Doc. Ing. Roman Rak, PhD.
Prof. JUDr. Ing. Viktor Porada, DrSc., dr.h.c.

VLASTNOSTI DIGITÁLNÍCH STOP A JEJICH DOPADY NA FORENZNÍ ŠETŘENÍ

1. DEFINICE DIGITÁLNÍ STOPY (DS)

Existuje mnoho definic pojmů digitální stopa. Dnes v zahraniční literatuře nejčastěji používaná, a nechá se říci i nejširším okruhem specialistů akceptovatelná definice byla navržena již v roce 1999 pracovní skupinou *SWGDE – Scientific Working Group on Digital Evidence* [1], [2]:

Digitální stopa je jakákoliv informace s vypovídající hodnotou pro danou relevantní událost, uložená nebo přenášená v digitální podobě.

Tato definice je otevřená jakékoliv digitální technologii. Tímto způsobem definovaná digitální stopa pokrývá jak oblast počítačů a počítačové komunikace, tak i oblast digitálních přenosů (mobilní telefony, ale do budoucna i digitální TV apod.), videa, audia, digitální fotografie, data uzavřených kamerových (CCTV[1)]) systémů, data elektronických zabezpečovacích systémů, a jakýchkoliv dalších technologií potenciálně spojených s Hi-Tech kriminalitou.

2. PRAKTICKÝ VÝZNAM VLASTNOSTÍ DIGITÁLNÍCH STOP

Digitální stopy (DS), ostatně jako každý jiný druh kriminalistických stop, mají své obecné i individuální druhové charakteristiky a vlastnosti, které z pohledu orgánů činných v trestním nebo jiném řízení mají typické pozitivní i negativní aspekty a důsledky. Tyto aspekty je pak třeba mít neustále na vědomí po celou dobu a ve všech stádiích práce s digitálními stopami.

Digitální stopy vznikají působením (ovládáním, využíváním) člověka (uživatele, pachatele) na aplikační nebo systémový software, funkčnost digitálního zařízení nebo automatickým (předem naprogramovaným) působením jednoho zařízení, technologie na druhé.

Digitální stopy proto v neobvykle vysoké míře odrážejí specifické vlastnosti high-tech technologií s bohatou rozmanitostí lidského ducha jejich uživatelů, kteří je využívají.

Specifika digitálních stop, společně s jejich pozitivními i negativními aspekty využití jsou shrnuty v tab. 1.

2.1 Nehmotnost digitálních stop

Při zajišťování digitálních stop musí ten, kdo tento výkon realizuje, velice dobře znát nejrůznější druhy médií, na kterých se mohou krátkodobě či dlouhodobě vyskytovat data, tedy digitální stopy. Jak vyplývá z definice digitální stopy, vyšetřující nebo expertní orgány mohou zajímat jak uložená data, tak i data zpracovávaná nebo přenášená. V praxi pracujeme spíše s daty uloženými na nosičích nejrůznějších forem – pevných discích, disketách, CD a DVD discích, Flash/USB pamětí, „zipkách", páskách, optických discích, paměťových kartách. Nemusí se nutně jednat ale jen o klasická média známá z běžných prodejen výpočetní a komunikační techniky. Mohou to být i průmyslová média měřících a regulačních jednotek, palubní počítače, černé skříňky letadel apod. Např. identifikační číslo vozidla (VIN – Vehicle Identification Number) je digitálně uloženo v řídící jednotce motoru apod.

Pozornost musíme věnovat jak datům uloženým v HW komponentách (sálových počítačích – tzv. mainframech, PC, noteboocích, PDA[2)] zařízeních apod.), tak i datům na transportních médiích, umožňujících datové přenosy „off line" z jednoho zařízení do druhého (již zmiňované diskety, CD, DVD, paměti atd.). Při ohledání a zajištění místa trestného činu nesmíme opomenout, že tato média mohou být uložena mimo pracoviště (kancelář, soukromá pracovna apod.) ve zcela jiných fyzických objektech, v bankovních trezorech apod.

V prostředí institucí je situace o to složitější, neboť data bývají uložena ve společně sdílených prostorech (sdílené souborové adresáře, uložiště dokumentů, elektronické pošty, databázích, atd.), takže data zpracovávaná nebo využívaná jednou a toutéž osobou mohou být uložena fyzicky na mnoha místech, dokonce i mimo fyzický prostor patřící dané instituci (uživatel si může např. zcela zadarmo vytvořit veřejnou e-mailovou schránku, kam je možné z instituce přeposílat citlivá data a ta ukládat pod smyšlenou identitou).

V případě počítačů a periférií, či datových nosičů, přidělených, spravovaných a využívaných jednotlivou osobou, nebývá zpravidla problém zajištění hmotného nosiče jako důkazního prostředku. Podstatně komplikovanější situace nastává v případě masově sdílených výpočetních a komunikačních prostředků, které nepřetržitě zajišťují významné procesy v instituci, takže je nelze vypnout nebo

---

1) CCTV – Closed Circuit TV.
2) PDA - personal digital assistant

Doc. Ing. Roman Rak, PhD., manažer kompetenčního centra vnitropodnikových aplikací, Český Telecom a.s., Olšanská 5, 130 00 Praha 3, e-mail: roman.rak@ct.cz
Prof. JUDr. Ing. Viktor Porada, DrSc., dr.h.c., vedoucí oddělení vědy a výzkumu PA ČR, P. O. BOX 54, 143 01 Praha 4, e-mail: porada@polac.cz
Katedra trestního práva, kriminalistiky a forenzních disciplín, Vysoká škola Karlovy Vary, o. p. s., T. G. Masaryka 3, 360 01 Karlovy Vary

