Acta Informatica Pragensia, 2015, 4(3): 242–257
DOI: 10.18267/j.aip.72
Peer-reviewed paper

Praxe digitálního forenzního vyšetřování v České republice a norma ISO/IEC 27037:2012

Practice of Digital Forensic Investigation in the Czech Republic and ISO/IEC 27037:2012

Jaromír Veber[*], Zdeněk Smutný[*], Ladislav Vyskočil[†]

Abstrakt

Digitální forenzní vyšetřování prodělalo v uplynulých dvou dekádách velkou proměnu. Důvodem je jak technologický pokrok, tak již naprosto běžné používání ICT ve společnosti. Tento článek se zabývá standardizaci postupů sběru digitálních stop v souvislosti s normou ISO/IEC 27037:2012. V článku jsou prezentovány některé důležité principy uvedené v normě. Dále jsou představeny názory dvou expertů z České republiky – vyšetřovatele kriminální policie a analytika forenzní laboratoře. Jsou uvedeny jejich zkušenosti z praxe, týkající se sběru a analýzy digitálních stop, a dále diskutovány jejich názory na obsah normy. Na tomto základě je možné poukázat na neshody mezi doporučeními uvedenými v normě a praxí. Dále jsou v článku obecná doporučení normy komentována s odkazem na některé základní postupy při zajišťování digitálních stop v České republice.

Klíčová slova: Sběr digitální důkazů, ISO 27037, praxe, digitálního forenzního vyšetřování, Česká republika.

Abstract

Digital forensics investigation undergone a great transformation in the past two decades. This is due to technological progress and already quite common use of ICT in society. This article deals with the standardization of the procedures for collecting potential digital evidence in connection with the ISO/IEC 27037:2012. This article presents some of the important principles presented in the standard. It also presents the views of two experts from the Czech Republic – criminal police investigator and forensic analyst. They introduce their practical experience regarding the collection and analysis of potential digital evidence and also discuss their views on the content of the standard. This makes it possible to point out the discrepancies between the recommendations laid down in the standard and practice. The general recommendations of the standard are commented in the article with references to some basic procedures used in the Czech Republic for potential digital evidence acquisition and collection.

Keywords: Digital evidence collection, digital evidence acquisition, ISO 27037, practice, digital forensic investigations, Czech Republic.

[*] Department of Systems Analysis, Faculty of Informatics and Statistics, University of Economics, Prague, nám. W. Churchilla 4, 130 67 Praha 3, Czech Republic
✉ jaromir.veber2@vse.cz, zdenek.smutny@vse.cz

[†] Department of Information Crime, Office of Criminal Police Services and Investigation, Police of the Czech Republic, Strojnická 935/27, 170 89 Praha 7, Czech Republic

1 Úvod

Metody pro zajišťování stop v digitální formě se stále vyvíjí, a s tím, jak roste množství a objem stop získaných v digitální formě, samozřejmě roste i množství lidí, kteří se zabývají zajišťováním digitálních stop a následnou analýzou (Hegarty, Lamb & Attwood, 2014). S tím jak narůstá důležitost digitálního vyšetřování v rámci kriminalistiky a v důsledku rozvoje informační společnosti, tak vznikají také rámce, modely, metodiky (Agarwal & Kothari, 2015; Jang & Kwak, 2014; Shrivastava & Gupta, 2014) a další relevantní rigorózní postupy – často založených na bayesovské síti, teorie složitosti, teorie informace a teorie pravděpodobnosti – (Overill, 2014) provádění této činnosti – tzn. sběr, zpracování, vyhodnocování a uchování digitálních stop.

Oproti příspěvku (Ajijola, Zavarsky, & Ruhl, 2014), který se zabývá porovnáním dvou forenzních metodik NIST SP 800-101 Rev.1:2014 a ISO/IEC 27037:2012, tak chceme prezentovat jiný pohled. V předkládaném článku se zaměříme na porovnání vybrané ISO normy (forenzní metodiky) s praxí v České republice. Mezinárodní organizace pro standardizaci ISO se zaměřuje na tvorbu a vydávání standardů pro téměř všechny oblasti lidské činnosti. Jedná se o standardy pro výrobky, služby a nejlepší postupy v praxi. Rodina norem ISO 27000 řeší bezpečnost informací (Veber, & Klíma, 2014), a právě do této rodiny norem patří i norma ISO/IEC 27037:2012 (2012) – dále v textu jen ISO 27037 nebo norma. ISO 27037 se specializuje na postupy pro sběr digitálních stop a patří do skupiny standardů pro nejlepší postupy v praxi (best practices). Norma shrnuje postupy, které by měly být dodržovány při identifikaci, sběru, zpracování a uchování digitálních stop. Dodejme, že tato norma nebyla, a pravděpodobně ani nebude přeložena do češtiny (důvodem je poměrně nízký počet zainteresovaných stran). V rámci České republiky se touto problematikou zabývá úzký okruh vědecky zaměřených výzkumníků, a proto odkážeme alespoň na některé publikace či závěrečné práce v souvislosti se zde uvedenou problematikou (Rak & Porada, 2006; Porada & Rak, 2006; Gřivna & Polčák, 2008; Vyskočil, 2013; Porada & Bruna, 2013; Kothánek, 2014).

V tomto článku bychom nejprve stručně představili vybraný obsah normy ve volném překladu a dále bychom rádi diskutovali nejen obsah této poměrně nové normy zaměřené na sběr digitálních stop, ale také bychom konfrontovali postupy uvedené v normě s postupy v současnosti používanými profesionály v České republice. Dále je uveden názor analytiků digitálních důkazů (soudního znalce a kriminalisty) jak na současné postupy uplatňované v ČR, tak na postupy uvedené v normě.

Tento článek vychází z přepracovaného a rozšířeného konferenčního příspěvku (Veber & Smutný, 2015), který byl prezentován na 14. Evropské konferenci o kybernetické válce a bezpečnosti, která se konala na University of Hertfordshire (Spojené království).

