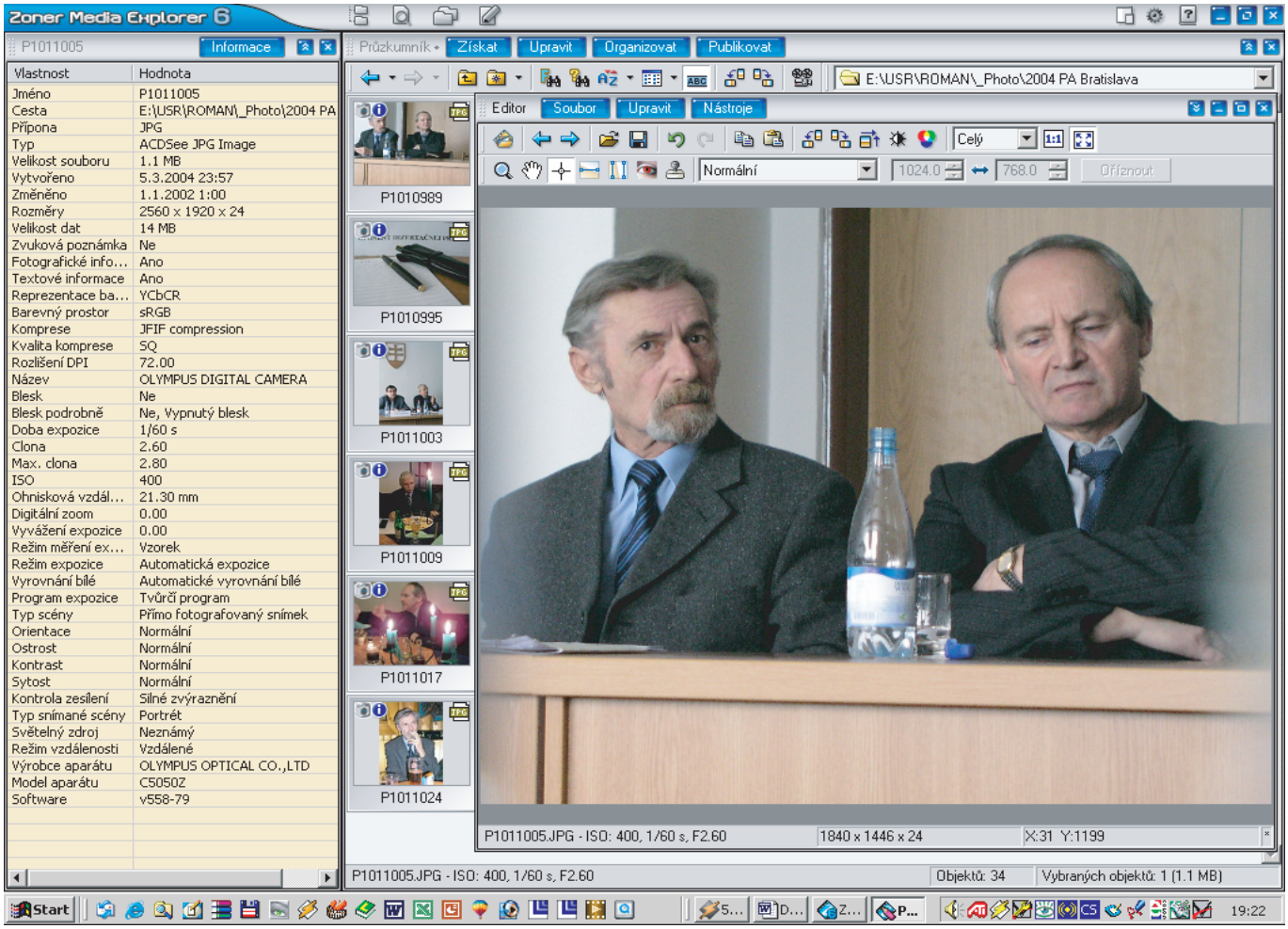
Doc. Ing. Roman Rak, Ph.D
Prof. JUDr. Ing. Viktor Porada, DrSc., dr.h.c

Policejní akademie ČR Praha

DIGITÁLNÍ STOPY V KRIMINALISTICE A FORENZNÍCH VĚDÁCH

Pojem počítačová kriminalita vznikl již v době sálových a prvních PC. Od té doby ale tato oblast prošla bouřlivým rozvojem a další trendy rovněž předpokládají pokračující vývoj. Kromě sálových a personálních počítačů jsou běžnou realitou i jiné technologické prostředky, které spojují nebo vhodně doplňují výpočetní možnosti s komunikací v nejrůznějších podobách. Jejich společnou platformou je digitalizace téměř všeho, co nás obklopuje.

Denně jsou používány mobilní telefony, bezdrátové přenosy dat z našich personálních elektronických zařízeních (WiFi[1], Bluetooth), elektronické diáře, handheldery (osobní počítače do dlaně velikosti krabičky od cigaret), audio digitální záznamníkové přístroje, digitální videokamery a fotoaparáty, video a DVD[2] přehrávače nebo rekordery, platební a identifikační karty, nejrůznější záznamová média (CD[3], DVD, USB[4] paměti, digitální paměti videokamer a otoaparátů, optická média apod.), bohaté příslušenství rozmanitých druhů periférií ke všem těmto výše uvedeným zařízením. Součástí mnoha dalších technologií jsou vestavěné, jedno nebo víceúčelové procesory, zajišťující činnost daného zařízení – palubní počítače automobilů, letadel, lodí; rozmanitá zabezpečovací a monitorovací zařízení, elektronická identifikace objektů, zboží atd.



Obr. 1 *Datové soubory často obsahují kromě primárního obsahu (textu, fotografie, zvuku, videa atd.) i tzv.* ***metadata****, která charakterizují další informace o souboru, v našem případě o snímku. Lze pak např. určit, kdy byl snímek pořízen, za jakých světelných podmínek, s jakým nastavením a typu fotoaparátu apod. (levá část printscreenu) Tyto informace, nalezené v počítači, který nějakým způsobem souvisí s trestným činem, mohou přinést podstatné informace pro vyšetřování.*

1 WiFi – Wireless Fidelity. Standard pro bezdrátový přenos rychlostí až 11 MB/s v pásmu 2,4 GHz.

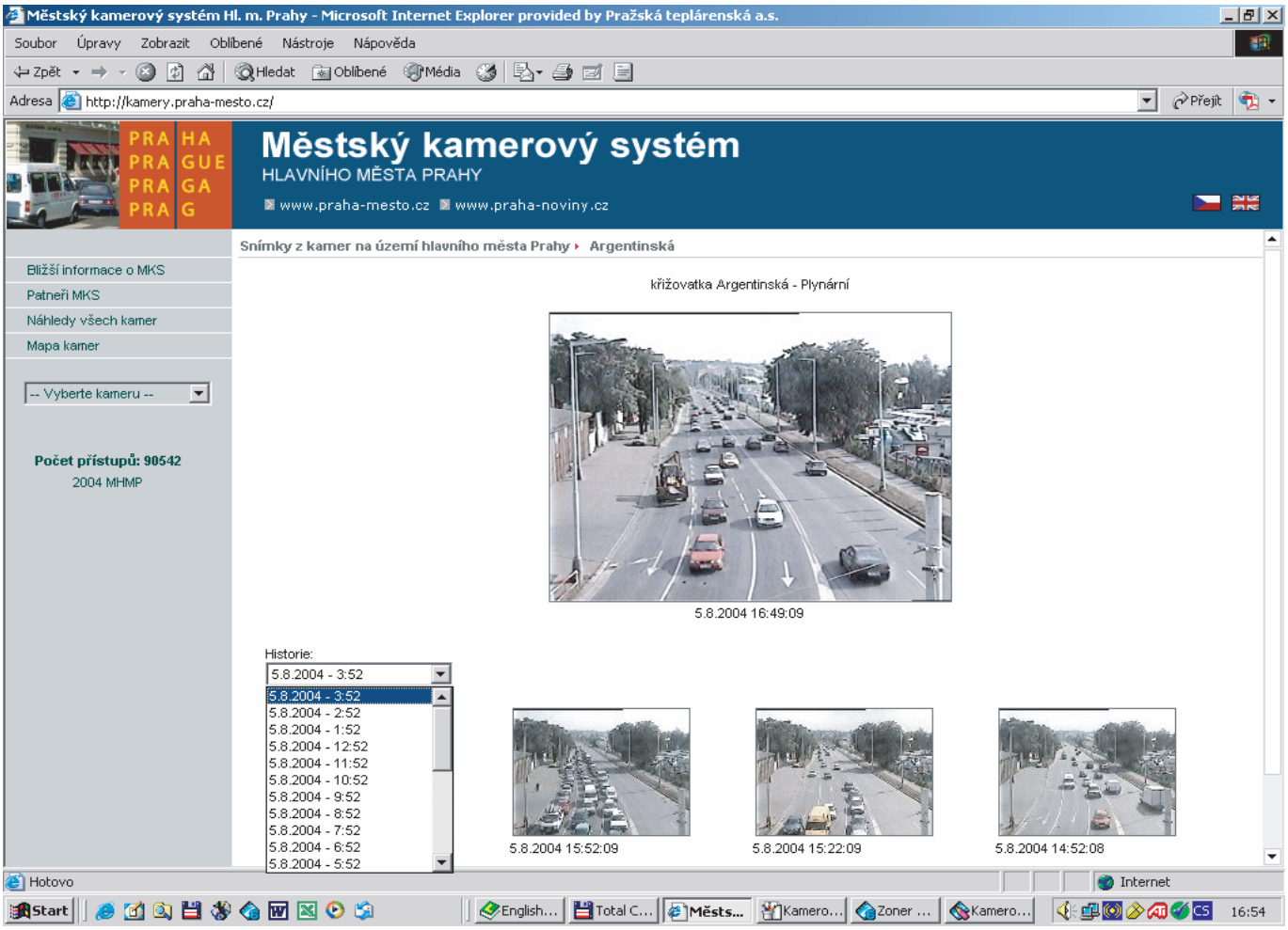
2 DVD – Digital Versatil Disc, Digital Video Disc.

3 CD – Compact Disc.

4 USB – Universal Serial Bus.

Všechna tato zařízení z kriminalistického a forenzního pohledu zanechávají prokazatelné stopy své činnosti, které mají své obecné i individuální zákonitosti a které jsou prakticky využitelné. Je rovněž zřejmé, že pojem „počítačová“ kriminalita má dnes mnohem širší význam, než v minulosti. Počítačová kriminalita byla v minulosti správně logicky chápána ve vztahu pouze s počítači. Nic jiného tehdy neexistovalo. Kam ale zařadit dnešní trestnou činnost spojenou např. s platebními nebo identifikačními kartami, obsahujícími magnetické nosiče dat, pozměňování nechráněných dat během jejich bezdrátového přenosu apod.? Celá řada technologických zařízení, i když nejsou prostředkem nebo cílem trestného činu, obsahují velké množství rozmanitých dat, které v průběhu vyšetřování jiného trestného činu, přestupku či zcela jiné aktivity v první fázi mají klasický charakter kriminalistické stopy a v konečné etapě v ideálním případě pak charakter soudního důkazu. Pomocí všech těchto stop je pak možné prověřovat vyšetřovací verze případu, sbírat důkazy proti pachateli nebo naopak potvrzovat alibi nevinných osob. Stopy se v procesu soudní obhajoby stávají přímými či nepřímými důkazy. Na datovém médiu mohou být záznamy o činnosti uživatele na počítači, v mobilním telefon seznam posledních hovorů oběti trestného činu, na videozáznamu dohledového centra obchodního domu či banky zákazníci v inkriminované době, v palubním počítači automobilu identifikační čísla (VIN[5]), které pachatel zapomněl při mechanické falzifikaci ostatních čísel na vozu změnit nebo to nevěděl, či neuměl; v telefonní centrále výpis všech uskutečněných hovorů, v systémech GPS[6] souřadnice objektu (např. automobilu) v konkrétním čase atd.

Důležitým zdrojem stop mohou být i webkamery, které snímají v reálném čase určitou zájmovou oblast. Živé záběry je možné prohlížet prostřednictvím Internetu z druhého konce zeměkoule. Tyto kamery je dokonce možné ovládat vzdáleně z našeho počítače. Provozovateli kamerových monitorovacích systémů jsou státní i nestátní instituce, soukromé osoby. Kamery snímají nejrůznější objekty a scény, průběžně zachycují prostory křižovatek, obchodních domů, přepážek bank, peněžních automatů, čerpacích stanic, hraničních přechodů, technologických nebo servisních (obslužných i bezobslužných) prostorů, turisticky zajímavých objektů, hotelových vestibulů atd. Důležité je, že mnoho aplikací, pracujících s (web)kamerami, archivují pořízené záběry spolu



Obr. 2 Digitální záznamy pořízené webkamerou, zobrazující reálný pohled na dopravní situaci v konkrétním místě, které jsou navíc ukládány do archivu a označovány časovou známkou.

5 VIN – Vehicle Identification System.

6 GPS – Global Position System.

s časem a místem pořízení. Obrazové snímky či jejich sekvence mohou tak vystupovat i v podobě stop, důkazního materiálu a hrát důležitou roli při vyšetřování zcela běžných trestných činů. Jestliže dříve se na místě trestného činu vyslýchali svědci a byla snaha co nejlépe popsat danou situaci, prostor v inkriminovanou dobu (a popisy byly velice subjektivní a často záleželo na představě vyšetřujícího orgánu). Dnes navíc můžeme (musíme) vyhodnocovat, zda prostor nebyl monitorován technologickými prostředky s digitálními výstupy, které mohou posloužit jako stopy, základní vodítko pro vyšetřování a následně i jako důkazní materiál s daleko větší vypovídací schopností (podstatně větším objemem objektivních informací), než subjektivní popisy svědků, které se mohou i diametrálně od sebe odlišovat.

DEFINICE DIGITÁLNÍ STOPY

Každé technologické zařízení, které získává, zpracovává, předává nebo uchovává data zanechává záznamy (odrazy) o své činnosti. Tyto záznamy z kriminalistického hlediska jsou stopami. Podle klasické teorie odrazu [13], [14] člověk (nebo jiný objekt či subjekt) ovládá (spouští, modifikuje apod.) SW vybavení, popř. jeho nastavení nebo ovládá jiným způsobem elektronické technologie. Tyto činnosti či změny se následně odrážejí do materiálního prostředí směrem dovnitř i ven dané technologie.

Ve smyslu výše definované počítačové nebo kybernetické kriminality nebo kriminality počítačově či kyberneticky související pojem zařízení pracujícími s daty je mnohem širší než pouhý počítač. V některých pracích renomovaných českých či slovenských autorů se setkáváme s pojmem počítačová stopa, který je spíše intuitivně používán než věcně definován. Pojem počítačová stopa vznikl ve stejném časovém období jako pojem počítačová kriminalita, tedy přibližně ve druhé polovině 80. let minulého století. Je zřejmé, že s pojmem „počítačová“ (stopa) dnes již nevystačíme, protože i jiná, elektronická zařízení zanechávají stopy, které mají stejnou podstatu, charakter, obecné nebo individuální vlastnosti jako stopa počítačová.