Tab. 1 Specifika digitálních stop

Charakteristické vlastnosti digitálních stop (DS)	Popis vlastností	Pozitiva využití	Negativa využití
Nehmotnost	Data, informace jako takové jsou nehmotné. Pro jejich uložení je nutné hmotné prostředí.	DS má reálný fyzikální význam. Médium se zachovanými DS je věcným důkazem.	Vysoká variabilita různých druhů médií. K médiu musí existovat zařízení, které je schopno číst. S časem se snižuje schopnost přečíst médium.
Latentnost	DS jsou bez technologických periférií nebo jiných speciálních prostředků pro lidské smysly nezaznamenatelné. Většina DS je pro běžné uživatele neviditelná i za pomoci těchto prvků.	Neznalý uživatel zanechává DS, aniž by si to sám uvědomoval.	Nutnost speciálních periférií, HW a/nebo SW, přístupových/ administrátorských práv nebo znalostí pro zviditelnění DS.
Časová trasovatelnost	Velké množství DS je ve výpočetních a komunikačních systémech prokazatelně spojeno s velmi přesným časovým údajem.	Nežádoucí uživatelské aktivity lze determinovat v čase.	Znalý uživatel s příslušnými administrátorskými oprávněními může pozměnit (antidatovat) systémový čas nebo změnit časové značky.
Vysoká obsažnost	DS mají vysokou informační hodnotu. Informace, tedy i DS mají dnes multimediální charakter.	Dostatečné množství informací relevantních ke kriminalistickým nebo forenzním šetřením.	Vysoké množství informací může způsobit informační přesycení a relevantní údaje mohou být přehlédnuty nebo nedoceněny.
Velmi nízká životnost	Záznamy v informačních a komunikačních systémech mohou být smazány nebo přepsány jinými. Je to dáno vlastnostmi ICT technologií i cílenou činností pachatele.	V některých specifických případech a za příznivých okolností je možné obnovit původní informace z datových nosičů.	Do rozsáhlých ICT technologií, kde chceme zajistit auditovatelnost datových záznamů je nutné investovat značné finanční i jiné zdroje.
Uchování a kvalita je ovlivněna řadou subjektivních faktorů	Determinujícím faktorem jsou legislativní a interní předpisy, odbornost administrace ICT a institucionální kultura úrovně informační bezpečnosti.	Při správně nastavených parametrech auditovatelnosti IS a jejich praktické realizaci jsou v ICT systémech zachovány požadované informace, využitelné jako DS.	Při nedodržování základních pravidel je praktická použitelnost DS zpravidla nízká.
Velký datový objem	Na paměťových médiích je dnes uchováváno obrovské množství informací.	Velké množství informací predikuje naději nalézt potřebný důkazní materiál.	Velký objem dat a častá neznalost toho, co hledáme může generovat informační přesycení a/nebo nulový výsledek hledání.
Datová hustota v čase a s rozvojem nových technologií neustále klesá	V důsledku rozvoje levných velkokapacitních datových médií a intenzivního využívání výpočetní techniky se ukládají stále větší objemy dat, ve kterých se DS stále hůře nalézají.		Vyhledávání digitálních stop v souvislosti se snižující se jejich hustotou je neustále komplikovanější.
Extrémní dynamičnost prostředí	Provoz podnikových klíčových informačních a komunikačních systémů nelze přerušit, jinak jejich majiteli hrozí značné ekonomické ztráty.		Všechny DS není možné za plného provozu v některých případech nalézt a fixovat. Naopak hrozí, že v důsledku provozu IS budou zničeny nebo znehodnoceny.

Tab. 1 Specifika digitálních stop (pokračování)

Charakteristické vlastnosti digitálních stop (DS)	Popis vlastností	Pozitiva využití	Negativa využití
Heterogennost a komplexnost prostředí	Prostředí výpočetních a komunikačních technologií v institucích bývá velmi rozmanité, heterogenní.	Heterogenní systémy často tvoří integrované celky, napříč kterých probíhá zpracování informací. V každé části složitých komplexů je možné tak najít důkazní materiál, i když v jiných částech absentuje nebo je zničen.	Pro vyhledávání, fixaci a analýzu DS je často potřebné velké množství vysoce kvalifikovaných specialistů. Tyto procesy mohou být časově velmi náročné a spotřebovávat velké množství nejrůznějších zdrojů.
Velký geografický rozsah prostoru	Počítačové sítě, výpočetní a komunikační prostředky neznají geografických hranic. Z tohoto pohledu je prostředí „homogenní“, technologicky standardizované. Promyšlené útoky jsou např. cíleně vedeny přes několik serverů v cizích zemích.	V každém geograficky odlišném elementu výpočetního nebo komunikačního komplexu se mohou nalézat DS.	Forenzní zkoumání takovéhoto prostředí může být extrémně rozsáhlé. Rozdílná legislativa v různých zemích, vyšetřovací postupy a různé způsoby zajišťování DS. Toto prostředí je z pohledu vyšetřování silně „heterogenní“, legislativně nestandardizované.
Vysoký stupeň ochrany dat znesnadňuje nebo znemožňuje práci s DS	Zašifrovaná, zakódovaná data neobsahují v této formě pro vyšetřování žádnou použitelnou informaci ve vztahu k obsahu zprávy.		Dekódování je časově velmi náročné, ne-li nemožné.
DS je specializovanými prostředky automaticky identifikovatelná a zpracovatelná.	Některé digitální stopy vznikají jako důsledek působení aplikačního nebo systémového SW nezávisle na uživateli.	DS automaticky generované aplikačním nebo systémovým SW je možné identifikovat pomocí jiného specializovaného SW.	Automatizované prostředky pro vyhledávání DS generují velké množství informací, které je nutné dále manuálně zpracovávat. Automatizace není samospasitelná.
Vysoká úroveň zahlazování digitálních stop kvalifikovanými pachateli	Pachatelé s vysokou odborností v oblasti ICT mají předpoklady způsobit největší škody a zároveň kvalifikovaně zahladit stopy.	Důsledně aplikovaná informační, „vrstvená“ bezpečnost v prostředí administrátorů ICTa dalších specialistů může podstatně snížit toto riziko.	Vyhledávání a zajišťování DS může být více komplikované.
Restaurovatelnost DS	Některé smazané nebo zničené záznamy – digitální stopy lze restaurovat (z „košů“, back-upů, archivních médií, datových nosičů apod.).	Tato vlastnost z forenzního hlediska je jedinečná a nevyskytuje se u jiných druhů stop.	
Originálnost DS	Datové záznamy, jejich nosiče lze snadno kopírovat, vytvářet duplikáty, aniž by došlo ke kvalitativní nebo kvantitativní změně obsahu nebo vlastností DS.	Vytváření kopií garantuje zachování dat v případě poškození, zničení, ztráty originálního nosiče.	Nelze vyloučit podvrhy, padělky se změněným obsahem dat. Nesnadné prokazování originálnosti datových nosičů v soudních procesech. Zdroj nedůvěry k DS.
Současně nízká úroveň soudní akceptace DS v právní praxi	DS poskytují obrovské množství informací – data, obraz, zvuk apod.	Z pohledu obsahu jsou mnohem obsažnější a komplexnější než klasické kriminalistické stopy. V různých informačních systémech je/bude o nás mnohem více komplexnějších a přesnějších informacích, než znají o nás např. naši sousedé, známí, kolegové.	Digitální stopy jsou v právní praxi zcela nové. Neexistuje příslušná legislativa, zkušenosti. Neexistují standardizované postupy pro vyhledávání, zajišťování, dokumentaci a předávání DS.

je jinak fyzicky zajistit, či dokonce odvézt do laboratoře nebo na specializované odborné pracoviště k expertize.

