Č.j.: 3680/2016 V Plzni, dne 13. října 2016

POLICIE ČESKÉ REPUBLIKY
NÁRODNÍ CENTRÁLA PROTI
ORGANOZOVANÉMU ZLOČINU
SLUŽBY KRIMINÁLNÍ POLICIE A VYŠETŘOVÁNÍ
SEKCE TERORISMU A EXTREMISMU
156 80 Praha 5 - Zbraslav

Výtisk číslo: 1
Počet stran: 15
Přílohy: 1 ks CD-R
(u výtisku 1 a 2)

DODATEK ZNALECKÉHO POSUDKU Č.j. 3316-10

z oboru Kybernetika
odvětví Výpočetní technika

Ing. Jan Janka, soudní znalec v oborech Kybernetika, odvětví Výpočetní technika a Elektronika, odvětví Elektronika, specializace Bezpečnost informačních systémů, podává tento

znalecký posudek

na základě: opatření podle § 105 odst. 1 trestního řádu v trestní věci:

S odkazem na předchozí opatření ze dne 5. května 2015 pod č.j. UOOZ-1513/TČ-2014-290050 (

, kteří jsou stíhání pro zvlášť závažný zločin teroristický útok ve stádiu přípravy dle ust. § 20 odst. 1 tr. zákoníku č. 40/2009 Sb. k ust. § 311 odst. 1, písm. c) odst. 3, písm. a), písm. d) tr. zákoníku č. 40/2009 Sb. a který je stíhán pro přečin nedovolené ozbrojování § 279 odst. 3, písm. a) tr. zákoníku č. 40/2009 Sb.)

Č.j.: NCOZ-1329/TČ-2016-413100 Praha 7. září 2016

Obsah:

1 Úvod

1.1 Věci, stopy a vzorky, které byly zkoumány

Notebook zn. ACER BCM 92044NMD v.č. 83813801520 s napájecím kabelem, vydání č. 1 igelitový pytel s označením Policie ČR bez pečeti vydaný pod.

1.2 Otázky, které mají být zodpovězeny

Ve znaleckém posudku je třeba posoudit a zodpovědět následující otázky:

1) Zpřístupnit veškerá data a provést zálohu pevných disků předloženého notebooku.

2) Zjistit programové vybavení zařízení.

2 Nález

2.1 Zkoumání zajištěného notebooku

2.1.1 Hardwarová konfigurace zkoumaných stop

Před vlastním zahájením zkoumání počítače byla nejprve zjištěna jeho hardwarová konfigurace. Ta byla zjišťována pomocí softwarových prostředků (PC Certify Pro v. 7, SiSoft SANDRA), pomocí výpisu hardware, poskytovaných operačním systémem a fyzickou kontrolou hardwarových komponent PC po demontáži skříně. Zároveň byl zjištěn tzv. systémový čas – tj. čas, který je interně udržován vnitřními hodinami počítače. Na základě takto nastaveného času pak počítač automaticky vykonává některé funkce, např. zaznamenává čas vytvoření nebo modifikace souborů apod.

2.1.2 Zadokumentování obsahu

U zkoumaného počítače byl vytvořen textový soubor, který dokumentuje adresářovou strukturu a provádí výpis všech souborů na pevném disku (včetně všech relevantních atributů). K provedení výpisu bylo použito programu HyperDir. Vzniklý soubor byl následně uložen do příslušného adresáře na optický disk, který tvoří přílohu tohoto znaleckého posudku. Pro zamezení možnosti modifikace takto uložených souborů a k zajištění možnosti ověření jejich integrity byl vypočítán tzv. MD5 hash. Jedná se o číselnou reprezentaci obsahu souboru. Číslo (hash) je závislé na všech znacích přiloženého souboru. Dojde-li nějakým způsobem k pozměnění obsahu souboru, bude MD5 hash reprezentován odlišným číslem. Naopak, pokud je vypočítán hash z obsahu souboru, který tvoří přílohu znaleckého posudku a získané číslo odpovídá číslu v nálezové části znaleckého posudku, nebyl soubor modifikován.
Pro možnost ověření integrity souborů (výpočet hashe) je na optickém disku umístěn soubor md5.exe, umožňující provedení kontroly neporušenosti textového souboru s výpisem obsahu zkoumaného média. Použití je: md5.exe <jméno_souboru>
Výstupem programu je textový řetězec (hash), který je nutné porovnat s údajem, vytištěným v nálezové části znaleckého posudku.