2 Směrnice pro identifikaci, sběr, akvizici a uchování digitálních důkazů – Norma ISO 27037:2012

Norma ISO 27037 v úvodních kapitolách definuje pojmy, se kterými se bude pracovat. Důležitým pojmem je **DEFR** (Digital Evidence First Responder), což je fyzická osoba, která je oprávněna, vyškolena a kvalifikována ke sběru a hledání digitálních důkazů na místě činu. V České republice se jedná o policistu s osvědčením o odborné způsobilosti k provádění

kriminalisticko-technických úkonů při zajišťování výpočetní techniky a dat na místě činu (alternativně se může jednat o osvědčeného soudního znalce s potřebným zaměřením[1]).

Dále norma stanovuje základní rámec pro zacházení s digitálními stopami. Mezi *základní požadavky **sběru** digitálních stop* dle normy patří: **relevantnost**, **spolehlivost** a **dostatečnost**. *Při **zacházení** s digitálními stopami* by měly být podle normy dodrženy tyto hlavní požadavky: **kontrolovatelnost, ospravedlnitelnost, opakovatelnost a reprodukovatelnost**. Dodejme, že tato norma nedefinuje procesy zabývající se souběžně použitelnými digitálními forenzními principy, v tomto ohledu musíme odkázat na článek (Valjarevic & Venter, 2015).

2.1 Práce s digitálními stopami

Mezinárodní standard ve formě uvedené normy se zabývá pouze prvotním procesem manipulace potenciálními digitálními důkazy a nezohledňuje další práci s těmito stopami, jako je jejich analýza, prezentace a likvidace. To je obsahem jiných norem – viz (ISO/IEC FDIS 27041, 2012; ISO/IEC 27043, 2015; ISO/IEC FDIS 27042, 2012). Prvotní a níže popsaný proces se zabývá identifikací, zajištěním a uchováním digitálních stop. Digitální stopy jsou ze své povahy nestabilní/křehké. Osoby manipulující s digitálními stopami by měly být schopny určit a řídit rizika, která mohou nastat při práci s tímto druhem stop, tak aby nedošlo k jejich znehodnocení.

DEFR by měl postupovat tak, aby zajistil zachování integrity a spolehlivosti digitálních stop. Zvolené konkrétní postupy se musí řídit následujícími základními principy:

- Minimalizovat manipulaci s digitálním zařízením či digitálními daty.
- Zdokumentovat veškeré akce a změny provedené s danou digitální stopou tak, aby si mohl nezávislý expert vytvořit názor na spolehlivost předložených důkazů.
- Postupovat v souladu se zákony dané země.
- DEFR by neměl postupovat nad rámec své působnosti.

Dodržení těchto fundamentálních principů zajistí zachování stop pro účely vyšetřování, respektive v případě, že dojde k jejich nevyhnutelné změně, tak všechny provedené akce a důvody jsou náležitě zdokumentovány. Dále uvádíme zkrácený popis dílčích procesů prvotní manipulace s digitálními důkazy.

A) Identifikace

Identifikační proces zahrnuje vyhledávání, rozpoznávání a dokumentaci digitálních stop, která je reprezentována ve fyzické a logické formě. Během tohoto procesu by měla být identifikována všechna zařízení, na kterých by se mohly nacházet digitální stopy. DEFR by měl systematicky prohledávat místo činu tak, aby nepřehlédl malá, maskovaná zařízení či na první pohled nepodstatný materiál. Kromě toho by měl DEFR zvážit i možnost existence skrytého důkazu ve formě virtuální komponenty – např. Cloud Computing viz články (Chung et al., 2012; Federici, 2014). V případě nestálosti některých zařízení, je třeba provést upřednostnění těchto zařízení při zajišťováním dalších důkazů. Správné pořadí sběru a následné zpracování by mělo minimalizovat možné poškození digitálních stop.

[1] Tady je třeba se pozastavit nad termínem „osvědčeného soudního znalce s potřebným zaměřením“. Jestliže u Policie ČR existuje určitý systém kvalifikace kriminalistických techniků, kde určitě i zajišťování digitálních stop je jednou ze součástí prověřované odbornosti, u soudních znalců odpovídající prověřování neboli certifikace neexistuje.

B) Zajištění zařízení

Po identifikaci zařízení, která mohou obsahovat digitální stopy, jsou tato zařízení přesunuta z jejich původního místa do laboratoře, kde jsou v dalším kroku analyzována a zpracována. Tato zařízení mohou být ve dvou základních stavech – zapnutá a vypnutá. Proces zajištění zařízení je nutné celou dobu dokumentovat včetně balení a transportu do laboratoře.

C) Zajištění dat

Proces zajištění dat, tedy prvotní zpracování digitální stopy, spočívá především ve vytvoření bitové kopie digitální stopy (např. obsahu celého harddisku) a dokumentaci použitých metod při jejím vytváření. Pokud je to potřeba, tak by při zajištění dat mělo být získáno jak alokované, tak nealokované místo včetně vymazaných souborů. Obecně platí, že originál a každá jeho kopie by měly vytvářet při stejné verifikační funkci stejný výstup.

DEFR by měl v závislosti na okolnostech (situace, čas, cena) vybrat nejvhodnější postup a metodu pro zajištění dat. V případě že výsledkem tohoto procesu jsou nevyhnutelné změny ve vytvořené kopii oproti originálu, tak je potřeba zdokumentovat jaká data byla změněna. V případech, kde nemůže být proces ověřování proveden (např. při zajištění dat z běžícího systému) by DEFR měl použít nejlepší možný způsob, který má k dispozici tak, aby byl schopen zdůvodnit a obhájit výběr použité metody. Pokud vytvořenou bitovou kopii nelze verifikovat, pak to musí být zdokumentováno a odůvodněno. ***Veškeré další kroky forenzní analýzy se provádí na kopiích digitálních stop***.

