**Č.j.: 3316-10/2015** V Plzni, dne 1. září 2015

POLICIE ČESKÉ REPUBLIKY
Útvar pro odhalování organizovaného zločinu
Služba kriminální policie a vyšetřování
Odbor terorismu a extremismu
Pošt. schr. 41/V5

**156 80 Praha 5 - Zbraslav**

Výtisk číslo: 1
Počet stran: 40
Přílohy: 1 ks DVD-R
(u výtisku 1 a 2)
Bitové kopie:
*s/n: W1E8WFS3*

# ZNALECKÝ POSUDEK

## 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:

, kteří jsou stíháni 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.

**Zajištěné věci**

Č.j.: UOOZ-1513/TČ-2014-290050 Praha 5. května 2015

# Obsah:

# 1 Úvod

## *1.1 Věci, stopy a vzorky, které byly zkoumány*

**Pozn.:** V této části znaleckého posudku označeného číslem 3316-10, byly zkoumány zajištěné věci obsahující výpočetní techniku. Zkoumaní mobilních zařízení (SIM karty, mobilní telefony a tablety) jsou uvedeny ve znaleckém posudku označeném číslem 3616-13.

**Znalci byly ke zkoumání předány níže specifikované věci (Vydáno u pod. ) :**

- Hard disk 40 GB Toshiba, v.č. A149G63W6 včetně USB kabelu a obalu - stopa č. 1, orgatech č. 00019058
- Videokamera HD 3 LCD Touch, včetně USB kabelu,s SD kartou Kingston 8 GB, v.č. 884521B - stopa č. 2, orgatech č. 00019057
- Flash disk Verbatim - stopa č. 3, orgatech č. 00019056
- Flash disk Jetflash 8 GB - stopa č. 4, orgatech č. 00019055
- Notebook zn. ACER BCM 92044NMD, v.č. 83813801520 s napájecím kabelem - vydání č. 1, igelitový pytel s označením Policie ČR bez pečeti
- Mobilní telefon zn. Nokia 3510i, IMEI 351536007822263 se SIM kartou Sazka mobil č. 8942031013942285280, PIN 1234-vydání č. 2, orgatech č. 00225213
- SIM karta zn. Vodafone č. 894203101219254149 1V128 - vydání č. 3, orgatech č. 00225213
- SIM karta zn. Vodafone č. 8942031013802055427V128LTE - vydání č. 4, orgatech č. 00225213

## *1.2 Otázky, které mají být zodpovězeny*

Ve znaleckém posudku je třeba posoudit a zodpovědět následující otázky:

1. Provést základní prohlídku a popis předložených osobních PC a notebooků se zaměřením na technická data a výrobní čísla.

2. Zpřístupnit veškerá data a provést zálohu pevných disků přiložených PC a notebooků.

3. Zjistit programové vybavení jednotlivých zařízení.

4. Provést základní prohlídku a popis předložených paměťových zařízení (přehrávače, externí disky, flash disky, paměťové karty, videokamery, apod.).

5. Zpřístupnit data a provést zálohu všech zařízení dle bodu č. 4.

6. Uvést veškeré další skutečnosti, jež vyplynou ze znaleckého zkoumání a mohou přispět k objektivnímu posouzení věci.

# 2 Nález

## 2.1 Zkoumání zajištěných stop

### 2.1.1 Provedení bitové kopie

Na žádost PČR byla u každé zkoumané stopy provedena znalcem její bitová kopie. Jednotlivé bitové kopie (datové soubory vytvořené v operačním systému Linux) byly poté nakopírovány na pevné disky, které budou po jejich zaplnění předány vyšetřovateli. Přičemž bylo z kapacitních důvodů domluveno, že pevné disky mohou obsahovat bitové kopie stop, které byly zajištěny na různých místech. Bitové kopie stop analyzovaných a popisovaných v tomto posudku byly uloženy na pevný disk zn. Seagate S/N: *W1E8WFS3.*

Znalec provedl bitovou kopii každé stopy pod operačním systémem *Linux* pomocí příkazu *dd*.

V následující tabulce je uveden seznam zkoumaných stop, její označení v tomto posudku a soubor obsahující bitovou kopii dané stopy:

| Označ. stopy | Název souboru |
|---|---|
| Stopa_1_PC | Stopa1_PC.dd |
| Stopa_1_HDD | Stopa1_HDD.dd |
| Stopa_2 | Stopa2.dd |
| Stopa_3 | Stopa3.dd |
| Stopa_4 | Stopa4.dd |

Věrnou kopii zkoumané stopy (obraz) lze následně zpřístupnit opět za pomoci příkazu *dd* v Linuxu. Na takto vytvořené kopii lze provést i obnovu dříve smazaných souborů.

### 2.1.2 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.

### 2.1.3 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.

### 2.1.4 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.

### *2.1.5 Obnova smazaných dat z pevných disků*

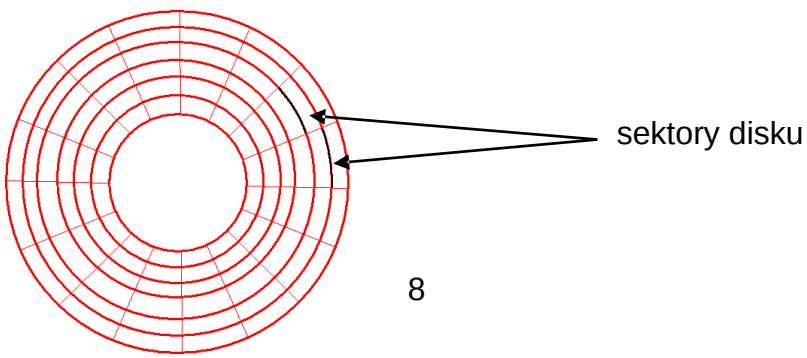
Součástí znaleckého zkoumání bylo i provedení obnovy dat – tj. rekonstrukce souborů, které se na pevném disku počítače v minulosti nacházely a následně byly odstraněny (smazány).

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.