2.1.3 Zdokumentování programového vybavení

V další etapě zkoumání bylo provedeno zdokumentování nainstalovaného software. To bylo prováděno procházením adresářové struktury a vyhledáváním programových souborů. Ty pak byly binárně porovnány se softwarovými vzory v archivu znalce. V případě, že se daný software (jeho programový kód) nenacházel v archivu znalce, byl program spuštěn a údaje o něm zjištěny vizuální kontrolou.

Na základě zjištěných údajů o nainstalovaném software pak proběhla kontrola oprávnění jeho šíření. Software může spadat do jedné z několika skupin, které upravují možnosti jeho šíření. Do které kategorie program spadá, určuje jeho autor při uvolnění tohoto programového vybavení.

Základní skupiny jsou:

- **Public domain** – programy, zařazené do této skupiny lze volně šířit, lze je jakýmkoli způsobem dále upravovat a používat.
- **Freeware** - programy, zařazené do této skupiny lze volně šířit, autor však nedovoluje jejich úpravu a modifikaci
- **Shareware** - programy, zařazené do této skupiny lze volně šířit. Program sám je určen k vyzkoušení. To znamená, že po definovaném čase, případně počtu spuštění program může program přestat fungovat, uživatel je vyzýván k zaregistrování (zaplacení registračního poplatku). Shareware je obvykle distribuován ve verzi, která je oproti registrované verzi nějakým způsobem omezená. Velmi často proto někteří programátoři píší tzv. cracky – tj. programy, jejichž cílem je provést registraci bez vědomí autora (a bez zaplacení registračního poplatku) a tím zfunkčnit zablokované části programu.
- **Komerční software** – jedná se o software, které lze získat pouze jeho zakoupením. Jeho volné šíření není dovoleno.

2.1.4 Obnova smazaných dat z pevných disků

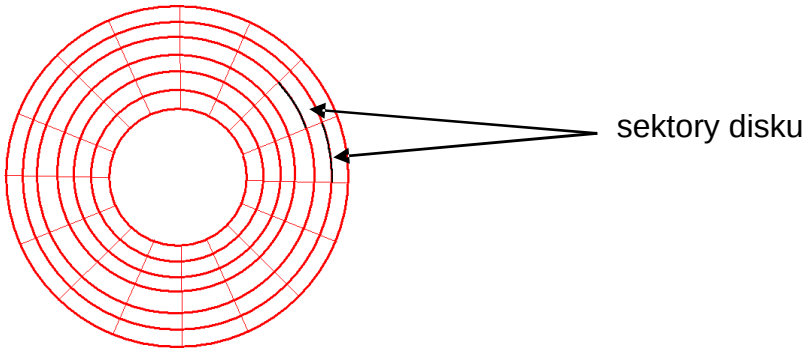
Součástí znaleckého zkoumání bylo i provedení obnovy dat – tj. rekonstrukce souborů, které se na pevném disku počítače v minulosti nacházely a následně byly odstraněny (smazány).

Vzhledem k tomu, že jakýkoli zásah do počítače, včetně jeho pouhého spuštění, může významně zasáhnout do struktury dat na disku, byl tento úkon realizován jako první (po vytvoření bitové kopie) ve sledu jednotlivých úkonů znaleckého zkoumání.