D) Uchování

Z hlediska uchování digitálních stop je nutné ochránit jejich integritu tak, aby byla zajištěna jejich použitelnost při vyšetřování. DEFR by měl být schopen prokázat, že důkazy nebyly změněny od doby jejich sběru, případně poskytnout odůvodnění a dokumentaci všech akcí, které vedly k jejich změnám.

2.2 Hlavní komponenty práce s digitálními důkazy

Uveďme nyní devět klíčových součástí práce s digitálními důkazy tak, jak je uvádí norma:

Sled činností (chronologický záznam provedených akcí)

Nutností při práci s digitálními stopami je vedení podrobného chronologického záznamu jednotlivých akcí s digitální stopou. Účelem tohoto záznamu je umožnit identifikaci přístupu k dané stopě a monitorovat pohyb digitální stopy, včetně možnosti sledovat časový sled prováděných akcí.

Bezpečnostní opatření na místě incidentu

DEFR by měl vykonávat všechny činnosti směřující k ochraně místa, kde se nacházejí digitální stopy, co nejdříve po svém příjezdu na místo.

Role a odpovědnosti

Role DEFR zahrnuje identifikaci, zajištění a uchování digitální stopy na místě činu. S tím je spojeno vytvoření zprávy o zajištění stopy[2]. DEFR není nutně zodpovědný za zprávu o výsledcích forenzní analýzy. Úloha DEFR zahrnuje také zajištění integrity a věrohodnosti digitální stopy.

[2] V ČR může být záznam o zajištění stopy zaznamenán i do jiných protokolů – domovní/nebytová prohlídka nebo dobrovolné vydání.

Kompetence

DEFR by měl mít příslušné technické a právní kompetence, musí být schopen prokázat, že je řádně vyškolen a má dostatečné technické a právní znalosti, aby odpovídajícím způsobem zajistil digitální stopy.

Použití přiměřené péče

Je nutné vyhnout se činnostem, které by mohly vést ke znehodnocení digitálních stop, ať už se jedná o úmyslné či neúmyslné jednání.

Dokumentace

Zejména je nutné dokumentovat veškeré provedené aktivity, čas, stav systému (pokud je zapnutý), veškeré přesuny a sériová čísla zařízení.

Instrukce před vlastním úkonem

Je nezbytné, aby DEFR byl před vlastním úkonem zajištění digitálních stop dostatečně informován příslušným orgánem o dodržení všech zákonů, případně důvěrnosti. Je důležité, aby se konala formální informační schůzka před samotným zásahem na místě činu, aby nedošlo ke znehodnocení stop.

Upřednostnění zajišťování digitálních stop

DEFR může[3] upřednostnit stopy dle relevance neboli důkazní hodnoty. Položky vysoké relevance respektive vysoké potenciální důkazní hodnoty jsou ty, které s největší pravděpodobností obsahují údaje týkající se vyšetřovaného činu.

Uchování digitálních stop

Získané digitální stopy je důležité zabezpečit takovým způsobem, který eliminuje možnost zničení stop nebo manipulaci s nimi. Ke zničení stop může dojít v důsledku magnetické degradace, elektrické degradace, tepelné degradace, vystavení vysoké nebo nízké vlhkosti, jakož i vibracemi a nárazy. Digitální stopy by neměly být ponechány bez dozoru ani v průběhu jejich přepravy.

2.3 Příklady – identifikace, sběru, zpracování a uchování

Norma obsahuje také konkrétní příklady postupů pro sběr digitálních stop. Tyto příklady upřesňují jednotlivá obecná doporučení a uvádí způsob jejich nasazení v praxi. Příklady se zaměřují na postupy zajištění digitálních stop podle druhu zařízení – samostatná zařízení, síťová zařízení, kamerové systémy.

2.3.1 Zajištění stop ze samostatných digitálních zařízení (počítačů), periferních zařízení a úložných médií.

Identifikace

V souvislosti s normou, jsou počítače považovány za samostatná digitální zařízení, která získávají, zpracovávají, uchovávají data a produkují výstupy. Tato zařízení nejsou připojena k síti, ale mohou být spojena s periferními zařízeními, jako jsou tiskárny, skenery, kamery, MP3 přehrávače, GPS systémy, RFID zařízení aj. Digitální zařízení, které má síťové rozhraní,

[3] V ČR specialista na zajišťování digitálních stop (DEFR) navrhne/doporučí upřednostnění stop, nicméně rozhodnutí o postupu je zodpovědnost vyšetřovatele (zpracovatele spisu).

ale není připojeno k síti v době sběru, by mělo být považováno (pro účely této normy) za samostatné digitální zařízení.

Místo činu obvykle obsahuje různé typy digitálních paměťových médií. Příklady digitálních paměťových médií zahrnují externí přenosné pevné disky, flash disky, CD, DVD, Blu-Ray disky, diskety, magnetické pásky, paměťové karty a další.

Před tím, než může být provedeno zajištění digitálního zařízení, by měl DEFR vyhodnotit a ujistit se, zda zdánlivě samostatná zařízení nebyla v poslední době připojena k síti. V případech, kdy existuje podezření, že zdánlivě samostatné zařízení bylo nedávno odpojeno od sítě, je třeba zvážit, zda k zařízení nepřistupovat jako k síťovému z hlediska sběru digitálních stop.

Zajištění celých digitálních zařízení

Postupy pro zajištění digitálních zařízení se liší v závislosti na tom, o jaké zařízení se jedná, nicméně existují určité základní postupy, které je nutné dodržet, a následně přizpůsobit další postupy dotyčnému zařízení, kterého se sběr týká. Následující základní činnosti by měl DEFR provádět v případech, kdy mají být zajištěna *zapnutá* digitální zařízení*:*

- Zvažte zajištění dat, která jsou závislá na aktuálním stavu zařízení před vypnutím systému.
- Podle nastavení zařízení rozhodněte, zda vypnout zařízení prostřednictvím běžných postupů, nebo zda přímo odpojit zařízení od zdroje energie.
- Označte, odpojte a zajistěte všechny kabely z digitálního přístroje a popište porty tak, aby systém mohl být později rekonstruován.
- Umístěte pásku přes vypínač, aby se zabránilo změně stavu spínače. Zdokumentujte stav spínače zařízení před zabalením a přesunem.[4]
- Pokud se jedná o notebook místo vypínání rovnou raději odstraňte baterii hlavního zdroje napájení.
- Vložte pásku přes slot disketové mechaniky, je-li přítomna[5].
- Ujistěte se, že optické mechaniky jsou zasunuty na místo; a zaznamenejte, zda jsou mechaniky prázdné, obsahují disky, nebo není známo; a zapečeťte slot mechaniky páskou, aby se zabránilo jejímu otevření.