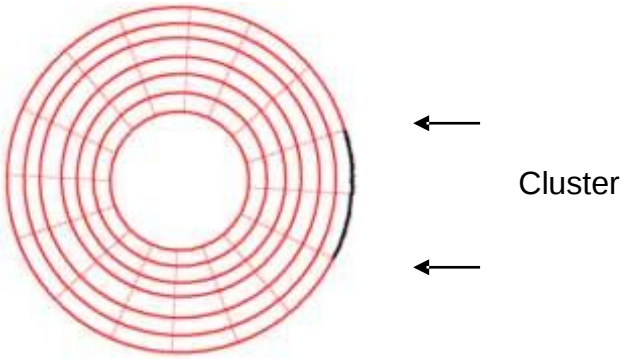
Pevný disk byl připojen k technologickému počítači znalce. Na tomto počítači pak byla provedena analýza struktury oblastí disku i vlastní proces obnovy dat. Všechny soubory, které se při realizaci obnovy dat podařilo rekonstruovat, byly kopírovány na externí disk tak, aby nedošlo ke změnám na disku zkoumaném.

**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.

### *2.1.6 Operační systém a uživatelské účty*

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

### *2.1.7 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.

### *2.1.8 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.

### *2.1.9 Způsob vyhledávání zájmových dat*

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

### *2.1.9.1 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).

### *2.1.9.2 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.

#### *2.1.9.3 Manuální vyhledávání a audiovizuálních souborů*

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

### *2.1.10 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 zajištěných stop (Vydáno u pod. )*

### *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*

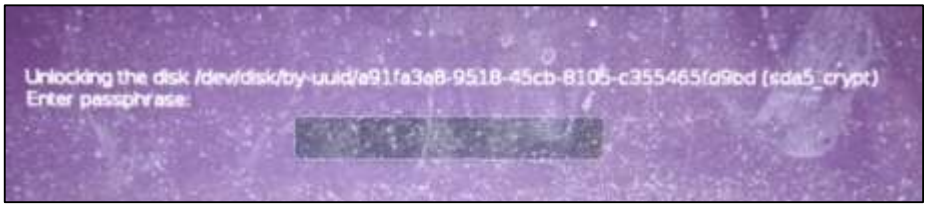
Notebook byl ke zkoumání předán v níže uvedeném plastovém pytli bez pečeti.


### *2.2.1.2 Vytvoření bitové kopie*

Zkoumaný pevný disk byl připojen k počítači znalce, kde byla vytvořena jeho bitová kopie. Výsledný soubor *„Stopa1_PC.dd“* byl pro možnosti dalšího šetření umístěn na přílohový pevný disk, který tvoří přílohu tohoto znaleckého posudku, do složky *„3316-10“.*

### *2.2.1.3 Výsledky zkoumání*

Po spuštění zkoumaného počítače bylo zjištěno, že pevný disk je kompletně zašifrován, jak dokládá níže uvedený snímek. Bez znalosti hesla není možné obsah dat na pevném disku zkoumaného počítače zpřístupnit. Další zkoumání bylo z tohoto důvodu ukončeno.




***výřez obsahu obrazovky, po spuštění zkoumaného počítače***

## *2.2.2 Stopa č. 1 – HDD zn. Toshiba 40 GB,S/N: 94LL6601T*

Zkoumaný pevný disk byl v opatření k tomuto znaleckému posudku popsán následovně: **Hard disk 40 GB Toshiba, v.č. A149G63W6 včetně USB kabelu a obalu - stopa č. 1, orgatech č. 00019058**