Významným zdrojem potenciálních digitálních stop jsou i archivní média, na kterých jsou zaznamenány údaje k určitému, jasně definovanému času jako konkrétní časový snímek událostí, které proběhly. Archivace mnohdy probíhá mimo vědomí i možnost ovlivnění běžných uživatelů (výjimkou bývají zpravidla IT specialisté, kteří za určitých předpokladů – zejména špatně nastavěné bezpečnostní politice – mohou ovlivnit archivovaná data).

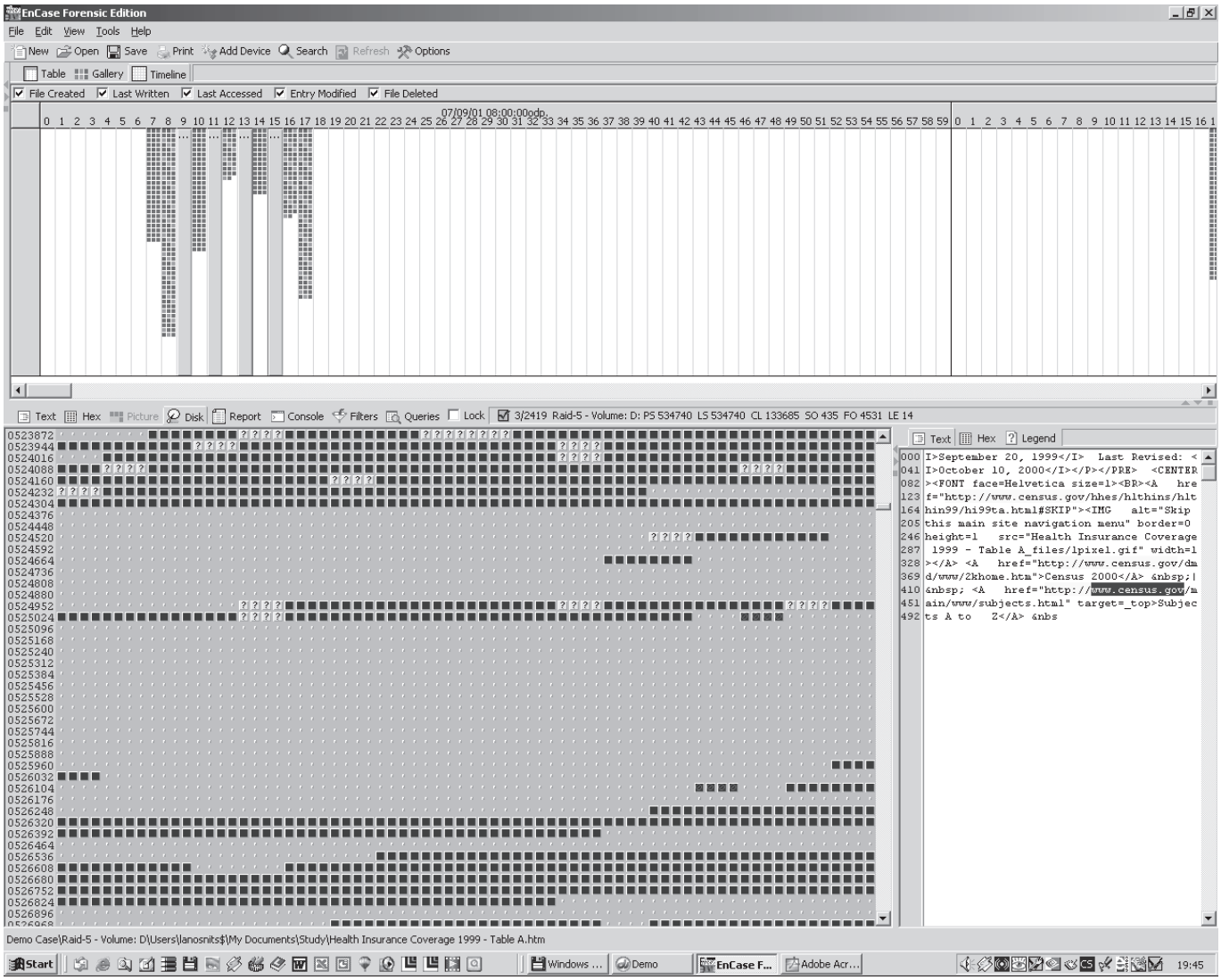
Samostatnou, velmi specifickou kapitolou vyhledávání a analýzy digitálních stop jsou přenášená data (po pevném metalickém spojení nebo jakoukoliv bezdrátovou technologií), nebo data zpracovávaná v operační paměti. Tato data v procesu jejich přenosu nebo zpracování nejsou nikde primárně uložena. Pouze v situaci, kdy předpokládáme výskyt určitých dat, která mohou mít charakter digitálních stop, můžeme zabezpečit jejich uložení na vhodné médium a následně (někdy i dokonce paralelně) je analyzovat. Tento způsob práce s digitálními stopami (jejich vyhledávání, zajišťování i analýza) má často operativní charakter a je blízký metodám odposlechů, monitorování radioprovozu apod. se všemi jejich dalšími specifičnostmi.

2.2 Latentnost digitálních stop

Ke zviditelnění latentních digitálních stop používáme různé druhy softwaru:

a) Aplikační software. Ten je dostupný běžným uživatelům, kteří disponují příslušnými oprávněními na jeho využívání. Např. v textovém editoru Word je možné zjistit datumy posledních změn v dokumentu, jejich autorství apod.

b) Systémový software. S ním běžně pracují IT specialisté, systéméví inženýři, databázoví specialisté, síťaři apod. V transakčních logovacích tabulkách databází nebo operačních systémů tak najdeme např. informace o provedených operacích, jejich původcích a dalších souvislostech. V souborovém systému



Obr. 1 Obrázek znázorňuje časoprostorový snímek fyzického uložení dat. Čtverečky v levé spodní části obrazovky znázorňují fyzické umístění dat na disku počítače, v pravém spodním rohu vidíme textovou reprezentaci obsahu dat ve vybraném diskovém segmentu v konkrétním čase. „Sloupcový graf" v horní části obrazovky je časovým snímkem práce s datovými soubory (vytvoření souboru, poslední zápis, přístup, modifikace nebo smazání) s minutovou přesností v časovém úseku od 8 do 9 hodin večera dne 7. 9. 2005.

zjistíme základní informace o vytvoření a modifikacích souborů, jejich vlastnictví atd.

c) **Specializovaný forenzní software.** Ten využívají zpravidla jen certifikovaní specialisté – auditoři, bezpečnostní specialisté, soudní znalci. Pomocí tohoto SW lze vyhledávat, zajišťovat a protokolovat i data, které se běžní uživatelé nebo IT specialisté pokusili skrýt nebo zničit (smazání souborů, logů, formátování disků apod.).