V zahraniční literatuře existuje několik velmi podobných definic, vymezujících již běžně vžitý termín **digitální stopa (***digital evidence***)**. Nutno podotknout, že slovo „evidence“ má

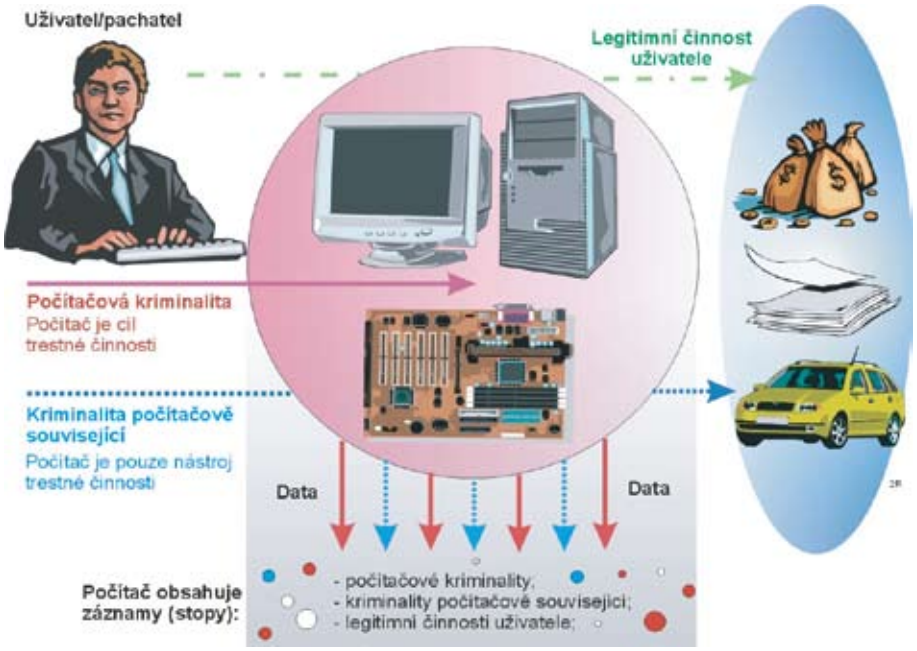
v angličtině primární význam „důkaz“. České slovo „stopa“ v souvislosti s moderními technologiemi v zahraniční literatuře nenalezneme (můžeme se setkat s významem *potential digital evidence*, který má blízký smysl českému pojmu „stopa“). Příčina je jednoduchá a pragmaticky založená – zahraniční teorie i praxe jsou silně orientovány na výsledek trestního procesu, tj. stopa musí být soudem akceptovatelná a proto ve vnímání a následném používání termínů dochází k automatickému ztotožňování pojmů stopa a důkaz (angl. *evidence*).

Při využití počítače k padělání úřední listiny je použit legálně zakoupený SW na skenování a následně pro grafické úpravy (např. programy Nero a Photoshop). Aplikace i počítač fungují zcela standardně. Jediným důkazem je datový soubor s hotovým padělkem uložený v počítači a záznamy, že byl zpracován daným programovým vybavením, v určitém čase, určitou osobou apod. K žádnému narušení funkcionality nebo bezpečnostních opatřeních ale nedošlo.

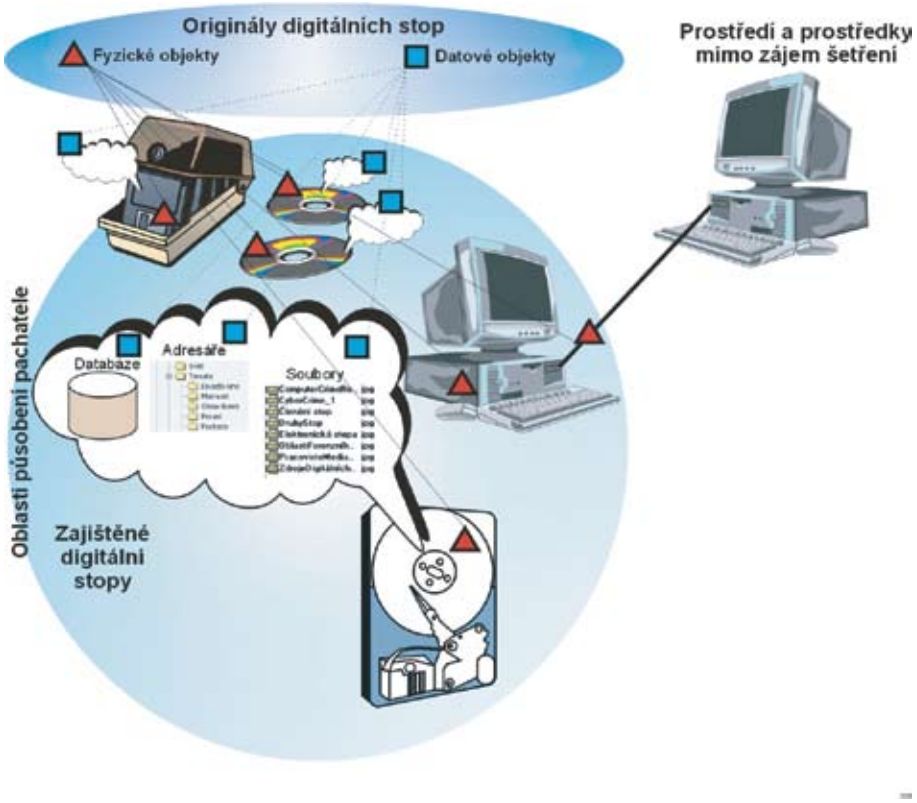
Dnes v zahraniční literatuře nejčastěji používaná, a nechá se říci i nejširším okruhem specialistů akceptovatelná definice byla navržena již v roce 1999 pracovní skupinou *SWGDE – Scientific Working Group on Digital Evidence*[7] [21], [22]:

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

Tato definice je otevřená jakékoliv digitální technologii. Tímto způsobem definovaná digitální stopa pokrývá jak oblast počítačů



Obr. 3 ***Grafické znázornění rozdílu mezi počítačovou kriminalitou a kriminalitou počítačově související. V první kategorii počítač vystupuje jako cíl, ve druhé jako nástroj trestné činnosti nebo jen zdroj relevantních informací ve vztahu k trestnému činu. Počítač je pak zdrojem informací o trestné činnosti pachatele i o legitimní činnosti uživatele.***



Obr. 4 *Grafické znázornění definic základních pojmů – část I. Ve známých oblastech působnosti pachatele jsou zajištěny fyzické objekty (zařízení, datová média) s uloženými datovými objekty, obsahujícími digitální stopy.*

a počítačové komunikace, tak i oblast digitálních přenosů (mobilní telefony, ale do budoucna i digitální TV apod.), videa, audia, digitální fotografie, data kamerových (CCTV) systémů, data elektronických zabezpečovacích systémů, a jakýchkoliv dalších technologií potenciálně spojených s Hi-Tech kriminalitou. V původním návrhu se hovořilo o binární podobě uložené nebo přenášené informace. Slovo binární bylo následně změněno na digitální, protože tento pojem je obecnější (binární forma je podmnožinou obecnější digitální formy). Na rozdíl od jiných definic je definice navíc obecná i v tom smyslu, že digitální stopu nespojuje nutně s trestným činem, což , jak uvidíme dále, je velmi důležité. Digitální stopa musí být využitelná nejenom pro silové resorty, kriminalistiku, ale i pro obecné forenzní šetření prováděné státními orgány (občansko-právní spory, obchodní zákony apod.), tak i na komerční bázi, pro potřeby nezávislých interních či externích auditů apod.

International Organization of Computer Evidence (IOCE) definovalo původně digitální stopu jako jakoukoliv informaci, uloženou nebo přenášenou v binární formě, která může být předložena soudu jako věcný důkaz. Slovo binární versus digitální jsme již diskutovali. V této definici je kladen důraz na předkládání důkazů soudu. V praxi, např. při forenzním šetřením na komerční bázi (konzultantskou, forenzní nebo jinou firmou či fyzickou osobou) ale žádný výstup směrem k soudu nemusí být, výsledek studie je předložen managementu nebo akcionářům společnosti. Pojem digitální stopa, jako jakákoliv jiná stopa, by proto měl být orientován jen a jen na korektní průběh vyšetřování a ve svém důsledku standardizovat pracovní postupy, pojmy a prvky kvality pro jakýkoliv vyšetřující orgán a zaručovat přenositelnost stop (důkazů), vyšetřovacích metod mezi různými účastníky šetření, tj. mezi státními orgány i nezávislými expertními institucemi a subjekty.

V jiných návrzích [2] byla digitální stopa definována jako data[8], charakterizující (dokazující) spáchání trestného činu, nebo ustanovující vztah mezi spáchaným trestným činem a jeho obětí nebo trestním činem a pachatelem. I zde byla snaha stopu spojovat definici pouze se spáchaným trestným činem. V první definici, pod digitální stopou rozumíme i výsledek legitimní činnosti uživatele,

7 Skupina SWGDE byla založena z iniciativy FBI v roce 1998. Prvních jednání pracovní skupiny se účastnili zástupci Bureau of Alcohol, Tobacco and Firearms (ATF), U.S. Customs, the Drug Enforcement Administration (DEA), FBI, Immigration and Naturalization Service (INS), Internal Revenue Service (IRS), National Aeronautics and Space Administration (NASA), U.S. Secret Service (USSS) a U.S. Postal Inspection Service. Postupně docházelo ke slaďování projektu s International Organization on Computer Evidence (IOCE) a Interpolem.

8 Data versus informace. Z hlediska teorie je zásadní rozdíl mezi pojmy data a informace. Definic existuje mnoho. Každý vědní obor se na tyto pojmy dívá nepatrně jinak. Pro potřeby forenzních věd se nejlépe hodí matematický přístup, pracující s pojmem entropie. Data – jsou zprávy, výroky (i výstupy z různých měřičů, SW aplikací apod.), které mohou (ale nemusí) snižovat neznalost daného jevu (neurčitost, entropii). Informace – jsou data, která snižují tuto neurčitost. Z uvedeného vyplývá, že informace jsou podmnožinou dat. Data sami o sobě jsou nehmotné, ale pro jejich uložení potřebujeme hmotné médium. Z hlediska forenzní praxe tedy informace přinášejí nové poznatky, které upřesňují příčiny, průběh nebo důsledky určité aktivity (trestného činu).

která je jakýmkoliv způsobem relevantní obecnému šetření, kterým může být i např. hloubkový finanční audit, jdoucí až do úrovně IS technologie. Definice [3] je nekorektně jen zúžena a orientována na trestný čin, což nemusí být vždy pravda.

V souvislosti s digitálními stopami bývají definovány další související procesy a entity, které jsou logicky spojeny s digitálními stopami a tvoří homogenní celek. Ten je velmi významný pro celý další proces práce s digitálními stopami. Jsou to pojmy:

- zajištění digitálních stop,
- datové objekty,
- fyzické objekty,
- originály digitální stopy,
- duplikát digitální stopy,
- kopie digitální stopy.

Tyto pojmy jsou dále definovány následujícím způsobem:

Zajištění digitálních stop je proces, který začíná okamžikem, kdy informace a/nebo zařízení jsou zajištěna nebo uložena pro expertizní zkoumání. Předpokládá se, že digitální stopa bude před soudními orgány akceptována jako důkaz. Dále se předpokládá, že proces zajištění je přiměřený a legální pro práci s důkazním materiálem v dané geografické lokalitě (zemi). Fyzické a datové objekty se stávají důkazy teprve tehdy, jsou-li akceptovatelné orgány činnými v trestním řízení.

Datové objekty. Objekty nebo informace s věrohodnou vypovídající hodnotou, jež jsou asociovány s fyzickými prvky. Datové objekty mohou mít různé formáty, ale nikdy nesmí změnit původní informaci.

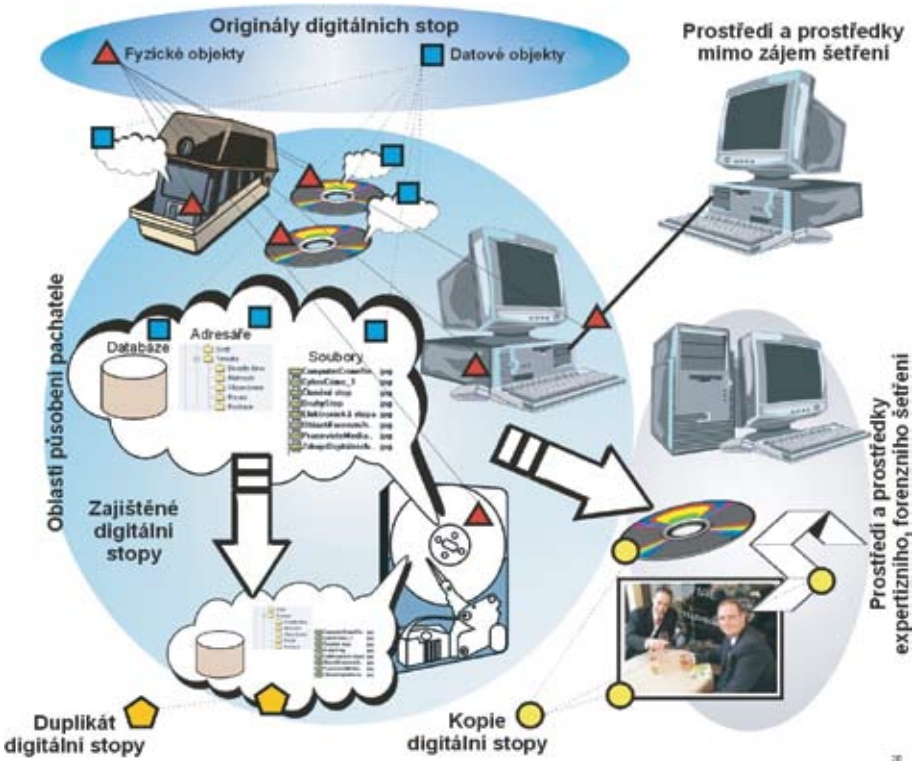
Datovými objekty jsou např. databáze, adresáře, soubory, informační obsahy virtuálních pamětí, digitální video nebo audio nahrávky apod.

Fyzické objekty. Prvky na kterých jsou uloženy datové objekty a/nebo přes které jsou tyto přenášeny.

Fyzickými objekty rozumíme technologické části, zařízení, určené ke zpracování, uložení nebo k přenosu dat. V praxi to jsou pevné disky počítačů, různá paměťová média (diskety, CD a DVD disky, paměťové karty, datové pásky atd.). V širším smyslu slova to jsou celá zařízení (např. počítače, tiskárny, síťové prvky apod.), obsahující kromě digitálních stop i další informace, jako jsou výrobní čísla, daktyloskopické nebo mechanické či biologické stopy a další, které dokazují logický vztah fyzického zařízení (vlastnický, uživatelský, časový …), jeho uživatele (pachatele) a trestného činu nebo jiné aktivity, které jsou předmětem zájmu vyšetřování (zkoumání, šetření, interního nebo externího auditu). Fyzické objekty bývají často předmětem obecně širšího kriminalistického zájmu, než jen zkoumání digitálních stop. Podle potřeby jsou využívány všechny běžné metody kriminalistického zkoumání.