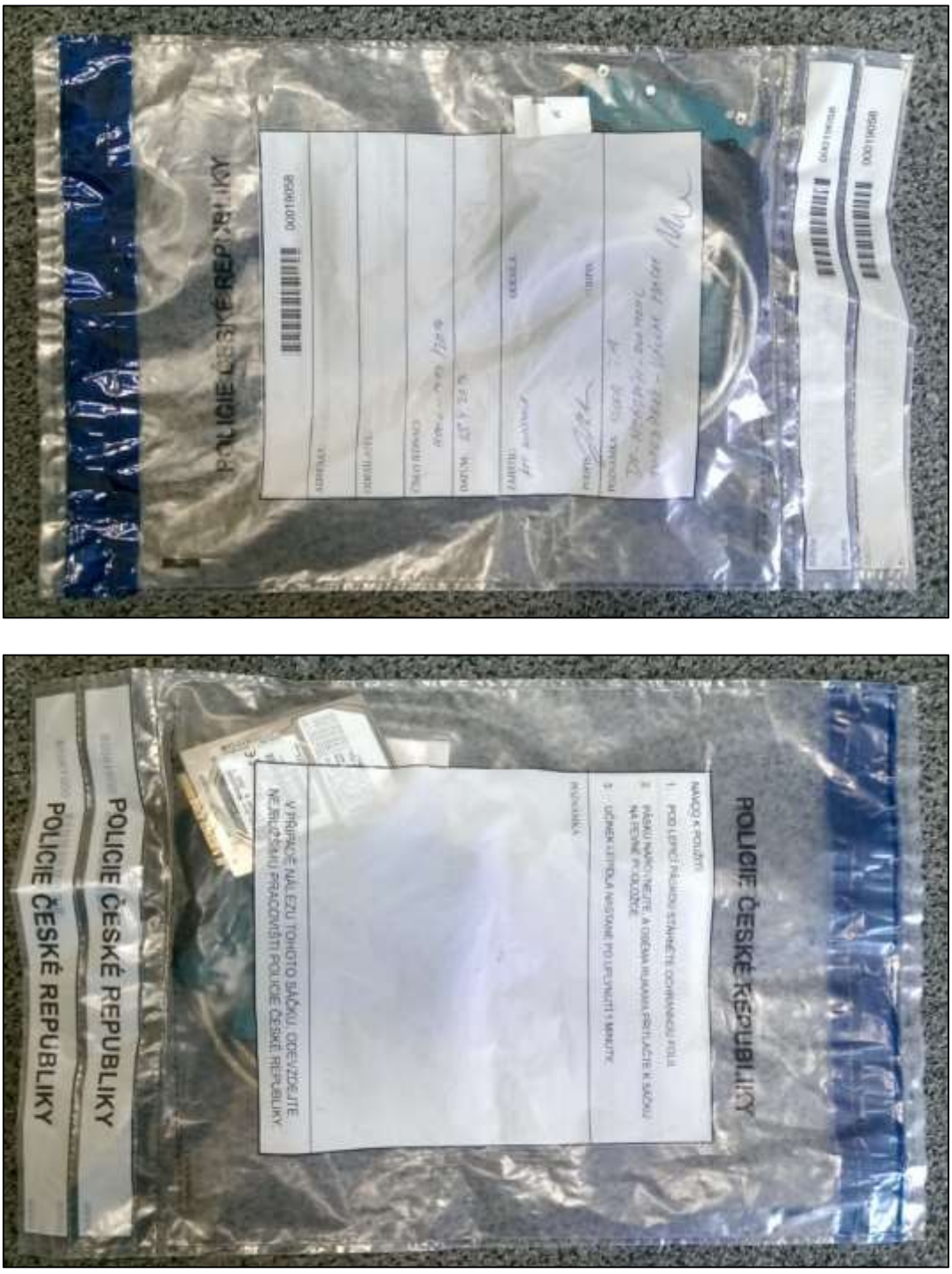

*Fotografie zkoumaného pevného disku, pořízené znalcem*

*Fotografie USB redukce pro IDE/SATA disky, pořízená znalcem*

### *2.2.2.1 Zajištění proti neoprávněné manipulaci*

Pevný disk byl ke zkoumání předán v neporušeném bezpečnostním sáčku PČR číslo 00019058. Zabezpečení bránilo připojení pevného disku k PC.

Zabezpečení pevného disku dokládají následující fotografie:




*fotografie zajištění, pořízená znalcem*

### *2.2.2.2 Diskový subsystém pevného disku*

Zkoumaný pevný disk obsahuje jeden primární oddíl naformátovaný souborovým systémem NTFS.

Dále jsou zadokumentovány zjištěné informace:

| **disk & part INFO** | |
|---|---|
| **disk:** | TOSHIBA MK4025GAS USB Device |
| **kapacita:** | 37,26 GB |
| **rozhraní:** | IDE |
| **sériové číslo:** | 94LL6601T |
| **----------** | **----------** |
| **počet partition:** | 1 |
| **----------** | **----------** |
| **číslo partition:** | 0 |
| **velikost:** | 37,25 GB |
| **bootovací:** | ne |
| **logický disk:** | F: |
| **file systém:** | NTFS |
| **jmenovka svazku:** | Nový svazek |
| **obsazenost:** | 86,11 MB / 37,25 GB |

### *2.2.2.3 Výpis adresářové struktury (výpis souborů externího disku)*

Zkoumaný pevný disk neobsahoval v době zkoumání žádné existující soubory.

### *2.2.2.4 Vytvoření bitové kopie*

Zkoumaný pevný disk byl připojen k počítači znalce, kde byla vytvořena jeho bitová kopie. Výsledný soubor *„Stopa1_HDD.dd“* byl pro možnosti dalšího šetření umístěn na přílohový pevný disk, který tvoří přílohu tohoto znaleckého posudku, do složky *„3316-10“.*

### *2.2.2.5 Vyhledávání v obnovených souborech*

Před vlastním začátkem znaleckého zkoumání byla na pevném disku provedena obnova dat způsobem principiálně shodným s postupem popsaným v kapitole 2.1.5 tohoto znaleckého posudku.

Ze zkoumaného pevného disku nebyly obnoveny žádné dříve smazané soubory.

### *2.2.3 Stopa č. 2 – Videokamera HD 3 LCD Touch*

Zkoumaná digitální videokamera byla v opatření k tomuto znaleckému posudku popsána následovně: **Videokamera HD 3 LCD Touch, včetně USB kabelu,s SD kartou Kingston 8 GB, v.č. 884521B - stopa č. 2, orgatech č. 00019057**


*Fotografie zkoumané digitální videokamery, pořízené znalcem*

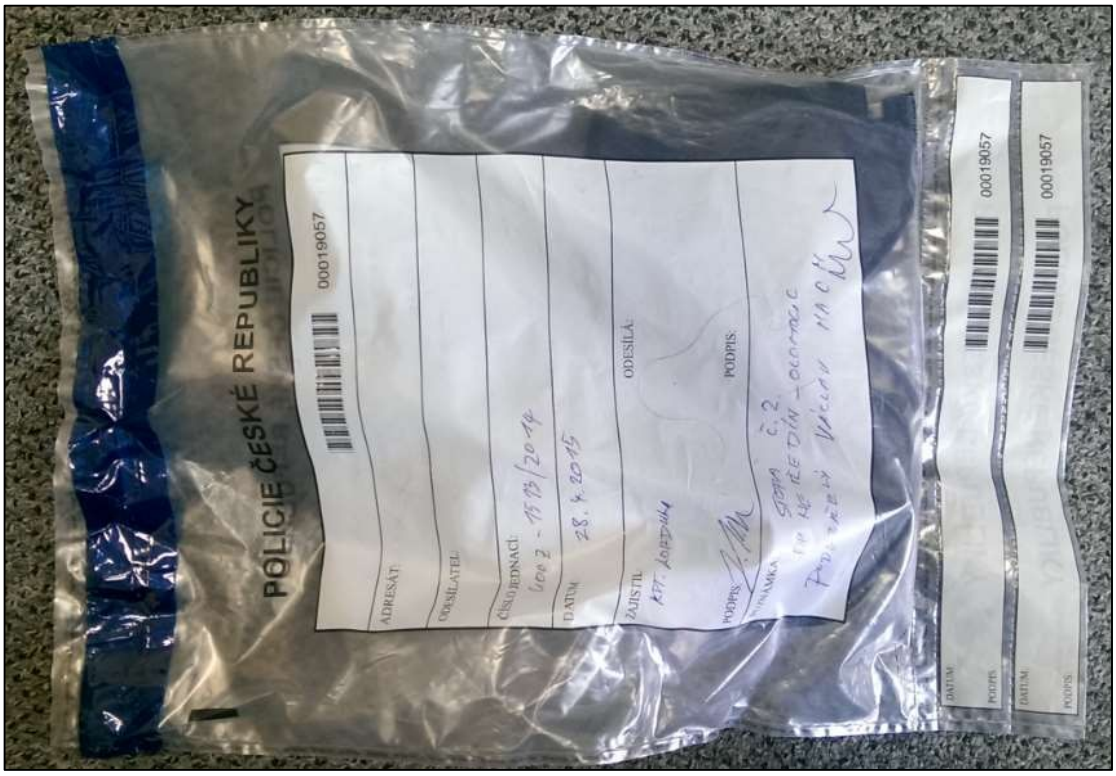

*Fotografie paměťové SD karty, pořízené znalcem*

*Fotografie datového kabelu, pořízená znalcem*

### *2.2.3.1 Zajištění proti neoprávněné manipulaci*

Zkoumané zařízení bylo ke zkoumání předáno v neporušeném bezpečnostním sáčku PČR číslo 00019057.