Zajištění dat ze zařízení na místě

Existují tři scénáře, které mohou nastat během zajišťování dat: digitální zařízení je zapnuté, digitální zařízení je vypnuté a digitální zařízení je zapnuté a nelze jej vypnout (kritická digitální zařízení). Ve všech těchto případech je nutné provést přesnou kopii médií, která mohou obsahovat digitální stopy. V případě, že není možné získat přesnou bitovou kopii médií, měly by být získány vybrané soubory, u kterých existuje podezření, že obsahují digitální stopy. V ideálním případě by měla být vytvořena jak hlavní kopie, tak pracovní kopie. Pokud zařízení nelze vypnout, je vhodné zvážit zajištění dat z běžícího zařízení.

[4] Tady je nutné podotknout, že uvedené opatření je sice dobré, ale ne optimální. Vhodnější je zabránit opětovnému připojení zdroje elektrické energie (např. přelepením odpovídajícího konektoru). V některých případech může být také důležitou informací stav hlavního vypínače (zapnut/vypnut).

[5] Další opatření, svědčící o historickém vývoji celé uvedené normy, protože aktuálně se disketové mechaniky vyskytují už jen skutečně historicky. Jestliže také zabráníme opětovnému zapnutí zařízení, přelepování páskou postrádá opodstatnění.

Následující základní činnosti by měl DEFR provádět ve všech případech týkajících se zajišťování digitálních stop (dat) ***z běžících zařízení na místě:***

- Nejprve si určíme, zda zajistit digitální stopy, které by mohly být v případě vypnutí přístroje ztraceny.
- Zajištění dat přímo z běžícího zařízení vyžaduje, aby zařízení stále běželo, ale umožní získat i data z paměti RAM, jako je stav sítě a dešifrovací hesla k aplikacím.
- DEFR by nikdy neměl věřit programům v systému. Z tohoto důvodu se doporučuje využívat externí důvěryhodné nástroje (statické binární programy).
- Při zajišťování nestálých dat v paměti RAM by měl DEFR vytvořit bitovou kopii a ukládat data do logického souboru a okamžitě vytvořit kontrolní součet (hash), který zadokumentuje. Výsledné soubory by měly být uloženy na digitálním paměťovém médiu, které bylo připraveno k tomuto účelu, tedy bylo formátováno[6].
- Vytvořte image stálých dat (na disku) pomocí ověřeného nástroje.
- Zkontrolujte, zda není použito šifrování dat, to lze provést prohlídkou surových dat disku, nebo za použití nástrojů pro detekci šifrování. Pokud je použito šifrování, zvažte uložení nestálých dat v paměti RAM.
- Použijte spolehlivý zdroj času a dokumentujte dobu každé provedené akce. (nespoléhejte na čas běžícího systému)
- Bývá vhodné spojit osobu DEFR se získanými digitálními stopami za použití podpisů[7] (případně digitálních), pomocí biometrie nebo pomocí fotografií.

Následující základní činnosti by měl DEFR provádět ve všech případech týkajících se zajišťování dat ***z vypnutých zařízení:***

- Ujistěte se, že je přístroj opravdu vypnutý.
- Odstraňte úložné médium z vypnutého digitálního zařízení, pokud ještě není odstraněno.
- Vytvořte bitovou kopii pomocí ověřeného nástroje pro vytvoření bitových kopií podezřelého disku.

Na místě činu lze nalézt různé typy digitálních paměťových médií. Obvykle se jedná o stabilní data, tento typ dat může mít nejnižší prioritu při zajišťování.

Uchování digitálních stop

Po dokončení procesu zajištění digitálních stop by DEFR měl zaznamenat výsledky ověřovací funkce (hash), případně použít další postupy, které umožní kontrolovat správnost dat využitých pro následnou forenzní analýzu. DEFR také musí zajistit integritu, důvěrnost a dostupnost dat originálu (případně primární kopie) digitální stopy. Dále by DEFR měl při uchovávání stop provést následující:

- Použijte příslušnou ověřovací funkci, která umožní poskytnout důkaz o tom, že kopie, se kterými se pracuje, jsou shodné s originály.

[6] Formátování není tou nejdůležitější a nezbytnou podmínkou přípravy datového nosiče. Mnohem důležitější je předem ověřit jeho spolehlivost, aby později nedošlo ke znehodnocení stop právě jeho nízkou spolehlivostí. K tomu je nutné použít speciální nástroje.

[7] V ČR se praxi používají pouze vlastnoruční podpisy.

- Bývá také vhodné spojit osobu DEFR se získanými digitálními stopami, k tomu lze použít podpisy, digitální podpisy, biometrii nebo fotografování[7].

Všechny digitální přístroje, které byly shromážděny, musejí být odpovídajícím způsobem chráněny. Potenciální digitální důkazy musí být dostupné po celou dobu řešení případu, která se může lišit v závislosti na právním řádu.

2.3.2 Síťová zařízení

V tomto případě považujme za síťová zařízení počítače nebo zařízení pro uchování dat, která jsou připojena k síti. Síťová zařízení mohou zahrnovat sálové počítače, servery, stolní počítače, přístupové body, přepínače, rozbočovače, směrovače, mobilní zařízení, tablety, bluetooth zařízení, kamerové systémy a mnoho dalších. Zdůrazněme, že v případě, kdy jsou digitální zařízení propojená k síti, je obtížné zjistit, kde jsou uloženy digitální stopy. Data by mohla být umístěna kdekoliv na síti.