Originály digitální stopy. Fyzické a datové objekty, které jsou zajištěny pro potřeby expertizního, forenzního zkoumání.

Originály digitálních stop jsou základním důkazním materiálem. Pro pracovní účely uživatele (pachatele) nebo vyšetřující orgány se z nich vytvářejí pracovní duplikáty nebo kopie digitálních stop. Proces jejich vytvoření je jednoznačný a nedochází k žádné změně informačního obsahu. Tento proces při splnění základních podmínek je vždy opakovatelný se stejnými výsledky.



Obr. 5 Grafické znázornění definic základních pojmů – část II. Pro potřeby vyšetřování jsou zajištěny originály digitálních stop. Zároveň je vytvořeno/použito speciální prostředí s odpovídajícími prostředky pro vyšetřování. Při vyšetřování kromě původních originálů datových stop se pracuje s jejich kopiemi. Ty nemusí být vždy nutně v digitální podobě. Informace, digitální stopy, v podobě různých datových objektů mohou být vytištěny na papír, zhotoveny z nich klasické fotografie atd.

Uživatelé i nezávislí experti mají pak k dispozici získaný nebo jimi vytvořený výchozí materiál k dalšímu zkoumání se stejnou informační hodnotou. Tak je garantována neměnnost originálů digitální stopy jako důkazního materiálu.

Duplikát digitální stopy. Přesná digitální reprodukce všech datových objektů obsažených na originálním fyzickém objektu na fyzicky stejný typ datového média.

Duplikát digitální stopy vzniká vždy kopírováním **všech** datových objektů daného fyzického objektu na jiné fyzické médium stejného typu.

S duplikáty digitální stopy se poměrně dobře pracuje zejména ve složitém digitálním prostředí počítačů či jiných digitálních zařízení, kde jsou nejrůznější vazby nebo interfacy mezi jednotlivými datovými objekty. Protože při duplikátu se vytváří reprodukce všech datových objektů, zachovávají se vzájemné logické i fyzické vazby. S duplikátem lze pohodlně, bezpečně a plnohodnotně pracovat. Nevýhodou může být až gigantický objem informací uložených na duplikátu. Objem dat a informační obsah všech datových objektů jsou v poměru 1:1 mezi originálem a duplikátem.

Duplikáty digitálních stop vytváříme zejména pro potřeby důkazního šetření, abychom mohli předložit původní materiál k opětovnému přešetření jiným, nezávislým znalcem v těch případech, kdy samotný fyzický objekt (např. podnikový počítač) nelze z různých důvodů přímo zajistit pro potřeby práce orgánů činných ve vyšetřování. V praxi v oblasti personálních počítačů se běžně používají tzv. *image disků*, což je věrný duplikát jeho obsahu, tedy jakési zrcadlo jeho původního obsahu uložené v digitální podobě.

Kopie digitální stopy. Přesná reprodukce informace z původního fyzického objektu na jiné, fyzicky nezávislé datové médium.

Při vytváření kopie digitální stopy vytváříme datové objekty se stejným informačním obsahem, ale na fyzické médium, které může být odlišného typu.

Při procesu vytvoření kopie nemusí být nezbytně nutně reprodukovány všechny datové objekty původního fyzického objektu, ale vybrány jen některé z nich, které jsou podstatné a tedy nezbytné pro další vyšetřování. Příkladem může být zkopírování jediné digitální fotografie z paměťové karty digitálního fotoaparátu, kde je uloženo podstatně více fotografií a její následný detailní rozbor. V případě počítačových systémů nebo digitálních zařízení sice kopírujeme jednotlivé datové objekty, aniž bychom měnili jejich informační obsah, ale vytrháváme je ze širšího kontextu komplexního prostředí. V důsledku nemusí být zachovány všechny funkční a logické vazby s ostatními datovými objekty. Kopie vytváříme tehdy, je-li to pro účely vyšetřování účelné, např. z důvodu velikosti datového objemu digitálních stop. Kopie obsahují jen část datových objektů původního fyzického objektu. Informační hodnota každého kopírovaného objektu se od svého originálu ale nemění.

Pouhé kopie digitálních stop nemusí být dostatečným důkazem, protože jsme se při jejich výběru mohli mýlit, zajistit jenom určitou část atd. Z pohledu forenzního šetření je proto rozhodující mít k dispozici originály digitálních stop nebo jejich duplikáty. Pomocí nich lze následně transparentně prokázat oprávněnost a správnost zvoleného postupu vyšetřování a přípravy důkazního materiálu.

OBECNÝ VÝZNAM DEFINICE DIGITÁLNÍ STOPY

Pojem digitální datové stopy je nutné vždy chápat obecně, v širokém kontextu rozvíjejících se technologií. Pod digitálními stopami se nesmíme představovat jen odrazy činností softwaru a člověka do materiálního prostředí datových paměťových médií počítačů. Digitální stopy jsou dnes vytvářeny všemi technologiemi, které pracují na základě moderní elektroniky.

V různých forenzních laboratořích, světových policejních agenturách či ústavech historicky vznikly specializované audio a video laboratoře ještě dříve, než se začaly vytvářet analytická pracoviště, zaměřená na expertní zkoumání počítačů a s mimi spojenými periferiemi či technologiemi. Audio a video laboratoře provádějí klasickou analýzu zvuku a obrazu, ať už zaznamenaných analogovou nebo digitální technikou.

Současná světová expertizní praxe naráží na problémy určité rivality mezi všemi výše popsanými specializovanými oblastmi. Každá z oblastí má své opodstatnění, své historické momenty vzniku, svá určitá specifika a tedy své místo v kriminalistické i forenzní praxi. Žádná z nich není ale nijak výjimečná, prioritní proti ostatním zbývajícím.

Světové trendy globalizace a informačních společností silně stírají rozdíly mezi funkcionalitou jednotlivých digitálních zařízeních, jež stále častěji používají společné mezinárodní standardy pro výměnu a přenos dat.

Obrazový i zvukový záznam lze totiž dnes pořizovat a dále zpracovávat videokamerami či digitálními fotoaparáty přímo v těchto zařízeních nebo k nim vyráběným specializovaným nástavbám, tak i v počítačích či dalších zařízeních, které nejsou původně prodávány jako příslušenství k fotoaparátům nebo k videokamerám. Digitální fotoaparát dokáže zaznamenávat video, digitální snímky lze pořizovat mobilními telefonními přístroji a řenášet je do jiných telefonních přístrojů nebo počítačů. Mohutná je integrace s TV. Již nyní existují reálné projekty, kdy na miniaturní obrazovce svého mobilního telefonního přístroje můžeme sledovat libovolný zvolený kanál vysílací stanice nebo film z virtuální videopůjčovny, anebo jen obraz, scénu z našeho dětského pokoje a tím hlídat naše děti.

Zde všude vznikají digitální stopy, které se prolínají mezi nejrůznějšími digitálními zařízeními a dokáží vypovídat o průběhu mnoha činností s daleko větší přesností i obsahem, než jsme schopni dlouhodobě uchovat v naší lidské paměti.

Z tohoto pohledu i praktická forenzní činnost začíná vnímat integraci technologických objektů a expertizní činnost je chápána komplexně. Digitální záznamy (tedy stopy), jejich standardizované datové a komunikační formáty jsou tmelem, spojujícím dříve samostatně existující, úzce specializované laboratoře. Tato specializace vždy do určité míry zůstane zachována, ale je nutno přihlížet ke společné podstatě digitálních stop.

Proto pro všechna tato zařízení musí splňovat stejné nároky na obecnou práci s digitálními stopami – způsoby jejich vyhledávání, zajišťování, předávání, analýzy atd. Všechny procesy z hlediska nutnosti výměny informací mezi vyšetřujícími orgány v mezinárodním měřítku musí být standardizovány. Procesy musí mít rovněž zajištěnu garanci jejich kvality a transparentnosti.

DIGITÁLNÍ STOPA A JEJÍ MÍSTO V KLASICKÉ TEORII STOP

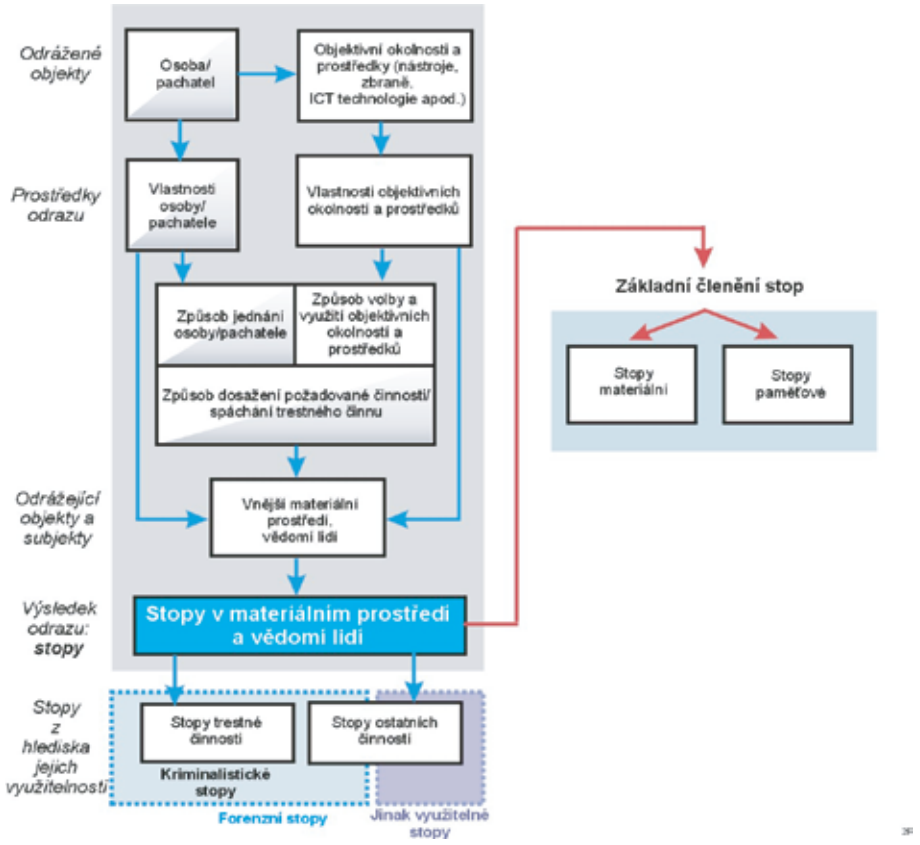
Podstatou kriminalistických stop je exaktně zjištěná skutečnost formulovaná v obecné filosofické teorii odrazu: *„Působí-li na sebe současně dva nebo více objektů, dochází ke vzájemnému předávání informací o jednotlivých objektech navzájem“*. Přitom je v podstatě lhostejné, jaký je charakter jednotlivých navzájem na sebe působících objektů [14, str.69]. Výsledkem vzájemného působení objektů a předávání informací je tzv. *odraz*, který je pak v praxi za předpokladu splnění následujících tří podmínek považován za stopu:

1. *Odraz (změna) musí být v souvislosti s kriminalisticky relevantní událostí, abychom hovořili o kriminalistické stopě*. Výpočetní technika, digitální zařízení zanechávají velké množství digitálních záznamů (obsahujících informace), tedy obecných digitálních stop, které precizně dokumentují aktivity technologického zařízení a jejich uživatelů. Digitální stopy můžeme proto považovat za obecnou množinu, relevantní ke všem typům událostí. O kriminalistických digitálních stopách v kriminalistickém pojetí hovoříme tedy jen v souvislosti s počítačovou nebo kybernetickou kriminalitou, nebo s kriminalitou počítačově či kyberneticky související. Ostatní části digitálních stop se vztahují k událostem relevantních k obecnějším forenzním šetřením – např. finanční audity jdoucí až do hloubky informačních systémů v instituci, technologické audity (porovnání projektových požadavků se skutečnými výsledky po implementaci IS), dodržování bezpečnostních pravidel (bezpečnostní audity) či interní legislativy – nebo k událostem obecně se vztahujících k legitimní činnosti uživatele.
2. *Odraz (změna) musí existovat alespoň od svého vzniku do zjištění*. Zmíněná podmínka je logická, protože neexistující změnu nelze využít. Důležitým aspektem je proto objektivní, nepopiratelná dokumentace digitálních stop.
3. *Odraz (změna) musí být vyhodnotitelný současnými metodami a prostředky*. Jedná se o podmínku, která se bezprostředně vztahuje ke znalecké činnosti spojené se zkoumáním (kriminalistických) stop. Pokud nelze získat z nalezených a zjištěných změn potřebné (kriminalisticky) relevantní informace, nemá taková změna prakticky upotřebitelný význam. Digitální stopy, jejich charakter vyplývající z podstaty bouřlivě se vyvíjejících technologií, vyžadují vysokou znaleckou odbornost v celém průběhu prací s nimi, tj. od jejich vyhledávání, dokumentaci až po analýzu a prezentaci výsledků.

V souvislosti s obecnou teorií stop, kde stopy jsou výsledkem odrazu, hovoříme o *odrážených objektech*, *prostředcích odrazu* a *odrážejících objektech a subjektech*.

Odrážený objekt – osoby a prostředky (nástroje, zbraně, technologie apod.), které působí nebo vyvolávají aktivity. V našem případě to jsou uživatelé výpočetní a digitální techniky a tato technika samotná.

Prostředek odrazu – vlastnosti odrážených objektů a objektivní okolnosti. U osob to jsou obecně jejich psychologické vlastnosti,



Obr. 6 Základní schéma vzniku a členění stop. Obrázek též znázorňuje vztah způsobů spáchání trestné činnosti k procesu odrazu stop trestného činu(upraveno podle Musil (1978, s.85)

znalosti a dovednosti, které se odrážejí výběrem softwaru nebo zařízení pro svou činnost, úrovní jeho ovládání či využití. Složitý, sofistikovaný SW či zařízení nabízejí vysokou variabilitu jejich využití. Odlišné výsledky při použití stejných nástrojů dosáhnou průměrní uživatelé a vysoce specializování specialisté. Objektivní okolností z pohledu práce běžného uživatele je např. úroveň administrace systému, která rozhoduje o tom, co je uživateli v systému dovoleno a co nikoliv.

Odrážející objekty a subjekty – vnější materiální prostředí a vědomí lidí, na které odrážené objekty za pomoci prostředků odrazu působí. Technologie (výpočetní, komunikační, digitální) v konečném důsledku působí na záznamové médium, na které se ukládají data. Kromě tohoto materiálního prostředí jsou stopy o aktivitách odraženy i ve vědomí lidí. Tyto stopy jsou nemateriálního charakteru a v teorii kriminalistických stop je obecně nazýváme paměťovými stopami. Pozor na možnou nežádoucí záměnu pojmu s paměťovými zařízeními technologického charakteru, které jsou vždy hmotné a nazýváme je proto paměťové médium! V souvislosti s digitálními stopami proto nikdy nehovoříme o paměťových stopách.

