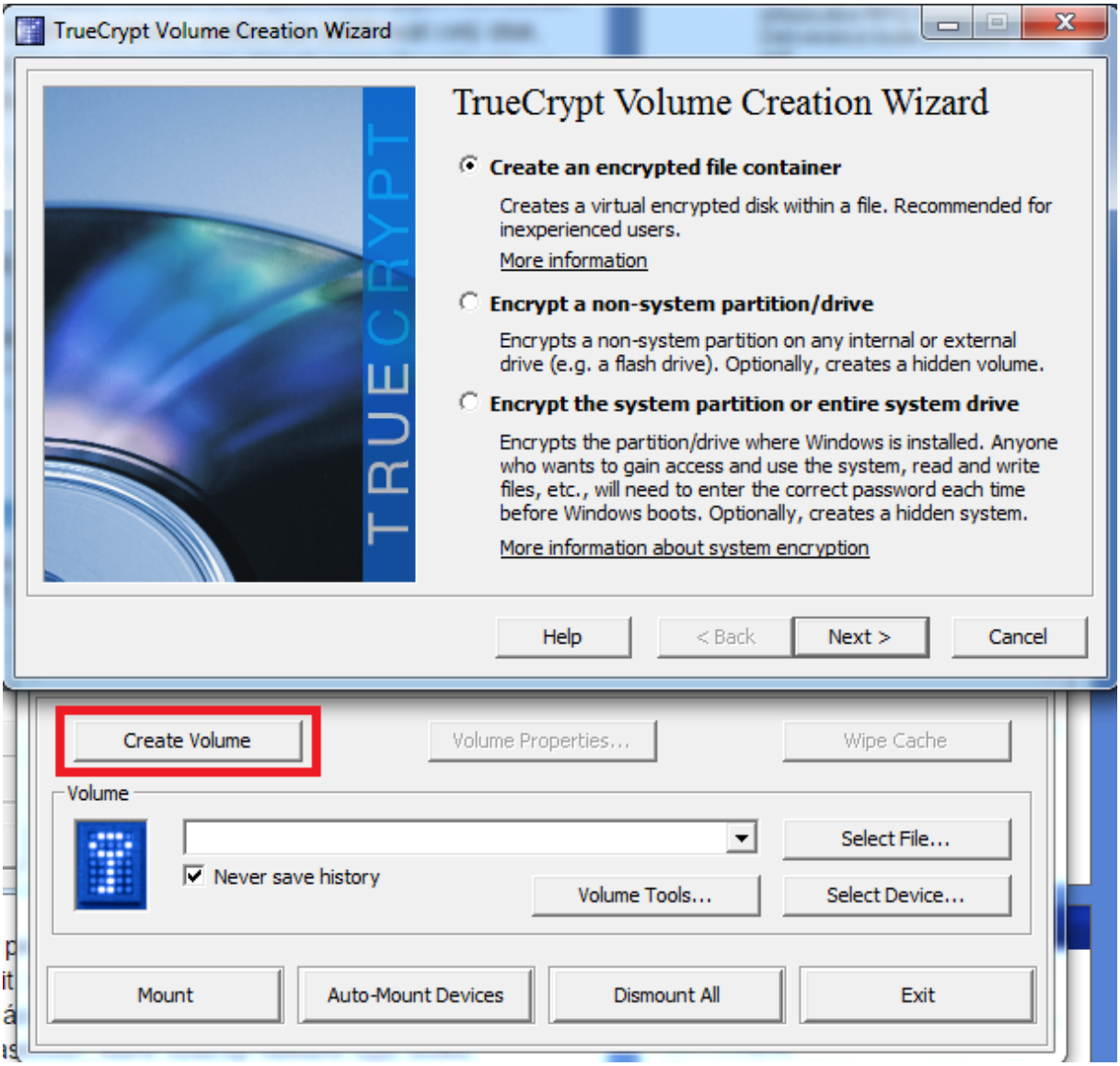
Poslední plnohodnotná aktualizace byla vypuštěna v únoru 2012 (verze 7.1a). Spolu s koncem projektu byla vypuštěna „nová“ verze tohoto programu (7.2), která ovšem již dokáže již jen dešifrovat dříve vytvořené zašifrovaná data a nepodporuje vytváření nových zabezpečených dat.

2.2.1 Obecné informace

Jedná se o multiplatformní FDE software využívající technologii OTFE. Tento program umožňuje různé možnosti zabezpečení elektronických dat. Například vytvoření virtuálních disků v podobě souboru, který lze načíst a následně s ním pracovat jako s kterýmkoliv jiným diskovým oddílem. Dále je zde možnost zašifrovat celý disk. Od verze 5.0 lze také šifrovat bootovací oddíl (jen u operačního systému Microsoft Windows)a mnohé další možnosti. [3]

2.2.2 Možnosti šifrování

1. virtuální disková jednotka v podobě souboru
    - velikost souboru si uživatel zvolí při vytváření jednotky
    - v souborovém systému lze vytvořit jednotku s pohyblivou kapacitou
2. šifrovaný diskový oddíl
    - možnost zašifrovat celý diskový oddíl
    - možnost výběru šifrovacího a hashovacího algoritmu
3. šifrovaný systémový oddíl
    - při spouštění počítače je uživatel dotázán na heslo, a až po úspěšném zadání je spuštěn operační systém
4. cestovní mód
    - vhodné k zabezpečení přenosného média (flashdisk)
    - TrueCrypt nastaví přenosné medium tak, aby po připojení do libovolného počítače požadovalo heslo a následně bylo po zadání správných údajů dešifrováno (není nutná instalace softwaru na cílovém počítači)
5. skrytý oddíl
    - pokročilá ochrana pro případ nutnosti z nějakého důvodu prozradit heslo k šifrovanému oddílu (fyzický nátlak)
    - uložen uvnitř běžného šifrovaného oddílu, ale má vlastní heslo
    - systémový oddíl lze také vytvořit jako skrytý



Obrázek 6: Vytvoření šifrovací jednotky v programu TrueCrypt verze 7.1.

2.2.3 Šifrovací algoritmy

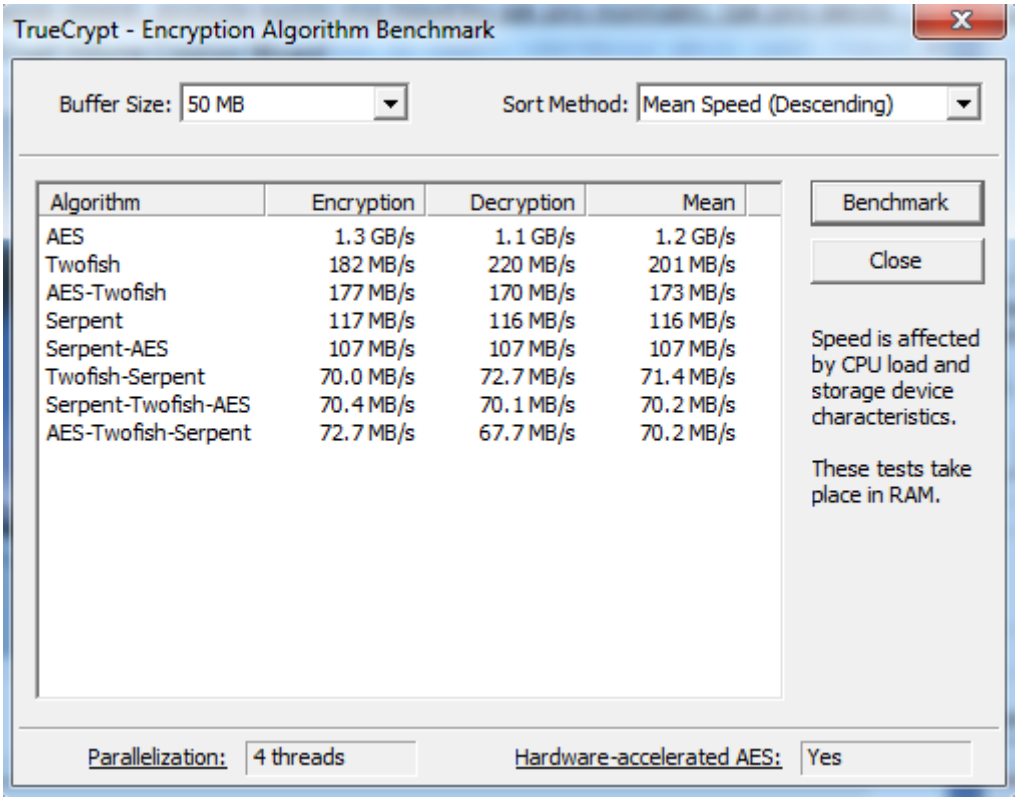
V tomto softwaru je na výběr z více šifrovacích algoritmů. V poslední plně funkční verzi 7.1a lze vybírat pro šifrování virtuálních disků mezi těmito algoritmy:

- AES, Twofish, Serpent
- Kombinace: AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES a Twofish-Serpent
- Od verze 4.3 již nejsou ve výběru algoritmi Blowfish, DES, Triple DES, CAST-128. Diskové oddíly vytvořené těmito algoritmy lze nadále dešifrovat a pracovat s nimi.

Uživatel může dále vybírat ze tří hashovacích algoritmů:

- RIPEMD-160, SHA-512 a Whirlpool

Obrázek 7: Možnosti algoritmů v softwaru TrueCrypt.

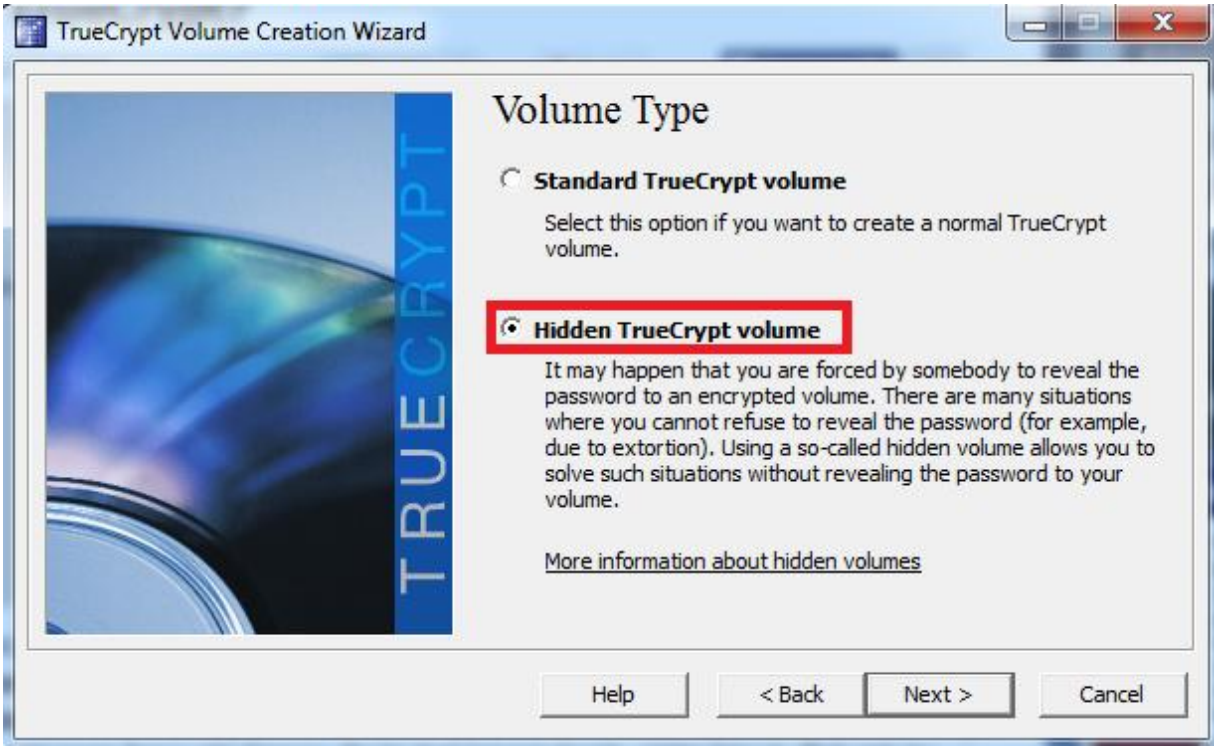


Obrázek 8: Výsledky rychlostí pro šifrování/dešifrování různých algoritmů (pomocí 4x CPU i5-2430M).

2.2.4 Způsob vytváření šifrovaných dat

Zašifrované virtuální disky vytvořené do souboru lze bez omezení přenášet. V průběhu vytváření oddílu je celý prostor zaplněn náhodně vygenerovanými daty, což velice ztěžuje situaci případné analýzy na zjištění počtu zašifrovaných oddílů, a jestli se případně na disku nacházejí tzv. skryté oddíly. Tato skutečnost zaručuje, že zcela prázdný zašifrovaný oddíl je prakticky nerozeznatelný od libovolně zaplněného oddílu. A tento fakt tvoří jednu z důležitých výhod od ostatních softwarů tohoto druhu a vylučuje určité druhy útoků na takto zašifrovaná data.

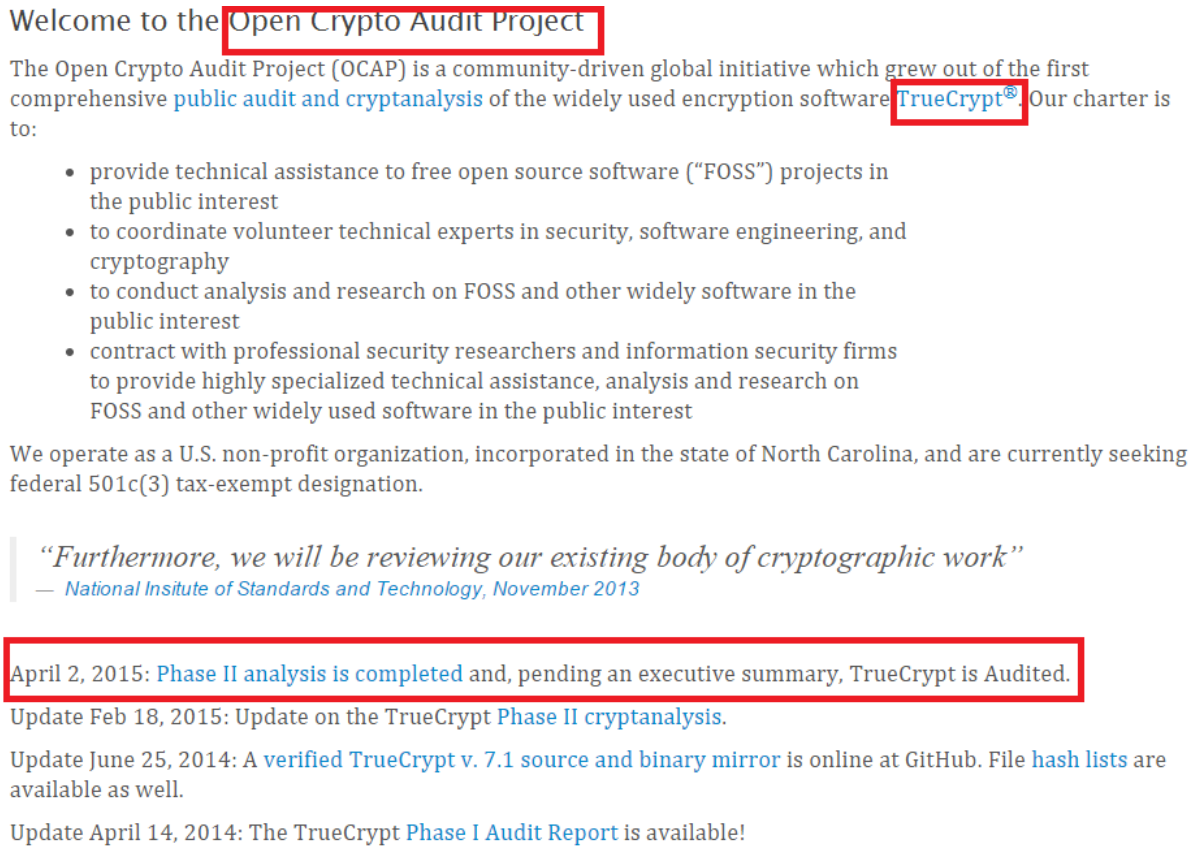
Dále má tento program velice unikátní vlastnost, a to že každý vytvořený zašifrovaný oddíl (kontejner) může, ale nemusí, obsahovat skrytý oddíl (jak již bylo zmíněno výše). Oba tyto oddíly vypadají stejně, protože oba mají v prvním sektoru (512 bytů) hlavičku, za kterou následují šifrované datové sektory. Ani TrueCrypt sám nepozná, o jaký oddíl se jedná. Pokud uživatel vloží heslo pro dešifrování, tak se program pokusí nejprve dešifrovat skrytý oddíl tímto heslem. Pokud je heslo nesprávné nebo skrytý oddíl nenajde, pak se teprve pokusí odemknout hlavní oddíl. Tato vlastnost jde využít při tzv. „věrohodné popiratelnosti“ (plausible deniability). To znamená, že při fyzickém nátlaku nebo při právním naléhání, vydáme vedlejší heslo, které odemkne vedlejší zašifrovaný oddíl, kde se nacházejí předem připravená nezájmová data (skrytý zašifrovaný oddíl zůstane neprozrazen). Co se týče právního naléhání, tak některé státy (Kanada, Velká Británie, Německo…) mají právně ukotveno, že heslo musíte vydat, pod pohrůžkou trestu. V České Republice, stejně tak jako v USA, je právo mlčet, pokud byste výpovědí způsobili nebezpečí trestního stíhání sobě nebo osobě blízké (v Americe to garantuje pátý dodatek ústavy, u nás článek 37 Listiny základních práv a svobod).



Obrázek 9: Možnost skrytého oddílu v programu TrueCrypt.

2.2.5 Používat dál nebo přejít ke konkurenci?

Toto je velice důležitá otázka, ale odpověď na ní se nehledá lehce. Ačkoliv někdo na stránky projektu umístil, jak již bylo výše napsáno, upozornění s možným nebezpečím při používání daného softwaru, tak právě skončená práce (2. 4. 2015) „Open Crypto Audit Project TrueCrypt“, která analyzovala zdrojové kódy a hledala slabé stránky tohoto programu, uvedla, že byly nalezeny slabiny v kódu a tento program využívá zastaralých překladačů kódu. Ale audit nenalezl „žádné náznaky backdoorů pro tajný přístup či úmyslně vytvořeného škodlivého kódu, nalezené problémy vypadají spíše jako neúmyslné chyby než jako úmyslně vytvořené slabiny". Prozatím jediným důvodem přechodu na jiný software může být neaktualizovatelnost tohoto projektu. Software nebude reagovat na požadavky uživatelů a na nové technologie pro prolamování hesla hrubou silou nebo na nové druhy útoku. Jednu takovou neaktualitu již můžeme vnímat nyní a to, že u operačního systému Microsoft Windows 8 s GPT tento program neumí zašifrovat systémový disk, ale nainstalovat a používat lze.



Welcome to the Open Crypto Audit Project

The Open Crypto Audit Project (OCAP) is a community-driven global initiative which grew out of the first comprehensive public audit and cryptanalysis of the widely used encryption software TrueCrypt®. Our charter is to:

- provide technical assistance to free open source software ("FOSS") projects in the public interest
- to coordinate volunteer technical experts in security, software engineering, and cryptography
- to conduct analysis and research on FOSS and other widely software in the public interest
- contract with professional security researchers and information security firms to provide highly specialized technical assistance, analysis and research on FOSS and other widely used software in the public interest

We operate as a U.S. non-profit organization, incorporated in the state of North Carolina, and are currently seeking federal 501c(3) tax-exempt designation.

> *"Furthermore, we will be reviewing our existing body of cryptographic work"*
> — *National Insitute of Standards and Technology, November 2013*

April 2, 2015: Phase II analysis is completed and, pending an executive summary, TrueCrypt is Audited.

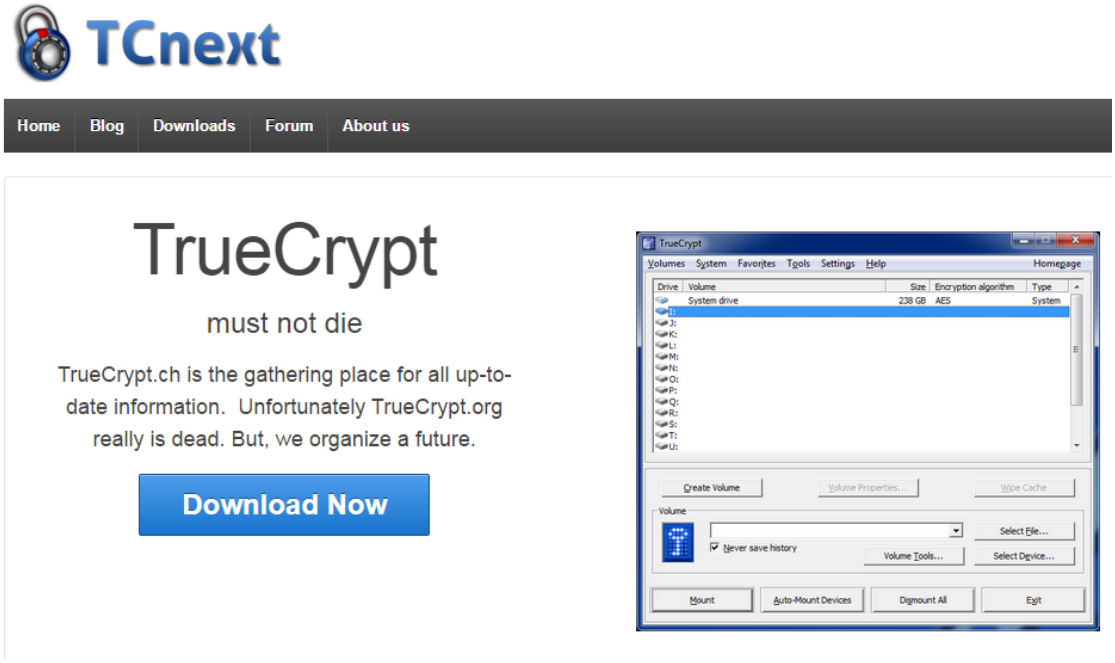
Update Feb 18, 2015: Update on the TrueCrypt Phase II cryptanalysis.

Update June 25, 2014: A verified TrueCrypt v. 7.1 source and binary mirror is online at GitHub. File hash lists are available as well.

Update April 14, 2014: The TrueCrypt Phase I Audit Report is available!

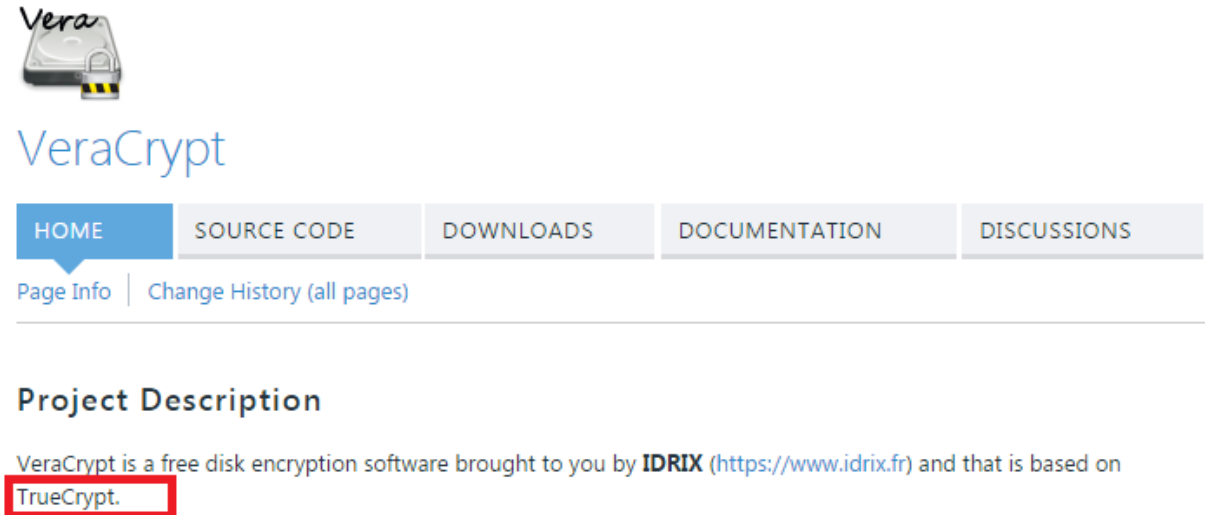
Obrázek 10: Dokončení auditu na software TrueCrypt.

S návazností na ukončení projektu TrueCrypt, jak byl znám před svým ukončením, vznikly i projekty, které více méně pokračují nebo navazují, tam kde tento projekt skončil. Například na stránkách „https://truecrypt.ch/" vznikl projekt s názvem „TCnext", který chce navázat a pokračovat ve vývoji ukončeného projektu. Na těchto stránkách také lze stáhnout starší plnohodnotnou verzi programu TrueCrypt (7.1a). Tento projekt chce navázat na to dobré, co bylo v ukončeném projektu a vyvarovat se chyb, které měl. Jeho oficiální lokace se změnila ze státu Nevada v USA na Švýcarsko, a tudíž již nespadá pod jurisdikci USA. To by mělo zajistit „menší " vlivy zahraničních agentur. Dále tento projekt chce více spolupracovat na vývoji s uživatelskou komunitou a nechce zůstat v anonymitě, nýbrž jmenovitě uvádí vývojářský tým.



Obrázek 11: Nový projekt TCNext využívající zdrojové kódy projektu TrueCrypt.

Z dalších příkladů softwarů využívajících zdrojových kódů TrueCryptu může být uveden software „VeraCrypt“ („https://veracrypt.codeplex.com/“).

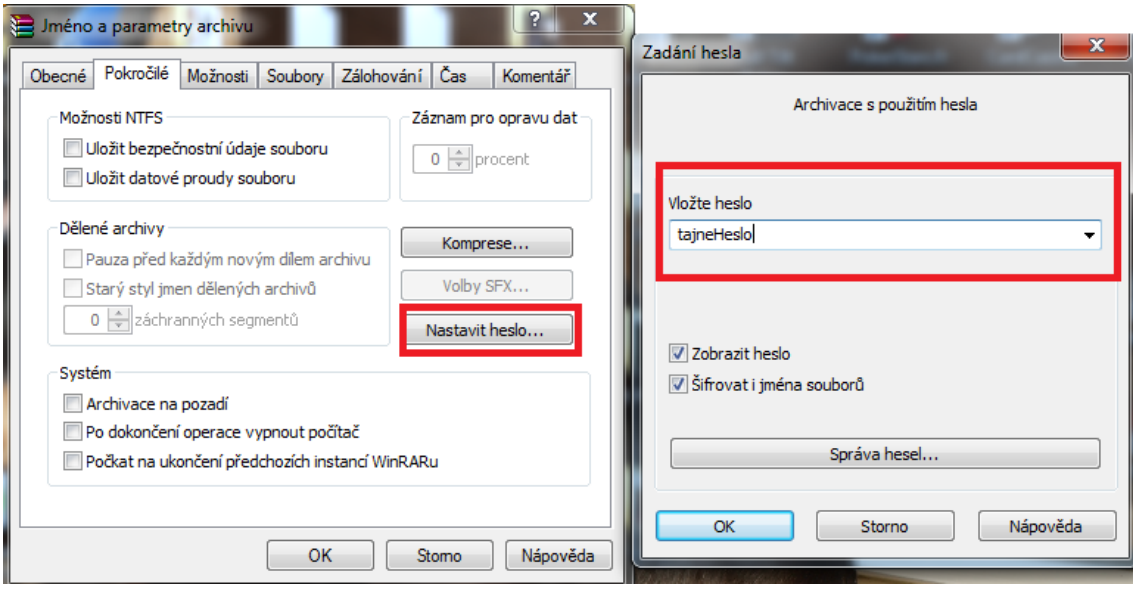


Obrázek 12: Další šifrovací software založený na projektu TrueCrypt.

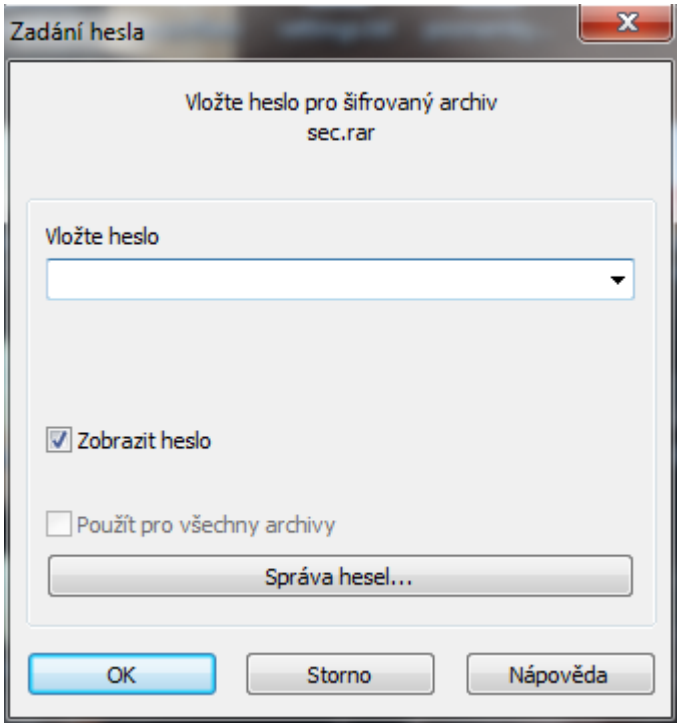
2.3 WinRAR

Jedná se o typického zástupce programu, který kromě svých hlavních vlastností (archivace dat), umožňuje šifrování dat za využití vlastností FES.

Tento program umožňuje při komprimaci data také šifrovat. Od verze programu řady 5 je využívané šifrování AES zvýšeno ze 128 bitů na 256 bitů s hash algoritmem BLAKE2 (místo původního CRC32 32 bitů) využívající CBC mód. Funkce derivačního klíče je založena na PBKDF2 používající HMAC-SHA256.



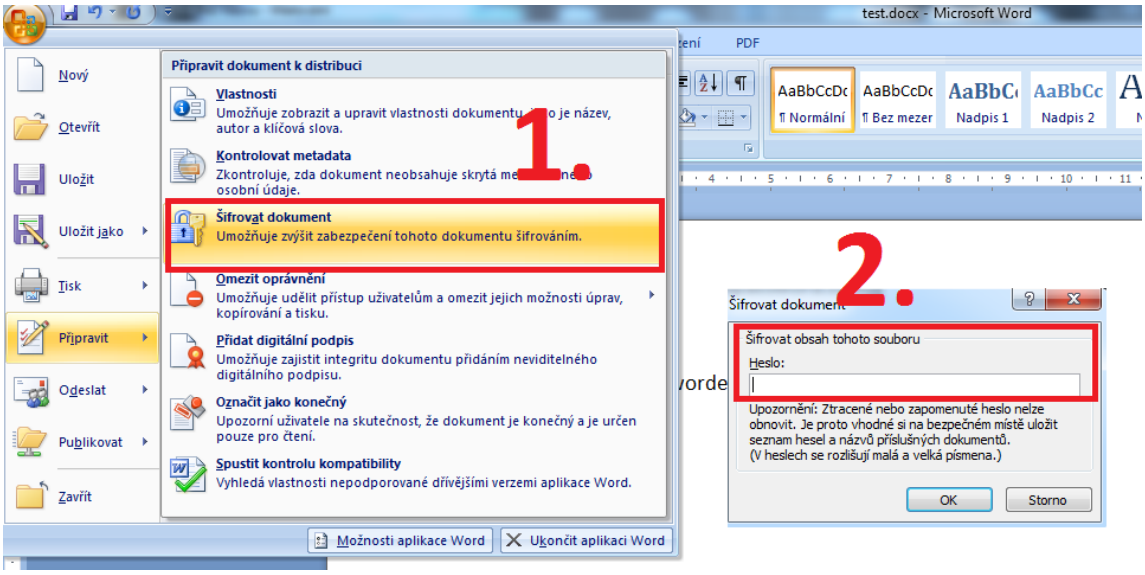
Obrázek 13: Zabezpečení jednotlivého souboru pomocí hesla v programu WinRAR.



Obrázek 14: Otevření zaheslovaného souboru za pomoci WinRAR.

2.4 Microsoft Office

Tento dobře známý kancelářský balík umožňuje vytvořené dokumenty chránit heslem. Microsoft Word a Excel 95 používaly pro zabezpečení 16 a 32 bitový algoritmus, poté následoval u balíku Office 97 a 2000 40 bitový a s verzí Office 2007 se přešlo na zabezpečení pomocí AES 128 bitového algoritmu.