2.3 Časová trasovatelnost digitálních stop

Časová trasovatelnost digitálních stop ve srovnání s ostatními druhy stop používaných ve forenzních vědách je unikátní. V kriminalistice nenajdeme jiný druh stop, který by byl přesně určen v čase, jako digitální stopa. Její podstatou je časová známka, která je základním atributem zpracování dnes libovolné informace v digitálním prostředí.

Klasická kriminalistika se snaží obvykle vyjasnit alespoň přibližnou dobu smrti oběti, časový průběh nehodového děje, výskytu jiných osob na místě trestného činu, definovat časové závislosti, prověřit alibi ve vztahu k určitému časovému bodu apod.

Při zajišťování a analýze digitálních stop (pokud jsou nalezeny), nebývá zpravidla problém s jejich časovým určením s přesností na zlomek sekundy, neboť drtivá většina dat si nativně nese tyto informace s sebou.

Virtualita digitálního prostředí, komunikační prostředí sítí přináší s sebou ale jiný problém. Ne vždy je možné vymezit přesně prostor (počítač, či jakékoliv jiné zařízení), kde primárně data vznikla, nebo kdo je jejich autorem. V digitálním časoprostoru je časová hodnota mnohem lépe definovatelná než souřadnice místa vzniku dat. Toto je další rozdíl oproti klasické kriminalistice, kde je ve většině případech známo přesně místo trestného činu na úkor definice času jeho uskutečnění. Výjimky pochopitelně existují – vražda může být spáchána na jiném místě, než je nalezeno mrtvé tělo oběti, stejně jako doba smrti nemusí být vůbec lehce určitelná. Tímto si pachatel zajišťuje větší neurčitost časoprostoru, a tedy výhodu před vyšetřovateli.

2.4 Vysoká obsažnost digitálních stop

Díky vysoké obsažnosti digitálních stop lze s nimi pracovat mnoha způsoby.

Důkazní digitální stopy. Digitální stopy mohou sloužit především jako věcný důkaz, tj. dokázat vykonání určité činnosti pachatelem, která je v rozporu se zákonem nebo interními předpisy– např. pachatel elektronickou poštou odeslal utajovaný dokument konkurenční instituci, provedl neoprávněnou finanční transakci, kterou poškodil svého zaměstnavatele, pořizoval pornografický materiál s mladistvými, nelegálně kopíroval audio nebo video nosiče a tím porušoval autorský zákon atd. Tento druh digitálních stop souvisí přímo s trestným činem.

Indikativní digitální stopy. Kromě toho digitální stopy často obsahují další nepřímé informace, které neprokazují sice trestný čin, ale lze z nich odvozovat různé souvislosti a pomocí nich nalézt další usvědčující materiál, jež je již důkazní. V počítači nalezneme např. další utajované, zatím neodeslané informace, ke kterým má pachatel profesní, legitimní přístup; seznam bankovních kont

Obr. 2 Digitální fotografie si sebou nese základní metada, tj. i datum pořízení snímku, jeho editaci apod.

(pomocí dalšího šetření lze na nich zjistit finanční pohyby, svědčící o nevysvětlitelných příjmech této osoby); seznam nezletilých osob nebo potenciálních odběratelů pirátských kopií atd. Tento druh digitálních stop má indikativní charakter. Forenzní prohlídka personálního počítače je z tohoto pohledu podobná klasické domovní prohlídce.

Profilové digitální stopy. V neposlední řadě veškeré informace, se kterými člověk pracoval jakoukoliv formou (četl je, prohlížel, poslouchal, vytvářel, modifikoval atd.) a jsou uloženy v digitálních zařízeních, svědčí o jeho profesních i osobních zájmech a preferencích. Jsou to nejrůznější autorské texty, komunikace s přáteli, kolegy, zákazníky a dodavateli, odkazy, nejrůznější transakční aktivity atd. Multimediálnost dnešních technologických zařízeních dává digitálním stopám zcela nový rozměr a v určitém smyslu jsou svým způsobem prodlouženým zrakem a sluchem vyšetřovatele či jiného forenzního specialisty. Dokážeme-li s těmito informacemi pracovat, správně je dávat do souvislostí a ověřovat, analyzovat, můžeme velice efektivně profilovat osobnost majitele informací, uložených v jeho technologickém zařízení. V počítačích a jejich periferiích se dnes dozvíme mnohem více informací, než z okruhu sousedů, kolegů, přátel apod. dané osoby. Podobným způsobem na základě analýzy digitálních dat můžeme usuzovat o klasifikaci, zařazení nejenom jedné, jediné osoby, ale i o určitých týmech, skupinách, organizačních celcích, institucích, které tyto data sdílejí.

2.5 Velmi nízká životnost digitálních stop

Výpočetní a komunikační technika je primárně zaměřena na co „nejrychlejší“ zpracování a přenos dat. Zpracování probíhá v omezeném HW prostoru (disková kapacita, operační paměť), kde neustále přibývá nových dat. Pevné disky počítačů jsou přepisovatelné. Dynamika změn v datových uložištích je obrovská. Aplikace určené pro průmyslové, komerční i státní využití jsou projektovány a používány k nepřetržitému provozu, takže v mnoha případech je není dokonce ani možné odstavit a data v klidu fixovat, pořídit kopie. Ideální by bylo odstavení výpočetní a komunikační techniky a zajistit dále již neměnné prostředí pro práci počítačových expertů. To v praxi není obvykle možné. Takováto odstávka pro postiženou instituci by ve většině případů znamenala řádově vyšší škody, než škody způsobené pachatelem, jež chceme vyšetřit.

Nízká životnost digitálních stop klade vysoké nároky na jejich vyhledávání, fixaci a dokumentaci. Rozhodující je proto rychlost, s jakou jsou digitální stopy zajištěny ze všech potenciálních médií. Velký objem dat, heterogennost prostředí a další specifika digitálních stop jsou v rozporu s požadavky na jejich zajištění a vyhodnocení.