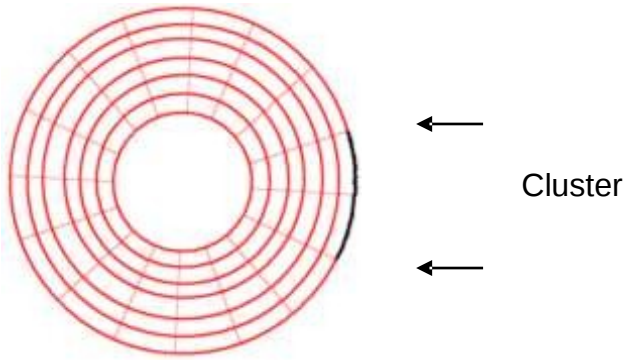
Pevný disk byl připojen k technologickému počítači znalce. Na tomto počítači pak byla provedena analýza struktury oblastí disku i vlastní proces obnovy dat. Všechny soubory, které se při realizaci obnovy dat podařilo rekonstruovat, byly kopírovány na externí disk tak, aby nedošlo ke změnám na disku zkoumaném.

Analýza pevného disku zkoumaného počítače

Na pevném disku mohou být data uložena různým způsobem. Vždy se jedná o magnetický záznam informace na diskových plotnách. Odlišnost uložení vychází z použitých operačních systémů. Z fyzického hlediska je disková plotna, na kterou jsou data ukládána, rozdělena na řadu soustředných kružnic, tzv. stop. Tyto stopy jsou dále rozděleny na tzv. sektory, z nichž každý má velikost 512 B. Sektor je nejmenší část disku, ke které lze přistupovat.



Souborový systém, používaný u operačních systémů Windows, patří do skupiny FAT16, FAT32 nebo NTFS (pozn. u disket je použit souborový systém FAT12). Souborové systémy v tomto případě nejsou schopny zapisovat a číst přímo jednotlivé sektory z disku. Namísto toho používají tzv. clustery. Cluster je tvořen vždy několika sektory, jejichž počet je odvozen od násobku čísla 2 (pouze u disket je cluster roven sektoru).



Na obrázku je uveden cluster, který se skládá ze dvou sektorů. Vzhledem k tomu, že velikost sektoru je 512 B (byte – jeden byte umožňuje uložení jednoho znaku), je velikost clusteru v tomto případě 1024 B.

Velikost clusteru může obvykle dosahovat hodnoty dvou, čtyř, osmi, šestnácti nebo dva a třiceti sektorů – podle velikosti disku. Čím je velikost disku větší, tím roste i velikost clusteru. V případě, že velikost clusteru dosahuje běžných osmi sektorů, je velikost tohoto clusteru 4096 B. To znamená, že pro uložení i sebemenšího souboru, obsahujícím např. jediný znak, je spotřebován vždy celý cluster – operační systém k menším částem diskového prostoru přistupovat neumí.

Uložení dat v souborech je jediný způsob, jakým lze data v operačních systémech rodiny MS Windows použít. U každého souboru je zaznamenán v souborovém systému jeho název, velikost, datum a čas, vztahující se k souboru, a číslo clusteru, kde soubor začíná. V případě souborového systému FAT pak existuje tzv. tabulka FAT, která popisuje využití jednotlivých clusterů na disku. U souborového systému NTFS je použito odlišné schéma, využívající tzv. MFT bloků – dále uvedený popis lze však vztáhnout i na tento souborový systém.

Jak již bylo uvedeno, souborové systémy uchovávají na discích u každého souboru různé údaje. Tyto informace jsou uloženy na jiném místě – v adresářovém záznamu - než vlastní data (obsah) souboru.

Dojde-li ke smazání souboru, nejsou vlastní data, tj. obsah souboru žádným způsobem přepsány ani zničeny. Záznam o souboru je označen jako neplatný zapsáním speciálního znaku 227hex namísto prvního znaku jména souboru. Datová oblast, obsazená smazaným souborem, je souborovým systémem označena jako volná a může být využita pro zápis nového souboru; k tomu dojde vymazáním příslušných položek v tabulce FAT.

Do doby, než je datová oblast, ve které byl uložen obsah souboru, přepsána, nebo než je přepsán údaj o původním smazaném souboru, lze soubor po jeho smazání obnovit. Vlastní problematika obnovy souborů je ve skutečnosti komplikovanější vinou skutečnosti, že data souboru mohou být uložena v clusterech, které neleží v řadě za sebou – dochází k tzv. fragmentaci souborů. To může proces obnovy smazaných souborů zkomplikovat nebo v některých případech i znemožnit.