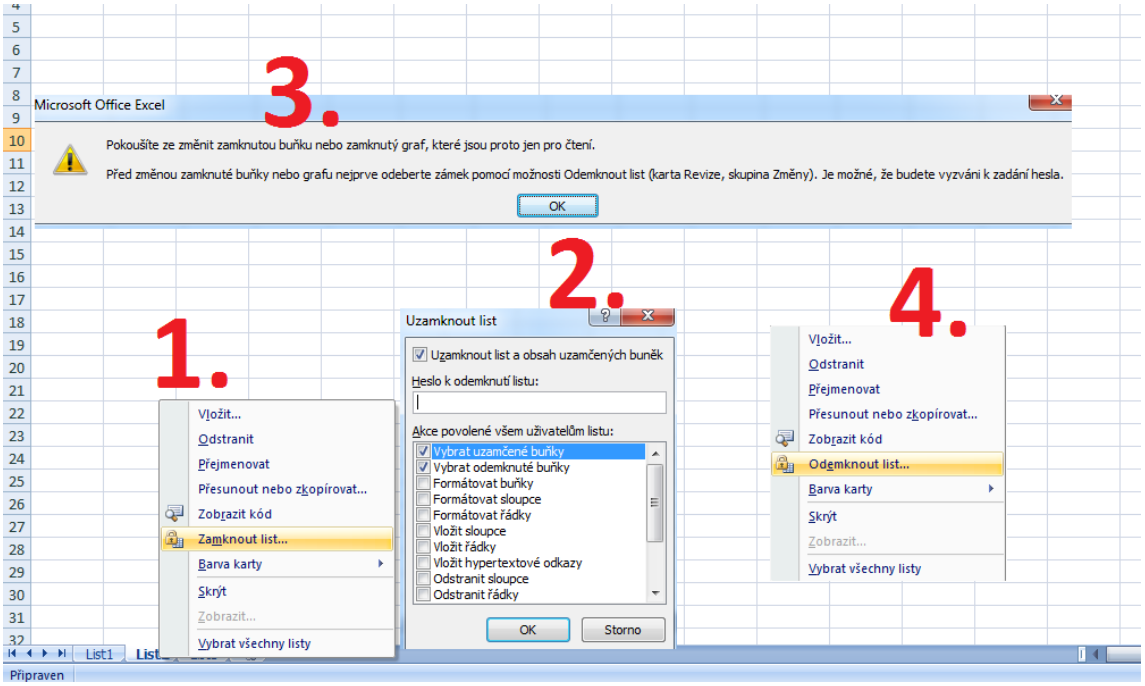


Obrázek 15: Zašifrování dokumentu v programu Microsoft Word 2007.

Jednotlivé programy balíku Microsoft Office nabízejí dvě hlavní možnosti šifrování dokumentů, a to šifrování celého dokumentu nebo jeho jednotlivých částí:

- Microsoft Word - šifrování celého dokumentu
- Microsoft Excel – šifrování celého dokumentu, jednotlivého listu, individuálního elementu v daném listu
- Microsoft PowerPoint – šifrování celého dokumentu

Ovšem tento druh šifrování, vzhledem k použitým slabým algoritmům, je vhodný spíše pro omezení funkcí dokumentu mezi spolupracovníky, než pro „ukrytí“ důvěrných informací. Tyto druhy šifer, které jsou využívány v balíku Microsoft Office do verze 2007, jsou prolomitelné mnohými forenzními (dešifrovacími) softwary během pár sekund. Z tohoto důvodu je doporučováno spolu s tímto druhem zabezpečení ještě uložit celý dokument do zašifrovaného kontejneru (software TrueCrypt) nebo na soubor použít další druh zabezpečení (například využití PGP).



Obrázek 16: Zamčení a odemčení jednotlivých „listů“ v programu Microsoft Excel 2007.

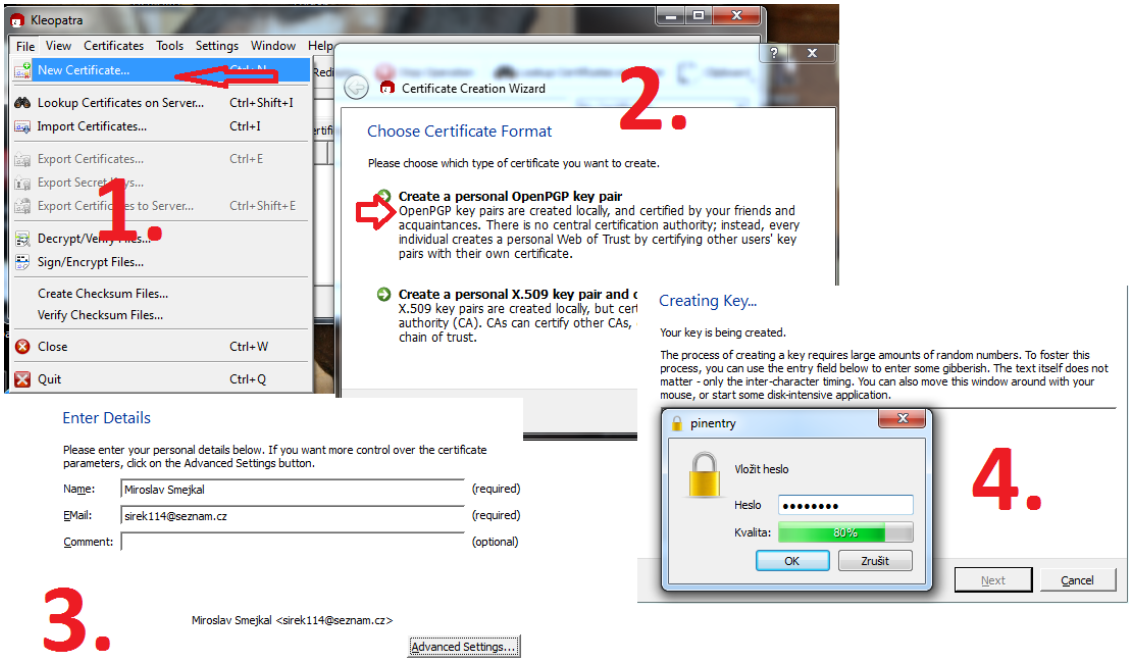
2.5 Standard OpenPGP

Jedná se o počítačový kód, který je využíván v mnoha počítačových programech a zabezpečeních pro šifrování. PGP je velice často využíváno pro podepisování, šifrování a dešifrování textů, e-mailů, souborů, složek nebo celých disků. Je založen na algoritmu RSA využívajícím asymetrické šifrování. První verze byla vyvíjena a následně uvolněna Philem Zimmermannem v roce 1991.

PGP bylo tak hojně využíváno, že došlo k jeho standardizaci, aby byla umožněna jednodušší spolupráce mezi jednotlivými verzemi PGP a podobnými softwary. Byl přijat jako internetový standard pod názvem „**OpenPGP**“. Nyní se jedná o otevřený standard používaný softwary, jako jsou právě PGP a další (GnuPG, GPG, Hushmail, Veridis a jiné).

2.5.1 Gpg4Win

Gpg4win podporuje, jak šifrovací standard OpenPGP, tak S/MIME (X.509). Dále se jedná o oficiální distributora GnuPG pro operační systémy Microsoft Windows. Tento software je zdarma, jak pro nekomerční, tak pro komerční účely. [4]

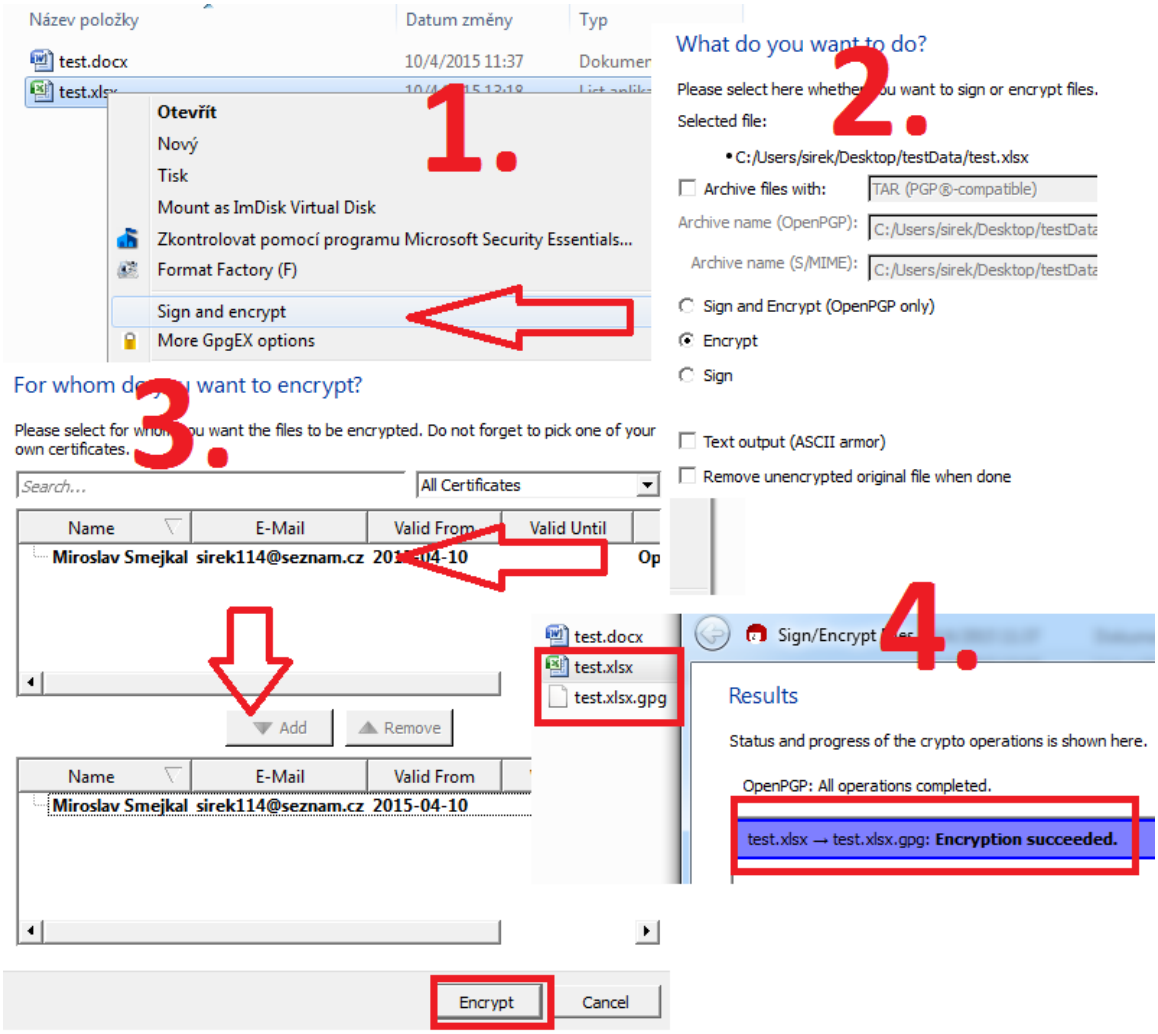


Obrázek 17: Vytvoření soukromého certifikátu v aplikaci Kleopatra (program Gpg4win).

Tento software je doporučován státní agenturou pro počítačovou a komunikační bezpečnost (Federal Office for Information Security), což samozřejmě nezaručuje, že daný software nemá zadní vrátka.

Komponenty programu Gpg4win (verze 2.2.4 - 17. 3. 2015):

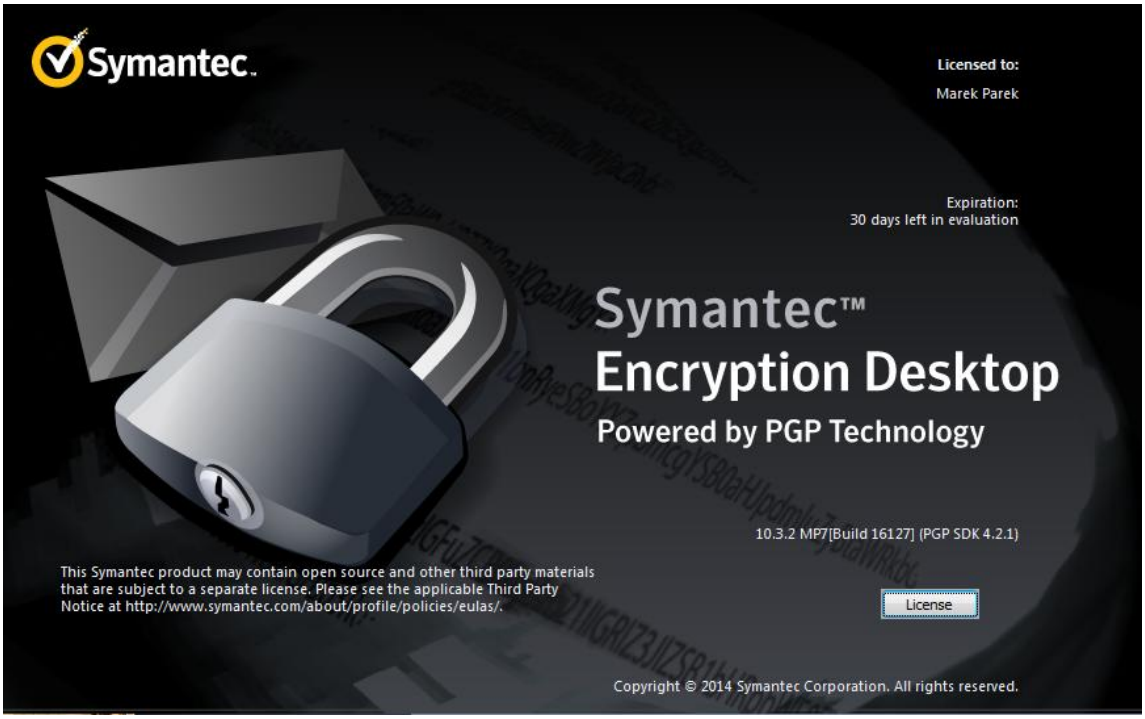
- GnuPG – jádro, šifrovací nástroj
- Kleopatra – manažer certifikátů
- GPA – alternativní manažer certifikátů
- GpgOL – doplněk pro Microsoft Outlook – šifrování e-mailů
- GpgEX – doplněk pro prohlížeč souborů v operačním systému Microsoft Windows – šifrování souborů
- Claws Mail – kompletní e-mailová aplikace s podporou šifrování
- Gpg4win Compendium – dokumentace – v angličtině a němčině



Obrázek 18: Zašifrování souboru soukromým klíčem pomocí programu Gpg4win.

2.5.2 Symantec Encryption Desktop (PGP)

Jedná se o balík šifrovacích softwarů, který je založen na standardu PGP a podporuje jak FDE tak FES. Díky využití PGP je použita velice silná šifra postavená na technologii hybridního kryptografického optimizéru (HCO).



Obrázek 19: Softwarový balík šifrovacích nástrojů – Symantece Encryption Desktop 10.3.2.

2.5.2.1 Obecné informace

Tento balík se skládá ze 4 hlavních kategorií pro šifrování:

- **Endpoint Encryption**
- **File and Folder Encryption**
- Email Encryption
- Secure Scoket Layer (SSL) Encryption [3]

Pro nás jsou nejzajímavější, z pohledu ochrany dat na koncovém počítači, první dvě kategorie.

2.5.2.2 Endpoint Encryption

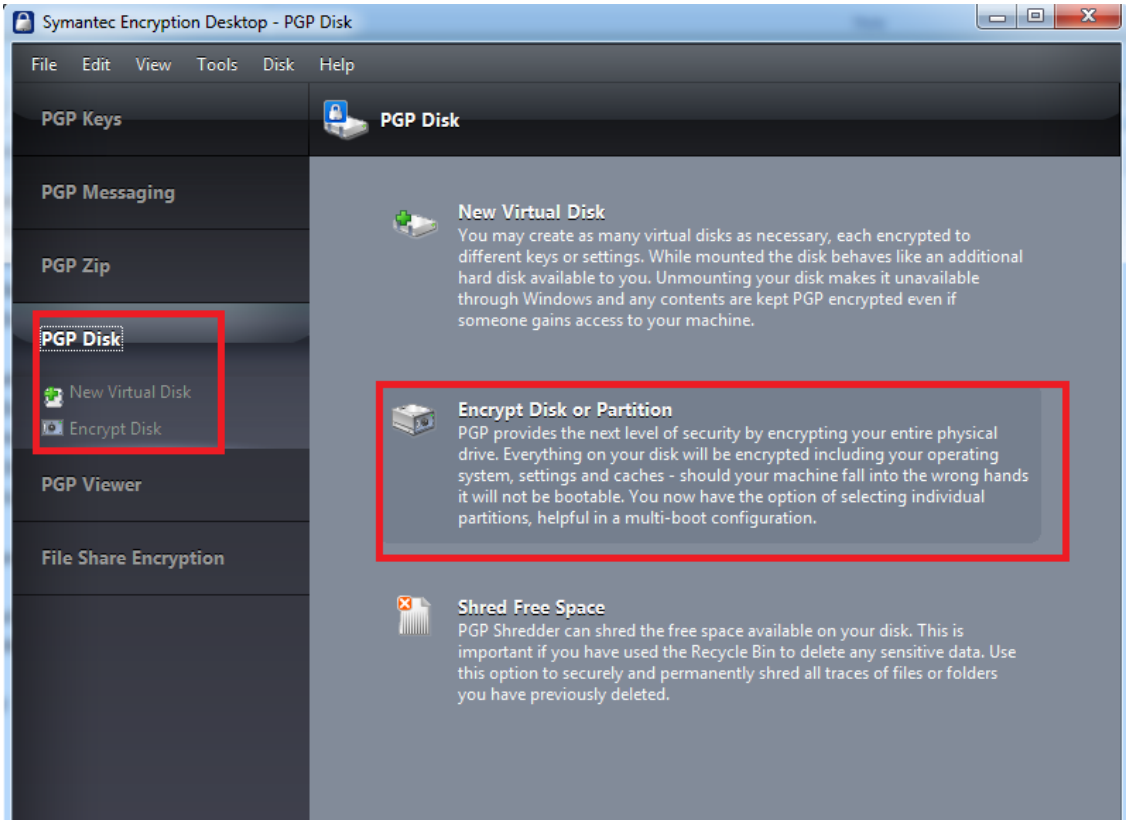
Jedná se o šifrování koncového zařízení a je možné ho dále rozdělit:

- **Drive Encryption** – šifrování celého disku

[3] **Symantec.** Keeping Your Private Data Secure. *www.symantec.com.* [Online] http://securityresponse.symantec.com/content/en/us/enterprise/white_papers/b-keeping-your-private-data-secure_WP_21349382.pdf.

- **Removable media encryption** – šifrování odpojitelných zařízení
- Mobile encryption – šifrování mobilních telefonů

Šifrování celého disku (u softwaru Symantec pojmenováno jako "whole disk encryption"), jak již bylo napsáno výše, je nejběžnější způsob toho, jak chránit data pomocí šifrování. Jedná se o šifrování celého disku, včetně operačního systému, aplikací, ovladačů a samozřejmě uživatelských dat. Použitím tohoto druhu šifrování docílíme toho, že veškerá data budou nečitelná a nepoužitelná pro neautorizované uživatele (ztracení, odcizení, přístup neautorizované osoby).



Obrázek 20: Šifrování disku (nebo oddílu) pomocí programu Symantec Encryption Desktop.

Obrázek 21: Výzva pro vložení hesla při startu počítače – zašifrovány celý diskový oddíl pomocí programu Symantec Encryption Desktop.

Šifrováním odpojitelných zařízení se myslí šifrování dat nacházejících se na zařízeních, jako jsou flashdisky, externí disky, optická média a další přenosná zařízení. Toto řešení automaticky šifruje data uložená na předem nastavených odpojitelných zařízeních.

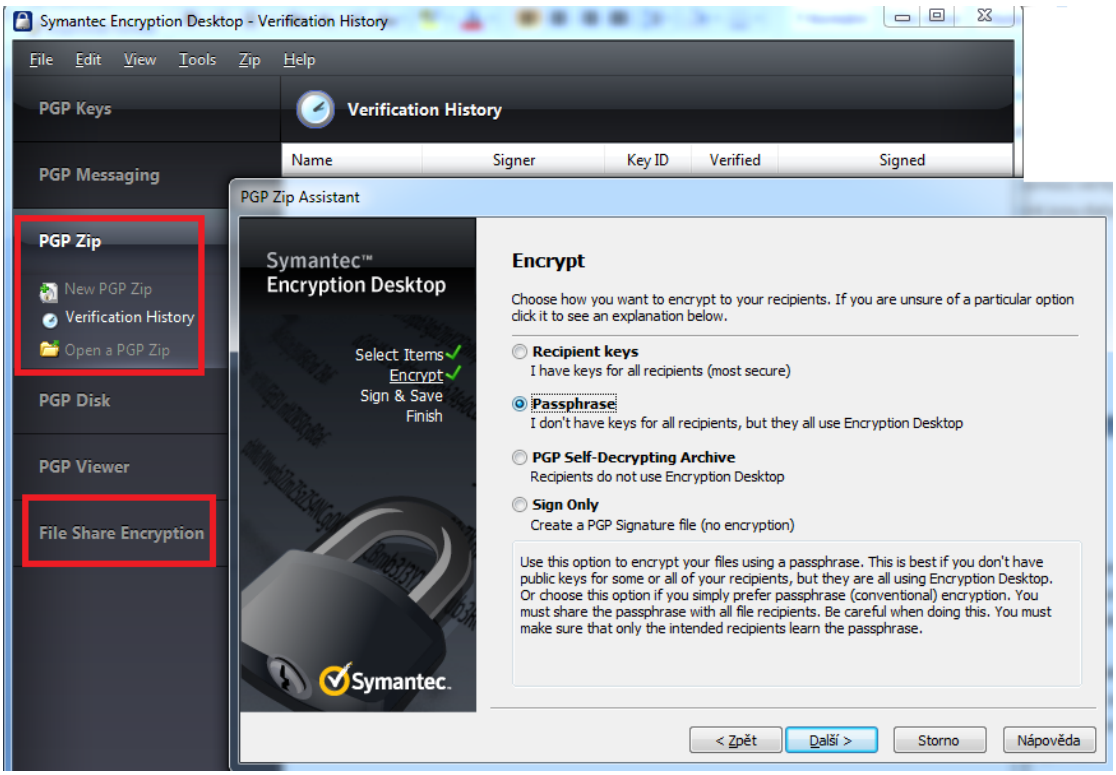
2.5.2.3 File and Folder Encryption

Jedná se o šifrování specifikovaných dat na stolních počítačích, noteboocích, dat sdílených po síti nebo dat uložených na cloudových úložištích. Jakmile je složka nebo soubor kopírován, archivován nebo sdílen s ostatními uživateli, tak si samozřejmě svoje šifrování nese sebou, a tak k informacím uložených v těchto datech mají přístup opět jenom autorizované osoby.

Je zde více možností, jak koukat na to, jaké soubory či složky šifrovat. Asi nejpoužívanější (nejvíce se blíží šifrování celého disku) možnost je šifrovat veškeré soubory a složky, až na pár vybraných dat (například systémové soubory). Druhá možnost je samozřejmě vybrat jen konkrétní soubory či složky a vše v nich šifrovat. Další možnost může být šifrovat pouze data vytvořená konkrétním programem.

Tento šifrovací balík obsahuje dvě funkce jak šifrovat jednotlivá data. Jedná se o funkce:

- **PGP Zip** – tato funkce umožňuje šifrování jednotlivých souborů nebo složek a jsou zde 4 druhy možností zabezpečení daných dat za pomocí různých přístupů:
    1. Recipient keys – dojde k zašifrování dat pomocí veřejných klíčů všech příjemců, takže musíme mít klíče všech uživatelů, pro které jsou data určena – jedná se o nejvíce bezpečnou možnost.
    2. Passphrase – tuto možnost využijeme, pokud nemáme k dispozici veřejné klíče všech příjemců nebo pokud chceme k následnému otevření souboru použít heslo – je nutné toto heslo sdílet se všemi příjemci a dále je nutné, aby všichni příjemci měli nainstalovaný Symantec Encryption Desktop.
    3. PGP Self-Decrypting Archive – jedná se o variantu zabezpečení, kdy některý z příjemců nepoužívá tento šifrovací balík – dojde k zašifrování vybraných dat do samospustitelného souboru, který pří svém spuštění vyžaduje heslo pro dešifrování dat – opět je nutné sdílet heslo se všemi příjemci.
    4. Sign Only – tato možnost nešifruje vybrané soubory, ale pouze vytváří archiv, který obsahuje PGP podpis – když příjemce dostane tento archiv, tak za pomoci tohoto nástroje zkontroluje, jestli daný soubor nebyl pozměněn, a kdo byl jeho autorem.
- **File Share Encryption** – tato funkce umožňuje šifrování jednotlivých souborů nebo složek a lze v této funkci nastavit přístup jednotlivým uživatelům, měnit role těchto uživatelů, vytvářet skupiny uživatelů a další. [5]



Obrázek 22: Šifrování jednotlivých dat za pomocí funkcí balíku Symantec Encryption Desktop.

2.5.2.4 Systémové požadavky

Podpora Symantec Encryption Desktop pro operační systém Microsoft Windows je:

- Windows 8 Enterprise a Pro (32 i 64 bitová verze)
- Windows 7 (všechny 32 i 64 bitové verze)
- Windows Vista (všechny 32 I 64 bitové edice)
- Windows XP (32 bitové Service Pack 2 nebo 3, 64 bitové Service Pack 2)
- Windows Server 2003 (Service Pack 1 a 2)
- Windows Server 2008 Service Pack 1 a 2 (64 bitová verze)
- Windows Server 2008 R2 (64 bitová verze)

2.5.2.5 Cena

Tento šifrovací balík je zpoplatněn. Zde jsou uvedené ceny z oficiálních stránek společnosti Symantec (ke dni 11. 4. 2015):

- Endpoint Encryption – 1 licence na 1 rok – 55 EUR
- File Share Encryption - 1 licence na 1 rok – 144 EUR

Je možné si všechny produkty tohoto balíku zdarma vyzkoušet v tzv. trial verzi na 30 dnů.

3 DODATEČNÉ INFORMACE PRO NÁSLEDNOU ANALÝZU

3.1 Standardní útoky používané pro hledání hesel

Brute Force – útok hrubou silou

Jedná se o velice jednoduchý způsob hledání hesla, program vyzkouší všechny možné kombinace. Toto hledání je limitováno uživatelským nastavením hledání: délka hesla (počet symbolů), možnosti symbolů (malá nebo velká písmena, číslice, speciální znaky a jejich kombinace).

Mask Scans – mask útok

Jedná se o druh útoku, kde známe alespoň nějaký zpřesňující parametr hesla (délku hesla, použitý specifický znak, použití pouze malých písmen), a tak můžeme využít tento druh útoku. Protože jakákoliv informace týkající se hesla je velice užitečná a hlavně snižuje čas potřebný k nalezení hesla.

Například víme, že naše heslo má 8 znaků a první znak je Z a poslední 4 znaky jsou číslice 2007, pak můžeme nastavit v našem softwaru vyhledávání za pomocí Mask útoku takto: „Z???2007“.

Dictionary Attacks – útok pomocí slovníků

Jedná se o typ útoku, kdy program zkouší hesla z připraveného seznamu (slovníku). Tento typ útoku je samozřejmě řádově rychlejší než útok například hrubou silou (malé množství zkoušených hesel). Jedná se o slovníky, které obsahují například: křestní jména, slovníky jazykových mutací, zvířata, fotbalové týmy, nejpoužívanější hesla. Tento typ útoku je velice účinný hlavně na hesla vytvořená méně zkušenými uživateli, kteří nedodržují základy bezpečnosti nastavení hesla.

Rainbow Attacks – útok pomocí Rainbow tabulek

Tento útok je založen na principu předpřipravených tabulek. Tyto tabulky je nutné si vytvořit nebo stáhnout ze sítě internet a použít již vytvořené (pro každý algoritmus je nutné vytvořit svojí tabulku). Poté speciální program načte tyto tabulky a díky rychlosti operační paměti, kde jsou tato data uložena je hledání hesel 1000x rychlejší než klasickém hledání hesel. Například vytvoření tabulek pro NTLM hashe o délce hesla 8 znaků při použití alfa-

numerických znaků potrvá několik dnů (v závislosti na výkonu konkrétního PC), ale jejich následné použití a najití hesla o této délce bude trvat řádově desítky sekund.[4]

3.2 FPGA

Tato zkratka znamená „Field Programmable Gate Array“, česky programovatelná hradlová pole. Jedná se o speciální číslicové integrované obvody, které obsahují programovatelné bloky propojené konfigurovatelnou maticí spojů. Právě díky své programovatelnosti nacházejí tyto obvody širokou škálu uplatnění a jeden z nich je právě využití pro kryptoanalýzu. Jejich historie sahá do 70 let minulého století, ale až poslední roky, díky snižující se ceně a snižující se spotřebě dochází k jejímu masivnějšímu použití.

Obrázek 23: Využití technologie FPGA pro kryptoanalýzu – komerční produkt od společnosti SciEngines. [6]

[4] **ElcomSoft.** The easy way to restore access passwords to files, applications and databases. *https://www.elcomsoft.com.* [Online] https://www.elcomsoft.com/WP/easy_way_to_restore_access_passwords_to_files_applications_and_databases_en.pdf.

Menší problém nastává při konkrétním využití pro vyhledávání hesel, protože žádný z výše zmíněných programů FPGA nepodporuje. To znamená, že prodejce FPGA využitelných pro kryptoanalýzu, musí prodávat tyto pole včetně se svým naprogramovaným speciálním softwarem a to celou sestavu prodražuje. Ale následný výsledek při vyhledávání hesel je velice dobrý – mělo by se jednat o zrychlení v porovnání s dnešními grafickými kartami o 10 až 100 násobky (viz. kapitola: „Porovnávání rychlostí získávání hesel za pomoci dešifrovacích softwarů – Využití FPGA“).

3.3 Forenzní metody pro získání fyzické paměti a dalších „živých“ dat

Vytvoření bitové kopie a následná analýza paměti RAM vyžaduje speciální forenzní software a hardware, protože většina běžných programů nemá přístup k paměti RAM (\\.\PhysicalMemory) a velice často je také zapotřebí přistupovat k datům pomocí tzv. kernel módu. K následné analýze obrazu paměti je také zapotřebí speciálních skriptů a znalostí.

Obrázek 24: Paměti RAM.

Vzhledem k tomu, že od operačního systému Windows Vista a v něm přidaného nástroje BitLocker pro šifrování celého disku a spousty dalších možností jak šifrovat svá data, se analýza paměti RAM stává čím dál více důležitá pro možnosti kryptoanalýzy. Dále z těchto prostředků lze získat informace, jako jsou IP adresy, běžící procesy, aktivní virusy, webové adresy, otevřené porty a mnohé další.

3.3.1 Vytvoření obrazu paměti RAM – Hardwarové nástroje

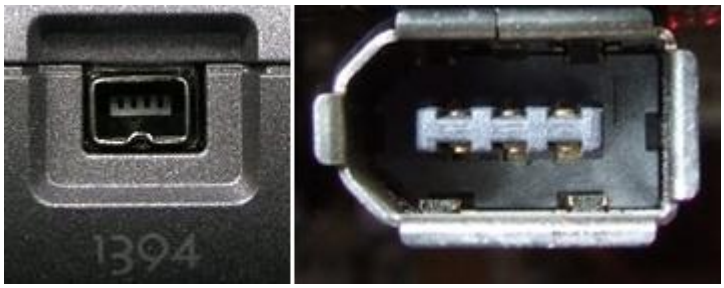
Hlavní myšlenkou hardwarových nástrojů je vytvoření obrazu paměti RAM bez nutnosti využívat procesy operačního systému nainstalovaného na zájmovém počítači

a tudíž nedojde k přepsání dat v paměti během přípravy a samotného vytváření obrazu. Hlavní nevýhodou tohoto druhu přístupu je, že využitý hardware musí být instalován před začátkem vytváření samotné bitové kopie.

V této části práce budou představeny známé hardwarové nástroje a jejich možnosti, výhody a nevýhody.

3.3.1.1 Využití sběrnice FireWire

Jedná se o metodu, která využívá sběrnici FireWire. Tato sběrnice má přímý přístup k fyzické paměti (tzv. DMA), jedná se o druh přístupu bez nutnosti využití procesoru. Tato metoda byla vyvinuta především kvůli velké rychlosti přenosu dat (například pro přenos videa) a také řeší problém některých softwarových nástrojů, které umějí využívat pouze tzv. „user mód“ pro přístup k paměti RAM. [7]



Obrázek 25: Rozhraní sběrnice FireWire1394.

Adam Boileau vyvinul software pomocí programovacího jazyka Python, který umožňuje extrakci paměti RAM využitím sběrnice FireWire pro operační systém Linux. Tento kód je využitelný stejně tak dobře pod operačním systémem Windows díky již zmíněném principu DMA a „namaskování“ výstupního na zařízení iPod a podobně. Tento kód je využitelný i pro získání paměti u systémů, které jsou zamčené.

Tento druh přístupu využívají i některé softwarové nástroje, jako například Inception nebo Passware FireWire Memory Imager (Obrázek 26).

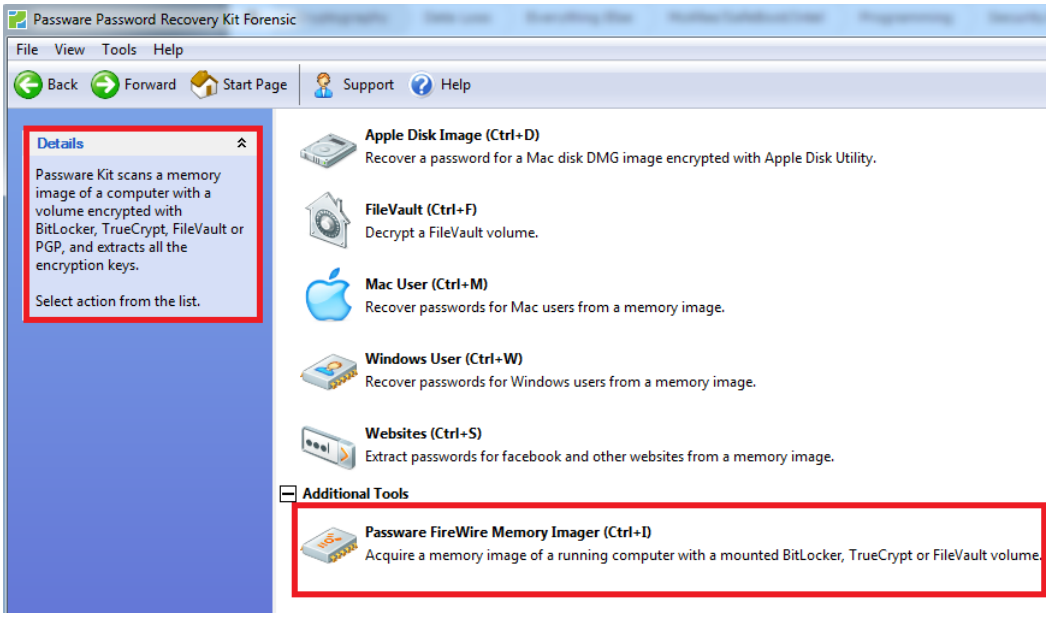
Inception

- Zdarma – licence GPL.
- Aktuální verze 0.4.0.
- Stabilní (bezproblémový) pro kapacitu paměti RAM 4GB a menší.