Velký důraz je kladen na zajištění co největšího množství digitálních stop v co nejrannějším stadiu šetření. Jestliže časem zjistíme, že bychom potřebovali zajišťovat další specifické digitální stopy, nemusí již v tuto chvíli existovat. Mohou být smazána, přepsána uživatelem nebo samotným (operačním, databázovým) systémem nebo uživatelskou aplikací. V informačních a komunikačních systémech, které není možné odstavit z nejrůznějších důvodů, všichni uživatelé, včetně případných pachatelů, mohou pracovat dál a tedy i v určitých případech měnit údaje pod rukami expertů.

2.6 Uchování a kvalita digitálních stop je ovlivněna řadou subjektivních faktorů

Dobrá znalost subjektivních faktorů je předpokladem pro efektivní a úspěšné zajištění digitálních stop a následné úkony. Dobře nastavená ICT bezpečnost v instituci, znalost úrovně jejího dodržování (či porušování) otevírají vyšetřujícím orgánům další cesty ke shromažďování důkazů.

Kromě formálních vztahů a procesů v každé instituci existují i vztahy a procesy neformální, takže je možné najít osoby, znající systémová hesla, mající přístup k datovým uložištím, ač z z oficiálních pověření k nim nemají mít přístup. Znalost „místního“ prostředí může expertům velmi pomoci a urychlit práci. Technická expertiza může být proto vhodně spojována s vytěžováním technického obslužného personálu.

Havarijní plány, záložní, archivní média jsou dalším zdrojem užitečných dat. Jejich kvalita záleží i na subjektivní míře dodržování bezpečnosti, politiky dané instituce. V mnoha institucích neexistuje dokonce ani pravidelné, centralizované zálohování dat informací na koncových stanic uživatelů, takže tato data jsou zálohována vlastními silami uživatele a můžeme je nalézt jak na záložních médiích, tak i na soukromých zařízeních, mnohdy i v prostorách bydliště pracovníka instituce.

2.7 Velký datový objem digitálních stop

Vyhledávání digitálních stop v praxi často připomíná hledání jehly v kupce sena. Aby bylo efektivní, směřujeme jej proto do prohledávání standardních prostor, kde se stopy určitého druhu vyskytují (logy databází, operačních systémů), zkoumáme poslední změněné záznamy, analyzujeme datové záznamy podle autorství změn, používaných aplikací uživatelem apod. Zkoumáme digitální stopy zanechávané systémovými prostředky a aplikacemi (např. naposledy otevřené soubory, změny přístupových oprávnění, statistické údaje dokumentů, tzv. metadata). V jiných případech prohledáváme textové soubory pomocí fulltextových technologií, tj. hledáme předem zadaná slova a jejich spojení. V tomto případě pracujeme s obsahem uživatelsky vytvářených souborů, databázových tabulek apod.

Skrývá-li uživatel určité informace, nebo nemá-li standardně nastavené systémové parametry (standardně instalované programy), požadovaná systémová nebo aplikační data jsou ukládány do uživatelsky (nikoliv systémově) definovaných prostor, které nejsou nijak standardizované a práce experta je o to složitější nebo časově náročnější.

Vyhledávání digitálních stop velice účinně pomáhají odborné znalosti a zkušenosti experta, stejně tak specializované forenzní analytické SW nástroje, s pomocí kterých (často i automaticky) vyhledáváme data podle určitých předdefinovaných scénářů či parametrů.

2.8 Datová hustota digitálních stop v čase a s rozvojem nových technologií neustále klesá

Neustále se snižující hustota datových stop je skutečností, se kterou musíme reálně počítat. O to intenzivnější musí být efektivita práce forenzních specialistů. Základním východiskem pro řešení této

situace je dlouhodobá cílená strategie a koncepce při budování forenzních týmů specializovaných na digitální stopy, podpora jejich znalostní potenciálu i praktických dovedností. Účinnou pomocí jsou standardizované postupy a SW forenzní nástroje.

Jednotné a sdílené znalosti o základních vyšetřovacích postupech specifických kategorií reálných nebo potenciálních uživatelských aktivit pomohou provést základní vyšetřovací úkony a odhalit běžné digitální stopy (analýza obsahu elektronické pošty, posledně vytvořené nebo modifikované soubory, přehledy počítačových a komunikačních aktivit uživatele za poslední nebo jinak specifikované období apod.).

Analýza běžných (obvyklých) digitálních stop je potom rychlá a zbytek času je možné věnovat vytvářením komplexnějších hypotéz, zaměřených na sofistikované páchání trestné činnosti ve specializovaných SW: billingové (platební) systémy, vnitropodnikové aplikace, překonávání bezpečnostních opatření atd. Zatímco běžné digitální stopy jsou typické pro standardizovaný SW (produkty MS Office, operační systémy, adresářové služby …), stopy zanechané sofistikovaným pácháním trestné činnosti jsou zpravidla jedinečné a typické pro konkrétní prostředí v dané instituci.

V tomto případě vyšetřovací postupy nejsou standardní a automaticky opakovatelné, ale individuální a velmi náročné, protože přesně neznáme, co hledáme a zpravidla nemůžeme ovlivnit fenomén hustoty datových stop.

2.9 Extrémní dynamičnost prostředí digitálních stop

Z praktických důvodů při vyšetřování nelze tyto aplikace (a vše co s nimi souvisí) odstavit (zastavit jejich provoz), následně zajistit digitální stopy, provést nezbytné analýzy, případě korekce z nich vyplývající a po té aplikace znovu pustit do živého, produkčního provozu. Tento postup by u kritických aplikací měl větší negativní dopady než škody, které jsou vyšetřovány. Z tohoto důvodu komerčně orientované organizace (pokud zde není střet se zákonem) nikdy samy nedopustí „klasické ohledání místa trestného činu" s vyloučením všech osob a činností po dobu ohledání a zajištění věcných důkazů, tedy včetně digitálních stop. Vyšetřování, expertiza musí být vedena v živém, produkčním prostředí, v krajním případě ze záložních nebo archivních médií[3)]. Produkční prostředí je ale extrémně dynamické, generuje obrovské množství transakcí, které mohou přepisovat, zneplatňovat či mazat skutečné, relevantní digitální stopy (důkazy). Není-li znám pachatel (podezřelé osoby) a s aplikací, v prostředí obecně pracuje větší množství uživatelů, pravděpodobnost zajištění relevantních důkazů s rostoucím časem prudce klesá. Naopak pachatel má dostatek času a prostoru aby stopy smazal nebo pozměnil. Situace je komplikována tím víc, má-li tato osoba dostatečné znalosti a oprávnění (administrátorské, superuživatelské, aplikační apod.). Kritické aplikace musí být proto navrženy podle přísných bezpečnostních pravidel (oddělení pracovních rolí zaměstnanců, žurnálování transakcí, archivace dat, průběžný monitoring apod.). Pokud tyto pravidla při vývoji nebo v provozu nejsou dodržována, hledání pachatele je velmi komplikovanou záležitostí s vysokou mírou nejistoty výsledku a velkou investicí do zdrojů vyšetřování.