Odrazem v materiálním prostředí i ve vědomí lidí vznikají stopy jako důsledek objektivních okolností, aktivit lidí, jejich nástrojů či prostředků, majících své specifické vlastnosti.

KRIMINALISTICKÉ, FORENZNÍ A JINAK VYUŽITELNÉ DIGITÁLNÍ STOPY

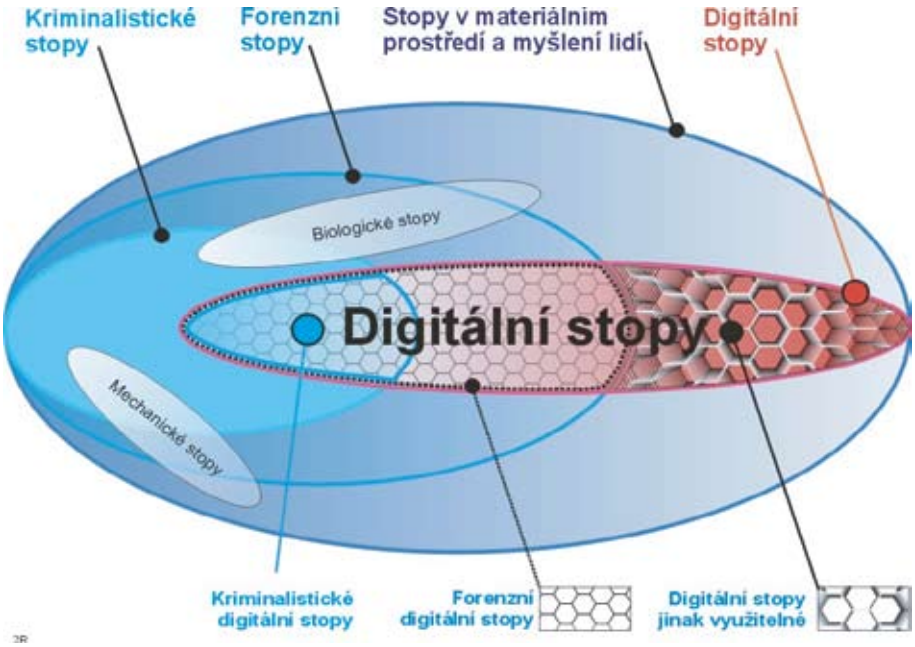
Lidské aktivity, nástroje a prostředky, objektivní okolnosti mohou být velmi různorodé. Záznamy, digitální stopy jsou důsledkem celého komplexu výše uvedených faktorů. Při zkoumání digitálních stop v první fázi nemusí být vždy zřejmé, zda digitální stopy odpovídají aktivitám kriminálního charakteru, nebo zda mohou být využity pro forenzní šetření obecnějšího charakteru či se jedná o stopy běžné, legitimní činnosti pachatele. Záleží tedy na tom, co vyšetřujeme, co hledáme. V každém případě je nutné prověřovat každou relevantní stopu, potvrzovat nebo vyvracet pracovní vyšetřovací hypotézy.

Stopy v materiálním prostředí a ve vědomí lidí lze podle jejich využitelnosti pro různé druhy vyšetřování rozdělit do tří základních kategorií:

a) Kriminalistické stopy. Vztahují se k vyšetřování trestných činů a přestupků, specifikovaných zákonem. Pro potřeby kriminalistické (stejně tak ovšem i forenzní) praxe je požadována vysoká kvalita, objektivita zajištěných stop. Kriminalistické stopy chápeme jako podmnožinu forenzních stop.

b) Forenzní stopy. Obecně jakékoliv stopy využitelné pro potřeby forenzní vyšetřování, včetně šetření orgánů činných v trestním řízení. Na rozdíl od klasického kriminalistického vyšetřování sem ale i patří vyšetřování charakteru forenzních auditů v civilní nebo komerční sféře. Výstupy vyšetřování jsou připravovány tak, aby svou kvalitou a formálním zpracováním obstály před soudními orgány. V praxi se setkáváme s případy, kdy na základě šetření interního auditu nebo nezávislé expertní (nestátní) instituce je podáno trestní oznámení. Zajištěné důkazy (stopy) by auditorskými orgány měly být předány státním orgánům činným v trestním řízení v dostatečné, standardně požadované kvalitě. Zajištění originálů některých digitálních stop je neopakovatelný proces, tj. dalším orgánům se nepodaří zajistit již jednou zajištěné stopy (vůbec nebo v požadované kvalitě tak, aby byly akceptovatelné).

c) Jinak využitelné stopy. Tento typ stop odráží všechny ostatní aktivity objektů a subjektů, které nespadají do dvou výše uvedených kategorií. Jsou to důsledky legitimních činností uživatele nebo objektivního působení vnějších sil a energií, které nemají logickou vazbu na forenzní stopy a které lze využít např. při nejrůznějších analýzách, zaměřených na zvyšování výkonu nebo zlepšování funkčnosti zařízení, ekonomičnosti provozu,



Obr. 7 Digitální stopy a jejich praktické využití.

dostupnosti služeb, stupně bezpečnosti apod. Kvalita a forma zpracování stop v tomto případě je obvykle poplatná účelu, ke kterému mají být výstupy použity. Často jsou to i interní materiály vnitřní kontroly dodržování institucionálních pravidel atd. Svým charakterem a kvalitou tento druh stop nemusí (ale může) být akceptovatelný soudními orgány.

DIGITÁLNÍ STOPY Z POHLEDU KRIMINALISTICKÉ KATEGORIZACE STOP

Stopy jsou odrazem působení odráženého objektu na objekt odrážející. Pokusíme se v souvislosti s digitálními stopami provést zatím pouze orientačně novou kategorizaci kriminalistických stop. Objekty neživé přírody v navrhované klasifikaci účelově dělíme na objekty neživé přírody a umělé artefakty. Obecně existují pouze tři základní typy objektů nebo subjektů, které na sebe mohou vzájemně působit. Jsou to:

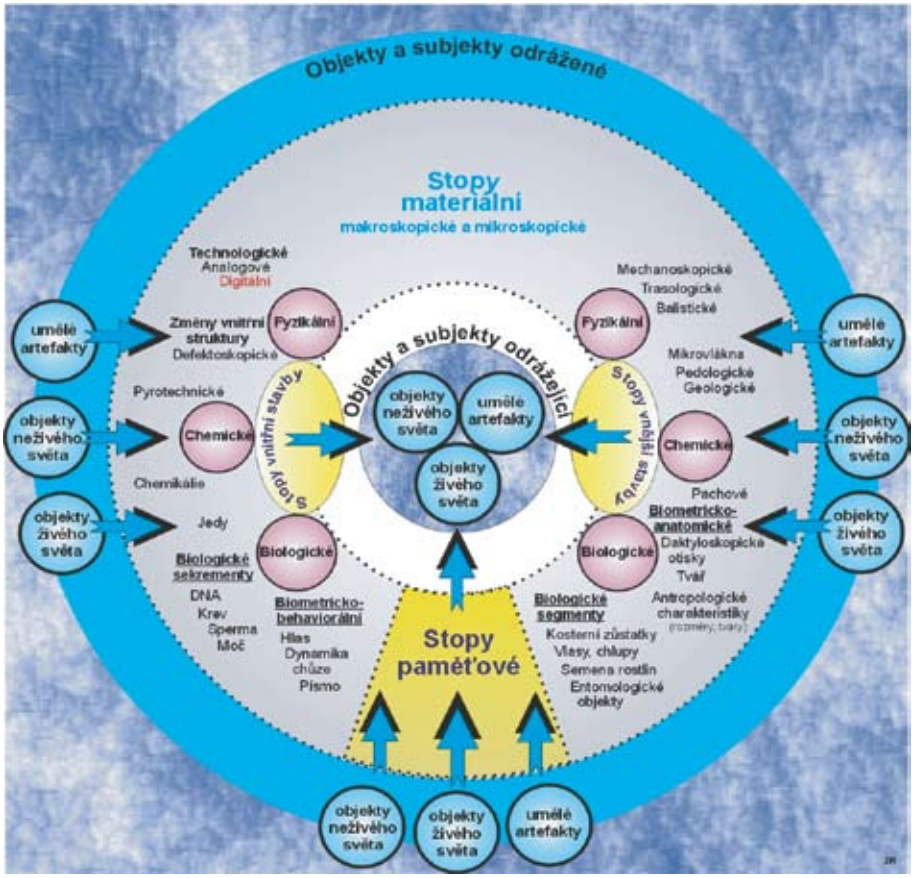
Objekty živé přírody. K těmto objektům zařazujeme teoreticky veškeré živé tvorstvo, živočichy a rostliny, tedy faunu a floru ve všech svých vývojových úrovních. Svébytné postavení má člověk, schopen myšlení a realizace svých představ a tužeb. Je to právě jen člověk, který z rozmanitých důvodů dosahuje svých cílů i nezákonným způsobem nebo je obětí podobné činnosti jiných organizovaných i neorganizovaných podobných individuí.

Objekty neživé přírody, kam patří např. horniny, rudy, zkameněliny (fosílie), půda, voda, vzduch, oheň apod. Tyto objekty vznikly v procesu zrodu a stárnutí kosmických těles v důsledku působení přírodních sil a energií. Do této skupiny můžeme zařadit objekty, které vznikají v důsledku působení přírodních sil (fyzikální, chemické podstaty), jako je led, sníh, kroupy apod. Často na odrážející objekty působí samotné přírodní síly, které zanechávají stopy fyzického nebo chemického charakteru – stopy úderu blesku, prudkého deště, tornáda atd.

Umělé artefakty. Jsou to obecně všechny produkty neživé (hmotné i nehmotné) podstaty, které vznikly jako důsledek lidské činnosti ve velké rozmanitosti jejich druhových forem a oborů lidské působnosti. Od primitivních forem z doby kamenné, přes umělecká díla všech historických období, až po produkty stavitelství, dopravy, nejrůznější současné technologie včetně těch high-tech. Z hlediska kriminalistiky jsou to právě artefakty, které jsou zpravidla cílem nebo prostředkem (nástrojem) trestné činnosti.

Z teoretického hlediska všechny tyto tři základní typy objektů mohou na sebe vzájemně působit, tj. „každý s každým“ v procesu nebo na pozadí trestné činnosti a přitom zanechávají hmotné i nehmotné (paměťové) stopy, jež jsou pro vyšetřování trestného nebo jiného činu či aktivity kriminalisticky nebo jinak relevantní.

Je nutné zdůraznit, že objekty na sebe působí vždy navzájem. Záleží jen na podstatě a charakteristikách těchto objektů, na



Obr. 8 *Stopy jsou produktem (odrazem) vzájemného působení objektů a subjektů. Mechanismus působení a následné kategorizace je uveden na tomto obrázku. Vycházíme z předpokladu, že na sebe mohou působit pouze tři základní skupiny objektů či subjektů (objekty živého světa, objekty neživého světa a umělé artefakty vytvořené člověkem). Stopy mají materiální nebo paměťový charakter. Materiální stopy jsou biologické, chemické nebo fyzikální podstaty a odrážejí vnitřní nebo vnější strukturu působícího objektu či subjektu.*

stupni lidského poznání a používaných technologií, jak tyto stopy odhalit a vysvětlit. V některých případech stopy zůstávají na obou vzájemně působících objektech (oba objekty mají tedy funkci odráženého i odrážejícího objektu), v jiných pouze na jednom (nebo nejsme momentálně technologicky schopni stopy na druhém objektu zaznamenat).

Bez ohledu na kriminalisticko technickou a kriminalisticko taktickou hodnotu kriminalistických stop je nutné se zmínit o kategorizaci kriminalistických stop. V úvodu je vhodné připomenout, že neexistují žádné všeobecně uznávané systémy dělení kriminalistických stop, které by měly obecnou platnost. V minulosti takovéto snahy existovaly, ale jejich výsledek byl neuspokojivý. *Pro kriminalistickou praktickou činnost není totiž důležité určení (taxativní výčet) kriminalistických stop, ale je potřeba se zabývat všemi kriminalistickými stopami, které byly ke konkrétní události nalezeny* [14, str. 70].

Při členění kriminalistických stop záleží totiž na tom, z jakého úhlu pohledu se na stopy, a tedy na jejich zařazování do určitých kategorií, díváme. Čím více těchto pohledů je, tím více je problém multidimenzionální a každá stopa určitého druhu (mající stejné druhové charakteristiky shodné pro všechny podobné stopy) může být současně zařazena do několika kategorií, mnohdy dokonce podle velice subjektivního pohledu nebo určité kriminalistické školy či zvyklostí.

V dostupné literatuře nalezneme následující základní pohledy na kategorizaci stop podle:

Materiální podstaty (stopy materiální nebo paměťové).

Obsahu informací o základní struktuře působících objektů (stopy vnější a vnitřní stavby působících objektů).

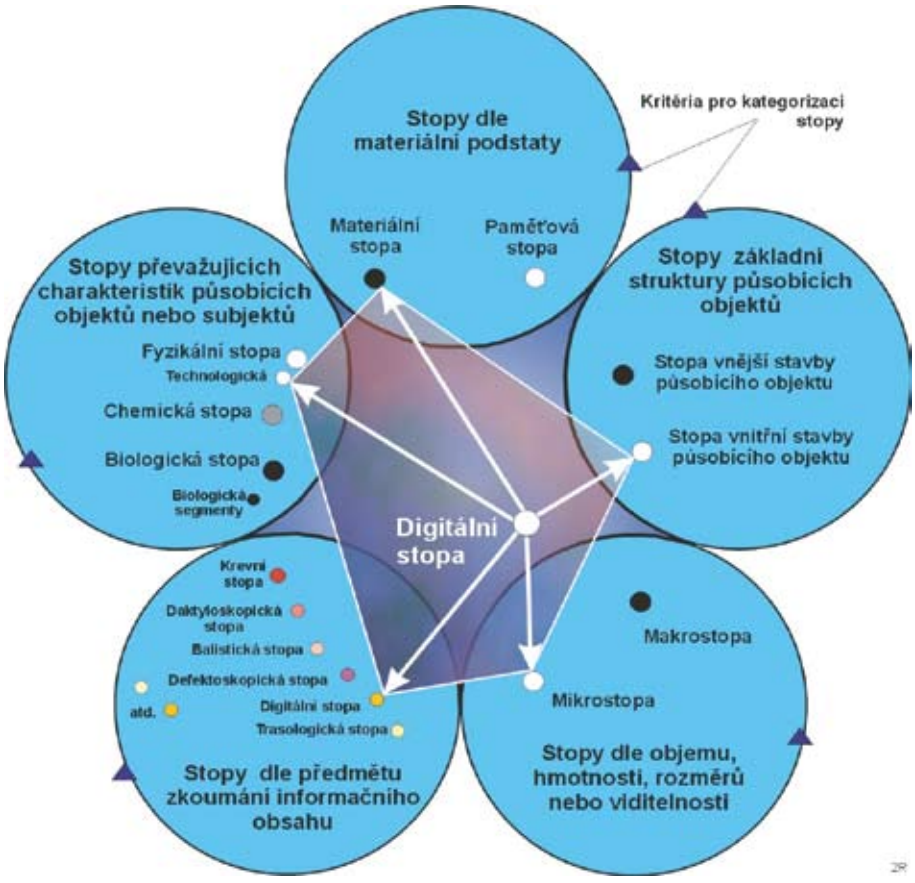
Původu převažujících charakteristik odráženého objektu nebo subjektu (materiální stopy biologického, chemického nebo fyzikálního charakteru).

Předmětu zkoumání informačního obsahu stopy (stopy krve, daktyloskopické stopy, trasologické stopy, digitální stopy, defektoskopické atd.).

Objemu, hmotnosti, rozměrů nebo viditelnosti zanechané stopy (makrostopy a mikrostopy).

Způsobu interakce při vzniku stopy (stopy navrstvení nebo odvrstvení – otisky, stopy dynamické nebo statické, plošné nebo objemové, vzniklé předáním nebo odebráním energie či hmoty atd.).

Každou stopu lze zařadit ke každé kategorii z uvedené šestice. Jinými slovy – stopa je buď materiální nebo paměťová, odráží informace o základní vnitřní nebo vnější struktuře působícího objektu; je-li materiální ho charakteru, pak vznikla biologickým, chemickým nebo fyzikálním působením (nebo jejich kombinací), u každé stopy lze zkoumat její informační obsah, každá stopa je makrostopou nebo mikrostopou (a podle toho volíme vhodné postupy, prostředky a nástroje k jejímu zpracování), každá stopa vznikla specifickým způsobem interakce mezi vzájemně působícími objekty.



Obr. 9 Grafické znázornění kategorizace digitální stopy.

KATEGORIZACE A ZAŘAZENÍ DIGITÁLNÍ STOPY

Výchozím kritériem pro kategorizaci stopy je samotný předmět jejího zkoumání, informační obsah, který je kriminalisticky nebo jinak relevantní. Stopy se stejnými charakteristikami zařazujeme do stejných kategorií. Každou stopu lze zařadit do všech základních kategorií stop současně, tj. vyřknout výrok, zda je materiální či paměťová, zda se jedná o mikrostopu či makrostopu apod. Z každé základní kategorie může mít stopa ale jen jeden atribut (stopa materiální nebo paměťová – viz obr. 9).

Podle definice je digitální stopa jakákoliv informace s vypovídající hodnotou relevantní pro vyšetřování konkrétního činu nebo aktivity, uložená nebo přenášená v digitální podobě. Informace jako taková je nehmotná. V okamžiku jejího ukládání se zhmotňuje v prostředí paměťového média, které je technologického charakteru. Abychom mohli přenášenou informaci analyzovat, musíme ji nejprve technologicky zachytit a následně opět trvale nebo dočasně uložit na paměťové médium. **Digitální stopa je hmotného, materiálního charakteru.**

Digitální stopa vzniká působením člověka (obecně uživatele, vývojáře, administrátora apod., neboť pachatel trestného činu může mít jakoukoliv z právě uvedených rolí) na uživatelský nebo systémový SW, automaticky předem naprogramovaným jiným softwarem či fyzikálním působením (např. silné vnější magnetické pole dokáže zničit data na paměťovém médiu a přitom zanechá stopy tohoto působení, jež jsou rovněž digitální) nebo jinými technickými prostředky. Interakcí vzájemného působení objektů se v případě digitálních stop účastní objekty živé přírody (zejména člověk), objekty neživé přírody (např. nahodilé fyzikální úkazy) nebo uměle vytvořené artefakty člověkem, kam patří SW, technická zařízení a prostředky apod. Ve všech těchto případech se na odrážející objekt přenášejí charakteristiky vnitřní stavby působícího, odráženého objektu. **Digitální stopa je stopou vnitřní stavby odráženého objektu.**

Digitální stopa je ve své primární formě, tedy uložená nebo přenášená, až na určité, nepatrné výjimky, **mikrostopou**. K jejímu zviditelnění jsou nutná technologická zařízení nebo uživatelský, systémový a zejména forenzní software. K nejjednodušším, uživatelům blízkým technologiím patří monitory nebo displeje zobrazující digitální informace do lidsky přijatelnému formátu (písmo, obrazy, zvuk, videosekvence, vibrace atd.), které navíc umožňují převod digitálních dat pro uživatele na nativní paměťové médium – např. kancelářský papír, klasická fotografie. Takto transformované digitální informace (stopy) jsme schopni vnímat našimi smysly, zejména zrakem a sluchem, popř. hmatem (slepecké Braillovo písmo[9]). Uživatelský SW (textové, grafické editory, tabulkové procesory) dokáže zobrazit běžné stopy, podobně jako systémový software, který je běžným uživatelům z hlediska vnímání a možností využití podstatným způsobem vzdálen. Specializovaný software forenzního charakteru dokáže navíc číst informace o smazaných souborech, rozbíjet hesla chránící přístup k zakódovaným informacím apod.

Digitální stopa vzniká zejména působením fyzikálních sil a energií. **Digitální stopu zařazujeme** především **mezi fyzikální stopy** technologického charakteru jako odraz přímého nebo nepřímého působení umělých artefaktů nebo vnějších přírodních sil fyzikálního charakteru. Pod přímým působením umělých artefaktů rozumíme přímé, automatické, nahodilé nebo předem naprogramované působení jednoho technologického prvku (artefaktu) na druhý. V případě nepřímého působení rozumíme působení člověka na artefakt (v podobě SW nebo technického zařízení či technologie). Teoreticky i prakticky (zatím v omezené míře determinované výzkumnými a vývojovými pracovišti) může být technologie uložení nebo přenosu digitální stopy založena i na jiných principech než fyzikálních – tedy chemických nebo dokonce biologických. Pro dnešní technologie a trendy přenosu, zpracování a uložení digitálních informací je markantní snaha o maximální miniaturizaci zařízení a co největší hustotu uložených informací (co největší datový objem v co nejmenším fyzickém objemu paměťového média). Z tohoto pohledu se fyzikální principy zdají být v určitém ohledu vyčerpány a vědecká pozornost se zaměřuje na technologie blízké biologickým či biochemickým způsobům zpracování informací, tedy procesům, podobným či přímo probíhajícím v lidském mozku. Nelze proto do budoucna vyloučit obecně žádné přírodě blízké charakteristiky uložení a zpracování informací.

ZDROJE DIGITÁLNÍCH STOP

Je zřejmé, že existuje velké množství rozmanitých zdrojů digitálních stop. Jejich množství i typová různorodost se dnem ode dne zvyšuje. Je proto účelné datové zdroje rozdělit do několika typických skupin, ve kterých digitální stopy mají obdobný charakter a tedy i způsob jejich vyhledávání, zajišťování, zpracování a dalšího využití je obdobný. Typická skupina vyžaduje specifické nároky na technické vybavení a znalosti úzce orientovaných specialistů pro zajištění digitálních stop.

V zahraniční literatuře (např. [6]) se setkáváme velice často s logickým uspořádáním do tří následujících skupin:

1. *Otevřené počítačové systémy.* Sem patří vše, co si obvykle lidé představují pod pojmem počítač a jeho bezprostřední periférie – PC (desktopy), notebooky, hardisky, klávesnice, monitory, servery atd. Byť jejich disková kapacita je vždy omezená (ale neustále se vyrábějí zařízení se stále větším diskovým prostorem), obsahují obrovské množství informací a tedy digitálních stop. Obyčejný datový soubor – např. dokument Wordu – může svým obsahem i systémovými informacemi (tzv. metadaty[10]) posloužit jako klíčový důkazní prostředek a podstatně ovlivnit a urychlit průběh vyšetřování.
2. *Komunikační systémy.* Tradičně do této skupiny patří klasické pevné telefony, bezdrátové telekomunikační systémy, počítačové sítě a Internet. Ty vše mohou poskytnout digitální stopy. Tak například prostřednictvím internetových služeb

[9] V universitním prostředí jsou dokonce intenzivně vedeny výzkumy na generování elektronických vůní, které by se nechaly vzdáleně přenášet (např. Internetem).

[10] Metadata – informace o informacích, informace popisující jiné informace. V našem případě datum a čas vytvoření souboru, datum jeho modifikace, vlastník souboru, informace o tom, na jakém počítači byl soubor vytvořen, velikost souboru, počet slov, editační poznámky – autorství změn atd.

Obr. 10 Příklady zdrojů digitálních dat. Pracoviště počítačového administrátora. 1 – PC s dvěma pevnými disky (kapacita 60 GB každý). 2 – připojení k USB paměti (kapacita 2 MB), 3 – disketa 3.5" (kapacita 1,4 MB), 4 – zipka (kapacita 100 MB), 5 – pásková paměťová cartridge (kapacita 2 GB), 6 – personální organizér (PDA[11]) (základní paměť 4 MB), 7 – xD Picture karta do fotoparátu (různé kapacity – od 32 do 512 MB), 8 – CD (800 MB), 9 – digitální fotoaparát se záznamovými médii typu xD Picture card a SmartMedia, 10 – digitální pevný přístroj se záznamníkem, 12 – mobilní telefon.

je e-mail přenášen po celém světě. Čas odeslání nebo autor e-mailu, jeho obsah, logové soubory poštovních serverů, které přenášely e-mail, to vše jsou velmi důležité digitální stopy.

3. *Zařízení s integrovaným počítačovým čipem.* Mobilní telefony, osobní digitální asistenti (PDA), čipové platební karty a mnoho dalších zařízení s počítačovým čipem jsou též velmi cenným zdrojem dat, vhodných pro vyšetřování. Navigační technologie založené na GPS dokáží determinovat polohu dopravního prostředku i jedince, černá schránka letounu si pamatuje všechny letové charakteristiky, podobně jako diagnostické moduly počítačových řídících jednotek automobilových motorů uchovávají základní provozní a servisní údaje (rychlost, činnost brzd, počet ujetých kilometrů, diagnostika poruch, druhy servisních zásahů apod.). Další skupina zařízení vybavených integrovaným čipem a určených pro využití v běžné domácnosti obsahuje důležité informace a tedy další zdroje stop. Tato zařízení dokáží navíc standardně, zpravidla již i bezdrátově, komunikovat s okolním světem, dalšími zařízeními a prostředími, včetně Internetu.

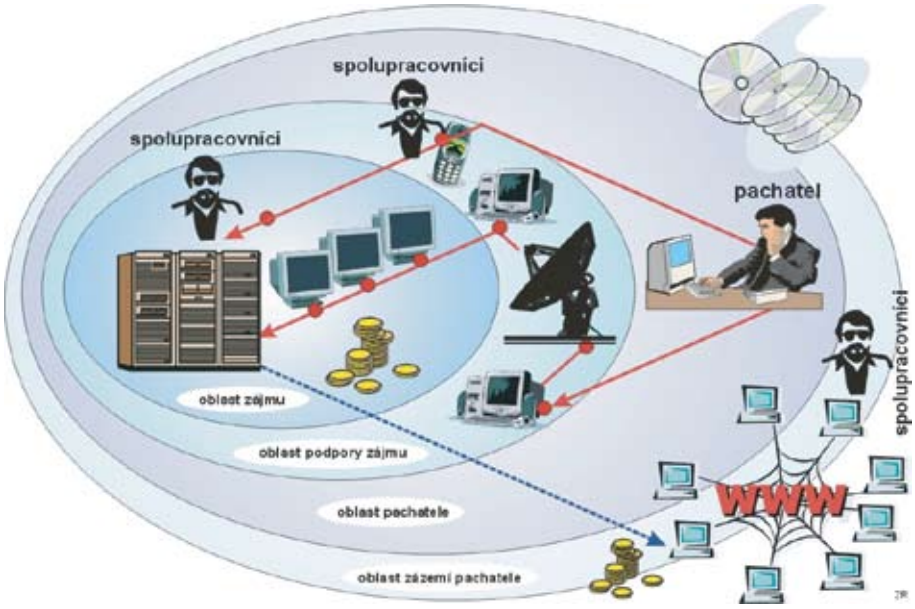
Díky všudypřítomnosti digitálních stop je dnes jen velmi málo zločinů, které by nebyly spojeny s uloženými nebo přenášenými informacemi. Trénované oko vybavené příslušnými znalostmi a prostředky dokáže tyto stopy nalézat a spojovat je s jednotlivými osobami, trestnými činy nebo jinými aktivitami. Personální počítače a nezbytné periférie jsou archivní pokladnicí moderního lidského počínání a snažení, které je v mnohém tak intimní, že ani nejbližší rodinný kruh či přátelé neznají o svém blízkém tolik, kolik je možné vyčíst z digitálních stop. Rovněž databáze elektronického obchodu obsahují velice intimní údaje o tom, co a kdy nakupujeme, co máme rádi, jaké máme slabosti (nákup alkoholu, léčiv, intimních hygienických potřeb) atd. To vše umožňuje hluboký psychologický pohled do duše pachatele nebo jeho oběti.

I přes obrovský rozmach digitálních technologií existuje pořád málo specialistů, kteří by dokázali efektivně v digitálních stopách číst a vyvozovat relevantní závěry využitelné pro orgány činné v trestním nebo jiném řízení. Nejsme mnohdy dostatečně technicky, znalostně ani právně připraveni pracovat s digitálními stopami. Ty jsou často přehlíženy nebo podceňovány, nekorektně shromažďovány nebo neefektivně analyzovány.

DIGITÁLNÍ STOPY A MÍSTO TRESTNÉHO ČINU

Relativně novým teoretickým i praktickým fenoménem jsou prostředky výpočetní, telekomunikační, záznamové techniky a další techniky, uchovávající digitální záznamy, které se mohou na místě trestného činu vyskytovat přímo nebo zprostředkovaně (notebook si důležitými informacemi mohl pachatel či kdokoliv jiný odnést, zničit nebo naopak pachatel pomocí PC na místě trestného činu mohl komunikovat s dalšími vzdálenými počítači, aplikacemi, vozidlo pachatele s navigačním systémem mohlo odjet spolu s pachatelem apod.). Význam digitálních stop, jejich obsažnost, způsoby zajišťování a následné analýzy, bývají mnohdy

11 PDA – Personal Digital Assistant.



Obr. 11 Znázornění čtyř základních oblastí, kde lze vyhledávat digitální stopy.

v praxi v celosvětovém měřítku dosud neopodstatněně přezírány či podceňovány. Rozhodující roli mají nejenom specializované forenzní laboratoře či ústavy, ale především ty složky vyšetřujících orgánů, které jsou na místě trestného činu jako první nebo které vedou bezprostředně následně vyšetřování. Bez odborných znalostí v první frontové linii nemůže být vyšetřování nikdy úspěšné. Nemyslíme tím ale nutnost odborných znalostí ICT prostředků, jako spíše organizační a metodické postupy, které musí garantovat včasné zajištění kvalitních digitálních stop a zabránit jejich znehodnocení či zneužití, tedy spolupráce s dalšími specializovanými útvary.

Místo trestného činu v případě digitálních stop může být za určitých okolností velice těžko geograficky vymezitelné. Situace je poměrně jednoduchá, jedná-li se o důkazy, uložené v samostatném, od sítě odděleném PC, notebooku nebo o samostatné zařízení (fotoaparát, videokamera, personální digitální asistent (PDA) atd.). Za těchto okolností jsou digitální stopy uloženy přímo v těchto zařízeních nebo na datových médiích s nimi kompatibilními.

Podstatně složitější je situace, kde počítač je propojen do institucionální (podnikové) sítě, do prostředí Internetu a má-li uživatel přístup k většímu množství nejrůznějších aplikací, serverech, zařízení apod. Servery mohou být uloženy mimo instituci, v zemi na druhé straně polokoule.

Je známo, že profesionální pachatelé, jejichž činnost směřuje zejména k počítačové nebo kybernetické kriminalitě, velice dobře si uvědomují podstatu a význam digitálních stop, jež jsou pro ně velmi nebezpečné. Z pochopitelných důvodů (ostatně jako všichni pachatelé, vědomě připravující a plánující trestný čin), se snaží stopy skrýt, svést vyšetřování jiným směrem nebo vyšetřovatele zahltit nemírným množstvím lživých, těžko ověřitelných informací. Používají pro to nejrůznější metody – sociotechniky[12], krádeže počítačové identity jiného uživatele (pod jehož identitou, uživatelským kontem pak dále vystupují), usilují o ovládnutí nejvyšších administrátorských práv správce systému. To jim pak v maximální míře dovoluje zahlazovat stopy a v digitálním prostředí se pohybovat téměř neviditelně, protože mají dostatek oprávnění a prostředků k této činnosti. Rozhodující jsou pak především znalosti operačních systémů, databází, rozmanitých služeb apod. Při útocích na různé servery se zpravidla neútočí přímo, ale postupným, několikanásobným, řetězovým ovládnutím většího počtu serverů. V konečném důsledku pak poškozený neví, kdo ve skutečnosti útočí. Vyšetřovatelé mají navíc podstatně stíženou práci, protože musí nalézt celý řetězec těchto postupných kroků pachatele. K tomu potřebují vědět, co hledat a navíc zajistit všechny relevantní digitální stopy podporující dané vyšetřovací verze s dostatečnou kvalitou důkazního materiálu. Místo trestného činu je mnohem hůře vymezitelné, než v případě klasického trestného činu, pro které jsou charakteristické mechanické, biologické, daktyloskopické, trasologické, balistické, pyrotechnické (a mnohé další) druhy stop, ohraničené na poměrně malý fyzický prostor. V případě digitálních stop se často jedná i o velké množství relativně fyzicky velmi malých prostor (dané např. velikostí zařízení), které jsou mezi sebou velmi vzdálené a kde nemusí být na první pohled zřejmé propojení.

Dalším faktorem, znesnadňujícím sledování digitálních stop je potenciálně velká pravděpodobnost kombinace různých technologií, umocněná zapojením většího množství pachatelů. Ti se dělí o určité činnosti nebo naopak sdílejí společné prostředky či poznatky, nebo naopak působí z různých míst. I digitální stopy mohou být důsledkem organizované trestné činnosti, kde kromě pachatelů mohou figurovat i nastrčené, nic netušící osoby (tzv. „koně“).

Globální oblast trestného činu může být nesmírně složitá, členitá a rozsáhlá. V případě počítačové nebo kybernetické kriminality je proto účelné vyčlenit typické oblasti, kde je nutné hledat digitální stopy. Rozeznáváme následující čtyři oblasti, které v některých případech se mohou mezi sebou překrývat, splývat:

[12] Sociotechnika – je ovlivňování a přesvědčování lidí s cílem oklamat je tak, aby uvěřili, že sociotechnik je osoba s totožností, kterou předstírá a kterou si vytvořil pro potřeby manipulace. Díky tomu je sociotechnik schopný využít lidí, se kterými hovoří, případně dodatečné technologické prostředky, aby získal hledané informace. [Mitnick]

Oblast zájmu – obvykle cíl útoku, kde pachatel realizuje své požadavky, cíle, zájmy: získává, mění, ničí data, provádí nelegální transakce apod.

Oblast podpory zájmu – okolní prostředí, bezprostředně hraničící s oblastí zájmu. V praxi to mohou být různé servery na přístupových trasách, technologicky rozmanité komunikační cesty a neposlední řadě spolupachatelé, nastrčené osoby, prostředníci. Oblast podpory zájmu může hrát roli krycího prostředí, jehož cílem je získat legendu pro nelegální činnost nebo zahladit či zničit digitální stopy vedoucí přímo k pachateli a tím popřít logickou souvislost mezi oblastí zájmu a oblastí pachatele. V jiných případech oblast podpory zájmu slouží jako skutečný prostředek k realizaci trestného činu, bez kterého by nebylo možné požadovaný záměr pachatele realizovat. Technologické prostředky z oblasti pachatele nemusí být dostatečně silné, výkonné či efektivní k vedení přímého nebo skrytého útoku do oblasti zájmu.

Oblast pachatele – místo, ze kterého pachatel organizuje, koordinuje aktivity směřované do oblasti jeho zájmu. Odsud se jako nitky mohou rozbíhat digitální stopy k různým prostředníkům nebo technologickým prostředkům podpory zájmu. Zajištění digitálních stop v této oblasti zpravidla vede k rozkrytí celé organizační struktury nebo technologických kanálů a prostředků pro vedení útoku. Digitální stopy z této oblasti jsou klíčové i z pohledu dokázání přímé vazby mezi pachatelem a jeho činnostmi, což je pro vyšetřování velmi důležité a jedná se o klíčové důkazy.

Oblast zázemí pachatele. Jestliže pachatel svůj útok dlouhodobě připravuje, obvykle přemýšlí kam skrýt hodnoty („kořist“) získané z útoku. Bezprostřední oblast pachatele zpravidla nezajišťuje bezpečí v případě vyšetřování. Jedná se o další způsob skrývání úspěšné trestné činnosti. Cílem je přerušit logickou i fyzickou vazbu mezi pachatelem a výsledky jeho činností. Tak např. získané citlivé informace lze uložit na speciální předem připravené a vytvořené místo, které má specifickou strukturu, formát datového média. Zrovna tak může fyzicky velmi dobře posloužit trezor ve zcela jiné bance, kam bude skryta výsledná aktivita trestného nebo jiného činu, např. peníze, média s informacemi apod. Jako správce oblasti zázemí pachatele může opět figurovat i další spolupracovník, který předem zná nebo vůbec naopak neví, co spravuje a chrání před „nepovolanými“ osobami. Oblast zázemí pachatele může obsahovat „kořist“ z trestného činu a/nebo může poskytovat klíčové informace k jejímu nalezení, v našem případě i digitální stopy.

Pro všechny oblasti je typické, že bývají ve většině případů dlouhodobě nebo krátkodobě digitálně propojeny, tj. jsou zde souvislosti a návaznosti digitálních (či jiných) stop.

CHARAKTERISTIKY A SPECIFIKA DIGITÁLNÍCH STOP

Digitální stopy, 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 jsou následující:

- nehmotnost digitálních stop,
- latentnost digitálních stop,
- časová trasovatelnost digitálních stop,
- vysoká obsažnost digitálních stop,
- velmi nízká životnost digitálních stop,
- uchování a kvalita digitálních stop je ovlivněna řadou subjektivních faktorů,
- velký datový objem digitálních stop,
- datová hustota digitálních stop v čase a s rozvojem nových technologií neustále klesá,
- extrémní dynamičnost prostředí digitálních stop,
- heterogennost a komplexnost prostředí digitálních stop,
- velký geografický rozsah prostoru s digitálními stopami,
- vysoký stupeň ochrany dat znesnadňuje nebo znemožňuje práci s digitálními stopami,
- digitální stopa je specializovanými prostředky automaticky identifikovatelná a zpracovatelná,
- vysoká úroveň zahlazování digitálních stop kvalifikovanými pachateli,
- restaurovatelnost zničených digitálních stop,
- originálnost digitálních stop,
- současně nízká úroveň soudní akceptace digitálních stop v právní praxi.

NEHMOTNOST DIGITÁLNÍCH STOP

Data, informace, jako takové jsou nehmotné. Pro jejich ukládání je ale vždy nutné hmotné médium, které má nejrůznější technologické provedení, formát, datovou strukturu, konektivitu, spolehlivost, životnost apod. Toto médium obsahuje digitální stopy a je fyzickou součástí důkazního prostředku. V soudní praxi může být požadováno jako fyzická část důkazu, ze kterého je možné kdykoliv nezávisle a opakovatelně získat stejné informace pro stanovení expertního nálezu. Takto jsou vnímány především technologie pro digitální zpracování dat pro osobní potřeby (PC, notebooky, paměťové karty, kazety, diskety, CD a DVD disky, mobilní telefony, osobní organizéry (PDA[13]) apod.), které jsou na místě trestného činu zajištěny a předány do laboratoře k expertnímu zkoumání. Po dobu trestního řízení jsou k dispozici orgánům činným v trestním řízení. Podstatně složitější je situace u rozsáhlých datových sítí, podnikových serverů, kde toto z provozních nebo jiných důvodů není možné realizovat.

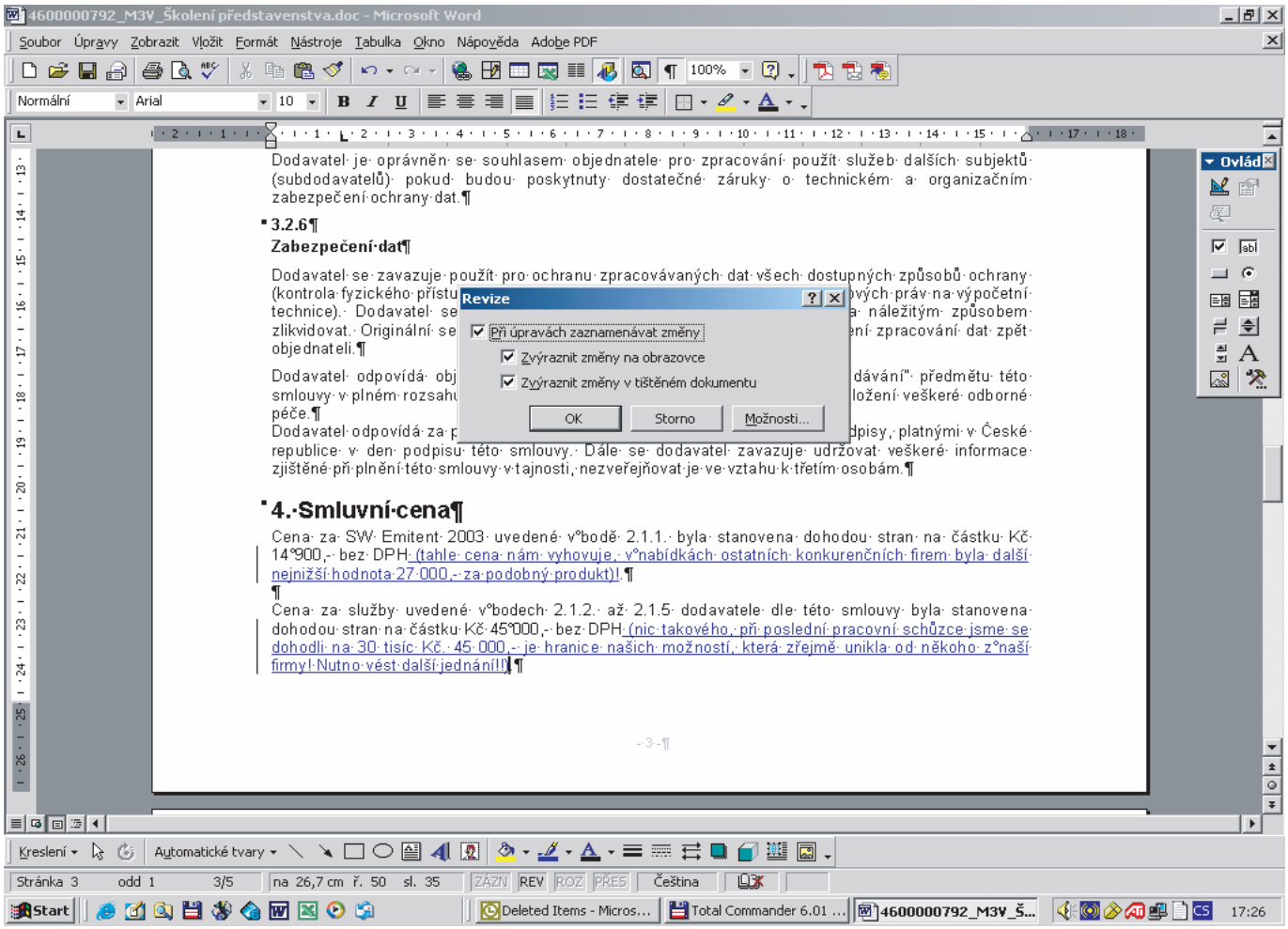
13 PDA – Personal Digital Assistant.

LATENTNOST DIGITÁLNÍCH STOP

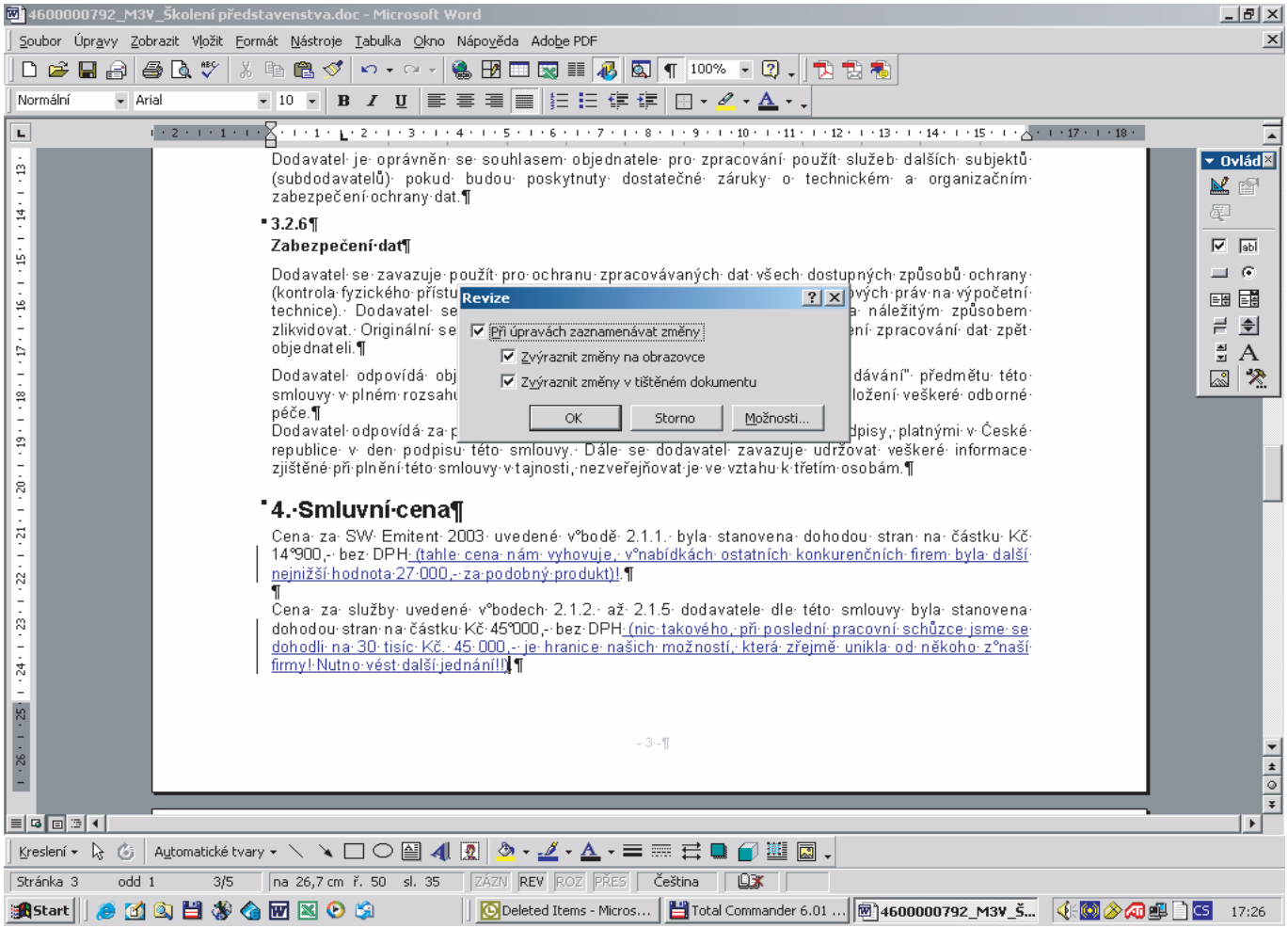
Digitální stopy jsou neviditelné. Latentnost je vícenásobná. Záznamy, zpracovávané nebo uchovávané na datovém médiu, nelze vidět pouhým okem (výjimku tvoří pohledy na obrazovku monitoru, printscreeny, fotografie nebo videozáznamy obrazovek, vytištěné dokumenty). Druhý stupeň neviditelnosti spočívá v tom, že některé záznamy, soubory jsou pro běžné uživatele výpočetní nebo digitální techniky neviditelné, protože mají nastaven atribut „hidden" a musí být zvoleny speciální nastavení uživatelských práv nebo speciální aplikační či systémové prostředky, nebo jiné speciální nástroje pro jejich zviditelnění. Do další kategorie latentních stop („příčin neviditelnosti") patří smazané záznamy, přeformátované disky či jiným nástroji pozměněná nebo zničená data na datovém médiu. K jejich restauraci je nutný specializovaný software. Podobným způsobem řešíme i zašifrované údaje, které jsou pro uživatele sice viditelné, ale bez informačního obsahu.

ČASOVÁ TRASOVATELNOST DIGITÁLNÍCH STOP

Na rozdíl od většiny jiných stop známých z kriminalistické nebo forenzní praxe, digitální stopy v některých případech mohou s přesností na sekundy (někdy i s přesností ještě vyšší) určit přesné časové vymezení probíhajících aktivit. Mohou to být aktivity jednorázové, nebo řetězec na sebe logicky navazujících činností. Tato skutečnost je dána tím, že počítače a stejně tak další digitální zařízení (videokamery, fotoaparáty atd.) mají v sobě zabudované digitální hodiny, které označují aktivity aplikačního, systémového SW nebo jiných činností digitálních zařízení tzv. časovou známkou. Je běžné, že správné nastavení času větších systémů je v praxi prováděno automatickou synchronizací prostřednictvím služeb Internetu, specializovanými rádiomajáky (vysílači), takže časový údaj je naprosto věrohodný. Lze pak zjistit, kdy se uživatel přihlásil/odhlásil do/z počítače, vytvořil, smazal, modifikoval soubor, provedl databázovou transakci (vybral peníze z účtu, prohlédl si



Obr. 12 I běžný kancelářský SW dovoluje uživateli skrývat určité informace. Záleží jen na jeho znalosti, které mu umožňují plně využívat funkcionalitu aplikačního programového vybavení. Pokud uživatel některé znalosti nemá, v dokumentu mohou být nalezeny velmi významné digitální stopy. Příkladem může být využívání funkcionality revizí ve Wordu. Jestliže si uživatel neuvědomuje všechny souvislosti, může např. komerční konkurenci nechtěně poskytnout důvěrné, interní informace, které byly jen v dokumentu skryty, ale nebyly vymazány. Dochází pak k velice choulostivým situacím, které v krajním případě mohou skončit i podáním trestního oznámení (pomluva, únik informací, zneužívání informací v obchodním styku, porušování pravidel zadávání zakázek pro výběrová řízení apod.). Podobným způsobem může interní audit (pokud jsou uchovávány všechny pracovní verze dokumentů) analyzovat určité postupy zpracování dokumentů, řešících konkrétní problematiku, jež je předmětem forenzního zájmu atd.



Obr. 13 Systémové logy, ale i obyčejné, uživateli vytvořené nebo revidované dokumenty v mnoha případech poskytují informace o autorství a časových údajích (tzv. časových známkách), provázející konkrétní akce.

záznam, zaplatil v pokladně, objednal služby atd.), odeslal e-mail, obdržel e-mail a přečetl si jej, odpověděl na něj atd. Pokud jsou digitální stopy s časovou známkou nalezeny, podstatným způsobem dokumentují průběh zcela konkrétních aktiv v čase. Pokud navíc existuje jednoznačná identifikace uživatele (pachatele) ve vztahu k výpočetní nebo jiné digitální technologii, lze využít digitálních stop k dokumentaci všech jeho aktivit spojených s počítači a digitálními zařízeními, pokud jsou tato zařízení takto navržena, konstruována a provozována podle stanovených zásad.

VYSOKÁ OBSAŽNOST DIGITÁLNÍCH STOP

Digitální stopy mají ve specifických případech velmi vysokou informační hodnotu o osobních zájmech a aktivitách osoby, počítačového uživatele nebo pachatele trestného činu. Z tohoto pohledu jsou pro kriminalistiku a další forenzní vědy velmi význačné a z hlediska teorie stop ve srovnání s jinými druhy stop jedinečné. V mnoha případech je možné sledovat nejenom konkrétní aktivity uživatele v počítači (co vše dělal), ale i o jaké informace se zajímal, jaké informace získával, zpracovával, uchovával či předával jiným. Z toho pak lze usuzovat na určité oblasti zájmu pachatele, jeho motivaci, psychologicky jej profilovat. Příkladem mohou být adresy (a obsahy) prohlížených webových stránek, obsah fotografií, videa, textových souborů atd. Analýza obsahu osobního digitálního prostředku prozradí velmi mnoho profesního i intimního o jeho majiteli.

VELMI NÍZKÁ ŽIVOTNOST DIGITÁLNÍCH STOP

Digitální záznamy (z kriminalistického nebo forenzního pohledu digitální stopy) jsou zapisovány na paměťové médium. Zde mohou být uživatelem cíleně smazány nebo systémově, automaticky (bez účasti člověka) přepsány jinými záznamy. Výjimku tvoří nepřepisovatelné optická média určená pro archivní účely. Ty jsou provozně velmi drahá a ne zcela běžně se v praxi používají. Tato média jsou určena jen pro zápis bez možnosti mazání s dobou životnosti záznamu na médiu 50 let a více. Lze sice obecně pomocí speciálního SW obnovovat i smazané záznamy (a např. i „vysypané z koše operačního systému Windows“), ale i zde platí, že obnova musí být provedena velice rychle, než je paměťové médium systémovými prostředky přepsáno. Rozhodující roli hraje rychlost obnovy a fixace požadovaných dat, kapacita paměťového média

a intenzita práce uživatele(ů) při vytváření datových souborů. Data mohou být navíc zničena počítačovými viry, skrytými programy (typu trójský kůň, zadní vrátka apod.). Při přenosu dat drátovým nebo bezdrátovým způsobem, nemáme-li přístup k souborovým systémům odesílatele nebo příjemce (kde jsou data uložena podstatně déle než při samotném transferu), je doba přenosu velice krátká a pohybuje se řádově v sekundách (a i méně!). Je nutno nasazovat speciální prostředky (monitorovací SW), které ukládají data na paměťové médium a bez kterých není praktické možné zjistit smysluplný obsah dat přenášených v reálném čase. Zjišťování stop tímto způsobem má operativní charakter a realizuje se zpravidla až při prověřování různých vyšetřovacích verzí nebo při cíleném sledování aktivit zájmové osoby.

UCHOVÁNÍ A KVALITA DIGITÁLNÍCH STOP JE OVLIVNĚNA ŘADOU SUBJEKTIVNÍCH FAKTORŮ

Uchování a kvalita digitálních stop je přímo úměrné mezinárodní, národní nebo institucionální[14] legislativě, odbornosti administrace systémů z hlediska bezpečnosti a závisí i na institucionální kultuře, která zejména rozhoduje o úrovni realizace výše uvedených faktorů. Primární roli hraje pravidelné monitorování a audit klíčových transakcí, zabezpečení zálohování a archivace dat z důležitých zdrojů dat (podnikových IS, elektronické pošty atd.) na speciální média a jejich dlouhodobé uložení. Z těchto médií je pak možné v případě potřeby obnovit požadovaná data, která v produktivních systémech již nejsou dostupná. Rozhodující je pravidelnost a frekvence pořizování záložních nebo archivních médií, způsob jejich uchování, aby nedošlo k jejich poškození, dodržování institucionálních norem a pravidel, definovaných zejména v bezpečnostní informační politice a následně v provozním řádu ICT útvaru dané instituce.

VELKÝ DATOVÝ OBJEM DIGITÁLNÍCH STOP

Pro výpočetní a komunikační prostředky je dnes typická jejich silná centralizace, vycházející z provozně-ekonomických důvodů. Na paměťových médiích je uchováváno velké množství dat, vytvořených všemi zaměstnanci instituce a jejich externími partnery. Objem dat u středně velkého podniku v podmínkách ČR se pohybuje řádově v desítkách TB[15].

Příklad:

Jestliže bychom vytiskli textové soubory v digitální podobě o velikosti 3,2 GB na papír formátu A4 a listy na sebe naskládali, dostaneme papírová sloup o výšce 170 m! Pro zajímavost obelisk Washingtonského monumentu je vysoký 169,3 m, Petřínská rozhledna 60 m. Běžná kapacita hardisků dodávaných do PC se pohybuje v rozpětí 40 až 80 GB.

Jen nepoměrně malá část těchto dat má ale charakter digitální stopy. V praxi je často složité z takto velkého objemu dat selektovat nezbytné relevantní stopy a vyhodnotit je v reálně krátké době, nutné pro úspěšné vyšetřování. Z podobných důvodů je velmi komplikované zajišťování digitálních stop z prostředí Internetu, kde objem dat narůstá s počtem (i krátkodobě) připojených serverů, se kterými se pracovalo. Digitální stopy leží i na těchto vzdálených serverech.

DATOVÁ HUSTOTA DIGITÁLNÍCH STOP V ČASE A S ROZVOJEM NOVÝCH TECHNOLOGIÍ NEUSTÁLE KLESÁ

Samotná digitální stopa není v běžném smyslu slova limitována fyzickým objemem. Vznikají stále nové technologie na komprimaci dat, tj. stále větší objem dat se uloží do stejného objemu datového média. Paralelně vznikají nové a nové technologie datových médií, jejichž cílem je rovněž uložit větší množství dat do stejného nebo dokonce menšího objemového prostoru (3.5" disketa má kapacitu 1,4 MB, CD až 800 MB, DVD 6 GB apod.). Aby analýza dat ve forenzním šetření byla dostatečně efektivní a rychlá, musí být směřována na vyhledávání konkrétních druhových nebo individuálních digitálních stop. Víme-li co hledáme, podstatně urychlíme celý proces. V opačném případě analýza pohltí obrovské množství času a prostředků. Objem zpracovávaných a ukládaných dat s rozvojem technologií prudce narůstá. Množství zanechaných digitálních stop pachateli nemusí narůstat stejným tempem. Definujeme-li datovou hustotu digitálních stop jako poměr datového objemu digitálních stop zanechaných nežádoucími aktivitami a celkového objemu všech zpracovávaných nebo ukládaných dat, pak hustota digitálních stop bude do budoucna stále klesat, tj. vyšetřování forenzní vyšetřování bude stále kapacitně náročnějším.

EXTRÉMNÍ DYNAMIČNOST PROSTŘEDÍ DIGITÁLNÍCH STOP

Toto specifikum je typické především pro síťové prostředí společně, v reálném čase sdílených datových fondů velkých institucích. Rozsáhlé podnikové aplikace jsou z hlediska naplnění informačních potřeb instituce a ekonomicky-provozních charakteristik silně centralizované, s vysokým požadavkem na dostupnost aplikací, velmi dynamické. S aplikacemi pracuje velké množství interních uživatelů (zaměstnanců instituce) a/nebo externích partnerů či zákazníků. Aplikace mají zásadní dopad na naplnění cílů (ekonomických, konkurenčních, bezpečnostních apod.) instituce. Aplikace jsou zařazovány mezi tzv. kritické podnikové (institucionální) aplikace, tj. přerušení fungování aplikací po dobu i řádově minut (průmysl, doprava, telekomunikace, finanční instituce atd.) může mít pro instituci nebo jejího zřizovatele katastrofické existenční dopady. Z praktických důvodů pak při vyšetřování nelze tyto aplikace (a še 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

[14] Pod pojmem instituce rozumíme právnické osoby (firmy, neziskové organizace, státní i nestátní instituce apod.), fyzické osoby podnikatelé a fyzické osoby občané.

[15] TB – Terabyte, 10^{12} byte.

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[16]. 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.

HETEROGENNOST A KOMPLEXNOST PROSTŘEDÍ DIGITÁLNÍCH STOP

V běžné praxi jsou i ve stejných institucích používány souběžně různé operační systémy, databázové stroje, aplikační SW a jejich verze, datová rozhraní mezi aplikacemi (tzv. interfacy), datové formáty, přenosové protokoly, protokoly provozních záznamů, logů atd. Každá tato oblast v ICT je úzce specifická a vědomostně do detailu pokrytá různými specialisty. Složitost vyšetřování je dána komplexností problematiky, kterou nemusí koncepčně vnímat žádný vysoce kvalifikovaný specialista. Při vyšetřování není v první fázi zcela jasno, jaké digitální stopy hledáme, a při tom je nutné efektivně koordinovat činnost všech specialistů a operativně podle potřeby usměrňovat jejich součinnost. Digitální stopy mohou být nalezeny v nejrůznějších částech informačních a komunikačních technologií a jako niť se vinout přes různé aplikace a systémy, které kopírují vnitro institucionální procesy, odrážející se právě do digitálních technologií zpracování dat, jež se staly prostředkem nebo cílem určité formy útoku, spáchání trestného činu. 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.