Passware FireWire Memory Imager

- Součástí Passware Kit Forensic 13.7.

- Placené – od 995$.
- Intuitivní GUI prostředí.
- Neomezené kapacitou paměti.



Obrázek 26: Možnost vytvoření flashdisku s metodou FireWire útoku.

Tento druh zálohy paměti má ovšem i své nedostatky, kterými jsou UMA, dále pak nutnost přítomnosti konektoru FireWire na cílovém počítači pro připojení k forenznímu počítači. U některých verzí operačního systému dochází právě kvůli UMA k pádům celého systému. A druhý problém – přítomnost FireWire portu - je čím dál větším problémem, protože u nových počítačů a notebooků se již ve standardu konektory FireWire většinou nenachází. Tento problém se nechá částečně vyřešit pomocí externích karet s tímto portem, které se nechají za chodu systému připojit do notebooku (jedná se o rozhraní ExpressCard, PCMCIA…).

Výhody:

- Možnost obejití uzamčeného prostředí systému.
- Žádná přepsaná data v zájmové paměti RAM.
- Levné pořizovací náklady.
- Možnost připojení externích karet s tímto rozhraním do notebooků.

Nevýhody:

- Rozhraní FireWire není standardem u moderních počítačů.
- Částečný problém s kapacitou paměti RAM větší než 4GB.

- Občasná vyvolání BSoD (modrá smrt).
- Problém s UMA.
- Možnost zakázání přístupu tohoto portu uživatelem zájmového počítače.

3.3.1.2 Zařízení Tribble

V roce 2004 pánové Carrier a Grand představili jejich rozšiřující kartu do slotu PCI (Obrázek 27 a 28). Tato karta umožňuje vytvoření obrazu paměti RAM bez využití procesů operačního systému. Hlavní výhoda byla, že nedojde k žádnému přepisu dat v paměti. Velký nedostatek této karty je, že před použitím musí být nainstalována v zájmovém počítači. V dnešní době se tato karta nedá v podstatě sehnat k testování a tak se nevyužívá.

Tento systém je chráněn patentem: U.S. Patent #7,181,56. [8]

Obrázek 27: Připojené zařízení Tribble.

Obrázek 28: Zařízení Tribble.

3.3.2 Vytvoření obrazu paměti RAM - Softwarové nástroje

Hlavní rozdíl mezi softwarovými a hardwarovými nástroji je, že u softwarových často dochází k zapsání části kódu do paměti (přepsání zájmových dat), díky kterému se získává přístup k paměti RAM. Jsou tu určité odlišnosti jednotlivých nástrojů během vytváření bitové kopie paměti, a to hlavně různé druhy formátů kopie, které mohou být podporovány jen určitými forenzními nástroji pro následnou analýzu.

Největší omezení pro softwarové řešení vytváření obrazu paměti RAM je aktualizace service pack 2 pro Windows XP (nebo Windows 2003 SP1). Od tohoto operačního systému s touto aktualizací nebo s novějším operačním systém dochází k tomu, že objekt „\\.\PhysicalMemory“ již není dále přístupný pro programy, které jsou spuštěny pomocí tzv. user módu. Pro úplnou zálohu paměti je nutná podpora „kernel“ módu.

Další problém, s kterým je zapotřebí počítat je, že v průběhu spouštění softwaru a následného vytváření paměti může docházet ke změnám v samotné paměti. Je to z toho důvodu, že spouštění programu v systému Windows dochází k alokování částí paměti pro jeho potřeby. Při tomto procesu dochází samozřejmě ke ztrátě části zájmových dat, která se dříve nacházela v paměti na této adrese.

3.3.2.1 DD – data dumper

Data dumper je linuxový program, jehož jedním z účelů je přístup k fyzické paměti přes cestu „Device/ physical memory/“ (nebo jiná dle typu distribuce). Tento program je obecným standardem pro vytváření bitových kopií (obrazů) jak pamětí, tak hlavně pevných disků a dalších datových nosičů. Obraz vytvořený tímto programem je obecně podporovaný většinou forenzních analytických nástrojů.

Pan Garner z firmy GMG systems vyvinul modifikovanou verzi programu DD spustitelného v operačním systému Windows. Tento jeho program je také součástí forenzního nástroje (Forensic Acquisition Utilities), který je zdarma ke stažení. Jedna z výhod tohoto programu je, že při spouštění přepisuje jen malé množství originálních dat uložených v paměti. Vytvořený obraz může být dále uložen na externí disk nebo může být poslán po síti. Tento program také podporuje možnosti komprese a vytvoření kontrolní sumy vytvořeného souboru. Ovšem tento program má i své nevýhody a to veliké a limitující. Tou hlavní nevýhodou je skutečnost, že program využívá pro své spuštění user mód, takže nemá přístup do celé paměti RAM v určitých operačních systémech, jak již bylo výše zmíněno. Reakcí na tento problém bylo vyvinutí programu KntDD,

který je součástí utility KnTTools od stejné firmy. Další informace o tomto programu níže.

3.3.2.2 KntDD

Jedná se o součást nástroje KnTTools, která se používá na zálohování a následnou analýzu paměti operačního systému Windows. Tento nástroj byl vyvinut panem Georgem Garnerem. Garner vyvinul tento nástroj jako reakci na omezení k přístupu na adrese „\\.\PhysicalMemory“ pomocí user módu a podporuje Windows 2000, Vista a vyšší.

Vlastnosti této utility:

- Placená – od 250$.
- Spustitelná z externího disku (flashdisku).
- Podporuje zálohu pomocí FireWire sběrnice.
- Záloha pomocí sítě.
- Konverze z obrazu paměti na soubor typu „Microsoft crash dump“ – možná analýza pomocí nástroje: „Microsoft debugging tools“.
- Možnost komprese.
- Vyhledávání kryptografických klíčů a kontrola jejich integrity.
- Možnost zálohy souboru pagefile.sys.
- Podpora 32 i 64 bitové verze.

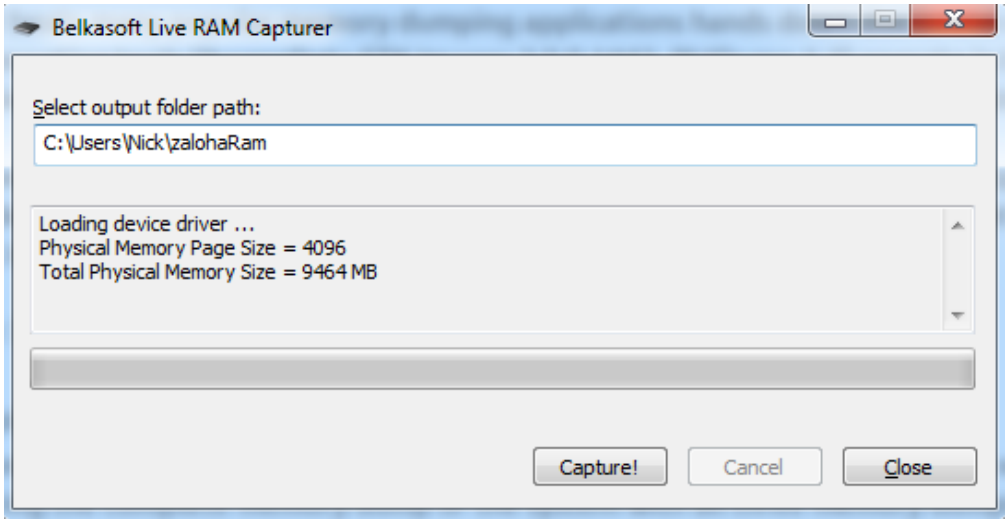
3.3.2.3 Belkasoft Live RAM Capturer

Jedná se o software od společnosti Belkasoft, který je poskytován bezplatně (nutná registrace). Tento program dokáže vytvořit zálohu celé paměti RAM a to i v případě, že cílový počítač má nastavenou ochranu právě proti vytváření zálohy paměti tzv. anti-debugging či anti-dumping systém.

Možnosti této utility:

- Spustitelná z externího disku (flashdisk).
- Podpora 32 i 64 bitové verze.
- Možnost zálohu analyzovat v programu Live RAM Analysis in Belkasoft Evidence Center (placená).
- Podpora všech verzí operačního systému Microsoft Windows včetně verze 7, 8, Server 2003 a Server 2008.

- Využívá tzv. kernel módu.



Obrázek 29: Program Belkasoft Live Ram Capturer.

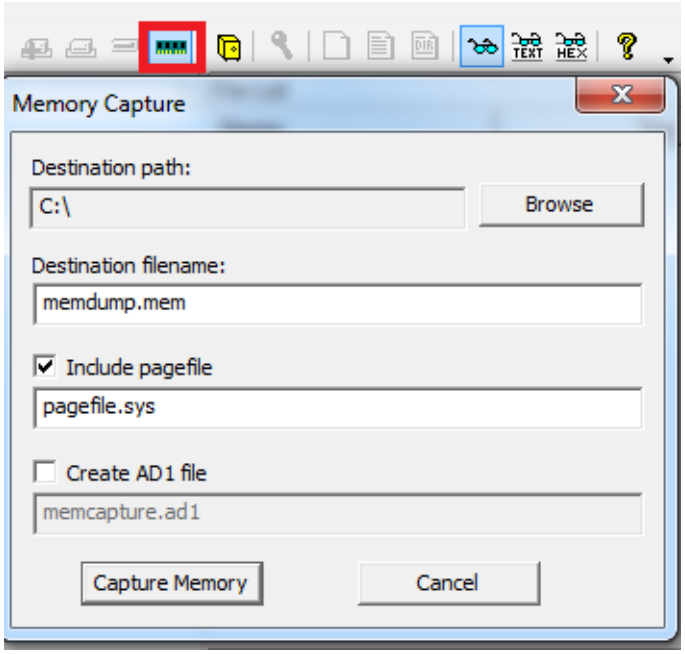
3.3.2.4 ManTech Memory DD

Tento program je k dostání zdarma pro nekomerční účely a pro státní orgány. Podle dokumentace k tomuto programu (rok 2008, verze 1.3) jsou podporovány operační systémy Microsoft Windows Server 2008, Windows Vista a starší systémy, a to jak v 32 bitové verzi tak 64 bitové. Tento program podporuje vytváření forenzního obrazu paměti RAM a jeho uložení v binární podobě a také možnost ověření tohoto obrazu pomocí hashovací funkce MD5. Tento program je například součástí programového balíčku s názvem Helix.

Bohužel má také své velké nevýhody. Tou hlavní je skutečnost, že se již od roku 2008 dále nevyvíjí a také to, že podporuje vytvoření obrazu pouze do kapacity paměti 4 GB.

3.3.2.5 FTK Imager – verze 3.2.0 2.

Jedná se o víceúčelový software vyvíjený firmou AccessData. Program podporuje vytváření obrazů disků, disket, optických nosičů a také paměti RAM včetně souboru Pagefile.sys. Dále tento program podporuje načtení obrazů těchto zařízení a to i v tzv. read-only módu, vytváření kontrolních souborů (MD5, SHA-1) a mnohé další. Tento software je zdarma ke stažení a je možné ho používat jako portálovou verzi (bez nutnosti instalace).



Obrázek 30: Vytváření obrazu RAM za pomoci programu FTK Imager.

3.3.3 Jiné možnosti zpřístupnění paměti RAM

3.3.3.1 Cold boot attack

Jedná se o typ útoku na získání obrazu paměti RAM, při kterém má útočník fyzický přístup k počítači a je možné získat data z paměti na spuštěném počítači po jeho restartování (tzv. cold boot – restartování počítače za pomocí tlačítka restart, místo pomocí operačního systému). Je totiž známo, že po restartování počítače, zůstanou data uložená v pamětích typu DRAM nebo SRAM po dobu několika sekund. Tato doba se díky zmražení (například použitím stlačeného vzduchu dnem vzhůru) pamětí může zvětšit až na desítky minut.

Tento typ útoku byl představen vědci z Princtnovy univerzity, kteří ukázali postup obnovení šifrovacích klíčů z paměti po tzv. cold boot restartu.

Po tomto druhu restartu musíme mít připravený externí disk (nebo flashdisk) s předinstalovaným softwarem, který spustí okamžitě zálohu paměti RAM do souboru. Pro funkčnost tohoto postupu musí mít zájmový počítač povolené bootování z USB zařízení. Další možností je, že po zmrazení dojde k fyzickému vyndání paměti RAM a zandání do připraveného forenzního počítač se správnou paticí na příslušnou paměť a zde dojde k záloze dat z této paměti.

Obrázek 31: Cold boot útok. [9]

Je zapotřebí udělat otisk paměti takovým způsobem (softwarem), aby došlo co k nejmenšímu přepisu dat na zájmové paměti.

Poznámka: Vzhledem k tomu, že se nejedná o úplně jednoduchý postup a může dojít k poničení hardwaru, tak je tato možnost zamýšlena, až jako poslední šance pro získání dat z paměti RAM. Tato možnost by měla být využívána, pokud nemáme aktivní přístup do operačního systému (systém je uzamčený) a zájmový počítač neobsahuje FireWire rozhraní.

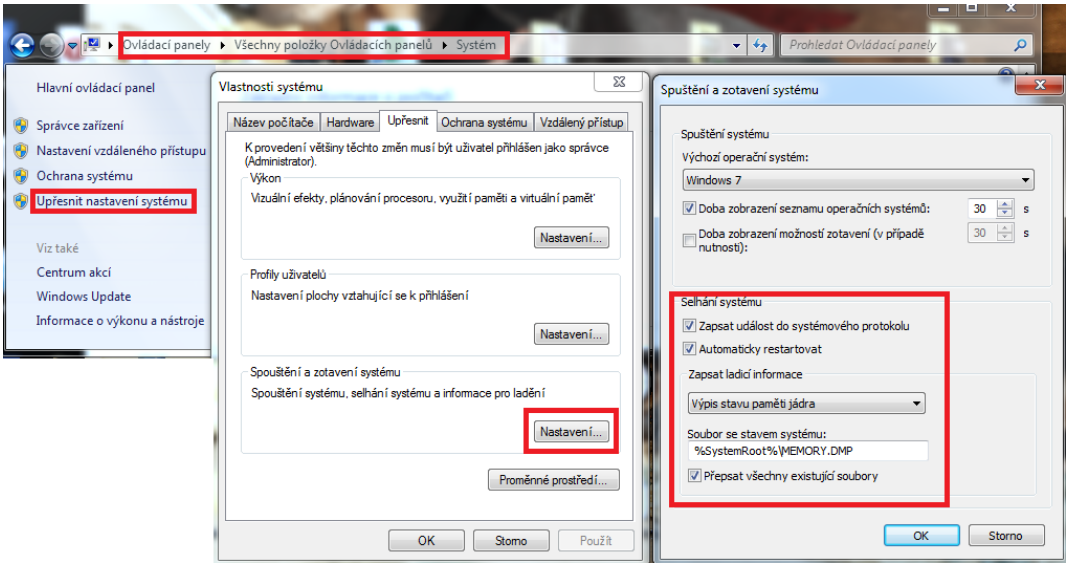
3.3.4 Další možnosti zkoumání aktivních dat v počítači:

3.3.4.1 Microsoft Crash Dump

Každý operační systém Microsoft Windows má přednastavené uložení aktuálních informací o stavu daného konkrétního operačního systému pro případ systémového pádu tzv. soubor typu „Microsoft Crash Dump“. Tato data se uloží do souboru s názvem „MEMORY.DMP“ (možno změnit). Jedná se o případ pádu celého operačního systému, nikoli o pád jednotlivé aplikace. Tento soubor lze pak podrobit forenzní analýze za použití různých nástrojů, například Microsoft debugging tools.

Nastavení pro tento soubor najdeme např. u operačního systému Windows 7:

Ovládací panely – Systém – Upřesnit nastavení systému – Upřesnit – Spouštění a zotavování systému – Nastavení (Obrázek 32).



Obrázek 32: Nastavení využívání souboru typu DMP.

Zde můžeme nastavit tři druhy záloh pro případ pádu systému:

- Complete Memory Dump

Tato záloha obsahuje celý obsah fyzické paměti v čase pádu systému. Tento typ zálohy je doporučován, jestliže je velikost souboru pagefile.sys nastavena nejméně na velikost fyzické paměti plus 1 MB (z důvodu zapsání hlavičky). Tento typ zálohy je možný použít pouze u některých distribucí operačního systému jako jsou NT4 a serverové distribuce.

- Kernel Memory Dump – Výpis stavu paměti jádra.

Tento druh zálohy obsahuje pouze informace z fyzické paměti, které jsou uloženy v tzv. kernel části v době systémového pádu. To znamená, že obsažená data v záloze neobsahují žádné informace ohledně procesů uložených v části paměti pomocí user módu. Například seznam spuštěných procesů, stav procesorových vláken a seznam načtených ovladačů je uložen v nenastránkované (nonpaged) části paměti, takže tato data jsou součástí tohoto typu zálohy. Velikost této zálohy je závislá na velikosti části kernel paměti, která je přidělena operačním systémem.

- Small Memory Dump – Zkrácený výpis stavu paměti.

Tento druh zálohy má většinou velikost 64 KB pro 32 bitovou verzi systému a 128 KB pro 64 bitovou verzi. Tato záloha obsahuje tzv. stop kódy, parametry, seznam načte-

ných ovladačů, informace o aktuálních spuštěných procesech, využití procesorových vláken a kernel proces, který zapříčinil spadnutí systému.

Obrázek 33: Systémový pád systému MS Windows - tzv. modrá smrt.

Struktura souboru „DMP“

Struktura tohoto souboru je odlišná podle architektury počítače (32 bitová nebo 64 bitová), na které byl soubor vytvořen. Tento formát byl vytvořen pro ladění systému a ne pro forenzní účely, a tak je v proprietárním (uzavřeném) stavu. V tomto souboru jsou také během jeho vytváření přidány zájmové informace.

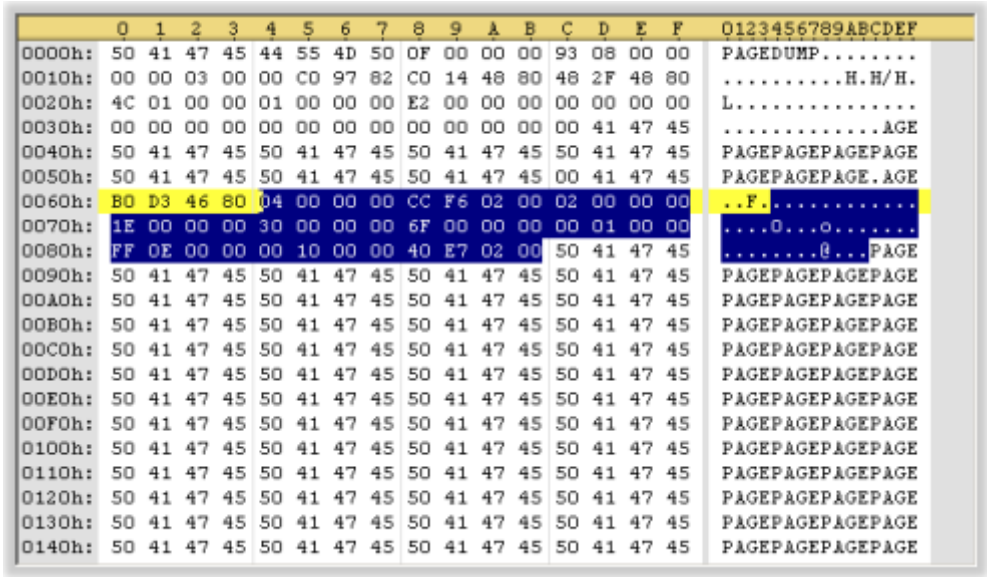
Na začátku souboru je hlavička (4096 bytů). Dále budou uvedeny informace z části této hlavičky. [10]

- 32 bitová verze:

Offset	Type	Field	Remarks
0x000	char	Signature[4]	'PAGE'
0x004	char	ValidDump[4]	'DUMP'
0x008	uint32	MajorVersion	
0x00c	uint32	MinorVersion	windows build no.
0x010	uint32	DirectoryTableBase	
0x014	uint32	PfnDataBase	
0x018	uint32	PsLoadedModuleList	
0x01c	uint32	PsActiveProcessHead	
0x020	uint32	MachineImageType	
0x024	uint32	NumberProcessors	
...			
0x05c	char	PaeEnabled	
...			
0x064	char	PhysicalMemoryBlockBuffer[700]	
...			
0xf88	uint32	DumpType	1 = full dump, 2 = kernel dump (smaller)
...			
0xfa0	int64	RequiredDumpSpace	should equal dump file size
...			
0xfb8	int64	SystemUpTime	measured in units of 100 ns
0xfc0	int64	SystemTime	FILETIME
...			

Obrázek 34: Struktura hlavičky souboru DMP v 32-bitové verzi

Dále je tu hlavička souboru (Obrázek 35) zobrazená v programu umožňující zobrazení v hexadecimální soustavě.



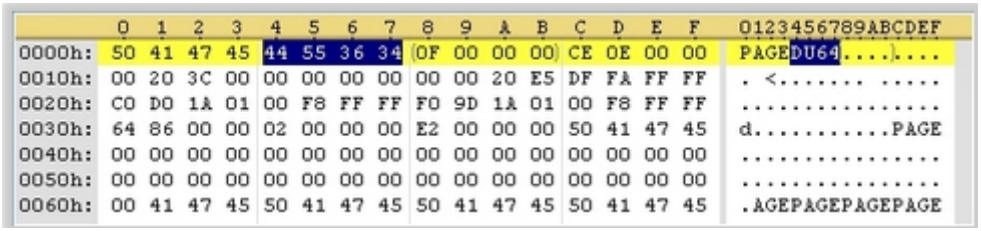
Obrázek 35: Hlavička 32 bitového souboru DMP v hexadecimální soustavě.

- 64 bitová verze:

Offset	Type	Field	Remarks
0x000	char	Signature[4]	'PAGE'
0x004	char	ValidDump[4]	'DU64'
0x008	uint32	MajorVersion	
0x00c	uint32	MinorVersion	Windows build no.
0x010	uint64	DirectoryTableBase	
0x018	uint64	PfnDataBase	
0x020	uint64	PsLoadedModuleList	
0x028	uint64	PsActiveProcessHead	
0x030	uint32	MachineImageType	
0x034	uint32	NumberProcessors	
...			
0x088	char	PhysicalMemoryBlock[0x80]	
...			
0xf98	uint32	DumpType	1 = full dump, 2 = kernel dump (smaller)
...			
0xfa0	int64	SystemUpTime	measured in units of 100 ns
0xfa8	int64	SystemTime	FILETIME

Obrázek 36: Hlavička 64 bitového souboru DMP v hexadecimální soustavě.

A dále část hlavičky souboru (Obrázek 37), na kterém je na první pohled patrný fakt, že se jedná o soubor vytvořený na 64 bitové architektuře. [11]

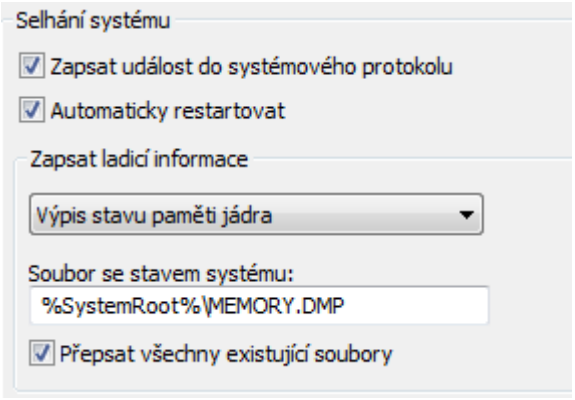


Obrázek 37: Část hlavičky 64-bitové architektury v hexadecimální soustavě.

Poznámka: Pokud máme nastavenou zálohu na možnost kompletní zálohy, pak při pádu systému dojde ke kontrole, jestli soubor pagefile.sys má dostatečnou velikost. Minimální velikost tohoto souboru s ohledem na kapacitu fyzické paměti RAM.

Tabulka 2: Minimální velikosti souboru pagefile.sys podle kapacity paměti RAM.

Fyzická paměť RAM	Minimální velikost souboru Pagefile.sys
< 128MB	50MB
<4GB	200MB
<8GB	400MB
>=8GB	800MB



Obrázek 38: Grafické nastavení systému při jeho selhání.

Poznámka: Při startu operačního systému dojde ke kontrole nastavení klíčů v registru z adresy HKLM\System\CurrentControlSet\Control\CrashControl. Tyto údaje se shodují s údaji, které se dají nastavit v grafické nástavbě (Obrázek 39).

Název	Typ	Data
(Výchozí)	REG_SZ	(Hodnota není nastavena.)
AutoReboot	REG_DWORD	0x00000001 (1)
CrashDumpEnabled	REG_DWORD	0x00000002 (2)
DumpFile	REG_EXPAND_SZ	%SystemRoot%\MEMORY.DMP
DumpFilters	REG_MULTI_SZ	MfeEpeHb.sys dumpfve.sys
LogEvent	REG_DWORD	0x00000001 (1)
MinidumpDir	REG_EXPAND_SZ	%SystemRoot%\Minidump
MinidumpsCount	REG_DWORD	0x00000032 (50)
Overwrite	REG_DWORD	0x00000001 (1)

Obrázek 39 - Nastavení systému při jeho selhání v registrech.

Vysvětlení hodnot v registrech:

- Zapsat událost do systémového protokolu = LogEvent.
- Automaticky restartovat = AutoReboot.
- Zapsat ladící informace = CrashDumpEnabled.
- Soubor se stavem systému = DumpFile.
- Přepsat všechny existující soubory = Overwrite.

Shrnutí:

- Pro forenzní analýzu je nejhodnotnější kompletní záloha.

- Nastavení kompletní zálohy není standardně přednastaveno u většiny systému a přednastavení vyžaduje restart.
- Problémy s nastavením kompletní zálohy u pamětí větších jak 2GB.
- Analýza za pomocí nástroje Microsoft debugging tools a dalších.

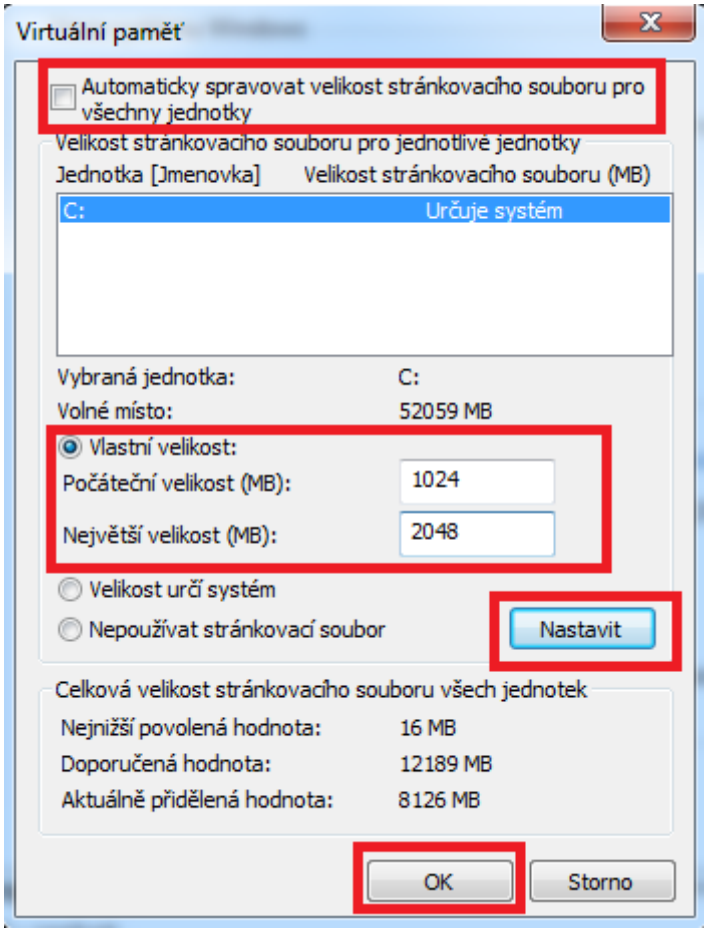
3.3.4.2 Pagefile.sys

Jedná se o systémový soubor, který využívá operační systém Windows k vytvoření a používání virtuální paměti, jeho umístění je v kořenové složce jednotky, na které je nainstalovaný operační systém. Po naistalování nového systému Windows je používání virtuální paměti zapnuto a jeho velikost je automaticky spravována systémem.

Ve více-úlohovém operačním systému je obecně nutné umístit do paměti více procesů najednou. Jestliže jsou k dispozici funkce na virtualizaci paměti, lze vytvořit každému z procesů jeho vlastní adresní prostor. Virtuální adresní prostor je rozdělen na stránky, které odpovídají různým stejně velkým stránkám ve fyzické paměti (RAM).

Stránkování na disku (pomocí souboru pagefile.sys) umožňuje rozšířit operační paměť o místo ve vnější paměti (na pevný disk, flashdisk…), kam jsou odkládány právě nepoužívané stránky paměti. Tím je možné uvolnit rychlejší operační paměť RAM a umožnit tak její efektivnější rozšíření a využívání. Při použití stránkování paměti na vnější paměť je tabulka stránek rozšířena o příznak, který umožňuje rozlišit, zda je stránka v paměti RAM nebo je odložena na vnější paměť. [12]

Například pokud máme paměť RAM v počítači o kapacitě 2GB a chceme nebo potřebujeme využívat paměť o velikosti 4GB, tak nastavíme v počítači možnost využívat virtuální paměť (Microsoft Windows 7: „Ovládací panely – Systém – Upřesnit nastavení systému – záložka upřesnit – výkon – nastavení – upřesnit – virtuální paměť – změnit..“) a nastavíme její maximální velikost na 2GB (Obrázek 40).

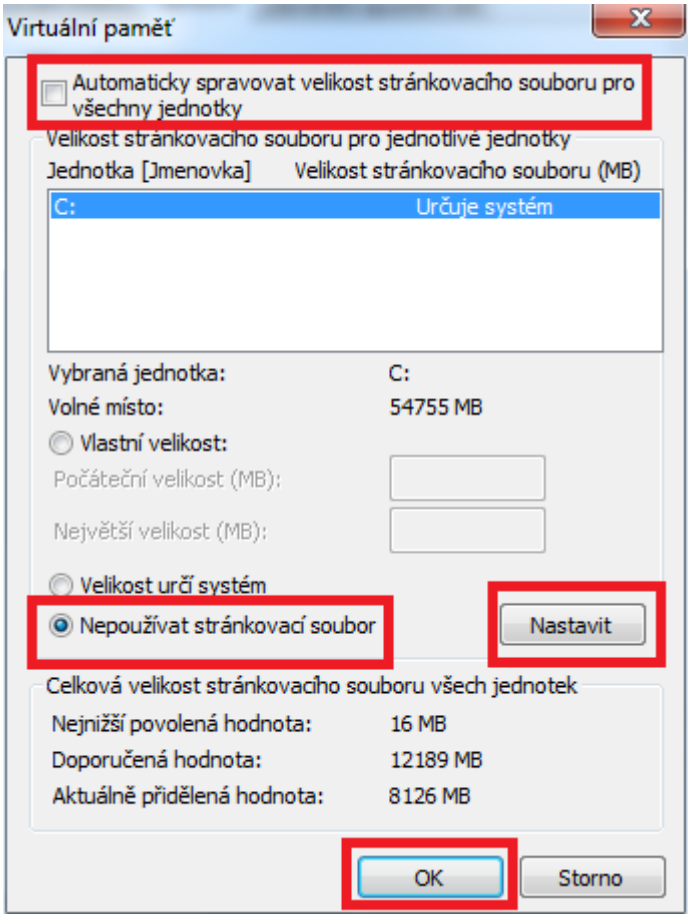


Obrázek 40: Nastavení velikosti virtuální paměti - soubor pagefile.sys.

Poznámka: Pokud chceme vypnout využívání virtuální paměti a následně vymazat tento soubor ze systému (získání místa na systémovém disku (problém SSD disků), obava z forenzní analýzy tohoto souboru)budeme postupovat takto:

Microsoft Windows 7

- Ovládací panely – Systém – Upřesnit nastavení systému – záložka upřesnit – výkon – nastavení – upřesnit – virtuální paměť – změnit (Obrázek 41).



Obrázek 41: Vypnutí využívání virtuální paměti.

Existuje několik možností jak se dostat k datům uložených v souboru Pagefile.sys, ale dnes je nejjednodušším způsobem získání za pomocí forenzního programu (který nemusí být instalován na cílovém počítači). Například již výše popsané: Belkasoft Live Ram Capturer, FTK Imager a jiné.

Nástroj PCT

Tento nástroj pojmenovaný PCT (page collection tool) byl vyvinut panem Soekhee a jeho kolegy k získání přístupu k tomuto souboru v běžícím systému Windows. Podle jejich experimentů byly schopni získat 1GB dat z tohoto souboru na externí úložiště za přibližně 3-4 minuty. Bohužel tento nástroj není uvolněn k používání.

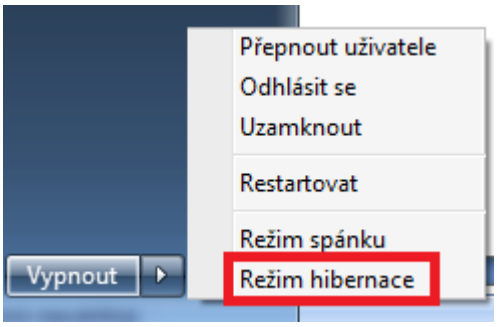
Komerční nástroje – nutná instalace na cílový počítač

- Disk Explorer
- Forensic Tool Kit
- X-Ways Forensics
- iLook

3.3.4.3 Hiberfil.sys

Jedná se o soubor, který je systémový a skrytý, jeho umístění je v kořenové složce jednotky, na které je nainstalovaný operační systém. Správce napájení jádra systému Windows vytvoří tento soubor při instalaci systému Windows. Velikost tohoto souboru se přibližně rovná velikosti operační paměti RAM nainstalované v počítači.