[3)] Záleží i na typu, charakteru digitálních stop, které zajišťujeme nebo zkoumáme.

2.10 Heterogennost a komplexnost prostředí digitálních stop

Vezmeme-li v úvahu analogii výjezdové kriminalistické skupiny, která na místě činu, např. vraždy, zajišťuje vyhledávání a fixaci klasických kriminalistických stop (tým se může skládat např. z policejního lékaře a specializovaných kriminalistických techniků, zodpovědných za zajišťování daktyloskopických, trasologických, balistických stop), pak při vyšetřování trestného činu spáchaného v prostředí ICT je nezbytností mít podobný tým, složený ale „jen" z IT specialistů (např. odborníků na správu elektronické pošty, operačních systémů, databází, podnikových aplikací – SAP apod.)! Na rozdíl od prvního příkladu kriminalistické výjezdové skupiny ale policie takovéto týmy pro vyšetřování počítačové kriminality nemívá k dispozici. Denní sazba špičkového specialisty se v podmínkách ČR počítá 20 až 50 tisíc korun osmihodinové pracovní doby. Kvalita a včasnost zajištění digitálních stop ale zásadně rozhoduje o úspěšnosti forenzního nebo kriminalistického vyšetřování. Nedostatky v rychlém a včasném zajišťování kvalitních digitálních stop jsou primární příčinou nízké objasněnosti kriminality spojené s informačními a komunikačními technologiemi. Zásadní roli hraje i komplexnost prostředí. Je-li např. objektem zkoumání PC (nebo jiná technologie orientována na pokrytí potřeb jejího uživatele/majitele – mobil, elektronický diář, videokamera, digitální fotoaparát apod.), které je možné z prostředí jednoduše vyjmout, pak je možné je při zachování určitých procesních a funkcionálních pravidel zaslat do specializované forenzní instituce a tam je zkoumat v laboratorních podmínkách vysoce profesionálním týmem. Z tohoto pohledu pak orgány činné v trestním řízení podle určitých zásad zajistí důkazní materiál již v první linii a předají je dál. V první linii, na místě trestného činu pak nemusí být ICT specialisté, pokud se jedná o standardní postup. Naopak v prostředí podnikových informačních systémů nebo kdekoliv tam, kde je silná integrace s okolním prostředím, vysoký stupeň požadavku na kritičnost aplikace (vysoká dostupnost služeb), tento postup bývá zcela vyloučen. Nelze demontovat např. bankovní server umístěný v klimatizovaných chráněných prostorách a odvézt jej na specializované pracoviště. Podobně není možné ani podobným způsobem přenést data ze záložních nebo archivních médiích do laboratorního prostředí a tam s nimi pracovat. Limitujícím faktorem bývá především velikost datového objemu a výkonnost „laboratorního" počítače. Ani velké instituce nemívají (především) z ekonomických důvodů testovací prostředí stejně dimenzované jako prostředí produkční. V takovém to případě je postup zajišťování a zkoumání digitálních stop zcela odlišný od jednoduchého zajištění doličného předmětu a jeho předání specializovanému pracovišti. Druhý případ vyžaduje mnohem komplexnější přístup a již v první linii zajišťování digitálních stop musí být vysoce kvalifikovaní ICT specialisté. Ve druhém případě je rozhodující i čas, který na rozdíl od prvního případu hraje proti vyšetřujícímu týmu.

2.11 Velký geografický rozsah prostoru s digitálními stopami

Vyšetřování je ale vždy založena na zákonech platných v dané zemi. Při forenzním šetření tak do celého procesu vstupují další aspekty, komplikující zajišťování digitálních stop na geograficky vzdálených místech, s rozdílně platnou legislativou V některých krajních případech nemusí v určité zemi být činnost trestná. Tyto

bariéry je nutné dokázat překonat, zpravidla cestou mezinárodních specialistů schopných zajistit digitální stopy a shromáždit přijatelné důkazy. K tomuto účelu se specialisté sdružují do mezinárodních virtuálních týmů. Vyšetřování bývá časově velmi náročné, v některých případech může trvat i několik let a svým charakterem připomíná odhalování dobře utajené špionážní sítě než pátrání po jednoduché formě trestné činnosti. Situace je tím komplikovanější, čím více pachatelů sdružuje své úsilí. Typické jsou hackerské skupiny, které dokonce v určitých časových obdobích útočí na cíl společně s dalšími skupinami, takže dochází i ke kumulaci digitálních stop, jež směřují k několika na sobě nezávislých trestným činnostem, které kromě zájmového objektu nemají nic společného. Místo trestného činu determinované způsobem jeho spáchání s využitím informačních a komunikačních technologií a s ním zajišťování digitálních stop nabývá v pojetí kriminalistiky zcela nového pojmu a rozměru oproti klasickému místu trestního činu. Místo trestného činu u informačních a komunikačních technologií nelze v některých případech geograficky omezit triviálním způsobem na plošně malé teritórium, byť digitální stopy jsou svým fyzickým rozměrem limitovány na nevelký prostor technologického charakteru (paměťový čip, datový disk atd.). Místo trestného činu může mít i dokonce virtuální charakter, protože určité typy aplikací používají distribuované zpracování na několika fyzicky vzdálených serverech z nejrůznějších důvodů.

2.12 Vysoký stupeň ochrany dat znesnadňuje nebo znemožňuje práci s digitálními stopami

Vyšetřování může mít z výše uvedených důvodů různé formy. V některých případech je složité, nebo nemožné pokračovat ve vyšetřování (pachatelé zpravidla dobrovolně nesdělují své technologické know-how a záměrně využívají nejmodernější technologie, které nemusí být přístupné ani státnímu aparátu), v jiných případech poškozený subjekt může za určitých okolností vyšetřujícímu orgánu poskytnou nezbytné znalosti a technologické prostředky (poškozený podnik, který má kryptograficky zabezpečenou databázi, ve které došlo k transakci defraudačního charakteru, v rámci snahy odhalit pachatele, zpřístupní veškeré informace a přidělí nejvyšší systémová oprávnění).

