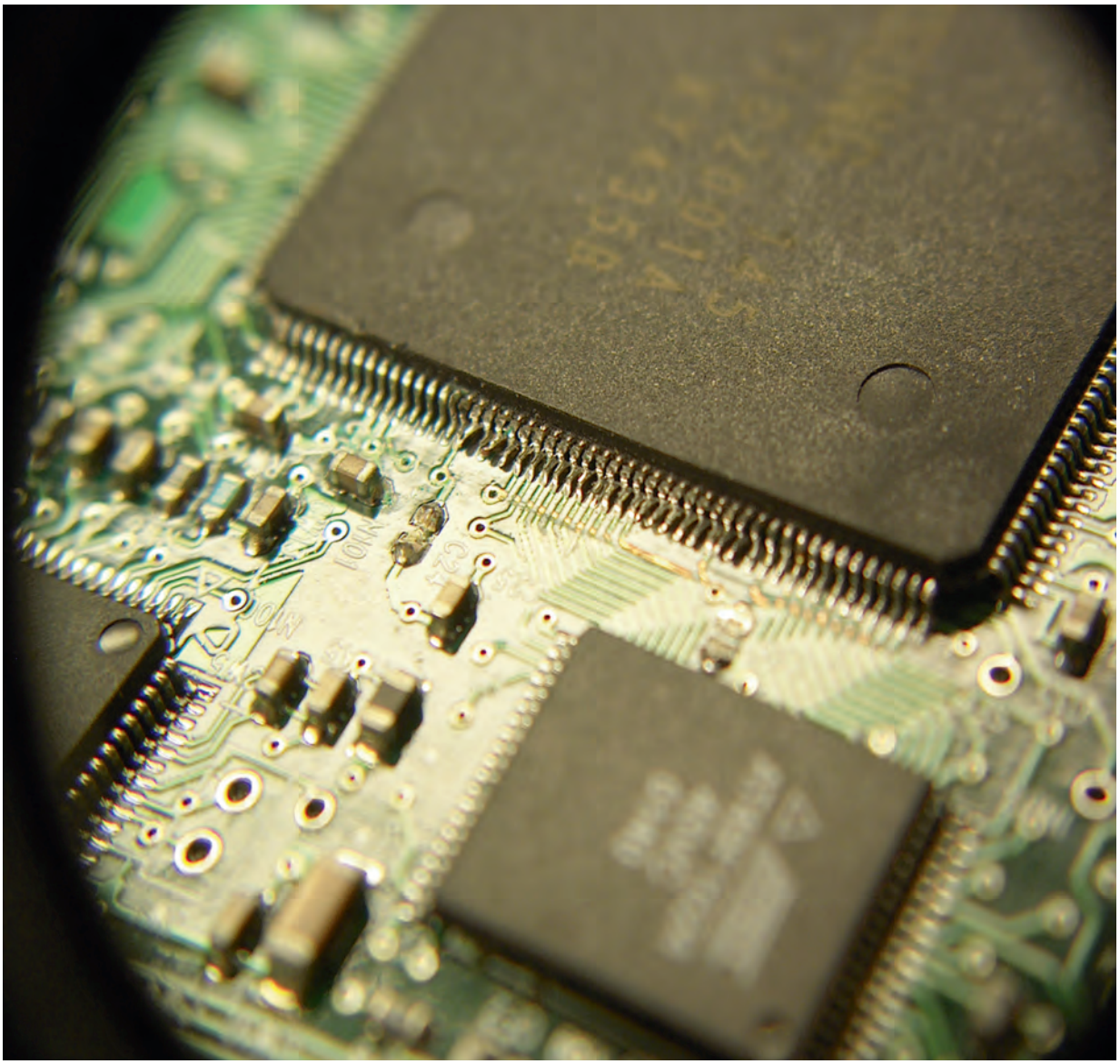
Digital Forensic Journal

2/2015 31. prosinec 2015



Digital Forensic Journal je odborný časopis věnovaný problematice forenzního zkoumání digitálních dat. Zabývá se nejenom problematikou samotného forenzního zkoumání, ale i dalších oblastí souvisejících s digitálními informacemi, s jejich bezpečností, ochranou, zjištěním a zkoumáním.

Znalecký ústav RAC konečně přináší český komplet

DEAT

DIGITAL EVIDENCE ACQUISITION TOOLS

DEAT je přenosná sada, obsahující kompletní sadu nástrojů pro pořizování forenzních binárních kopií dat.
DEAT obsahuje prakticky vše, co můžete potřebovat - od sady redukcía kabelů, přes HW write-blockery pro různé typy disků nebo paměťových médií, až po speciální kopírovací zařízení.
DEAT je možné na přání vybavit i dalšími pomůckami a nástroji, které můžete na místě zajištění potřebovat.
DEAT je unikátně vybaveni nástrojem **DEAS** - forenzním bootovacím CD, které je pro účely práce na místě zajištění vytvořeno v laboratoři Znaleckého ústavu RAC.
Pomocí **DEAT** dostáváte kompletní přenosnou sadu HW a SW nástrojů pro forenzní pořizování kopií dat na místě zajištění.

Digital Forensic Journal

2/2015 31. prosinec 2015

Úvodník

Vážení čtenáři,

předně se omlouváme za zpoždění distribuce tohoto čísla.

Aktuální číslo se vrací v úvodním článku opět k obecnějšímu pohledu na problematiku znaleckého zkoumání. Nevíme, co konkrétně se aktuálně děje, ale bylo možné zaznamenat několik událostí, které svědčí o určitých dalších aktivitách kolem nového zákona o znalcích. Mezi jinými byl poslán k připomínkám nový návrh členění znaleckých oborů. K tomu se vyjadřovat aktuálně nechceme, protože podle našeho názoru to byl pokus opět hodně "pracovní". Právě úvodní článek se zčásti této problematice věnuje, byť to není přímo reakce na zmíněné události.

Z dalšího obsahu Vás chci upozornit na Case Study - popis případu, který skončil díky chybám v práci s digitálními důkazy zrušením rozsuku v plném rozsahu v odvolacím řízení. Doufáme, že bude poučným čtením nejen pro OČTŘ. Když si jej přečte poznáte, že zrušení rozsudku bylo pravděpodobně správné nejenom z formálních důvodů, respektivě z důvodů chyb vyšetřovatelů, st. zástupce a soudce okresního soudu, byť nikomu nechci podsouvat názor na věc. To ani není účelem článku. Jeho cílem je spíše upozornění na základní vlastnosti digitálních důkazů a na správné postupy jejich použití.

Druhým článkem, který by neměl ujít Vaší pozornosti, je návod, jak lze pracovat s obrazem disku, který je chráněn šifrováním pomocí Bitlockeru. Všechny významné forenzní nástroje se sice chlubí, že to umí, ale tento článek uvádí návod, jak to jednoduše udělat pomocí open-source nástrojů pod linuxem. Doufáme, že Vám poslouží jako užitečný návod, protože s použitím Bitlockeru se začínáme setkávat stále častěji a jak jistě odhadnete, lepší to už nebude.

Příjemné a užitečné čtení i ostatních článkůVám přeje Marián Svetlík

Obsah

Risk Analysis Consultants, s.r.o.
Táborská 5
140 00 Praha 4
Tel. + 420 222 360 001
E-mail dfj@rac.cz
Web www.rac.cz/dfj
IČ: CZ 63672774

Digital Forensic Journal (Print) ISSN 2336-4750
Digital Forensic Journal (On-line) ISSN 2336-4769
Ev. č. MK ČR: E 21 763

Ročník 2 / Rok 2015 / Číslo 4 / Vyšlo 31. 12. 2015 v Praze

Zázraky forenzního zkoumání

s podtitulem "**... se nekonají**"

Ing. Marián Svetlík st., vedoucí Znaleckého ústavu RAC, soudní znalec v oboru Kriminalistika, specializace Kriminalistická počítačová expertíza.
svetlik@rac.cz

Anotace:

Na příkladech z prostředí znaleckého zkoumání digitálních dat se budu věnovat obecnější problematice kvality znaleckého zkoumání. Postupně proberu očekávání, která by taková zkoumání měla naplňovat, problémy, se kterými se dnes a denně potkáváme, rozeberu příčiny, které podle mých zkušeností takové problémy způsobují, včetně dopadů jak na použitelnost takových znaleckých posudků, tak na následné postavení a hodnocení znalců a v závěru nastíním možné a hypoteticky i realizovatelné způsoby řešení.

Úvod

Nejdříve je nutné si vyjasnit alespoň jeden základní pojem, který jsem použil v anotaci. Je to „znalecké zkoumání digitálních dat", jinak také pojem „digitální forenzní analýza".

Digitální forenzní analýza je exaktní forenzní věda, která zkoumá procesy a zákonitosti vzniku, existence a zániku digitální informace a interpretuje tyto poznatky na objasňování dějů a procesů s tím souvisejících.

Úmyslně není v definici uvedeno, že se jedná o prostředí počítačů, informačních technologií nebo jinde, protože digitální informace je fenomén, který se vyskytuje i mimo výše uvedených prostředí (respektive museli bychom si nejdříve vyjasnit, co přesně ve vztahu k digitálním informacím znamená pojem počítač, *ale to už by bylo na jiné a mnohem delší pojednání*).

Také není v definici použita klauzule o účelu takové analýzy, byť se v moha obdobných definicích apriori uvádí, že forenzní analýza se používá pro poskytnutí důkazů pro soudy. Jednak to je nadbytečné, protože už z názvu je jasné, že forenzní analýzy vznikly primárně pro tyto účely, a jednak digitální forenzní analýza je unikátní právě tím, že její metody a výsledky nacházejí široké uplatnění i pro další účely, které nemají žádnou přímou souvislost s řešením trestné činnosti.

Původně nechtěným, ale zjevně logickým výstupem výše uvedené definice je na tomto místě asi první veřejná deklarace požadavku, **aby se digitální forenzní analýza oficiálně zařadila jako samostatný znalecký obor do seznamu znaleckých oborů, které vede Ministerstvo spravedlnosti ČR**. Neuváděl bych pro tento obor odvětví, ale jen specializace (jako tomu je aktuálně u oboru „kriminalistika"), stačí se jen podívat do některých prací, které už v poslední době byly i u nás publikovány. Např. specializace „analýza statických dat", „analýza volatile dat - živých dat paměti počítačů", „analýza

síťových dat", „analýza programového kódu", „analýza databázových systémů", „analýza mobilních telefonů" a mohl bych pokračovat až do konce tohoto článku *výčtem specifických skupin digitálních dat*, přičemž každá z nich má svá specifika a vyžaduje speciální vědomosti a zkušenosti.

Očekávání

Asi tím nejdůležitějším očekáváním, které by znalecké zkoumání digitálních dat mělo naplňovat, je jeho pravdivost. Z filozofického pohledu je sice pojem „pravda" pojmem relativním, ale existují určité skutečnosti, které nejsou filozofickými kategoriemi a které mají jednoznačně definované atributy. Například že těleso, které neodráží žádné světlo, je černé nebo že jeden bajt má 8 bitů.

Digitální forenzní analýza je exaktní forenzní technická věda a tedy může jednoznačně dokumentovat existenci nebo neexistenci určitých informací a parametrů. Je jen potřebné si tuto skutečnost uvědomit a dokumentování těchto faktů nekompromisně vyžadovat. Aby nedocházelo k takovým situacím, kdy znalec v oboru kybernetika, odvětví výpočetní technika porovnával dva digitální videozáznamy tak, že si je postupně zobrazoval na monitoru počítače. A aby dodal na přesnosti (a tedy hodnověrnosti svých závěrů) tvrdil, že pro porovnání použil monitor s vysokým rozlišením (který si jako přímý náklad na znalecké zkoumání nechal proplatit).

Pak můžeme očekávat, že digitální forenzní analýza bude splňovat i další obecné parametry, jakými jsou (sice regulativně nevyžadované a tudíž často nedodržované) požadavky na legalitu, integritu, objektivitu, opakovatelnost, přezkoumatelnost a pod. Tyto požadavky jsou sice poměrně často deklarovány v odborných a akademických kruzích, avšak v reálném životě to bývá až neuvěřitelně často jinak. *Ale to je opět problematika, která je na jiné téma a která si vyžaduje samostatné pojednání [1][2].*

Asi jako u každého znaleckého oboru, vyskytují se situace, kdy objektivně zjištěné skutečnosti vyžadují určitou **odbornou interpretaci**, kterou lze podložit v zásadě pouze odbornou zkušeností a odborným názorem znalce. Zdá se být tedy opodstatněným očekáváním, že **objektivní nálezy a odborné názory budou jednoznačně identifikovatelné** a tedy bude možné jejich důkazní sílu hodnotit odděleně, resp. nezávisle (aniž bych přirozeně naváděl, že odborný názor by měl mít apriori menší důkazní sílu než objektivně zjištěná skutečnost). Hodnocení důkazů mi však, jako znalci, nepřísluší. Ale to neznamená, že by nemělo být mou povinností tyto dvě kategorie (objektivní skutečnost a odborný názor) jednoznačně oddělovat [3]. Už jenom proto, že u odborně náročných oblastí nemohu toto oddělení dvou kategorií závěrů nechat na objednateli posudku nebo na soudci.

Z mnoha dalších bych na tomto místě uvedl ještě jedno očekávání. Je jím naplnění požadavku na **opakovatelnost nebo přezkoumatelnost**. Znalecký posudek by měl být opakován nebo přezkoumán vždy, když vzniká jakákoliv pochybnost ohledně použitých metod nebo závěrů. Má to ale jeden podstatný háček, který je způsoben leností a šetře-

ním na nepravém místě. Téměř vždy pro přezkoumání/zopakování zkoumání nelze vytvořit stejné výchozí podmínky, protože nikdo se nenamáhal zachovat vstupní data. Obrazy paměťových médií nebyly vytvořeny vůbec nebo nebyly zachovány, nelze tedy vytvořit stejné výchozí podmínky a tedy ani přezkoumat/zopakovat původní posudek. Původní zajištěná data lze přitom velice jednoduše a levně uchovávat alespoň do doby pravomocného ukončení případu.

Problémy

Postavení znalce je dáno aktuálně platným zákonem z roku 1967 (tedy s platností téměř půl století). Aniž bych vnucoval někomu svůj názor z pohledu praktického výkonu znalecké činnosti za posledních cca 25 let, já vidím znalce podle dikce tohoto zákona, jako osobu kvalifikovanou ve svém civilním oboru a znalectví vykonávající jako koníčka, resp. jako „veřejnou službu" [4].

Přestože je „jmenovací listina znalce" zatížena 1000Kč kolkem jako živnost, k žádné profesionalizaci nedochází, pořád je to „veřejná služba" vykonávaná jako služba státu nebo jako koníček mimo řádného zaměstnání znalce. Aby bylo možné prohlásit, že znalectví je profesí, tak v systému, který je apriori řízen státem, by musely existovat objektivně hodnotitelné profesní kritéria a parametry (viz např. v [5] o hodnocení, str. 10).

Jenže, nezávisle na tom, jak se postavení znalců (ne)vyvíjelo podle zákona už téměř půlstoletí, problematika znaleckého zkoumání doznala (zejména, ale nejenom, v oboru digitální forenzní analýzy) převratných změn, které, alespoň podle mne, již nelze pokrýt stávající dikcí zákona (např. v [5], str. 7).

Aby mohly být naplněny současné požadavky na znalecké posudky, znalci musí být na tak špičkové úrovni, která odpovídá vysoké profesionalizaci jejich práce. Nejenom složitost problematiky (tedy obecná znalost problematiky), ale i specifika metod a postupů již neodpovídají běžným „civilním" profesím. Tak, jako se (pravděpodobně oddělením z kriminalistiky) vyčlenili samostatné vědecké forenzní disciplíny, stejně se **vytvořili specifické plnohodnotné profese - forenzní vědci a forenzní znalci**. A tyto profese už nelze vykonávat jen jako „něco navíc" k běžné civilní profesi, jak to chápe aktuálně platný zákon o znalcích.

Dá se samozřejmě namítat, že nikomu není bráněno, provozovat znalectví jako profesi a že právě proto je jmenovací listina znalce postavena na úroveň živnostenského listu. To by ale nesměla být tato „živnost" takovým restriktivním způsobem ekonomicky regulována státem. I na to by se dal najít argument (a kdo chce, ten vždy najde formální argumenty, které se od zeleného stolu ministerstva zdají být zcela logické), že znalec může vykonávat tuto „živnost" nejenom pro orgány státní moci (kde je stanovena směšná částka za hodinu práce), ale i na smluvním základě pro komerční subjekty. Výsledek takového pojetí, které je odtrženo od reality, je tristní a způsobuje zjevnou nerovnost postavení znalců v různých oborech (blíže viz. [5], str. 6 vlevo dole). Praxe je bohužel taková, že právě ty ekonomicky nejnáročnější obory znalectví reálně nemají velké uplatnění v tzv. „volné kon-

kurenci na trhu", protože je nejvíce využívají právě orgány státní moci kde je jejich odměna restriktivní a naopak, obory, které nejsou až natolik ekonomicky náročné na výkon, mají (paradoxně i ze zákona) dostatek možností uplatnit se i mimo regulované cenové zakázky od orgánů státní moci a tudíž mohou stanovovat smluvní ceny za výkon.

Znalecká činnost je organizována a řízena státem. To vyplývá jak ze zákona, tak např. i z výkladu v [4]. **Prakticky ale stát znaleckou činnost neřídí, pouze stanovuje podmínky zápisu znalců do jakéhosi seznamu nedefinovaných oborů a odvětví a dále stanovuje pravidla využití znalců pro orgány státní moci**.

Asi by se patřilo, abych se hned na tomto místě vyjádřil k použitému pojmu „jakýsi seznam nedefinovaných oborů a odvětví". *Problematika taxonomie znaleckých oborů je oblast, která by (opět, v tomto článku už několikrát) vyžadovala samostatné zkoumání.* Jenomže **jestliže rozdělení znaleckých oborů je jedním ze základních kritérií pro výběr a ustanovení znalce** (a odvozeně pak i pro hodnocení jeho práce), a **jestliže ani tento základní kámen není podložen erudovanou definicí, celý systém, který se od něj odvíjí, je potom postaven na vodě**. Pak už o systému (jako entitě, obsahující vzájemně cíleně a účelově propojené prvky) mluvit nelze. Trochu více je o systému znaleckých oborů pojednáno v [5]. Tady jen uvedu paradox, který se objeví hned po několika kliknutích na web MSp s evidencí znalců.

Když bychom chtěli najít znalce, který by měl zkoumat digitální data, našli bychom např. pojem „výpočetní technika" v oborech ekonomika, elektrotechnika, elektronika, kybernetika a kriminalistika (a možná i v některých dalších, kde jsem už nehledal). Celkem lehce také zjistíme, že máme:

- 75 znalců, kteří mají ve specializaci „výpočetní technika";
- 17 znalců, kteří mají ve specializaci „informační systémy";
- 4 znalce, kteří mají ve specializaci „mobilní telefony".

Ale už nezjistíme, na co specificky se např. znalec na mobilní telefony specializuje, zda ohodnotí závadu tlačítka na mobilu pro účely reklamace nebo prozkoumá možnost „padělat" přijatou výhružnou SMS.

Jaký je tedy rozdíl v tom, když je znalec sice v odvětví "Výpočetní technika", ale pro různé základní znalecké obory, jako je např. "EKONOMIKA" (asi dělá nějaké odhady cen), "ELEKTRONIKA" (asi měří proudy a napětí na číslicových integrovaných obvodech), "ELEKTROTECHNIKA" (asi zkoumá zátěž nebo spotřebu velkých informačních systémů nebo datových center), "KYBERNETIKA" (tady si moc dobře nedovedu představit jeho zaměření vzhledem k definici vědního oboru kybernetiky) nebo "KRIMINALISTIKA" (tady jsem také na vážkách, co by mělo být popisem takového zkoumání a to i přesto, že já sám jsem zapsán v tomto oboru, přičemž odvětví není určeno, pouze specializace je "kriminalistická počítačová expertíza"). Na toto téma je k přečtení také článek [6].

Nedá se říct, že by se zákon o znalcích nenovelizoval. To, že byly přijaty novely, ale nic nemluví o tom, že tyto novely

měly vliv na kvalitu. Přestože se u každé novelizace zákona deklaruje, že je namířena zejména na zvýšení kvality výkonu znalectví (protože to je to, co je na výkonu znalectví kritizováno zejména), o podmínkách zvyšování kvality se určitě nedá mluvit.

Kvalita znaleckého posudku závisí od toho, jaké podmínky jsou vytvořeny k tomu, aby byla naplněna stanovená očekávání (např. ta, která byla uvedena v úvodu tohoto článku). O tom ale zákon mlčí. A, jak už bylo uvedeno výše, opět platí, že jestli chceme něco hodnotit (v tomto případě kvalitu - posudků a/nebo znalců), musíme mít nejdříve stanoveno, podle čeho má být hodnocení realizováno. **Jestliže nejsou stanovena relevantní a měřitelná hodnotící kritéria, nelze nic měřit, výsledek bude vždy jen blábol.** Jestliže jsou znalecké obory jenom deklarovány ale nejsou definovány, nelze pro ně stanovit ani kritéria, podle kterých by měli být jmenováni znalci (kromě velice obecných požadavků). Ale bez takových konkrétních a měřitelných kritérií ani nelze hodnotit kvalitu jejich výkonu.

Forenzní zkoumání je dnes již dávno speciální profese, jen si to mnozí neuvědomují. Když to někdo dělá jako koníčka, nemůže odpovídajícím způsobem plnit náročná kritéria, která se ve světe pro práci znalce používají. Možná nás v mnoha případech situace ve světe nepálí, protože většina řešených případů má jenom lokální dopad v rámci naší jurisdikce. Ale neplatí to paušálně. Kybernetická kriminalita nezná hranice. Když nic jiného, tak alespoň zajišťování a zkoumání digitálních dat musí mít úroveň srovnatelnou ze světem.

Jestliže ve světě jsou obecně známá kritéria a požadavky na práci s digitálními stopami a u nás je to doslova pole neorané, jak potom můžeme spolupracovat na mezinárodním poli? Jak vypadají výsledky práce našich znalců, když:

► jejich odbornost je u nás posuzována paušálně a obecně (viz předchozí kapitola);
► specifické forenzní vzdělávání neexistuje (ono už ve světě celkem běžně existuje, jenomže za odměnu, kterou znalec od státu za svoji práci dostává, si takové vzdělání nemůže dovolit, nemluvě o tom, že k tomu potřebuje (mimo prostředků) jako minimální požadavek také dobré jazykové vybavení);
► neexistuje podle oborů osvěta, výměna a předávání zkušeností (a když, tak jenom jako individuální aktivita několika zapálených dobrovolníků, ale na tom se systém budovat nedá);
► ohodnocení práce znalce je marginální (na úrovni 14% průměru EU, jsme poslední v EU, a na ostudné úrovni minimální mzdy Německa).

Jaké výkony potom za takovýchto podmínek lze od znalců očekávat?

Když to dovedeme do důsledků - **stát zneužívá odbornost, vědomosti a zkušenosti znalců, které tito získali dlouholetou vlastní pílí**. Znalec, aby udržel špičkovou profesní úroveň a byl schopen podávat kvalitní znalecké posudky (jinak mu hrozí ze zákona sankce), investuje značné prostředky do svého vlastního vzdělávání, do přístrojové techniky, která je pro výkon nutná, do prostor pro výkon znalecké činnosti, do své jazykové výbavy, protože v ČR se k posledním poznatkům forenzních věd prakticky nedostane. Jsou to stovky tisíc ročně. Jediné, co je stát ochoten uhradit, jsou prakticky pouze

přímé náklady na zpracování posudku a ušlý čas, který při zpracování posudku stráví a i to jenom na úrovni platu řemeslníka. Nebudu se na tomto místě ani snažit rozebírat, jaké možnosti má znalec, aby si přeúčtoval např. 100 stránek barevně potištěného papíru a dalších 200 stran, které spotřeboval v průběhu zkoumání, amortizaci počítače apod. A o té skutečné realitě proplácení jednotlivých znaleckých úkonů orgány státní moci tady vůbec ani nechci hovořit, je to často až ponižující.

Investice do odborné kvality a do prostředků, které pro výkon znalectví znalec potřebuje (aby se minimálně sám před sebou nemusel stydět), musí získat jinde, v rámci své „civilní" profese. Tím se ochuzuje o řádně vydělané prostředky, které by jinak použil pro svoji vlastní potřebu. On to ale je nucen (fakticky ze zákona) investovat do toho, aby zajistil kvalitu své znalecké práce.

Právě v tom je zásadní rozpor aktuálně platného zákona o znalcích. V chápání postavení znalce. Před bezmála padesáti lety byly jiné podmínky a i postavení znalce bylo jiné, na znalce byly kladeny objektivně jiné nároky, byla to prostě úplně jiná situace. Dnes stát, prosazováním stejného přístupu k výkonu znalectví, diskriminuje znalce odborně a ekonomicky a pokřivuje základní zásady fungování naší společnosti.

Aby to nebylo jenom obecné povídání a nebylo to chápáno jako stěžování si, dovolím si odkaz na vývoj situace v oblasti digitální forenzní analýzy za posledních 10 let [7]. **Na v článku uvedeném příkladě je vidět, jak současná dikce zákona o znalcích vůbec není schopna pokrýt reálnou situaci**. Dopady takového přístupu k výkonu znalecké činnosti jsou zřejmé. Ani desetinásobné pokuty za nekvalitní výkon znalecké práce nezapůsobí na její úroveň, ba naopak, bude způsobovat její degradaci a jen ještě víc odborníků opustí řady znalců.

Jak řešit problém?

Pro řešení složitých problémů neexistují jednoduché recepty. Při úvahách možného řešení, tedy průběžného a trvalého zajišťování kvality znaleckého zkoumání a jejího neustálého dalšího zdokonalování, je potřebné udělat politické (resp. strategické) rozhodnutí, kdo bude mít tuto oblast na starosti, resp. kdo bude za ni odpovědný.

V současnosti to je MSp ČR, které řídí výkon znalecké služby ze zákona a které stanovuje veškerá další kritéria a požadavky pro realizaci tohoto výkonu. Platí tedy, že v ČR je výkon znalecké služby řízen výhradně státem.

Nabízejí se i další modely, které jsou běžně v Evropě používané, a to řízení znalectví pomocí profesní komory (ať už zřízené ze zákona nebo na dobrovolné bázi) nebo ponechání výkonu znalectví na znalcích samotných (resp. na tržních principech). Všechny modely se v Evropě používají (byť u nás z historických důvodů nemají veké nebo dokonce žádné tradice).