Tento soubor je využíván, pokud je operační systém Windows přiveden do tzv. stavu hibernace. Do tohoto souboru je zapsán obsah systémové paměti v době hibernace. To znamená, že z tohoto souboru jde získat identická data jako ze zálohy paměti RAM.



Obrázek 42 - Přivedení systému do režimu hibernace.

Tento soubor je komprimovaný pomocí vlastního formátu firmy Microsoft a pro analýzu je nejprve nutné tento formát převést do čitelné podoby. Tento převod umožňují některé softwary pro analýzu aktivních dat (Belkasoft Evidence Center,Volatility, a další).

Poznámka: Operační systém Microsoft Windows má dva režimy pro uvedení počítače do úsporného stavu. První z nich je režim spánku, který dostane počítač pouze do stavu malé spotřeby energie a počítač po spuštění z tohoto stavu může téměř okamžitě pokračovat v práci (fyzické paměti RAM zůstávají stále napájené tzn. data jsou stále aktivní v paměti). Druhým režimem je hibernace, který po aktivování zapíše veškerá data z paměti do souboru (hiberfil.sys) na pevný disk a počítač je vypnut a může být odpojen od napájení.

Poznámka 2: Pokud chceme vypnout režim hibernace a následně vymazat tento soubor ze systému (získání místa na systémovém disku (problém SSD disků), obava z forenzní analýzy tohoto souboru)budeme postupovat takto:

Windows 7 nebo Vista:

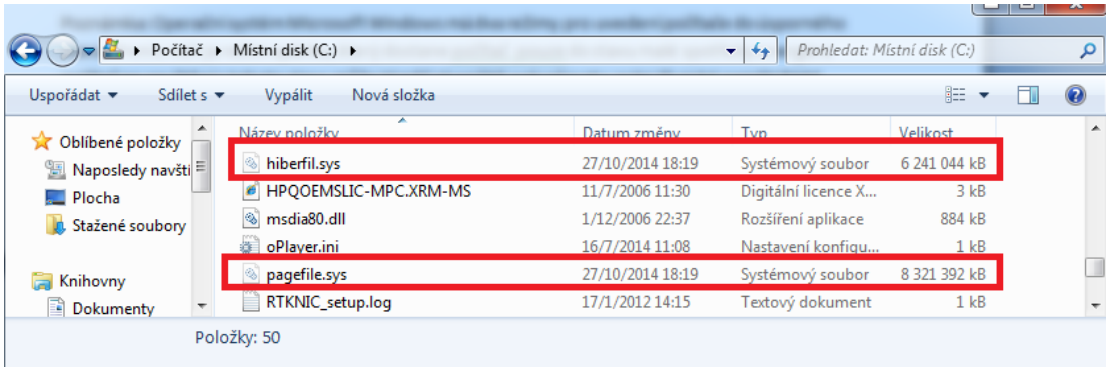
- Zapnutí příkazového řádku (příkaz cmd) jako administrátor a spuštění příkazu:

„powercfg.exe /hibernate off“ nebo „powercfg.exe -h off“.

Windows XP:

- Vypnutí se provede v nastavení: „Ovládací panely – Možnosti napájení “ a zde se vybere záložka hibernace, v které lze režim hibernace vypnout.

Poté by mělo dojít k automatickému odstranění souboru hiberfil.sys a nebo již lze soubor manuálně vymazat.



Obrázek 43: Systémové soubory v operačním systému Windows 7, 64 bitová verze, s 8 GB operační pamětí.

4 NEJPOUŽÍVANĚJŠÍ SOFTWARY PRO ZÍSKÁVÁNÍ INFORMACÍ ZE ZAŠIFROVANÝCH DAT A JEJICH VLASTNOSTI

4.1 ElcomSoft Password Recovery Bundle

Jedná se o kompletní balík umožňující obnovu hesel pro většinu běžných zašifrovaných dat (jednotlivé programy se dají koupit také samostatně) od ruské firmy ElcomSoft. Tato firma je jednou z průkopníků softwaru na obnovu zašifrovaných dat. Tento software umožňuje získání hesel z operačních systémů, produktů Microsoft Office, produktů firmy Adobe (soubory typu PDF), archivačních souborů (typu RAR a ZIP), zašifrovaných oddílů nebo kontejnerů (TrueCrypt, BitLocker, Symantec Encryption Desktop …) a mnohé další. [13]

4.1.1 Obecné informace

Tento software podporuje akceleraci pomocí grafických karet a tento způsob zrychlení má tato firma také patentováno. Jedná se o podporu jednotek všech grafických karet značek NVIDIA i AMD. U určitých šifrovacích algoritmů se může jednat o zrychlení vyhledávání hesel až o 50 násobek.

Tento balík dále podporuje distribuovaný útok (při útoku je využíváno více jednotlivých počítačů) – u licence Standard (5 klientů), Forensic (20 klientů), Business (100 klientů).

Jak již bylo napsáno výše, jedná se o softwarový balík, který obsahuje jednotlivé programy podle zakoupené edice. Zde je přehled těch nejvíce používaných podle typu vyhledávaných hesel pro určitou skupinu dat:

- Dokumenty Microsoft Office
  - Advanced Office Password Recovery
    - Podporuje dokumenty od verze Microsoft Office 95 po aktuální verzi.
    - K najití hesla je možno využít: útok hrubou silou, mask útok, slovníkový útok.
    - Ve třech verzích: Home, Standard, Professional.
  - Advanced Office Password Breaker
    - Pouze pro dokumenty Microsoft Word a Excel 97/2000/2003 (koncovky souboru doc a xls).
    - Nehledá heslo jako takové, ale vzhledem k použití slabé šifry u těchto dokumentů dojde k odemčení dokumentu téměř okamžitě (heslo se odstraní).
- E-maily a IM klienti

    - Advanced Mailbox Password Recovery
        - Obnova hesel z nejběžnějších e-mailových klientů (údaje musí být uloženy lokálně).
        - Obsahuje POP3/IMAP server emulator – podpora pro obnovu hesel z dalších e-mailových klientů.
        - Všechna hesla jsou nalezena okamžitě a zobrazena pomocí dekódování.
    - Advanced Instant Messengers Password Recovery
        - Obnova hesel z nejběžnějších IM klientů (údaje musí být uloženy lokálně) – přes 30 nejpoužívanějších klientů.
        - Všechna hesla jsou nalezena okamžitě a zobrazena pomocí dekódování.
- Adobe Acrobat
    - Advanced PDF Password Recovery
        - Podpora všech verzí a všech použitých šifrovacích algoritmů.
        - Odstranění všech omezení (otevření, editace, tisk a další) okamžitě bez rozdílu síly hesla.
        - Tři verze: Standard, Professional, Enterprise.
- Archivační dokumenty
    - Advanced Archive Password Recovery
        - Podpora nejpoužívanějších archivačních nástrojů : ZIP (PKZIP, WinZIP), ARJ/WinARJ, RAR/WinRAR and ACE/WinACE.
- Komplexní software využívající distribuovaný útok
    - Distributed Password erecovery
        - Podpora velkého množství šifrovaných dat: Microsoft Office, Microsoft Money, Microsoft OneNote, Adobe Acrobat, Intuit Quicken, Lotus Notes, přístupová hesla do Windows 2000/XP/2003/Visa/7/8, PGP privátní klíče (*.skr), PGP Disk (*.pgp), TrueCrypt (*.tc) a mnohé další.
        - Obsahuje tři komponenty: server (instalován na jednom z počítačů v síti a pomocí něho se spravují procesy vyhledávání hesel), agent (instalovaný na jakémkoli počítači v sítí, testuje hesla vygenerovaná serverem) a konsole (může být nainstalována na jakémkoli počítači a pomocí ní se ovládá server).

Tento balík se prodává ve 3 různých edicích (Obrázek 44).

Compatibility Chart

	Standard Edition	Forensic Edition	Business Edition
Advanced Archive Password Recovery Pro	1	1	10
Advanced EFS Data Recovery Pro	1	1	10
Elcomsoft Internet Password Breaker	1	1	10
Advanced Instant Messengers Password Recovery	1	1	10
Advanced Intuit Password Recovery	1	1	10
Advanced Lotus Password Recovery	1	1	10
Advanced Mailbox Password Recovery	1	1	10
Advanced Office Password Breaker	1 (Pro)	1 (Ent)	1 (Ent)
Advanced Office Password Recovery Pro	1	1	10
Advanced PDF Password Recovery	1 (Pro)	1 (Ent)	1 (Ent)
Advanced Sage Password Recovery	1	1	10
Advanced SQL Password Recovery	1	1	10
Advanced WordPerfect Office Password Recovery	1	1	10
Proactive System Password Recovery	1	1	10
Proactive Password Auditor	-	up to 100 accounts	up to 500 accounts
Elcomsoft Distributed Password Recovery	up to 5 clients	up to 20 clients	up to 100 clients
Elcomsoft System Recovery	1 (Std)	1 (Pro)	1 (Pro)
Elcomsoft Wireless Security Auditor Pro	-	1	1
Elcomsoft Phone Breaker Forensic	-	1	1
Elcomsoft Blackberry Backup Explorer Pro	-	1	1
Elcomsoft Forensic Disk Decryptor	-	1	1
Elcomsoft Phone Viewer Standard Edition	-	1	1
Free delivery by Express Mail (EMS)	✓	✓	✓
	Order now	Order now	Order now

Obrázek 44: ElcomSoft Passwotd Recovery Bundle – porovnání edic. [14]

4.1.2 Cena

Verze softwarového balíku ElcomSoft recovery Bundle:

- Standard Edition – 1599 Eur
- Forensic Editon – 4995 Eur
- Business Edition – 13995 Eur

Všechny tyto verze se prodávají s 1 roční podporou.

4.1.3 Systémové požadavky a možnosti

- Podporované operační systémy:
  - Windows 7 (32 i 64 bitové verze)
  - Windows Server 2003 a 2008
  - Windows Vista (32 i 64 bitové verze)
  - Windows XP
- Je nutné mít administrátorská práva.

- Zapotřebí je okolo 13 GB volného místa (především kvůli rainbow tabulkám – základní tabulky).
- Podpora NVIDIA a ATI grafických karet.
- Podpora hardwarového akcelerátoru - Tableau TACC1441.

4.2 Passware Password Recovery Kit

Jedná se o komplexní software pro získávání informací ze zašifrovaných dat a aktuální dostupná verze tohoto programu je 2015 V.2.

4.2.1 Obecné informace

Hlavními rysy tohoto programu jsou:

- Obnova z více jak 200 typů souborů (včetně zašifrovaných disků a diskových oddílů).
- Okamžitý přístup do některých zašifrovaných souborů – soubory typu Microsoft Word a Excel do verze 2003 (nutný přístup na internet nebo přikoupení dalšího softwaru).
- Možnost vytvoření skriptu pro vymazání administrátorského hesla do operačního systému Microsoft Windows.
- Obnova přístupových hesel do operačního systému Microsoft Windows z paměti RAM nebo ze SAM souboru.
- Obnova hesel z účtu Facebook, Google a jiné za pomoci paměti RAM nebo hibernačních souborů.
- Možnost hledání hesel z hash souborů.
- Podpora 9 různých útoků pro obnovu hesla.
- Podpora vícejádrových procesorů a neomezeného množství grafických karet typu NVIDIA a ATI.
- Podpora hardwarových akcelerátorů Tableau TACC.
- Podpora pro 64-bitovou verzi.
- Vyhledávání zašifrovaných souborů a diskových oddílů.
- Obsahuje podporu pro vytvoření bitové kopie paměti RAM pomocí FireWire útoku.
- Podora vyhledávání šifrovacích klíčů ze zálohy paměti RAM.
- Možnost využít distribuovaný útok – agenti jsou k dispozici, jak pro verzi operačních systémů Microsoft Windows, tak pro Linux.
- Možnost spuštění z flashdisku – nic není nutné instalovat na cílovém počítači.
- Možnost integrace se softwary: Guidance EnCase (verze 7 a vyšší) a Oxygen Forensic Suite (verze 2014 a vyšší). [15]

Tento software je nabízen hned v několika verzích: Basic, Standard, Professional, Enterprise, Forensic a Forensic Lab. Jelikož tato práce pojednává o forenzní analýze, tak se budeme zabývat verzemi programu Forensic a Forensic Lab.

4.2.2 Rozdíly mezi Forensic a Forensic Lab

- Počet agentů: 5 ku 100.
- Podpora: 1 rok ku 3 roky.
- Cena: 995$ ku 3995$.

4.2.3 Systémové požadavky

- Podporované operační systémy:
  - Windows 7 (32 i 64 bitové verze)
  - Windows 8 (32 i 64 bitové verze)
  - Windows Server 2003, 2008 a 2012
  - Windows Vista
- Je nutné mít administrátorská práva.
- Podpora NVIDIA a ATI grafických karet.
- Podpora hardwarového akcelerátoru - Tableau TACC1441.
- 150 MB volného místa na disku (další kapacita podle použitých rainbow tabulek a slovníků).

4.3 Extreme GPU Bruteforcer

Jedná se o software vyvinutý firmou insidePro, který slouží k obnovení hesel z hashí pomocí grafických karet. Hlavní vlastnosti toho programu jsou:

- Podpora více jak 70 druhů hashí.
- Využití až 16 grafických karet najednou.
- Neomezené množství načtených hashí.
- 32 i 64 bitová verze.
- Hash moduly jako samostatné DLL soubory.
- Podpora útoku hrubou silou, mask útoku, slovníkového útoku a hybridního útoku (kombinovaný útok z předešlých možností).
- Podpora pouze grafických karet na bázi CUDA technologie (NVIDIA).
- Podpora přerušení/pokračování hledání hesel.
- Tento produkt je zcela zdarma.
- Aktuální verze: 3.2. [16]

4.4 oclHashcat

Jedná se o čistě GPGPU naprogramovaný software pro obnovu hesel z hashí. OclHashcat vznikl vývojem a spojením velice známých softwarů na obnovu hesel oclHashcat-plus a oclHashcat-lite.[5]

Hlavními vlastnostmi tohoto programu jsou:

- Podpora více grafických karet najednou (až 128).
- Možnost načtení velkého množství hashí k „louskání“ najednou (až 100 miliónů hashí).
- Podpora operačních systémů Microsoft Windows i Linux.
- Podpora, jak CUDA, tak OpenCL (grafické karty značek NVIDIA a ATI).
- Při spuštění programu je daný počítač stále použitelný na ostatní práci.
- Podpora přerušení/pokračování hledání hesel.
- Podpora útoku hrubou silou, mask útoku, slovníkového útoku a hybridního útoku (kombinovaný útok z předešlých možností).
- Integrované hlídání teplot GPU.
- Tento produkt je zcela zdarma.
- Aktuální verze: 1.35. [17]

[5] **hashcat.** oclhashcat. *http://hashcat.net.* [Online] http://hashcat.net/oclhashcat/

II. PRAKTICKÁ ČÁST

5 ZÍSKÁVÁNÍ INFORMACÍ ZE ZAŠIFROVANÝCH DAT

Následné informace a postupy budou brány z pohledu soudního znalce v oboru kybernetika (ať již soukromého nebo příslušníka Policie ČR), protože nikdo jiný není oprávněn v České Republice vykonávat zajišťování digitálních stop spolu s manipulací na „živých" strojích a provádět následnou analýzu (sepsání odborného vyjádření nebo znaleckého posudku).

Získávání informací ze zašifrovaných dat nezačíná, jak by se mohlo zdát, rozbalením kriminalistické stopy (notebook, stolní počítač, externí disk, flashdisk a další) a její následnou forenzní analýzou, nýbrž samotným správným zajištěním dané stopy.

5.1 Správné získání kriminalistické stopy (výpočetní techniky)

Jedna z důležitých otázek při přípravě například před domovní prohlídkou, kde by mělo dojít k zajištění digitálních dat, je správné naplánování celého postupu. Tento postup musí být konzultován s vedoucím dané realizace a následně musí být dohodnut postup, kde bude minimalizována šance ztráty zájmových dat. V dnešní době každodenní možnosti šifrování (viz. programy, které jsou popsány výše) je nutné předpokládat, že pokud mají být zajišťována digitální data, tak existuje poměrně velká šance, že se na daných stopách budou nacházet právě data šifrovaná. A právě informace z těchto šifrovaných dat bývají často nejvíce důležitými. Z tohoto důvodu autor této práce doporučuje ke každému výjezdu a každé digitální stopě přistupovat tak, jako by se na ní nacházela šifrovaná data. Z tohoto důvodu, pokud to povaha zásahu umožňuje, je zapotřebí maximalizovat šanci, aby pří zásahu danou „šifrovanou" stopu pachatel používal. Ať už se jedná o přihlášený počítač, kde jsou připojeny šifrované kontejnery nebo o přihlášený počítač, na kterém je využíváno šifrování celého disku.

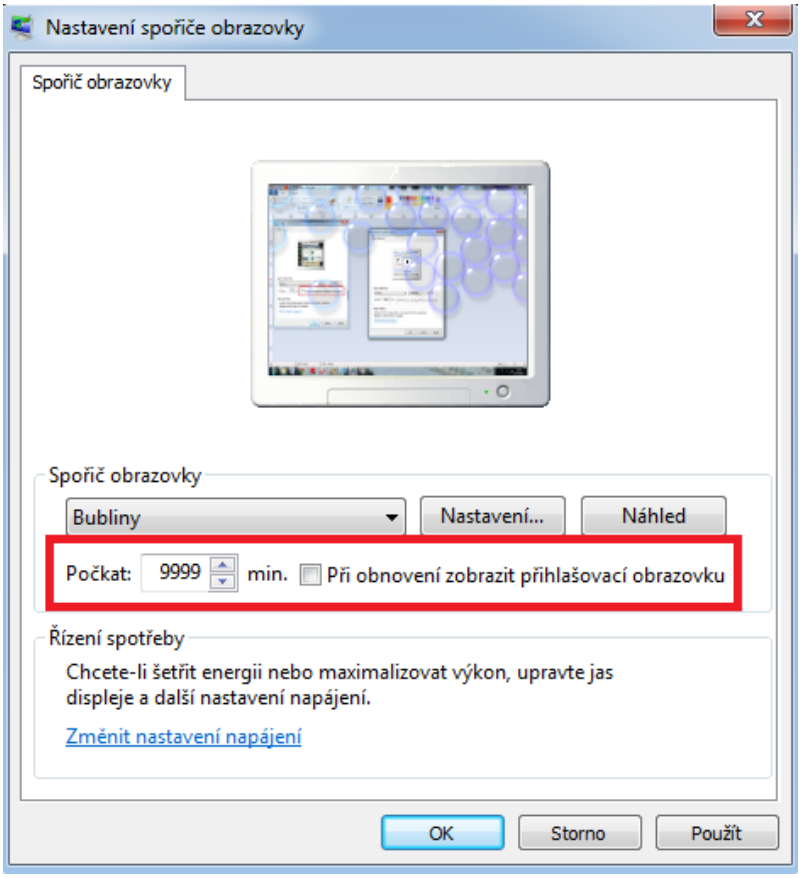
Dále je samozřejmě velice důležité mít s sebou při zásahu potřebné vybavení, ať už softwarové nebo hardwarové. Vše důležité je nutné mít při ruce ve forenzních kufrech:

- Softwarové vybavení:
  - FTK Imager
  - Passware Kit Forensic Portable
  - EDD, TCHunter
  - RAM Capturer, Belkasoft Live RAM Capturer
- Hardwarové vybavení:
  - Notebook s FireWire vstupem/výstupem
  - FireWire kabel

- Externí FireWire karty do notebooků – PCMCIA, ExpressCard
- Pevné disky – alespoň 2 kusy s minimální kapacitou 3 TB
- Flashdisky – forenzní programy, záloha zájmových dat, live operační systémy…

5.2 Postup na zásahu - zabezpečení stop

Po domluvě s vedoucím zásahu se jde na daný zásah v době, kdy je největší pravděpodobnost aktivity pachatele na zašifrovaných datech. Po přístupu do zájmového objektu provede soudní znalec, jakmile to okolnosti dovolí, okamžité zabezpečení zájmových počítačů – vypnutí spořiče obrazovky, vypnutí možnosti hibernace/uspání. Dále je doporučeno, pokud je to možné z povahy věci, odpojit zájmové počítače od sítě, včetně WiFi připojení (z důvodu možnosti vypnutí nebo manipulace s počítačem na dálku). Podle trestního řádu §84 (předchozí výslech), lze vykonat domovní prohlídku jen po předchozím výslechu toho, u koho nebo na kom se má takový úkon vykonat. Ale zároveň je zde poznamenáno, že předchozího výslechu není třeba, jestliže věc nesnese odkladu. A to z mého pohledu je tento případ, protože pokud by nebyly zabezpečeny zájmové počítače, tak by mohlo dojít ke znehodnocení části zájmových dat (stop).



Obrázek 45: Deaktivace spořiče obrazovky (Windows 7).

5.3 Zajištění dat na zájmových stopách před jejich zapečetěním

Poté (nebo již v průběhu), co jsme provedli nezbytné úkony vedoucí k tomu, aby žádná data (stopy) nebyla znehodnocena, proběhnou úkony, které jsou stanoveny v trestním řádu (poučení, předběžný výslech a další).

Dále soudní znalec postupuje chronologicky od stop s největší prioritou po ty méně zájmové (může dojít například k výpadku/vypnutí přívodu elektrického proudu). Zde může nastat několik možností, v jakém stavu se bude daná zájmová stopa nacházet:

- Počítač se nachází v zapnutém stavu a zájmový uživatel je přihlášen.
- Počítač se nachází v zapnutém stavu, ale zájmový uživatel není přihlášen (heslo nevíme a pachatel ho nevydá).
- Počítač se nachází ve vypnutém stavu.

5.3.1 Zapnutý počítač a zájmový uživatel přihlášen

Postup v jednotlivých krocích, které budou dále podrobněji popsány:

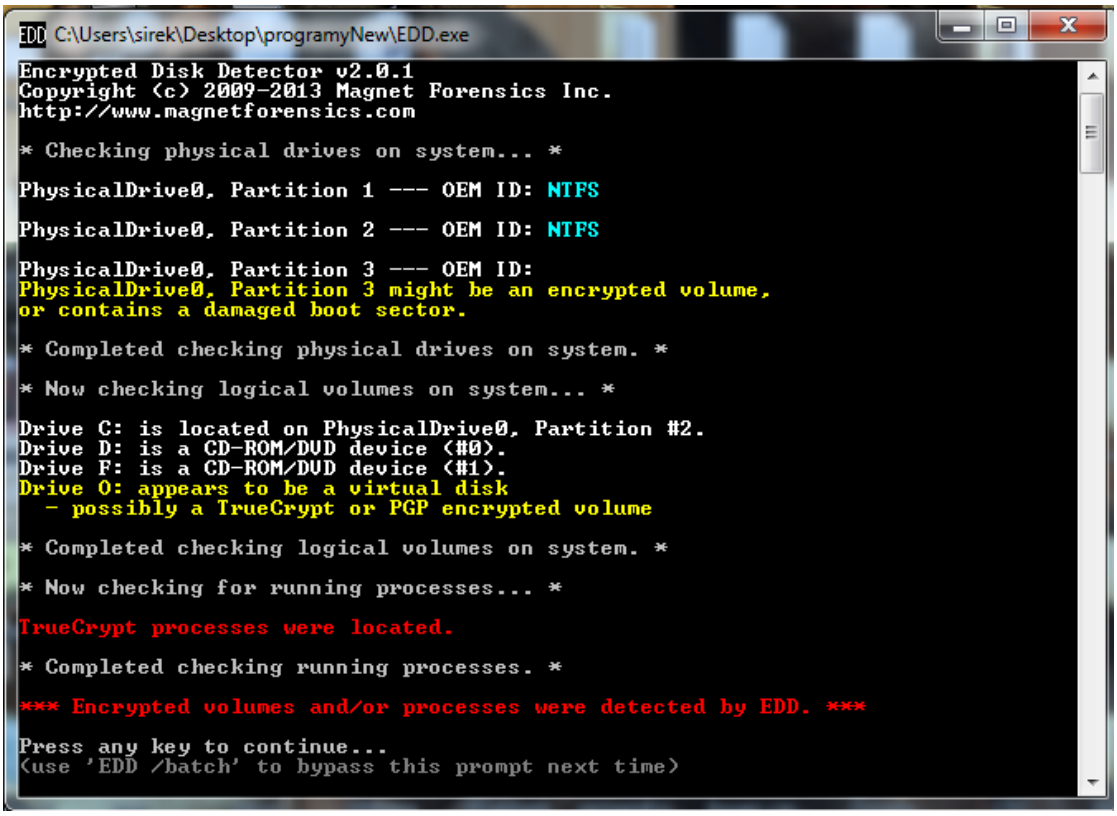
1. Hledání aktivních zašifrovaných dat.
2. Případné vytvoření bitové kopie šifrovaného oddílu.
3. Vytvoření bitové kopie paměti RAM a vykopírování souborů: hiberfil.sys, pagefile.sys a souborů pádu systému Windows.
4. Vyhledání uložených hesel.

Jedná se o ideální stav, v kterém se může zájmový počítač nacházet. Jako **krok číslo 1** soudní znalec provede manuální prohledání operačního systému – kontrola nainstalovaných programů, projití spuštěných procesů a zkontrolování hlavního panelu. Zde hledá programy, které souvisejí s možností šifrovat data, jak spuštěné, tak nainstalované a především dojde k vyhledání aktivně používaných šifrovaných dat.

Obrázek 46: Vizuální kontrola hlavního panelu – aktivní šifrovací softwary TrueCrypt a BitLocker.

Následuje spuštění programů pro automatickou detekci připojených šifrovaných diskových jednotek (oddílů, kontejnerů) – EDD, TCHunt.

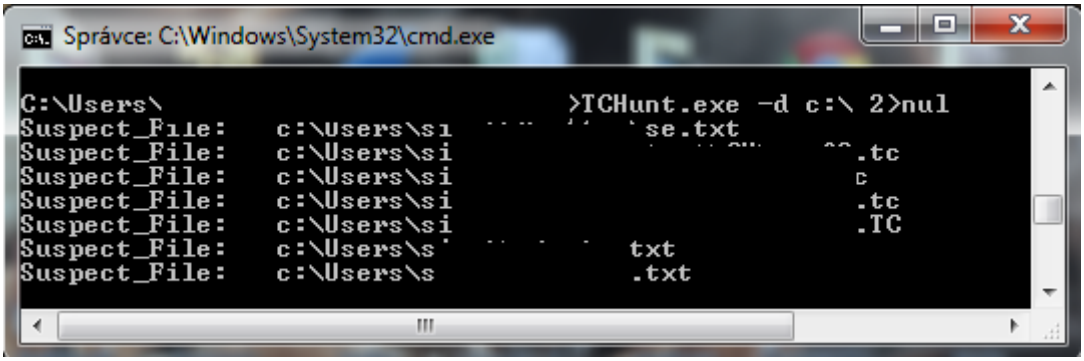
- EDD (Encrypted Disk Detector)
  - Nástroj detekující připojené šifrované diskové jednotky.
  - Aktuální verze: v2 (vydaná: 22. 4. 2013).
  - Od firmy Magnet Forensics.
  - Není potřeba žádné instalace (portablová verze).
  - Podporované šifrovací softwary: TrueCrypt, PGP, Safeboot, Bitlocker.
  - Zdarma po vyplnění formuláře ke stažení na stránkách výrobce.



Obrázek 47: Program EDD – detekce aktivních procesů programu TrueCrypt a upozornění na šifrovaný oddíl.

- TCHunt
  - Nástroj detekující zašifrované soubory (kontejnery) programu TrueCrypt.
  - Aktuální verze: 1.6.
  - Zdarma ke stažení.
  - Není potřeba žádné instalace (portablová verze).
  - Možnost falešně pozitivních výsledků.
  - Podporované šifrovací softwary: TrueCrypt.
  - Spuštění příkazu s Administrátorskými právy:
    - „TCHunt.exe –d c:\“ – vyhledává na diskovém oddílu C

- TCHunt -d c:\ 2>nul - vyhledává na diskovém oddílu C, ukáže pouze podezřelé soubory

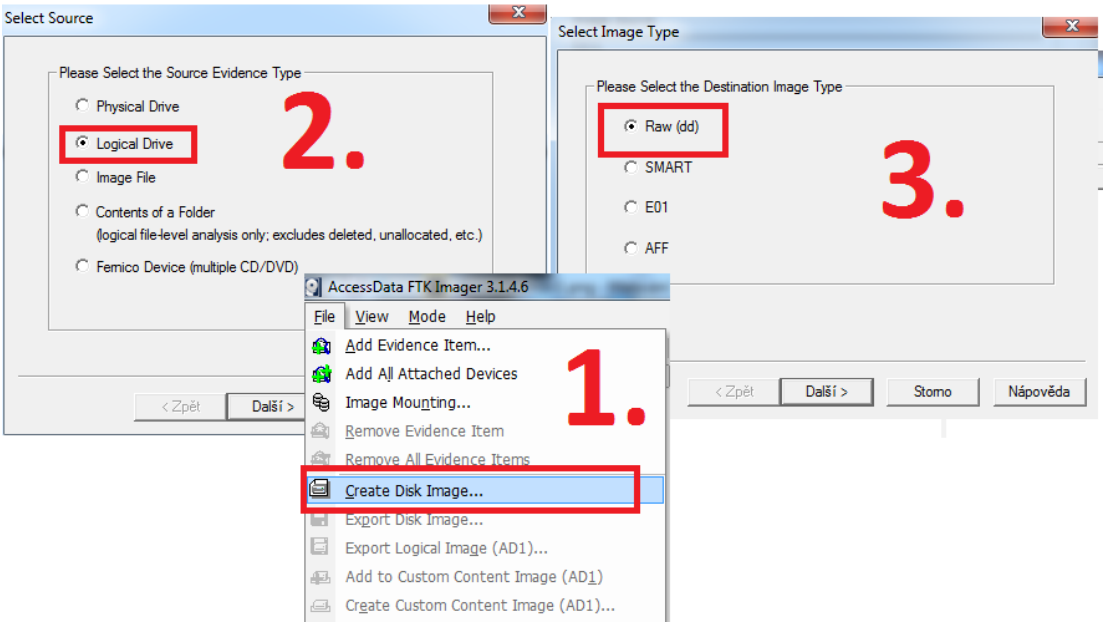


Obrázek 48: Program TCHunt nalezl na disku C podezřelé (zašifrované) soubory programem TrueCrypt.

Tyto programy jsou pro znalce pouze doplňkové a slouží k dalším možnostem ověření, že se na disku nachází šifrovaná data.

Pokud jsou na zájmové stopě nalezeny načtené/aktivní (přimountované) diskové oddíly (kontejnery), tak soudní znalec vytvoří bitovou kopii tohoto oddílu (**krok číslo 2**). Případně může být jako první zvolen postup - vykopírování zájmových dat ze zašifrovaného oddílu – tento postup je vhodný zvolit, pokud je například zašifrován celý systémový disk a my víme lokaci zájmových souborů – vykopírování těchto souborů by podle velikosti těchto dat, mělo zabrat z pravidla pár minut namísto vytváření bitové kopie kapacitně velikého oddílu, to by mohlo zabrat několik hodin (v tomto čase může dojít k nechtěnému vypnutí počítače, ale v takto vykopírovaných datech není možné obnovit smazaná data).

K vytváření bitové kopie šifrovaného oddílu může být použit software FTK Imager. Ať již za pomoci toho softwaru nebo jiného, tak je při nastavování vytváření bitové kopie nutné nastavit, aby se bitová kopie vytvářela z **logického** oddílu (namísto fyzického). Jinak by po načtení tohoto obrazu byla data nečitelná (stále v zašifrované podobě). Jako výstupní formát dat je doporučován tzv. raw (dd) formát, pokud není jasné, kdo bude a čím data zkoumat. Jedná se o "čistou" bitovou kopii bez přidaných informací a bez komprese (tento formát je podporován všemi forenzními softwary). Další možností jsou tzv. chytré formáty typu: „s01 a e01". Jedná se o formáty, které jsou doplněny informacemi o dané kopii a je zde možné nastavit velikost komprese dat (tento druh dat nemusí být podporován všemi softwary).



Obrázek 49: Vytváření bitové kopie logického disku pomocí softwaru FTK Imager.

Po vytvoření bitové kopie je velice důležité, si tuto bitovou kopii zkontrolovat. To může být provedeno tak, že načteme tuto kopii do softwaru, který podporuje načtení bitových kopií (například FTK Imager). Takto načtená kopie musí obsahovat čitelná data.