Základním principem v případě zajištěné kódovaných, šifrovaných dat je jejich zajištění, tj. izolace, aby nebylo možné nikomu z původních uživatelů k nim přistupovat a jejich co nejrychlejší předání forenzním specialistům, kteří se zaměřují na dešifrování elektronicky uložených dat.

2.13 Digitální stopa je specializovanými prostředky automaticky identifikovatelná a zpracovatelná

Jestliže např. známe hledanou strukturu nebo např. textový (či jiný) obsah předpokládané digitální stopy, můžeme ji pomocí specializovaného SW průběžně nebo dodatečně vyhledávat na základě určité sekvence znaků, které se vyskytují během přenosu, zpracování nebo uložení dat. Na tomto principu pracuje jakýkoliv software, včetně forenzního. Takto můžeme vyhledávat např. v počítači datové soubory, obsahující klíčová slova, čísla nebo sekvence znaků, charakteristické pro rodná čísla, platební karty, soubory vytvořené SW konkrétního výrobce apod. Spouštění vyhledávání může být nastaveno na manuální nebo automatický režim. V automatickém režimu pracují např. antivirové softwary. Každý virus má svou specifickou sekvenci znaků která jej identifikuje, Jakmile se soubor s tímto virem objeví na vstupu do výpočetního systému, je detekován (a „zneškodněn“). Jeho výskyt můžeme rovněž chápat jako digitální stopu, zanechanou škodlivým SW. Podobně pracují antispamové filtry při vstupu elektronické pošty. Jiným příkladem mohou být úzce specializované SW, monitorující elektronickou komunikaci a vyhledávající zájmové informace podle jejich obsahu. Zejména pro zpravodajské účely se využívají tzv. tematické filtry, které z obrovského množství v komunikačním prostoru tekoucích informací selektují jen ty, jež jsou předmětem zájmu. Podobné vyhledávání se využívá ve forenzních aplikacích při analýze např. pracovních stanic uživatelů s tím rozdílem, že vyšetřovatel nebo expert musí primárně definovat základní informace nebo jejich dílčí prvky, které hledá, aby pak bylo možné automaticky prohledat velmi objemný datový prostor.

2.14 Vysoká úroveň zahlazování digitálních stop kvalifikovanými pachateli

Při cílených útocích na předmět svého zájmu kvalifikovaní pachatelé (obvykle z řad počítačových specialistů), velmi dobře znalí prostředí výpočetní a komunikační techniky, zcela účelově zahlazují stopy. Je-li útok veden po počítačových sítích, k cílovému počítači pachatelé přistupují prostřednictvím jiných počítačů. Navíc účinně skrývají svou pravou identitu.

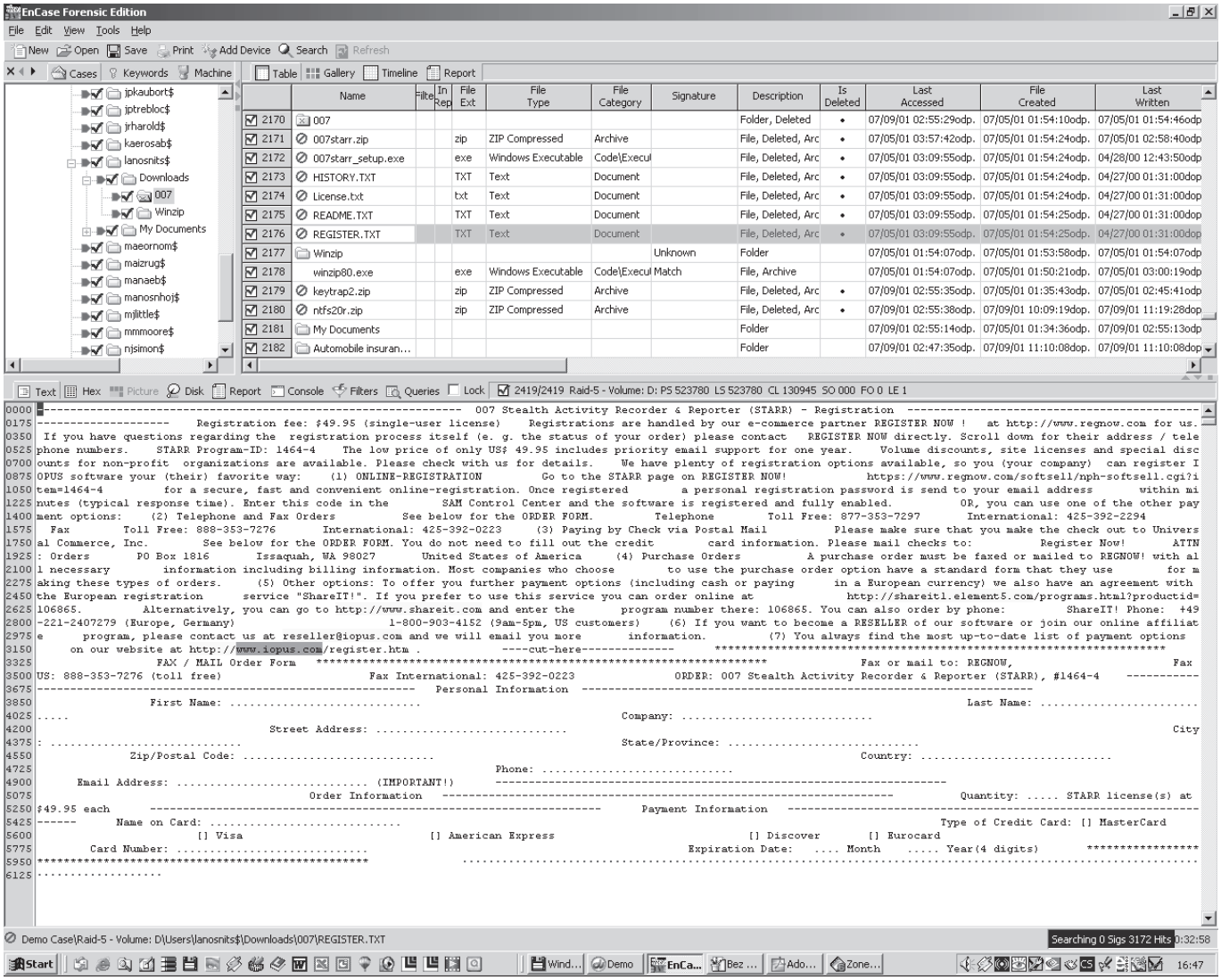
Vyšetřování bývá velmi zdlouhavé, vyžaduje rozsáhlé týmy expertů a mezinárodní součinnost. Významnou roli hrají vysoké odborné znalosti, jednotný způsob zajišťování digitálních stop v různých zemích, komunikace a týmová spolupráce.