Pro obnovu smazaných souborů z pevného disku zkoumaného počítače byly použity následující specializované programy pro obnovu dříve smazaných souborů:

- Norton DiskEdit z programového balíku Norton Utilities 9.0
- Search and Recover 1.0A společnosti IOLO Technologies, LLC
- EasyRecovery Professional 6.03 společnosti Ontrack Data Recovery Inc.

2.1.5 Operační systém a uživatelské účty

Informace o použitém operačním systému a o uživatelských účtech byly získány přímo z operačního systému, případně ze systémových souborů.

2.1.6 Zkoumání elektronické pošty

Na předložené výpočetní technice byly vyhledávány datové soubory, obsahující elektronickou poštu. Pokud by byly takovéto soubory znalcem nalezeny, byl by jejich obsah (jednotlivé elektronické zprávy) převeden do formátu „.htm“ a to včetně přílohových souborů jednotlivých elektronických zpráv.

2.1.7 Zkoumání historie IM komunikace

Na předložené výpočetní technice byly vyhledávány datové soubory, obsahující historii uživatelské komunikace pomocí IM (Instant Messaging) programů, jako jsou např. ICQ, QIP, Skype atd. Pokud byly takovéto soubory znalcem nalezeny, byl jejich obsah dle potřeby převeden a uložen do souborů ve formátu PDF, XLS a DOC.

2.1.8 Způsob vyhledávání zájmových dat

Znalec při zkoumání obsahu předložené výpočetní technicky a vyhodnocování jejího obsahu jakožto zájmového, vycházel z informací uvedených v opatření.

2.1.8.1 Manuální vyhledávání a prohlídka textových souborů

Mezi textovými soubory byly vyhledávány manuálním procházením veškeré uživatelem vytvořené textové soubory. Ty byly následně otevřeny v příslušném programu a prohlédnuty, zda neobsahují informace, relevantní pro vyšetřovaný případ.

V některých případech může být důležitá informace vložena např. jako grafický objekt – v tomto případě by vyhledávání klasickými postupy, jako je např. vyhledávání zájmových textových řetězců v souborech nebylo úspěšné. Prohledávány byly zejména dokumenty formátů doc, rtf, txt, xls, wri, pdf, htm a další (včetně archivů).

2.1.8.2 Vyhledávání a prohlídka grafických souborů

Grafické soubory, které mohou být použity pro ukládání potenciálně důležitých dat z hlediska trestního řízení, se dělí na bitmapové a vektorové.

Mezi soubory, byly vyhledávány grafické soubory následujících formátů:

Grafický formát	Přípona souboru
Windows Bitmap	BMP, DIB, RLE
Windows Enhanced Metafile	EMF
FlashPix	FPX
CompuServe GIF	GIF
Corel DRAW	CDR
ICO	ICO, CU, ANI
Interchange File Format Image (ILBM)	IFF, LBM, ILBM
JPEG	JPG, JPEG, JPE, JIF, JFIF
KDC	KDC
MAG	MAG
Portable Bitmap	PBM
PIC	PIC
Macintosh PICT	PICT, PCT
Alias PIX	PIX
Portable Network Graphics	PNG
Portable Pixmap	PPM
Adobe Photoshop	PSD
Sun Rasterfile	RAS
SGI	SGI, RGB, RGBA, BW, INT, INTA
Targa	TGA
Tag Image File Format	TIF, TIFF, XIF
Windows Metafile	WMF
X-Bitmap	XBM
X-Pixmap	XPM

Bylo provedeno vyhledání grafických souborů (včetně archivů) bez ohledu na jejich jméno, každý grafický soubor byl otevřen – následně byla provedena vizuální kontrola, zda obrázek neobsahuje jakékoli informace týkající se předmětné věci (dokumenty vzniklé např. naskenováním apod.)

K automatizaci těchto činností bylo využito grafického programu Thumbs Plus verze 7 společnosti Cerious Software.