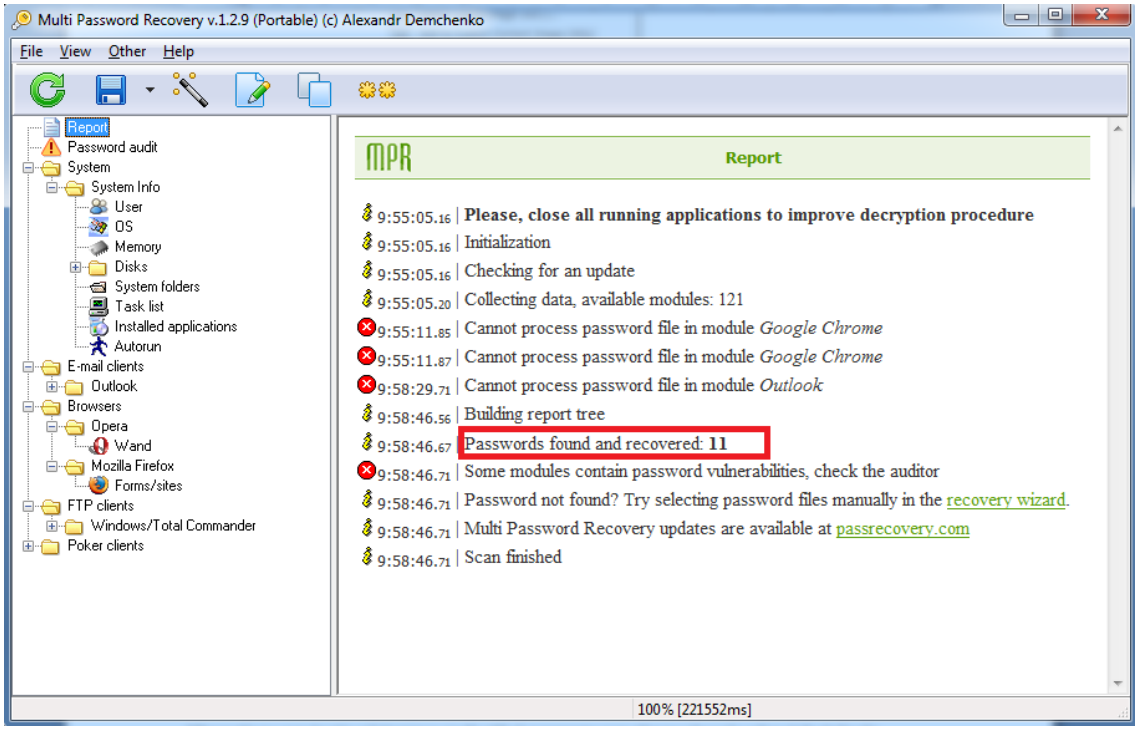
Poté, ať již byla vytvářena bitová kopie logického disku, nebo nebyla, následuje **krok číslo 3** - vytvoření bitové kopie paměti RAM (včetně vykopírování souborů: hiberfil.sys, pagefile.sys a souboru pádu systému Windows). Tento postup je podrobně popsán v kapitole: „Vytvoření obrazu paměti RAM – Softwarové nástroje“.

Následuje poslední úkon (**krok číslo 4**), a to vyhledání uložených hesel. Tento krok je velice důležitý z toho důvodu, že standardní uživatel nepoužívá rozdílná hesla na všechny svoje aplikace. Většinou bývá, že uživatel používá 2-5 rozdílných hesel na veškeré aplikace, které využívá. Potom je velice reálné, že když soudní znalec vyhledá uložená hesla (přihlašování do e-mailů, FTP, IM a další), že budou shodná s nějakým heslem použitým k zašifrování dat.

K tomuto úkonu se nechá využít velice dobrý softwarový nástroj - Multi Password Recovery. Jeho hlavními vlastnostmi jsou:

- Aktuální verze: 1.2.9 (7. 3. 2015).
- Ihned nalezne a obnoví hesla z více jak 110 nejpoužívanějších aplikací.
- Dokáže zobrazit hesla „schovaná“ za hvězdičkami.
- Zobrazuje systémové informace.

- Možnost uložení nalezených hesel do souboru.
- Je možné používat jako přenosnou (portablovou) verzi.
- Cena: 19.95$.



Obrázek 50: Obnovení uložených hesel za pomoci softwaru Multi Password Recovery.

Alternativou pro tento nástroj jsou jednotlivé programy pro obnovu hesel z webových stránek: www.nirsoft.net. Tyto programy jsou zcela zdarma.

5.3.2 Počítač se nachází v zapnutém stavu, ale zájmový uživatel není přihlášen

Pokud je počítač zapnut, ale není k dispozici uživatelské heslo, tak ještě existují možnosti, jak získat bitovou kopii paměti RAM. Z paměti RAM, jak již bylo napsáno výše, je možné „vytěžit“ uživatelská hesla, šifrovací klíče a mnohé další užitečné informace, a tudíž by měli být využity všechny možnosti pro její získání.

Tyto možnosti jsou:

- využití sběrnice FireWire
- zařízení Tribble
- tzv. Cold boot attack

Všechny tyto možnosti jsou popsány v kapitole „Vytvoření obrazu paměti RAM“ a podkapitolách „Hardwarové nástroje“ a „Jiné možnosti zpřístupnění paměti RAM“.

5.3.3 Počítač se nachází ve vypnutém stavu

V tomto případě je nutné se skutečně přesvědčit, jestli daný počítač/notebook není pouze uspaný/hibernovaný (v tom případě by paměť RAM byla stále naplněna daty do doby než by se vybila baterie notebooku nebo než by se neodpojil počítač z elektrické sítě). Jedná se o vizuální kontrolu, jestli nebliká dioda, netočí se větráky a další. Pokud by se našla uspaná/hibernovaná stopa, dojde k jejímu spuštění a následně se postupuju podle postupů viz. výše (podle toho jestli je počítač chráněn přístupovým heslem a heslo známe nebo naopak).

Poznámka 1: Vše, co na zásahu dělá soudní znalec, stejně tak jako ostatní lidé provádějící zásah, je prováděno při přítomnosti nezúčastněné osoby (nebo i zájmové osoby), případně všechny postupy mohou být natáčeny na kameru.

Poznámka 2: Zásah = domovní prohlídka nebo prohlídka jiných prostor.

5.4 Hledání zašifrovaných dat a jejich následná analýza na předložených stopách

V následujícím textu je předpokládáno, že hledání zašifrovaných dat a jejich následná analýza bude probíhat u soudního znalce na forenzním počítači, na kterém je nainstalovaný speciální forenzní software potřebný pro analýzu šifrovaných dat:

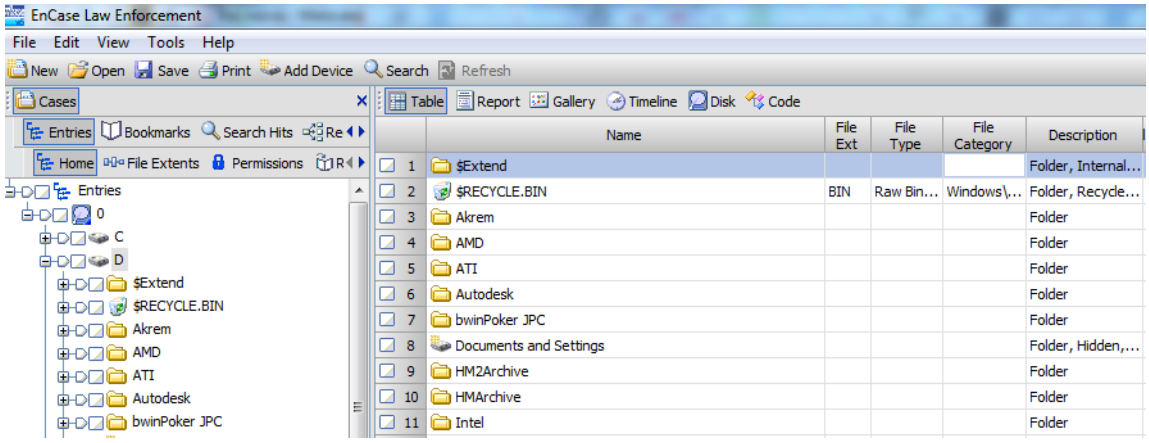
- základní software pro analýzu – EnCase, FTK, X-ways
- software pro analýzu paměti RAM – Volatility, WindowsSCOPE
- software pro získání informací ze zašifrovaných dat – Passware Forensic Kit, Elcomsoft Passware Recovery

5.4.1 Krok 1. – vytvoření bitové kopie

Po provedení prvotních úkonů s danou stopou (kontrola pečetí, rozbalení, nafocení) je vytvořena bitová kopie daného datového nosiče. Zkoumaný datový nosič (pevný disk) je zapotřebí vymontovat z dané stopy (notebook, stolní počítač, externí disk a další). Zde mohou nastat první komplikace – daný datový nosič nelze vymontovat ze zájmové stopy (týká se hlavně notebooků). Následuje dohodnutí s dožadujícím orgánem, aby bylo povoleno spuštění této stopy. Když máme toto potvrzení dojednáno, tak spustíme daný počítač a v BIOSu nastavíme prioritu bootování na námi použité zařízení pro provedení bitové kopie (USB nebo optická mechanika).

Obrázek 51: Nastavení priority pro bootování operačního systému v BIOSu.

Tento postup lze aplikovat pouze v tom případě, že BIOS není chráněn (heslo, PIN, otisk prstů a jiné). Pokud je BIOS chráněn a nemáme k němu příslušné heslo, tak existují metody jak toto heslo obejít/deaktivovat (použít resetující „jumper", speciální softwary na vyresetování hesla, vyndat CMOS baterii, vygenerování tzv. "defaultního" hesla, kontaktovat dodavatele základní desky). Následné vytvoření bitové kopie (ať již pomocí samotného zkoumaného počítače nebo připraveného forenzního počítače) se provede za pomoci operačního systému Linux, a to příkazem „dd" nebo „dcfldd". Po vytvoření je vždy nutné si bitovou kopii zkontrolovat, zdali obsahuje čitelná data. To provedeme načtením této kopie do jednoho z námi používaných softwarů – FTK Imager, EnCase nebo jiného. Pokud by kopie (vytvořená za pomoci forenzního počítače) neobsahovala čitelná data (ani jeden z diskových oddílů) může daný počítač obsahovat čip TPM (viz. kapitola TPM) a je nutné vytvořit novou bitovou kopii za pomoci samotného zkoumaného počítače (viz. popsáno výše).

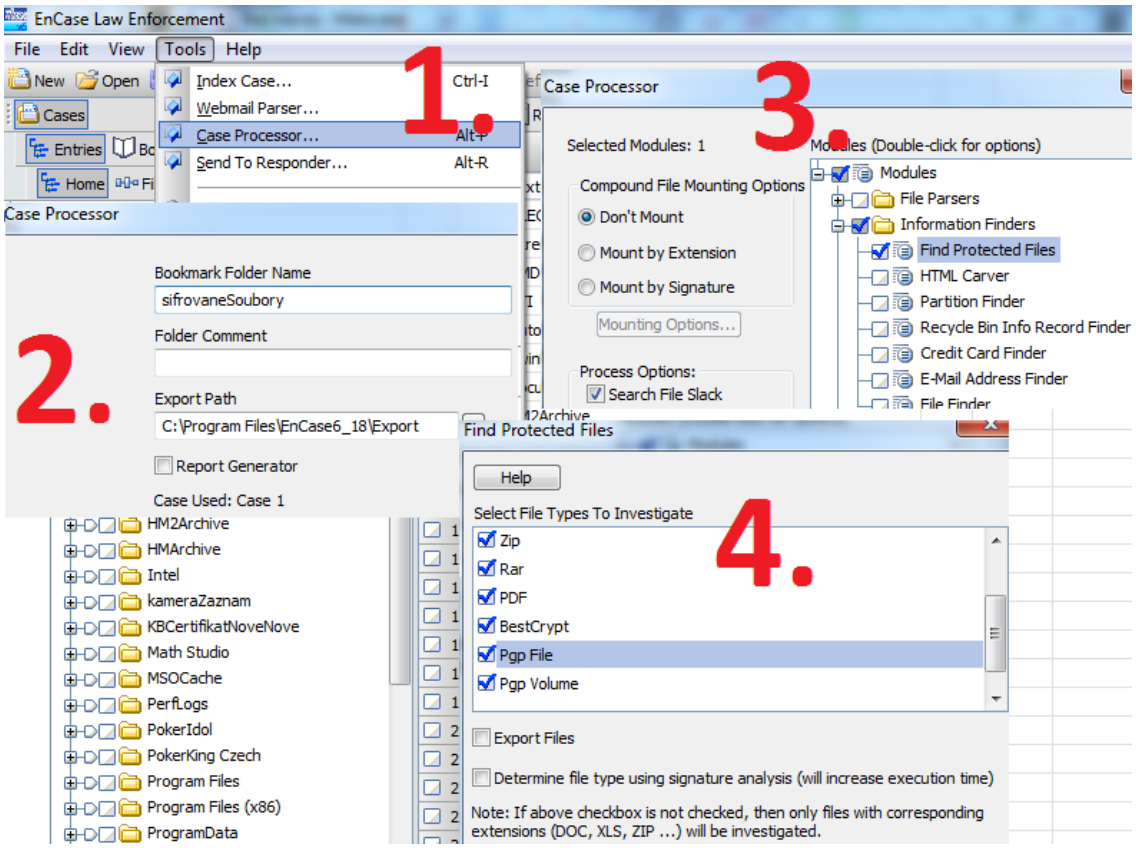


Obrázek 52: Načtená bitová kopie do forenzního programu EnCase 6.18 – viditelně čitelná data.

5.4.2 Krok 2. – vyhledání zašifrovaných dat - EnCase

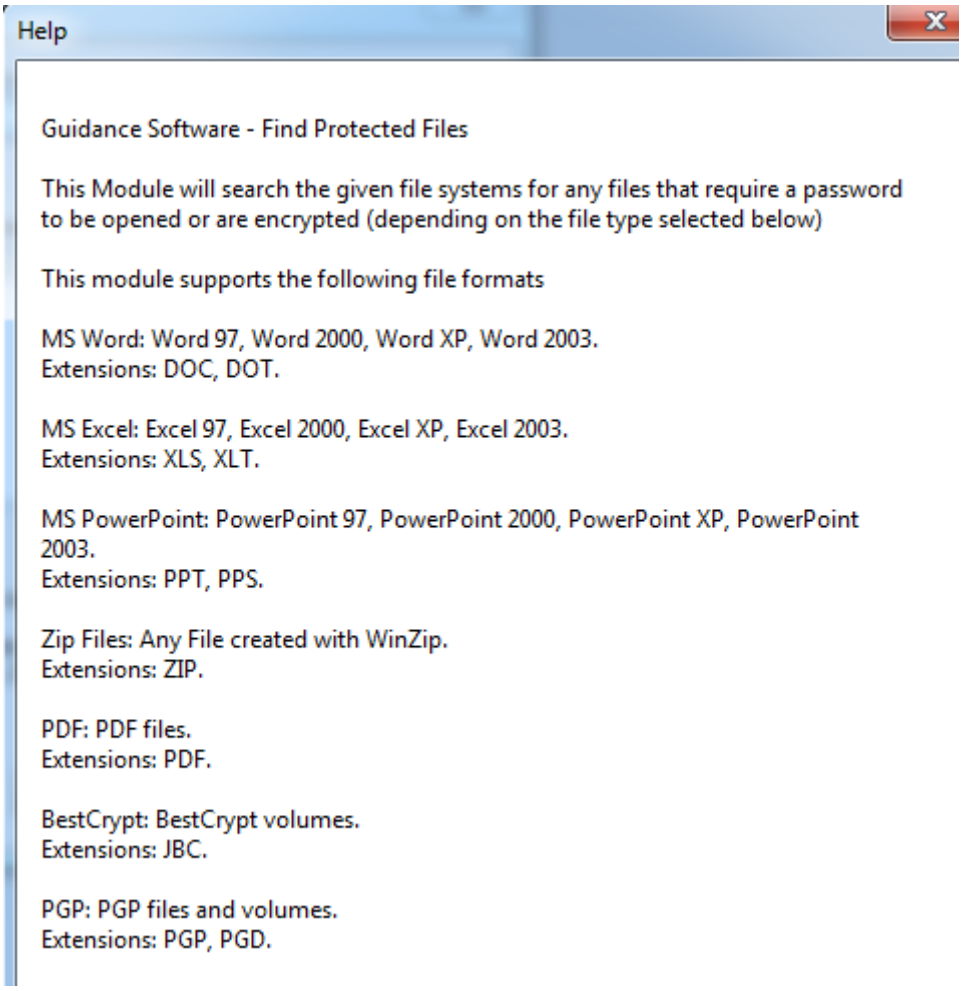
V tomto kroku se předpokládá, že máme vytvořenou funkční bitovou kopii. Tuto kopii načteme do forenzního programu EnCase a pak postupujeme podle následujících kroků:

a) pomocí nástroje „case procesor“ – zapneme možnost „find protected files“ a zaškrtneme všechny typy pro vyhledávání.



Obrázek 53: Použití nástroje „find protected files“ v programu EnCase.

Tento nástroj má velkou nevýhodu v tom, že podporuje málo druhů zašifrovaných dat. Podpora ve verzi EnCase 6.18:



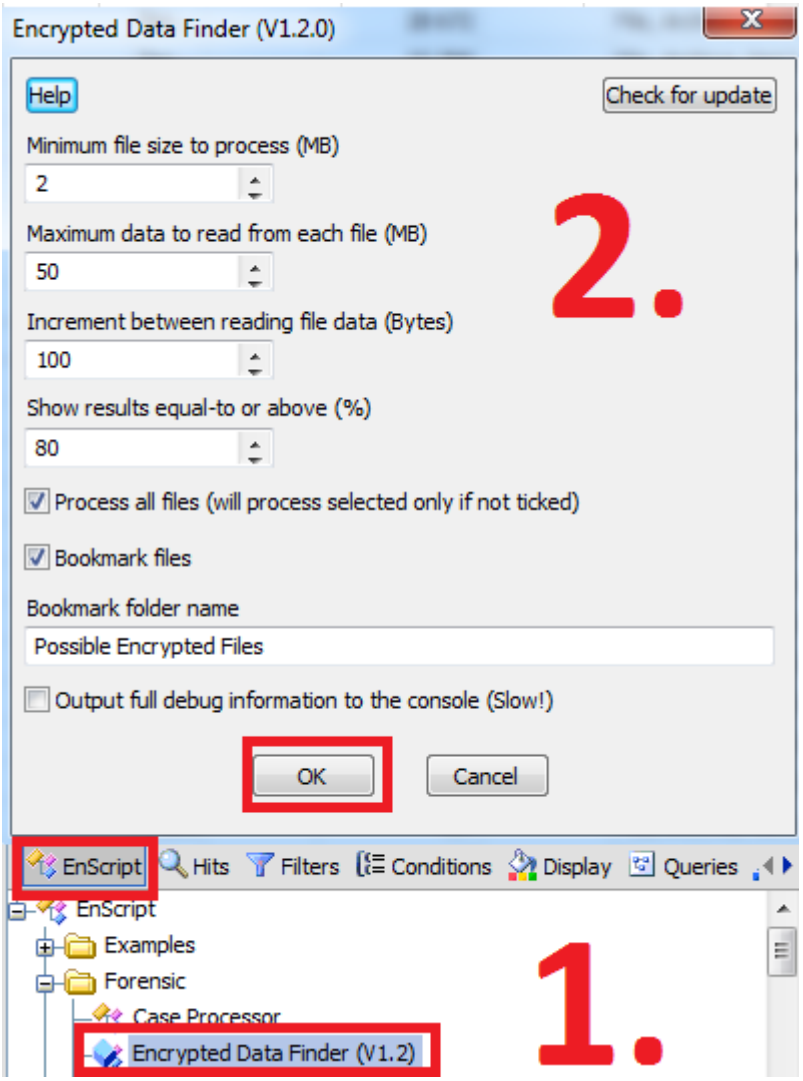
Obrázek 54: Podpora druhů zašifrovaných dat pro nástroj „Find Protected Files“ v programu EnCase 6.18.

Od verze EnCase 7 je do tohoto softwaru integrovaná funkce na vyhledávání zašifrovaných dat pomocí softwaru Passware Kit Forensic pojmenovaná „Passware's Encryption Analyzer“, a tak již odpadnou starosti s malou podporou pro šifrovaná data. A navíc ubyde jeden z kroků tohoto postupu na vyhledání zašifrovaných dat (krok 3 – hledání zašifrovaných dat za pomocí programu Passware Kit Forensic).

b) stáhnout a přidat skripty „Encrypted Data Finder v1.2“ a „TrueCrypt File Locator v2.2“

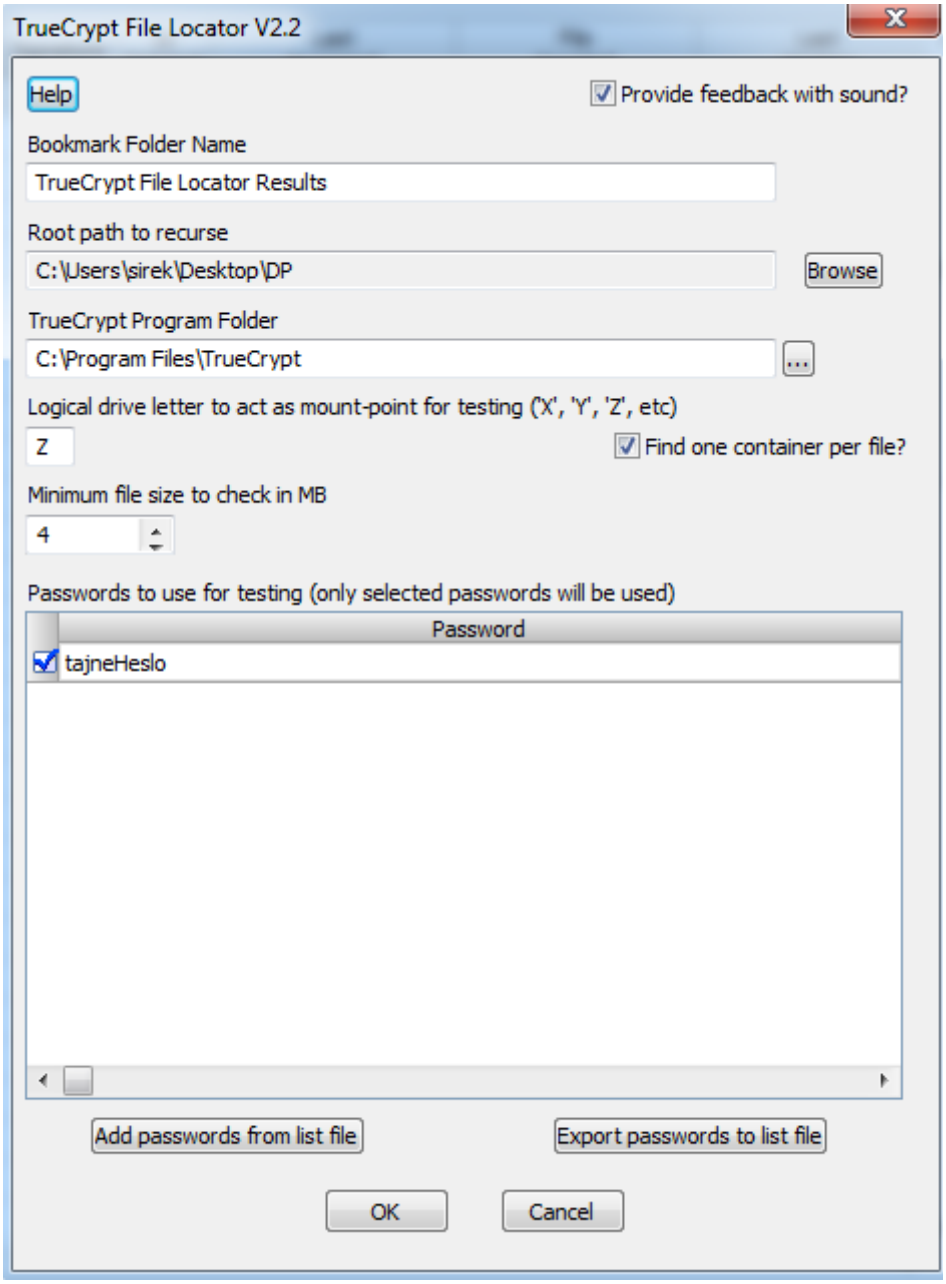
Jedná se o skripty napsané panem Simonem Keyem (vývojář ze společnosti Guidance Software). Nyní jsou pro majitele forenzního program EnCase (verze 7) k dispozici novější verze těchto skriptů, ale tyto verze jsou poslední kompatibilní s verzí EnCase 6:

- Encrypted Data Finder v1.2 – Tento skript se pokouší identifikovat zašifrovaná data a využívá jedné z vlastností zašifrovaných dat – data (soubor) obsahují velké množství náhodných bitů.



Obrázek 55: Využití skriptu „Encrypted Data Finder“ v programu EnCase pro nalezení zašifrovaných dat.

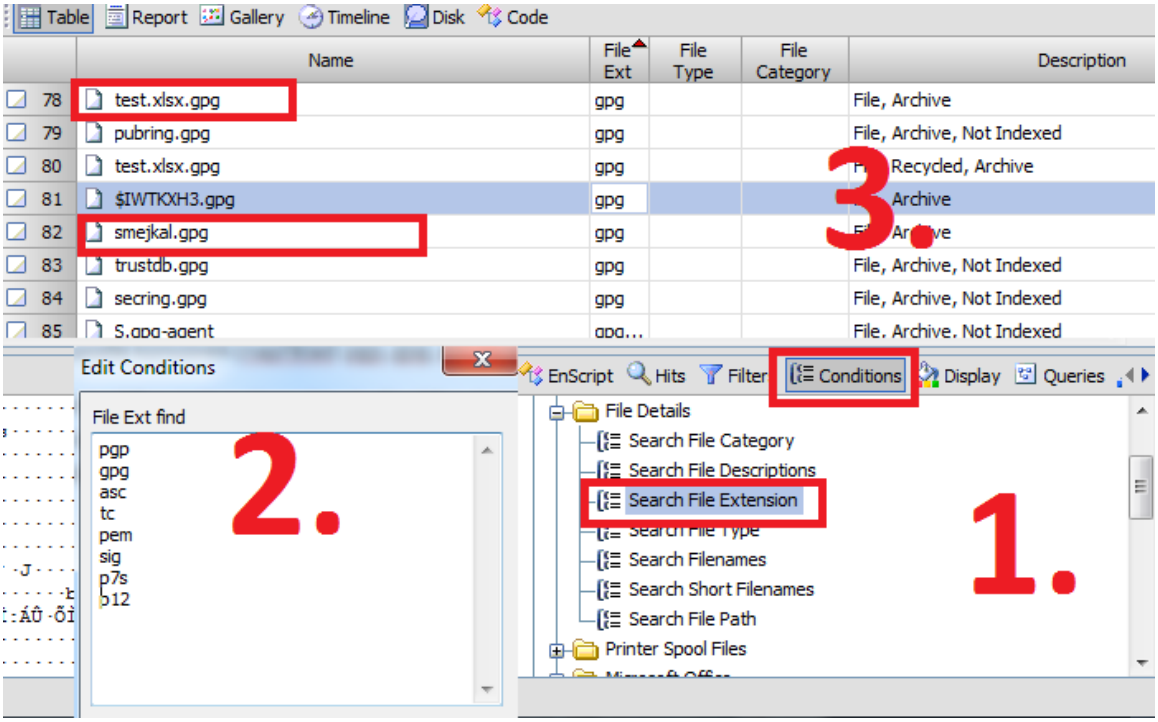
- TrueCrypt File Locator v2.2 – Tento skript hledá kontejnery vytvořené programem TrueCrypt.U tohoto skriptu je nutné nastavit lokaci, kde mají být teoreticky zašifrované soubory (kontejnery) uloženy a zadat přístupové heslo do tohoto kontejneru (pokud ho známe, nebo jestliže máme nalezená hesla do jiných aplikací). Skript následně zkouší vyhledat soubory větší než námi nastavená hodnota a připojovat je pomocí nastaveného hesla (nutné mít na forenzním počítači nainstalovaný program TrueCrypt).



Obrázek 56: Využití skriptu „TrueCrypt File Locator“ v programu EnCase pro nalezení zašifrovaných dat.

c) vyhledání souborů podle koncovek (například: pgp, gpg, asc, tc, pem, sig, p7s, p12 a další)

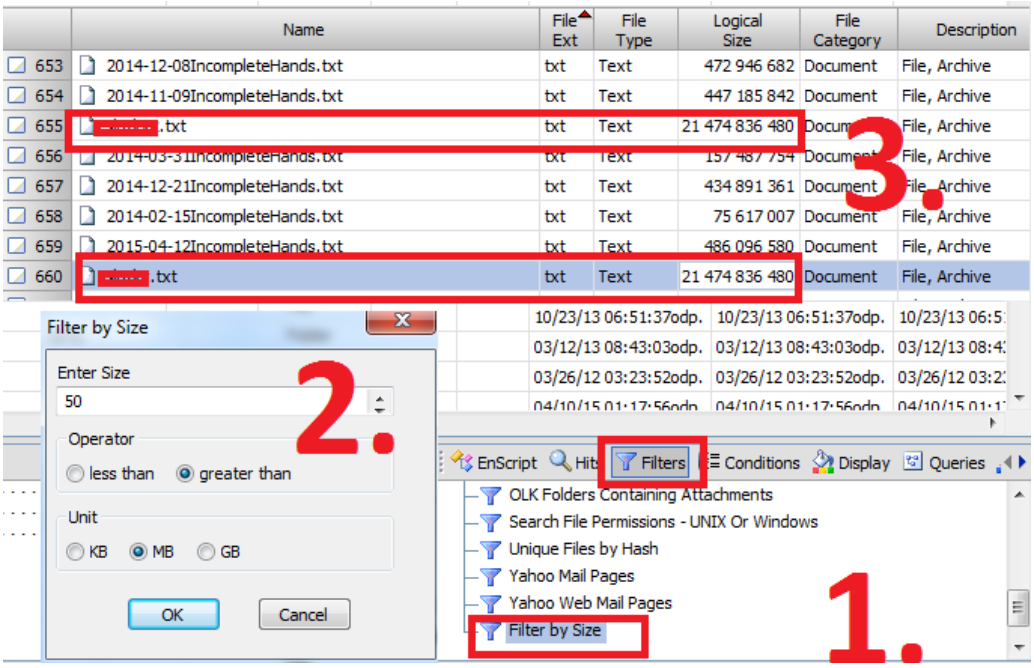
V tomto kroku jde o to nalézt zašifrované soubory, které při zašifrování dostanou přednastavenou koncovku (například soubory zašifrované pomocí programu Gpg4win dostanou koncovku gpg) a také vyhledat soukromé klíče.



Obrázek 57: Vyhledání zašifrovaných dat za pomocí koncovek – EnCase 6.18.

d) seřazení souborů podle velikosti

V tomto kroku jde o to nalézt zašifrované kontejnery, které se „skrývají“ za jinými typy souborů. Například soubory typu „xxxxx.txt“ nebo „xxxx.jpg“, větší jak 50 MB jsou podezřelé a je potřeba je analyzovat. Podobných výsledků lze také získat porovnáním shodnosti hlaviček jednotlivých souborů.



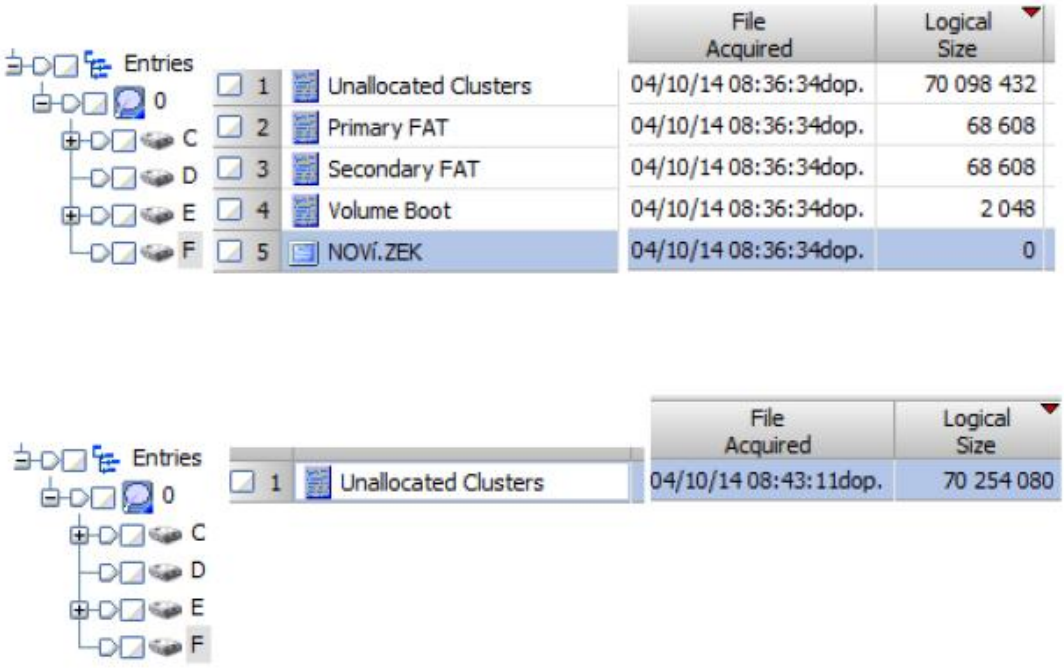
Obrázek 58: Vyhledání zašifrovaných kontejnerů podle velikosti – EnCase 6.18.

e) analyzovat nainstalované programy

Tento krok je důležitý, protože v dnešní době existují desítky softwarů umožňujících nějakým způsobem šifrovat data, a tyto programy stále přibývají. A protože není možné všechny programy znát a vědět, jak přesně fungují, je důležité zanalyzovat nainstalované programy (programy obsahující v názvu slova jako: "crypt, pgp, security, encrypt" a další). Následně se pokusit u programů, které neznáme, zjistit co nejvíce podrobností k čemu slouží, a jak přesně fungují.

f) analyzovat jednotlivé diskové oddíly

Na obrázcích níže je vidět rozdíl mezi zašifrovaným oddílem (pomocí programu TrueCrypt) a prázdným oddílem (chybí název oddílu, tabulky FAT a další).



Obrázek 59: Porovnání prázdného diskového oddílu a zašifrovaného oddílu (dolní část obrázku).