2.15 Restaurovatelnost zničených digitálních stop

K restaurování digitálních stop využívají forenzní specialisté standardní systémové prostředky, úzce zaměřený SW výrobců třetích stran, které je vhodně doplňují nebo vysoce specializovaný, integrovaný SW vytvořený pro potřeby forenzní praxe (zde je kladen důraz na forenzní požadavky, jako je např. korektní dokumentace prostředí před zahájením šetření, nalezených poznatků apod.). Software bývá zpravidla psán pro specifické prostředí operačních systémů – Windows, Macintosh, Unix, Linux atd. Jako zástupce SW např. jmenujme EnCase, Forensic Toolkit (FTK), The Sleuth Kit, Foremost, Lazarus, Autopsy Forensic Browser, Regmon, Filemon, Regsnap, Tripwire, Easy-Recovery Pro, DataLifter a další.

2.16 Originálnost digitálních stop

Základní zásadou při forenzní práci s digitální stopou je zajištění originálního datového média, např. pevného disku počítače. Na toto médium není přípustné instalovat jakékoliv programy, měnit data apod. Data, tedy i digitální stopy, musí zůstat ve své původní podobě. Tento požadavek je realizovatelný bohužel většinou pouze v případě, že s médiem pracuje jedna nebo několik málo osob (případ PC, notebooků, PDA apod.) a zařízení je možné pro forenzní šetření odstavit a zajistit.



Obr. 3 Forenzní SW EnCase při vyhledávání podle klíčových slov nalezl smazanou složku se soubory prokazujícími objednávku prostřednictvím Internetu.

Tento požadavek se ale velmi těžko realizuje v prostředí výkonných serverů, databází s mnoha tisíci uživateli atd., kde odstávka je z ekonomických důvodů nemyslitelná. Tady se z důvodu bezpečnosti uplatňují jiné mechanismy – žurnálování transakcí, archivace záznamů apod. Mechanismy musí být navrženy jako součást implementace řešení a vyšetřující orgány jej používají pouze dodatečně, a to jen v případě, že výše uvedené mechanismy byly prakticky realizovány. Vyšetřovatel pak v praxi naráží na subjektivní faktory, které ovlivňují kvalitu digitálních stop.

2.17 Současně nízká úroveň soudní akceptace digitálních stop v právní praxi

Digitální stopy v roli důkazů nejsou soudy vždy akceptovány. Chybí širší povědomí o jejich možnostech, vlastnostech, spolehlivosti, průkaznosti a tedy následně o jejich praktickém využití. Není dosud rozpracována jednotná metodika pro vyhledávání, zajišťování, analýzu a dokumentaci digitálních stop. V národním i mezinárodním měřítku, byť se na těchto postupech intenzivně pracuje.

Otevřenými otázkami zůstávají rovněž příprava forenzních specialistů, jejich certifikace, stejně jako otázky zajištění standardizovaných a certifikovaných HW a SW prostředků, financování. Problematická zůstává i spolupráce státních i privátních organizací na poli digitálních stop. Absence jednotných metodik a standardů znesnadňují efektivní výměnu digitálních stop mezi různými orgány a expertními týmy forenzních pracovišť.

Řada bezpečnostních incidentů informačního charakteru, které proběhnou v privátní sféře, v prostředí rozmanitých institucí, se do fáze vyšetřování státními institucemi vůbec nedostanou. Komerčním institucím, kde došlo k interním bezpečnostním incidentům, v konkurenčním prostředí, zveřejněním jakýchkoliv citlivých informací hrozí ztráta důvěry zákazníků (banky, pojišťovny, telekomunikační společnosti apod.). Vyšetřování probíhá interními silami nebo za pomoci specializovaných externích privátních bezpečnostních nebo auditorských firem. Chybí pak následně i odborná publicita, sdílení příčin, způsobů řešení kritických situací, předávání znalostí a zkušeností. Ve zcela výjimečných případech je vyšetřování předáváno státním institucím.

Pokud k tomu dochází, tak s poměrně velkým časovým zpožděním. Bez vzájemně akceptovaných standardů je problematické ověřování věrohodnosti zajištěných a dále předávaných digitálních stop mezi různými expertními pracovišti a orgány.

Ve forenzní praxi převládají především pouze zkušenosti z expertizy HW a SW prostředků pro osobní využití (PC, notebooky, PDA, mobilní telefony, elektronické diáře, paměťová média personálního charakteru, záznamová zařízení (video, digitální fotografie) atd.). Oblast velkých institucionálních informačních systémů není zatím nijak hluboce pokryta znalostmi a zkušenostmi pro šetření v heterogenním a komplexním technologickém prostředí státními orgány.

3. ZÁVĚR

Vlastnosti digitálních stop předurčují dále všechny postupy a metody, které je nezbytné soustavně aplikovat při vyhledávání, zajišťování, dokumentace a analýze digitálních stop. Uvědomíme-li si vlastnosti digitálních stop, dokážeme nejenom efektivně vést forenzní vyšetřování v oblasti informačních a komunikačních technologií, ale i realizovat velmi účinnou prevenci nebo v reálném prostředí ICT nastavit takové podmínky, že následující forenzní činnost splní veškerá naše profesní očekávání.

4. LITERATURA

[1] Digital Evidence: Standards and Principles. *Report of Scientific Working Group on Digital Evidence (SWGDE) and International Organization on Digital Evidence (IOCE).* http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm

[2] WHITCOMB C. M.: An Historical Perspective of Digital Evidence: A Forensic Scientist's View. In: *International Journal of Digital Evidence, Spring 2002 Volume 1, Issue 1.*

[3] MATOUSKOVA I., RAK R.: The role of the safety manager when enforcing comprehensive information security. *5th International Conference Information Security Summit, 2004, pp. 85–98, Tate International.* ISBN 80-86813-00-2

[4] RAK R.: Digital evidence I. In: *Security Magazin, No 1, 2005, pp. 55–59.* ISSN 1210-8723

[5] RAK R.: Digital evidence II. In: *Security Magazin, No 2, 2005, pp. 34–39.* ISSN 1210-8723