Identifikace

Identifikace digitálních zařízení zahrnuje i vyhledání loga výrobce, sériových čísel, kolébek a napájecích adaptérů. Vzhledem k obecně malé velikosti mobilních zařízení musí DEFR dbát zvýšené opatrnosti při identifikaci všech typů mobilních zařízení, které mohou být relevantní pro daný případ. DEFR musí zabezpečit místo činu a zajistit, aby žádné osoby nemohly odstranit mobilní nebo jiné digitální zařízení z místa činu. Digitální zařízení, které může obsahovat digitální stopy, by mělo být chráněno před neoprávněným přístupem.

Prohledání místa činu a dokumentace

Před tím, než dojde k jakémukoliv zásahu do původního stavu místa činu (sběr důkazů), by mělo být místo vizuálně zdokumentováno buď kamerou, fotografováním, nebo kreslením, aby existovala dokumentace, jak místo vypadalo při příchodu DEFR. Volba metody musí být v souladu s okolnostmi, náklady, časem a dostupnými zdroji. DEFR zdokumentuje všechny ostatní položky na místě, které mohou obsahovat relevantní materiály, jako jsou napsané poznámky, lístky s poznámkami, diáře a další.

Zajišťování a uchování digitálních stop

DEFR se musí rozhodnout, zda zajistit celá zařízení nebo jen zajistit data z digitálních zařízení. Volba závisí na okolnostech, nákladech, času, dostupných zdrojích a prioritách.

Pokud se DEFR rozhodl odpojit zařízení, následný proces shromažďování digitálních stop bude popsán níže. V případě, že zařízení nemůže být odpojeno od sítě z důvodu kritičnosti jeho funkce nebo pravděpodobnosti zničení digitálních stop, měl by DEFR provést zajištění stop z běžícího zařízení, zatímco zařízení zůstává připojeno k síti.

Obecně platí, že mobilní zařízení jako jsou tablety a mobilní telefony, musí být zapnuty, aby bylo možné získat digitální stopy. Tato zařízení pokud jsou v provozu, plynule mění své provozní prostředí (například bývá aktualizován čítač hodin). Související problém je, že dvě bitové kopie dat ze stejného zařízení se liší, a proto neprochází standardní ověřovací funkcí jako je hash. V takové situaci je nutné využít alternativní funkce pro ověření dat, které identifikují standardní a měnící se oblasti.

Pokud se DEFR rozhodl zajistit data zařízení, síťová zařízení by měla zůstat spuštěna po dobu identifikace dalších zařízení připojených k síti. DEFR by však měl zvážit možnost sabotáže

vyšetřované sítě prostřednictvím aktivního síťového připojení a podle toho se rozhodnout, zda monitorovat systém nebo jej raději odpojit[8].

V některých případech může být vhodné ponechat síťová zařízení připojená, aby jejich činnost mohla být monitorována a dokumentována příslušným orgánem.

- Pokud je upřednostněno zajištění zařízení a je známo, že zařízení obsahuje energeticky závislou paměť (RAM), zařízení by mělo být trvale připojeno ke zdroji elektrické energie.
- Pokud je mobilní přístroj vypnutý, měl by být označen a pečlivě zabalen a zapečetěn. Mělo by se tak přecházet náhodnému stisku kláves nebo tlačítek při převozu. Jako preventivní opatření, by DEFR měl rovněž zvážit použití stíněné krabičky nebo Faradayovy klece[9].
- Za určitých okolností, je lepší mobilní zařízení po sběru vypnout, aby se zabránilo změně dat.

V případě že, zařízení je připojeno k síti, existuje i možnost, že zařízení je připojeno k více než jedné fyzické a/nebo virtuální síti. Například zařízení, které vypadá, že má jedno viditelné fyzické síťové připojení, může být ve skutečnosti připojeno pomocí virtuální privátní sítě (VPN) a provozovat více virtuálních strojů s více než jednou IP adresou. Proto by DEFR před odpojením měl analyzovat i logická datová spojení.[10]

Při zajišťování dat u síťového zařízení, které musí být trvale zapnuté, by mělo být zabráněno zařízení jakkoliv datově komunikovat včetně signálů mobilních operátorů nebo GPS. DEFR by měl použít metody povolené místními zákony, aby izoloval rádiové signály. Metody izolace mohou zahrnovat, ale nejsou omezeny pouze na:

- Použití rušičky, která vysílá silné signály, které blokují příchozí i odchozí signály, tento způsob může být ale v některých zemích zakázán[11].
- Použití stíněného pracovního prostoru (Faradayovy klece).
- U mobilních telefonů je možné použití náhradní SIM - speciální zachovávající identitu zařízení ale blokující datový provoz.
- Zakázat zařízení síťové služby po domluvě s mobilním operátorem.

DEFR by měl provést zajištění informací před vyjmutím baterie z telefonu.

2.3.3 Zajišťování a uchovávání kamerových systémů

DEFR by měl pochopit, že zajištění video sekvencí z počítačově založeného nebo zabudovaného DVR kamerového systému se liší od zajišťování digitálních stop z počítače. Níže jsou uvedeny specifické pokyny pro zajišťování digitálních stop z kamerových systémů:

---

[8] V praxi při sběru mobilních zařízení bývá postup takový, že je zařízení přepnuto do režimu letadlo, (případně i dobito) a předáno odborníkovi na mobilní zařízení.

[9] V praxi je toto použito pouze v extrémních případech (např. nebezpečí odpálení bomby). Doplníme také, že současné „chytré telefony“ (Smartphone) a tablety by v zapnutém stavu měly být raději ukládány do stíněných obalů, protože v současnosti je již běžně používaná služba dálkového smazání dat (v případech krádeží).