5.4.3 Krok 3. - hledání zašifrovaných dat - Passware Kit Forensic

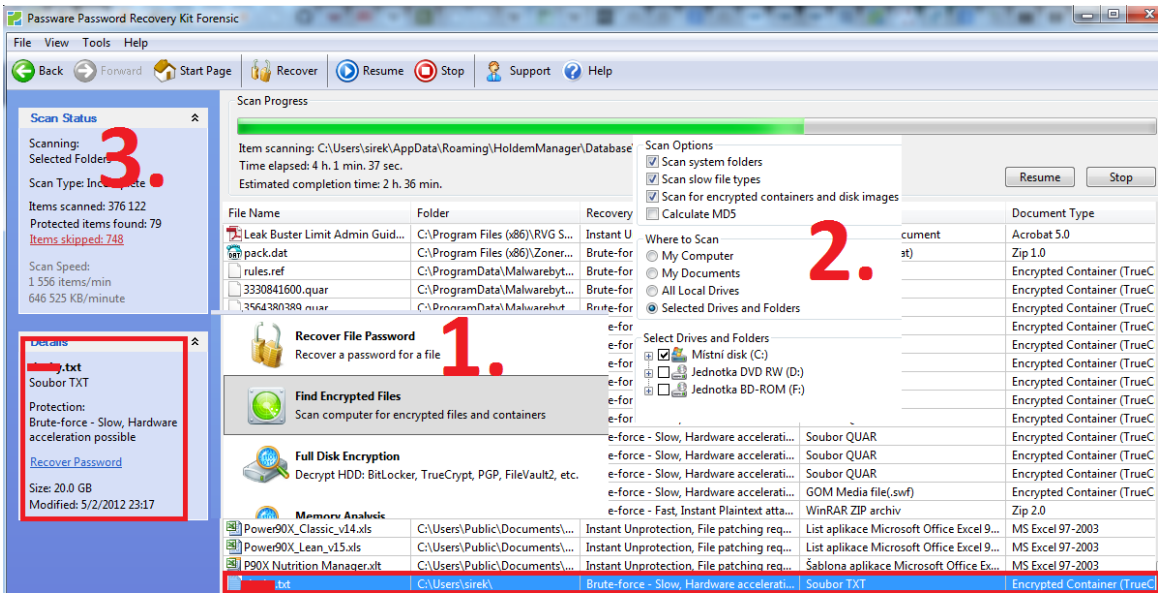
Pro využití tohoto programu a jeho funkce „**Find Encrypted Files**" (verze programu 2015 v2) je zapotřebí připojit (načíst) předloženou bitovou kopii do operačního systému (vzniknou nové diskové oddíly) za pomoci speciálního softwaru (například FTK Imager).

Vlastnosti funkce „Find Encrypted Files":

- velice rychlé prohledávání souborů – až 4000 soborů za minutu

- rozpoznává přes 200 druhů zašifrovaných souborů
- detekuje zašifrované kontejnery a zašifrované oddíly (pouze u verze Professional)
- detailní informace o nalezených datech
- možnost vytvoření kontrolní MD5 sumy (pouze u verze Professional)
- možnost vyhledávat zašifrovaná data na síťových discích (pouze u verze Professional)
- možnost spustit tento program z flashdisku bez nutnosti instalace (pouze u verze Professional)

Tato funkce je součástí nástroje Passware Kit nebo je také možné tuto funkci (program – Encryption Analyzer) koupit samostatně. Tohoto programu jsou k dispozici dvě verze: Free (zdarma), Professional (295$), rozdíly mezi těmito verzemi jsou popsány výše ve vlastnostech této funkce.



Obrázek 60: Použití funkce „Find Encrypted Files“ pro vyhledání zašifrovaných dat v programu Passware Kit Forensic.

A dále je u tohoto programu také funkce „**System & Registry**“, která umožňuje vyhledat hesla z registrů – nejdříve je možné zjistit heslo do operačního systému, to je možné zkoušet pomocí několika druhů útoku (nebo heslo znát nebo zjistit jiným softwarem/útokem). A poté tato funkce umožňuje plnohodnotně obnovit hesla uložená ve webových prohlížečích, internetových připojeních, e-mailových klientů, IM…

Alternativou pro tyto funkce jsou opět jednotlivé programy pro obnovu hesel z webových stránek: „www.nirsoft.net“. Tyto programy jsou zcela zdarma.

Poznámka: Pro ukázky v této práci je využit program EnCase verze 6.18.

5.4.4 Krok 4. - virtualizace

Někdy se využívá ještě **krok číslo 4**, a to virtualizování operačního systému a následné zkoumání na takto „živém“systému. Jedná se o náhradu toho, když není možné danou stopu spustit (nedostane se povolení od dožadujícího orgánu). Po spuštění nebo virtualizování by následovalo použití programu Passware Kit Forensic a jeho funkce „**internet & network**“ nebo programu multi password recovery (tento program je popisován více v kapitole „Správné získání kriminalistické stopy (výpočetní techniky) - Zajištění dat na zájmových stopách před jejich zapečetění – krok číslo 4“).

Těmito třemi (čtyřmi) kroky hledáme co největší množství zašifrovaných dat a uložených hesel, které se na daných stopách nalézají. Z takto nalezených hesel se vytváří slovník pro danou stopu (celý případ), který se poté používá k dešifrování dalších dat. Nalezená zašifrovaná data jsou vykopírována (v případě souborů) nebo poznamenána (v případě zašifrování celých disků nebo oddílů) a jsou následně dešifrována za pomoci speciálních dešifrovacích softwarů (Passware Forensic Kit, Elcomsoft Recovery Bundle…).

5.5 Analýza bitové kopie paměti RAM a dalších systémových souborů

Tato analýza je prováděna opět soudním znalcem na forenzním počítači a těmito systémovými soubory jsou myšleny soubory: „hiberfil.sys“, „pagefile.sys“ a „crash dump soubory“. Tyto systémové soubory jsou využívány k analýze, pokud není k dispozici záloha paměti RAM a je k dispozici jeden z těchto systémových souborů (možnost vykopírovat tyto soubory na zásahu nebo při následné analýze zájmové stopy). Pro tuto analýzu se používají následující softwary:

- Volatility
- Passware Kit Forensic
- Elcomsoft Recovery Bundle

Jak již bylo zmíněno výše, analýzou paměti je možné získat informace, jako jsou: spuštěné procesy, načtené ovladače, informace o socketech, **hesla,** konfigurační informace, informace o přihlášených uživatelích, **zašifrované soubory**, otevřené soubory, neuložené dokumenty, VOIP volání, **šifrovací klíče** a mnohé další.

5.5.1 Analýza RAM – Volatility 2.4

Analýza pomocí softwaru Volatility může být například provedena podle následujících kroků (program volatility se spouští z příkazové řádky – spustit jako správce):

1. příkaz „imageinfo“ – získání základních informací o zájmové kopii – zjištění, jaký operační systém byl spuštěn na zájmovém počítači při vytváření kopie

příkaz: *volatility-2.4.standalone.exe -f „cesta k bitové kopii RAM“ imageinfo*

```
C:\>volatility-2.4.standalone.exe -f E:\DP\zalohaRAM\PC1\belkasoft\20150127.mem
imageinfo
Volatility Foundation Volatility Framework 2.4
Determining profile based on KDBG search...

          Suggested Profile(s) : Win7SP0x86, Win7SP1x86
                     AS Layer1 : IA32PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (E:\DP\zalohaRAM\PC1\belkasoft
\20150127.mem)
                      PAE type : No PAE
                           DTB : 0x185000L
                          KDBG : 0x82d6cc28L
          Number of Processors : 2
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x82d6dc00L
                KPCR for CPU 1 : 0x80dc2000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2015-01-27 10:55:22 UTC+0000
     Image local date and time : 2015-01-27 11:55:22 +0100
```

Obrázek 61: Využití softwaru Volatility k analýze paměti RAM – příkaz „imageinfo“.

2. příkaz „pslist“ – vypsání aktivních procesů

příkaz: *volatility-2.4.standalone.exe -f „cesta k bitové kopii RAM“ --profile=Win7SP1x86 pslist*

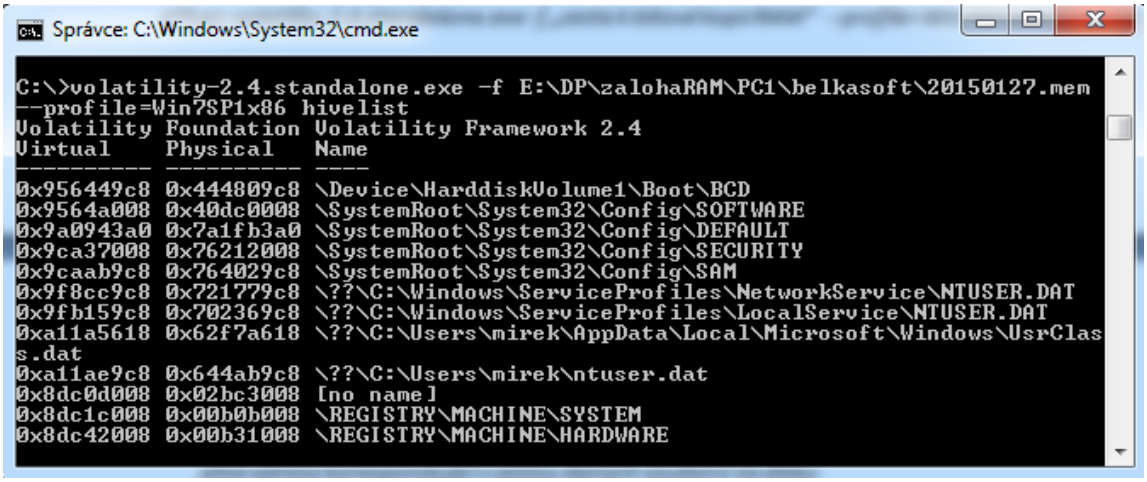
Poznámka: Od tohoto příkazu se již používá syntaxe „--profile“ se zadaným profilem operačního systému, který jsme zjistili z předešlého příkazu.

3. příkaz „timeliner“ – vypsání procesů spolu s časy spuštění

příkaz: *volatility-2.4.standalone.exe -f „cesta k bitové kopii RAM“ --profile=Win7SP1x86 timeliner*

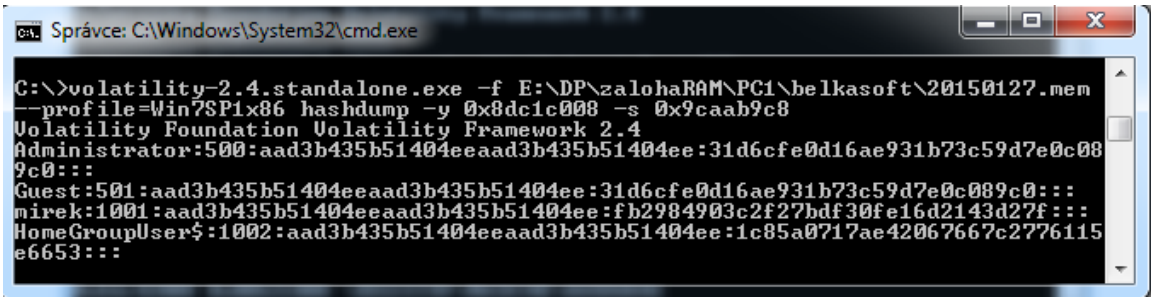
4. příkaz „hivelist“ – lokalizace registrů a zobrazení jejich virtuálních adres, fyzických adres a plných adres korespondujících s cestami daných souborů na disku

příkaz: *volatility-2.4.standalone.exe -f „cesta k bitové kopii RAM“ --profile=Win7SP1x86 hivelist*



Obrázek 62: Využití softwaru Volatility k analýze paměti RAM – příkaz „hivelist“.

5. příkaz „hashdump“ – extrahování hashí s přístupovými hesly do operačního systému Microsoft Windows



Obrázek 63: Využití softwaru Volatility k analýze paměti RAM – příkaz „hashdump“.

příkaz: *volatility-2.4.standalone.exe -f „cesta k bitové kopii RAM“ --profile=Win7SP1x86 hashdump -y 0x8dc1c008 -s 0x9caab9c8*

Poznámka 1 : syntaxe „-y“ označuje virtuální adresu souboru SYSTEM a syntaxe „s“ označuje virtuální adresu souboruSAM.

Poznámka 2: tyto hashe se následně dají použít k vyhledání hesla pomocí specializovaných softwarů.

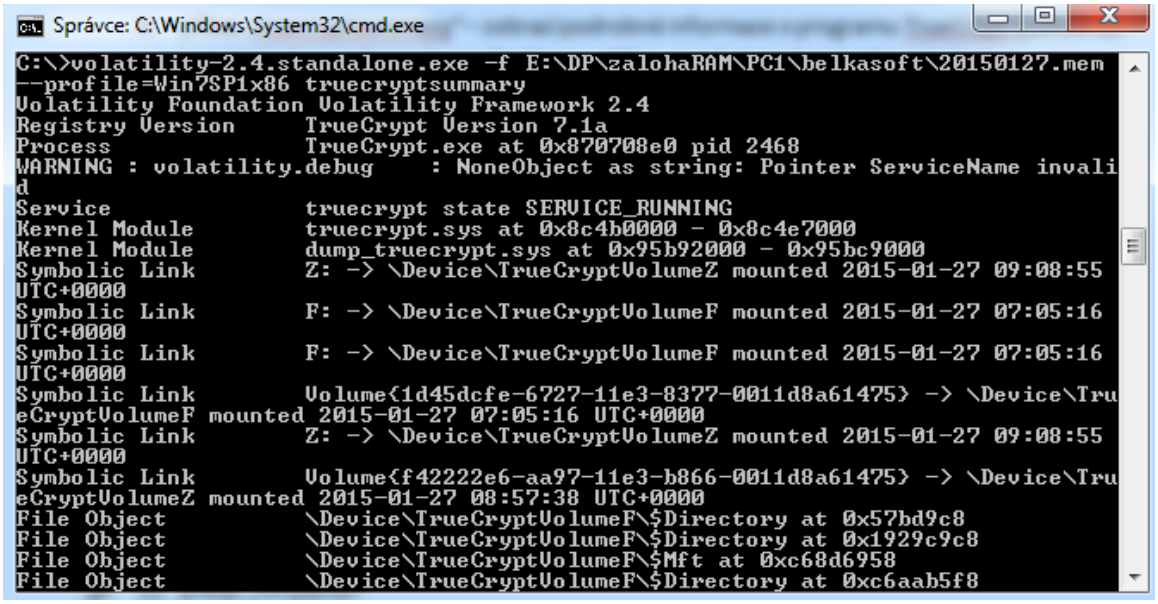
6. příkaz „bioskbd“ – vyčte stisknuté klávesy z části paměti určené pro BIOS – může obsahovat hesla do BIOSu nebo pro přístup do zašifrovaných celých disků

příkaz: *volatility-2.4.standalone.exe -f „cesta k bitové kopii RAM“ --profile=Win7SP1x86 bioskbd*

7. příkaz „truecryptpassphrase“ - vyhledává, jestli je v kopii RAM uloženo heslo do zašifrovaných dat vytvořených programem TrueCrypt v nezašifrované podobě

příkaz: *volatility-2.4.standalone.exe -f „cesta k bitové kopii RAM“ --profile=Win7SP1x86 truecryptpassphrase*

8. příkaz „truecryptsummary“ – zobrazí podrobné informace o programu TrueCrypt (pokud byl nainstalován na zájmovém počítači) a o zašifrovaných datech vytvořených tímto programem



Obrázek 64: Využití softwaru Volatility k analýze paměti RAM – příkaz „truecryptsummary“.

příkaz: *volatility-2.4.standalone.exe -f „cesta k bitové kopii RAM“ --profile=Win7SP1x86 truecryptsummary*

9. příkaz „truecryptmaster“ – vyhledá a zobrazí „master key“ využitý programem TrueCrypt 7.1a pro šifrování dat

příkaz: *volatility-2.4.standalone.exe -f „cesta k bitové kopii RAM“ --profile=Win7SP1x86 truecryptmaster*

10. příkaz „devicetree“ – ukáže vztahy mezi ovladači a jejich zařízeními – například ukáže, na jakých diskových jednotkách jsou přimountovány zašifrované kontejnery vytvořené programem TrueCrypt

příkaz: *volatility-2.4.standalone.exe -f „cesta k bitové kopii RAM“ --profile=Win7SP1x86 devicetree*

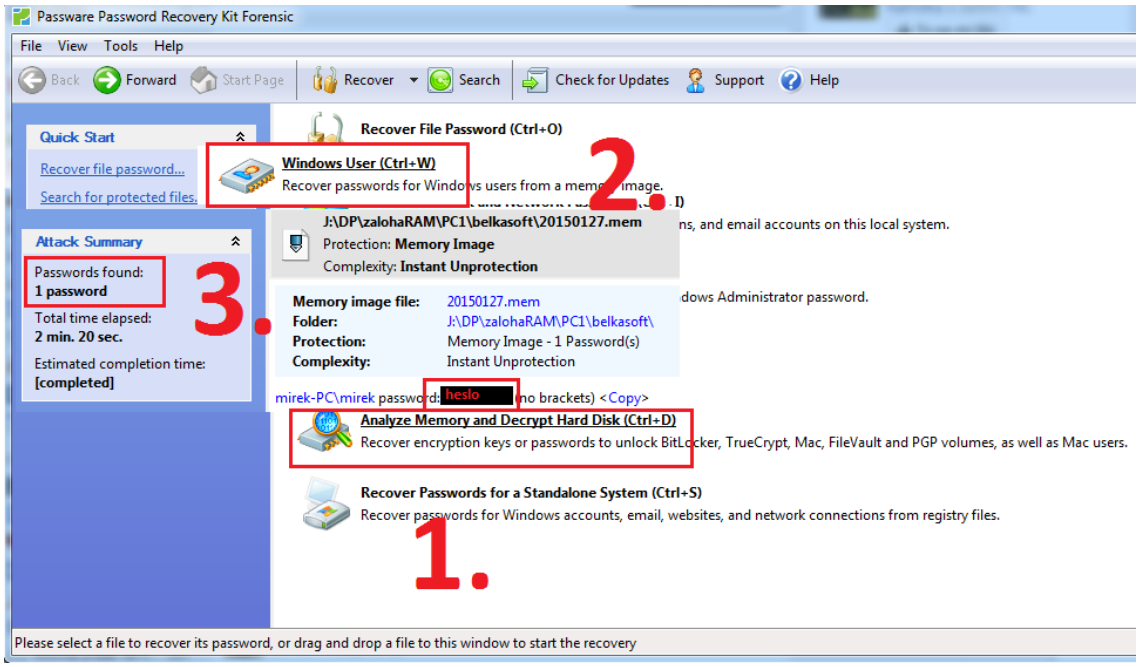
11. příkaz „mftparser“ – rekonstruuje tabulku „MFT“ – například je zde vidět celá cesta k nainstalovanému programu TrueCrypt a souboru „configuration.xml“, který obsahuje informace o posledních připojených zašifrovaných kontejnerech

příkaz: *volatility-2.4.standalone.exe -f „cesta k bitové kopii RAM“ --profile=Win7SP1x86 mftparser*

5.5.2 Analýza RAM – Passware Forensic Kit

Analýza bitové paměti RAM nebo systémových souborů pomocí softwaru Passware Forensic Kit probíhá zcela automaticky. Programu stačí pouze nastavit, jaký soubor má analyzovat (podporuje bitové kopie paměti RAM, soubory: hiberfil.sys a pagefile.sys) a následně vybrat jaký typ dat hledáme.

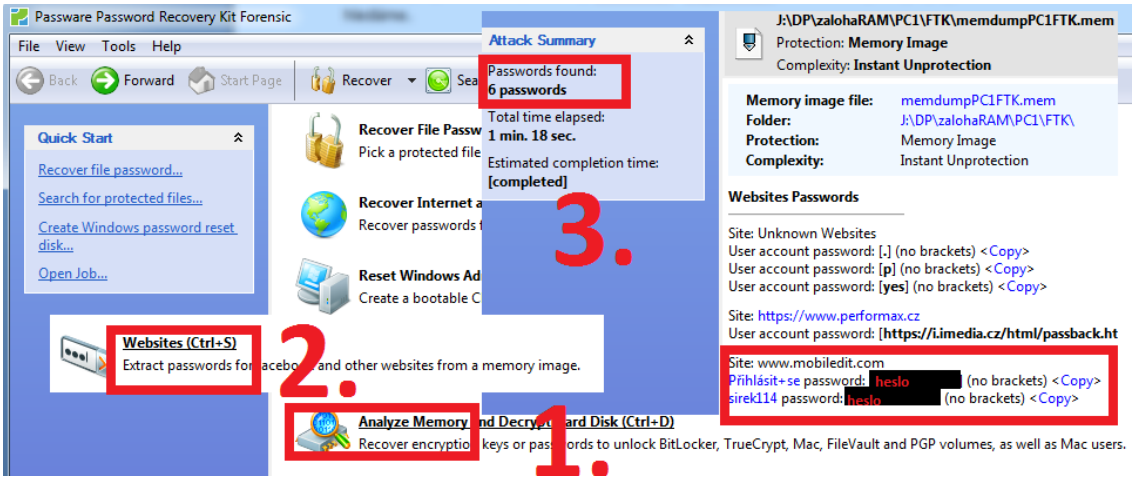
1. vyhledání přístupových hesel do operačního systému Microsoft Windows



Obrázek 65: Vyhledání přístupových hesel do operačního systému pomocí programu Passware Forensic Kit.

Poznámka: Tímto způsobem dojde k vyhledání hesel pouze k aktuálně přihlášeným uživatelům v průběhu vytváření bitové kopie paměti RAM.

2. vyhledání hesel z webových prohlížečů



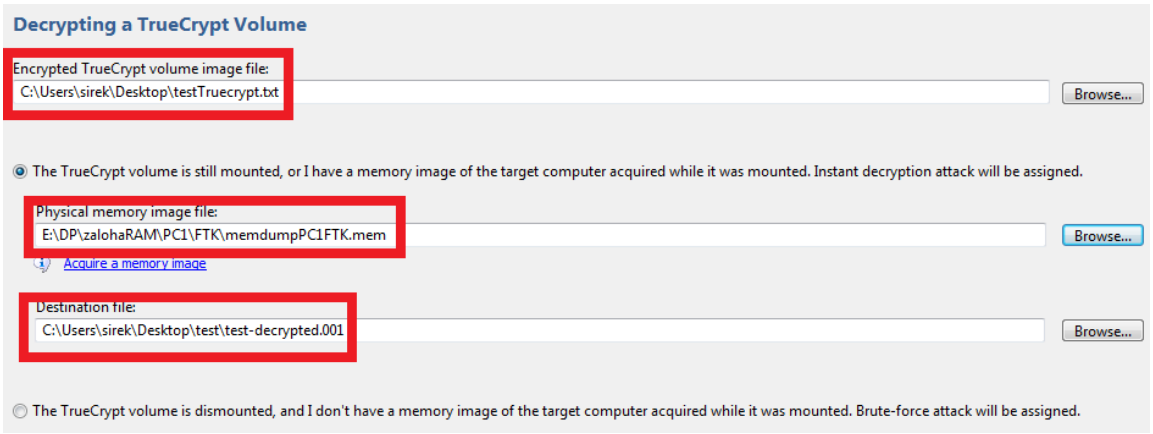
Obrázek 66: Vyhledání hesel z webových prohlížečů za pomoci programu Passware Forensic Kit.

3. hledání přístupu do zašifrovaných dat

Jedná se o způsob dešifrování zašifrovaných dat, pokud máme k dispozici kopii paměti RAM (nebo soubor pagefile.sys, hiberfil.sys), vytvořenou (vykopírovanou) v době, kdy byla zašifrovaná data aktivní (přimountovaná).

Podporované typy zašifrovaných dat podle programů, které byly použity na jejich vytvoření:

- BitLocker
- TrueCrypt
- PGP WDE
- Apple Disk Image
- FileVault



Obrázek 67: Dešifrování kontejneru (TrueCrypt) pomocí bitové kopie paměti RAM – Passware Forensic Kit.

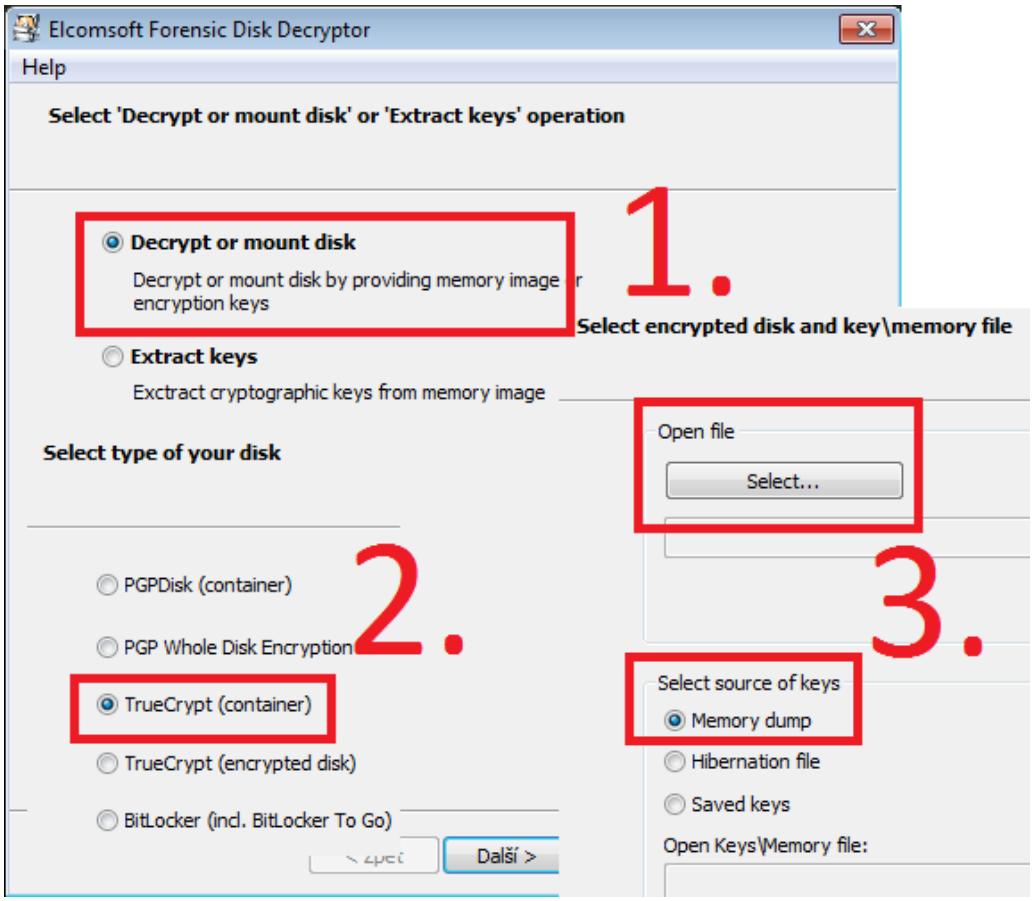
5.5.3 Analýza RAM – Elcomsoft Recovery Bundle

Analýza bitové paměti RAM nebo systémových souborů pomocí softwarového balíku Passware Forensic Kit probíhá za pomoci programu Elcomsoft Forensic Disk Decryptor (tento program je součástí balíku nebo lze samostatně zakoupit za 299EUR). V programu je zapotřebí nastavit, jaký soubor má být analyzován (podporuje bitové kopie paměti RAM, soubory: hiberfil.sys a pagefile.sys) a následně vybrat jaký typ dat hledáme.

Jedná se opět o způsob dešifrování zašifrovaných dat, pokud máme k dispozici kopii paměti RAM (nebo soubor pagefile.sys, hiberfil.sys), vytvořenou (vykopírovanou) v době, kdy byla zašifrovaná data aktivní (přimountovaná).

Podporované typy zašifrovaných dat podle programů, které byly použity na jejich vytvoření:

- BitLocker
- TrueCrypt
- PGP WDE



Obrázek 68: Dešifrování zašifrovaného kontejneru (TrueCrypt) za pomoci programu Elcomsoft Forensic Disk Decryptor.

6 POROVNÁNÍ RYCHLOSTÍ ZÍSKÁVÁNÍ HESEL ZA POMOCI DEŠIFROVACÍCH SOFTWARŮ

Testování probíhalo na forenzním stolním počítači skládajícího se z následujících komponent:

- základní deska: Asus Rampage IV Formula
- procesor: Intel Core i7-3970X Extreme
- grafická karta: 2x NVIDIA GeForce GTX Titan
- paměť RAM: 4x 8GB Kingston DDR3
- operační systém: Microsoft Windows 7 Professional SP1 64-bitová verze

Pro dešifrování byly použity forenzní dešifrovací softwary:

- Elcomsoft Distributed Password Recovery (dále značeno jako „Elcomsoft“)
  - Verze: 2.99 build 485
- Passware Kit Forensic (dále značeno jako „Passware“)
  - Verze: 13.7 64-bitová
- Extreme GPU Bruteforcer (dále značeno jako „EGB“)
  - Verze: 3.2
- oclHashcat (dále značeno jako „oclHashcat“)
  - Verze: 1.36

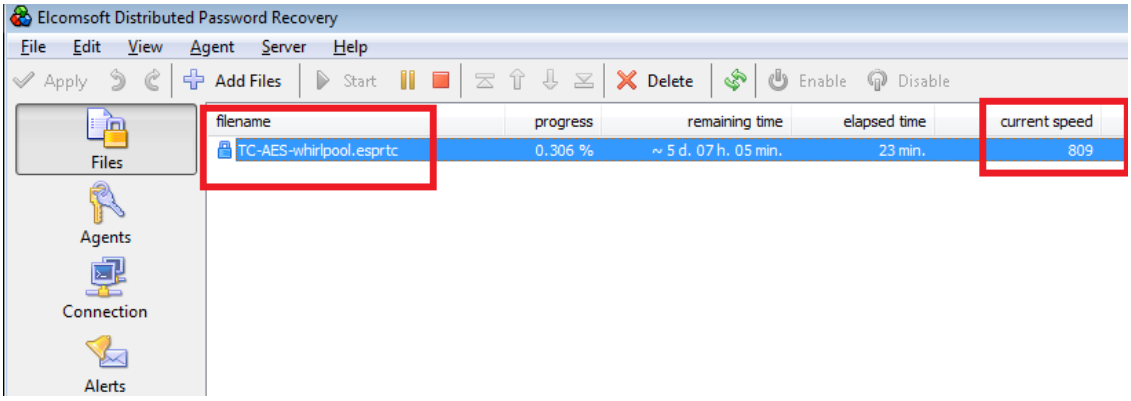
Poznámka 1: Rychlost hledání hesel je vždy udávána v hodnotách počtu hesel vyzkoušených za sekundu.

Poznámka 2: Dešifrování za pomoci daných softwarů bylo vždy necháno puštěné minimálně 5 minut, aby se rychlost dostatečně ustálila.

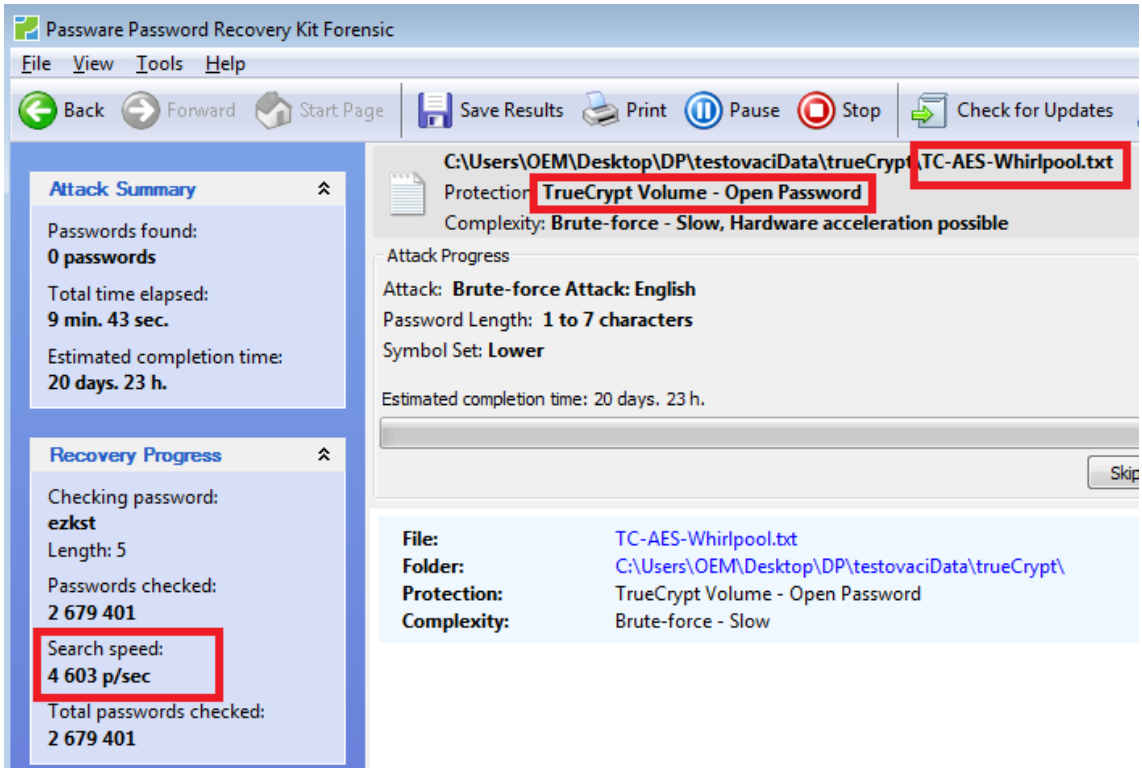
Poznámka 3:

- *První tabulka – jedná se o tabulku se základními informacemi o daných šifrovaných datech – název souboru, použitý program při šifrování daných dat a typ šifrování pokud je znám.*
- *Druhá tabulka – tato tabulka porovnává rychlosti hledání hesel pomocí daných programů a popisuje tato data: dešifrovací program – ukazuje jaký z programů byl použit (podrobnější informace o jednotlivých programech viz. kapitoly výše), typ útoku – udává jaký typ útoku byl při testování použit, rychlost hledání hesel – tato hodnota ukazuje rychlost zkoušení hesel za jednu sekundu, použití GPU – udává jestli daný program při konkrétním útoku využívá k hledání hesel grafické karty. Data označená červeně jsou ta, která u konkrétního útoku na konkrétních datech jsou rychlejší – vítězná v porovnávání s dalším softwarem. A tato vítězná hodnota (rychlost hledání hesel) je dále použita pro výpočet ve třetí tabulce.*

- *Třetí tabulka ukazuje počet dní potřebných k vyhledání hesla v závislosti na použití délky hesla a využití znakové sady (26 – malá písmena bez diakritiky, 36 – malá písmena bez diakritiky a číslice, 52 – malá a velká písmena bez diakritiky, 62 – malá a velká písmena bez diakritiky a číslice, 96 – veškerá znaková sada). Červená čísla zvýrazňují čas, kdy hledání hesla nepřesáhne 1 měsíc (obecně heslo bude dlouhodobě vyhledáno za půlku této vypočítané časové jednotky – protože někdy bude heslo nalezeno na začátku hledání, někdy uprostřed a někdy na konci…).*



Obrázek 69: Vyhledávání hesla pomocí útoku hrubou silou prostřednictvím softwaru Elcomsoft Password Recovery –TrueCrypt kontejner.