VELKÝ GEOGRAFICKÝ ROZSAH PROSTORU S DIGITÁLNÍMI STOPAMI

Pomocí privátních počítačových sítí i Internetu jsou počítače po celém světě propojené, takže je možné sdílení vzdálených dat a aplikací. Kvalifikovaný pachatel, který chce po sobě zanechat minimum stop, nebo co nejvíce znesnadnit či znemožnit následné vyšetřování, zpravidla nikdy nepřistupuje na zájmový počítač přímo, ale přes počítače další, které teoreticky i prakticky leží v cizích zemí. Počítačové sítě neznají geografických hranic. 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

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

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.

Dalším faktorem, který přispívá k distribuci digitálních stop do velkého prostoru, je kompatibilita zařízení, jejich rozhraní, datových formátů. Názorným příkladem může být jeden a tentýž datový soubor (dokument Wordu nebo digitální fotografie např. formátu *.jpg), který může být uložen jak v notebooku pachatele, osobním digitálním asistentovi (PDA), tak na disketě, CD disku, USB paměti nebo na datovém disku podnikového serveru apod. Má-li pachatel tušení, že může být vyšetřován, pak bude důkazní materiál chtít zničit – tedy smazat. Ale protože soubor, informace v něm obsažené, mají velkou hodnotu, bude se zároveň kromě zničení důkazního materiálu intenzivně snažit je ukrýt někam jinam. Může si např. vytvořit novou privátní schránku na zahraničním poštovním serveru a tam kritický soubor přeposlat, uložit je na jakémkoliv jiné médiu a to dobře schovat, nebo naopak dát do velkého objemu dat – např. na sdílený diskový prostor do adresáře, kde má přístup více lidí a pouze obsah souboru zašifrovat a ochránit jej heslem apod. Tím ale zanechává další potenciální stopy. Jak je vidět, i z tohoto pohledu mají digitální stopy svou specifičnost, která vyusťuje ve vysokou mobilitu digitálních stop a klade na jejich odhalování vysoké odborné, koordinační, týmové, manažerské nároky.

VYSOKÝ STUPEŇ OCHRANY DAT ZNESNADŇUJE NEBO ZNEMOŽŇUJE PRÁCI S DIGITÁLNÍMI STOPAMI

Z bezpečnostních důvodů je řada datových přenosů a uložišť (v souborových systémech, databázích atd.) kryptograficky chráněna. Pokud není znám příslušný algoritmus nebo technologický prostředek na jejich rozkódování, data v digitální formě nemají pro vyšetřující orgán žádnou vypovídací formu, informační hodnotu a nelze proto žádnou jejich část prohlásit za digitální stopu a tedy vést jakékoliv další vyšetřování. Zašifrovaný soubor obsahuje změť nic neříkajících dat. Teprve po jeho dešifrování jsme schopni číst jeho obsah. Data se pro nás stávají informací. Z tohoto pohledu se v některých průmyslově vyspělých zemích odehrává velice intenzivní diskuse mezi státními orgány činnými v trestním řízení (logicky i se zpravodajskými službami) a SW a HW výrobci o automatické povinnosti zajišťovat státní administraci přístup k prostředkům výrobce kryptografického řešení pro potřeby národní bezpečnosti a forenzní šetření. Dochází k antagonistickým střetům mezi státními a privátními zájmy výrobců, které jsou dále podstatně ovlivňovány zákony na ochranu osobní svobody a soukromí; střetům mezi zájmy společnosti (ochrana proti terorismu) a zájmu jedinců (ochrana osobních svobod). Vyšetřování může mít pak 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).

DIGITÁLNÍ STOPA JE SPECIALIZOVANÝMI PROSTŘEDKY AUTOMATICKY IDENTIFIKOVATELNÁ A ZPRACOVATELNÁ

Protože digitální stopy jsou vytvořeny v konečném důsledku vždy určitou technologií, lze je rovněž v dalších kompatibilních technologiích při zachovaní nezbytných podmínek automaticky vyhodnocovat. Část digitálních stop je výstupem uživatelského softwaru nebo systémového softwaru. Ty jsou naprogramované podle určitých principů a algoritmů, takže výstupy z těchto programů mají určitou, zcela konkrétní logiku a strukturu, datový formát, které lze s určitým stupněm přesnosti určit. Tohoto aspektu lze využít v některých specifických případech pomocí jiného specializovaného SW, který dokáže automaticky digitální stopy zanechané algoritmizovanými prostředky identifikovat a vyhodnocovat. Příkladem může být porušování autorského práva instalací nelegálního SW na podnikových PC. Každá instalace SW (legálního i nelegálního) zanechává v tzv. systémových registrech Windows informace o instalovaném produktu. Z pohledu kriminalistické a forenzní praxe se jedná o digitální stopy. Jestliže máme celopodnikovou databázi oficiálně zakoupených SW produktů a PC jsou zapojeny v podnikové síti, pak lze běžně dostupným, specializovaným SW prohledat (proskenovat) systémové registry všech PC a výsledek porovnat s uvedenou databází. Výstupem je seznam všech nelegálně pořízených instalací na jednotlivých počítačích a lze rovněž zcela automaticky vyčíslit cenu nepořízených licencí.

VYSOKÁ ÚROVEŇ ZAHLAZOVÁNÍ DIGITÁLNÍCH STOP KVALIFIKOVANÝMI PACHATELI

Jak praxe ukazuje, největší škody způsobují pachatelé s vysokou odborností v oblasti ICT. Ti znají nejlépe podstatu fungování klíčových informačních technologií, jež jsou předmětem jejich zájmu, způsoby ochrany dat (kterým se musí dokázat vyhnout)

a často i zvyky a chování zaměstnanců a managementu v instituci. Běžnou taktikou hackerů, napadajících počítače, je získání přístupu k administrátorským heslům, které umožňují neomezené činnosti v prostředí operačního systému, databází, informačních systémů, včetně mazání provozních nebo monitorovacích záznamů (tzv. logů) o uživatelských nebo systémových aktivitách. Útočník takto dokáže získat přístupová práva i jiné osoby, používat její uživatelský účet a tím vystupovat pod cizí identitou. V případě odhalení je pozornost svedena jiným směrem.

RESTAUROVATELNOST ZNIČENÝCH DIGITÁLNÍCH STOP

Některé záměrně smazané (zničené) digitální stopy je možné za určitých okolností restaurovat. To není zpravidla možné u jiných druhů kriminalisticky relevantních stop provést. Jednou setřený otisk prstu už nelze obnovit. Digitální restaurovatelnost je dána podstatou fungování operačních systémů výpočetních a komunikačních systémů, které se mohou z pohledu podstaty fungování mezi sebou nepatrně nebo i zcela zásadně lišit. Smažeme-li si soubor ve Windows nebo v poště, lze jej uživatelsky obnovit vytažením z „koše“ nebo z „odstraněné pošty“. Dokonce jsou-li i tyto záznamy uživatelem cíleně odstraněny, v souborovém systémů, jeho fragmentech, zůstávají informace po určitou dobu zachovány a je možné speciálním SW nebo postupy kompletně obnovit!

ORIGINÁLNOST DIGITÁLNÍCH STOP

Datové záznamy, soubory, jejich nosiče lze velice snadno kopírovat, vytvářet jejich duplikáty. Při kopírování nebo přenosu dat nedochází ke ztrátě nebo zkreslení dat. To vyplývá ze samé podstaty digitálních technologií, kde je tato vlastnost požadována. Velice těžko se pak prokazuje, co je originál a co kopie, tedy původnost, originalita důkazu. Ta může být problematická při předkládání důkazů v soudní síni. Problematické rozlišování originálu od jeho kopie může vést v krajním případě při špatném výkladu a vnímání i v nedůvěru vůči elektronickým stopám jako takovým.

Digitální stopy mohou být ve specifických případech lehce měněny, aniž by tyto procesy zanechaly další průkazné stopy této aktivity. Digitální stopy (kopie a/nebo originály) mohou být kdykoliv zničeny (záměrně i nahodile), ať už jsou uloženy na paměťovém médiu nebo právě přenášeny.

Digitální stopy mohou být snadno změněny nebo zničeny i v okamžiku jejich sběru či fixace pro potřeby vyšetřování. Nejsou-li dodržovány standardní postupy při zajišťování digitálních stop, důsledná a kompletní dokumentace, pak je teoreticky možné s digitálními stopami manipulovat. Je zřejmé, že tyto nedostatky je nutné zajistit metodicky a organizačně, aby digitální stopa byla soudně akceptovatelná.

Hovoříme-li o změnách původních digitálních stop, většina z nás si pod tímto procesem zpravidla představuje změnu k horšímu. Ne vždy tomu ale musí tak být. Změny mohou být i velice pozitivní. Představme si, že máme v digitální podobě uloženu fotografii (záběr) velice nízké kvality – špatně exponovaný, rozostřený, s nesprávným vyvážením barev, různými systémovými defekty (kácení svislic architektury, soudkovitost snímku, šum typu „pepř a sůl“ u snímků pořízených s nastavením vysoké citlivosti filmu atd.). Toto vše dnes ale specializovaný SW dokáže odstranit, takže výsledkem je rozpoznatelná tvář osoby nebo SPZ vozidla. Bez softwarové podpory by to dříve nebylo možné realizovat. Zpracování je exaktní, lze jej kdykoliv zopakovat se stejným efektem. Z primární, originální stopy (která nepřinášela žádnou podstatnou informaci) se rázem stává vysoce kvalitní digitální stopa, která přináší nové poznatky do vyšetřování. Totožnost osoby nebo vozidla lze pak dodatečně ověřit i jinými způsoby (např. svědeckými výpověďmi), takže z tohoto pohledu nemusí být v některých případech digitální stopa uznatelná jako primární důkaz, ale přesto ona jediná umožní tento důkaz zabezpečit jinými prostředky.

SOUČASNĚ NÍZKÁ ÚROVEŇ SOUDNÍ AKCEPTACE DIGITÁLNÍCH STOP V PRÁVNÍ PRAXI

Digitální záznamy zachycují obraz, zvuk, nejrozmanitější provozní hodnoty, aktivity uživatelů nebo automatických programů, poskytují hodnoty z přesných měření, datových přenosů apod. Tyto záznamy na rozdíl od lidské subjektivní paměti jsme schopni kdykoliv znova reprodukovat vždy ve stejné kvalitě před libovolně velkou skupinou expertů. Problematickým aspektem digitálních stop je teoretická a v určitých případech i praktická možnost falsifikace a tím jejich zpochybnění. V praxi se častěji setkáváme s lidskými předsudky humanitně vzdělaných osob vyplývající z neznalosti dané problematiky než se skutečnými slabinami vyspělých technologií. Řada informačních a komunikačních technologií je bezpečnostně klasifikována a certifikována, obsahuje dostatečné množství protokolovaných kontrolních mechanismů, takže při dodržování objektivních vyšetřovacích postupů a nakládání se získanými digitálními stopami jsou tyto věrohodným a nezpochybnitelným důkazem o aktivitách, které se odehrály prostřednictvím dané technologie.

LITERATURA

[1] ASHCROFT, J. – DANIELS, D., J. – HART., S., V.: Forensic Examination of Digital Evidence: A Guide for Law Enforcement, Office of Justice Programs, National Institute of Justice, Washington. http://www.ojp.usdoj.gov/nij

[2] CASEY, E.: Digital Evidence and Computer Crime, 2000, Academic Press Elsevier, 1st edition, London, UK.

[3] CASEY, E.: Digital Evidence and Computer Crime, 2004, Academic Press Elsevier, 2nd edition, London, 677 pp. ISBN 0-12-163104-4

[4] CASEY, E.: Handbook of Computer Crime Investigation, 2003, Academic Press Elsevier, 2nd edition, London, 439 pp. ISBN 0-12-163103-6

[5] DOSEDĚL, T.: Počítačová bezpečnost a ochrana dat, Computer Press, 2004, Brno, 190 str. ISBN 80-251-0106-1

[6] HENSLER J.: Computer Crime and Computer Forensics, in Encyclopedia of Forensic Science, 2000, Academic Press, London.

[7] JIRKOVSKÝ, V.: Defacement – graffiti nebo zbraň terorismu, 5th International Conference Information Security Summit, 2004, s.110-116, Tate International, ISBN 80-86813-00-2

[8] MATĚJKA, M.: Počítačová kriminalita, Computer Press, Praha, 2002, str. 102.
ISBN 80-7226-419-2

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

[10] MATOUŠKOVÁ, I.: Psychologie a taktika prosazování investic do informační bezpečnosti ve firemní sféře, Security Magazín, č. 4/2004, str. 48–49.

[11] NEČAS, S.: Lidský faktor a bankovní bezpečnost. Bratislava. Policajná teória a prax č. 2, 2001, s. 84–91.

[12] NEČAS, S.: Personální činnosti v přípravě managementu. Sborník z konference Teoretická reflexe a identifikace společenských potřeb ve vazbě na aktuální problémy policejní praxe, Praha, PA ČR, 2003.

[13] PORADA, V.: Teorie kriminalistických stop a identifikace. Technické a biomechanické aspekty. 1987, nakladatelství Academia, Praha, 328 str.

[14] PORADA, V. a kol.: Kriminalistika, 2001, Akademické nakladatelství CERM, Brno, 737 str.
ISBN 80-7204-194-0

[15] PROSISE, CH., MANDIA, K.: Počítačový útok. Detekce, obrana a okamžitá náprava. Computer Press, Praha, 2002, 410 str.
ISBN 80-7226-682-9

[16] ROWLINGSON, R.: Forensic Readiness – Enabling a Corporate Approach to Digital Evidence, White Paper, QineiQ, 2003, 5 p.

[17] SMEJKAL, V.: Současný stav počítačové kriminality, jejího odhalování, vyšetřování a prevence proti ní. Kriminalistická problematika při odhalování, vyšetřování a prevenci počítačové kriminality, str. 103–120, Policejní akademie, Praha, 1997.
ISBN 80-85981-50-5.

[18] SMEJKAL, V. a kol.: Právo informačních a telekomunikačních systémů, C H Beck, Praha, 2004, 2. vydání, str. 770.
ISBN 80-7179-765-0

[19] WHITCOMB, C., M.: An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, Spring 2002 Volume 1, Issue 1.
www.ijde.org

[20] A Road Map for Digital Forensic Research, Report From the First Digital Research Workshop (DFRWS), August 7–8, 2001, Utica, New York.

[21] 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

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

[23] MUSIL, J.: Projev způsobu spáchání trestného činu ve stopách. Československá kriminalistika č. 2/1978, str. 85.