[10] Tyto činnosti již zjevně přesahují kompetence a kvalifikaci DEFR, protože vyžadují analýzu operační paměti zařízení, což je vysoce kvalifikovaná činnost znalce a DEFR nepřísluší takové činnosti provádět na místě.

[11] V ČR je nutné povolení soudu, aby mohla být rušena neveřejná frekvence.

- Před zahájením procesu zajištění digitálních stop musí DEFR nejprve zjistit, zda systém zdokumentoval potřebnou video sekvenci.
- DEFR by měl získat všechny záznamy z relevantních kamer v době činu k zajištění dodatečných informací.

V případech, kdy není možné provádět zajištění stop přímo na místě činu, DEFR musí zajistit digitální paměťová média. Nejčastěji tak, že nahradí pevný disk kamerového systému prázdným nebo klonovaným pevným diskem[12]. Nicméně je nutné posoudit rizika spojená s použitím této metody, jako je například slučitelnost nového pevného disku se systémem a slučitelnost odstraněného pevného disku s jinými systémy použitými při vyšetřování.

3 Diskuze

V této části přinášíme diskuze odborníků z praxe k normě ISO 27037, včetně odchylek typických pro Českou republiku. Neomezujeme se pouze na problematiku sběru digitálních stop, ale zabýváme se také hlediskem odborníka, který se zabývá analýzou získaných digitálních stop.

Prvním odborníkem (část 3.1.) především v oblasti zajišťování digitálních stop je Ing. Ladislav Vyskočil, který působí na Oddělení informační kriminality (Odbor analytiky a informační kriminality, Služba kriminální policie a vyšetřování, Krajské ředitelství policie Jihomoravského kraje) Policie ČR.

Druhým odborníkem (část 3.2.) především v oblasti analýzy digitálních stop je Ing. Marián Světlík, který je vedoucím Znaleckého ústavu společnosti Risk Analysis Consultants, s.r.o. a zároveň soudním znalcem v oboru kriminalistika, kriminalistická počítačová expertíza.

3.1 Názor odborníka z praxe – Zajištění digitálních stop

V normě jsou zpočátku standardní a v oboru dobře známá obecná doporučení (část 2.1 a 2.2), kterých se obecně vyšetřovatelé v ČR, a pravděpodobně i kdekoliv jinde ve světě, drží. Nicméně dále uvedená praktičtější doporučení (část 2.3) jsou již dokonce na dnešní dobu zastaralá. Např. zajištěná zařízení bývají dnes již běžně kompletně zabalena a zapečetěna nejlépe v neprůhledném obalu tak, aby s nimi nemohl nikdo nijak manipulovat – nikoli jak norma doporučuje přelepit mechaniky a spínač zařízení.

Norma dělí vyšetřování na postupy pro zajištění zařízení, která nejsou připojena k síti, a zařízení, která jsou připojena k síti. Toto dělení je již zbytečné, protože v dnešní době jsou téměř všechna zařízení připojena k síti a je nutné ke všem zařízením přistupovat, jako by byla připojena k síti. Zajištění stop v kamerových systémech je v ČR obsahem práce expertů na audiovizuální techniku, a ne specialistů na zajišťování digitálních důkazů. Důvodem jsou určitá specifika audiovizuálních zařízení, zvláště pak jejich úložišť, a hlavně fakt, že jsou z nich nejčastěji zajišťovány audiovizuální záznamy (stopy).

Norma zbytečně zmiňuje, že je nutné při zajištění dat ze zařízení na místě vytvořit bitovou kopii kopie, na které se dále pracuje. Avšak tento fakt je již uveden v rámci obecných doporučení – viz předchozí část 2.1 bod c). Je podivující, že norma vůbec nezmiňuje existenci třetí strany (nezúčastněné), která se velmi často při vyšetřování vyskytuje, a ta v ČR nesmí

[12] Formát disku v kamerových systémech bývá často specifický danému zařízení, a po vyjmutí disku ze zařízení často nebývá možné získat záznamy, z toho důvodu se disky ze zařízení nevyndávají a zajišťuje se celý server.

být při provádění vyšetřování poškozena. Minimálně zmínka o třetích stranách by podle našeho názoru měla být obsahem světové normy.

V normě se na několika místech objevuje zmínka o tom, že je třeba vytvořit kontrolní součet, aby bylo možné ověřit data, nicméně dále již není zmíněno, že vytvořenou hash je třeba zaznamenat do protokolu. Tak je zajištěno ověření, že se zajištěnou stopou dále nemanipulovalo.

Norma obsahuje víceméně popis již zaběhlých případně i vylepšených postupů, které Policie ČR dlouhodobě využívá. Zavedení normy do praxe policie by pravděpodobně nepřineslo nic nového kromě dodatečných nákladů na implementaci dané normy. Dodejme, že norma nebyla od svého uvedení aktualizována, což s vývojem v oblasti ICT, přidává nové problémy související s její implementací. Současná praxe při sběru a následné analýze digitálních stop v ČR je popsána v (Vyskočil, 2013).

3.2 Názor odborníka z praxe – Analýza digitálních stop

Není snadné se vyjádřit stručně k normě, která byla vydána organizací ISO, vzhledem k tomu, že odborníci Znaleckého ústavu RAC se přímo podíleli na jejím připomínkování. Je nutné také zmínit, že naše připomínky, které byly v zásadě v souladu s předchozím názorem policistů z praxe, nebyly organizací ISO přijaty.

Abychom paušálně nekritizovali určitou technickou zastaralost nebo nekonzistenci zejména posledních částí normy, musíme si uvědomit, že to je prakticky první soupis doporučení, který má oficiálně mezinárodní váhu. Musíme také bohužel konstatovat, že pro jednotný výklad normy (implementaci) do prostředí v ČR nejsou vytvořeny organizační ani kompetenční podmínky. A nemyslíme tím jenom implementaci do policejní praxe, ale i do praxe výkonu znalecké činnosti v daném oboru a také do výkonu činnosti CERT týmů a dalších subjektů, které řeší například bezpečnostní incidenty v informačních komunikačních systémech. Protože tady všude probíhá zajišťování digitálních stop, které mohou být posléze použity jako důkazy.