Obrázek 70: Vyhledávání hesla pomocí útoku hrubou silou prostřednictvím softwaru Passware Password Recovery Kit Forensic – TrueCrypt kontejner.

6.1 Microsoft Office

Microsoft Word 1997 a 2003

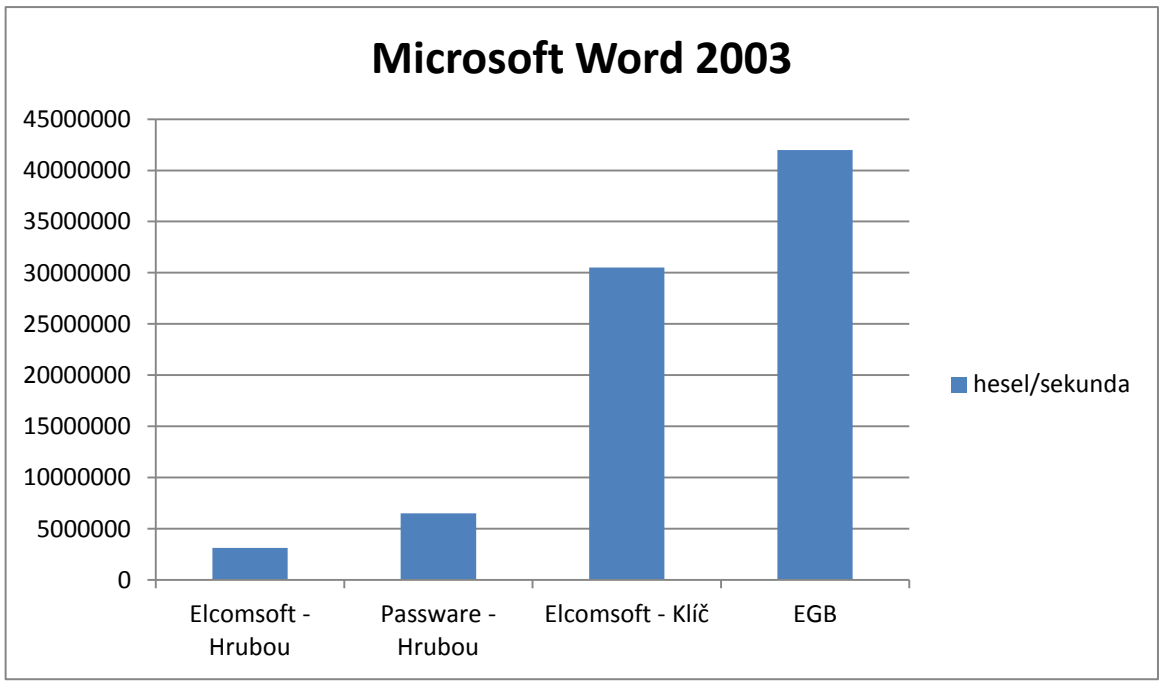
Tabulka 3: Základní informace o testovaném souboru – MS Office 2003.

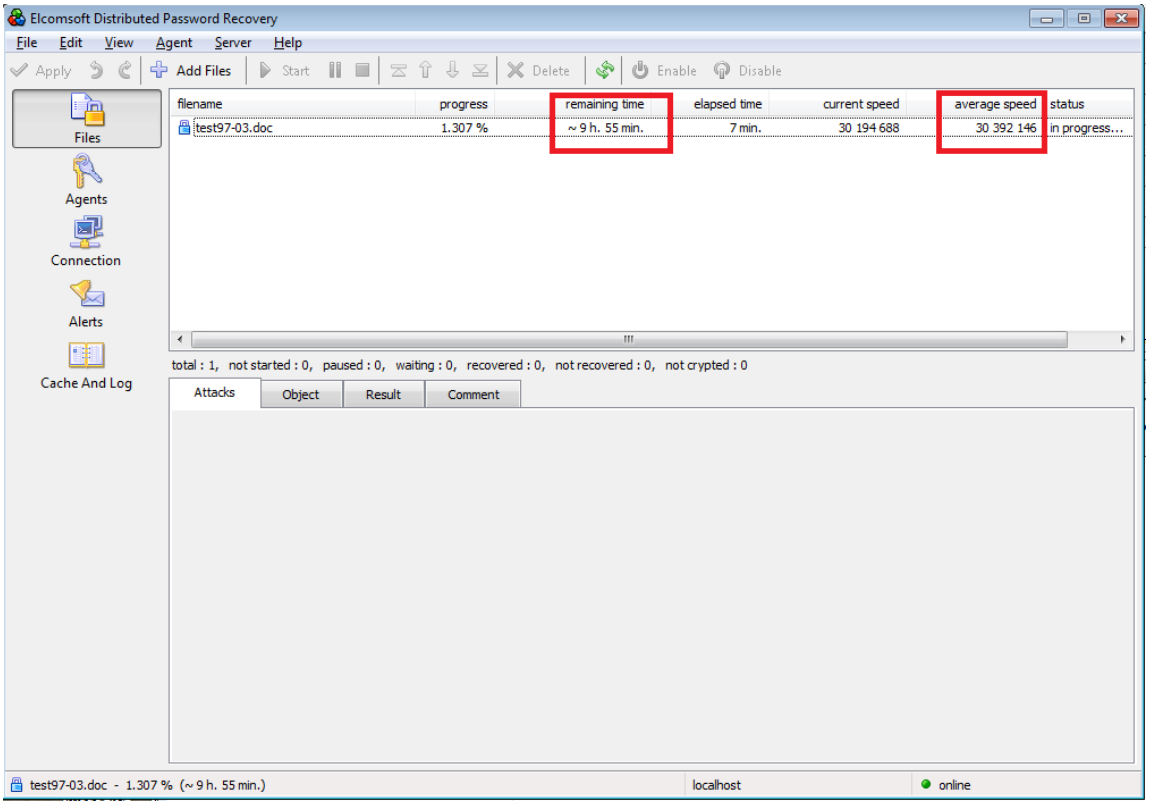
Název souboru:	Použitý program:	Typ šifrování:
Test97-03.doc	MS Office 2003	RC4 40-bitové

Tabulka 4: Porovnání rychlostí ve vyhledávání hesel pomocí daných programů a typů útoků – MS Office 2003.

Dešifrovací program:	Typ útoku:	Rychlost hledání hesel:	Použití GPU:
Elcomsoft	Hrubou silou	3,1 milionů	ne
Passware	Hrubou silou	6,5 milionů	ne
Elcomsoft	**Útok na klíč***	**30,5 milionů**	**ne**
EGB	**Hrubou silou**	**42 milionů**	**ano**

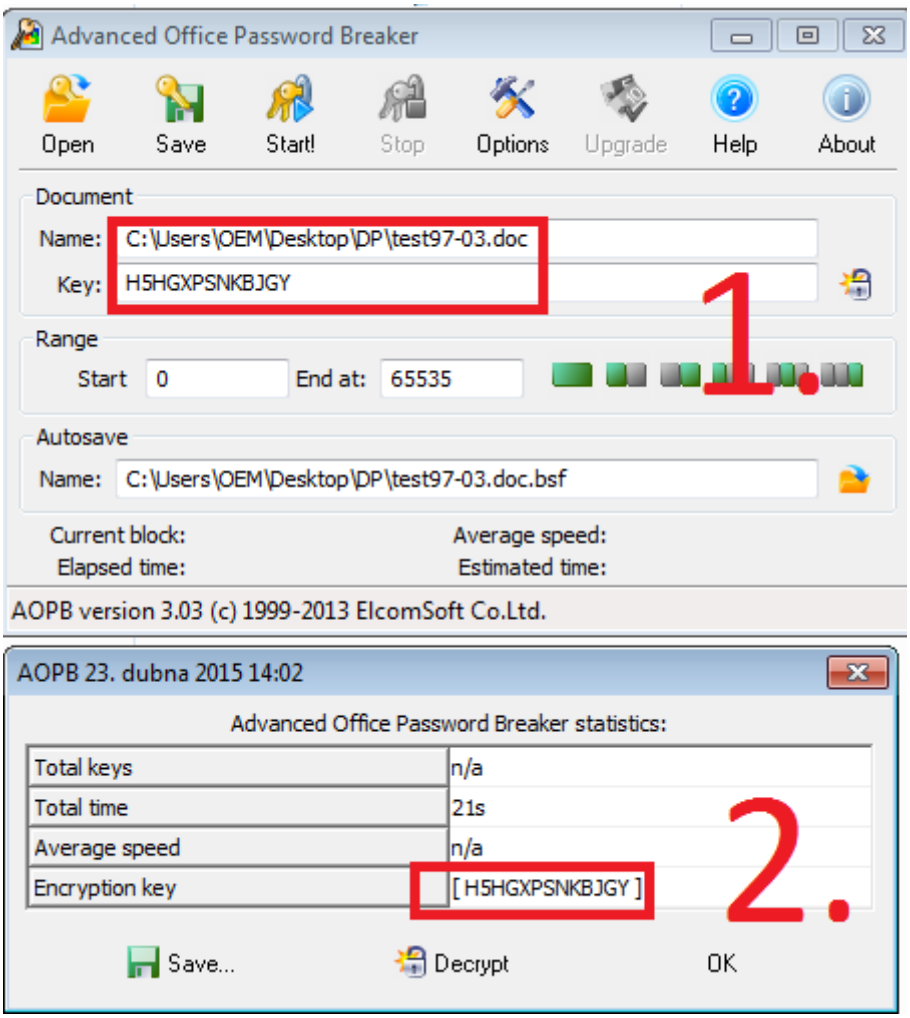
Poznámka: * Útok na klíč – garantované nalezení hesla – při této rychlosti – maximální doba nalezení hesla je přibližně 10 hodin.





Obrázek 71: Hledání hesla u zašifrovaného souboru typu MS Word 2003 za pomoci útoku na klíč prostřednictvím softwaru Elcomsoft.

U dokumentů kancelářského balíku Microsoft Office 1997 a 2003 je využito tak slabé šifrování, že existují speciální programy, které dokážou tento druh souboru otevřít během pár vteřin. Okamžitě nedojde k nalezení hesla jako takového, ale je umožněn přístup do souboru. Tento způsob umožňuje například software (je součástí balíku ElcomSoft Password Recovery Bundle) Advanced Office Password Breaker. Tento software využívá útok pomocí „rainbow tabulek“.



Obrázek 72: Okamžitý přístup do zašifrovaného souboru typu MS Word 2003 pomocí programu Advanced Office Password Breaker.

Tento druh útoku umožňuje také softwarový balík Passware Kit, ale podle stránek prodejce se pro tento druh útoku musí program připojit na stránky „www.decryptum.com“ a také je potřeba mít pro tento druh útoku extra kredity (u verze Forensic jich je 20 zdarma). Tento kredit lze dokoupit na stránkách prodejce. Pro dešifrování bez nutnosti se připojovat k internetu, lze zakoupit verzi “Decryptum Portable” za 1990$.

Tabulka 5: Počet dní potřebných k vyhledání hesla v závislosti na délce hesla a použité znakové sadě – MS Word 2003.

Znaková sada / délka hesla	26	36	52	62	96
5	0	0	0	0	0
6	0	0	0	0	0

7	0	0	0	0	20
8	0	0	14	60	1987
9	1	27	766	3730	190843
10	38	1007	39835	231288	18321005

Microsoft Word 2007

Tabulka 6: Základní informace o testovaném souboru – MS Office 2007.

Název souboru:	Použitý program:	Typ šifrování:
test2007.docx	MS Office 2007	RSA a AES 128-bitové

Tabulka 7: Porovnání rychlostí ve vyhledávání hesel pomocí daných programů a typů útoků – MS Office 2007.

Dešifrovací program:	Typ útoku:	Rychlost hledání hesel:	Použití GPU:
Elcomsoft	Hrubou silou	56 tis.	ano
Passware	Hrubou silou	69 tis.	ano
EGB	Hrubou silou	60 tisíc	ano

Tabulka 8: Počet dní potřebných k vyhledání hesla v závislosti na délce hesla a použité znakové sadě – MS Word 2007.

Znaková sada / délka hesla	26	36	52	62	96
5	0	0	0	0	1
6	0	0	3	9	131
7	1	13	172	590	12604
8	35	473	8967	36624	1210060
9	910	17035	466301	2270713	116165793

Microsoft Word 2010

Tabulka 9: Základní informace o testovaném souboru – MS Office 2010.

Název souboru:	Použitý program:	Typ šifrování:
test.docx	MS Office 2010	AES 128-bitové

Tabulka 10: Porovnání rychlostí ve vyhledávání hesel pomocí daných programů a typů útoků – MS Office 2010.

Dešifrovací program:	Typ útoku:	Rychlost hledání hesel:	Použití GPU:
Elcomsoft	Hrubou silou	28 tisís	ano
Passware	**Hrubou silou**	**34 tisíc**	**ano**
EGB	Hrubou silou	30 tisíc	ano

Tabulka 11: Počet dní potřebných k vyhledání hesla v závislosti na délce hesla a použité znakové sadě – MS Word 2010.

Znaková sada / délka hesla	26	36	52	62	96
5	**0**	**0**	**0**	**0**	**2**
6	**0**	**0**	**6**	**19**	266
7	**2**	**26**	349	1198	25580
8	71	960	18198	74326	2455710
9	1848	34572	946318	4608213	235748228

6.2 TrueCrypt

Tabulka 12: Základní informace o testovaném souboru – TrueCrypt (AES + RIPEMD).

Název souboru:	Použitý program:	Typ šifrování:
TC-AES-RIPEMD160.txt	TrueCrypt 7.1a	AES + RIPEMD 160-bitů

Tabulka 13: Porovnání rychlostí ve vyhledávání hesel pomocí daných programů a typů útoků – TrueCrypt (AES + RIPEMD).

Dešifrovací program:	Typ útoku:	Rychlost hledání hesel:	Použití GPU:
Elcomsoft	Hrubou silou	800*	ano
Passware	Hrubou silou	4,3 tisíc	ano
EGB	**Hrubou silou**	**132 tisíc**	**ano**

Tabulka 14: Počet dní potřebných k vyhledání hesla v závislosti na délce hesla a použité znakové sadě – TrueCrypt (AES + RIPEMD).

Znaková sada / délka hesla	26	36	52	62	96
5	**0**	**0**	**0**	**0**	**0**
6	**0**	**0**	**1**	**4**	68
7	**0**	**6**	90	308	6588
8	18	247	4687	19144	632531

Tabulka 15: Základní informace o testovaném souboru – TrueCrypt (AES + SHA512).

Název souboru:	Použitý program:	Typ šifrování:
TC-AES -SHA512.txt	TrueCrypt 7.1a	AES + SHA 512-bitů

Tabulka 16: Porovnání rychlostí ve vyhledávání hesel pomocí daných programů a typů útoků – TrueCrypt (AES + SHA512).

Dešifrovací program:	Typ útoku:	Rychlost hledání hesel:	Použití GPU:
Elcomsoft	Hrubou silou	800*	ano
Passware	Hrubou silou	4,3 tisíce	ano
EGB	**Hrubou silou**	**116 tisíc**	**ano**

Tabulka 17: Počet dní potřebných k vyhledání hesla v závislosti na délce hesla a použité znakové sadě – TrueCrypt (AES + SHA512).

Znaková sada / délka hesla	26	36	52	62	96
5	**0**	**0**	**0**	**0**	**0**
6	**0**	**0**	**1**	**5**	78
7	**0**	**7**	102	351	7497
8	20	281	5334	21785	719777

Tabulka 18: Základní informace o testovaném souboru – TrueCrypt (AES + Whirlpool).

Název souboru:	**Použitý program:**	**Typ šifrování:**
TC-AES-Whirlpool.txt	TrueCrypt 7.1a	AES + Whirlpool

Tabulka 19: Porovnání rychlostí ve vyhledávání hesel pomocí daných programů a typů útoků – TrueCrypt (AES + Whirlpool).

Dešifrovací program:	**Typ útoku:**	**Rychlost hledání hesel:**	**Použití GPU:**
Elcomsoft	Hrubou silou	800*	ano
Passware	**Hrubou silou**	**4,3 tisíce**	**ano**
EGB	nestabilní	nestabilní	nestabilní

Při použití dalších typů šifrovacích algoritmů jsou již rychlosti vyhledávání stejné a vyhledávání za pomocí programu EGB není zatím podporováno.

Tabulka 20: Počet dní potřebných k vyhledání hesla v závislosti na délce hesla a použité znakové sadě – TrueCrypt.

Znaková sada / délka hesla	26	36	52	62	96
5	0	0	0	2	21

6	0	5	53	152	2106
7	21	210	2767	9478	20262
8	562	7593	143894	587694	19417247

Poznámka: Jedná se o zašifrované kontejnery, kde nemáme k dispozici bitovou kopii paměti RAM nebo soubor hiberfil.sys (vytvořené v době aktivního připojení daného kontejneru).

*Poznámka: * - pro dešifrování těchto druhů dat za pomoci programu Elcomsoft Distributed Password Recovery je zapotřebí nejdříve použít nástroj "EDPR Disk Encryption Info" pro získání informací (v tomto nástroji je možné nastavit jaký druh šifrování je použit, pokud je znám, ale to není moc obvyklé, tak s touto variantou není počítáno – při pokusu bylo zjištěno, že se tím (nastavením druhu šifrování) docílí zrychlení asi o 1/3), které se následně uloží do souboru s koncovkou "esprtc" a již je lze dešifrovat pomocí tohoto program.*

6.3 Archivační soubory

Tabulka 21: Základní informace o testovaném souboru – WinRAR 4.01 – RAR – RAR 3.x – 4.x AES.

Název souboru:	Použitý program:	Typ šifrování:
testData.rar	WinRAR 4.01 32-bitová	RAR 3.x – 4.x - AES

Tabulka 22: Porovnání rychlostí ve vyhledávání hesel pomocí daných programů a typů útoků – WinRAR 4.01 – RAR – RAR 3.x – 4.x AES.

Dešifrovací program:	Typ útoku:	Rychlost hledání hesel:	Použití GPU:
Elcomsoft	Hrubou silou	24 tisíc	ano
Passware	Hrubou silou	32 tisíc	ano

Tabulka 23: Počet dní potřebných k vyhledání hesla v závislosti na délce hesla a použité znakové sadě – WinRAR 4.01 – RAR – RAR 3.x – 4.x AES.

Znaková sada / délka hesla	26	36	52	62	96

5	**0**	**0**	**0**	**0**	**2**
6	**0**	**0**	**7**	**20**	283
7	**2**	**28**	371	1273	27179
8	75	1020	19335	78971	2609192

Tabulka 24: Základní informace o testovaném souboru – WinRAR 4.01 – ZIP 2.0.

Název souboru:	**Použitý program:**	**Typ šifrování:**
testData.zip	WinRAR 4.01 32-bitová	ZIP 2.0

Tabulka 25: Porovnání rychlostí ve vyhledávání hesel pomocí daných programů a typů útoků – WinRAR 4.01 – ZIP 2.0.

Dešifrovací program:	**Typ útoku:**	**Rychlost hledání hesel:**	**Použití GPU:**
Elcomsoft	nepodporováno	nepodporováno	nepodporováno
Passware	**Hrubou silou**	**88 milionů**	**ne**
Elcomsoft-ARCHPR*	Hrubou silou	33 milionů	ne

Tabulka 26: Počet dní potřebných k vyhledání hesla v závislosti na délce hesla a použité znakové sadě – WinRAR 4.01 – ZIP 2.0.

Znaková sada / délka hesla	26	36	52	62	96
5	**0**	**0**	**0**	**0**	**0**
6	**0**	**0**	**0**	**0**	**0**
7	**0**	**0**	**0**	**0**	**9**
8	**0**	**0**	**7**	**28**	948
9	**0**	**13**	365	1780	91084
10	**18**	480	19012	110387	8744116

Poznámka: - pro dešifrování těchto druhů dat je zapotřebí použít software Advanced Archive Password Recovery (je součástí softwarového balíku Elcomsoft Recovery Bundle). Pro toto testování byla použita verze tohoto programu: 4.54 Professional Edition.*

Tabulka 27: Základní informace o testovaném souboru – WinRAR 5.21 – RAR 3.x – 4.x AES.

Název souboru:	**Použitý program:**	**Typ šifrování:**
testData5.rar	WinRAR 5.21 64-bitová	RAR 3.x – 4.x - AES

Tabulka 28: Porovnání rychlostí ve vyhledávání hesel pomocí daných programů a typů útoků – WinRAR 5.21 – RAR 3.x – 4.x AES.

Dešifrovací program:	**Typ útoku:**	**Rychlost hledání hesel:**	**Použití GPU:**
Elcomsoft	Hrubou silou	24 tisíc	ano
Passware	**Hrubou silou**	**32 tisíc**	**ano**

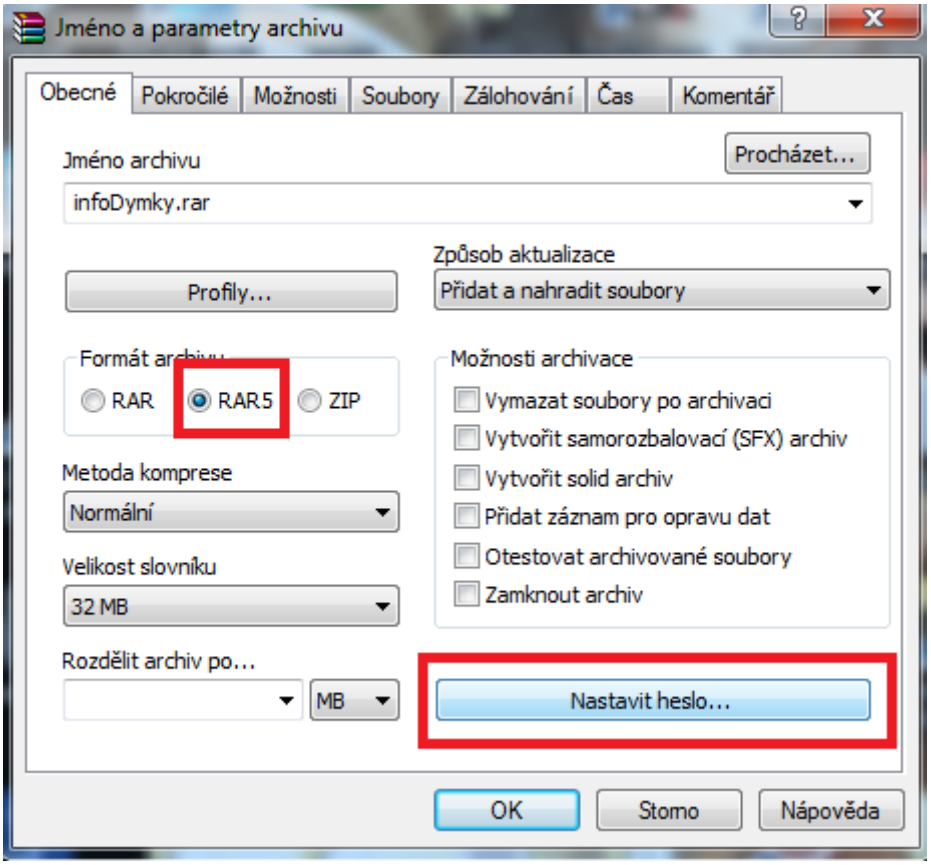
Tabulka 29: Počet dní potřebných k vyhledání hesla v závislosti na délce hesla a použité znakové sadě – WinRAR 5.21 – RAR 3.x – 4.x AES.

Znaková sada / délka hesla	26	36	52	62	96
5	**0**	**0**	**0**	**0**	**2**
6	**0**	**0**	**7**	**20**	283
7	**2**	**28**	371	1273	27179
8	75	1020	19335	78971	2609192

Tabulka 30: Základní informace o testovaném souboru – WinRAR 5.21 – RAR 5.x AES.

Název souboru:	**Použitý program:**	**Typ šifrování:**
testData5-rar5.rar*	WinRAR 5.21 64-bitová	RAR 5.x - AES

Poznámka: - při zašifrování tohoto souboru bylo využito přepínače formátu archivu a byla zvolena hodnota: „RAR5“, tím dojde k vytvoření archivu pomocí nového formátu, který využívá silnější typ šifrování.*



Obrázek 73: Nastavení nového formátu archivačního programu WinRAR 5.21.

Tabulka 31: Porovnání rychlostí ve vyhledávání hesel pomocí daných programů a typů útoků – WinRAR 5.21 – RAR 5.x AES.

Dešifrovací program:	Typ útoku:	Rychlost hledání hesel:	Použití GPU:
Elcomsoft	nepodporováno	nepodporováno	nepodporováno
Passware	**Hrubou silou**	**16,5 tis.**	**ano**
Elcomsoft-ARCHPR	nepodporováno	Nepodporováno	nepodporováno

Tabulka 32: Počet dní potřebných k vyhledání hesla v závislosti na délce hesla a použité znakové sadě – WinRAR 5.21 – RAR 5.x AES.

Znaková sada / délka hesla	26	36	52	62	96
5	**0**	**0**	**0**	**0**	**2**
6	**0**	**0**	**7**	**20**	283
7	**2**	**28**	371	1273	27179
8	75	1020	19335	78971	2609192

Tabulka 33: : Základní informace o testovaném souboru – WinRAR 5.21 – ZIP 2.0.

Název souboru:	**Použitý program:**	**Typ šifrování:**
testData5.zip	WinRAR 5.21 64-bitová	ZIP 2.0

Tabulka 34: Porovnání rychlostí ve vyhledávání hesel pomocí daných programů a typů útoků – WinRAR 5.21 – ZIP 2.0.

Dešifrovací program:	**Typ útoku:**	**Rychlost hledání hesel:**	**Použití GPU:**
Elcomsoft	nepodporováno	nepodporováno	nepodporováno
Passware	**Hrubou silou**	**88 mil.**	**ne**
Elcomsoft-ARCHPR*	Hrubou silou	33 mil.	ne

Tabulka 35: Počet dní potřebných k vyhledání hesla v závislosti na délce hesla a použité znakové sadě – WinRAR 5.21 – ZIP 2.0.

Znaková sada / délka hesla	26	36	52	62	96
5	**0**	**0**	**0**	**0**	**0**
6	**0**	**0**	**0**	**0**	**0**
7	**0**	**0**	**0**	**0**	**9**

8	**0**	**0**	**7**	**28**	948
9	**0**	**13**	365	1780	91084
10	**18**	480	19012	110387	8744116

6.4 GPG4Win

Tabulka 36: Základní informace o testovaném souboru – GPGWin 2.2.4 – PGP Private Key.

Název souboru:	**Použitý program:**	**Typ šifrování:**
Secring-4096.gpg*	GPG4Win 2.2.4 - Kleopatra	PGP Private Key, RSA, PGP

Tabulka 37: Porovnání rychlostí ve vyhledávání hesel pomocí daných programů a typů útoků – GPGWin 2.2.4 – PGP Private Key.

Dešifrovací program:	**Typ útoku:**	**Rychlost hledání hesel:**	**Použití GPU:**
Elcomsoft	Hrubou silou	350	ne
Passware	**Hrubou silou**	**52 tis.**	**ano**

Tabulka 38: Počet dní potřebných k vyhledání hesla v závislosti na délce hesla a použité znakové sadě – GPGWin 2.2.4 – PGP Private Key.

Znaková sada / délka hesla	26	36	52	62	96
5	**0**	**0**	**0**	**0**	**1**
6	**0**	**0**	**4**	**12**	174
7	**1**	**17**	228	783	16725
8	46	627	11898	48597	1605657

Poznámka: Jedná se o privátní klíč, který se automaticky vygeneruje po vytvoření certifikátu například programem Kleopatra do složky „C:\Users\uzivatel\AppData\Roaming\gnupg“. Při generování tohoto certifikátu byla pou-*

žita šifra o délce klíče 4096 bitů. Jedná se o totožný klíč, který dostaneme při vytváření nového klíče a jeho následné zálohy nebo pokud v programu Kleopatra vyexportujeme stávající klíč (je nutné znát heslo).

Tabulka 39: Základní informace o testovaném souboru – GPGWin 2.2.4 – GpgEx.

Název souboru:	Použitý program:	Typ šifrování:
test.xlsx-4096.gpg*	GPG4Win 2.2.4 - GpgEX	neznámé

Tabulka 40: Porovnání rychlostí ve vyhledávání hesel pomocí daných programů a typů útoků – GPGWin 2.2.4 – GpgEx.

Dešifrovací program:	Typ útoku:	Rychlost hledání hesel:	Použití GPU:
Elcomsoft	nepodporováno	nepodporováno	nepodporováno
Passware	nepodporováno	nepodporováno	nepodporováno

Poznámka: Jedná se zašifrovaný soubor vytvořený za pomoci softwarového balíku GPG4Win a jeho programu GpgEX.*

6.5 Symantec Encryption Desktop

Tabulka 41: Základní informace o testovaném souboru – Symantec Encryption Desktop – PGP SDA Archive.

Název souboru:	Použitý program:	Typ šifrování:
test.xlsx-4096.exe*	Symantec Encryption Desktop	PGP SDA Archive

Tabulka 42: Porovnání rychlostí ve vyhledávání hesel pomocí daných programů a typů útoků – Symantec Encryption Desktop – PGP SDA Archive.

Dešifrovací program:	Typ útoku:	Rychlost hledání hesel:	Použití GPU:
Elcomsoft	Hrubou silou	10,5 tis.	ne
Passware	**Hrubou silou**	**750 tis.**	**ano**

Tabulka 43: Počet dní potřebných k vyhledání hesla v závislosti na délce hesla a použité znakové sadě - Symantec Encryption Desktop – PGP SDA Archive.

Znaková sada / délka hesla	26	36	52	62	96
5	**0**	**0**	**0**	**0**	**0**
6	**0**	**0**	**0**	**0**	**12**
7	**0**	**1**	**15**	54	1159
8	**3**	43	824	3369	11325

Poznámka: Jedná se o samorozbalitelný zašifrovaný soubor vytvořený za pomoci softwarového balíku Symantec Encryption Desktop a jeho programu PGP ZIP.*

Tabulka 44: Základní informace o testovaném souboru – Symantec Encryption Desktop – PGP AES 256 bitů.

Název souboru:	**Použitý program:**	**Typ šifrování:**
Testovani.doc-symantec.pgp*	Symantec Encryption Desktop	PGP AES 256 bitů

Tabulka 45: Porovnání rychlostí ve vyhledávání hesel pomocí daných programů a typů útoků – Symantec Encryption Desktop – PGP AES 256 bitů.

Dešifrovací program:	**Typ útoku:**	**Rychlost hledání hesel:**	**Použití GPU:**
Elcomsoft	Hrubou silou	150	ne
Passware	**Hrubou silou**	**20 tis.**	**ano**

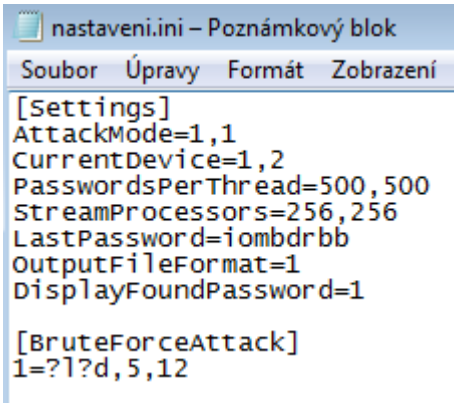
Tabulka 46: Počet dní potřebných k vyhledání hesla v závislosti na délce hesla a použité znakové sadě - Symantec Encryption Desktop – PGP AES 256 bitů.

Znaková sada / délka hesla	26	36	52	62	96
5	**0**	**0**	**0**	**0**	**4**
6	**0**	**1**	**11**	**32**	452
7	**4**	**45**	594	2037	43486

8	120	1632	30937	126354	4174708

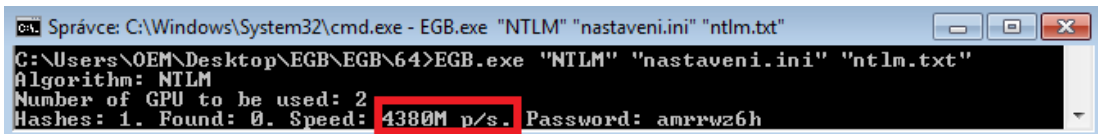
6.6 HASHe

U softwaru EGB je zapotřebí před začátkem vyhledávání hesel nastavit vlastnosti použitých grafických karet a možnosti vyhledávání hesel.