Zabezpečení zkoumaného zařízení dokládají následující fotografie:




*fotografie zajištění, pořízené znalcem*

### *2.2.3.2 Diskový subsystém videokamery*

Zkoumané zařízení obsahuje jeden primární oddíl naformátovaný souborovým systémem FAT16. Pro pracovní účely bylo logickému disku znalcem v operačním systému přiřazeno označení „G:“.

Dále jsou zadokumentovány zjištěné informace:

| **disk & part INFO** | |
|---|---|
| **disk:** | Storage USB Device |
| **kapacita:** | 70,6 MB |
| --- | --- |
| **počet partition:** | 1 |
| --- | --- |
| **číslo partition:** | 0 |
| **velikost:** | 73,71 MB |
| **bootovací:** | ano |
| **logický disk:** | G: |
| **file systém:** | FAT16 |
| **jmenovka svazku:** | DV |
| **obsazenost:** | 864 kB / 73,69 MB |

### *2.2.3.3 Diskový subsystém paměťové karty*

Zkoumaná paměťová karta obsahuje jeden primární oddíl naformátovaný souborovým systémem FAT32. Pro pracovní účely bylo logickému disku znalcem v operačním systému přiřazeno označení „I:“.

Dále jsou zadokumentovány zjištěné informace:

| **disk & part INFO** | |
|---|---|
| **disk:** | Storage USB Device |
| **kapacita:** | 7,42 GB |
| ---------- | ---------- |
| **počet partition:** | 1 |
| ---------- | ---------- |
| **číslo partition:** | 0 |
| **velikost:** | 7,42 GB |
| **bootovací:** | ne |
| **logický disk:** | I: |
| **file systém:** | FAT32 |
| **jmenovka svazku:** | neuvedeno |
| **obsazenost:** | 320 kB / 7,41 GB |

### *2.2.3.4 Výpis adresářové struktury (výpis souborů)*

Na disku DVD-R, tvořícím přílohu tohoto znaleckého posudku, jsou v adresáři „*Výpisy_dat*“ uloženy tyto soubory, jejichž obsahem je výpis všech souborů, které se na zkoumaných zařízeních nacházely.

| soubor | délka (B) | hash |
|---|---|---|
| Stopa2_kamera.txt | 1094 B | fd5262ecf0b00aeef7c3c4f782e46544 |
| Stopa2_Karta.txt | 1095 B | b1ac63eb12c5c563520a8dd5b41a5128 |

### *2.2.3.5 Vytvoření bitové kopie*

Zkoumaný pevný disk byl připojen k počítači znalce, kde byla vytvořena jeho bitová kopie. Výsledný soubor *„Stopa1.dd“* byl pro možnosti dalšího šetření umístěn na přílohový pevný disk, který tvoří přílohu tohoto znaleckého posudku, do složky *„3316-10“.*

### *2.2.3.6 Vyhledávání v existujících souborech*

#### 2.2.3.6.1 Vyhledávání v textových souborech

V následující etapě znaleckého zkoumání byly vyhledávány a prozkoumány veškeré textové soubory. Vyhledávání bylo realizováno manuálním procházením adresářové struktury a vyhledáváním textových souborů. Vyhledávány byly zejména dokumenty datových formátů doc, xls, pdf, odt, ods, rtf, htm a další. Textové soubory byly rovněž vyhledávány v archivech.

V následující tabulce je uvedeno celkové množství prohledávaných textových souborů, uložených v existujících datech na zkoumaných zařízeních:

**Videokamera:**

| .txt |
|---|
| 1 |

**Paměťová karta:**

| .txt |
|---|
| 1 |

Ve zkoumaných zařízeních nebyly nalezeny žádné uživatelské textové soubory.

#### 2.2.3.6.2 Vyhledávání v grafických souborech

Dále byly znalcem vyhledávány a prozkoumávány veškeré grafické soubory. Vyhledávání bylo realizováno manuálním procházením adresářové struktury a vyhledáváním uživatelských grafických souborů.

Ve zkoumaných zařízeních nebyly nalezeny žádné grafické soubory.

#### 2.2.3.6.3 Vyhledávání v audiovizuálních souborech

Dále byly znalcem vyhledávány a prozkoumávány veškeré audiovizuální soubory. Vyhledávání bylo realizováno manuálním procházením adresářové struktury a vyhledáváním uživatelských audiovizuálních souborů.

Ve zkoumaných zařízeních nebyly nalezeny žádné audiovizuální soubory.

### *2.2.3.7 Vyhledávání v obnovených souborech*

Před vlastním začátkem znaleckého zkoumání byla u videokamery a paměťové karty provedena obnova dat způsobem principiálně shodným s postupem popsaným v kapitole 2.1.5 tohoto znaleckého posudku. Tímto způsobem bylo získáno celkem 54 obnovených souborů o celkové kapacitě 11,2 GB.

Další analýzou všech obnovených dat byly zaznamenány soubory, u kterých byla programem pro obnovu dříve smazaných dat chybně detekována přípona souboru. Z tohoto důvodu byla dalším krokem znalce validace všech obnovených dat, s cílem získat veškeré takové obnovené soubory. Následně byly vyhledávány soubory relevantní pro vyšetřování dané věci.

#### 2.2.3.7.1 Vyhledávání v obnovených textových souborech

Znalcem byly vyhledávány a prozkoumány veškeré obnovené textové soubory. Vyhledávání bylo realizováno manuálním procházením a vyhledáváním textových souborů. Vyhledávány byly zejména dokumenty datových formátů doc, xls, pdf, odt, ods, rtf, htm a další. Textové soubory byly rovněž vyhledávány v archivech.

Ze zkoumaných zařízení nebyly obnoveny žádné dříve smazané textové soubory.

#### 2.2.3.7.2 Vyhledávání v obnovených grafických souborech

Znalcem byly vyhledávány a prozkoumány veškeré obnovené grafické soubory. Vyhledávání bylo realizováno manuálním procházením a vyhledáváním grafických souborů. Grafické soubory byly rovněž vyhledávány v archivech.

V následující tabulce je uvedeno celkové množství prohledávaných souborů, které byly obnoveny ze zkoumaných zařízení:

| .jpg |
|---|
| 81 |

Znalec prozkoumal veškeré obnovené grafické soubory. Na zkoumaném flashdisku nebyly obnoveny žádné funkční uživatelské grafické soubory.

#### 2.2.3.7.3 Vyhledávání v obnovených audiovizuálních souborech

Znalcem byly vyhledávány a prozkoumány veškeré obnovené audiovizuální soubory. Vyhledávání bylo realizováno manuálním procházením a vyhledáváním audiovizuálních souborů.

Ze zkoumaných zařízení nebyly obnoveny žádné dříve smazané audiovizuální soubory.

### *2.2.4 Stopa č. 3 – Flash disk zn. Verbatim*

Zkoumaný flashdisk byl v opatření k tomuto znaleckému posudku popsán následovně: **Flashdisk Verbatim - stopa č. 3, orgatech č. 00019056**


*Fotografie zkoumaného USB flashdisku, pořízené znalcem*

### *2.2.4.1 Zajištění proti neoprávněné manipulaci*

USB flashdisk byl ke zkoumání předán v neporušeném bezpečnostním sáčku PČR číslo 00019056. Zabezpečení bránilo připojení flashdisku k PC.

Zabezpečení USB flashdisku dokládají následující fotografie:


*fotografie zajištění, pořízené znalcem*

### 2.2.4.2 Diskový subsystém flashdisku

Zkoumaný USB flashdisk obsahuje jeden primární oddíl naformátovaný souborovým systémem FAT16. Pro pracovní účely bylo logickému disku znalcem v operačním systému přiřazeno označení „G:“.

Dále jsou zadokumentovány zjištěné informace:

| **disk & part INFO** | |
|---|---|
| **disk:** | Verbatim STORE N GO USB Device |
| **kapacita:** | 1,86 GB |
| **rozhraní:** | USB |
| ---------- | ---------- |
| **počet partition:** | 1 |
| ---------- | ---------- |
| **číslo partition:** | 0 |
| **velikost:** | 1,86 GB |
| **bootovací:** | ne |
| **logický disk:** | G: |
| **file systém:** | FAT16 |
| **jmenovka svazku:** | STORE N GO |
| **obsazenost:** | 109,47 MB / 1,86 GB |

### 2.2.4.3 Výpis adresářové struktury (výpis souborů na flashdisku)

Na disku DVD-R, tvořícím přílohu tohoto znaleckého posudku, je v adresáři „*Výpisy_dat*“ uložen tento soubor, jehož obsahem je výpis všech souborů, které se na flashdisku nacházely.

| soubor | délka (B) | hash |
|---|---|---|
| Stopa3_flashdisk.txt | 68123 B | dda316567615d38ae1b6036f6741c1ed |

### 2.2.4.4 Vytvoření bitové kopie

Zkoumaný flashdisk byl připojen k počítači znalce, kde byla vytvořena jeho bitová kopie. Výsledný soubor *„Stopa3.dd“* byl pro možnosti dalšího šetření umístěn na přílohový pevný disk, který tvoří přílohu tohoto znaleckého posudku, do složky *„3316-10“.*

### 2.2.4.5 Zdokumentování programového vybavení

Na zkoumaném flashdisku nebylo nalezeno žádné programové vybaveni.

### *2.2.4.6 Vyhledávání v existujících souborech*

#### 2.2.4.6.1 Zpracování elektronické pošty

Dalším krokem znaleckého zkoumání bylo zjistit, zda zkoumaný USB flashdisk obsahuje soubory obsahující zprávy, případně zajistit vykopírování veškerých takových souborů (zpráv) pro další šetření.

Prohlídkou obsahu flashdisku nebyly zaznamenány žádné typy souborů obsahující elektronickou poštu.

#### 2.2.4.6.2 Komunikační programy

V této kapitole znaleckého zkoumání byly v obsahu USB flashdisku vyhledávány datové soubory obsahující on-line komunikaci. Jedná se např. o datové soubory software využívající pro práci protokoly ICQ, Jabber, Skype apod., přičemž cílem takového zkoumání bylo nalezení a vyhodnocení případně uložené historie takové komunikace.

Prohlídkou obsahu flashdisku nebyly zaznamenány žádné typy souborů obsahující historii komunikace vedenou za pomoci programů pro instant messaging.

#### 2.2.4.6.3 Vyhledávání v textových souborech

V následující etapě znaleckého zkoumání byly vyhledávány a prozkoumány veškeré textové soubory. Vyhledávání bylo realizováno manuálním procházením adresářové struktury a vyhledáváním textových souborů. Vyhledávány byly zejména dokumenty datových formátů doc, xls, pdf, odt, ods, rtf, htm a další. Textové soubory byly rovněž vyhledávány v archivech.

Na zkoumaném USB flashdisku nebyly nalezeny žádné textové soubory.

#### 2.2.4.6.4 Vyhledávání v grafických souborech

Dále byly znalcem vyhledávány a prozkoumávány veškeré grafické soubory. Vyhledávání bylo realizováno manuálním procházením adresářové struktury a vyhledáváním uživatelských grafických souborů.

Na zkoumaném USB flashdisku nebyly nalezeny žádné textové soubory.

#### 2.2.4.6.5 Vyhledávání v audiovizuálních souborech

Dále byly znalcem vyhledávány a prozkoumávány veškeré audiovizuální soubory. Vyhledávání bylo realizováno manuálním procházením adresářové struktury a vyhledáváním uživatelských audiovizuálních souborů.

Na zkoumaném USB flashdisku nebyly nalezeny žádné audiovizuální soubory.

### *2.2.4.7 Vyhledávání v obnovených souborech*

Před vlastním začátkem znaleckého zkoumání byla na flashdisku provedena obnova dat způsobem principiálně shodným s postupem popsaným v kapitole 2.1.5 tohoto znaleckého posudku. Tímto způsobem bylo získáno celkem 532 obnovených souborů o celkové kapacitě 8,25 GB.

Další analýzou všech obnovených dat byly zaznamenány soubory, u kterých byla programem pro obnovu dříve smazaných dat chybně detekována přípona souboru. Z tohoto důvodu byla dalším krokem znalce validace všech obnovených dat, s cílem získat veškeré takové obnovené soubory. Následně byly vyhledávány soubory relevantní pro vyšetřování dané věci.

#### 2.2.4.7.1 Zpracování elektronické pošty

Dalším krokem znaleckého zkoumání bylo zjistit, zda se mezi obnovenými soubory nacházejí datové soubory obsahující e-mailovou komunikaci.

Ze zkoumaného flashdisku nebyly obnoveny žádné funkční soubory obsahující zprávy poštovních klientů (programů sloužících pro příjem a odesílání elektronické pošty).

#### 2.2.4.7.2 Komunikační programy

V této kapitole znaleckého zkoumání byly mezi obnovenými soubory vyhledávány datové soubory programů umožňující on-line komunikaci (tzv. instant messaging). Jedná se např. o software využívající pro práci protokoly ICQ, Jabber, Skype apod., přičemž cílem takového zkoumání bylo nalezení a zpracování případně uložené historie takové komunikace.

Ze zkoumaného flashdisku nebyly obnoveny žádné datové soubory obsahující historii komunikace skrze instant messaging programy.

#### 2.2.4.7.3 Vyhledávání v obnovených textových souborech

Znalcem byly vyhledávány a prozkoumány veškeré obnovené textové soubory. Vyhledávání bylo realizováno manuálním procházením a vyhledáváním textových souborů. Vyhledávány byly zejména dokumenty datových formátů doc, xls, pdf, odt, ods, rtf, htm a další. Textové soubory byly rovněž vyhledávány v archivech.

V následující tabulce je uvedeno celkové množství prohledávaných souborů, které byly obnoveny ze zkoumaného flashdisku.

| .txt |
|---|
| 463 |

Znalec prozkoumal veškeré obnovené textové soubory. Na zkoumaném flashdisku nebyly obnoveny žádné funkční uživatelské textové soubory.

#### 2.2.4.7.4 Vyhledávání v obnovených grafických souborech

Znalcem byly vyhledávány a prozkoumány veškeré obnovené grafické soubory. Vyhledávání bylo realizováno manuálním procházením a vyhledáváním grafických souborů. Grafické soubory byly rovněž vyhledávány v archivech.

Ze zkoumaného flashdisku nebyly obnoveny žádné dříve smazané grafické soubory.

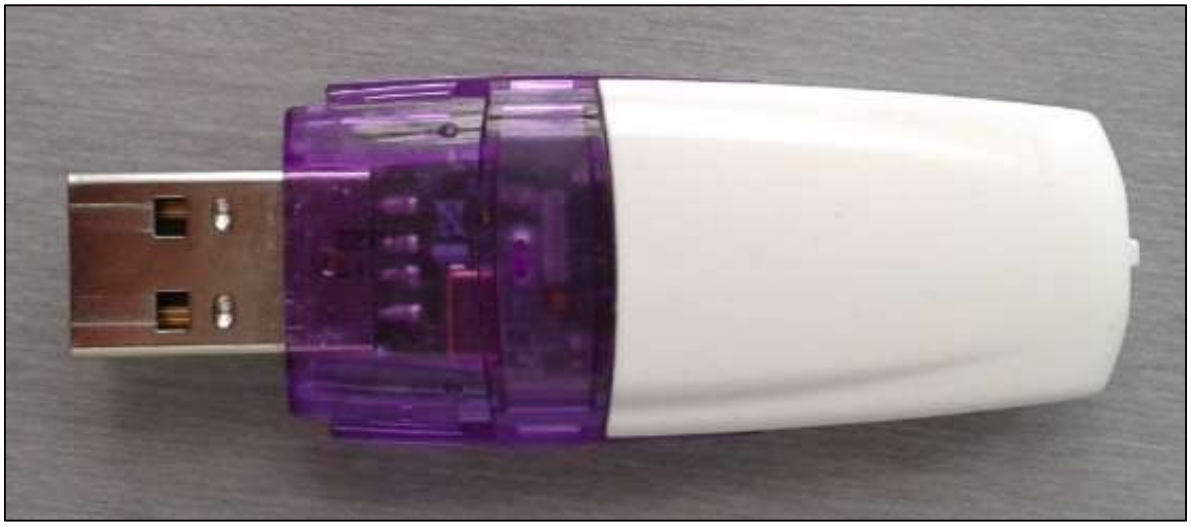
#### 2.2.4.7.5 Vyhledávání v obnovených audiovizuálních souborech

Znalcem byly vyhledávány a prozkoumány veškeré obnovené audiovizuální soubory. Vyhledávání bylo realizováno manuálním procházením a vyhledáváním audiovizuálních souborů.

Ze zkoumaného flashdisku nebyly obnoveny žádné dříve smazané audiovizuální soubory.

### *2.2.5 Stopa č. 4 – Flash disk Jet Flash 8GB*

Zkoumaný flashdisk byl v opatření k tomuto znaleckému posudku popsán následovně: **Flash disk Jetflash 8 GB - stopa č. 4, orgatech č. 00019055**

*Fotografie zkoumaného USB flashdisku, pořízené znalcem*

### *2.2.5.1 Zajištění proti neoprávněné manipulaci*

USB flashdisk byl ke zkoumání předán v neporušeném bezpečnostním sáčku PČR číslo 00019055. Zabezpečení bránilo připojení flashdisku k PC.

Zabezpečení USB flashdisku dokládají následující fotografie:


*fotografie zajištění, pořízené znalcem*

### 2.2.5.2 Diskový subsystém USB disku

Zkoumaný USB flashdisk obsahuje jeden primární oddíl naformátovaný souborovým systémem FAT32. Pro pracovní účely bylo logickému disku znalcem v operačním systému přiřazeno označení „G:“.

Dále jsou zadokumentovány zjištěné informace:

| **disk & part INFO** | |
|---|---|
| **disk:** | JetFlash Transcend 8GB USB Device |
| **kapacita:** | 7,48 GB |
| **rozhraní:** | USB |
| ---------- | ---------- |
| **počet partition:** | 1 |
| ---------- | ---------- |
| **číslo partition:** | 0 |
| **velikost:** | 7,48 GB |
| **bootovací:** | ne |
| **logický disk:** | G: |
| **file systém:** | FAT32 |
| **jmenovka svazku:** | PEACE |
| **obsazenost:** | 1,64 GB / 7,48 GB |

### 2.2.5.3 Výpis adresářové struktury (výpis souborů na flashdisku)

Na disku DVD-R, tvořícím přílohu tohoto znaleckého posudku, je v adresáři „*Vypisy_dat*“ uložen tento soubor, jehož obsahem je výpis všech souborů, které se na flashdisku nacházely.

| soubor | délka (B) | hash |
|---|---|---|
| Stopa4_flashdisk.txt | 158093 B | 3483c5f435c865024ba38a343c4eaad3 |

### 2.2.5.4 Vytvoření bitové kopie

Zkoumaný flashdisk byl připojen k počítači znalce, kde byla vytvořena jeho bitová kopie. Výsledný soubor *„Stopa4.dd“* byl pro možnosti dalšího šetření umístěn na přílohový pevný disk, který tvoří přílohu tohoto znaleckého posudku, do složky *„3316-10“.*

### 2.2.5.5 Zdokumentování programového vybavení

Na zkoumaném flashdisku nebylo nalezeno žádné programové vybaveni.

### *2.2.5.6 Vyhledávání v existujících souborech*

#### 2.2.5.6.1 Zpracování elektronické pošty

Dalším krokem znaleckého zkoumání bylo zjistit, zda zkoumaný USB flash disk obsahuje soubory obsahující zprávy, případně zajistit vykopírování veškerých takových souborů (zpráv) pro další šetření.

Prohlídkou obsahu flashdisku nebyly zaznamenány žádné typy souborů obsahující elektronickou poštu.

#### 2.2.5.6.2 Komunikační programy

V této kapitole znaleckého zkoumání byly v obsahu USB flash disku vyhledávány datové soubory obsahující on-line komunikaci. Jedná se např. o datové soubory software využívající pro práci protokoly ICQ, Jabber, Skype apod., přičemž cílem takového zkoumání bylo nalezení a vyhodnocení případně uložené historie takové komunikace.

Prohlídkou obsahu flashdisku nebyly zaznamenány žádné typy souborů obsahující historii komunikace vedenou za pomoci programů pro instant messaging.

#### 2.2.5.6.3 Vyhledávání v textových souborech

V následující etapě znaleckého zkoumání byly vyhledávány a prozkoumány veškeré textové soubory. Vyhledávání bylo realizováno manuálním procházením adresářové struktury a vyhledáváním textových souborů. Vyhledávány byly zejména dokumenty datových formátů doc, xls, pdf, odt, ods, rtf, htm a další. Textové soubory byly rovněž vyhledávány v archivech.

V následující tabulce je uvedeno celkové množství prohledávaných textových souborů, uložených v existujících datech na zkoumaném USB flashdisku:

| .doc | .docx | .htm | .ods | .odt | .pdf | .rtf | .txt | .xls | .xlsx |
|---|---|---|---|---|---|---|---|---|---|
| 81 | 92 | 1 | 5 | 15 | 343 | 3 | 8 | 231 | 103 |

Veškeré uživatelské textové dokumenty nalezené na flashdisku byly pro možnosti případného dalšího šetření uloženy na přílohový disk DVD-R do složky *„Uživatelská_data\stopa_4\exist\“* tak, aby jejich umístění odpovídalo původní adresářové struktuře.

#### 2.2.5.6.4 Vyhledávání v grafických souborech

Dále byly znalcem vyhledávány a prozkoumávány veškeré grafické soubory. Vyhledávání bylo realizováno manuálním procházením adresářové struktury a vyhledáváním uživatelských grafických souborů.

V následující tabulce je uvedeno celkové množství prohledávaných grafických souborů:

| .jpg | .png | .tif | .tiff |
|---|---|---|---|
| 62 | 4 | 27 | 5 |

Veškeré uživatelské grafické dokumenty nalezené na flashdisku byly pro možnosti případného dalšího šetření uloženy na přílohový disk DVD-R do složky *„Uživatelská_data\stopa_4\exist\“* tak, aby jejich umístění odpovídalo původní adresářové struktuře.

#### 2.2.5.6.5 Vyhledávání v audiovizuálních souborech

Dále byly znalcem vyhledávány a prozkoumávány veškeré audiovizuální soubory. Vyhledávání bylo realizováno manuálním procházením adresářové struktury a vyhledáváním uživatelských audiovizuálních souborů.

Na zkoumaném USB flashdisku nebyly nalezeny žádné audiovizuální soubory.

### *2.2.5.7 Vyhledávání v obnovených souborech*

Před vlastním začátkem znaleckého zkoumání byla u flashdisku provedena obnova dat způsobem principiálně shodným s postupem popsaným v kapitole 2.1.5 tohoto znaleckého posudku. Tímto způsobem bylo získáno celkem 100 obnovených souborů o celkové kapacitě 16,1 MB.

Další analýzou všech obnovených dat byly zaznamenány soubory, u kterých byla programem pro obnovu dříve smazaných dat chybně detekována přípona souboru. Z tohoto důvodu byla dalším krokem znalce validace všech obnovených dat, s cílem získat veškeré takové obnovené soubory. Následně byly vyhledávány soubory relevantní pro vyšetřování dané věci.

#### 2.2.5.7.1 Zpracování elektronické pošty

Dalším krokem znaleckého zkoumání bylo zjistit, zda se mezi obnovenými soubory nacházejí datové soubory obsahující e-mailovou komunikaci.

Ze zkoumaného flashdisku nebyly obnoveny žádné funkční soubory obsahující zprávy poštovních klientů (programů sloužících pro příjem a odesílání elektronické pošty).

#### 2.2.5.7.2 Komunikační programy

V této kapitole znaleckého zkoumání byly mezi obnovenými soubory vyhledávány datové soubory programů umožňující on-line komunikaci (tzv. instant messaging). Jedná se např. o software využívající pro práci protokoly ICQ, Jabber, Skype apod., přičemž cílem takového zkoumání bylo nalezení a zpracování případně uložené historie takové komunikace.

Ze zkoumaného flashdisku nebyly obnoveny žádné datové soubory obsahující historii komunikace skrze instant messaging programy.

#### 2.2.5.7.3 Vyhledávání v obnovených textových souborech

Znalcem byly vyhledávány a prozkoumány veškeré obnovené textové soubory. Vyhledávání bylo realizováno manuálním procházením a vyhledáváním textových souborů. Vyhledávány byly zejména dokumenty datových formátů doc, xls, pdf, odt, ods, rtf, htm a další. Textové soubory byly rovněž vyhledávány v archivech.

V následující tabulce je uvedeno celkové množství prohledávaných souborů, které byly obnoveny ze zkoumaného flashdisku.

| .pdf |
|---|
| 18 |

Veškeré obnovené funkční uživatelské textové dokumenty nalezené v obnovených datech byly pro možnosti případného dalšího šetření uloženy na přílohový disk DVD-R do složky *„Uživatelská_data\stopa_4\obn\“* tak, aby jejich umístění odpovídalo obnovené adresářové struktuře.

#### 2.2.5.7.4 Vyhledávání v obnovených grafických souborech

Znalcem byly vyhledávány a prozkoumány veškeré obnovené grafické soubory. Vyhledávání bylo realizováno manuálním procházením a vyhledáváním grafických souborů. Grafické soubory byly rovněž vyhledávány v archivech.

Ze zkoumaného flashdisku nebyly obnoveny žádné dříve smazané grafické soubory.

#### 2.2.5.7.5 Vyhledávání v obnovených audiovizuálních souborech

Znalcem byly vyhledávány a prozkoumány veškeré obnovené audiovizuální soubory. Vyhledávání bylo realizováno manuálním procházením a vyhledáváním audiovizuálních souborů.

Ze zkoumaného flashdisku nebyly obnoveny žádné dříve smazané audiovizuální soubory.

## 2.3 Struktura a obsah přílohového média (příloha znaleckého posudku)

DVD-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) |
| **Výpisy_dat** | Tento adresář obsahuje textové soubory, které dokumentují soubory a adresáře, obsažené na zkoumaných stopách. |
| **Uživatelská_data** | Adresář, ve kterém jsou umístěny uživatelské soubory, které byly nalezeny na zkoumaných stopách. |
| **md5.exe** | Soubor, umožňující provedení kontroly neporušenosti textových souborů s výpisem adresářové struktury.<br>Použití: md5.exe <jméno_souboru><br>Výstupem programu je textový řetězec (hash), který je nutné porovnat s údajem, vytištěným v nálezové části posudku. |

# 3 Závěr

1. **Provést základní prohlídku a popis předložených osobních PC a notebooků se zaměřením na technická data a výrobní čísla.**

   Znalcem byla provedena základní prohlídka předložených zařízení. Zjištěné informace jsou zadokumentovány v nálezové části tohoto znaleckého posudku.

2. **Zpřístupnit veškerá data a provést zálohu pevných disků přiložených PC a notebooků.**

   V obsahu zkoumaných zařízení byly po dohodě s policejním orgánem vyhledávány veškeré uživatelské textové, grafické a audiovizuální soubory. Nalezené soubory byly vykopírovány, pro případ dalšího šetření, na přílohový DVD-R disk do adresáře „*Uživatelská_data*“ v původní adresářové struktuře.

3. **Zjistit programové vybavení jednotlivých zařízení.**

   U všech zkoumaných paměťových médií byl proveden výpis veškerého software, který se na zkoumaných stopách v době znaleckého zkoumání nacházel. Nalezený software byl rozdělen na volně šiřitelný a komerční. Výsledky zkoumání jsou uvedeny v kapitolách s názvem „*Zdokumentování programového vybavení*“ tohoto znaleckého posudku.

4. **Provést základní prohlídku a popis a ověřit funkčnost předložených mobilních telefonů a tabletů**

   V této části znaleckého posudku označeného číslem 3316-10, byly zkoumány zajištěné věci obsahující výpočetní techniku.

5. **Zpřístupnit veškerá data a provést zálohu předložených mobilních telefonů a tabletů včetně přiložených SIM karet a paměťových karet k nim.**

   V této části znaleckého posudku označeného číslem 3316-10, byly zkoumány zajištěné věci obsahující výpočetní techniku.

6. **Provést základní prohlídku a popis předložených paměťových zařízení (přehrávače, externí disky, flash disky, paměťové karty, videokamery, apod.).**

   Znalcem byla provedena základní prohlídka předložených zařízení. Zjištěné informace jsou zadokumentovány v nálezové části tohoto znaleckého posudku.

7. **Zpřístupnit data a provést zálohu všech zařízení dle bodu č. 6.**

   V obsahu zkoumaných zařízení byly po dohodě s policejním orgánem vyhledávány veškeré uživatelské textové, grafické a audiovizuální soubory. Nalezené soubory byly vykopírovány, pro případ dalšího šetření, na přílohový DVD-R disk do adresáře *„Uživatelská_data“* v původní adresářové struktuře. Dále byly na žádost PČR u zkoumaných zařízení vytvořeny bitové kopie, jak je uvedeno v kapitole 2.1.1 tohoto znaleckého posudku.

8. **Provést základní prohlídku a popis předloženého serveru se zaměřením na administrátorská data, IP adresy, hesla, provedené změny a jeho obsah.**

   V této části znaleckého posudku označeného číslem 3316-10, nebyl zkoumán předložený server.

9. **Zpřístupnit veškerá data a provést zálohu předloženého serveru.**

   V této části znaleckého posudku označeného číslem 3316-10, nebyl zkoumán předložený server.

10. **Uvést veškeré další skutečnosti, jež vyplynou ze znaleckého zkoumání a mohou přispět k objektivnímu posouzení věci.**

    Po dohodě s policejním orgánem byla dále u zkoumaných stop provedena jejich bitová kopie, jak je uvedeno v kapitole 2.1.1 tohoto znaleckého posudku. Obnovené, dříve smazané, soubory byly, po dohodě s policejním orgánem, znalcem prohledávány a zpřístupněny veškeré funkční uživatelské soubory. Tyto jsou pro možnosti případného dalšího šetření umístěny na přílohový DVD-R disk do adresáře *„Uživatelská_data/obn/“*.

# 4 Znalecká doložka

Znalecký posudek byl zpracován ve dnech 18. 5. 2015 – 1. 9. 2015.
Technické úkony byly realizovány pracovníky znalecké kanceláře.
Posudek je vyhotoven ve třech kopiích – Výtisk č. 1 a 2 pro POLICII ČR, útvar pro odhalování organizovaného zločinu, SKPV, poštovní schránka 41/V5, Praha 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 3316-10 znaleckého deníku.

Znalečné a náhradu nákladů účtuji podle připojené likvidace.

Znalec si je vědom následků vědomě nepravdivého znaleckého posudku.

**Ing. Jan Janka**