Norma by měla být také určitým východiskem pro posuzování kvalifikačních předpokladů pro výkon znalecké činnosti. Protože reálná praxe ukazuje, že mnoho soudních znalců nezná ani základní požadavky na zajištění digitálních stop, které jsou v úvodu normy uvedeny. Soudní znalci se dostávají do různých pozic – například konzultantů při zajišťovacích úkonech při práci policie, nebo tyto úkony provádějí jako znalci samostatně v ostatních případech, anebo tyto úkony provádějí již jako znalci ve svých laboratořích. Proto by uvedená norma také měla být jedním z mnoha důležitých podkladů kvalifikačních požadavků bezpečnostních specialistů ICT.

Norma ISO 27037 má už od svého vzniku některé, možná i zásadní, nedostatky. Můžeme zde diskutovat, proč jako základ normy nebyly použity jiné podklady a doporučení, která jsou již léta akceptována mezinárodní komunitou digitálních forenzních odborníků (např. doporučení ACPO, DFRWS, IOCE, ENFSI a další). Přesto norma alespoň elementární sjednotila zásady a pravidla práce při zajišťování digitálních stop. Mnohé z nich (pravděpodobně u nás hlavně v policejní praxi) se jeví jako samozřejmé a dlouhá léta již aplikované do praxe. Nicméně naše zkušenosti říkají, že ani policejní praxe není zcela ideální z hlediska schopnosti vytváření obecných postupů.

Na základě této normy by mohlo vzniknout i regulatorní opatření, protože zajišťování digitálních stop je proces, jehož přímým následovníkem je získávání důkazů. To už je natolik závažná skutečnost, že některá elementární pravidla by neměla v žádném případě být

porušována. K porušování i těch základních pravidel však v České republice dochází. Jestliže je biologická stopa prokazatelně kontaminována, tak nemůže být jako důkaz použita. Porušení základních postupů zajištění a práce s digitální stopou však kontaminovanou stopu z důkazního řízení paradoxně nevylučuje.

Závěrem tedy můžeme konstatovat, že uvedenou normu chápeme jako užitečným prvním krokem k procesu, který ve svém důsledku povede ke zvýšení povědomí o specifikách práce s digitálními stopami a důkazy - i přes některé její zjevné nedostatky. Tím přispívá také k postupnému zkvalitnění práce všech, kteří se s digitálními stopami jakýmkoliv způsobem potkávají, ať to jsou policejní technici a experti, soudní znalci, vyšetřovatelé, advokáti, soudci, ale i bezpečnostní specialisté a správci ICT nebo členové CERT týmů.

4 Závěr

V článku jsme prezentovali a diskutovali obsah normy ISO 27037 z roku 2012. Obsah normy jsme podrobili diskuzi odborníků, kteří se problematikou zabývají. Výsledkem je zajímavá konfrontace postupů z praxe s postupy, které zmiňuje norma. Tento článek má i své limity, na které musí být čtenář upozorněn. Jedná se zejména o diskuzi, která je omezena pouze na názory dvou expertů. Na jednu stranu by článek mohl být založen na větším počtu expertů (např. panel expertů), na druhou stranu je třeba brát do úvahy specifičnost představené oblasti a také úzkou komunitu expertů v České republice, jež se tímto tématem zabývá. Shrňme dále hlavní implikace tohoto článku.

První expert z Policie ČR, probírá hlavní odlišnosti při sběru potenciálních digitálních důkazů. Identifikuje zejména některé nedostatky jako opomenutí třetích stran, rozdíly v přístupu k balení důkazů nebo specifické rozdělení práce mezí více expertů. Druhý expert ze Znaleckého ústavu RAC se vyjadřuje k normě obecněji z pohledu expertů, kteří zajištěné důkazy analyzují. Dochází k dvěma propojeným problémům:

- Malá znalost základních principů sběru potencionálních důkazů všemi osobami, které jsou zapojeni na různých úrovních do řešeného případu (např. zasahující policisté na místě činu, soudní znalci). Není výjimkou, že sběr potenciálních digitálních důkazů provádí odborník na zajišťování fyzických stop a nikoli odborník na informační kriminalitu a sběr digitálních stop.
- S tím související problém užívání jiných postupů, které však v českém prostředí nemusí mít dopad na hodnotu důkazu v soudním řízení. Což je celkem nezvyklé a je třeba se této problematice v českém kontextu věnovat.

Názory odborníků říkají, že obecná doporučení uvedená v úvodu standardu jsou formulována dobře. První část normy lze proto považovat za závazný podklad v případě tvorby postupů pro sběr digitálních důkazů. Nicméně druhá část normy, která již obsahuje konkrétní postupy, je na dnešní dobu částečně zastaralá.

Poděkování:

Tento článek byl zpracován za podpory prostředků grantu F4/74/2014 (Inovace systému řízení digitální forenzní laboratoře) řešeném na Fakultě informatiky a statistiky, VŠE v Praze.