2.1.9 Záloha uživatelských dat

Součástí znaleckého zkoumání bylo vytvoření zálohy všech uživatelských dat, které byly nalezeny na zkoumaných stopách. Uživatelské soubory byly vykopírovány na DVD-R disk do adresáře „*Uživatelská_data*“, který tvoří přílohu tohoto znaleckého posudku.

2.2 Výsledky zkoumání zajištěného notebooku

2.2.1 Stopa č. 1 – Notebook zn. ACER BCM 92044NMD, v.č. 83813801520 s napájecím kabelem - vydání č. 1, igelitový pytel s označením Policie ČR bez pečeti

Zkoumaný notebook byl v opatření k tomuto znaleckému posudku popsán následovně: **Notebook zn. ACER BCM 92044NMD, v.č. 83813801520 s napájecím kabelem - vydání č. 1, igelitový pytel s označením Policie ČR bez pečeti.**

fotografie zkoumaného notebooku, pořízené znalcem

fotografie zkoumaného notebooku, pořízená znalcem

detail zkoumaného počítače

2.2.1.1 Zajištění zkoumaného notebooku

Notebook byl ke zkoumání předán v níže uvedeném plastovém pytli bez pečeti.

2.2.1.2 Výsledky zkoumání

Po spuštění zkoumaného notebooku bylo zjištěno, že pevný disk je kompletně zašifrován, jak dokládá níže uvedený snímek. Bez znalosti hesla není možné obsah dat na pevném disku zkoumaného notebooku zpřístupnit.

výřez obsahu obrazovky, po spuštění zkoumaného počítače

Pro zjištění hesla byl použit specializovaný program se slovníkovým útokem, jelikož pevný disk byl zabezpečen šifrovacím programem LUKS (Linux Unified Key Setup). Ani po vyčerpání všech možných kombinací písmen a čísel nebylo heslo pro dešifrování pevného disku zjištěno. Jelikož nebyl získán přístup k datům uložených na pevném disku zkoumaného notebooku, bylo další zkoumání ukončeno.

2.3 Struktura a obsah přílohového média (příloha znaleckého posudku)

CD-R, které tvoří přílohu tohoto znaleckého posudku, má následující obsah:

posudek.docx	Tento znalecký posudek v elektronické formě (ve formátu Microsoft Word).
posudek.pdf	Tento znalecký posudek v elektronické formě (ve formátu Adobe Acrobat).

3 Závěr

1) **Zpřístupnit veškerá data a provést zálohu pevných disků předloženého notebooku.**

   Výsledky zkoumání jsou uvedeny v kapitole 2.2.1.2 tohoto znaleckého posudku.

2) **Zjistit programové vybavení zařízení.**

   Výsledky zkoumání jsou uvedeny v kapitole 2.2.1.2 tohoto znaleckého posudku.

4 Znalecká doložka

Znalecký posudek byl zpracován ve dnech 7. 9. 2016 – 13. 10. 2016.
Technické úkony byly realizovány pracovníky znalecké kanceláře.
Posudek je vyhotoven ve třech kopiích – Výtisk č. 1 a 2 pro POLICII ČR, NÁRODNÍ CENTRÁLA PROTI ORGANOZOVANÉMU ZLOČINU, SLUŽBY KRIMINÁLNÍ POLICIE A VYŠETŘOVÁNÍ, SEKCE TERORISMU A EXTREMISMU, 156 80 Praha 5 - Zbraslav, Výtisk č. 3 (bez příloh) pro archiv znalce.
Znalecký posudek jsem podal jako znalec, jmenovaný rozhodnutím Krajského soudu Praha, nám. Kinských 5, ze dne 14. 10. 1999, spr. 4049/98, pro obory:

- Kybernetika, odvětví Výpočetní technika
- Elektronika, odvětví Elektronika, specializace Bezpečnost informačních systémů

Znalecký úkon je zapsán pod pořadovým číslem 3680 znaleckého deníku.

Znalečné a náhradu nákladů účtuji podle připojené likvidace.

Znalec si je vědom následků vědomě nepravdivého znaleckého posudku.

Ing. Jan Janka