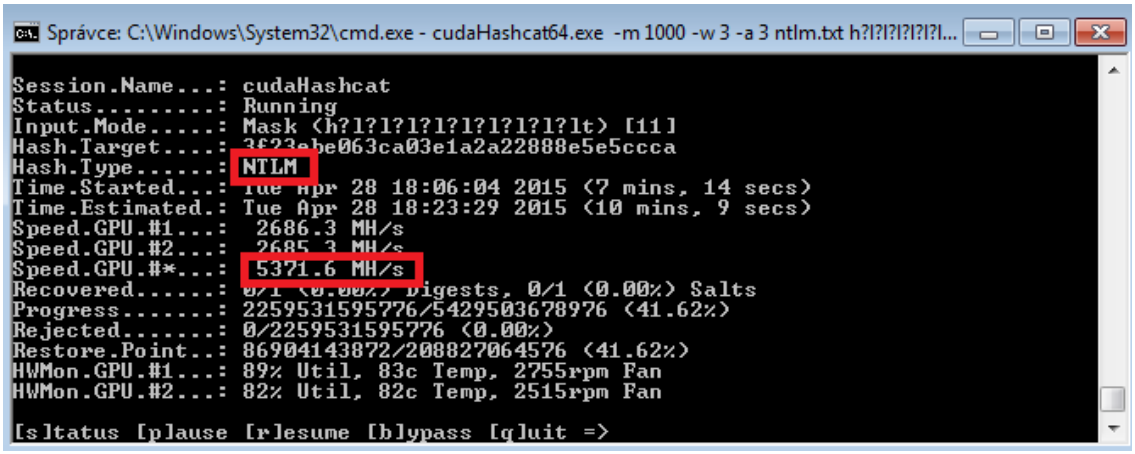


Obrázek 74: Soubor s nastavením pro software EGB.

Software oclHashcat si načte ovladače daných grafických karet automaticky a sám vytvoří nejlepší nastavení pro dané vyhledávání hesel (toto nastavení lze manuálně upravovat).



Obrázek 75: Vyhledávání hesla pomocí útoku hrubou silou prostřednictvím softwaru Extreme GPU Bruteforcer – NTLM hash.



Obrázek 76: Vyhledávání hesla pomocí útoku hrubou silou prostřednictvím softwaru oclHashcat – NTLM hash.

Tabulka 47: Základní informace o testovaném HASH souboru – hash NTLM.

Typ hashe:	Používaný pro:	Velikost:
NTLM	operační systém MS Windows	128 bitů

Tabulka 48: Porovnání rychlostí ve vyhledávání hesel pomocí daných programů a typů útoků – hash NTLM.

Dešifrovací program:	Typ útoku:	Rychlost hledání hesel:	Použití GPU:
EGB	Hrubou silou	4,4 miliardy	ano
oclHashcat	**Hrubou silou**	**5.4 miliardy**	**ano**

Tabulka 49: Počet dní potřebných k vyhledání hesla v závislosti na délce hesla a použité znakové sadě – hash NTLM .

Znaková sada / délka hesla	26	36	52	62	96
5	0	0	0	0	0
6	0	0	0	0	0
7	0	0	0	0	0
8	0	0	0	0	15

9	0	0	5	29	1484
10	0	7	309	1798	142496
11	7	282	14111	111532	13679683

Tabulka 50: Základní informace o testovaném HASH souboru – hash MD5.

Typ hashe:	Používaný pro:	Velikost:
MD5	integrita souborů, uložení hesel	128 bitů

Tabulka 51: Porovnání rychlostí ve vyhledávání hesel pomocí daných programů a typů útoků – hash MD5.

Dešifrovací program:	Typ útoku:	Rychlost hledání hesel:	Použití GPU:
EGB	Hrubou silou	3,7 miliardy	ano
oclHashcat	Hrubou silou	12 miliard	ano

Tabulka 52: Počet dní potřebných k vyhledání hesla v závislosti na délce hesla a použité znakové sadě – hash MD5.

Znaková sada / délka hesla	26	36	52	62	96
5	0	0	0	0	0
6	0	0	0	0	0
7	0	0	0	0	0
8	0	0	0	0	15
9	0	0	2	13	667
10	0	3	139	809	64123
11	3	126	7250	50189	6155857

Tabulka 53: Základní informace o testovaném HASH souboru – hash SHA-1.

Typ hashe:	**Používaný pro:**	**Velikost:**
SHA-1	integrita souborů, uložení hesel	160 bitů

Tabulka 54: Porovnání rychlostí ve vyhledávání hesel pomocí daných programů a typů útoků – hash SHA-1.

Dešifrovací program:	**Typ útoku:**	**Rychlost hledání hesel:**	**Použití GPU:**
EGB	Hrubou silou	1,6 miliardy	ano
oclHashcat	**Hrubou silou**	**3 miliard**	**ano**

Tabulka 55: Počet dní potřebných k vyhledání hesla v závislosti na délce hesla a použité znakové sadě – hash SHA-1.

Znaková sada / délka hesla	26	36	52	62	96
5	**0**	**0**	**0**	**0**	**0**
6	**0**	**0**	**0**	**0**	**0**
7	**0**	**0**	**0**	**0**	**0**
8	**0**	**0**	**0**	**0**	**15**
9	**0**	**0**	**10**	52	2671
10	**0**	**14**	557	3238	256494
11	**14**	507	29000	200758	24623430

HASHe používáné programem TrueCrypt:

Tabulka 56: Základní informace o testovaném HASH souboru – hash SHA-512.

Typ hashe:	**Používaný pro:**	**Velikost:**
SHA-512	integrita souborů, uložení	512 bitů

	hesel, TrueCrypt	

Tabulka 57: Porovnání rychlostí ve vyhledávání hesel pomocí daných programů a typů útoků – hash SHA-512.

Dešifrovací program:	Typ útoku:	Rychlost hledání hesel:	Použití GPU:
EGB	Hrubou silou	169 milionů	ano
oclHashcat	**Hrubou silou**	**259 milionů**	**ano**

Tabulka 58: Počet dní potřebných k vyhledání hesla v závislosti na délce hesla a použité znakové sadě – hash SHA-512.

Znaková sada / délka hesla	26	36	52	62	96
5	**0**	**0**	**0**	**0**	**0**
6	**0**	**0**	**0**	**0**	**0**
7	**0**	**0**	**0**	**0**	**5**
8	**0**	**0**	**3**	**14**	494
9	**0**	**6**	190	927	47428
10	**9**	250	9899	57479	4553149

Tabulka 59: Základní informace o testovaném HASH souboru – hash RipeMD160.

Typ hashe:	Používaný pro:	Velikost:
RipeMD160	integrita souborů, uložení hesel, TrueCrypt	160 bitů

Tabulka 60: Porovnání rychlostí ve vyhledávání hesel pomocí daných programů a typů útoků – hash RipeMD160.

Dešifrovací program:	Typ útoku:	Rychlost hledání hesel:	Použití GPU:

EGB	nepodporováno	nepodporováno	nepodporováno
oclHashcat	**Hrubou silou**	**2,2 miliard**	**ano**

Tabulka 61: Počet dní potřebných k vyhledání hesla v závislosti na délce hesla a použité znakové sadě – hash RipeMD160.

Znaková sada / délka hesla	26	36	52	62	96
5	**0**	**0**	**0**	**0**	**0**
6	**0**	**0**	**0**	**0**	**0**
7	**0**	**0**	**0**	**0**	**5**
8	**0**	**0**	**0**	**1**	37
9	**0**	**0**	**14**	71	3643
10	**0**	**19**	760	4415	349764
11	**19**	692	39545	273761	33577405

Tabulka 62: Základní informace o testovaném HASH souboru – hash Whirlpool.

Typ hashe:	**Používaný pro:**	**Velikost:**
Whirlpool	integrita souborů, uložení hesel, TrueCrypt	512 bitů

Tabulka 63: Porovnání rychlostí ve vyhledávání hesel pomocí daných programů a typů útoků – hash RipeMD160.

Dešifrovací program:	**Typ útoku:**	**Rychlost hledání hesel:**	**Použití GPU:**
EGB	nepodporováno	nepodporováno	nepodporováno
oclHashcat	**Hrubou silou**	**123 milionů**	**ano**

Tabulka 64: Počet dní potřebných k vyhledání hesla v závislosti na délce hesla a použité znakové sadě – hash Whirlpool.

Znaková sada / délka hesla	26	36	52	62	96
5	**0**	**0**	**0**	**0**	**0**
6	**0**	**0**	**0**	**0**	**0**
7	**0**	**0**	**0**	**0**	**7**
8	**0**	**0**	**5**	**20**	678
9	**0**	**9**	261	1273	65166
10	**13**	344	13602	78976	6255952

6.7 Využití FPGA

Získané hodnoty nejsou naměřené autorem tohoto textu, ale jsou deklarovány jedním z prodejců, který využívá technologii FPGA.

K hledání hesel byl použit server s 64 FPGA jednotkami. Cena tohoto serveru se softwarem na vyhledávání hesel je zhruba 50000Eur.

Tabulka 65: Základní informace o testovaném souboru – TrueCrypt (AES + RIPEMD).

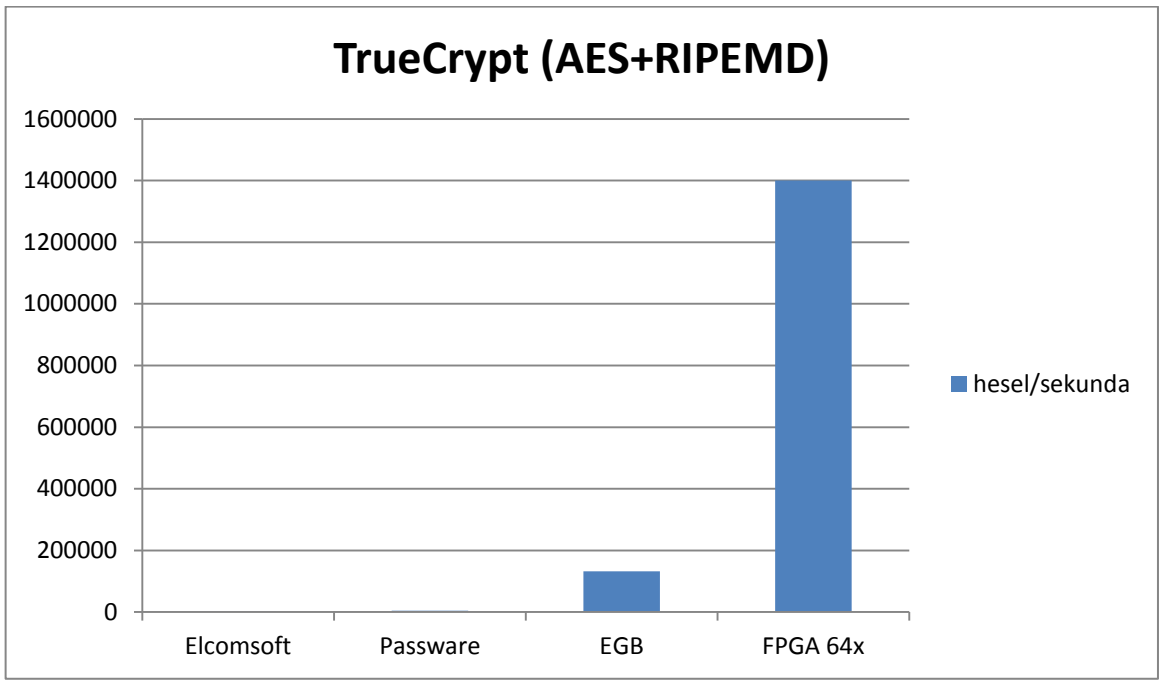
Název souboru:	**Použitý program:**	**Typ šifrování:**
TC-AES-RIPEMD160.txt	TrueCrypt 7.1a	AES + RIPEMD 160-bitů

Tabulka 66: Porovnání rychlostí ve vyhledávání hesel pomocí daných programů a typů útoků – TrueCrypt (AES + RIPEMD).

Dešifrovací program:	**Typ útoku:**	**Rychlost hledání hesel:**	**Použití GPU:**
Elcomsoft	Hrubou silou	800	ano
Passware	Hrubou silou	4,3 tisíc	ano
EGB	Hrubou silou	132 tisíc	ano
FPGA 64x	**Hrubou silou**	**1,4 milionu**	**ne**

Tabulka 67: Počet dní potřebných k vyhledání hesla v závislosti na délce hesla a použité znakové sadě – TrueCrypt (AES + RIPEMD).

Znaková sada / délka hesla	26	36	52	62	96
5	**0**	**0**	**0**	**0**	**0**
6	**0**	**0**	**0**	**0**	**6**
7	**0**	**0**	**8**	**29**	621
8	**1**	**23**	441	1805	59638
9	44	839	22982	11913	5725314

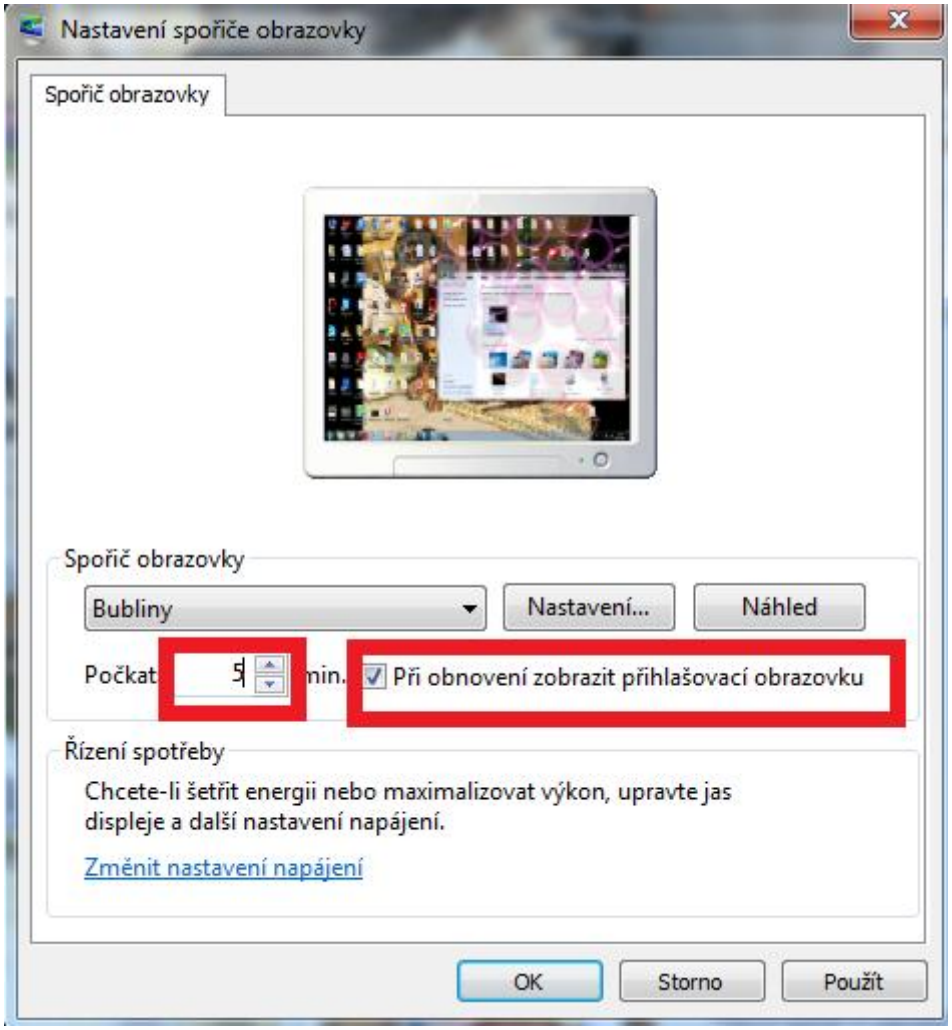


7 ZABEZPEČENÍ OSOBNÍHO POČÍTAČE A DŮLEŽITÝCH DAT PŘED NEOPRÁVNĚNÝM PŘÍSTUPEM

7.1 Obecné základy pro zabezpečený počítač

V této podkapitole je pojednáno o základních faktorech, které určují, zdali je daný počítač zabezpečený a ochráněný, jak proti přístupu k datům nežádoucí osobou, tak proti útoku z internetu. Následuje několik základních kroků vedoucích k více bezpečnému používání počítače:

- Jak jistě každý, počítačově alespoň trochu poskvrněný, uživatel ví, je velice důležité využívat v počítači správně nastavený firewall, antivirový program a mít zaktualizovaný operační systém.
- Je důležité mít nastavené u každého uživatele v počítači silné heslo. Pokud počítač využívá jen jediný uživatel, tak je i tak možné mít nastavené dva účty, a to jeden s administrátorskými právy a jeden se standardními právy. A právě ten standardní využívat na všechnu práci, kde nepotřebujeme administrátorské privilegia a to z důvodu nutnosti spuštění určitých programů (pro vyhledávání zašifrovaných dat, vytvoření bitové kopie a další) případného fyzického přístupu útočníka na náš odemčený (přihlášený) počítač.
- Nastavení spuštění spořiče obrazovky počítače po dobu nečinnosti. Toto nastavení pokud je aplikováno spolu s nutností zadat heslo pro zrušení spořiče obrazovky velice ztěžuje „vytěžení“ počítače případnou nežádoucí osobou. Zvolení času, po kterém má dojít k aktivaci spořiče, bych nastavil na hodnotu mezi 3-10 minutami.



Obrázek 77: Nastavení zapnutí spořiče obrazovky na 5 minut po dobu nečinnosti na PC.

- Nepoužívat režim hibernace nebo po každé obnovené relaci z režimu hibernace vymazat speciálním programem (mnohonásobné přepisy náhodnými daty) soubor hiberfil.sys.
- Využívat metodu „šifrování celého disku“.
- Nastavit si administrátorské heslo pro BIOS.
- Obecně je důležité všechna hesla vedoucí k citlivým informacím držet v tajnosti a s nikým toto heslo nesdílet, nepoznamenávat si ho, a pokud se potřebujeme připojit na internet mimo vlastní internetové připojení (internetová kavárna, KFC…), tak nezadávat (nepřihlašovat se) hesla do důležitých aplikacích (e-mailů, IM, internetové bankovnictví a další).
- Nepoužívat stejná hesla pro více důležitá přihlašování… Je teoreticky možné mít jedno stejné (nemusí být ani složité - silné) heslo pro „nedůležité“ přihlašování – diskusní fóra, e-shopy a všechny možné aplikace, kde je nutné zadat heslo, ale neobsahují žádné citlivé informace. Ale toto stejné heslo nesmí být využito pro přihlašování do jakéhokoli důležitého systému/aplikace – zašifrovaný

disk/kontejner, přihlašovací heslo do operačního systému, heslo do e-mailového účtu, privátní klíč a další.

- Ta hesla, která chrání citlivá data, by měla být po nějakém časovém intervalu (přibližně 3 – 12 měsíců) měněna a v budoucnu by nemělo být použito již jednou používané heslo.

7.2 Ochrana před vytvořením bitové kopie paměti RAM

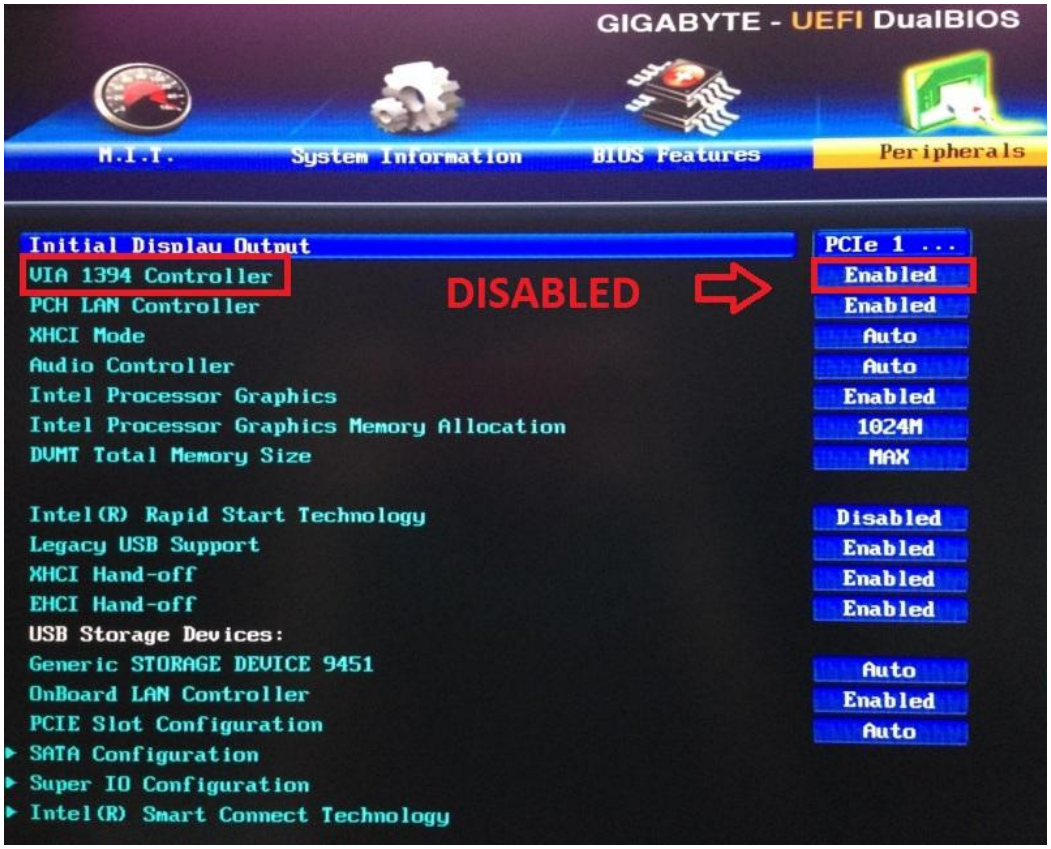
Jak již bylo napsáno výše, z paměti RAM se dají získat velice důležité informace a je to často jediná možnost, jak se dostat k zašifrovaným datům. A proto je velice důležité co nejvíce zabezpečit/znemožnit přístup k paměti RAM.

1. **odstranění FireWire 1394 rozhraní**

   Tento krok spočívá v odmontování/vypnutí rozhraní FireWire. Toto rozhraní není dnes již tak běžné jako dříve a nebývá součástí nových počítačových sestav a notebooků. Dříve toto zařízení sloužilo hlavně pro připojení videokamer k počítači. Pokud je toto zařízení součástí počítače/notebooku a je připojeno pomocí nějaké externí karty (PCI, EpressCard, PCMCIA…) a toto zařízení není používáno, tak je doporučeno ho odstranit.

2. **deaktivování FireWire 1394 rozhraní**

   Další možností je toto zařízení deaktivovat v BIOSu. Následně, pokud by nežádoucí osoba chtěla využít toto zařízení pro získání bitové kopie paměti RAM, by musela toto zařízení zase aktivovat v BIOSu, a tím by samozřejmě došlo při restartu počítače k vymazání paměti RAM.



Obrázek 78: Deaktivování FireWire rozhraní (1394) v BIOSu.

7.3 Silné heslo

Jak již bylo uvedeno výše, je velice důležité používat u „citlivých“ přihlášení/aplikací silné heslo a toto heslo nepoužívat u více přihlášení. Pojmem silné heslo je myšlena taková posloupnost znaků, kterou nebude možné pomocí útoku hrubou silou v reálném čase (řekněme jeden rok) nalézt.

Je velice důležité použít takové heslo, aby bylo nutné k jeho vyhledání použít právě útok hrubou silou. To znamená, že heslo neobsahuje žádné znaky související s daným uživatelem a není možné ho najít ve slovníku ani v případě modifikace (pepa123, slavie14, papoušekKKK a další). Dále, jak vyplývá z jednotlivých tabulek ukazujících potřebný počet dnů k vyhledání hesel, je účelné použít v hesle speciální znak (doba hledání hesla exponenciálně vzroste). A nakonec co se týká délky hesla, je dnes dostačující použít u většiny druhů šifrovaných dat (ne taková, která jdou prolomit okamžitě – MS Office 2003) 10 znaků. I při využití technologie FPGA a dodržení výše popsaných pravidel, se hledání daného hesla za použití útoku hrubou silou dostává útočník do času potřebného k nalezení do řádově desítek let a více.

7.4 Konkrétní ochrana dat

Co se týká využití konkrétních programů pro šifrování dat, tak autor doporučuje využívat pro šifrování celého disku (a využití šifrovaných kontejnerů) software TrueCrypt. Ač tento software již není aktualizován a skončil za nejasných okolností, tak v projektu, který testoval jeho bezpečnost, nebyly nalezeny kritické chyby. Stejně tak, lze využít jednoho z jeho následovníků – TCnext, VeraCryt, kteří využívají stejné zdrojové kódy jako program TrueCrypt. Při volbě algoritmů autor doporučuje využití jednoho ze zkombinovaných algoritmů (AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES a Twofish-Serpent) a pro HASH algoritmus je doporučován Whirlpool. Tato kombinace zaručuje co největší bezpečnost před případnými útoky.

A jako druhý software pro zabezpečení důležitých dat je doporučen software Gpg4win, který je také zdarma k použití. A zejména kombinací s předchozím softwarem je utvořena velice bezpečná vrstva, která chrání před nežádoucími průniky k citlivým datům. Při vytváření privátního klíče je doporučováno vždy zapínat největší možnou délku šifrovacího klíče (momentálně u tohoto programu 4096 bitů).

ZÁVĚR

Jak je napsáno v této práci, je velice důležité si chránit svá citlivá data nejen v reálném životě, ale také v tom digitálním. A tato ochrana nespočívá pouze v základních principech zabezpečeného počítače, jako jsou používání silných hesel, udržování aktualizovaného softwaru, správné nastavení uzamykání počítače a mnohé další, ale také ve využití speciálních softwarů pro šifrování elektronický dat. V této práci je pojednáno o výhodách a nevýhodách jednotlivých možností šifrování dat a také o vlastnostech těchto speciálních softwarů. Pro zabezpečení koncového počítače je autorem doporučovaná kombinace softwarů TrueCrypt, pro zašifrování celého disku (nebo vytvoření šifrovaného kontejneru) a Gpg4win, pro šifrování jednotlivých souborů. Právě tato kombinace dvou velice dobrých šifrovacích nástrojů zaručuje bezpečnost pro citlivá data i v případě prolomení jednoho ze softwarů (jako největší hrozbu vidí autor v přítomnosti utajeného kódu nějaké vládní organizace).

Druhou problematikou, kterou se autor v práci zajímá, je správný postup při zajišťování kriminalistické digitální stopy a její následná forenzní analýza. Je zde zdůrazněna důležitost správného zajištění zájmové stopy a to hlavně se zaměřením na možnosti, že zájmová data jsou šifrovaná. A s tím je velice spjata nutnost vytvářet bitové kopie paměti RAM a získávat forenzní informace ze spuštěných zájmových počítačů již na domovních prohlídkách. Následná forenzní analýza (zaměřená na získávání informací ze zašifrovaných dat) prováděná soudním znalcem se snaží v prvních krocích vyhledat informace, které by vedly k dešifrování zájmových (zašifrovaných) dat – hesla k různým aplikacím, privátní klíče, systémové soubory (pagefile.sys, hiberfil.sys, crash dump soubory) a další. Pokud tyto informace nevedou k získání zájmových zašifrovaných dat, tak lze využít speciální softwary (Passware Forensic Kit, Elcomsoft Recovery Bundle, Extreme GPU Bruteforcer, oclHashcat a jiné) a pomocí různých útoků (většinou se jedná o tzv. útok hrubou silou) se pokusit dané informace získat. První dva jmenované softwary jsou placené a měly by být přímými konkurenty, ale ve srovnání rychlostí (zkoušení hesel za sekundu) a funkcí jasně vítězí Passware, který je navíc výrazně levnější. Druhé dva softwary jsou zcela zdarma a nabízejí podobné možnosti, jen EGB umožňuje využít o trochu větší rychlosti a podporuje více zašifrovaných typů dat.

SEZNAM POUŽITÉ LITERATURY

[1] **Microsoft.** Windows BitLocker Drive Encryption Frequently Asked Questions. [Online] https://technet.microsoft.com/en-us/library/cc766200(v=WS.10).aspx#BKMK_Form.

[2] **GRAAF, CHRISTINE VAN DE.** Hardware and Software Work Together to Secure Systems. *http://www.cotsjournalonline.com/.* [Online] Únor 2013. http://www.cotsjournalonline.com/articles/view/103196.

[3] **TrueCrypt.** TrueCrypt Users Guide version 7.1a. *truecrypt.ch.* [Online] https://download.truecrypt.ch/documentation/TrueCrypt%20User%20Guide.pdf.

[4] **Gpg4win.** About Gpg4win. *http://www.gpg4win.org.* [Online] http://www.gpg4win.org/about.html.

[5] **Symantec.** Keeping Your Private Data Secure. *www.symantec.com.* [Online] http://securityresponse.symantec.com/content/en/us/enterprise/white_papers/b-keeping-your-private-data-secure_WP_21349382.pdf.

[6] **sciengines.** The next generation of performance-optimized reconfigurable computing. *http://www.sciengines.com/.* [Online] http://www.sciengines.com/products/computers-and-clusters/rivyera-s6-lx150.html.

[7] **Simon, Hunt.** Firewire Attacks Revisited. *http://ctogonewild.com/.* [Online] Říjen 2009. http://ctogonewild.com/2009/09/14/firewire-attacks-revisited/.

[8] **Carrier Brian D., Grand Joe.** A hardware-based memory acquisition procedure for digital investigations. *http://grandideastudio.com/.* [Online] Prosinec 2003. http://grandideastudio.com/wp-content/uploads/tribble_paper.pdf.

[9] **Schoen Sethn, Appelbaum Jacob.** Memory remanence. *https://citp.princeton.edu.* [Online] https://citp.princeton.edu/research/memory/media/.

[10] **Andreas, Schuster.** DMP File Structure. *http://computer.forensikblog.de/.* [Online] Březen 2006. http://computer.forensikblog.de/en/2006/03/dmp-file-structure.html.

[11] —. 64bit Crash Dumps. *http://computer.forensikblog.de/.* [Online] http://computer.forensikblog.de/en/2008/02/64bit-crash-dumps.html.

[12] **Nisarg, Trivedi.** Study on Pagefile.sys in Windows System. *http://www.iosrjournals.org/.* [Online] Duben 2014. http://www.iosrjournals.org/iosr-jce/papers/Vol16-issue2/Version-5/C016251116.pdf.

[13] **ElcomSoft.** The easy way to restore access passwords to files, applications and databases. *https://www.elcomsoft.com.* [Online] https://www.elcomsoft.com/WP/easy_way_to_restore_access_passwords_to_files_applications_and_databases_en.pdf.

[14] —. CORPORATE & FORENSIC SOLUTIONS. *https://www.elcomsoft.com.* [Online] https://www.elcomsoft.com/eprb.html#chart.

[15] **Passware.** Passware Recovery Kit Forensic 2015 V.2. *http://www.lostpassword.com/.* [Online] http://www.lostpassword.com/passware-kit-forensic/index.html.

[16] **insidepro.** *http://www.insidepro.com/.* [Online] http://www.insidepro.com/.

[17] **hashcat.** oclhashcat. *http://hashcat.net.* [Online] http://hashcat.net/oclhashcat/.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

RAM	(random-access memory) Označení operační paměti vytvořené pomocí polovodičových pamětí.
DMA	(Direct Memory Access) Přímý přístup do paměti. Data neprocházejí skrze procesor a lze tak dosáhnout vyššího výkonu.
MBR	(Master Boot Record) Je hlavní spouštěcí záznam, který je v IBM PC kompatibilních počítačích umístěn v prvním sektoru pevného disku (nebo obdobného média), tj. na jeho úplném začátku.
SSD disk	(Solid-state drive) Je v informačních technologiích typ datového média, které na rozdíl od magnetických pevných disků neobsahuje pohyblivé mechanické části.
NTFS	(New Technology File System) Je v informatice označení pro souborový systém, který vyvinula firma Microsoft pro svoje operační systémy řady Windows NT.
NSA	(The National Security Agency/Central Security Service) Je vládní kryptologická organizace Spojených států amerických, spadající pod ministerstvo obrany.
NSL	(National Security Letter) Jedná se o administrativní „obsílku“ vydanou FBI z důvodu šetření národní bezpečnosti.
GnuPG	(GNU Privacy Guard) Je svobodná alternativa k PGP kryptografickému softwaru, vydaná pod GNU licencí.
iPod	Je multimediální přehrávač firmy Apple.
UMA	(Upper memory area) Odkazuje na část paměti RAM mezi adresami 640 KB a 1024 KB pro přístup periferních zařízení.
soubor DMP	Soubory vzniklé v počítači s operačním systémem Microsoft Windows po tzv. modré smrti.
Soubor DLL	(Dynamic-link library) Je implementace konceptu sdílených knihoven společnosti Microsoft pro operační systém Microsoft Windows.
GPGPU	(General-purpose computing on graphics processing units) Je způsob vyu-

	žití paralelizace na grafické kartě k výpočtu obecných algoritmů.
GPU	(graphic processing unit) Je specializovaný řídící procesor umístěný na grafické kartě uvnitř počítače, který zajišťuje vykreslování dat uložených v operační paměti na zobrazovacím zařízení.
WiFi	(Wireless Ethernet Compatibility Aliance) Je označení pro několik standardů IEEE 802.11 popisujících bezdrátovou komunikaci v počítačových sítích.
BIOS	(Basic Input-Output System) Implementuje základní vstupně–výstupní funkce pro počítače.
Tabulka FAT	(File Allocation Table) Jedná se o tabulku obsahující informace o obsazení disku v souborovém systému vytvořeném pro DOS.
IM	(Instant messaging) je internetová služba, umožňující svým uživatelům sledovat, kteří jejich přátelé jsou právě připojeni, a dle potřeby jim posílat zprávy, chatovat, přeposílat soubory mezi uživateli a i jinak komunikovat.
VOIP	(Voice over Internet Protocol) Je technologie, umožňující přenos digitalizovaného hlasu v těle paketů rodiny protokolů UDP/TCP/IP prostřednictvím počítačové sítě nebo jiného média, prostupného pro protokol IP.
Tabulka MFT	(Master File Table) Je místo, kde jsou uloženy veškeré informace o souborech a složkách na jednotce typu NTFS.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK