Zajišťování a analýza digitálních důkazů

Survey and Analysis of Digital Evidence

Bc. Ladislav Vyskočil

Diplomová práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Ladislav Vyskočil**
Osobní číslo:	**A11515**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Forma studia:	**kombinovaná**
Téma práce:	**Zajišťování a analýza digitálních důkazů**

Zásady pro vypracování:

1. **Zpracujte úvod do problematiky digitálních důkazů.**
2. **Popište způsoby a metody zajišťování digitálních důkazů na místě činu.**
3. **Specifikujte postupy a způsoby vytváření bitových kopií digitálních stop.**
4. **Určete metody autentizace bitových kopií digitálních stop.**
5. **Zpracujte postupy a způsoby forenzní analýzy digitálních dat.**
6. **Popište možná ohrožení a rizika při procesu práce s digitálními stopami.**
7. **Navrhněte protiopatření pro zmírnění nebo odstranění možných rizik při práci s digitálními stopami.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Risk Analysis Consultants s.r.o. Forenzní zkoumání digitálních důkazů – Příručka vyšetřovatele. Praha, 2005. Dostupný z: http://www.rac.cz/rac/homepage.nsf/CZ/883AABB42333CB35C12570FC0034A328.**
2. **Kothánek, J. Zajišťování výpočetní techniky a dat pro potřeby důkazního řízení. Policie ČR, Praha, 2006.**
3. **Formánek Martin. Forenzní analýza digitálních nosičů dat pro počítače. Praha 2008. Bakalářská práce. ČVUT FEL. Dostupný z: https://dip.felk.cvut.cz/browse/pdfcache/formam1_2008bach.pdf.**
4. **Porada Viktor, Roman Rak. Digitální stopy v kriminalistice a forenzních vědách. Soudní inženýrství č.17, 2006.**
5. **Porada Viktor, Roman Rak. Teorie digitálních stop a její aplikace v kriminalistice a forenzních vědách. Karlovarská právní revue č.4, 2006.**
6. **Formánek Martin. Metodika zajištování důkazů při vyšetřování počítačové kriminality – FORENZNÍ ANALÝZA POČÍTAČE. Praha 2007. Semestrální projekt. ČVUT FEL. Dostupný z: http://service.felk.cvut.cz/anc/ofa/pub/doc/metodika.pdf.**
7. **Kadlec Josef. Forenzní analýza unixových systémů. Hradec Králové 2006. Diplomová práce. UHK FIM. Dostupný z: http://www.root.cz/knihy/forenzni-analyza-unixovych-systemu.**

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

Datum zadání diplomové práce: **22. února 2013**

Termín odevzdání diplomové práce: **22. května 2013**

Ve Zlíně dne 22. února 2013

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Roman Jašek, Ph.D.
ředitel ústavu

ABSTRAKT

Tato diplomová práce se zabývá problematikou zajišťování a analyzování digitálních důkazů. V úvodu této práce je uvedeno seznámení s problematikou digitálních důkazů a základní principy práce s těmito důkazy. V teoretické části je popsáno zajišťování digitálních důkazů na místě činu a právní aspekty těchto úkonů, dále jsou zde popsány postupy forenzního vytváření bitových kopií zajištěných digitálních stop a jejich autentizace. Jako poslední jsou v této části uvedeny i následné forenzní analýzy digitálních dat. Teoretická část přibližuje pojmy jako digitální stopa a její autentizace, bitová kopie digitální stopy a důvody jejího vytváření, kriminalisticko-technická činnost, činnost znalců a princip provádění forenzních analýz digitálních dat. V praktické části jsou uvedeny nejčastější postupy při zajišťování digitálních stop a nejčastější metody při provádění forenzních analýz digitálních dat. V závěru této práce jsou popsána možná ohrožení a rizika při práci s digitálními stopami a navržena vhodná protiopatření pro zmírnění, nebo odstranění těchto rizik.

Klíčová slova: Digitální stopa, Bitová kopie digitální stopy, Autentizace digitálních stop, Forenzní analýza digitálních dat, Znalecká činnost, Místo činu, Disk Doubler, HW Blokátor zápisu, Hash, MD5, SHA-1, SHA-2.

ABSTRACT

This thesis deals with securing and analyzing digital evidence. At the beginning of this work can be find the issue of digital evidence and the basic principles of working with such evidence. The theoretical section describes securing digital evidence at the crime scene and the legal aspects of these operations, then there are depicted forensic imaging of secured digital evidence and authentication. The last in this section are mentioned the subsequent forensic analysis of digital data. The theoretical part explains terms like digital evidence and its authentication, digital image and traces the reasons for its creation, forensic and technical activities, work of experts and implementation of the principle of forensic analysis of digital data. In the practical part there are shown the most frequent ways and procedures for securing digital evidence and the most common procedures and methods for carrying out forensic analysis of digital data. In conclusion, this study describes the potential hazards and risks when working with digital evidence and appropriate countermeasures designed to mitigate or eliminate these risks.

Keywords: Digital evidence, Image, Authentication digital evidence, Forensic analysis of digital data, expert activity, crime scene, Disk Doubler, hardware write blocker, Hash, MD5, SHA-1, SHA-2.

Děkuji Ing. Davidu Malaníkovi, Ph.D. za poskytnutí praktických rad a informací a za odborné vedení při realizaci této diplomové práce.

Motto:

Mezi dobrem a zlem je těžké hledat hranici.

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 s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- 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 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

OBSAH

ÚVOD DO PROBLEMATIKY DIGITÁLNÍCH DŮKAZŮ

Digitální technika v dnešním světě zasahuje do většiny oblastí lidského konání. Rychlým vývojem a snadnou dostupností se zařadila mezi běžné součásti našeho každodenního života. Každé technologické zařízení, které získává, uchovává, předává, nebo různými způsoby zpracovává elektronická data, zanechává záznamy o své činnosti. Takové záznamy jsou z kriminalistického hlediska stopami. Pro termíny digitální stopa a digitální důkaz existuje v angličtině pouze jeden termín „digital evidence“. Slovo „evidence“ má v angličtině primární význam „důkaz“, naproti tomu české slovo „stopa“ v souvislosti s moderními technologiemi v zahraniční literatuře nenalezneme. Je to z toho důvodu, že teorie i praxe jsou především orientovány na výsledek trestního procesu. Stopa musí být soudem akceptovatelná a tím prakticky dochází k automatickému ztotožnění pojmů stopa a důkaz.

K definování digitální stopy se v současnosti ve většině vyspělých států akceptuje definice, která byla v roce 1999 navržena pracovní skupinou SWGDE – Scientific Working Group on Digital Evidence:

„Digitální stopa je jakákoliv informace s vypovídající hodnotou, uložená nebo přenášená v digitální podobě“. [1]

Tato definice je obecně platná pro jakoukoliv digitální technologii a takto definovaná digitální stopa pokrývá nejen oblast počítačů a počítačové komunikace, ale i oblasti digitálních přenosů, mobilních telefonů, digitálních TV, audia, videa, digitálních fotografií, kamerových systémů, elektronických zabezpečovacích systémů, a mnoha dalších technologií potenciálně spojených s páchaním nějakého druhu trestné činnosti.

V dalších akceptovaných návrzích je digitální stopa definována jako data, dokazující spáchání trestného činu, nebo data, která dokazují vztah mezi spáchaným trestným činem a jeho obětí nebo trestním činem a pachatelem.

Zajištění digitálních stop je proces, který začíná okamžikem, kdy data obsahující relevantní informace, nebo zařízení, na kterých jsou taková data uložena, jsou zajištěna, nebo uložena pro znalecké zkoumání. Zajištění digitálních stop probíhá za předpokladu, že tyto stopy budou před soudními orgány akceptovány jako důkaz.[2]

Ve své podstatě jsou digitální stopy velmi křehké. Nevhodným zpracováním, nebo v průběhu, popřípadě i v procesu zkoumání, mohou být velice snadno poškozeny, změněny, nebo zničeny. Z tohoto důvodu musí být učiněna patřičná opatření, která zajistí v celém průběhu zkoumání původní sterilitu a integritu digitálních stop. Pokud by se takové opatření nedodrželo, mohlo by zkoumání digitálních stop vést k nepřesným závěrům, nebo by se digitální stopy mohly stát zcela nepoužitelnými. V praxi se toto opatření realizuje tzv. forenzní duplikací digitálního média, například vytvořením identické bitové kopie zajištěných datových médií, obsahujících digitální stopy a následné zkoumání pak probíhá na této kopii. Ve výjimečných případech může dojít k situaci, kdy nelze forenzní duplikaci média provést. V tomto případě, pokud je to možné, musíme dané médium nastavit tak, aby bylo použitelné pouze ke čtení a nebylo možné na něj zapisovat a tím digitální stopu znehodnotit.

Aby byla digitální stopa akceptovatelná soudem, je nutné již při jejím zajištění zabezpečit také její autentizaci, která kdykoliv prokazatelně potvrdí, že digitální stopa je shodná s původní zajištěnou stopou. Tím je zaručeno, že zajištěná digitální stopa nemůže být v průběhu vyšetřování jakkoliv modifikována, nebo zaměněna. Toto ověření pravosti musí být možné kdykoliv opakovat. V praxi se autentizace zajištěných dat řeší vypočtením jejich kontrolních otisků pomocí vhodné hašovací funkce, nebo zabalením a zapečetěním objektů, obsahující digitální stopy.

Po zajištění a autentizaci digitálních stop musí následovat také jejich zkoumání a vyhodnocení, které provádí soudní znalci při forenzních analýzách digitálních dat. Forenzní analýza digitálních dat se zabývá všemi oblastmi digitální technologie a za použití vědeckých metod provádí hodnocení, analýzy, identifikaci a interpretaci zkoumaných digitálních stop za účelem pomoci s objasněním vyšetřovaného případu. Z výsledků těchto analýz se znalci snaží nalézt odpovědi na otázky důležité pro daný případ. O výsledcích zkoumání digitálních stop pomocí forenzních analýz digitálních dat znalci vyhotovují písemný znalecký posudek, nebo odborné vyjádření. Pro trestní, nebo soudní řízení pak tento znalecký posudek slouží jako odborná interpretace informací získaných ze zajištěné digitální stopy, které se vztahují k vyšetřovanému případu.

Práce s digitálními stopami vyžaduje dodržení vysoké úrovně bezpečnostních opatření a vyžaduje také vysokou odbornost osob, které s digitálními stopami pracují. I při dodržení všech bezpečnostních pravidel a doporučených postupů však můžou nastat situace, při kterých hrozí ztráta, nebo zničení digitálních stop. Tyto rizika mohou být způsobeny

například selháním techniky, nebo selháním lidského faktoru. Proto je nutné tyto rizika včas identifikovat a vhodnými protiopatřeními je minimalizovat, nebo odstranit.

V dalším textu této diplomové práce budou podrobněji popsány jednotlivé etapy práce s digitálními stopami a nejčastější postupy, kterých se v těchto etapách využívá. Na závěr bude také uveden popis možných rizik a ohrožení, které při každé etapě práce s digitální stopou může hrozit a také vhodná protiopatření, kterými se tato rizika mírní.

I. TEORETICKÁ ČÁST

1 ZAJIŠŤOVÁNÍ DIGITÁLNÍCH STOP

Zajišťování digitálních stop je jedním z nejdůležitějších úkonů při vyšetřování počítačové kriminality, nebo vyšetřování trestných činů, ve kterých mají důležitou úlohu digitální informace. Jak již bylo v úvodu této práce zmíněno, zajištění digitálních stop je úkon, který začíná okamžikem, kdy data obsahující relevantní informace, nebo zařízení, na kterých jsou taková data uložena, jsou zajištěna, nebo uložena pro znalecké zkoumání. Celý proces zajištění digitálních stop probíhá za předpokladu, že tyto stopy budou před soudními orgány akceptovány jako důkaz, proto musí být celý proces přiměřený a legální pro práci s důkazním materiálem. Digitální stopy pro následné znalecké zkoumání jsou získávány mnoha způsoby. Zajišťují je nejčastěji orgány činné v trestním řízení prováděním úkonů podle trestního řádu, nebo dalšími legálními způsoby, které vedou k zajištění relevantních digitálních stop. Jedná se zejména o tyto úkony:

- domovní prohlídka,
- osobní prohlídka,
- prohlídka jiných prostor a pozemků,
- vydání, nebo odnětí věci,
- ohledání místa činu,
- kontrolní nákup ve spolupráci s českou obchodní inspekcí,
- zajištění dat z Internetu,
- a další úkony

Při zajišťování digitálních stop pro účely forenzní analýzy digitálních dat, které nemají souvislost s trestním řízením, musí být dodrženy všechny zákony a právní předpisy dané země a úkony lze provádět pouze se souhlasem vydávajícího, nebo na jeho objednávku. Jedná se například o provádění firemních softwarových auditů a podobně, kde zajištění digitálních stop ke zkoumání provádí znalecké pracoviště, které je ve smluvním vztahu se zadavatelem, který je zároveň vlastníkem vydávaných dat.

Následující text se bude zabývat zásadami a možnostmi zajišťování digitálních stop především pro potřeby trestního řízení.

1.1 Právní aspekty

Zajišťování digitálních stop pro potřeby trestního řízení se řídí podle trestního řádu, tzn. podle zákona 141/1961 Sb. o trestním řízení soudním. Dle tohoto zákona se zajišťování digitálních stop může provádět v rámci provádění domovní prohlídky, osobní prohlídky a prohlídky jiných prostor a pozemků podle § 82, případně dobrovolným vydáním, nebo odnětím věci podle § 78 a § 79 trestního řádu. Při získávání digitálních stop má nezastupitelnou úlohu také provádění ohledání místa činu, které je také právně zakotveno v zákoně 141/1961 Sb. o trestním řízení soudním.

1.1.1 Domovní prohlídka, osobní prohlídka a prohlídka jiných prostor

Provádění domovní prohlídky, osobní prohlídky a prohlídky jiných prostor a pozemků se řídí ustanovením § 82 trestního řádu. Domovní prohlídku lze vykonat, je-li důvodné podezření, že v bytě nebo jiné prostoře sloužící k bydlení nebo v prostorách k nim náležejících (obydlí) je věc nebo osoba důležitá pro trestní řízení. Ze stejného důvodu lze vykonat i prohlídku prostor nesloužících k bydlení (jiných prostor) a pozemků, pokud nejsou veřejně přístupné. Osobní prohlídku lze vykonat, je-li důvodné podezření, že někdo má u sebe věc důležitou pro trestní řízení.

Domovní prohlídku lze provést pouze na základě písemného příkazu k domovní prohlídce podle § 83 trestního řádu, vydaného předsedou senátu, nebo v přípravném řízení na návrh státního zástupce soudcem, který musí být odůvodněn. Domovní prohlídku vykonává policejní orgán.

Také provedení prohlídky jiných prostor a pozemků lze provést pouze na základě příkazu k prohlídce jiných prostor a pozemků podle § 83a trestního řádu a k nařízení je oprávněn předseda senátu. Příkaz musí být vydán písemně a musí být odůvodněn. Bez příkazu může policejní orgán provést prohlídku jiných prostor nebo pozemků, jestliže vydání příkazu nelze předem dosáhnout a věc nesnese odkladu. Policejní orgán je však povinen si bezodkladně dodatečně vyžádat souhlas orgánu oprávněného k vydání příkazu. Pokud oprávněný orgán souhlas dodatečně neudělí, nelze výsledek prohlídky použít v dalším řízení jako důkaz. Bez příkazu může policejní orgán provést prohlídku jiných prostor nebo pozemků také tehdy, pokud uživatel dotčených prostor nebo pozemků písemně prohlásí, že s prohlídkou souhlasí a své prohlášení předá policejnímu orgánu.

Osobní prohlídka se provádí na základě příkazu k osobní prohlídce podle § 83b trestního řádu. K jejímu nařízení je oprávněn předseda senátu a v přípravném řízení státní zástupce nebo s jeho souhlasem policejní orgán. Bez příkazu může policejní orgán vykonat osobní prohlídku jen tehdy, jestliže příkazu předem dosáhnout nelze a věc nesnese odkladu, nebo pokud jde o osobu přistiženou při činu.

Domovní prohlídky, osobní prohlídky a prohlídky jiných prostor a pozemků jsou citlivým zásahem do práv a svobod osob, proto, podle § 84 trestního řádu, před vlastním provedením některé z těchto prohlídek je nutné provést předchozí výslech osob, kterých se provedený úkon bude týkat. Pokud osoba na základě předchozího výslechu dobrovolně vydá hledanou věc, která je důležitá pro trestní řízení podle orgánů činných v trestním řízení, nelze pak již domovní prohlídku provést. Předchozího výslechu není třeba, jestliže věc nesnese odkladu a výslech nelze provést okamžitě.

Provedení domovní prohlídky a prohlídky jiných prostor a pozemků musí být přítomna i nezúčastněná osoba. Orgán vykonávající domovní prohlídku, nebo prohlídku jiných prostor musí umožnit účast při prohlídce osobě, u níž se prohlídka vykonává.

1.1.2 Vydání a odnětí věci

Kdo má u sebe věc důležitou pro trestní řízení, je podle § 78 trestního řádu povinen ji na vyzvání předložit soudu, státnímu zástupci nebo policejnímu orgánu a je-li ji nutno pro účely trestního řízení zajistit, je povinen věc na vyzvání těmto orgánům vydat. Při vyzvání je třeba ho upozornit na to, že nevyhoví-li výzvě, může mu být věc odňata, jakož i na jiné následky nevyhovění podle § 66. Vyzvat k vydání věci je oprávněn předseda senátu, v přípravném řízení státní zástupce nebo policejní orgán a to jak písemně, tak i ústně.

Nebude-li věc důležitá pro trestní řízení na vyzvání vydána tím, kdo ji má u sebe, může mu být na příkaz předsedy senátu a v přípravném řízení na příkaz státního zástupce, nebo policejního orgánu odňata podle § 79 trestního řádu. Policejní orgán potřebuje k vydání takového příkazu předchozí souhlas státního zástupce. Pokud věc nesnese odkladu, může být věc důležitá pro trestní řízení odejmuta policejním orgánem i bez předchozího souhlasu státního zástupce, například při hrozícím zničení věci. K odnětí věci se podle možnosti přibere osoba, která není na věci zúčastněna.

Při vydání, nebo odnětí věci vystavuje policejní orgán protokol o vydání a odnětí věci, který musí obsahovat dostatečně přesný popis vydané nebo odňaté věci, sloužící k její

jednoznačné identifikaci. Osobě, která věc vydala nebo jí byla věc odňata, vydá orgán, který úkon provedl, ihned písemné potvrzení o převzetí věci nebo opis protokolu.

1.1.3 Ohledání věci a místa činu

Ohledání je samostatný procesní úkon, který je rámcově upraven v hlavě V., oddíl sedmý, zákona č. 141/1961 Sb., o trestním řízení soudním, ve znění pozdějších předpisů, ale souvisí s ním i další ustanovení trestního řádu. Ohledání věci a místa činu patří mezi nejvýznamnější druhy ohledání. Provádění tohoto úkonu je zakotveno v § 158 a § 113 trestního řádu.

Za místo činu se považuje ta část prostoru, kde se uskutečnil proces, nebo děj, o kterém je možné podle jeho vnějších projevů předpokládat, že se jedná o proces protispolečenský a u něhož je třeba ohledáním zjistit a zajistit takové znaky jednání, podle nichž by bylo možné věrohodně posoudit, zda jde o trestný čin.

Místo činu je většinou výchozím bodem při vyšetřování a je také většinou jediným místem, kde je možno nalézt stopy potřebné pro objasnění případu. Z kriminalistického hlediska je to místo trestné činnosti pachatele.

Ohledání věci a místa činu je specifická kriminalistická metoda, která na základě přímého pozorování zkoumá, hodnotí a podchycuje materiální situace nebo stav objektů, které jsou důležité pro trestní řízení, za účelem jejího poznání a získání důkazů, jakož i dalších informací. K ohledání se zpravidla přibírá znalec.

Tento úkon má pevně dané zásady jako neodkladnost, neopakovatelnost, nezastupitelnost a řízení ohledání jediným odpovědným vedoucím.

Při provádění ohledání věci a místa činu musí být sepsán protokol o ohledání místa činu podle § 113 trestního řádu. Tento protokol musí poskytovat úplný a věrný obraz předmětu ohledání a jeho nedílnou součástí jsou přiložené fotografie, náčrty a jiné pomůcky.

1.2 Digitální stopa a Policie ČR

Zajišťování výpočetní techniky a dat patří mezi kriminalisticko-technické činnosti, které Policie České republiky provádí. Kriminalisticko-technická činnost je u Policie ČR upravena několika předpisy, zejména z důvodu zachování vysoké odborné úrovně při zajišťování a vyhodnocování kriminalisticky relevantních stop za účelem důkazního řízení

před soudy. Tyto předpisy určují, aby zajišťování stop z místa trestné činnosti prováděla osoba odborně způsobilá, která disponuje odpovídajícím oprávněním k této činnosti.

Zajišťování výpočetní techniky a dat upravují následující interní akty řízení:

- Závazný pokyn policejního prezidenta č. 100/2001 ke kriminalisticko-technické činnosti Policie ČR,
- Závazný pokyn policejního prezidenta č. 77/2009, kterým se upravuje věcná, funkční a místní příslušnost znaleckých pracovišť Policie ČR,
- Metodický pokyn ředitele KÚP č. 7/2001, kterým se upravuje činnost orgánů Policie ČR při zajišťování výpočetní techniky a dat pro účely následného znaleckého zkoumání.

V souladu s výše uvedenými interními akty řízení a Metodického pokynu ředitele KÚP č. 2/2003 se po absolvování příslušného školení a vykonání závěrečných zkoušek vydává pracovníkům Policie ČR zařazených na pracovištích KÚP, OKTE a SKPV „**Osvědčení o odborné způsobilosti k provádění kriminalisticko-technických úkonů při zajišťování výpočetní techniky a dat na místě činu**“. Uvedené osvědčení opravňuje jeho držitele k zajišťování výpočetní techniky a dat i k vytváření bitových kopií paměťových médií v rozsahu výše uvedených interních aktů řízení.

1.3 Příprava před zajištěním digitálních stop

Vlastní provádění úkonů zajišťování digitálních stop musí předcházet jejich příprava, která je k bezchybnému zajištění těchto stop velmi důležitá. Jelikož zajištění digitálních stop provádí většinou specialista vlastnící patřičné osvědčení k zajišťování digitálních stop, který se jinak nepodílí na vyšetřování případu, je nutné přípravu zajištění digitálních stop posuzovat z tohoto pohledu.

Příprava před zajištěním digitálních stop zahrnuje několik obecných kroků, které pokud to okolnosti dovolí, je doporučeno provést. Kroky přípravy jsou následující:

- Získání nutných a nezbytných informací o vyšetřovaném případu, kterého se úkon bude týkat. Z těchto informací lze vyvodit, jakým způsobem a jaké digitální stopy se mohou zajišťovat.
- Získání dostupných údajů o informačních a komunikačních technologiích, které se na místě zajištění digitálních stop mohou vyskytovat. Jedná se například

o rozmístění výpočetní techniky v objektu, počet PC a serverů, odhad datové kapacity, provozované operační systémy a aplikace, databázové systémy, strukturu počítačové sítě a další důležité technické informace. V tomto kroku zároveň získáváme informace o odbornosti personálu, správcích a administrátorech počítačů a sítí, použitých bezpečnostních technologiích, kryptografii apod.

- Vyhodnocení včasnosti úkonů vzhledem k digitálním stopám. Je doporučeno provádět úkony zajištění co nejdříve, protože od doby předpokládaného spáchání trestné činnosti může postupem času dojít ke ztrátě digitálních stop vymazáním, nebo přepsáním, například i běžným užíváním výpočetní techniky.
- Podle zjištěných informací je nutné připravit potřebné technické vybavení a materiál, který je nezbytný k předpokládanému provedení zajištění digitálních stop. Z technického vybavení se jedná hlavně o technologické PC, nebo duplikátory disků, které se používají na vytváření bitových kopií digitálních stop, dále potřebné nářadí a další technologické přípravky. Z materiálu k provedení zajištění digitálních stop to jsou zejména pevné disky pro uložení bitových kopií a dále obaly, ve kterých jsou zajištěné digitální stopy uloženy po jejich zajištění.
- Případné zajištění experta v daném oboru. Ve specifických případech, kdy je například použita některá nová technologie, nelze pokrýt celé její spektrum znalostmi specialisty na zajištění digitálních stop. V tomto případě je důvodná potřeba vše konzultovat s expertem v daném oboru, který by měl doporučit nejvhodnější postup, čímž se zamezí případným ztrátám, nebo znehodnocení digitálních stop.
- Zohlednění dopadů prováděných úkonů na obchodní, nebo jinou činnost komerčních firem a dalších organizací, nebo zásahu do práv třetích osob, které by při zajištění digitálních stop mohly být způsobeny. K minimalizaci těchto dopadů je nutné provést zhodnocení prostředí. Z důvodu zdlouhavého zajišťování a následného zkoumání digitálních stop je nutné rozhodnout, kde bude provedeno vytvoření bitových kopií těchto stop a následné zkoumání a analýzy. Obecně platí zásada, že zkoumání digitálních stop má probíhat v kontrolovaném prostředí specializované znalecké laboratoře. Když ale okolnosti případu vyžadují znalecké zkoumání digitálních stop na místě, je nutné zajistit přítomnost patřičného znalce a na celou situaci se co nejlépe připravit.

Do přípravy před zajištěním digitálních stop lze zahrnout i kriminalistické operativní úkony, za účelem možného zjištění přístupových hesel k počítačovým systémům, šifrovaným souborům, nebo ke zjištění dalších důležitých informací. Pokud to okolnosti dovolí, je velmi přínosné předem získat od správců sítí, případně administrátorů a uživatelů, důležité informace o informačních a databázových systémech, způsobech práce s nimi a jejich přístupové kódy. Jakékoliv předem získané informace následně usnadní a zjednoduší vlastní provedení úkonu zajištění digitálních stop.

1.4 Postupy na místě činu

Postupy při zajišťování digitálních stop jsou vždy závislé na prováděném úkonu, v jehož rámci se digitální stopy zajišťují. Každý úkon má své specifické postupy, pravidla a bezpečnostní opatření. Ať už se jedná o domovní prohlídku, prohlídku jiných prostor, o vydání, nebo odnětí věci, nebo o ohledání místa činu, musí se vždy postupovat v souladu s tímto prováděným úkonem. Nebudou zde uvedeny obecné postupy provádění těchto úkonů, ale následující text bude zaměřen jen na situace a přímé souvislosti se zajišťováním digitálních stop.

Ještě před zahájením provádění úkonů podle trestního řádu je nutné zvážit a vyhodnotit bezpečnostní rizika, které by mohly před i během provádění úkonu hrozit. Jedná se zejména o zabezpečení místa provádění úkonu a také bezpečnost personálu. Neměla by být opomíjena skutečnost, že úkony podle trestního řádu slouží k zajištění důkazů důležitých pro trestní řízení, proto všechny činnosti a pohyb na místě provádění úkonu by měly být vykonávány s co největší opatrností. Během provádění úkonů je nutné zamezit případnému úmyslnému, nebo nedbalostnímu zničení digitálních stop ze strany uživatelů, proto je nutné postupovat systematicky a koordinovaně. Velkou roli při prováděných úkonech hraje i moment překvapení, který riziko úmyslného zničení stop minimalizuje. U některých trestných činů a zejména při vyšetřování počítačové kriminality se musí předpokládat, že pachatel je kvalifikovaný odborník na výpočetní techniku. Z tohoto důvodu je nutné již předem naplánovat a zajistit situaci tak, aby při provádění úkonů byla výpočetní technika zabezpečena proti manipulaci jinou osobou, případně předpokládat další softwarová zabezpečení. V takových případech může s výpočetní technikou manipulovat pouze specialista na zajištění dat, protože neodbornou manipulací by mohlo být způsobeno zničení všech důležitých důkazů.

V praxi, z důvodu neodkladnosti, může nastat situace, ve které na místě činu provádějí první nezbytné kroky policisté, kteří nejsou speciálně proškoleni pro zajišťování digitálních důkazů. V tomto případě je po vykonání neodkladných úkonů, z důvodu správného zajištění důkazů, doporučeno přivolat specialisty. Zajištění digitálních stop bývá velmi složité a může jej provádět pouze policista s dostatečnou kvalifikací, nebo v případě vytváření bitových kopií digitálních stop policista, který je držitelem osvědčení o odborné způsobilosti k provádění kriminalisticko-technických úkonů při zajišťování výpočetní techniky a dat, nebo příslušný civilní soudní znalec, který je případně přizván. Činnosti na místě činu jsou vždy závislé na okolnostech a podmínkách a také na konkrétní výpočetní technice, která se na místě nachází. V případech informační kriminality je zajištění důkazů a digitálních stop jedním ze základních úkonů trestního řízení, a proto by měl tyto úkony řídit a koordinovat přímo vyšetřovatel případu.

Při zvažování právních aspektů při zajišťování důkazů, je nutné určit možné komplikace vzhledem k místnímu prostředí, a pokud jsou nalezeny i důkazy, které nespadají pod původní pověření, určit jaké další právní kroky mohou být zapotřebí k dalšímu zkoumání, například dodatečné zajištění soudního příkazu a podobně.

Pro provedení následné forenzní analýzy digitálních dat ve forenzní laboratoři soudního znalce, je nutné při provádění úkonů zjistit i následují informace, aniž by bylo prováděno zkoumání výpočetní techniky a dat:

- zjištění počtu a typů počítačů,
- zjištění používaných operační systémů,
- zjištění, jestli jsou počítače zapojeny do sítě, případně zjistit informace o této síti,
- vyslechnout správce systému a uživatele,
- zjištění a zaznamenání typů a množství záznamových médií, včetně přenosných a zdokumentovat místa, kde byla média nalezena,
- zjištění míst ukládání dat mimo místo činu, nebo vzdálená výpočetní centra,
- zjištění a případná identifikace speciálního software,
- zhodnocení obecného stavu místa.

Během provádění úkonů podle trestního řádu provádí vyšetřovatel, na doporučení specialisty na zajišťování dat, výběr objektů, které budou zajištěny k dalšímu znaleckému zkoumání.

Při výběru objektů k zajištění se současně provádí i zhodnocení důkazů podle následujících kritérií:

- určení priority důkazu,
- zjištění stavu důkazu a vliv způsobu zajištění, transportu a skladování na jeho stav,
- zhodnocení místa nálezu důkazu,
- zjištění stability zajišťovaného digitálního média,
- zhodnocení potřeby zásobovat zajištěné zařízení stálým napájením,
- zhodnocení negativních vlivů prostředí a elektromagnetického pole na důkaz,
- určení jak bude důkaz zadokumentován, zajištěn a zapečetěn.

V případě, že nelze objekt obsahující zájmová data zajistit, musí specialista na zajištění dat tyto data zajistit na místě, například vykopírováním na jiná záznamová média. K tomuto úkonu může být potřebné speciální vybavení, případně i spolupráce s odborníkem v oboru.

Často se při provádění úkonů setkáváme s firmami, které využívají Outsourcing, kdy firma vyčlení různé podpůrné a vedlejší činnosti, například správu počítačů, a svěří je smluvně jiné společnosti, specializované na příslušnou činnost. V těchto případech, pokud je to nutné, je třeba zajistit a kontaktovat i vnější dostupné zdroje, které zahrnují například dodavatele technického vybavení, dodavatele software, nebo servisní a správcovské organizace, případně pro další šetření sestavit seznam kontaktů a pověřených pracovníků těchto vnějších zdrojů.

Při provádění úkonů ve velkých firmách se lze často setkat také s rozsáhlými centralizovanými, nebo distribuovanými počítačovými systémy, kdy se mohou digitální stopy nacházet i v síťových úložištích mimo počítače uživatele. Takové systémy často využívají nejmodernější, nebo těžko dostupné technologie, které k zajištění digitálních důkazů nezbytně vyžadují součinnost s počítačovými experty, techniky výrobců, nebo správců těchto systémů. S nimi je pak nutné určit možné způsoby zajištění digitálních stop, nebo jejich případné uložení na jiné záznamové médium. Na prováděné činnosti těchto externích počítačových expertů, správců a techniků při zajišťování dat potom dohlíží kriminalistický specialista na zajištění dat, nebo soudní znalec.

U případů, kdy vinou okolností, nebo z důvodu nepřekonatelných technických překážek nelze zajistit digitální stopy pro další zkoumání, je nutné provést forenzní analýzu

digitálních dat přímo na místě provádění úkonu, na „živých systémech“. V takových případech ji může provádět pouze policejní, nebo civilní soudní znalec.

Uvedené postupy vycházejí z všeobecně uznávaných praktik a byly popsány velice obecně. Provádění úkonů zajištění digitálních stop mohou vyžadovat i další alternativní postupy, než byly uvedeny. V případě potřeby se vždy doporučuje konzultovat nastalé situace se znalcem, nebo právním poradcem.

1.4.1 Specifika jednotlivých úkonů vzhledem k zajištění digitálních stop

1.4.1.1 Ohledání místa činu

Místo činu je při celém vyšetřování většinou výchozím a často také jediným místem, kde je možno nalézt stopy po činnosti pachatele konkrétního trestného činu a první učiněné kroky na místě činu jsou často nejdůležitější při dalším vyšetřování daného trestného činu. Ohledání je řazeno mezi neodkladné úkony. Včasným zajištěním místa činu a následným vyhledáním a zajištěním důkazních materiálů se zjišťují nejdůležitější okolnosti potřené k objasnění skutkové podstaty trestného činu. Chyby a nedostatky při ohledání bývají základem neúspěchu a v mnoha případech se již nedají dodatečně napravit.

Při tomto úkonu se uskutečňuje zkoumání a hodnocení situace na určité části území, místnosti apod., kde došlo k vyšetřované události, také se může jednat i o ohledání předmětů nebo dokumentů, jestliže se na místě činu nacházejí. Při tomto úkonu se zjišťují fakta o událostech a jejich charakteru, která mají operativní nebo důkazní význam. Výsledky ohledání by měly dávat odpovědi na sedm základních kriminalistických otázek: CO bylo spácháno? KDY byl čin spáchán? KDE byl čin spáchán? KDO čin spáchal? JAK byl čin spáchán? ČÍM byl čin spáchán? PROČ byl čin spáchán? K zodpovězení některých otázek bývá často nutné zajistit odpovídající digitální stopy.

Nutností při tomto úkonu je, aby se policisté provádějící tento úkon nenechali ovlivnit prvním dojmem, poškozenými ani svědky a zachovávali objektivnost a nestrannost. Důležité je také prověření všech možných verzí případu.

Při ohledání místa činu a zajišťování digitálních stop lze postupovat ze dvou pohledů na místo činu:

- **Materiální místo činu**, což je místo odkud byl trestný čin spáchán, nebo na jakém místě se projevily jeho účinky. Je to například nějaký objekt, budova, místnost, stůl, počítač apod. Při zajišťování digitálních stop je nutné brát na

zřetel i nejbližší okolí výpočetní techniky, ve kterém se mohou nacházet další důležité informace, které by mohly být užitečné k dalšímu zkoumání zajištěných digitálních stop. Zde se jedná například o pracovní stoly, odpadkové koše, nástěnky, diáře a poznámky. Toto pravidlo platí i u ostatních úkonů, jako jsou domovní prohlídka, nebo prohlídka jiných prostor a pozemků.

- **Digitální místo činu**, které lze chápat, jako místo, kde se nachází digitální stopy související se spáchaným trestným činem. Například data na pevném disku, nebo flash disku, v paměti RAM, na síťovém serveru, v databázi, nebo na Internetu. Při tomto pohledu na místo činu se vychází od možného výskytu digitálních stop až k médiím a zařízením, která je mohou obsahovat.

1.4.1.2 Vydání a odnětí věci

Při dobrovolném vydání věci podle § 78 trestního řádu se postupuje s vědomím, že pachatel spolupracuje. Velmi často se však stává, že tato spolupráce není úplná a pachatel nevydá všechny věci, které jsou důležité pro trestní řízení. Proto je vhodné, aby vyšetřovatel s takovou situací počítal a před vyzváním pachatele k vydání věci měl již k dispozici i příkaz k domovní prohlídce, kterou v případě pochybností může ihned vykonat. V oblasti počítačové kriminality se většina úkonů týkajících se vydání, nebo odnětí věci provádí v rámci domovní prohlídky, nebo prohlídky jiných prostor.

1.4.1.3 Domovní prohlídka

Domovní prohlídka se obvykle provádí v obydlí osoby pachatele, nebo osoby podezřelé ze spáchání trestného činu. Tento úkon je většinou plánovaný předem a proto je dobré si předem ujasnit, jaké digitální stopy se budou hledat a kde všude se mohou nacházet. V obydlí bývá obvykle vytvořen nějaký pracovní prostor, který pachatel používá k práci s výpočetní technikou. V tomto pracovním prostoru se obvykle nachází pracovní stůl, na kterém, nebo v jeho blízkosti, se nachází jak počítače, tak i různé periferní zařízení, paměťová média a dokumenty. Na takového pracovním místě a v jeho bezprostředním okolí se nachází většina důkazního materiálu. Prohlídka tohoto prostoru musí být proto provedena velmi pečlivě a podrobně a lze u při ní nalézt i skryté paměťové nosiče, nebo písemnosti související s pácháním trestné činnosti. Nesmí se však opomenout i důkladná prohlídka zbylých prostor obydlí. Při provádění domovní prohlídky je nutné se soustředit, kromě digitálních stop, také na zajištění dalších důkazů a informací, které by se mohly

vztahovat k případu, jako jsou například vytištěné dokumenty v tiskárně, výstupy monitorů, hesla napsaná na monitorech, klávesnicích a podobně.

Při nálezu spuštěného počítače by měl před jeho vypnutím a zajištěním specialista na zajištění digitálních stop, nebo znalec, provést kontrolu tohoto počítače, zda v něm není spuštěn nějaký šifrovací nástroj. Při použití takového nástroje hrozí, že vypnutím budou všechny digitální stopy nenávratně ztraceny. Specialista, nebo znalec v tomto případě může provést vytvoření bitových kopií dat ze spuštěného a rozšifrovaného systému. Při provedení kontroly spuštěného počítače by se měla prověřit i existence připojení k síťovým diskům, aplikacím, případně do Cloudu.

Nesmí se podceňovat ani přítomnost domácí sítě, nebo bezdrátové Wifi sítě. Při existenci Wifi sítě na místě úkonu je doporučeno provést vyhledání všech dostupných Wifi sítí na místě, které provede specialista. Mnoho typů síťových prvků může pracovat v domácí síti odděleně, bez nutnosti jakékoliv obsluhy a často bývají velice dobře ukryty. Z nejčastěji používaných se můžeme setkat například se síťovými disky a úložišti, NAS servery a podobně, které můžou obsahovat vlastní operační systém a provádět různé činnosti zcela automaticky. Při existenci sítě v místě provádění domovní prohlídky může být důležité i zajištění logů aktivních prvků sítě, jako jsou routery, firewally, nebo proxy servery.

Součástí domovní prohlídky jsou i výslechy osob, které jsou přítomny na místě úkonu, při nichž lze často získat další důležité poznatky k vyšetřovanému případu.

1.4.1.4 Prohlídka jiných prostor a pozemků

Prohlídka jiných prostor a pozemků probíhá ve stejném režimu jako domovní prohlídka, platí pro ni stejná pravidla, ale bývá obvykle prováděna u komerčních subjektů. Provedení této prohlídky je však mnohem náročnější a rozsáhlejší a bývá při ní zajištěno velké množství důkazního materiálu a digitálních stop. Před provedením tohoto úkonu je nutné sestavit tým, jehož členové prohlídku provedou. Součástí tohoto týmu jsou i specialisté na zajišťování digitálních stop, soudní znalci a technici vybavení záznamovou technikou.

Velmi důležitá je v tomto případě příprava samotného úkonu a zvážení všech možných okolností a situací, které v průběhu prohlídky mohou nastat. Při této přípravě se rozdělí úkoly podle odborností a znalci se zaměří na svoje oblasti, technik bude provádět dokumentaci průběhu celého úkonu i zajištěných stop, připraví se specifické otázky výslechu a určí se osoby, které povedou výslechy zaměstnanců apod.

Při provádění prohlídky jiných prostor a pozemků u komerčních společností se provádí také výslech vedoucích pracovníků společnosti ke konkrétní trestné činnosti za účelem ustanovení možného pachatele, pokud již není předem znám.

1.4.2 Dokumentace zajištěných digitálních stop u provedených úkonů

Při provádění všech úkonů podle trestního řádu je velmi důležité a také zákonem uložené dokumentovat celý postup při zajišťování digitálních stop. Dokumentace by měla být provedena písemně protokolem, který podepíší všechny osoby zúčastněné na úkonech, videozáznamem se slovním popisem policisty, nebo fotograficky, případně i plánkem umístění jednotlivých zajištěných objektů, nebo schématem zapojení jednotlivých zařízení. Při provádění úkonů dle trestního řádu se jedná například o následující protokoly:

- Protokol o ohledání místa činu, podle § 113 trestního řádu,
- Protokol o provedení domovní prohlídky, podle § 82 trestního řádu,
- Protokol o provedení prohlídky jiných prostor a pozemků, podle § 82 trestního řádu,
- Protokol o odnětí věci, § 79 trestního řádu,
- Protokol o vydání věci, § 78 trestního řádu,
- případně dalších.

Zajišťované objekty, které obsahují digitální stopy, je nutné do příslušného protokolu prováděného úkonu podrobně popsat, aby nemohlo dojít k jejich záměně, zároveň je také nutné provést pečlivou fotodokumentaci každého objektu.

Pokud je u provádění těchto úkonů přítomna i osoba podezřelého, nebo majitel zajišťované výpočetní techniky, je doporučeno, aby protokol také podepsala. Při dokumentaci se musí provést jednoznačná identifikace zajištěných zařízení a paměťových médií, zdokumentovat jejich množství a jednotlivé typy a také zaznamenat místa, kde byla nalezena, nebo odkud byla vyjmuta. Dokumentuje se také, jak byla v době zajištění výpočetní technika zapojena, například fotografiemi přední i zadní strany přístroje, co a jakým způsobem bylo zajišťováno, zda při zajišťování byly případně použity nástroje a jaké, a také do jakého obalu byla zajištěná technika zabalena.

Většina zajišťovaných zařízení je opatřena výrobním štítkem s uvedenými identifikačními údaji o zařízení, jako jsou sériová a výrobní čísla, určení typu a modelu zařízení a podobně, které slouží k jednoznačné identifikaci objektu. Proto je nutné informace z těchto štítků

uvést do protokolu. Je nutné také dokumentovat veškeré součásti zajišťovaných objektů a jejich stav i z hlediska možnosti následného uplatnění případné škody.

Zvláštní význam má dokumentace zejména při výskytu nestandardního zapojení různých zařízení, která je velmi důležitá pro následné provádění forenzních analýz. Při zajišťování spuštěných počítačů bývá důležité také fotograficky dokumentovat i obrazovky monitorů se spuštěnými aplikacemi.

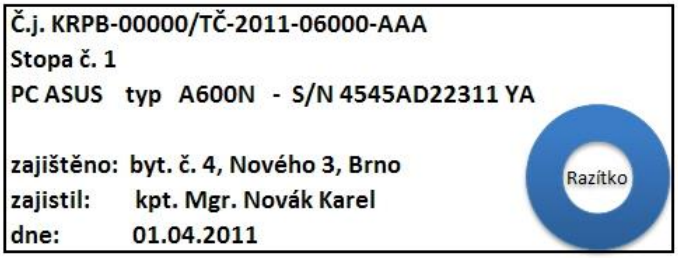
1.4.3 Ukládání a balení zajištěných digitálních stop

Ve většině případů bývá zajišťován objekt, který obsahuje, nebo může obsahovat digitální stopy, což je obvykle nějaké zařízení výpočetní techniky, nebo nějaké paměťové médium. Pro procesně správné a úplné zajištění digitálních stop je nutné všechny zajišťované objekty spolehlivě, řádně a průkazně zabezpečit proti neautorizované manipulaci. To se v praxi realizuje uložením, zabalením a zapečetěním zajištěných objektů do vhodných obalů, ve kterých je nutno zajištěné objekty zabezpečit proti pohybu tak, aby nedošlo k jejich poškození. K tomuto účelu se využívají například:

- bezpečnostní sáčky různých velikostí, označované také jako ORGATECH,
- silné plastové neprůhledné pytle,
- silné papírové pytle,
- lepenkové krabice,
- původní obaly od výrobce apod.

Obal se zajištěným objektem se zabezpečuje na všech spojích a jiných místech, kde by bylo možno obal neoprávněně a bez zjevného porušení otevřít a opětovně zavřít. Zabezpečení se provádí například lepicí páskou s razítkem policejního útvaru a podpisem zajišťující osoby, nezúčastněné osoby, případně i majitele zajištěného objektu, nebo pečetním voskem, individuální samolepící pečetí a podobně. Způsob zabezpečení obalu proti neautorizované manipulaci je nutné vyznačit v protokolu a dokumentovat videozáznamem, nebo fotograficky.

Takto zabezpečené a zapečetěné obaly musí být také řádně a prokazatelně označeny, aby nemohlo dojít k jejich záměně. Pro toto označení se doporučuje použít například samolepící štítky, na kterém se uvádí číslo jednací případu, stručný popis zajištěného objektu, místo zajištění, číslo stopy, případně další důležité informace.

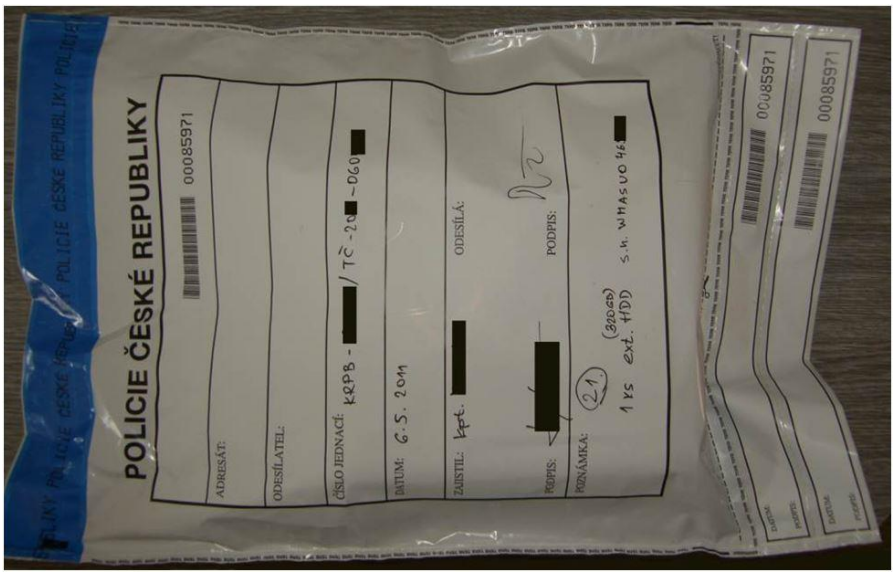


Obrázek 1. Možná varianta štítku

Obal by měl také zabránit případnému poškození zajištěných objektů, proto například u magnetických médií bývá nutné použít obaly, které chrání před vlivy elektromagnetického pole, nebo u médií CD a DVD je nutné použít neprůhledné obaly, které eliminují vliv UV a infračerveného záření.

V případě zajištění mobilního telefonu, nebo zařízení, které vyžaduje stálé napájení, je doporučeno provést zabalení tak, aby ze zapečetěného obalu vedl pouze napájecí kabel, kterým je možné zařízení dodávat elektrickou energii.

Celé opatření ukládání a balení zajištěných digitálních stop je prováděno také z důvodu, aby zajištěný objekt včetně všech vnitřních dílů, například osobní počítač, byl považován za jeden celek. Tím se zároveň předchází možným problémům a stížnostem ze strany majitele při následném vracení věci, kdy se po provedení analýz zajištěný objekt zase jako celek vrací.



Obrázek 2. Zajištěná stopa v bezpečnostním sáčku typu ORGATECH

2 VYTVÁŘENÍ BITOVÝCH KOPIÍ DIGITÁLNÍCH STOP

Tato kapitola se bude zabývat způsoby forenzního vytváření bitových kopií digitálních stop prováděných v rámci úkonů trestního řízení u Policie ČR. Výpočetní technika, na které se provádí tyto kriminalisticko-technické úkony, bývá zajištěna v průběhu provedené domovní prohlídky, nebo prohlídky jiných prostor a pozemků podle § 82 trestního řádu, případně dobrovolným vydáním, nebo odnětím věci podle § 78 a § 79 trestního řádu. Bitové kopie se vytváří u všech digitálních stop, které by mohly být v průběhu vyšetřování znehodnoceny. Jedná se zejména o digitální stopy, které jsou uloženy na přepisovatelných médiích, jako jsou například pevné disky, flash disky a paměťové karty.

Ve zvláštních případech se vytváření bitových kopií digitálních stop provádí přímo v průběhu domovní prohlídky, nebo prohlídky jiných prostor. Důvodem ve většině případů bývá možný vznik škody, která by byla způsobena odpojením výpočetní techniky na delší dobu. Jedná se například o výpočetní techniku, která řídí nějakou výrobní technologii, server velké společnosti a podobně.

U průběhu celého procesu vytváření bitových kopí může být přítomna osoba, která je v nějakém vztahu k zajištěné výpočetní technice, například majitel počítače, advokát, jednatel firmy a podobně. Přítomnost této osoby není povinná. V případě odmítnutí může dohlížet na celý proces nezúčastněná osoba.

Zajištěná výpočetní technika by měla být zabalena a zapečetěna v neporušených obalech a označena jednacím číslem případu a pořadovým číslem stopy. Neporušenost obalů a pečetí musí být před započetím úkonu zkontrolována všemi zúčastněnými osobami. Před rozpečetěním a zahájením vytváření bitových kopií i v průběhu celého procesu je podle metodického pokynu KÚP č. 7/2001 nařízeno provádět fotodokumentaci.

Obrázek 3. Zapečetěná zajištěná výpočetní technika

Jakoukoliv manipulaci se zajištěnými digitálními stopami může provádět pouze osoba, která je držitelem osvědčení o odborné způsobilosti k provádění kriminalisticko-technických úkonů při zajišťování výpočetní techniky a dat, nebo soudní znalec.

Po rozpečetění a vybalení zajištěné techniky proběhne vnější prohlídka, jejímž cílem je dokumentace stavu této zajištěné techniky v době jejího dodání k vytvoření bitových kopií. Vnější prohlídka obsahuje:

- Prohlídku a fotodokumentaci zajištěných předmětů, jejich případné poškození, chybějící části, výrobní štítky a sériová čísla, případně jinou identifikaci předmětu.
- Při prohlídce lze provést například rozebrání krytů zajištěné výpočetní techniky a tím zajistit přístup k vnitřním komponentám a paměťovým nosičům. Při tomto opět provádíme detailní fotodokumentaci vnitřní konfigurace zařízení tak, aby byly zdokumentovány všechny interní prvky a jejich vzájemné zapojení.
- Detailní vnější prohlídku paměťových nosičů a jejich dokumentaci. Při tomto úkonu bývá nutné paměťové nosiče odpojit a vyjmout ze systému. Dokumentuje se především typ paměťových nosičů (značka, model, velikost, nastavení, umístění, datové rozhraní) a jejich stav, případně poškození.
- Podle povahy případu je možná dokumentace dalších komponent.

Před vlastním zahájením vytváření bitových kopií je důležité předem znát parametry a kapacity zajištěných paměťových médií, například u pevných disků musí být zjištěno jejich datové rozhraní, kterým jsou připojeny k zařízení a také jejich celková úložná kapacita.

Bitová kopie bývá vytvořena na technologický pevný disk Policie ČR, který musí mít kapacitu větší, než zajištěná digitální stopa. Je to z důvodu ukládání dalších informací o této stopě, jako jsou informace o výrobci, topologii, souborovém systému sériová čísla a také autentizační soubory s kontrolními otisky. Pro zajištění čistoty dat je nutné technologický pevný disk, na který bude ukládána bitová kopie, před použitím vymazat, nejlépe vynulováním celého diskového prostoru nástrojem WIPE.

Vlastní vyhotovení bitových kopií z pohledu hardwaru lze provést několika způsoby:

- Vytvoření bitových kopií dat pomocí systému Policie ČR.
- Vytvoření bitových kopií dat pomocí zkoumaného systému.
- Vytvoření bitových kopií dat prostřednictvím počítačové sítě.
- Vytvoření bitových kopií ze „živého“ zkoumaného systému.

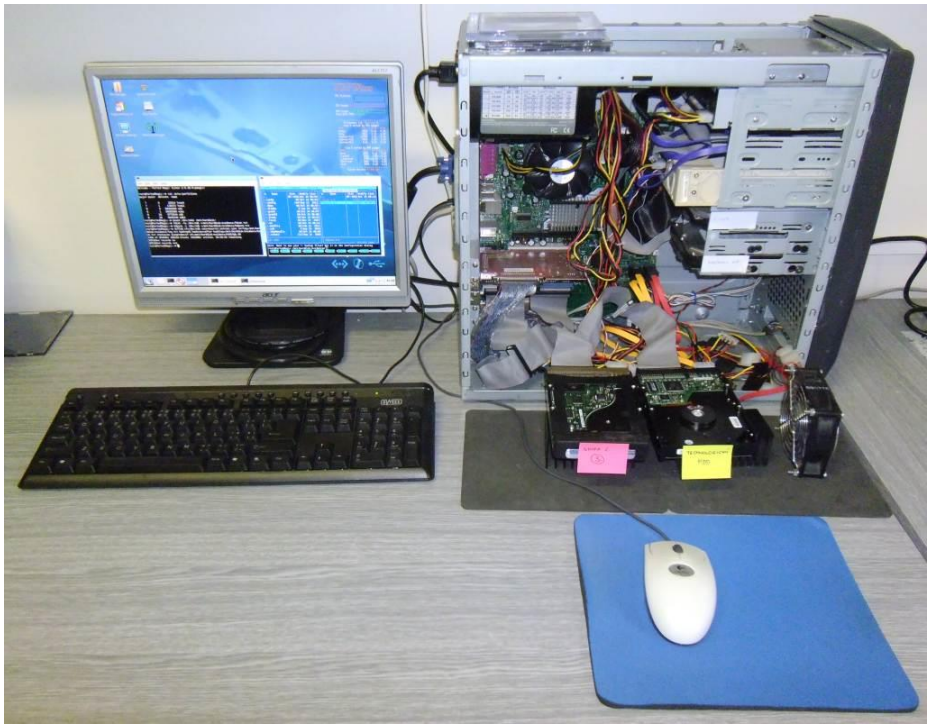
2.1 Vytváření bitových kopií dat pomocí systému Policie ČR

Jedná se o způsob, při němž je ze zajištěné výpočetní techniky odpojeno paměťové médium a následně je připojeno k rozhraní jiného přístroje. Je to zřejmě nejuniverzálnější metoda, která je vhodná pro většinu případů. Po odpojení paměťových médií se u počítačových systémů provádí kontrolované spuštění zkoumaného počítače bez paměťových médií, za účelem zjištění informací o nastavení konfigurace BIOSu, jako jsou bootovací sekvence, datum a čas, hesla, případně další relevantní informace, které budou následně dokumentovány v protokolu o zajištění dat.

Bitové kopie z odpojených paměťových médií lze provést buď připojením ke speciálnímu zařízení na duplikaci paměťových médií „Disk Doubler“, nebo připojením k technologickému počítači Policie ČR, nebo znalce. Speciální zařízení „Disk Doubler“, někdy označované také jako „Disk Duplicator“, umožňuje provádět kopii disku 1:1, nebo provést kopii disku do jednotlivých souborů, provádí výpočty kontrolních součtů MD5 a další. Výhodou je jeho rychlost a snadnost obsluhy, nevýhodou je vysoká pořizovací cena přesahující 100 000,- Kč.

Obrázek 4. Disk Doubler

Ve druhém případě se vytváří bitové kopie odpojených paměťových médií na technologickém počítači Policie ČR. Tento technologický počítač by měl být co nejmodernější a měl by obsahovat všechny nejpoužívanější rozhraní pro připojení paměťových médií. Při připojování paměťových nosičů k technologickému počítači je nutné důkladně ověřit, že paměťové nosiče byly tímto počítačem zaručeně rozpoznány.



Obrázek 5. Technologický počítač Policie ČR

Pro vlastní vytvoření bitových kopií lze použít buď speciální forenzní software pod operačním systémem Microsoft Windows, nebo některou z osvědčených forenzních distribucí systému Linux.

Při použití operačního systému Microsoft Windows je nutné použít speciální hardwarové zařízení, nebo software pro blokování zápisu na zajištěné paměťové nosiče. Hardwarová ochrana proti zápisu se zapojuje mezi zajištěné paměťové médium a technologický počítač. Je to z toho důvodu, že operační systém Microsoft Windows ihned po připojení paměťového média provádí na toto médium zápis. To je ve forenzní praxi nepřípustné, protože by došlo ke změně dat na zajištěném disku. Naproti tomu operační systém Linux nikdy bez vědomí uživatele nezapisuje a nemění informace na paměťovém médiu. To je také jedním z hlavních důvodů, proč se Linux vyžívá ve forenzní praxi.

Obrázek 6. HW Write blokátor

2.1.1 Vytváření bitových kopií pod OS Microsoft Windows

V současné praxi u Policie ČR se forenzní vytváření bitových kopií pod operačním systémem Microsoft Windows provádí výhradně za použití software EnCase Forensic, ve verzi 6 a vyšší, při současném použití hardwarové ochrany proti zápisu na zkoumaný disk. Komplexní forenzní softwarový nástroj EnCase Forensic zahrnuje snad všechny oblasti forenzní analýzy dat, umožňuje vytvářet přesné bitové kopie médií a jejich uchování podle forenzních požadavků a dále nabízí celou řadu analytických, archivačních a reportovacích prostředků.

Při vytváření bitových kopií paměťových nosičů EnCase provádí výpočty kontrolních otisků MD5, získává a ukládá evidenční informace o geometrii a výrobních datech paměťových médií, může používat kompresi dat, umožňuje načítání dat z RAID pole a mnoho dalšího.

2.1.2 Vytváření bitových kopií pod OS LINUX

Jak již bylo dříve uvedeno, operační systém Linux nezasahuje na připojená média bez aktivní účasti uživatele a zajišťuje řízený přístup k datovým oblastem. V Linuxu lze definovat připojení paměťového zařízení pouze pro čtení, čímž je zajištěno, že nedojde k nežádoucímu zásahu či změně uložených dat. Dále je zde možné zálohovat přímo celá paměťová média, nebo datové oblasti, bez nutnosti připojení do souborové struktury systému. Použití hardwarové ochrany proti zápisu se však stále doporučuje. Velkou výhodou OS Linux jsou také malé, hardwarově a paměťově nenáročné distribuce, kterých je, díky tomu, že je volně šiřitelný i se zdrojovými kódy, velké množství.

Pro vytváření bitových kopií digitálních stop se v praxi u Policie ČR často používají tzv. „Live“ distribuce, umožňující spuštění operačního systému z média CD/DVD, nebo USB flash disku. Z osvědčených distribucí lze jmenovat například: CAINE (Computer Aided INvestigative Environment), DEFT (Digital Evidence & Forensic Toolkit), Knoppix a diskově orientovaný Parted Magic.

Nyní zde bude popsán nejčastější postup vytváření bitové kopie z jednoho zajištěného paměťového média. Bootovací sekvence technologického počítače musí být ještě před spuštěním počítače nastavena na bootování z CD/DVD, případně USB. Technologický pevný disk, na který se bude ukládat bitová kopie, je dobré mít již naformátovaný do souborového formátu NTFS, nebo EXT3. Při dodržení všech dříve uvedených zásad a po připojení technologického pevného disku a zajištěného paměťového média, se technologický počítač spustí a provede se zavedení operačního systému Linux z CD/DVD-ROM, nebo USB flash disku. Po spuštění operačního systému se pracuje v systémovém terminálu.

Celý postup vytvoření bitové kopie je následující:

- Nejprve je nutné získat administrátorská práva zadáním příkazu „**#sudo su**”.
- Provede se výpis seznamu připojených zařízení zadáním příkazu „**#cat /proc/partitions**”. Z výpisu se identifikuje zkoumané paměťové médium

a také technologický disk. Například zkoumané paměťové médium bude označeno jako **sdb**, technologický disk jako **sda**. Ve výpisu budou uvedeny i logické oddíly jednotlivých zařízení, například **sda1, sdb1**.

- Do souborového systému se připojí pouze technologický pevný disk s možností zápisu. Zkoumané paměťové médium se nikdy do souborového systému nepřipojuje. Pro připojení technologického pevného disku se vytvoří v souborovém systému příkazem „**#mkdir /mnt/harddisk**" adresář, do kterého se následně připojí logická jednotka technologického pevného disku příkazem „**#mount /dev/sda1 /mnt/harddisk**". V případě, že je technologický pevný disk naformátován do souborového systému NTFS, připojuje se tento disk příkazem „**#mount -t ntfs-3g /dev/sda1 /mnt/harddisk -o force**".
- Na připojeném technologickém disku se vytvoří pracovní adresář, například „evidence", do kterého se bude následně ukládat vytvářená bitová kopie a další informační soubory. Vytvoření pracovního adresáře se provádí příkazem „**#mkdir /mnt/harddisk/evidence**".

Nyní již lze získávat a ukládat data ze zkoumaného paměťového média:

- Získání informací o rozdělení disku a diskových oddílech příkazem „**#fdisk -lu /dev/sdb >/mnt/harddisk/evidence/fdisk.txt**", který výsledky uloží do souboru fdisk.txt v pracovním adresáři.
- Získání informací o technických a výrobních parametrech disku příkazem „**#hdparm -i /dev/sdb >/mnt/harddisk/evidence/hdparm.txt**", který výsledky uloží do souboru hdparm.txt v pracovním adresáři. U novějších zařízení připojených prostřednictvím SATA, nebo USB se může jako ekvivalent použít příkaz „**#sdparm**" se stejnými parametry.

Poté se již může zahájit vytváření bitové kopie. Pro tento účel se používá speciální forenzní mutace programu „dd", který současně vytváří i kontrolní součet MD5. Program „dd" je standardní program, který je součástí každé distribuce OS Linux. Z důvodu usnadnění práce ve forenzní praxi byly vyvinuty další mutace, například „dcfldd", nebo „dc3dd", které jsou však součástí pouze forenzních distribucí. Variant použití těchto programů je mnoho, proto zde budou uvedeny pouze nejčastěji používané.

2.1.2.1 Vytvoření bitové kopie za použití příkazu „dd“ :

„**#dd if=/dev/sdb conv=noerror,notrunc,sync |md5tee /mnt/harddisk/evidence/md5.txt | split -b 700m - /mnt/harddisk/evidence/hddxxxgb_**“

Tento příkaz vytvoří bitovou kopii zařízení sdb a rozdělí ji po 700MB blocích do souborů, jejichž pořadí určí příponou souboru, např. hddxxxgb.aa - hddxxxgb.zz. Zároveň bude vytvořen soubor md5.txt obsahující kontrolní součet MD5. Rozdělování výstupního souboru lze vynechat odstraněním parametru "split -b 700m".

2.1.2.2 Vytvoření bitové kopie za použití příkazu „dc3dd“ :

„**#dc3dd if=/dev/sdb of=/mnt/harddisk/evidence/hddxxxgb_ conv=noerror,notrunc,sync progress=on sizeprobe=on hash=md5 hashwindow=700M split=700M splitformat=aa log=/mnt/harddisk/evidence/log.txt**“

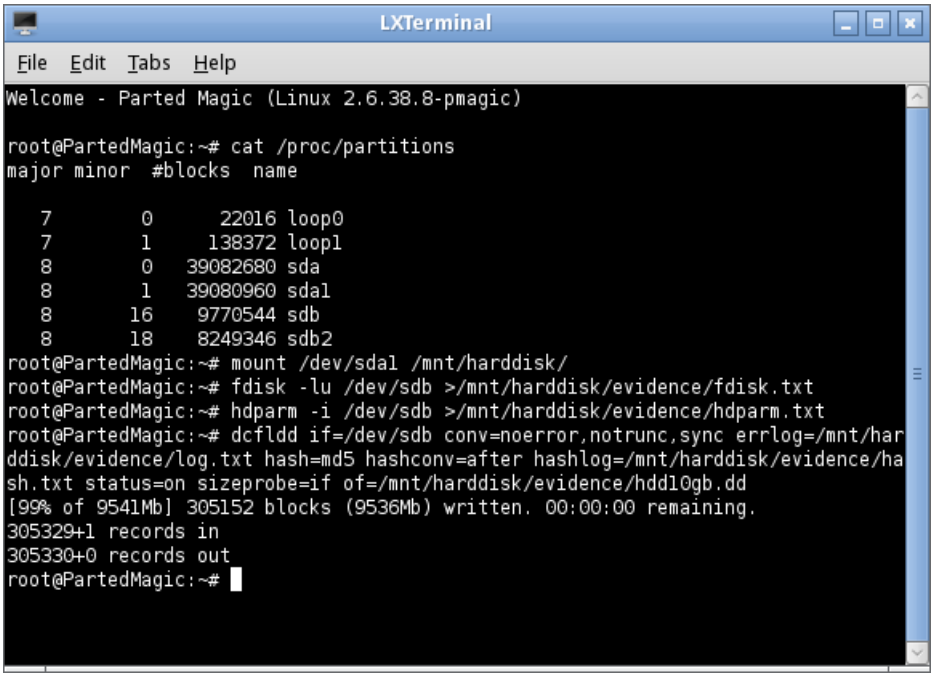
Použitím tohoto příkazu bude vytvořena bitová kopie zařízení sdb, která bude rozdělena také na soubory o velikosti 700MB. Celý průběh bude navíc zobrazován v okně terminálu. Zároveň bude vytvořen soubor log.txt, který bude obsahovat informace o průběhu tvorby bitové kopie a také kontrolní součet MD5.

2.1.2.3 Vytvoření bitové kopie za použití příkazu „dcfldd“ :

„**#dcfldd if=/dev/sdb conv=noerror,notrunc,sync errlog=/mnt/harddisk/evidence/log.txt hash=md5 hashconv=after hashlog=/mnt/harddisk/evidence/hash.txt status=on sizeprobe=if split=700M splitformat=aa of=/mnt/harddisk/evidence/hddxxxgb_**“

V praxi nejpoužívanější je tento příkaz, který vytvoří bitovou kopii zařízení sdb, kterou také rozdělí na soubory o velikosti 700MB a celý průběh také zobrazuje v okně terminálu. Po ukončení vytváření bitové kopie bude vytvořen soubor log.txt, který bude obsahovat informace o průběhu a také soubor hash.txt, který bude obsahovat kontrolní součet MD5.

Po dokončení vytvoření bitové kopie zajištěného paměťového média se provádí kontrola uložených dat na technologickém disku. Poté se odpojí od souborového systému připojený technologický pevný disk příkazem „**#umount /dev/sda**“ a počítač se vypne. [3]



Obrázek 7. Příklad průběhu vytvoření bitové kopie

2.2 Vytvoření bitových kopií dat pomocí zkoumaného systému

Za určitých okolností může nastat situace, při které je lepší neodpojovat paměťové nosiče od zkoumaného zařízení a bitovou kopii provést přímo na tomto zařízení. Jedná se zejména o tyto případy:

- Zkoumaný systém obsahuje RAID pole - odpojením a zajištěním dat z jednotlivých disků nemusí vést k získání použitelných výsledků.
- Laptopové systémy - v některých případech nelze pevné disky demontovat, v jiných případech nemusí být data z pevných disků použitelná při odpojení od původního systému.
- Závislost hardware - starší pevné disky nemusí být kompatibilní s novějšími systémy.
- Dostupnost vybavení - pokud není přístup k potřebnému vybavení.
- Síťové ukládání - k zajištění dat může být nutné síťové připojení.

V těchto případech se ke zkoumanému systému připojuje technologický pevný disk, na který se bude ukládat bitová kopie paměťového nosiče. Zároveň je i v tomto případě doporučeno zvážit použití hardwarové, nebo softwarové ochrany zápisu na originální paměťové nosiče zkoumaného systému.

Jako nejlepší možnost pro vytvoření bitových kopií pomocí zkoumaného systému je možnost spuštění zkoumaného systému pomocí forenzního „live“ operačního systému z CD ROM, nebo DVD ROM. Před spuštěním je však nutné zajistit, aby zkoumaný systém rozpoznal technologický pevný disk, na který se bude ukládat bitová kopie. Jako vhodné řešení se nabízí připojení technologického disku například prostřednictvím rozhraní USB. Vlastní provedení vytvoření bitových kopií paměťových médií zkoumaného systému se pak provádí stejným způsobem jako za pomocí systému Policie ČR.

Získávání dat přímo na zkoumaném systému nese mnoho úskalí, které je nutné vyřešit, proto se použití tohoto způsobu doporučuje jen ve výjimečných případech, přičemž se musí věnovat zvýšená pozornost dokumentaci všech skutečností, které při tomto úkonu nastanou.

2.3 Vytvoření bitových kopií prostřednictvím počítačové sítě

Další možnost z pohledu hardwaru je vytváření bitových kopií zajištěných digitálních stop prostřednictvím počítačové sítě. Tato možnost je velmi výhodná v případě zřízení tzv. centrálních úložišť a v současnosti je mnoha forenzními pracovišti v rámci Policie ČR využívaná. Počítačová síť musí být v tomto případě uzavřená z důvodu vyloučení přístupu třetích osob a tím i případného narušení průběhu ukládání dat.

Celý postup vytvoření bitových kopií paměťových médií zkoumaného systému se pak provádí stejným způsobem jako za pomocí systému Policie ČR, jediný rozdíl je v místě, kam budeme výslednou bitovou kopii ukládat. V tomto případě technologický pevný disk nahrazuje síťové centrální úložiště. V praxi se ukládání bitových kopií na servery realizuje pod protokoly Microsoft Windows (Samba), NFS, nebo SSH server.

Mezi výhody tohoto způsobu ukládání bitových kopií patří zejména možnost vytváření bitových kopií z několika paměťových médií současně, komprese za účelem zmenšení objemu dat a výhody plynoucí z centralizace zajišťovaných dat. Mezi nevýhody patří omezená rychlost počítačové sítě, nutnost opakovat celý úkon v případě výpadku sítě, případně i čas nutný k dekompresi zajištěných dat.

2.4 Vytvoření bitových kopií ze „živého“ zkoumaného systému

Poslední možností získání bitových kopií je vytvoření bitových kopií ze „živého“ zkoumaného systému. Ve výjimečných případech, nebo za zvláštních okolností, například při nutnosti zajištění dat ze spuštěného počítače, který používá nějaký šifrovací nástroj, kterým jsou v systému počítače dostupná aktuálně rozšifrovaná data a podobně, nebo pokud by vypnutím počítače hrozila nenávratná ztráta uložených dat, je nutné provést vytvoření bitových kopií paměťových médií přímo ve spuštěném zkoumaném systému. Postupy při tomto úkonu bývají velice často problematické a jsou vždy závislé na použitých technologiích, operačním systému zkoumaného počítače i na použitém šifrovacím nástroji. Může nastat i situace, kdy vytvoření bitové kopie ve spuštěném systému nebude vůbec možné. Z těchto důvodů se doporučuje celý postup získání bitové kopie ze spuštěného počítače konzultovat s příslušným expertem, nebo znalcem v oboru. Při správně zvoleném postupu může být získání bitových kopií rozšifrovaných paměťových médií zkoumaného počítače úspěšné.

Při tomto úkonu se současně provádí i zajištění obsahu paměti počítače. Výpis obsahu paměti je důležitou informací pro analýzu předchozí aktivity na počítači. Operační paměť počítače může obsahovat například informace o spuštěných procesech, smazaná data, data uživatelských relací a také kryptografické klíče. Se stále se rozvíjející informační bezpečností a zaváděním šifrování celých souborových systémů, je získání dešifrovacího klíče při úkonech zajišťování dat jedním z primárních úkolů. V systémech, které jsou zabezpečeny šifrovacím nástrojem, je často operační paměť jediným místem, kde se dešifrovací klíče nacházejí.

K vytváření bitových kopií ze „živého“ zkoumaného systému i pro zajištění obsahu paměti se používá mnoho komerčních i volně šiřitelných forenzních nástrojů. Jeden z nejčastěji používaných forenzních nástrojů je například FTK Imager, vyvíjený společností AccessData, který je dostupný jak pro operační systémy Microsoft Windows, tak i pro Linux. Z dalších lze uvést například forenzní „live“ distribuce Linuxu Helix a Caine, které obsahují také nástroje pro vytváření bitových kopií ze „živého“ zkoumaného systému i pro zajištění obsahu paměti pro oba typy operačních systémů.

Příklad možného postupu při vytváření bitové kopie ze „živého“ zkoumaného systému:

Předpokládá se, že ve zkoumaném počítači je spuštěn například operační systém Microsoft Windows XP s přihlášeným uživatelem, který je správcem systému.

1. Před započetím úkonu je nutné na spuštěném systému zjistit možnosti připojení externích paměťových médií, například prostřednictvím USB rozhraní. Při jakékoliv manipulaci se zkoumaným počítačem je nutné postupovat velice obezřetně, aby nehrozila ztráta dat.
2. Pokud to systém umožňuje, připojí se do spuštěného systému prostřednictvím USB rozhraní technologický pevný disk Policie ČR, na kterém je uložen forenzní nástroj k provedení bitové kopie, například FTK Imager. Tento technologický disk by měl mít také dostatek místa k uložení zajišťované bitové kopie.
3. Z technologického disku Policie ČR se spustí aplikace FTK Imager.
4. Z položky menu se zvolí Create Disk Image.
5. Zvolí se zdroj získání dat, což může být fyzická jednotka, logický disk, nebo i konkrétní adresář, který je nutné zajistit.
6. Zvolí se cíl, kam budou zajištěná data uložena, zadáním názvu souboru bitové kopie, který bude vytvořen na technologickém disku Policie ČR.
7. Vytvoření bitové kopie se spustí.
8. Po úspěšném dokončení vytvoření bitové kopie FTK Imager uloží do cílového umístění i textový log soubor, který obsahuje vypočtené kontrolní otisky HASH této bitové kopie a to jak MD5, tak SHA-1.

Po provedení vytvoření bitových kopií, ještě před vypnutím zkoumaného počítače, se doporučuje získanou bitovou kopii ověřit, zda obsahuje čitelná a použitelná data. V případě, že se nepodaří získat tímto způsobem použitelná data, je doporučeno provést zajištění dat jejich vykopírováním z rozšifrovaných médií na technologické médium Policie ČR.

Postupy při zajištění obsahu paměti:

Pro operační systémy Microsoft Windows je optimální využít pro zajištění obsahu paměti také FTK Imager, kde se z položky menu spustí volbou „Capture Memory“ vytvoření souboru s obsahem operační paměti do určeného souboru. Existuje však i mnoho dalších aplikací, které stejnou operaci provedou se stejným výsledkem.

V operačním systému Linux se zajištění obsahu paměti provádí v systémovém terminálu zadáním příkazu: "**# dd if = /dev/mem of = OutputFile**", nebo také za použití nástroje FTK Imager ve verzi pro Linux, který se spouští také v systémovém terminálu.

2.5 Dokumentace

Dokumentaci kriminalisticko-technického úkonu vytvoření bitových kopií digitálních stop u Policie ČR stanovují interní akty řízení „Metodický pokyn ředitele KÚP č. 7/2001“ a „Závazný pokyn policejního prezidenta č. 100/2001“. Podle těchto interních aktů řízení je policista provádějící kriminalisticko-technický úkon zajištění dat povinen vyhotovit o tomto úkonu písemný „Protokol o zajištění dat“ a provést fotodokumentaci.

Protokol o zajištění dat musí obsahovat:

- Číslo jednací případu, datum, čas a místo provedení úkonů
- Popis zajištěné výpočetní techniky a obsažených paměťových médií včetně uvedení jejich typů a sériových čísel, popis jejich stavu, poškození a chybějících částí.
- Podrobný popis provedení celého kriminalisticko-technického úkonu zajištění dat, včetně vytvořených logů a uvedení všech hodnot vytvořených kontrolních otisků.
- Popis přiložených technologických paměťových médií, obsahujících vytvořené bitové kopie digitálních stop.
- Seznam a podpisy všech osob, které byly přítomny u provedení kriminalisticko-technického úkonu.

Nedílnou přílohou protokolu o zajištění dat jsou všechny technologické pevné disky, které obsahují zajištěné bitové kopie digitálních stop provedené při tomto úkonu. Tyto technologické pevné disky musí být řádně označeny číslem jednacím případu.
Fotodokumentace celého úkonu vytváření bitových kopií bývá zpravidla uložena na médium CD-ROM, které je řádně označeno číslem jednacím a přiloženo k protokolu o zajištění dat.

3 AUTENTIZACE DIGITÁLNÍCH STOP

Na digitální stopu je vždy nutné pohlížet jako na důkaz, který bude předkládán soudním orgánům. Proto, již od okamžiku zajištění digitální stopy, nebo zařízení, které digitální stopy obsahuje, je nezbytně nutné zabezpečit, aby v celém průběhu práce s těmito stopami nemohla být zpochybněna jejich pravost, a aby zajištěná data nemohla být jakkoliv modifikována. Z těchto důvodů je nutné digitální stopy a média obsahující digitální stopy autentizovat.

Autentizace spočívá v prokazatelném potvrzení, že digitální stopa je shodná s původní zajištěnou stopou a během celého vyšetřování nebyla změněna, nebo upravena. Toto ověření pravosti musí být kdykoliv možné provést opakovaně. Při vlastní práci s digitálními důkazy je možné použít několik možných způsobů jejich autentizace:

- **Zabalení a zapečetění objektu obsahujícího digitální stopy**. Tento způsob autentizace se používá, pokud nezajišťujeme přímo data, ale například celá paměťová média, nebo celé zařízení výpočetní techniky. Zde je autentizace provedena jako u každé jiné materiální stopy, jejím zapečetěním a podpisem zajišťující osoby a nezúčastněné osoby, nebo osoby, která věc vydává. Ověření autenticity v tomto případě spočívá v kontrole neporušenosti obalu a pečetí a v ověření pravosti podpisů na pečetích.
- **Vytvoření kontrolního otisku HASH**. V případě přímého zajišťování dat, například při jejich vykopírování, nebo při vytváření bitové kopie zajištěného paměťového média, je třeba zvolit jiný způsob autentizace. Dle definice je digitální stopa jakákoliv informace s vypovídací hodnotou, uložená nebo přenášená v digitální podobě. Informace sama o sobě je nehmotná. Teprve okamžikem uložení se materializuje na paměťové médium. Na uložené digitální stopy na paměťových médiích se již pohlíží jako na stopy materiálního charakteru. Proto i autentizace těchto stop se musí vztahovat k uloženým datům. Za nejspolehlivější metodu autentizace dat je všeobecně považován výpočet kontrolního otisku pomocí vhodné hašovací funkce.

Hašovací funkce je matematická funkce *h*, reprezentovaná algoritmem, která převádí vstupní posloupnost libovolného počtu bitů na výstupní malou posloupnost pevné délky *n* bitů. Tato výstupní posloupnost *n* bitů hašovací funkce se označuje jako kontrolní otisk,

suma, miniatura, případně hash, nebo haš. Kontrolní otisk je tedy unikátní hodnota fixní délky vypočítaná pomocí hašovací funkce z obsahu souboru.

Důvod, proč jsou hašovací funkce vhodné k autorizaci digitálních stop, spočívá v jejích vlastnostech:

- malá změna ve vstupním souboru dat vede k velké změně vytvářeného výstupního kontrolního otisku, tj. k vytvoření zásadně odlišného otisku. Toho se využívá k provedení verifikace autentičnosti dat, ke kterým byl kontrolní otisk vytvořen.
- pro jakékoliv množství vstupních dat hašovací funkce poskytuje stejně dlouhý výstupní kontrolní otisk,
- z hodnoty kontrolního otisku nelze žádným způsobem zrekonstruovat původní vstupní posloupnost dat,
- výskyt totožného kontrolního otisku dvou různých vstupních posloupností dat je vysoce nepravděpodobný, proto pomocí tohoto otisku lze v praxi ověřit pravost právě jedné vstupní posloupnosti dat,

Z těchto důvodů k zajištěným digitálním stopám vytváříme vhodnou hašovací funkcí jejich kontrolní otisk, který je pak nedílnou součástí zajištěných dat, nebo pořízených bitových kopií digitálních stop a primárně je určen k autentizaci těchto stop. Hodnota tohoto kontrolního otisku se pak ukládá do textového souboru na stejném paměťovém médiu, kde jsou uloženy i zajištěná data. V praxi to znamená vypočíst kontrolní otisk pro každý zajištěný soubor, nebo vytvořenou bitovou kopii paměťového média. Kdykoliv později je pak možné provedení výpočtu kontrolního otisku opakovat za účelem ověření, že data nebyla žádným způsobem modifikována. Pro potvrzení autenticity musí být výsledný otisk tohoto opakovaného výpočtu shodný s otiskem, který vznikl při zajištění digitální stopy.

V souladu s interními akty řízení Policie ČR musí být hodnoty kontrolních otisků zároveň uvedeny i v příslušných protokolech prováděných úkonů, při kterých se digitální stopy zajišťují, nebo se kterým se zajištěná data dále předávají k forenznímu zkoumání, například v textovém protokolu o zajištění dat, protokolu o domovní prohlídce a dalších.

V případě vytváření bitových kopií zajištěných paměťových médií je doporučeno, pokud je to technicky možné, aby oprávněná osoba, která provádí vytváření bitové kopie, provedla autentizaci pomocí kontrolního otisku před pořízením bitové kopie i po ní, aby se ujistila o neporušení integrity dat.

3.1 Volba hašovací funkce

Pro vytváření kontrolních otisků je nutné zvolit takovou hašovací funkci, která zaručuje nejvyšší možnou bezpečnost. U hašovacích funkcí je zřejmé, že počet možných různých vstupních posloupností dat je mnohem větší než počet možných různých kontrolních otisků. Z toho vyplývá, že můžou nastat situace, kdy dvojice různých vstupních posloupností dat *x* a *y* bude mít stejný otisk, to znamená, že výstupy hašovacích funkcí budou shodné a $h(x) = h(y)$. Tyto situace nazýváme kolize. Kolize jsou samozřejmě nežádoucí, ale bohužel se jim z principu hašovacích funkcí nelze vyhnout. Při vhodné volbě hašovací funkce lze však podstatně snížit pravděpodobnost výskytu kolize, proto dosažení nejnižší pravděpodobnosti je primárním cílem při volbě hašovací funkce.

Zvolená hašovací funkce by proto měla patřit mezi kryptografické hašovací funkce, kde hlavní roli nehraje rychlost funkce, ale její bezpečnostní vlastnosti, které určují obtížnost nalezení kolizí hašovací funkce. Tato obtížnost je dána výpočetní složitostí, která by měla být i při použití nejmodernější výpočetní techniky nereálná.

Vlastnosti hašovací funkce, které určují obtížnost jejího napadení, jsou následující:

- Odolnost vůči získání původní vstupní posloupnosti dat. Pro daný otisk *c* je nereálně obtížné spočítat *x* takové, že $h(x)=c$. Z toho vyplývá jednosměrnost hašovací funkce. Zároveň by mělo být také nereálně obtížné spočítat i jen část vstupní posloupnosti dat *x* ze znalosti otisku $h(x)$.
- Odolnost vůči získání jiné vstupní posloupnosti dat se stejným otiskem. Pro vstupní posloupnost dat *x* je nereálně obtížné spočítat jinou posloupnost dat *y* takovou, že $h(x)=h(y)$.
- Odolnost vůči nalezení kolize. Je nereálně obtížné najít dvojici vstupních posloupností dat *x* a *y*, pro které budou otisky hašovacích funkcí shodné a $h(x) = h(y)$.
- Pro znemožnění statistické kryptoanalýzy je nutná vzájemná nekorelovatelnost vstupních a výstupních bitů hašovací funkce.
- Odolnost vůči částečným kolizím. Je obtížné nalézt takové vstupní posloupnosti dat *x* a *y*, že výstupní otisky $h(x)$ a $h(y)$ jsou odlišné jen v malém počtu bitů.

V praxi se nejčastěji používají hašovací algoritmy MD5, SHA-1, nebo SHA-2.

3.1.1 Algoritmus MD5 - Message-Digest algorithm

Hašovací funkce MD5 vytváří otisk o velikosti 128 bitů a popisuje ho internetový standard RFC 1321. Tento nejpoužívanější hašovací algoritmus byl vytvořen z důvodu nahrazení méně bezpečného algoritmu MD4 v roce 1991 Ronaldem Rivestem. Do současné doby se stále používá v mnoha aplikacích, kde se využívá k autentizaci, ukládání hesel, nebo pro kontrolu integrity dat. Dle interních aktů řízení Policie ČR je stále používán při autentizaci digitálních stop v rámci prováděných úkonů v trestním řízení.

3.1.2 Algoritmy SHA - Secure Hash Algorithm

Tyto algoritmy byly navrženy v roce 1993 americkou Národní bezpečnostní agenturou NSA a následně vydány jako americký federální standard FIPS. Vztahuje se na ně patent US 6829355. Tyto hašovací algoritmy ale následně Spojené státy uvolnily k použití bez licenčních poplatků.

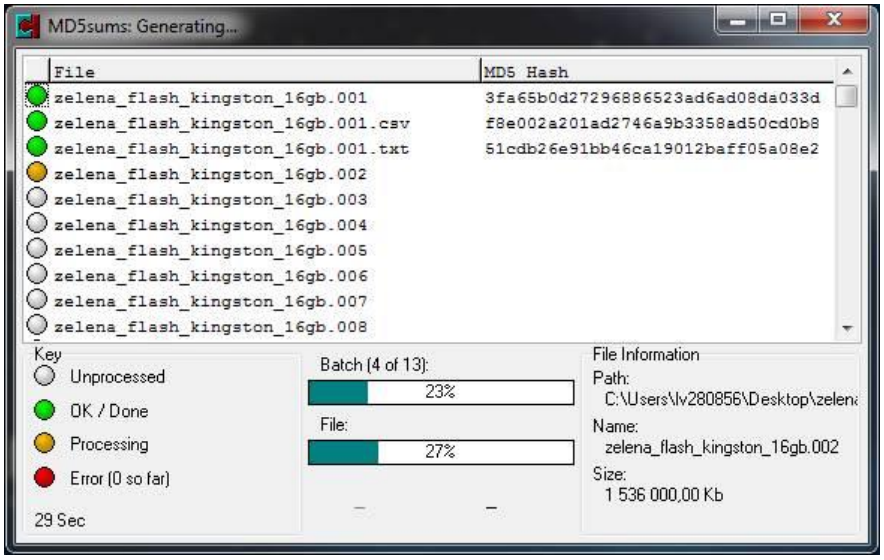
- **SHA-1** - Tento algoritmus vytváří otisk o velikosti 160 bitů. Maximální délka vstupní posloupnosti dat je 2^{64} - 1 bitů. Je založený na stejných principech, které jsou použity v algoritmech MD4 a MD5.
- **SHA-2** - Zahrnuje čtyři hašovací funkce, které jsou pojmenovány podle velikosti vytvářeného otisku v bitech: SHA-224, SHA-256, SHA-384 a SHA-512. Tyto algoritmy jsou součástí standardu FIPS 180-2. Uveřejnění algoritmů se datuje do roku 2001. U těchto hašovacích algoritmů dosud nebyly nalezeny žádné bezpečnostní slabiny. V České republice se hašovací algoritmy SHA-2 staly standardem například v aplikaci datové schránky.

Algoritmy SHA a zejména SHA-2 mají díky vyššímu počtu bitů výsledného otisku několikanásobně lepší zabezpečení, než algoritmus MD5. V současné době nejsou algoritmy SHA-2 široce rozšířeny, ale postupně by měly MD5 zcela nahradit. SHA se již dnes používá u mnoha protokolů i aplikací, například ke kontrole integrity softwarových balíků linuxových distribucí, nebo v DNSSEC.

3.2 Hašování při zajišťování dat

Pro výpočet kontrolních otisků existuje celá řada softwarových nástrojů, se kterými se velice snadno pracuje. Většina forenzních aplikací má podporu hašovacích nástrojů přímo integrovánu. Podporu hašovacích funkcí pod operačním systémem Linux mají i speciální forenzní programy „dd“, „dcfldd“, „dc3dd“, „ddrescue“, které byly speciálně vyvinuty pro forenzní praxi.

Pro následné ověřování autenticity se pak používá pod operačním systémem Linux například aplikace „md5sum“, nebo „sha1sum“, pod operačním systémem Microsoft Windows například „md5summer“.



Obrázek 8. Výpočet MD5 v aplikaci md5summer

Mnohdy se stává, například při zajištění dat vykopírováním, že je zajištěno velké množství souborů dat, například více jak 100 000 souborů. V tomto případě vytváření kontrolních otisků probíhá velmi dlouho. V praxi se proto, pokud to okolnosti případu dovolí, při úkonu zajištění dat provede uložení všech zajištěných souborů do jednoho souboru archivu bez komprese, například typu „rar“, pro který se provede jeden výpočet kontrolního otisku. Jako digitální stopu pak bereme tento archiv. Pokud tento způsob není možný, je nutné vypočítat kontrolní otisky pro každý zajištěný soubor.

Vypočítané kontrolní otisky HASH je nutné vždy uvést do příslušného protokolu úkonu, v rámci kterého se digitální stopy zajišťují. V případě, že je zajištěno velké množství souborů a k nim odpovídající velké množství kontrolních otisků, například několik tisíc, bývá jejich uvedení do protokolu velký problém. V tomto případě je doporučeno vytvořit jeden textový soubor, ve kterém budou uvedeny všechny názvy zajištěných souborů a u každého jeho vypočtený kontrolní otisk. Tento textový soubor je následně také opatřen kontrolním otiskem, k zaručení jeho autentičnosti. Do příslušného protokolu se poté uvádí název tohoto textového souboru a hodnota jeho kontrolního otisku.

V případě, že není možné při zajišťování dat na místě zajistit vytvoření kontrolních otisků HASH, je nutné média na které se zajišťovaná data ukládají zabalit a zapečetit, a tím zajistit autentizaci jako u materiální stopy.

Pokud jsou zajištěná data při úkonu uložena na nepřepisovatelné médium CD, nebo DVD, pak je nutné toto médium řádně a nesmazatelně označit číslem jednacím případu, datem, časem a podpisem zajišťující osoby a nezúčastněné osoby, nebo osoby, která věc vydává, přímo na toto médium. V tomto případě není nutné vytvářet kontrolní otisk, protože se jedná o nepřepisovatelné médium a autentizaci splňují uvedené podpisy na médiu, nicméně se doporučuje vždy provést.

4 FORENZNÍ ANALÝZA DIGITÁLNÍCH DAT

Po zajištění digitálních stop následuje doručení těchto stop znaleckému pracovišti, kde na nich bude provedena forenzní analýza digitálních dat. Tato forenzní analýza, jejíž název pochází z anglického názvu „digital forensics“, vzešla z původní forenzní analýzy počítačů a počítačových systémů, která obsahuje pouze souhrn technik a nástrojů k hledání důkazů na počítači a která byla dále rozšířena i o obory jako jsou kybernetika, informatika, nebo elektronika. Přesná definice forenzní analýzy digitálních dat je:

„užití vědecky odvozených a osvědčených metod k izolování (ochraně), sběru, zhodnocení, identifikaci, analýze, interpretaci, dokumentaci a prezentaci digitálních důkazů ze zdrojů digitálních dat s cílem usnadnění rekonstrukce událostí shledaných zločinnými nebo k odhalení neautorizovaných akcí, které působí rušivě na plánovaný běh operací“. [4]

Forenzní analýza digitálních dat se tak nyní zabývá všemi podobami digitální technologie. Z kriminalistického hlediska tato věda analyzuje jakákoliv digitální data a snaží se nalézt odpověď na sedm základních kriminalistických otázek: Kdo?, Co?, Kdy?, Kde?, Jak?, Čím?, Proč?, což je vlastně metodicky velmi podobné, jako při vyšetřování jakéhokoliv jiného incidentu, nebo trestného činu v reálném světě. Pro účely trestního řízení může provádět tyto forenzní analýzy pouze soudní znalec, nebo kriminalistický expert.

Forenzní analýzy digitálních dat se však neprovádí pouze pro účely trestního řízení. Tyto analýzy mohou být potřebné v celé řadě případů, jako například při různých soudních řízeních, u finančních i softwarových auditů a podobně. Pro potřeby soudního řízení, kde se nejedná o spáchání trestného činu, nebo v případě vyžádání analýz právnickou, nebo fyzickou osobou provádí tyto analýzy civilní soudní znalec. V těchto případech nemusí být digitální stopy zajištěny jako u kriminalistických stop, nicméně je to vždy výhodnější. Pokud by forenzní analýzou dat bylo zjištěno, že byl spáchán trestný čin, pak by tyto digitální stopy byly předány jako důkaz při trestním oznámení. V případě, že digitální stopa nebyla zajištěna jako kriminalistická stopa, může nastat situace, při které následná forenzní analýza dat pro trestní účely nebude možná. Proto by zajištění digitálních stop i mimo trestní řízení mělo splňovat určité standarty a postupy, které byly uvedeny v kapitole o zajišťování digitálních stop.

Vlastní provádění forenzních analýz digitálních dat však ve všech případech využívá stejné principy. Pevné postupy a metodiky provádění forenzních analýz digitálních dat však

nejsou přesně určeny. Specifika různých případů a množství druhů paměťových médií vyžadují rozdílné metody analýz. Vzhledem k rychlému vývoji a rozsáhlosti informačních a komunikačních technologií je určení univerzálních a optimálních postupů velmi obtížné. Pro tyto analýzy existují pouze různá doporučení a ověřené postupy, kterými se experti v kriminalistických ústavech a soudní znalci řídí.

Zajištěné digitální stopy mohou dokazovat spáchání trestného činu, nebo můžou podávat svědectví například o tom, že byla data nějakým způsobem zneužita a podobně. Zajištěná výpočetní technika tak může být jak v roli pachatele, tak i oběti. Relevantní informace, které se zjišťují při provádění forenzní analýzy digitálních dat, se často nacházejí na nepřístupných místech digitálních médií, například v podobě smazaných souborů, fragmentů dat, dat v paměti RAM, nebo jako záznamy a logy různých softwarových služeb, které jsou na daném zařízení instalovány. Z tohoto důvodu je k získání takových informací potřeba znalostí a zkušeností znalců i použití speciálních nástrojů.

4.1 Osoba znalce a její činnosti

Jak již bylo výše zmíněno, forenzní analýzy může provádět kriminalistický expert, nebo soudní znalec. Soudní znalce jmenuje ministr spravedlnosti nebo pověřený předseda krajského soudu. Toto jmenování se vztahuje pro určitou specifickou oblast s příslušnou kvalifikací a praxí, kterou stanovuje Zákon č.36/67 Sb. o znalcích a tlumočnících. U každého místně příslušného krajského soudu je veden seznam znalců podle znaleckých oborů. Mimo tohoto zákona má soudní znalec stanoven výkon činnosti vyhláškou ministerstva spravedlnosti č.37/67 Sb. o provedení zákona o znalcích a tlumočnících. Znalec skládá znalecký slib a je oprávněn zhotovovat znalecké posudky. V praxi se také často lze setkat i s odborným vyjádřením, které, podle § 105 trestního řádu, v jednodušších případech nahrazuje znalecký posudek. Při samotném soudním jednání může soud také jmenovat znalce ad hoc, například z řad odborníků v daném oboru.

Zákon č.36/67 Sb. o znalcích a tlumočnících také stanoví činnost znaleckých ústavů. Proto mohou znalecké posudky provádět i experti Policie ČR v Kriminalistickém ústavu v Praze, nebo na odděleních kriminalistických technik a expertíz krajských ředitelství Policie ČR, případně i dalších znaleckých ústavů zapsaných v seznamech znalců u krajských soudů.

Činnost soudních znalců, nebo policejních expertů v souvislosti se zajišťováním a analýzou digitálních stop v rámci trestního řízení je následující:

- Znalci se v případě potřeby mohou účastnit vyšetřování přímo na místě činu, kam jsou přizváni orgány činnými v trestním řízení, buď jako konzultanti z daného oboru, nebo jako experti na zajišťování digitálních stop. Po zajištění digitálních stop však následné analýzy provádějí zpravidla ve forenzní laboratoři.
- Po zajištění digitálních stop provádí soudní znalci také vytvoření bitových kopií ze zajištěné výpočetní techniky, nebo paměťových médií. Tato činnost je podrobně popsána v předcházejících kapitolách.
- Následně znalec provádí vlastní forenzní analýzy zajištěných digitálních dat. Postup znalce při těchto analýzách je následující:
    - Převzetí zajištěných objektů ke zkoumání. Předávání probíhá protokolárně, kdy v předávacím protokolu musí být zajištěný objekt jednoznačně popsán a identifikován, současně tento protokol musí obsahovat i poučení znalce. Při tomto úkonu znalec zkontroluje přebírané zajištěné objekty obsahující digitální stopy, zda jsou v neporušených a zapečetěných obalech.
    - Znalec obvykle zhotovuje vlastní fotodokumentaci převzatých objektů, která bývá následně součástí znaleckého posudku. Fotograficky se dokumentuje neporušenost obalů a pečetí zajištěných objektů, stav objektů po jejich vybalení a také jakákoliv další manipulace s objekty, jako například nezbytné rozebrání zařízení a podobně.
    - Znalec obdrží od zadavatele forenzní analýzy otázky pro znalecké zkoumání. Tyto otázky musí být přesně a konkrétně formulovány. Z otázek musí být zřejmé, co je od znalce požadováno a na jejich základě znalec stanoví, jaké metody a postupy při provádění forenzní analýzy dat budou použity. Při přebírání otázek znalec zároveň vyhodnotí své odborné a technické možnosti, zda je vůbec možné provést forenzní analýzu a z jejích výsledků odpovědět na položené otázky. Před vlastním sestavením otázek pro znalce se proto doporučuje, za účelem co nejpřesnější formulace otázek, konzultovat možnosti prováděných forenzních analýz a tím i v jakém rozsahu může být očekávána odpověď.
    - Na základě položených otázek provede znalec forenzní analýzu zajištěných dat, při níž použije takové postupy, kterými nejspolehlivěji získá jednoznačné odpovědi na tyto otázky.

4.2 Provádění forenzní analýzy digitálních dat

Forenzní analýza digitálních dat lze rozdělit, jak již plyne z její definice, na několik základních kroků:

- **Izolování a ochrana důkazů** - Tento krok určuje nutnost zachování původní sterility dat a zabránění pozměnění, nebo ztrátě zajištěných dat, což je pro následné kroky forenzní analýzy dat nezbytné. Pokud je to technicky možné, je vždy nutné provádět forenzní analýzy digitálních dat na kopiích zajištěných dat. Tuto zásadu je doporučeno vždy dodržet. V průběhu vykonávání některých postupů, například při spuštění zajištěného počítače, hrozí situace, při které budou digitální stopy pozměněny, nebo dokonce zničeny, například přepsáním přístupových časů souborů. Z tohoto důvodu se forenzní analýzy digitálních dat, pokud je to možné, provádějí právě na kopiích zajištěných digitálních stop, což zaručí následnou opakovatelnost jakéhokoliv úkonu. Výjimku tvoří zajištěná nepřepisovatelná média typu CD a DVD, u kterých se forenzní analýza dat provádí přímo, bez nutnosti vytváření bitových kopií dat. Pouze při výskytu výjimečných okolností, kdy není možné získat kopie originálních dat, lze forenzní analýzu provést na originálních datech. Při tom se však musí dodržovat zvláštní opatření, například použití speciálního hardwarového zařízení pro blokování zápisu na zajištěné paměťové nosiče a podobně.
- **Sběr důkazů** - V tomto kroku se provádí vyextrahování zkoumaných dat ze zajištěného, nebo pracovního paměťového média na jiné technologické paměťové médium, na kterém se budou provádět analýzy, nebo se extrahují data do formy vhodné pro tisk.
- **Identifikace důkazů** - Tento krok zahrnuje jak identifikaci relevantních paměťových médií, na kterých se mohou důležité informace nacházet, tak i potřebné analýzy, při kterých se již identifikují konkrétní data a informace. K paměťovým médiím je nutno přistupovat jako ke zdroji digitálních důkazů, protože samotné paměťové médium není považováno za digitální důkaz.
- **Interpretace informací** - V tomto kroku se získané informace a důkazy vyhodnocují. Je to zřejmě nejvýznamnější krok celé forenzní analýzy digitálních dat, kde je správné vyložení zjištěných informací velice důležité. Tato interpretace

potvrdí, nebo vyvrátí předpokládané hypotézy a dává odpovědi na otázky, které znalec před provedením analýzy obdržel.

- **Dokumentace** - V posledním kroku se dokumentují všechny prováděné činnosti znalce. Znalec v průběhu provádění analýz vede detailní záznamy o provedených činnostech v poznámkách znalce. Závěry a zjištěné skutečnosti, dle položených otázek pro znalce, prezentuje znalec po skončení zkoumání ve svém znaleckém posudku. Je doporučeno prezentovat pouze podstatné skutečnosti a závěry, které se bezprostředně týkají případu a vyhnout se technickým detailům, které by byly v konečném důsledku zbytečné. [5]

K provádění forenzních analýz digitálních dat se používají dva druhy analýz:

- **Fyzická analýza** - Při analýze tohoto druhu se pohlíží na celý prostor paměťového média, například pevného disku, jako na jeden fyzický celek, bez ohledu na souborový systém, který obsahuje. Typickou úlohou tohoto druhu analýzy je například vyhledávání určitého řetězce znaků v celém obsahu disku, tzn. ve všech jeho sektorech. Dále je pomocí tohoto typu analýzy možné zkoumat jednotlivé struktury logických oddílů souborových systémů a podobně. Při provádění fyzické analýzy se musí počítat i s daty, která se nachází v neobsazeném prostoru zkoumaného média, nebo s daty, kde aktivně zapsaná data nedosahují minimální velikosti bloku definovaného operačním systémem a neobsazené místo tohoto bloku tzv. „slack space“ obsahuje fragment dat předchozího souboru, který ale byl již přepsán aktivními daty v bloku.
- **Logická analýza** - Tento druh analýzy již spočívá v logické analýze konkrétních souborů a aplikací, kdy se analýza již zabývá hledáním různých souvislostí se spáchaným trestným činem, nebo jinými skutečnostmi, které jsou nějak důležité pro zadavatele analýzy, nebo objasnění případu. Při této analýze se již zohledňuje i souborový systém, takže je nutná volba správné metody extrakce dat, které se může u různých souborových systémů lišit. [5]

V některých případech se při forenzních analýzách využívají oba druhy forenzních analýz digitálních dat současně.

Při provádění forenzních analýz digitálních dat se lze setkat s několika typy dat:

- **Aktivní data** - Aktivní data tvoří soubory a adresáře aktivně dostupné a viditelné uživatelem z běžícího zařízení výpočetní techniky. Tyto data jsou běžně uložená na zkoumaném paměťovém médiu. Jejich získání pro potřeby analýz bývá nejjednodušší.
- **Archivovaná data** - Tyto data tvoří soubory uložené na výměnných, nebo externích digitálních médiích, nejčastěji na médiích typu CD, DVD, Zip, Jazz, paměťových kartách, flash discích, nebo disketách a dalších.
- **Latentní data** - Zde se jedná o data, která jsou běžnému uživateli skrytá. Jsou to například data smazaných, nebo částečně přepsaných souborů, data po přepsaných souborech v nevyužitých místech média v tzv. "slack space" a podobně. Latentní data se mohou nacházet v alokovaném i nealokovaném prostoru média Tento typ dat se velice obtížně získává a většinou toto zpracování vyžaduje nejdelší dobu.

Při forenzní analýze dat musí znalec počítat i se situací, kdy získané extrahované soubory, nebo případně i celé souborové oddíly na zajištěném médiu budou nějakým způsobem zašifrovány. V tomto případě buď získá od uživatele dešifrovací klíč, nebo se pokusí vhodným nástrojem, nebo za pomocí odborníka na šifrování, takové soubory dešifrovat. Avšak pokud budou použité metody pro zašifrování dostatečně silné, nemusí se dešifrování v reálném čase vůbec podařit a forenzní analýza těchto dat nebude možná.

V průběhu provádění forenzních analýz může znalec nalézt například i informace o páchání jiné trestné činnosti, na kterou se prováděné analýzy nevztahují. V tomto případě je doporučeno tyto informace zdokumentovat a informovat o nich příslušného vyšetřovatele.

4.3 Dokumentace provedených analýz

Celý průběh provádění forenzních analýz digitálních dat je nutné pečlivě dokumentovat. Při této dokumentaci se přesně zaznamenávají jednotlivé kroky, které byly v průběhu analýzy provedeny. Znalec si obvykle vede k danému případu poznámky znalce. Tyto poznámky následně slouží jako podklad k vypracování znaleckého posudku, nebo odborného vyjádření. Součástí těchto poznámek zpravidla bývají kopie povolení ke zkoumání, žádosti o provedení forenzní analýzy a dokumentace, potvrzující integritu důkazů.

Poznámky znalce by měly obsahovat [5]:

- Záznamy z konzultací se zadavatelem forenzní analýzy a poznámky k případu.
- Datum, čas a detailní popisy a důsledky prováděných postupů.
- Z poznámek musí být možné kdykoliv následně provedené postupy opakovat.
- Dokumentace by měla obsahovat informace, jako je verze operačního systému, nainstalované opravné balíčky, verze nainstalovaných aplikací, seznam uživatelů, hesla, topologie sítě a další.
- Dokumentují se i změny provedené v systému, nebo na síti, které mohly vzniknout při úkonu zajištění digitálních stop.
- Informace o vzdálených ukládacích místech, vzdálených přístupů uživatelů, provádění záloh dat na jiné místo, nebo vzdálené úložiště a podobně. Tyto informace bývají v některých případech získány už v průběhu zajištění digitálních stop.
- Dokumentují se i odchylky, které se v případu vyskytly a akce na tyto odchylky v průběhu provádění analýz.

4.3.1 Znalecký posudek

Na vypracování znaleckých posudků se vztahuje vyhláška ministerstva spravedlnosti č. 37/1967 Sb., ve které jsou pevně stanoveny všechny jeho náležitosti. Znalecký posudek musí obsahovat přesný a detailní písemný popis všech provedených úkonů, kterými byly z předložených digitálních stop zjištěny skutečnosti a data, související s položenými otázkami a požadavky v zadání forenzní analýzy digitálních dat. Současně musí obsahovat i přehled všech použitých hardwarových zařízení a softwarových nástrojů, které byly při této analýze použity. Písemný popis znaleckého posudku musí obsahovat také detaily o nálezech, kde musí být podrobně popsány výsledky provedených analýz. Jedná se například o přesný popis místa, kde byly nalezeny digitální stopy související s případem, například na jakém disku, v jakém adresáři a v jakém souboru, dále pak popis ostatních souborů, které podporují nálezy, výsledky hledání řetězců s uvedením použitých filtrů, určení vlastnictví z registračních údajů, popis technik použitých pro šifrování a podobně.

Znalecký posudek by měl obsahovat:

- Číslo jednací případu, nebo jeho podací číslo
- Identifikace znalecké laboratoře, případně i žadatele o zkoumání.
- Datum převzetí žádosti, datum zahájení práce, datum vyhotovení posudku.
- Seznam položek určených ke zkoumání, včetně výrobců, modelů a sériových čísel.
- Seznam požadavků na zkoumání, včetně otázek, které je potřebné znaleckým zkoumáním zodpovědět.
- Popis provedených kroků v průběhu zkoumání, například obnovení smazaných souborů, vyhledání textových řetězců, analýza komunikace a podobně.
- Shrnutí výsledků zkoumání.
- Identifikace a podpis osoby znalce.

V závěru znaleckého posudku musí být uvedeno shrnutí výsledků zkoumání, které bylo provedeno na položkách dodaných k analýze, nebo z odpovědí na otázky, které byly znalci položeny v zadání forenzní analýzy. Informace uvedené ve shrnutí výsledků musí být možné odvodit z popisu provedených úkonů, nebo z detailů o nálezech.

Znalecký posudek obvykle obsahuje ve formě přílohy i fotodokumentaci, pořízenou v průběhu provádění analýz, nebo datová média obsahující nalezené digitální stopy, které souvisejí s odpověďmi na otázky zadání forenzní analýzy, tiskové výstupy jednotlivých důkazních položek a další výstupy vyplývající z provedeného zkoumání. [5]

4.3.2 Odborné vyjádření

V praxi může být po znalci požadováno vystavení odborného vyjádření, například při zkráceném přípravném řízení, kdy se jedná o důkazně jednoduché a méně závažné trestné činy. Rámcově se jedná o zjednodušenou variantu znaleckého posudku. Odborné vyjádření se podle § 112 odst. 2 a § 213 odst. 1 trestního řádu považuje za listinný důkaz, který v těchto případech nahrazuje znalecký posudek. Formální náležitosti a obsah odborného vyjádření neupravuje, ani nestanoví žádný právní předpis. Vypracování odborného vyjádření bývá v mnoha případech rychlé, proto urychluje i vlastní průběh trestního řízení.

II. PRAKTICKÁ ČÁST

5 POSTUPY ZAJIŠTĚNÍ DIGITÁLNÍCH STOP

Zjištění a zajištění výpočetní techniky pro trestní řízení provádí zpravidla dva policisté za přítomnosti nezúčastněné osoby a případně i osoby soudního znalce. Vlastní provádění zajištění digitálních stop v rámci úkonů trestního řízení je možné rozdělit podle několika kritérií:

- Zajištění techniky, obsahující digitální stopy:
  - osobní počítače, servery, notebooky, netbooky, tablety,
  - datová média - pevné disky, flash disky, výměnná média, média CD a DVD, paměťové karty, diskety ZIP, JAZZ a podobně,
  - mobilní telefony a komunikátory, kapesní počítače, diáře, databanky,
  - aktivní síťové prvky - routery, firewaly, NAS servery,
  - ostatní elektronika, která může obsahovat digitální stopy.

- Zajištění dat:
  - zajištění e-mailové komunikace,
  - zajištění www stránek a serverů,
  - zajištění databází,
  - zajištění účetních dat,
  - zajištění ostatních dat dle specifikace spáchaného trestného činu.

- Zajištění tiskových a obrazových výstupů, popř. audio či video záznamů pořízených, nebo zpracovávaných prostřednictvím výpočetní techniky, případně zajištění písemné dokumentace, která má vztah k digitálním stopám.

V dalším textu budou popsány jednotlivé postupy konkrétního zajištění digitálních stop, se kterými se nejčastěji setkáváme.

5.1 Zajišťování výpočetní techniky

5.1.1 Zajištění počítačů

Tento postup popisuje zajištění osobních počítačů, serverů, notebooků a netbooků, případně i tabletů. Pokud je vyšetřovatelem požadováno zkoumání počítačů jako funkční sestavy, zajistí se jako celek. Zajištění celku je vždy výhodnější, protože se během vyšetřování mohou zjistit další skutečnosti, na které je později zaměřeno zkoumání, které by mnohdy nebylo možné provést, pokud by nebyl zajištěn celý počítač.

Monitory, klávesnice, myši a ostatní periferní zařízení se obvykle zajistí, pouze pokud se jedná o speciální, nebo nestandardní typy. V případě pochybností se vždy doporučuje konzultace s expertem. Pokud je to možné, zajišťujeme i technickou dokumentaci počítače, například technický list, evidenční list a podobné.

Postup při zajišťování počítačů:

1) Ihned po zahájení úkonů se zamezí jakékoliv činnosti uživatelů se zajišťovaným počítačem.
2) Fotograficky nebo videozáznamem se zadokumentuje aktuální stav místa nálezu počítače, fyzický stav počítače, zapojení kabeláže, všechny ostatní periferní zařízení a obrazovky monitoru.
3) Pokud je počítač v okamžiku zajišťování spuštěn, přítomný znalec, nebo specialista na zajišťování dat, za dohledu nezúčastněné osoby, by měl provést prvotní ohledání počítače se zaměřením na spuštěné aplikace, aktivované šifrovací nástroje, připojené síťové disky, nastavení a činnost síťové karty a podobně. Při tom je, pokud to okolnosti dovolí, doporučeno vyslechnout uživatele ohledně způsobu využívání počítače, používání šifrování, síťových disků, sdělení hesel a dalších okolností.
    a) Pokud není zjištěno použití šifrování dat, ani jiné překážky, které by mohly znehodnotit digitální stopy, počítač se vypne odpojením od elektrické sítě, vytažením napájecího kabelu. V tomto případě nepoužíváme standardní způsob vypnutí z důvodu zachování dočasných a odkládacích souborů obsahu paměti na pevném disku.
    b) V případě, že v počítači je spuštěn nějaký šifrovací nástroj a po vypnutí by nebylo možné zaručit úspěšné rozšifrování dat, nebo hrozí vypnutím počítače jiné

nebezpečí ztráty digitálních stop, zvolí znalec, nebo specialista na zajištění dat, po případné konzultaci s expertem, některou z následujících alternativ:

i) zajištění dat ze "živého" systému, například vytvořením bitové kopie rozšifrovaného disku, nebo vykopírováním zájmových dat,
ii) znalec provede forenzní analýzu digitálních dat na místě,
iii) pokud to okolnosti dovolí, provede se převoz spuštěného počítače do znalecké laboratoře, za použití speciálních prostředků.

4) Pokud je počítač vypnutý a pokud není přímo vyžadováno zkoumání periferních zařízení počítače, zajistí se pouze základní jednotka s procesorovou a paměťovou částí, tzn. vlastní skříň počítače. V případě zajištění notebooku, netbooku, nebo tabletu, jej vždy zajišťujeme jako celek včetně napájecího zdroje.
5) Zajištěný osobní počítač se zabalí, zajistí před neautorizovanou manipulací a zadokumentuje se způsobem, který je uveden v předcházejících kapitolách.
6) Zpracuje se protokol o provedení všech úkonů, který musí mimo jiné obsahovat přesný popis zajištěného počítače, včetně typu, výrobního čísla, a dalších zjištěných technických parametrů. Nedílnou součástí tohoto protokolu bývá i kopie technické dokumentace soupravy, pokud je možné ji zajistit.

V některých případech lze, po důkladném posouzení situace vyšetřovatelem a znalcem, zajistit z počítačů pouze pevné disky, jejichž zajištění je popsáno v následujícím textu. Tento postup se však nedoporučuje při zajištění počítačových serverů, nebo počítačů, které mají pevné disky zapojeny do RAID pole, protože v mnoha případech nelze bez použití původního řadiče RAID následně data zajistit.

Obrázek 9. Zajištění osobního počítače

5.1.2 Zajištění pevných disků

V případech, kdy je požadováno pouze zkoumání uložených dat bez návaznosti na zkoumání funkční sestavy počítače, lze provést zajištění pouze samotných pevných disků jejich vyjmutím z počítače, nebo jiného zařízení výpočetní techniky. Demontovat pevné disky z počítačů může provádět pouze znalec, nebo proškolený specialista na zajištění dat. V některých případech může být přímo při zajištění vytvořena bitová kopie takového disku.

- V případě notebooků, netbooků a podobných zařízení se nedoporučuje zajišťovat pouze pevné disky, a proto se zajišťují jako celek.
- Pokud není jisté, zda pro zajištění pevného disku postačí pouze jeho vymontování z počítače, zajišťujeme celý počítač také jako celek.
- Externí pevné disky, případně výměnné pevné disky, například v rámečku, se zajišťují vždy jako celek, včetně příslušenství a napájecích zdrojů.

Postup při zajišťování pevných disků demontáží z počítače:

Použije se stejný postup kroků 1 – 3 jako při zajištění počítačů. Pokud to okolnosti dovolí a počítač je vypnutý, je možné provést zajištění pevných disků. Přitom se postupuje následovně:

1) Počítač se odpojí od napájecího napětí vyjmutím kabelu ze zdroje, případně je z počítače odpojena veškerá kabeláž. Počítač musí být spolehlivě vypnutý a odpojený od elektrické sítě, jinak hrozí zničení elektroniky pevného disku, nebo jiných součástí počítače.
2) Demontuje se kryt počítače.
3) Fotograficky nebo videozáznamem se zadokumentuje aktuální stav hardware otevřeného počítače a detailně také zapojení pevných disků.
4) V počítači se identifikují všechny obsažené pevné disky, včetně nezapojených, nebo nestandardně montovaných a u každého se provede odpojení datového i napájecího kabelu.
5) Pevné disky se odšroubují, nebo demontují jiným doporučeným způsobem ze skříně počítače a opět se provede jejich detailní fotodokumentace.
6) Demontované pevné disky se vloží do antistatických obalů a poté se zabalí, nejlépe do bublinkových obálek, zajistí před neautorizovanou manipulací a zadokumentují způsobem, který je uveden v předcházejících kapitolách.
7) Zpracuje se protokol o provedení úkonu, který musí mimo jiné obsahovat přesný popis zajištěných disků s uvedením výrobce, typu, modelu, výrobního čísla, kapacity v GB a technické specifikace datového rozhraní - SATA / IDE / SCSI.

5.1.3 Zajištění výměnných datových médií

Předmětem zajištění jsou všechny typy výměnných datových médií:

- různé typy CD/ DVD/ BD médií,
- různé typy disket, nebo magnetooptických disků,
- média ZIP / JAZZ / SyQuest, a podobných,
- datové pásky,
- flash disky,
- paměťové karty všech typů.

Pokud okolnosti případu, nebo vyšetřovatel nestanoví jinak, obvykle nezajišťujeme lisované disky CD-ROM /DVD-ROM tovární výroby. Při nálezu a zjištění nestandardních a specifických výměnných datových médií se konzultuje způsob jejich zajištění s příslušným expertem.

Zajištění nalezených datových médií v průběhu provádění úkonů podle trestního řádu, je nutné provést vždy, tzn. i při současném zajištění počítačů, nebo demontovaných pevných disků.

Postup při zajišťování výměnných datových médií:

1. Nalezená datová média se roztřídí podle typu, pokud byla zajištěna na různých místech, roztřídí se také podle místností.
2. Roztříděná média se polepí štítkem, nebo jinak označí popisem a očíslují se v posloupné řadě od 1 výše. Toto číslování je součástí protokolu.
3. Všechna označená datová média se poté zabalí, stejný typ datových médií do společného obalu. Zajistí se před neautorizovanou manipulací a zadokumentují způsobem, který je uveden v předcházejících kapitolách s uvedením typů, místa nálezu, počtu kusů a výrobních čísel.
4. Zpracuje se protokol o provedení úkonu, který musí obsahovat i počet a popis zajištěných datových médií

Při balení a pečetění výměnných médií se musí vždy zhodnotit také vlivy elektromagnetického, ultrafialového, nebo tepelného záření na zajišťovaná média a tomu přizpůsobit i volbu vhodného obalu a způsob přepravy.

Zvláštní pozornost při zajišťování flash disků by měla být věnována jejich zjištění. Velice často se stává, že flash disky mívají zcela neočekávatelnou formu, například v podobě hračky, brože, přívěsku, náramku, zapalovače, klíče a dalších.

5.1.4 Zajištění mobilních telefonů, komunikátorů a organizační techniky

Při zajištění tohoto typu techniky se zajišťují také, pokud je to možné i napájecí adaptéry, nebo nabíječky. Je vhodné získat dotazem u dotčené osoby informace týkající se přístupových hesel, nebo kódu PIN a PUK, případně i technickou dokumentaci, ve které jsou tyto kódy uvedeny. Zjištěná hesla se následně uvedou do protokolu.

Postup při zajištění mobilních telefonů a komunikátorů:

Podle konkrétních okolnosti objasňovaného trestného činu mobilní telefon, nebo komunikátor:

- Ponechá se v zapnutém stavu, zapečetí se do bezpečnostního sáčku, který řádně označíme. V případě, že je k dispozici napájecí adaptér, je doporučeno provést zapečetění tak, aby ze zapečetěného obalu vedl napájecí kabel, kterým je možné zařízení dodávat elektrickou energii. Takto zajištěný přístroj je nutné ihned dopravit nejbližšímu znaleckému pracovišti, aby mohly být provedeny základní úkony zkoumání.
- V ostatních případech se vypne. Ve vypnutém stavu je zapínání mobilního telefonu a komunikátoru nepřípustné.
    - Vyjme se baterie a karta SIM. V případě komunikátorů se z důvodu hrozící ztráty dat vyjímat baterii ani kartu SIM nedoporučuje.
    - Z typového štítku přístroje a karty SIM se opíší do protokolu identifikační údaje.
    - Přístroj se uvede do původního stavu opětovným zkompletováním a spolu se zajišťovaným příslušenstvím se vloží se do bezpečnostního sáčku, který se zapečetí, zajistí před neautorizovanou manipulací a zadokumentuje způsobem, který je uveden v předcházejících kapitolách.

Obrázek 10. Zajištěný mobilní telefon

Zajištění digitální organizační techniky

Při zajištění digitální organizační techniky, digitálních diářů, palmtopů, subnotebooků a podobných zařízení se zajišťují také síťové napájecí zdroje, nebo nabíječky, propojovací kabely k počítači, návody k použití, případně i aplikační software. Také v tomto případě je vhodné zjistit od uživatele přístupová hesla.

- Z tohoto typu zařízení se při zajištění nedemontují akumulátory, nebo baterie.
- Zajištěná technika spolu se zajišťovaným příslušenstvím se vloží do bublinkové obálky, nebo bezpečnostního sáčku, zapečetí a zadokumentuje způsobem, uvedeným v předcházejících kapitolách
- Je nutné dopravit takto zajištěnou techniku co nejdříve znaleckému pracovišti.

Při zajištění je také nutno věnovat zvýšenou pozornost omezení vlivu vnějšího elektromagnetického záření na tuto zajišťovanou techniku.

5.1.5 Zajištění aktivních síťových prvků

V některých případech je nutné zajistit i aktivní síťové prvky, jako jsou routery, firewally, bezdrátové access pointy a podobně. U těchto zařízení je nutné rozhodnout, zda se budou zajišťovat celá, nebo jen jejich provozní data a nastavení. Toto rozhodnutí je dáno okolnostmi případu a použitými síťovými prvky, kterých se zajištění týká. Před vypnutím takových zařízení je vždy nutné prověřit možnost získání aktuálních provozních dat, protože mnoho typů těchto zařízení při vypnutí provozní data ztrácí.

Postup při zajištění aktivních síťových prvků:

1. Zajištění aktuálních provozních dat a nastavení. Aktivní síťové prvky ve většině případů umožňují přímou správu z některého počítače v síti. Vždy, pokud je to na místě možné, se nejprve nalezne místo, odkud jsou tyto prvky administrovány. Při tom bude ve většině případů potřeba spolupráce administrátora, nebo správce sítě, se kterým se provede přihlášení do aktivního síťového prvku. Celý tento proces je nutné pečlivě dokumentovat fotograficky, nebo videozáznamem a stejným způsobem dokumentovat i zařízení, kterého se tento úkon týká. Po přihlášení do administrace síťového prvku se může provést zajištění digitálních stop:
   a. Fotograficky, nebo uložením snímků jednotlivých obrazovek administrace síťového prvku, obsahující nastavení tohoto prvku, nebo provozní informace, jako jsou různé logy a podobně.

b. Vykopírováním dat aktivního prvku, nebo vytvořením bitové kopie paměti aktivního prvku, pokud to zařízení umožňuje. Pro všechna takto zajištěná data je nutné vypočítat vhodným hašovacím nástrojem kontrolní otisk tzv. HASH, nejčastěji typu MD5, SHA-1, nebo SHA-2.
   - Takto zajištěná data včetně jejich kontrolního otisku HASH se vypálí na médium CD / DVD, nebo uloží na technologický disk Policie ČR. Toto médium, nebo disk se prokazatelně označí, aby nemohlo dojít k záměně.
   - Zpracuje se protokol o provedení úkonu, který musí obsahovat přesný popis zajištěných dat s uvedením kontrolní sumy HASH.

2. Pokud je nutné zajistit celé zařízení aktivního síťového prvku, například pokud je důležité k objasnění trestného činu, nebo pokud na místě nelze zajistit jeho provozní data, nebo nastavení, postupuje se následovně:
   a. Fotograficky nebo videozáznamem se zadokumentuje aktuální stav místa nálezu aktivního síťového prvku, jeho fyzický stav, výrobní štítky a zapojení kabeláže.
   b. Síťový prvek se vypne odpojením od elektrické sítě vytažením napájecího kabelu.
   c. Zajištěné zařízení se zabalí, zajistí před neautorizovanou manipulací a zadokumentuje způsobem, který je uveden v předcházejících kapitolách.
   d. Zpracuje se protokol o provedení všech úkonů, který musí mimo jiné obsahovat přesný popis zajištěného zařízení, včetně typu, výrobního čísla a dalších zjištěných technických parametrů.

5.1.6 Zajištění ostatní elektroniky, která může obsahovat digitální stopy

Pokud existuje důvodné podezření, že nějaké elektronické zařízení, které nebylo popsáno v předchozím textu, obsahuje digitální stopy důležité pro vyšetřování, může být také zajištěno. Může se jednat například o digitální fotoaparáty a kamery, elektrické psací stroje s pamětí, faxy, satelitní přijímače, inteligentní televizní přijímače, video rekordéry s pevným diskem a mnoho dalších zařízení. Před zajištěním je vždy nutné zvážit všechny okolnosti tak, aby následně bylo možné důkazy ze zařízení získat a také, aby při zajišťování nehrozilo nebezpečí ztráty těchto digitálních stop.

Při zajištění ostatní elektroniky je nutné zajistit také návody k použití, síťové napájecí zdroje, nebo nabíječky, propojovací kabely a další součásti potřebné k jejich provozu.

Postup při zajištění ostatní elektroniky:

1. Fotograficky nebo videozáznamem se zadokumentuje aktuální místo nálezu zařízení, jeho stav, výrobní štítky, zapojení kabeláže a v případě, že je jeho součástí nějaký obrazový výstup a zařízení je spuštěno, dokumentujeme i tento výstup.
2. Zařízení se odpojí od napájení a odpojí se také všechny ostatní kabely.
3. Zajištěné zařízení se zabalí včetně jeho dokumentace, zajistí před neautorizovanou manipulací a zadokumentuje způsobem, který je uveden v předcházejících kapitolách.

Zpracuje se protokol o provedení úkonu, který musí obsahovat přesný popis zajištěného zařízení a výrobního čísla.

5.2 Zajišťování dat

Zajišťování dat je další z možností zajištění digitálních stop. Tento úkon vyžaduje vysokou odbornost osoby, která zajišťování provádí a pro účely trestního řízení jej může provádět pouze osoba soudního znalce, nebo specialista na zajišťování dat, který je držitelem osvědčení o odborné způsobilosti k provádění kriminalisticko-technických úkonů při zajišťování výpočetní techniky a dat na místě činu. Přímé zajištění dat se provádí v následujících případech:

- Pokud je nemožné, nebo neúčelné provést vytvoření bitové kopie digitálních stop.
- Pokud se jedná o dobrovolné vydání dat.
- Při získávání dat z veřejných zdrojů, např. Internetu.

V případě přímého zajištění dat je ve většině případů provedeno vykopírování určitých konkrétních dat, například ze síťového serveru na nějaké datové médium Policie ČR a takto vykopírovaná data jsou následně opatřena kontrolními otisky HASH, které slouží k jejich autentizaci. Takový úkon se provádí za účasti nezúčastněné osoby, případně za účasti správce, nebo vlastníka dat. V případě zajišťování dat z veřejně dostupných zdrojů se přítomnost nezúčastněné osoby nevyžaduje. Možnosti zajištění dat navrhuje znalec, nebo specialista na zajišťování dat a vyšetřovatel případu rozhoduje, jaký způsob zajištění bude proveden.

V následujícím textu budou uvedeny postupy zajištění dat, které se nejčastěji používají. Vždy však záleží na okolnostech a použité technologii, takže se některé postupy mohou v praxi mírně lišit, avšak v principu zůstávají stejné.

5.2.1 Zajištění e-mailových zpráv

Zajišťování e-mailových zpráv provádí policista vlastnící certifikát KUP k provádění kriminalisticko-technických úkonů a zajišťování dat lze rozdělit do dvou skupin:

1. **Zajišťování e-mailových zpráv u podezřelé osoby.** Realizuje se obvykle při domovní prohlídce, prohlídce nebytových prostor, nebo vydáním e-mailových zpráv u poskytovatelů e-mailových služeb.
2. **Zajišťování e-mailových zpráv u poškozeného, nebo oznamovatele.** Provádí se například při oznámení trestného činu páchaného prostřednictvím Internetu, například podvody, výhružné e-maily, phishing a podobně. Realizuje se za souhlasu poškozeného.

Postup a pravidla při zajišťování e-mailových zpráv:

- Zprávy se zajišťují vždy přímo z e-mailového účtu poškozeného, nebo pachatele, buď přímo v e-mailovém klientu uživatele, nebo přes webové rozhraní tohoto účtu.
- Zprávy se zajišťují, pokud je to možné, vždy ve formátu „eml“, nebo „msg“, pokud to možné není, tak vždy se záhlavím e-mailové zprávy.
- E-mailové zprávy se zajišťují výhradně v elektronické podobě.
- Pro všechna zajištěná data e-mailových zpráv se vypočítá vhodnou hašovací funkcí kontrolní otisk tzv. HASH, nejčastěji MD5, SHA-1, nebo SHA-2.
- Takto zajištěná data se včetně jejich kontrolních otisků HASH vypálí na médium CD / DVD, nebo uloží na technologický disk Policie ČR. Toto médium, nebo disk se prokazatelně označí, aby nemohlo dojít k záměně.
- Zpracuje se protokol o provedení úkonu, který musí obsahovat přesný popis zajištěných dat s uvedením hodnot kontrolních otisků HASH.

Z důvodu ztráty informací v záhlaví e-mailové zprávy, nelze zajišťovat e-mailové zprávy:

- které byly přeposlány – vždy je nutné zajistit prvotní přijatý e-mail,
- zkopírováním, nebo vytištěním pouze obsahu e-mailové zprávy.

U zpráv, které byly přeposlány, nebo pokud se pouze zkopíruje, nebo vytiskne obsah e-mailové zprávy, bude záhlaví e-mailové zprávy přepsáno, nebo úplně smazáno.

Vždy je nutné zajistit prvotně přijatou e-mailovou zprávu, protože záhlaví tohoto e-mailu obsahuje informace o přijatém e-mailu, jako například:

- Informace o IP adrese, ze které byl e-mail odeslán. Ta slouží k ustanovení konkrétního uživatele na Internetu. Může se zde nalézat například i IP adresa Intranetu přidělená NAT Routerem, což umožní lokalizovat uživatele i na lokálních sítích připojených k Internetu.
- Informace o celém putování e-mailu počítačovou sítí. Přes který poštovní server byl e-mail odeslán, přesné datum a čas odeslání, jak byl předáván dalšími poštovními servery až k adresátovi a také komu všemu byl dále adresován.
- Další informace o způsobu odeslání, použitém poštovním klientu a podobně.

5.2.2 Zajištění www stránek a web serverů

Zajišťování www stránek je jedním z nejčastějších úkonů zajišťování dat. Jedná se jak o zajištění dat z veřejně dostupných zdrojů Internetu, tak i zajištění www stránek na uzavřených Intranetech různých společností, nebo soukromých osob. Pro trestní řízení se vždy uvádí do protokolu o zajištění dat způsob, jak byla tato stopa v průběhu řízení získána. Rozsah zajištění dat www stránek může být následující:

- *Zajištění jednotlivých www stránek.* Například www stránka diskuse, osobní profil na facebooku a podobně.
- *Zajištění všech www stránek určité domény.* Například doména webu určité organizace, e-shop a podobně.
- *Zajištění všech dat určitého www serveru.* Kompletní zajištění všech dat i se zdrojovými kódy a scripty, databází, grafikou, například pro následnou analýzu autorství a podobně.

Postup zajištění jednotlivých www stránek:

1. Provede se načtení zajišťované www stránky do webového prohlížeče.
2. Provede se dokumentace načtené webové stránky v prohlížeči. Dokumentaci lze provést fotograficky, nebo uložení snímku obrazovky.

3. Kompletní zajišťovaná www stránka se uloží buď přímo z webového prohlížeče, nebo se pro uložení použije nástroj pro ukládání www obsahu, například aplikace HTTrack Website Copier.
4. Pro všechna zajištěná vykopírovaná data www stránky se vypočte kontrolní otisk HASH, nejčastěji MD5, SHA-1, nebo SHA-2.
5. Takto zajištěná data včetně jejich kontrolního otisku HASH se vypálí na médium CD / DVD, nebo uloží na jiné médium Policie ČR. Toto médium se prokazatelně označí, aby nemohlo dojít k záměně.
6. Zpracuje se protokol o provedení úkonu, který musí obsahovat přesné datum a čas zajištění www stránky, způsob provedení úkonu a popis zajištěných dat s uvedením kontrolního otisku HASH.

Postup zajištění všech www stránek určité domény:

1. Pro načtení a uložení všech www stránek určité domény se použije nástroj pro ukládání www obsahu, například HTTrack Website Copier, který se nakonfiguruje pro provedení zálohy celé domény. Průběh zajišťování je doporučeno dokumentovat fotograficky, nebo videozáznamem.
2. Pro všechna zajištěná vykopírovaná data www stránky se vypočte kontrolní otisk HASH, nejčastěji MD5, SHA-1, nebo SHA-2.
3. Takto zajištěná data včetně jejich kontrolního otisku HASH se vypálí na médium CD / DVD, nebo uloží na jiné médium Policie ČR. Toto médium se prokazatelně označí, aby nemohlo dojít k záměně.
4. Zpracuje se protokol o provedení úkonu, který musí obsahovat přesné datum a čas zajištění dat domény a způsob provedení úkonu zajištěných dat s uvedením kontrolních otisků HASH.

Postup zajištění všech dat určitého www serveru:

Zajištění dat probíhá v rámci úkonů trestního řízení přímo na počítači, kde zajišťovaný server běží, což ve většině případů bývá u poskytovatele webhostingu, nebo serverhostingu, který obvykle na příkaz k vydání věci data dobrovolně vydá. V případě zajištění dat na místě postupujeme následovně:

1. Zjištění typu a verze používaného www serveru a platformy, na níž je spuštěn. Zjištění kde a v jaké formě jsou uložena data zajišťovaného www serveru a zjištění přihlašovacích údajů a přístupových hesel.

2. Provede se vykopírování souborů www serveru na technologický disk Policie ČR.
    a. Dle rozhodnutí vyšetřovatele se stejným způsobem zajistí i provozní logy zajišťovaného www serveru.
    b. V případě, kdy aplikace běžící na zajišťovaném www serveru využívá databázový server, zvážit zajištění této databáze přímo z databázového serveru. Zajištění databází je popsáno v následujícím postupu.
3. Pro všechny zajištěné vykopírované soubory se vypočte kontrolní otisk HASH, nejčastěji MD5, SHA-1, nebo SHA-2, který se také uloží na tento technologický disk.
4. Tento technologický pevný disk Policie ČR se prokazatelně označí, aby nemohlo dojít k záměně.
5. Průběh celého zajištění dat se dokumentuje fotograficky, nebo videozáznamem.
6. Zpracuje se protokol o provedení úkonu, který musí obsahovat přesný popis zajištěných dat s uvedením kontrolních otisků HASH.

5.2.3 Zajištění databází

Zajištění databází je úkon, při kterém je nutné, aby specialista na zajištění dat byl velmi dobře seznámen s celou problematikou databází. Často bývá nezbytné způsob zajištění databází konzultovat s expertem. Vždy je nutné data databáze zajistit tak, aby bylo možné jejich následné načtení a analýza. Při tomto úkonu je téměř vždy potřebná spolupráce se správcem databázového serveru, nebo administrátorem.

V krajním případě, kdy vlastník databáze, případně správce databázového serveru odmítl spolupracovat, nebo pokud není zaručeno spolehlivé zajištění všech zájmových dat, je nutné zajistit databázový server, nebo počítač, na kterém se databáze nachází, jako celek.

Zajišťované databáze se můžou nacházet buď na osobním počítači jako lokální databáze, typický příklad je databáze Microsoft Office Access, nebo na databázovém serveru, například Microsoft SQL server, nebo MySQL. Databázový server může být fyzicky umístěn i na zcela jiném místě, například u správce databáze v jiném městě a podobně. Operace s daty databázového serveru se většinou provádí prostřednictvím počítačové sítě dálkově, přes administrační rozhraní databáze.

Postup při zajištění lokálních databází:

1. Zjištění umístění zájmové databáze v počítači.
2. Provede se vykopírování souborů zajišťované databáze na technologický disk Policie ČR. Pro všechny zajištěné vykopírované soubory se vypočte kontrolní otisk HASH, nejčastěji MD5, SHA-1, nebo SHA-2, který se také uloží na tento technologický disk.
3. Tento technologický pevný disk Policie ČR se prokazatelně označí, aby nemohlo dojít k záměně.
4. Průběh celého zajištění dat se dokumentuje fotograficky, nebo videozáznamem.
5. Zpracuje se protokol o provedení úkonu, který musí obsahovat přesný popis zajištěných dat s uvedením kontrolního otisku HASH.

Postup při zajištění databází umístěných na databázových serverech:

1. Zjištění typu a verze používaného databázového serveru a platformy, na níž je spuštěn. Zjištění kde a v jaké formě jsou uložena data zajišťované databáze a zjištění přihlašovacích údajů a přístupových hesel.
2. Za spolupráce správce databázového serveru, nebo administrátora se provede přihlášení k databázovému serveru přes administrační rozhraní.
3. V administračním rozhraní se provede vytvoření úplné zálohy zajišťované databáze, případně „dump“ databáze, nebo se zvolí jiný doporučený způsob zálohy dat. V tomto kroku je nutné spolehlivě zajistit všechna data všech tabulek a dalších součástí zajišťované databáze a uložit je na technologické médium Policie ČR. Tento úkon je vždy závislý na použité technologii a možnostech konkrétního administračního software. Ve výjimečných situacích je přípustné i zajištění celého obsahu databáze exportem do textových souborů.
4. Celý úkon se dokumentuje fotograficky, nebo videozáznamem, případně se ukládají snímky obrazovky.
5. Pro všechny zajištěné soubory databáze uložené na technologickém médiu Policie ČR se vypočítá kontrolní otisk HASH, nejčastěji MD5, SHA-1, nebo SHA-2.
6. Toto médium se prokazatelně označí, aby nemohlo dojít k záměně.
7. Zpracuje se protokol o provedení úkonu, který musí obsahovat přesný popis zajištěných dat s uvedením kontrolních otisků HASH.

5.2.4 Zajištění účetních dat

Zajištění účetních dat je úkon, při kterém se zajišťují pouze data účetního software. Při tomto úkonu je ve většině případů nutná spolupráce uživatele tohoto účetního software, nebo jeho správce. Celá aplikace účetního software se zajišťuje vykopírováním pouze v případě, kdy se nejedná o standardně dostupný software a byl například vytvořen přímo vlastníkem účetních dat, nebo subjektem, který již neexistuje a podobně.

V případě, že uživatel odmítl spolupracovat, nebo pokud není zaručeno spolehlivé zajištění všech dat, zajišťuje se počítač, na kterém jsou uložena data účetního software, jako celek.

Postup zajištění účetních dat:

1. Zjištění používaného účetního software, včetně jeho výrobce a verze a zjištění technologie, na které je spuštěn.
2. Zjištění přihlašovacích údajů a přístupových hesel do účetního programu.
3. Provede se vykopírování všech adresářů účetního software.
4. Za spolupráce uživatele se provede přihlášení do účetního software a vytvoření úplné zálohy všech zájmových dat účetnictví. Tato činnost se dokumentuje fotograficky, nebo videozáznamem. Provede se vykopírování takto vytvořené zálohy účetních dat. Současně se vykopírují i všechny nalezené dřívější zálohy účetních dat vytvořené uživatelem.
    a. V případě, že účetní software využívá databázový server, zvážit zajištění této databáze přímo z databázového serveru. Zajištění databáze je popsáno v předcházejícím postupu.
5. Pro všechna zajištěná vykopírovaná data se vypočte vhodnou hašovací funkcí kontrolní otisk HASH, nejčastěji MD5, SHA-1, nebo SHA-2.
6. Takto zajištěná data včetně jejich kontrolního otisku HASH se vypálí na médium CD / DVD, nebo uloží na technologický disk Policie ČR. Toto médium, nebo pevný disk se prokazatelně označí, aby nemohlo dojít k záměně.
7. Zpracuje se protokol o provedení úkonu, který musí obsahovat přesný popis zajištěných dat s uvedením kontrolního otisku HASH.

6 NEJČASTĚJŠÍ POSTUPY A ZPŮSOBY FORENZNÍ ANALÝZY DIGITÁLNÍCH DAT

Postupů a způsobů provádění forenzních analýz digitálních dat je velké množství. Vždy se jedná o individuální postupy, které mají potvrdit, nebo vyvrátit určité tvrzení, které se v rámci vyšetřování daného případu vyskytlo, a které bylo specifikováno v otázkách při zadání forenzní analýzy. Znalec při provádění forenzních analýz vždy odpovídá pouze na tyto položené otázky a není v jeho kompetenci vyhodnocování důkazní hodnoty zjištěných digitálních stop.

K provádění forenzních analýz digitálních dat se používá mnoho komerčních, nebo i volně šiřitelných softwarových aplikací. Žádný právní předpis naší republiky však neupravuje, ani nestanoví jejich vlastnosti ani použití. Proto o použití konkrétního forenzního software rozhoduje na základě svých potřeb a uvážení soudní znalec. V následujícím textu budou uvedeny pouze nejčastější postupy, které je možné univerzálně použít a u každého bude uvedeno i jakým forenzním nástrojem jej lze případně realizovat.

6.1.1 Příprava před forenzní analýzou

Tento krok předchází provádění většiny forenzních analýz a je v něm nutné důkladně připravit všechny nezbytné zdroje a také technologii, na které se budou analýzy provádět. K provádění forenzních analýz digitálních dat je nutné připravit potřebná technologická paměťová média, například pevné disky, se kterými budeme v průběhu analýz pracovat. Z praxe vyplývá, že ke zkoumání určitého paměťového média je potřeba dvojnásobek jeho úložné kapacity na technologických médiích. Tyto technologická datová média musí být před zahájením analýz forenzně čistá. K zajištění forenzní čistoty datového média je nutné celý datový prostor těchto médií před použitím spolehlivě vymazat, například přepsáním zvolenou hodnotou, nebo nejčastěji vynulováním celého prostoru nástrojem WIPE. V operačním systému Linux se „wipování“ provádí v systémovém terminálu zadáním příkazu:
„**# dd if = /dev/zero of = /dev/sda**“, kde označení sda odpovídá datovému médiu, které bude vynulováno.

Dalším přípravným krokem je obnovení dat z bitových kopií zajištěných digitálních stop. Před zahájením analýz znalec určí, zda bude zkoumání provedeno na duplikátu bitové kopie digitální stopy, nebo bude bitová kopie obnovena na technologické médium, čímž na

technologickém médiu vznikne identická kopie zajištěné stopy. Toto obnovení dat z bitové kopie se obvykle provádí také pod operačním systémem Linux v systémovém terminálu. Příklad možných příkazů k obnovení dat z bitové kopie je následující:

Obnovení dat z bitové kopie za použití příkazu „dd“ :

„**# dd if = /mnt/harddisk/evidence/image.dd of = /dev/sda**“, kde v parametru „if“ je uvedena cesta k souboru bitové kopie digitální stopy a v parametru „of“ je určeno cílové zařízení kam budou data z bitové kopie zapsány.

Obnovení dat z bitové kopie za použití příkazu „cat“ :

„**# cat /mnt/harddisk/evidence/image.dd > /dev/sda**“, kde prvním parametrem příkazu „cat“ je cesta k souboru bitové kopie digitální stopy a výstup tohoto příkazu je přesměrován znakem „>“ na cílové zařízení kam budou data z bitové kopie zapsány.

6.1.2 Extrakce a třídění dat

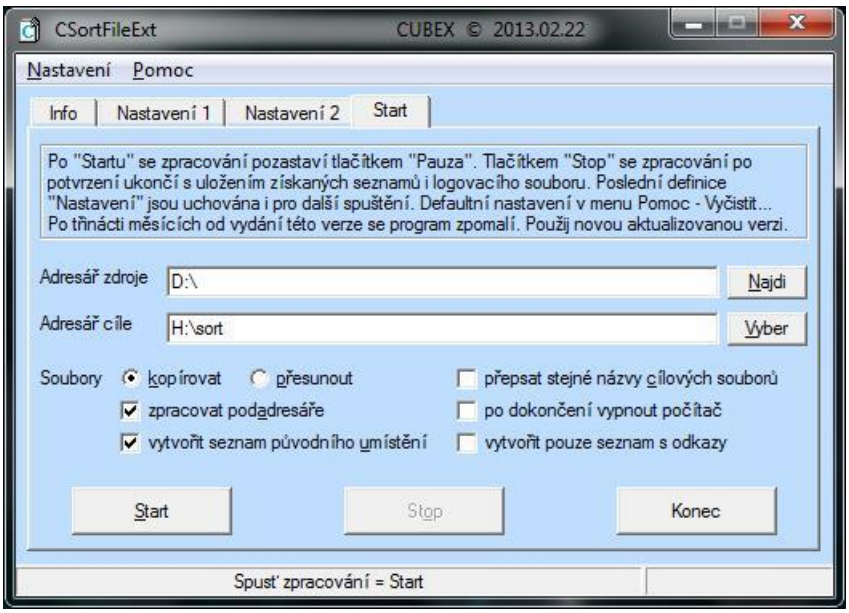
Jedním z nejčastějších požadavků při provádění forenzní analýzy dat bývá vyextrahování určitých typů souborů ze zajištěných datových médií, například vykopírování všech obrazových a video souborů, nebo vykopírování všech dokumentů, souborů „pdf“ a podobně. Mnoho profesionálních forenzních nástrojů, například EnCase, takovou extrakci pomocí filtrů souborů umožňuje přímým exportem.

K vytřídění a exportu souborů byl také na pracovišti informační kriminality krajského ředitelství Policie ČR v Brně vytvořen speciální nástroj CSortFileExt, který je volně šiřitelný a v poslední době velmi používaný pro svoji univerzálnost a jednoduchost použití. Lze jej použít například i k vykopírování zájmových souborů z uživatelských profilů nebo celých diskových oddílů, kam má uživatel povolen přístup. Aplikace pracuje pod operačním systémem Microsoft Windows XP, nebo vyšší.

Tento nástroj vyhledá všechny soubory ze zvoleného zdroje, například z celé logické jednotky disku a nalezené soubory zkopíruje, nebo přesune do cílového adresáře setříděné v podadresářích podle přípon nalezených souborů. Po dokončení zpracování vytváří výstupní textový log soubor a volitelně může být vytvořen také seznam uložených souborů s odkazy na jejich původní umístění. Umožňuje také nastavení filtrů pro zpracování, ve kterých je možné definovat konkrétní přípony souborů, které budou zpracovány, jejich minimální a maximální velikosti a také datum a čas vytvoření, změny či přístupu

k souboru. V nastavení je i možnost definovat názvy souborů a adresářů, které budou při zpracování vynechány.

V tomto nástroji je zohledněno mnoho způsobů a variant, které se při extrakci dat mohou nastat, například tzv. „softlinky“, dlouhé názvy souborů a mnoho dalších.



Obrázek 11. Aplikace CSortFileExt

6.1.3 Vyhledávání řetězců

Další z nejčastěji používaných metod forenzní analýzy dat je vyhledávání textových řetězců. Princip této analýzy spočívá ve vyhledávání konkrétních klíčových slov, které bývají přesně specifikovány v zadání analýzy, v celém datovém prostoru zajištěných digitálních stop. Většina komplexních forenzních aplikací má funkce vyhledávání řetězců přímo integrovány. Pro zadávání těchto řetězců do vyhledávacích nástrojů se velmi často a s velkou úspěšností využívá regulárních výrazů, které umožňují nalézt i různé modifikace klíčových slov, podobná slova a podobně. Podpora regulárních výrazů je v dnešní době u každého kvalitního forenzního nástroje samozřejmostí.

Z hlediska metody lze vyhledávání řetězců realizovat dvěma způsoby:

- **Vyhledávání na fyzické úrovni.** Tato metoda zahrnuje vyhledávání v celém fyzickém prostoru zkoumaného datového média, například u pevných disků se prohledává každý sektor. Výhodou této metody hledání je, že prohledává i neobsazený prostor a „slack space“ souborů. Nevýhodou je nemožnost nalezení

hledaného řetězce, který je nějakým způsobem zakódován, nebo komprimován v nějakém souboru, typicky archivy ZIP, RAR a podobně. Tento způsob vyhledávání řetězců lze realizovat například ve forenzních aplikacích The Sleuth Kit - Autopsy Forensic Browser pod operačními systémy Linux a Microsoft Windows, nebo v aplikaci EnCase Forensic pod operačním systémem Microsoft Windows.

- **Vyhledávání na logické úrovni.** Při použití této metody se vyhledávání řetězců provádí v logickém obsahu souborů. Vyhledávací nástroj otevře a prohledá každý soubor na výskyt hledaného řetězce. V tomto případě už se prohledávají i archívy a kódované soubory, čímž tato metoda doplňuje nedostatky vyhledávání na fyzické úrovni. V praxi se vyhledávání na logické úrovni používá jak pro aktivní data, tak i pro obnovená smazaná data zkoumaného datového média.

  Tuto metodu vyhledávání je možné provést například nástrojem FileLocator Pro, vyvinutý oxfordskou společností Mythicsoft Ltd.

Požadavky na způsob vyhledávání mohou být různé, avšak ke spolehlivému nalezení všech výskytů hledaných řetězců je doporučeno provést jak vyhledávání na fyzické úrovni, tak vyhledávání v aktivních i smazaných souborech na logické úrovni.

6.1.4 Obnovení a analýza smazaných dat

Obnovení a analýza smazaných dat zkoumaného digitálního média bývá standardní součástí většiny metod forenzních analýz zajištěných dat. Tyto úlohy lze také provádět ve většině komplexních forenzních aplikací jako je například EnCase Forensic.

V praxi se také často používají softwarové nástroje, které umožňují i hloubkovou analýzu smazaných dat, za účelem rekonstrukce nevratně smazaných souborů, nebo i jejich fragmentů. Je to například aplikace Recuva vyvíjená společností Piriform, která pracuje pod operačním systémem Microsoft Windows, nebo volně šiřitelné aplikace TestDisk s rozšířením PhotoRec, Foremost, nebo Scalpel pro operační systém Linux, se kterými se pracuje v systémovém terminálu.

Nalezené smazané soubory, nebo jejich fragmenty, se následně extrahují a ukládají na technologický pevný disk znalce. V některých případech se takto podaří obnovit i celou adresářovou strukturu, ve které se smazané soubory nacházely, ale většinou při rekonstrukci souborů hloubkovou analýzou lze získat pouze obsah souborů, bez jejich

názvu a místa uložení. Po dokončení obnovy se pro lepší přehlednost tyto data třídí podle typů výše popsaným nástrojem CSortFileExt. Na obnovených smazaných souborech lze následně provést analýzy stejným způsobem, jako na aktivních datech.

6.1.5 Analýzy souborů a aplikací

Při analýzách tohoto typu se zkoumají konkrétní soubory, nebo celé aplikace, včetně všech jejich souborů a nastavení. Analýzy jsou zaměřeny na získání důležitých informací k zodpovězení položených otázek a poskytují i celkový náhled na systém a na znalosti a zkušenosti uživatele. Analýzy souborů a aplikací zahrnují celou řadu dalších typů analýz, z nichž některé jsou v této kapitole také zmíněny, jako například časové analýzy, analýzy elektronické komunikace a využívání internetu, analýzy sdílení souborů v sítích P2P, analýzy obnovených smazaných souborů a další.

Principem je nalezení zájmových souborů, nebo aplikací na zkoumaném médiu a jejich následné vyhodnocení, které může také určovat další kroky analýz, nebo jiné nezbytné úkony. V průběhu těchto analýz se provádí například:

- Analýza názvů souborů, obsahu souborů a jejich atributů a metadat.
- Vyhledání a vyhodnocení neznámých typů souborů.
- Analýza operačních systémů a jejich konfigurace a nastavení.
- Analýza konkrétních aplikací s určením, vyhledáním a vyhodnocením všech souborů a nastavení, které daná aplikace používá. Současně se vyhodnocuje nastavení a způsob používání této aplikace konkrétními uživateli a zvážení všech vztahů mezi soubory, nebo aplikacemi.
- Analýza souborů logů, provozních a odkládací souborů, chybových hlášení aplikací, nebo služeb systému.
- Analýza smazaných dat k nalezení předchozích verzí dat zkoumané aplikace a podobně.

Často se stává, že se při provádění forenzních analýz nalezne virtualizační software a soubory virtuálních disků, například aplikace VirtualBox, Microsoft Virtual PC, nebo VMware. V tomto případě je nutné kopii nalezeného souboru virtuálního disku připojit, nejlépe v režimu jen pro čtení, k forenznímu virtuálnímu stroji znalce, ve kterém jsou nainstalovány potřebné forenzní nástroje a provést další analýzu i zde.

V jiném případě je zase naopak nutné zajištěnou bitovou kopii disku zkoumaného počítače převést do virtuální podoby, aby mohla být provedena analýza spuštěného počítače ve virtuálním stroji. Tento úkon je v některých případech potřebný pro provedení komplexní analýzy aplikací, nebo analýzu chování a způsobu práce uživatelů. I v těchto případech se nejčastěji používají aplikace VirtualBox, Microsoft Virtual PC, nebo VMware. Převod bitové kopie disku zkoumaného počítače na virtuální disk lze provést ve většině virtualizačních aplikací z příkazového řádku, nebo systémového terminálu.

6.1.6 Časové analýzy

V požadavcích na forenzní analýzu dat se také objevují žádosti o určení informací, které jsou vztaženy ke konkrétnímu datu a času, nebo je potřebné konkrétní datum a čas zjistit. Jedná se o typické úlohy zjištění: Kdy byl počítač naposledy spuštěn? Kdy byl vytvořen, vytisknut, naposledy načten, nebo upraven určitý soubor? Kdy byla spuštěna určitá aplikace, nebo služba operačního systému? Kdy se stala určitá událost v systému? Kdy prováděl konkrétní uživatel určitou činnost a podobně.

Z pohledu získávání časových dat mohou být použity dvě různé metody:

- **Analýzy atributů adresářů, souborů a jejich metadat**. Z datových a časových značek v adresářové a souborové struktuře, případně v metadatech souborů nalézáme odpovědi na otázky typu: kdy a kým byl soubor vytvořen, kdy byl naposledy modifikován, nebo vytištěn, nebo jaké je datum a čas posledního přístupu k souboru.
- **Analýzy systémových a provozních logů**. Zde se analyzují systémové a provozní záznamy, které se průběžně vytváří při práci s počítačem a ve kterých je také uváděn datum a čas provedení jednotlivých činností. Může se jednat o instalační logy, záznamy o chybách, bezpečnostní záznamy, soubory dokumentující historii činností a podobně.

Při provádění časových analýz je také nutné přihlížet na nastavení BIOSu zkoumaného počítače. Veškeré časové údaje v počítači jsou totiž svázány se systémovým časem BIOSu, který je však možné uživatelsky měnit. Proto je pro přesné určení časových údajů nutné znát současné nastavení systémového času, které se provádí kontrolovaným bootem zajištěného počítače, s odpojenými datovými médii, například již při úkonu vytvoření bitových kopií datových médií. [5]

K provádění časových analýz se v praxi často využívá vlastností operačního systému Linux, který za použití běžných příkazů v systémovém terminálu setřídí a zobrazí soubory podle zvolených časových atributů. Možné příkazy jsou následující:

Setříděný výpis posledního přístupu k souborům za použití příkazu „find“ :

„**# find . | while read FILE;do ls -l -d -A -g -G -Q -u --full-time "$FILE";done | cut --complement -d ' ' -f 1-3 | sort**“

Setříděný výpis poslední modifikace souborů za použití příkazu „find“ :

„**# find . | while read FILE;do ls -a -d -l --full-time "$FILE";done | cut --complement -d ' ' -f 1-5 | sort**“

6.1.7 Analýzy elektronické komunikace a využívání internetu

Velmi častým typem forenzní analýzy dat je také analýza elektronické komunikace, která kromě e-mailu zahrnuje také analýzu komunikačních aplikací typu ICQ, Skype, MSN, AIM a celé řady dalších typů elektronické komunikace. Provedení této analýzy spočívá ve vyhledání a vyhodnocení všech nainstalovaných komunikačních a e-mailových aplikací a jejich provozních dat na zkoumaném počítači.

Častým požadavkem bývá vykopírování souborů elektronické komunikace, nebo e-mailů ve formátech, které následně může vyšetřovatel prohlížet i bez nutnosti instalace nějakého forenzního nástroje. V případě e-mailových zpráv se provádí jejich export do souborů typu „eml“ a „msg“, v případě ostatní komunikace v textových souborech.

V mnoha případech je také požadována analýza záhlaví zajištěných e-mailových zpráv, které obsahuje všechny dostupné informace o analyzovaném emailu:

- Informace o IP adrese, ze které byl e-mail odeslán. Ta slouží k ustanovení konkrétního uživatele na Internetu. Může se zde nalézat například i IP adresa Intranetu přidělená NAT Routerem, což umožní lokalizovat uživatele i na lokálních sítích připojených k Internetu.
- Informace o celém putování e-mailové zprávy počítačovou sítí. Přes který poštovní server byla odeslána, přesné datum a čas odeslání i jak byl předáván dalšími poštovními servery až k adresátovi.
- Komu byl dále adresován.
- Další informace, například o způsobu odeslání, použitém poštovním klientu a další.

Při analýze využívání internetu se analýza zaměřuje na nainstalované internetové prohlížeče a jejich uložená data. Analýzou těchto dat zjišťujeme a vyhodnocujeme například historii prohlížení internetu, dočasné a stahované soubory, historie formulářů, případně i uložená hesla.

Zpracování analýz elektronické komunikace a využívání internetu v různém rozsahu je možné provádět v mnoha nástrojích, například SkypeLogView, nebo IEHistoryView a dalších vyvíjených společností NirSoft. Jednoznačně však na tomto poli dominuje forenzní nástroj Belkasoft Evidence Center 2013 vyvíjený ruskou společností Belkasoft.

6.1.8 Vyhledávání souborů podle známých otisků HASH

Podstatou tohoto typu analýz je vytvoření kontrolních otisků HASH všech souborů zkoumaného datového média a jejich následné porovnávání s databází známých otisků HASH. Tato databáze obsahuje kontrolní otisky známých souborů, jejichž držení je například nelegální, typicky se jedná o otisky souborů obsahující dětskou pornografii, nebo jsou v databázi kontrolní otisky autorských děl, které se na zkoumaném médiu budou hledat a podobně. Dle použitého nástroje pro vyhledávání volíme vhodnou hašovací funkci, kterou bývá obvykle funkce MD5. Nutno podotknout, že nález shody v kontrolním otisku není ještě bráno jako důkaz. V tomto případě je nutné provést důkladnou analýzu všech typů souborů na zkoumaném médiu, kterých se databáze známých otisků týká.

Vyhledávání souborů podle známých otisků HASH lze realizovat například ve forenzní aplikaci The Sleuth Kit - Autopsy Forensic Browser pod operačním systémem Linux, nebo Microsoft Windows, do které v průběhu práce lze přímo importovat soubory databází známých otisků a spouštět vyhledávání. Je nutné však počítat se situací, že vyhledávání bude probíhat velmi dlouho.

6.1.9 Analýzy sdílení souborů v sítích P2P

Tento typ analýzy spočívá v nalezení nainstalovaných aplikací a klientů pro sdílení v sítích P2P a všech jejich provozních dat na zkoumaném datovém médiu a jejich následné vyhodnocení. Zkratka P2P v tomto případě označuje síť peer-to-peer, pomocí které uživatelé sdílejí a stahují data. Typů sítí P2P je velké množství, proto je nutné věnovat velkou pozornost při vyhledávání takových aplikací na zkoumaném datovém médiu. Nejčastěji se lze setkat s aplikacemi pracujícími s protokoly „BitTorrent“ a „Direct Connect“.

Při nalezení aplikace sítě P2P na zkoumaném datovém médiu následuje podrobná analýza všech dat této aplikace, která zahrnuje:

- Analýzu souborů provozních logů za účelem zjištění kdy byla aplikace používána, jaká data byla sdílena a komu, nebo jaká data byla stahována a od koho.
- Analýzu nastavení aplikace a zjištění přihlašovacích údajů uživatelů.
- Analýzu místa ukládání a sdílení dat, která zahrnuje i analýzu vlastních sdílených, nebo stahovaných dat.
- Analýzu smazaných dat, za účelem nalezení dřívějších logů aplikace, nebo dat, která byla sdílena, nebo ukládána dříve.

Ve většině případů znalec obdrží seznam zájmových souborů, které měly být sdíleny, nebo stahovány a s tímto seznamem pak následně porovnává zjištěné informace.

K provádění tohoto typu analýz se v praxi osvědčil i forenzní nástroj Belkasoft Evidence Center 2013.

6.1.10 Analýza obsahu operační paměti

Pokud byl při zajištění dat získán i obraz obsahu operační paměti počítače provádí se jeho analýza, ke zjištění všech informací o činnostech a předchozí aktivitě na zkoumaném počítači. Tyto informace mohou být velice důležité pro vyšetřování případu, neboť rozsah získaných informací bývá velmi obsáhlý a vypovídající. Při této analýze lze získat například:

- Informace o systému, spuštěných procesech, jejich proces SID a proměnných prostředí.
- Obsah paměti a paměťové mapy pro každý proces, nebo knihovnu DLL.
- Informace o mapování pamětí.
- Obsah dat uživatelských relací a dočasných dat.
- Informace o otevřených připojeních k síti a otevřených síťových socketech.
- Historii příkazového řádku systémové konzole.
- Informace o událostech a zprávách systému a mnoho dalších.

V průběhu analýzy lze obraz paměti prohledávat na datové vzory, nebo textové řetězce a lze využít i vyhledávání s použitím regulárních výrazů. Z výsledků této analýzy lze

odhalit i skrytě běžící procesy, například keylogery, nebo také použité kryptografické klíče a podobně.

Pro extrakci digitálních artefaktů z obrazu operační pamětí RAM se v praxi používá aplikace Volatility Framework vyvíjený společností Volatile Systems LLC. Jedná se o otevřenou sbírku nástrojů, naprogramovanou v Pythonu pod licencí GNU General Public, která je určena k analýze operační paměti všech typů operačního systému Microsoft Windows.

6.1.11 Analýzy historie připojených USB zařízení

V některých případech je požadováno zjištění informací o tom, kdy a jaké zařízení bylo připojeno prostřednictvím rozhraní USB ke zkoumanému počítači. Jedná se převážně o historii používaných paměťových zařízení, například flash disky a podobně, které se ve velké míře používají pro zálohování, nebo přenos dat.

V systémech Microsoft Windows je tato historie USB zařízení uložena v souboru „setupapi.log“, nebo u novějších verzí v souborech „setupapi.dev.log“ a „setupapi.app.log“. V operačních systémech typu Linux lze historii připojení USB zařízení získat například z logů událostí jádra v souboru „/var/log/kern.log“. Z těchto textových souborů logů lze zjistit informace o všech USB zařízeních, které byly v minulosti připojené k systému, včetně data a času jejich připojení, případně i dalších podrobnějších informací k těmto zařízením.

V praxi se tato analýza zpracovává ve volně šiřitelném softwarovém nástroji USBDeview společnosti NirSoft, nebo v komplexní forenzní aplikaci Belkasoft Evidence Center 2013.

6.1.12 Analýzy vlastnictví, šíření a přechovávání dat

Velmi častým a žádaným typem forenzní analýzy je analýza vlastnictví, šíření a přechovávání dat. Spočívá v nalezení zájmových dat na zkoumaných datových médiích a v následném prokázání, že konkrétní uživatel tyto data vlastní, vytváří, modifikuje, šíří, nebo přechovává. Typicky se jedná o analýzy k případům, při kterých se objasňuje výroba, šíření a přechovávání nelegálního obsahu dat, například dětské pornografie a podobně. V těchto případech bývá také důležité prokázat, že se s těmito daty manipulovalo vědomě. Analýzy tohoto typu zahrnují i dalších typy analýz, jako jsou například analýzy souborů a aplikací, časové analýzy, nebo analýzy elektronické komunikace. Při provádění analýz vlastnictví, šíření a přechovávání dat zjišťujeme:

- Počet, typ a umístění nalezených zájmových souborů. Důležité jsou i názvy souborů a adresářů, zejména pokud je vytvořil uživatel počítače, také místa a soubory chráněné heslem.
- Informace z atributů a metadat zájmových souborů, ze kterých lze zjistit například konkrétního uživatele, který tento soubor vytvořil, modifikoval, nebo s ním jinak manipuloval a kdy.
- V případě šíření se zjišťuje jakým způsobem, komu a kdy byly zájmové soubory poskytnuty, nebo odkud byly získány, například prostřednictvím e-mailu, sítě P2P, odesláním přes aplikaci Skype a podobně.

6.1.13 Softwarový audit počítače

Na konec je třeba také zmínit softwarový audit počítače, který do forenzních analýz digitálních dat také patří. Softwarový audit spočívá ve zjištění veškerého nainstalovaného software ve zkoumaném počítači. Toto zjišťování se provádí skenováním všech datových médií zkoumaného počítače pomocí vhodného nástroje, tzv. softwarového scanneru.

Výstupem softwarového auditu je úplná inventarizace veškerého nainstalovaného software, který je obsažen na datových médiích zkoumaného počítače, většinou ve formě seznamu, nebo databáze, kde jsou ke každému nalezenému software uvedeny informace o názvu, verzi, použitém licenčním klíči a další. V případě softwarového auditu prováděném v rámci šetření trestné činnosti, například při porušování autorských práv podle § 270 trestního zákoníku, se výsledky nálezu prezentované ve znaleckém posudku předkládají orgánům činným v trestním řízení. Teprve orgány činné v trestním řízení vyhodnocují legálnost tohoto nalezeného software, kdy jej porovnají s účetními doklady a dalšími doklady, které prokazují legální nabytí software. V jiných případech může být softwarový audit prováděn například na objednávku ve společnosti objednatele a podobně.

V praxi u Policie ČR se k provádění softwarového auditu používá softwarový scanner AW Caesar, vytvořený společností Free RW Soft v. o. s., který je mezi znalci velmi používaný. Na vývoji tohoto nástroje se podílí i Kriminalistický ústav v Praze. AW Caesar porovnává výsledky skenování s velmi rozsáhlou databází softwarových programů, která je neustále aktualizována. Využívá strom závislostí souborů, umožňuje k získaným údajům doplňovat popisy a další podrobnosti a v případě nalezení nového software umožňuje jeho přidání do databáze. Při vyhledávání software používá i heuristické postupy, které odhalí možné maskování, nestandardní instalace a přejmenování aplikací.

7 OHROŽENÍ A RIZIKA PŘI PRÁCI S DIGITÁLNÍMI STOPAMI

Tato kapitola je zaměřena na popis možných ohrožení a rizik v celém procesu práce s digitálními stopami. Vznik rizik a ohrožení nelze při práci s digitálními stopami nikdy vyloučit. I při důsledném dodržení všech existujících bezpečnostních pravidel, zásad a doporučených postupů, mohou nastat situace, při kterých vzniknou rizika, nebo ohrožení digitálních stop. Tyto rizika mohou být způsobeny technikou, nebo použitou technologií, například při závadách, poruchách, nebo při selhání zajištěných zařízení, které obsahují digitální stopy, nebo technologických datových médií, na kterých jsou tyto stopy uloženy. Za dalšími riziky a ohroženími stojí většinou selhání lidského faktoru, nedodržení pravidel pro bezpečnou manipulaci s digitálními stopami, nebo nedodržení zásad pro jejich skladování. U rizik způsobených selháním lidského faktoru se může jednat o rizika způsobená úmyslně, neúmyslně, nebo způsobená nedbalostí. V následujícím textu budou podrobněji popsána nejdůležitější rizika a ohrožení v jednotlivých etapách práce s digitálními stopami a zároveň také navrhovaná protiopatření, kterými se uvedená rizika zmírní, nebo úplně eliminují.

7.1 Rizika při zajišťování digitálních stop

Riziko: Nezajištění všech digitálních stop.

Jedná se o situace v průběhu prováděných úkonů, při kterých se digitální stopy zajišťují, například při ohledání místa činu, nebo při provádění domovních prohlídek a podobně, kdy objekty, které obsahují digitální stopy, nebudou nalezeny a tím pádem nebudou ani zajištěny. Toto riziko se přímo netýká ztráty, nebo ohrožení dat, má však velký význam pro celé vyšetřování případu, které bez zajištění všech důkazů nemusí být úspěšné. Vyhledání všech elektronických zařízení, které mohou obsahovat digitální stopy, bývá v praxi velmi náročné. Běžně se lze setkat například s různými podobami flash disků, které mají mnohdy tvar hraček, ozdob, náramků, přívěšků a dalších objektů, kdy je velice obtížné takové flash disky identifikovat. Dále se může také jednat o zařízení, které bývá ukryto na nepřístupných místech, nebo v různých úkrytech, například NAS server skrytý na půdě, nebo Wifi zařízení skryté ve stropním podhledu a podobně.

Protiopatření: V tomto případě se jedná pouze o doporučení, provádět vyhledávání objektů k zajištění velmi důkladně a předvídat a nepodceňovat možná místa, nebo objekty, které by mohly digitální stopy obsahovat. V případě pochybností je doporučeno konzultovat problém s expertem v oboru.

Riziko: Neodborné zajištění digitálních stop.

Pokud digitální stopy, nebo zařízení obsahující digitální stopy, nezajišťuje odborník, který je pro tuto činnost vyškolený a je držitelem příslušných oprávnění, hrozí riziko, že digitální stopy nebudou správně zajištěny, nebo nebudou zajištěny všechny. V tomto případě může nastat například situace, kdy neodborník nesprávně vyhodnotí výběr objektů k zajištění, nebo neprovede zajištění dle doporučených postupů, případně opomene k zajištěným datům vytvořit kontrolní otisk pomocí hašovací funkce a podobně. V těchto případech tím znesnadní, nebo znemožní následné forenzní analýzy digitálních dat, nebo v nejhorším případě hrozí právní znehodnocení důkazu, kdy digitální stopu, například z důvodu absence kontrolního otisku HASH, vyloučí přímo soud.

Protiopatření: Aby se popsaným situacím předešlo, je nutné vždy volat specialisty na zajištění dat, nebo příslušného soudního znalce.

Riziko: Nesprávné zabalení, nebo autentizace digitální stopy.

Pokud jsou při zajištění objekty, obsahující digitální stopy, nesprávně zabaleny a zapečetěny, nebo nejsou zabaleny vůbec, například pokud by bylo možné i po zabalení s objektem neoprávněně manipulovat, rozebírat, nebo připojovat k němu jiná zařízení, hrozí napadení takto zajištěné digitální stopy jako důkazu, což může vést až k vyloučení důkazu soudem. Stejné riziko hrozí i v případech, kdy je nesprávně provedena autentizace digitálních stop a mohla by být zpochybněna jejich pravost. U zajištěných objektů, které obsahují digitální stopy, se jedná o nesprávné, nebo chybějící zapečetění zajišťovaného objektu, kdy pečeť musí obsahovat podpisy zúčastněných osob při zajištění. U zajištěných dat se jedná o chybějící kontrolní otisky HASH.

Protiopatření: Vždy dodržovat doporučené postupy pro balení a autentizaci digitálních stop a po zabalení provádět kontrolu, zda je zajištěný objekt dostatečně zajištěn proti neoprávněné manipulaci a řádně zapečetěn. Kontrola by měla být provedena i u vytvořeného kontrolního otisku HASH u zajištěných dat. Tyto kontroly by měly být provedeny zúčastněnými osobami při úkonu zajištění. Zajištěné objekty je po zabalení a zapečetění doporučeno fotograficky dokumentovat. Zároveň je doporučeno

dokumentovat fotograficky, nebo videozáznamem i vytváření kontrolních otisků při zajišťování dat.

Riziko: Nesprávná, nebo neúplná dokumentace zajištění digitálních stop v protokolu.

V tomto případě se jedná o nedbalost při provádění písemné dokumentace o zajištění digitálních stop v příslušných protokolech prováděných úkonů. Jde například o neuvedení hodnot vytvořených kontrolních otisků HASH u zajištěných dat, nebo překlepy ve výrobních číslech, hodnotách kontrolních otisků a podobně. Nesprávná, nebo neúplná dokumentace při zajištění digitálních stop může vést ke zpochybnění těchto stop, případně i k vyloučení nalezených důkazů soudem.

Protiopatření: I v tomto případě je jediné protiopatření důsledná kontrola všech uvedených údajů v příslušném protokolu, kterou by měly nezávisle provést všechny zúčastněné osoby podepsané v tomto protokolu.

Riziko: Znehodnocení digitální stopy při transportu.

Pokud nejsou zajištěné objekty obsahující digitální stopy zabezpečeny proti poškození, například zabezpečením proti posunutí, vhodným uložením, nebo dalším zabalením do bublinkových fólií a podobně, hrozí, že budou při transportu poškozeny, nebo zničeny.

Protiopatření: V tomto případě je k zabránění tohoto rizika nutné dbát na šetrné zacházení se zajištěnými stopami. Před transportem je nutné zajistit, aby zajištěné stopy byly vhodně zabezpečeny proti poškození a v průběhu transportu, pokud to situace umožňuje, provádět kontrolu tohoto zabezpečení.

7.2 Rizika při vytváření bitových kopií digitálních stop

Riziko: Vytváření bitových kopií z médií, které mají závadu.

V některých případech je zajištěno datové médium, které pravděpodobně obsahuje důležité digitální důkazy, ale je nějakým způsobem poškozeno, nebo má závadu technického rázu. V případě že se nám z tohoto datového média nepodaří vytvořit bitovou kopii, nezískáme žádná data, která by mohla být analyzována, nebo považována jako důkaz.

Protiopatření: Pro tento případ neexistuje žádné protiopatření, protože takovou situaci nelze předem ovlivnit. Lze pouze doporučit konzultaci s odborníkem na předmětný typ datového média, nebo servisním technikem a zkusit nalézt způsob, jakým bude možné data z poškozeného datového média získat. Například opravou tohoto média, pokud je vůbec

možná. V případě částečné závady, kdy má poruchu například jen určitá oblast pevného disku, je k vytvoření bitové kopie tohoto datového média nutné použít takové softwarové nástroje, které s výskytem závad na datovém médiu umí pracovat.

Riziko: Porucha datového média při vytváření bitové kopie.

Toto riziko má velmi malou pravděpodobnost, že nastane, nicméně je nutné je také zmínit. Porucha datového média může být způsobena buď nesprávným zapojením, nebo skrytou vadou datového média, která se projeví v okamžiku vytváření bitové kopie. Může se týkat jak originálního zajištěného datového média, ze kterého vytváříme bitovou kopii, tak i technologického datového média, kam se vytvářená bitová kopie ukládá. V případě poruchy originálního zajištěného datového média hrozí ztráta všech nenačtených dat, na druhé straně při poruše technologického datového média je nutná výměna tohoto vadného média a opakování celého úkonu vytvoření bitové kopie.

Protiopatření: Pro zmírnění rizika nesprávného zapojením datových médií je nutné, aby veškerou manipulaci a zapojování prováděl pouze proškolený odborník, za současného dodržení všech pravidel, zajišťujících bezpečnou manipulaci a bezchybný provoz předmětného zařízení, případně i provedení nezávislé kontroly zapojení před spuštěním. V případě výskytu skryté vady zajištěného datového média však většinou neexistují jiné možnosti a takovou situaci nelze ani jinak předvídat.

Riziko: Ztráta dat z nedbalosti při vytváření bitové kopie.

Za tímto rizikem stojí lidský faktor. Jedná se o omyly a chyby osoby, která provádí vytvoření bitové kopie, například při nastavování parametrů, volby zdrojového a cílového média, volby místa uložení a podobně. Pokud se při vytváření bitových kopií využívá operační systém Linux, bývá pravidlem, že se příkazy zadávají v systémovém terminálu. I malý překlep, nebo špatná volba místa uložení při zadávání příkazu může nevratně zničit zajišťovanou digitální stopu.

Protiopatření: Vždy provádět několikanásobnou kontrolu každého zadávaného příkazu před jeho vložením a potvrzením, například i jinou oprávněnou osobou. Vždy zvážit všechny možné důsledky prováděných operací. Případné nejasnosti je doporučeno konzultovat zadávané příkazy se znalcem v oboru.

Riziko: Úmyslné zničení dat při vytváření bitové kopie digitální stopy.

Toto riziko je také způsobeno lidským faktorem. Při vytváření bitových kopií na místě činu, nebo v průběhu konání domovních prohlídek, prohlídek jiných prostor, nebo ve forenzní laboratoři, bývají přítomny i dotčené osoby, například osoby, podezřelé ze spáchání nějakého trestného činu, majitelé počítačů, nebo jejich rodinní příslušníci. Tyto osoby by mohly mít zájem na zničení digitálních stop. Z jejich strany existuje reálné riziko, že se pokusí zničit digitální stopy, nebo se pokusí vytvoření bitové kopie nějakým způsobem znemožnit, nebo alespoň narušit.

Protiopatření: Vždy je nutné zajistit bezpečné provedení úkonu vytvoření bitové kopie digitální stopy. Dotčené a nepovolané osoby nesmí za žádných okolností manipulovat s jakýmkoliv zařízením, které by mohlo obsahovat digitální stopy. Tyto osoby je v průběhu prováděných úkonů nutné důsledně střežit a nenechat bez dozoru. Proto je nutné, aby střežení těchto osob bylo zajištěno jinými osobami, než specialisty na zajištění dat. V případě, že se bitové kopie digitálních stop vytvářejí ve forenzní laboratoři, je ke zmírnění rizik doporučeno po spuštění vytvoření bitové kopie digitální stopy místnost, kde se tento úkon provádí zabezpečit proti neoprávněnému vstupu a zapečetit. Při opětovném vstupu pak proběhne kontrola zabezpečení a neporušenosti pečetí.

Riziko: Nelze vytvořit bitové kopie datových médií ze spuštěného „živého“ systému.

Při nutnosti vytvořit bitovou kopii datových médií ze spuštěného "živého" systému, může nastat situace, kdy do zajištěného systému nelze připojit žádné USB zařízení, nebo nelze spustit žádný forenzní nástroj, například z důvodu uzamčení profilu uživatele, nebo při nedostatečném oprávnění uživatele a podobně. Potom je vytvoření bitových kopií z datových médií tohoto spuštěného "živého" systému nemožné. Pokud je v takovém systému navíc aktivně používáno šifrování a systém pak nelze bez ztráty dat vypnout, hrozí reálné riziko, že nebude možné zajistit rozšifrovaná data. Pokud uživatel takového systému nespolupracuje a odmítá sdělit hesla pro rozšifrování dat, nebo v případě, že úmyslně sdělí neplatné heslo, následné vytvoření bitových kopií datových médií z vypnutého systému bude zřejmě neúčelné, neboť se nemusí podařit zajištěná data rozšifrovat.

Protiopatření: Pro tyto případy neexistuje protiopatření, protože situaci předem není známa. V těchto případech, pokud to bude vůbec možné, je nutné provést forenzní analýzu digitálních stop přímo na místě ve spuštěném "živém" systému. Nalezené důkazy se pak dokumentují fotograficky, nebo videonahrávkou. Takové situace je vždy nutné neprodleně

konzultovat se specialisty z Kriminalistického ústavu v Praze, nebo příslušným znalcem pro určení nejvhodnějšího způsobu zajištění digitálních stop.

V případě neúspěchu všech známých metod k zajištění digitálních stop, je jako poslední možnost možné použít například i experimentální metody zmrazení operační paměti DRAM přímo ve spuštěném systému, jejichž obsah se následně zálohuje ve speciálním duplikačním zařízení. V obrazu zajištěné operační paměti pak forenzní analýzou dat znalec hledá použité šifrovací klíče [6].

7.3 Rizika při forenzní analýze digitálních dat

K odstranění většiny možných rizik ztráty, nebo poškození dat při forenzních analýzách digitálních dat je nutné, aby provádění těchto analýz bylo realizováno pouze na obnovených datech z bitových kopií, nebo na duplikátech bitových kopií.

Riziko: Znehodnocení zajištěných digitálních stop.

Pokud je ve výjimečných situacích nutné provádět forenzní analýzy digitálních dat přímo na zajištěných zařízeních, nebo na originálech datových médií, například při nemožnosti vytvoření bitové kopie a podobně, vždy hrozí velké riziko znehodnocení dat obsažených na těchto datových médiích.

Protiopatření: Jako možné protiopatření je v tomto případě použití hardwarové blokace zápisu na zajištěná originální média a dále dodržení všech zásad bezpečné manipulace a správného zapojení zkoumaného zařízení.

Riziko: Znehodnocení bitové kopie digitální stopy.

Při uchovávání bitových kopií digitálních stop na technologických datových médiích, například na pevných discích, hrozí riziko ztráty dat, pokud toto technologické médium bude mít poruchu, nebo skrytou vadu.

Protiopatření: Ke snížení tohoto rizika by se soubory bitových kopií, včetně jejich kontrolních otisků HASH, měly uchovávat duplicitně na více nezávislých technologických datových médiích. V případě, že zařízení, ze kterého byla vytvořena bitová kopie je stále zajištěno, je možné vytvoření jeho bitové kopie opakovat, nicméně duplicitní ukládání bitových kopií na více datových médií se doporučuje i v tomto případě.

Riziko: Nemožnost rozšifrování dat.

V mnoha případech jsou k provedení forenzních analýz digitálních dat dodána datová média, která jsou zašifrována, nebo se použité šifrování dat odhalí v průběhu provádění forenzní analýzy dat. V takových případech je rozšifrování dat klíčové, a pokud se nezdaří, nemůže být forenzní analýza těchto dat provedena.

Protiopatření: Žádné protiopatření proti tomuto riziku neexistuje. Při nálezu zašifrovaných dat je získání šifrovacího klíče jedinou možností ke snížení tohoto rizika. To je možné buď přímo od osoby, která data zašifrovala, nebo můžou být šifrovací klíče nalezeny například při ohledání místa činu v poznámkách uživatele a podobně.

Riziko: Ukládání výsledků forenzních analýz na stejné datové médium, na kterém jsou uloženy bitové kopie zajištěných digitálních stop.

Mnohdy se stává, že z důvodů úsporných opatření bývají výsledky forenzních analýz digitálních dat uloženy na stejné technologické datové médium, například na stejný pevný disk, jako bitové kopie digitálních stop. V tomto případě hrozí současně několik rizik:

- Riziko ztráty všech dat při poruše datového média.
- Riziko poškození datového média při transportu.
- Riziko ztráty dat neodborným zacházením s datovým médiem.

Protiopatření: Výsledky forenzních analýz digitálních dat a data bitových kopií digitálních stop ukládat zásadně na různá datová média a uchovávat také identické kopie těchto dat.

7.4 Ostatní rizika při práci s digitálními stopami

Riziko: Odcizení důkazů.

Toto riziko hrozí ve všech etapách práce s digitálními stopami. K odcizení digitálních důkazů může dojít při nedodržení bezpečnostních pravidel, například při prováděných úkonech, při transportu, při nesprávném skladování, při manipulaci s digitálními stopami a podobně.

Protiopatření: V tomto případě se jedná o striktní dodržení takových bezpečnostních pravidel, při kterých je toto riziko minimalizováno na nejnižší možnou úroveň.

Příklad bezpečnostních pravidel:

- Zajištěné objekty obsahující digitální stopy by měly být po celou dobu vyšetřování zapečetěny a uloženy ve střeženém a zabezpečeném skladu důkazů, nebo, ve výjimečných případech, v uzamčeném a zapečetěném ocelovém trezoru vyšetřovatele, který je umístěn v zabezpečené a střežené zóně.
- Pokud je jako důkaz považována bitová kopie zajištěného datového média, měla by být uložena stejným způsobem, jako zajištěné objekty obsahující digitální stopy.
- Veškeré předávání a přebírání digitálních stop je nutné provádět protokolárně s určením zodpovědnosti za přebíranou digitální stopu.
- Pro účely zkoumání a analýz vždy pracovat pouze s identickými kopiemi originálních dat. Pokud je nutné takové zkoumání provést s originálními daty, je nutné zvýšené zabezpečení a ostraha zajištěných objektů.
- Při transportu a manipulaci s digitálními stopami je nutné jejich nepřetržité střežení.

Riziko: Úmyslné a neúmyslné poškození, nebo zničení digitálních stop.

Také tyto rizika hrozí v celém procesu práce s digitálními důkazy. Může se jednat například o úmyslné, nebo neúmyslné zničení paměťových médií magnetickým, nebo elektrostatickým polem, jejich mechanické poškození při neopatrné manipulaci a podobně.

Protiopatření: V případě úmyslného poškození, nebo zničení digitálních stop je jediným protiopatřením striktní dodržení výše uvedených bezpečnostních pravidel, kdy originály digitálních důkazů nesmí být za žádných okolností přístupné nepovolaným osobám, a měly by být vždy střeženy a bezpečně uloženy. V případě neúmyslného poškození digitálních stop je ke snížení tohoto rizika nutné dodržení zásady práce s identickou kopií digitální stopy a všech doporučených postupů pro bezpečnou práci s předmětným typem digitální stopy, snaha o šetrné zacházení a manipulaci s digitální stopou a zvážení všech vnějších vlivů a okolností, které by při práci s důkazem mohly nastat.

Riziko: Podvržení souboru digitální stopy jiným souborem se stejným otiskem HASH.

Toto velmi závažné riziko se vztahuje na všechny digitální stopy, u kterých je k autentizaci použit kontrolní otisk vypočtený pomocí hašovací funkce. Při selhání bezpečnostních opatření v jakékoliv etapě práce s digitální stopou, kdy by mohl potenciální útočník neoprávněně manipulovat s digitálním důkazem, hrozí riziko, že by datové

soubory digitální stopy mohly být podvrženy jinými soubory se stejným kontrolním otiskem HASH. Princip tohoto podvržení důkazu spočívá v hledání kolizí hašovací funkce, kterým se, jak již bylo popsáno v předchozích kapitolách, už z principu hašovacích funkcí nelze vyhnout. Tímto způsobem by mohl útočník získat soubor, který má stejný kolizní kontrolní otisk HASH, avšak data tohoto kolizního souboru by byla zcela odlišná.

Již v roce 2004 byla čínským týmem, pod vedením Xiaoyun Wangové, objevena metoda pro úspěšné nalezení kolizí pro hašovací funkce MD4, MD5, HAVAL-128 a RIPEMD. Algoritmus této metody však nebyl dosud zveřejněn. Velkých úspěchů v této oblasti dosáhl i český tým, pod vedením RNDr. Vlastimila Klímy, který zveřejnil vylepšenou metodu, která je přibližně 3 - 6 krát rychlejší než čínský algoritmus a umožňuje nalézt úplnou kolizi MD5 otisku během několika hodin, za použití běžného notebooku. [7] V březnu roku 2006 publikoval tým RNDr. Vlastimila Klímy další novou metodu hledání kolizí založenou na tunelování hašovacích funkcí. Využitím tunelů v hašovacích funkcích se exponenciálně zkracuje čas nutný k nalezení kolize. Touto metodou lze nalézt kolize otisku hašovací funkce MD5 na běžném notebooku již během jedné minuty. [8]

U hašovací funkce SHA-1 byl v roce 2005 také objeven algoritmus, který nalézá kolize podstatně rychleji, než metodou hrubé síly. Jeho výpočetní náročnost je však dnešními prostředky stále nerealizovatelná.

Protiopatření: Ke zmírnění tohoto rizika je nutné v prvé řadě opět striktně dodržovat všechna bezpečnostní pravidla tak, aby zajištěné digitální stopy nebyly za žádných okolností přístupné nepovolaným osobám. Další kroky ke zmírnění tohoto rizika jsou následující:

- Pokud je to možné, používat bezpečnější hašovací algoritmy typu SHA-2.
- Protokolovat i velikost souborů, ke kterým je vypočten kontrolní otisk HASH. V případě podvržení digitálního důkazu nemusí mít podvržený soubor s kolizním otiskem stejnou velikost.
- Provádět autentizaci digitální stopy dvěma různými hašovacími algoritmy nezávisle na sobě. Například MD5 a nezávisle i SHA-1. Do příslušných protokolů pak uvádět hodnoty obou kontrolních otisků. Toto protiopatření využívá skutečnosti, že nelze v reálném čase nalézt takový soubor, kterému by odpovídaly kolizní otisky obou použitých hašovacích funkcí současně.

Riziko: Nedostatečná ochrana dat při manipulaci s datovými médii, které obsahují digitální stopy.

V praxi se často lze setkat se situací, kdy plně postačuje autentizace digitálních stop kontrolním otiskem MD5 a tyto digitální stopy spolu s kontrolními otisky jsou uloženy na technologickém datovém médiu, například na pevném disku. Tento technologický pevný disk však již dále není zapečetěn, protože se předpokládá jeho okamžité bezpečné uložení. Osoba, která technologické datové médium obsahující digitální stopy po jejich zajištění přebírá, obvykle osoba vyšetřovatele, přebírá veškerou zodpovědnost za tuto digitální stopu. Zde však hrozí riziko, pokud by se s tímto nezapečetěným datovým médiem před jeho bezpečným uložením neoprávněně manipulovalo, mohlo by dojít k jeho smazání, přepsání nebo k podvržení dat.

Protiopatření: K odstranění tohoto rizika je nutné při předávání technologických datových médií, obsahujících digitální stopy a jejich kontrolní otisky, tyto média zajistit proti neoprávněné manipulaci, například zabalením a zapečetěním. Následná manipulace s těmito datovými médii by měla probíhat protokolárně s určením, kdo, kdy a za jakým účelem s důkazy manipuloval.

Riziko: Neodborné zacházení s datovými médii, které obsahují digitální stopy.

Toto riziko je opět způsobeno lidským faktorem. V praxi může nastat situace, kdy osoba oprávněná k manipulaci s digitálními důkazy nemá potřebné znalosti v oblasti výpočetní techniky. Potom při neodborném zacházení s datovými médii obsahujícími digitální stopy, například při vyhodnocování důkazů, může dojít například k nechtěnému zformátování datového média, případně smazání, nebo přepsání dat.

Protiopatření: V tomto případě je nutné důkladné proškolení odpovědných osob s důrazem na bezpečnou manipulaci s datovými médii a možnost spolupráce specialistů. Dalším krokem ke snížení tohoto rizika je umožnění manipulace s digitálními důkazy, včetně zpřístupnění dat pouze specialistům na zajišťování dat, nebo znalcům. Pro potřeby vyšetřování by měly být vždy k dispozici pouze identické kopie digitálních stop.

Riziko: Uchovávání a archivace digitálních stop.

Posledním uváděným rizikem je riziko ztráty dat při uchovávání a archivaci digitálních stop. V praxi musíme vždy počítat s uchováváním digitálních stop po dlouhou dobu, například i 10 let, nebo více. V tomto případě je riziko vztaženo k životnosti a spolehlivosti datových médií, na kterých jsou digitální stopy uloženy a archivovány a také k dodržení doporučených podmínek k jejich archivaci. Výběr vhodného datového média pro archivaci dat se v praxi často podceňuje.

Protiopatření: K archivaci a uchovávání digitálních stop je nutné vždy používat datová média s garantovanou životností, určená výrobcem k archivaci dat. Zároveň je nutné zajistit podmínky pro tuto archivaci, jako jsou doporučené rozmezí teplot, vlhkosti a zamezení nežádoucích vlivů různých druhů záření a polí.

7.5 Ohodnocení rizik z hlediska pravděpodobnosti vzniku a míry ohrožení daného důkazního materiálu

Pro větší názornost popsaných rizik a ohrožení bylo provedeno jejich ohodnocení z hlediska pravděpodobnosti vzniku a míry ohroženi daného důkazního materiálu. Ke stanovení ohodnocení byl použit vzorek několika stovek realizovaných případů zajištění a forenzní analýzy digitálních stop.

V následující tabulce jsou uvedena jednotlivá, výše popsaná rizika. U každého konkrétního rizika je uvedena ve sloupci „P. vzniku“ pravděpodobnost jeho vzniku, kde bylo u hodnot 0.1% a menších provedeno stanovení pravděpodobnosti kvalifikovaným odhadem, protože ze vzorku hodnocených případů tyto rizika nenastala. Míra ohrožení důkazního materiálu určuje pravděpodobnost úplné ztráty důkazního materiálu při výskytu příslušného rizika.

Riziko	P. vzniku	Míra ohrožení
Nezajištění všech digitálních stop.	3%	100%
Neodborné zajištění digitálních stop.	2%	50%
Nesprávné zabalení, nebo autentizace digitální stopy.	1%	70%
Nesprávná, nebo neúplná dokumentace zajištění digitálních stop v protokolu.	0,1%	50%
Znehodnocení digitální stopy při transportu.	0,1%	50%
Vytváření bitových kopií z médií, které mají závadu.	5%	50%
Úmyslné zničení dat při vytváření bitové kopie digitální stopy.	1%	100%
Ztráta dat z nedbalosti při vytváření bitové kopie.	0,1%	100%
Porucha datového média při vytváření bitové kopie.	0,1%	100%
Nelze vytvořit bitové kopie datových médií ze spuštěného „živého“ systému.	0,1%	100%
Ukládání výsledků forenzních analýz na stejné datové médium, na kterém jsou uloženy bitové kopie digitálních stop.	30%	0,3%
Nemožnost rozšifrování dat.	2%	100%
Znehodnocení bitové kopie digitální stopy.	0,1%	50%
Znehodnocení zajištěných digitálních stop.	0,1%	100%
Neodborné zacházení s datovými médii, které obsahují digitální stopy.	1%	100%
Úmyslné a neúmyslné poškození, nebo zničení digitálních stop.	0,1%	100%
Uchovávání a archivace digitálních stop.	0,1%	100%
Nedostatečná ochrana dat při manipulaci s datovými médii, které obsahují digitální stopy.	0,1%	100%
Odcizení důkazů.	0,01%	100%
Podvržení souboru digitální stopy jiným souborem se stejným otiskem HASH.	0,001%	100%

Tabulka 1. Ohodnocení rizik

ZÁVĚR

Cílem této diplomové práce bylo popsat širokou problematiku zajišťování a analyzování digitálních důkazů. Úvodem práce bylo seznámení s touto problematikou, definování základních pojmů, principů a základních etap práce s digitálními stopami. V teoretické části bylo popsáno zajišťování digitálních stop a jeho právní aspekty při provádění úkonů v trestním řízení. Dále pak příprava před zajištěním digitálních stop a možné postupy na místě činu, včetně dokumentace digitálních stop a jejich ukládání, balení a pečetění. V této části byla také popsána problematika vytváření bitových kopií digitálních stop v praxi u Policie ČR a objasněny důvody vytváření bitových kopií s ohledem na křehkost digitálních stop. V několika kapitolách byly představeny všechny používané způsoby vytváření bitových kopií digitálních stop. Práce upozorňuje na výhody a nevýhody používání různých operačních systémů k tomuto úkonu a ukazuje, jak je možné využít distribuce operačního systému Linux pro forenzní praxi. Byla představena také praktická ukázka použití příkazů OS Linux k vytvoření bitové kopie. V teoretické části byly také podrobně popsány metody a důvody autentizace digitálních stop i vlastnosti a typy hašovacích funkcí, které se k autentizaci využívají. V závěru teoretické části byly uvedeny zásady a základní prvky provádění forenzních analýz digitálních dat, byla popsána osoba znalce a její činnosti i dokumentace provedených forenzních analýz ve znaleckém posudku, nebo odborném vyjádření.

Praktickou část tvoří nejčastější postupy zajišťování digitálních stop, kde byly v několika kapitolách podrobně popsány jak postupy při zajišťování výpočetní techniky, tak i postupy při zajišťování dat. Dále tuto část tvoří také podrobný popis nejčastějších postupů a metod při přípravě a provádění forenzních analýz digitálních dat v praxi. Ke každému typu forenzní analýzy digitálních dat byly také uvedeny forenzní softwarové nástroje, ve kterých lze danou analýzu realizovat. V závěru praktické části byly popsány nejdůležitější rizika a ohrožení v jednotlivých etapách práce s digitálními stopami a zároveň také navrhovaná protiopatření, kterými se uvedená rizika zmírní, nebo úplně odstraní. U jednotlivých rizik bylo uvedeno ohodnocení z hlediska pravděpodobnosti vzniku a míry ohroženi daného důkazního materiálu.

Text této práce vychází nejen z běžně dostupných zdrojů, ale i z interních aktů řízení Policie ČR a z velké části z mých osobních znalostí a zkušeností při zajišťování výpočetní techniky a digitálních stop. V této oblasti pracuji již od roku 2006 jako vrchní komisař

Služby kriminální policie a vyšetřování na Oddělení informační kriminality a jsem držitelem osvědčení o odborné způsobilosti k provádění kriminalisticko-technických úkonů při zajišťování výpočetní techniky a dat.

ZÁVĚR V ANGLIČTINĚ

The aim of this thesis was to describe the problems of securing and analyzing digital evidence. The introduction of this work makes a reader familiar with the issue, defines the basic concepts, principles and basic stages of digital evidence. In the theoretical part was described securing digital evidence and its legal aspects of the performing acts in criminal proceedings. Furthermore, the preparation before securing digital evidence and possible procedures at the scene, including documentation of digital evidence and storage, packaging and sealing. There were also described problems of imaging digital evidence in practice by the police in this section and explained the reasons for imaging with regard to the fragility of digital evidence. In several chapters there were presented all the modes of imaging digital evidence. The work highlights the advantages and disadvantages of using different operating systems for this task, and shows how it is possible to use the distribution of the Linux operating system for forensic practice. It was presented in a practical demonstration how to use Linux commands to create the image. In the theoretical part there were also described in detail the methods and reasons for authentication and digital evidence properties and types of hash functions that are used for authentication. At the end of the theoretical part there were the principles and basic elements of implementing forensic analysis of digital data, was shown the expert and his activities as well as documentation of the forensic analysis of the expert opinion or technical advice. The practical part consists of the most common procedures of securing digital evidence, where in the several chapters is described in detail the procedures for providing computational techniques and procedures for ensuring data. In addition, this part is a detailed description of the most common techniques and methods of preparing and implementing the forensic analysis of digital data in practice. For each type of forensic analysis of digital data there were also included forensic software tools, in which the analysis can be realized. In conclusion the practical part describes the key risks and threats in various stages of digital evidence while also proposes countermeasures which will mitigate or completely remove those risks. For each risk the assessment was stated in terms of the likelihood and extent of the risk evidence. The text of this work comes not only from commonly available sources but also from internal Police acts and greatly from my personal knowledge and experience in providing information technology and digital evidence. In this area I have been working since 2006 as the Chief Commissioner of the

Criminal Investigation in the Cyber-crime Police Department and I hold a certificate of competence to perform forensic-technical operations in securing computers and data.

SEZNAM POUŽITÉ LITERATURY

[1] Porada Viktor, Roman Rak. Teorie digitálních stop a její aplikace v kriminalistice a forenzních vědách. Karlovarská právní revue č.4, 2006.

[2] Porada Viktor, Roman Rak. Digitální stopy v kriminalistice a forenzních vědách. Soudní inženýrství č.17, 2006.

[3] Kothánek Jaroslav. Zajišťování výpočetní techniky a dat pro potřeby důkazního řízení. Policie ČR, Praha, 2006.

[4] Kadlec Josef. Forenzní analýza unixových systémů. Hradec Králové 2006. Diplomová práce. UHK FIM. Dostupný z: http://www.root.cz/knihy/forenzni-analyza-unixovych-systemu.

[5] Risk Analysis Consultants s.r.o. Forenzní zkoumání digitálních důkazů - Příručka vyšetřovatele. Praha, 2005. Dostupný z: http://www.rac.cz/rac/homepage.nsf/CZ/883AABB42333CB35C12570FC0034A328.

[6] J. A. Halderman, S. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, and E. W. Felten. Cold Boot Attacks on Encryption Keys. Princeton University, 2008. Dostupný z: https://citp.princeton.edu/research/memory/.

[7] Klíma, Vlastimil. Nalézání kolizí MD5 - hračka pro notebook. Praha, 2005. Dostupný z: http://cryptography.hyperlink.cz/md5/MD5_kolize.pdf.

[8] Klíma, Vlastimil. Tunely v hašovacích funkcích: kolize MD5 do minuty. Praha 2006. Dostupný z: http://cryptography.hyperlink.cz/2006/tunely.pdf.

[9] Formánek Martin. Forenzní analýza digitálních nosičů dat pro počítače. Praha 2008. Bakalářská práce. ČVUT FEL. Dostupný z: https://dip.felk.cvut.cz/browse/pdfcache/formam1_2008bach.pdf.

[10] Formánek Martin. Metodika zajištování důkazů při vyšetřování počítačové kriminality - FORENZNÍ ANALÝZA POČÍTAČE. Praha 2007. Semestrální projekt. ČVUT FEL. Dostupný z: http://service.felk.cvut.cz/anc/ofa/pub/doc/metodika.pdf.

[11] Interní akty řízení Policie ČR.

[12] Vyhláška ministerstva spravedlnosti č.37/67 Sb. o provedení zákona o znalcích a tlumočnících.

[13] Zákon 141/1961 Sb. o trestním řízení soudním. MV ČR, 2012.

[14] Zákon č.36/67 Sb. o znalcích a tlumočnících.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AP	Access point – přístupový bod k bezdrátové Wi-Fi síti
ATA	Advanced Technology Attachment - sběrnice pro připojení pevných disků
BIOS	Basic Input-Output Systém - inicializace a konfigurace hardware PC
ČR	Česká republika
dd	standardní příkaz Linuxu - slouží k blokovému kopírování dat
dc3dd	modifikace příkazu dd vyvinutý v DoD Cyber Crime Cente
dcfldd	modifikace příkazu dd vyvinutý v Defense Computer Forensics Lab
DLL	Dynamic-Link Library - dynamicky linkovaná knihovna
DNSSEC	Domain Name System Security Extensions - zabezpečení informací poskytované DNS systémem v IP sítích
DRAM	Dynamic Random Access Memory
eml	Textový formát souboru elektronické pošty
EXT3	žurnálovací systém souborů vytvořený pro operační systém Linux
HASH	kontrolní otisk vytvořený hašovací funkcí
IDE	Označení standardní počítačové sběrnice ATA
IP	Internet Protocol
KÚP	Kriminalistický ústav Praha
MD5	Message-Digest algorithm – hašovací algoritmus 128 bitů
msg	Textový formát souboru elektronické pošty
NAS	Network Attached Storage - síťová úložiště
NAT	Network Address Translation - překlad síťových adres
NTFS	New Technology File System – souborový systém
NFS	Network File System - internetový protokol
OKTE	Odbor kriminalistických technik a expertíz
OS	Operační systém

P2P	Peer to Peer – typ počítačových sítí klient-klient
PC	Personal Computer – osobní počítač
RAID	vícenásobné diskové pole nezávislých pevných disků
RAM	Random Access Memory – paměť s přímým přístupem
SATA	Seriál ATA – sběrnice datového rozhraní k připojení pevných disků
SCSI	Small Computer System Interface – rozhraní k připojení pevných disků
SHA-1	Secure Hash Algorithm– hašovací algoritmus 160 bitů
SHA-2	Secure Hash Algorithm– rodina hašovacích algoritmů 224 - 512 bitů
SIM	Subscriber Identity Module – karta k identifikaci účastníka v mobilní síti
SKPV	Služba kriminální policie a vyšetřování
SSH	Secure Shell - zabezpečený komunikační protokol v počítačových sítích
SQL	Structured Query Language - strukturovaný dotazovací jazyk databází
USB	Universal Serial Bus - univerzální sériová sběrnice
Wi-Fi	Wireless Fidelity – standard bezdrátové komunikace v počítačových sítích
WIPE	program pro nevratné smazání počítačových dat

SEZNAM OBRÁZKŮ

SEZNAM TABULEK