Použité Termíny

Digitální stopa	Digitální stopa je jakákoliv informace s vypovídající hodnotou, uložená nebo přenášená v digitální podobě.
ACPO	Asociace policejních ředitelů.
Zajištění digitálních stop	Je proces, který začíná okamžikem, kdy data, nebo zařízení, jsou zajištěna pro znalecké zkoumání.
Bitová kopie	Je kopie digitální stopy, která je uložena na přepisovatelných médiích, např. pevné disky, flash disky a paměťové karty.
DEFR	(Digital Evidence First Responder) je fyzická osoba, která je oprávněna, vyškolena a kvalifikována ke sběru a hledání digitálních důkazů na místě činu
DFRWS	Seminář digitálního forenzního výzkumu
Místo činu	Obecně v kontextu této práce se jedná o fyzické místo, kde probíhá hledání digitálních stop.
Hash	Jedná se o digitální otisk určitého souboru dat pomocí matematické funkce.
ICT	(Information and Communication Technologies) Informační a komunikační technologie
IOCE	Mezinárodní organizace přes digitální důkazy (International Organization on Digital Evidence)
CERT	(Computer Emergency Response Team) Bezpečnostní tým
ENFSI	Pracovní skupina pro forenzní IT
PUK	(PIN Unlock Key) Klíč pro reset PINu v případě jeho ztráty či zapomenutí
PIN	(Personal Identification Number) Klíč pro přístup k využívání určité SIM karty.
IP adresa	Číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti, která používá internetový protokol.
RAM	(Random-Access Memory) Paměť s přímým přístupem.
SIM	(Subscriber Identity Module) tzv. SIM karta pro identifikaci účastníka v mobilní síti.
ZIP	Souborový formát pro kompresi a archivaci dat.
GPS	(Global Positioning System) Jedná se o vojenský globální družicový polohový systém provozovaný Ministerstvem obrany USA.
RFID	(Radio Frequency Identification) Jedná se o novou generaci identifikátorů navazující na systém čárových kódů.
MP3	Jedná se o formát ztrátové komprese zvukových souborů, založený na kompresním algoritmu definovaném skupinou MPEG (Motion Picture Experts Group).
CD	(Compact Disk) Optický disk určený pro ukládání digitálních dat.
DVD	(Digital Video Disc) Jedná se o formát digitálního optického datového nosiče.
Blue-Ray	Třetí generace optických disků, určených pro ukládání digitálních dat.

Seznam použitých zdrojů

Agarwal, R., & Kothari, S. (2015). Review of Digital Forensic Investigation frameworks. In K. J. Kim (Ed.), *Information Science and Applications – Part V.* (pp. 561-571). Berlin: Springer. doi: 10.1007/978-3-662-46578-3_66

Ajijola, A., Zavarsky, P., & Ruhl, R. (2014). A review and comparative evaluation of forensics guidelines of NIST SP 800-101 Rev.1:2014 and ISO/IEC 27037:2012. In *World Congress on Internet Security, WorldCIS 2014* (pp. 66-73). New York: IEEE. doi: 10.1109/WorldCIS.2014.7028169

Chung, H., Park, J., Lee, S., & Kang, C. (2012). Digital forensic investigation of cloud storage services. *Digital investigation*, 9(2), 81-95. doi: 10.1016/j.diin.2012.05.015

Federici, C. (2014). Cloud data imager: A unified answer to remote acquisition of cloud storage areas. *Digital Investigation*, 11(1), 30-42. doi: 10.1016/j.diin.2014.02.002

Gřivna, T., & Polčák, R. (2008). *Kyberkriminalita a právo*. Praha: Auditorium.

Hegarty, R., Lamb, D., & Attwood, A. (2014). Digital Evidence Challenges in the Internet of Things. In *Proceedings of the 10th International Network Conference* (pp. 163-172). Plymouth: Centre for Security, Communications and Network Research.

ISO/IEC 27037:2012. (2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence*. Ženeva: International Organization for Standardization.

ISO/IEC FDIS 27041. (2012). *Information technology – Security techniques -- Guidance on assuring suitability and adequacy of incident investigative methods.* Ženeva: International Organization for Standardization.

ISO/IEC 27043:2015. (2015). *Information technology – Security techniques – Incident investigation principles and processes*. Ženeva: International Organization for Standardization.

ISO/IEC FDIS 27042. (2012). *Information technology – Security techniques -- Guidelines for the analysis and interpretation of digital evidence*. Ženeva: International Organization for Standardization.

Jang, Y.-J., & Kwak, J. (2014). Digital forensics investigation methodology applicable for social network services. *Multimedia Tools and Applications*, 74(14), 5029-5040. doi: 10.1007/s11042-014-2061-8

Kothánek, J. (2014). *Vytěžování důkazů z výpočetní techniky*. Diplomová práce. Brno: Masarykova univerzita.

Overill, R. E. (2014). Quantifying likelihood in digital forensic investigations. *Journal of Harbin Institute of Technology (New Series)*, 21(6), 1-4.

Porada, V. & Rak, R. (2006). Teorie digitálních stop a její aplikace v kriminalistice a forenzních vědách. *Karlovarská právní revue*, 2(4), 1-21.

Porada, V., & Bruna, E. (2013). Digitální svět a dokazování obsahu elektronických dokumentů. In *Bezpečnostní technologie, systémy a management* (pp. 1-10). Zlín: Univerzita Tomáše Bati ve Zlíně.

Rak, R., & Porada, V. (2006). Digitální stopy v kriminalistice a forenzních vědách. *Soudní inženýrství*, 17(1), 3-23.

Shrivastava, G., & Gupta, B. B. (2014). An encapsulated approach of forensic model for digital investigation. In *Proceedings of the IEEE 3rd Global Conference on Consumer Electronics* (pp. 280-284). New York: IEEE. doi: 10.1109/GCCE.2014.7031241

Valjarevic, A., & Venter, H. S. (2015). Introduction of concurrent processes into the digital forensic investigation process. *Australian Journal of Forensic Sciences*, (Article in press). doi: 10.1080/00450618.2015.1052754

Veber, J., & Klíma, T. (2014). Influence of Standards ISO 27000 Family on Digital Evidence Analysis. In: *Proceedings of the 22nd Interdisciplinary Information Management Talks* (pp. 103-114). Linz: Trauner.

Veber, J., & Smutny, Z. (2015). Standard ISO 27037:2012 and collection of digital evidence: Experience in the Czech Republic. In N. Abouzakhar (Ed.), *Proceedings of the 14th European Conference on Cyber Warfare and Security* (pp. 294-299). Reading: ACPI.

Vyskočil, L. (2013). *Zajišťování a analýza digitálních důkazů*. Diplomová práce. Zlín: Univerzita Tomáše Bati ve Zlíně.