Rozhodnutí, kdo bude mít odpovědnost za znalectví v ČR, ale je možné učinit až poté, co budou známá všechna kritéria a požadavky, která se na fungující systém (a tady cíleně myslím systém jako

souhrn prvků a jejich vzájemných vazeb, vytvořený s určitým cílem) vztahují. Není mi známo, že by se u nás někdo takový fungující systém pokoušel byť i jenom navrhnout, ne to vytvořit. Pro takové tvrzení mám minimálně jeden důležitý argument:

Jestliže mají znalci vykonávat znaleckou činnost kvalitně a na úrovni současných vědeckých požadavků, musí být vytvořeny podmínky, aby takové vědecké požadavky byly znalcům dostupné, aby byl někdo schopen je implementovat jak do našeho právního prostředí, tak do technických a procesních podmínek, odpovídajících naší současné situaci. Nikdo takový u nás není.

Formálně by to sice mohla být např. Policejní akademie ČR, Kriminalistický ústav PČR nebo nějaká jiná akademická instituce nebo třeba i státem zřízený ústav, ale žádnou takovou instituci, která by cíleně pokrývala požadavky na rozvoj a implementaci forenzních věd do znalecké, kriminalistické a soudní praxe neznám. Asi stát nemá na tom zájem?

Teprve až budou známy parametry systému (nazveme jej s velkým S - „Systém výkonu znalecké činnosti") lze zodpovědně zvážit, jakým způsobem je možné takový Systém (byť postupně) realizovat v praxi. Více je tato otázka rozebírána např. v [8].

Takže bychom měli teď zapomenout na žabomyší války o tom, jestli má být pokuta za špatně vedený znalecký deník 1000 nebo 100 000 Kč nebo zda by měl být znalec komerčně pojištěn a na jakou částku, a na podobné prkotiny.

Závěr

Jsem přesvědčen, že právě problematika digitálního forenzního zkoumání, díky své dynamice vývoje, šíři záběru, novosti přístupu, širokému uplatnění nejenom v trestním řízení a dalším specifickým vlastnostem, vyvolává ve stojatém rybníce našeho znalectví vlnobití.

Dynamický obor zkoumání digitálních dat se neslučuje se zkostnatělým přístupem a salámovou metodou přizpůsobování platného zákona o znalcích novým podmínkám. Takový přístup k řešení systému výkonu znalectví nemůže přinést žádný pokrok.

Zaváděním různých „opravných kliček" do nefungujícího systému nezpůsobí jeho zkvalitnění - naopak - povede k ještě větším problémům. Při neznalosti reality vždy (byť i drobná) změna v jedné entitě systému způsobí mnohdy výraznou a nepredikovatelnou změnu v úplně jiné jeho části.

Nechci tvrdit, že stát by se měl vzdát své role v oblasti řízení výkonu znalectví v ČR. Aby ale systém fungoval podle záměru jeho tvůrce, takový systém musí být nejdříve profesionálně navržen a posléze nalezen optimální způsob jeho realizace. Tím, že (např. jako na Slovensku) lehce „zmodernizujeme" stávající pojetí zákona o znalcích, nevyřešíme ten základní problém - problém vytvoření podmínek pro neustálé zvyšování kvality znaleckého zkoumání.

Literatura

[1] Svetlík, M., Digitální forenzní analýza a bezpečnost informací, Data Security Management, ISSN 1211-8737, 1/2010, str. 20-23.

[2] Hološka, J.,Svetlík, M., Sedm hříchů digitální forenzní analýzy, Digital Forensic Journal, ISSN 2336-4750, 2/2014, str. 5-11

[3] Porada, V., Bruna, E., Digitální svět a dokazování obsahu elektronických dokumentů, Bezpečnostní technologie, systémy a management, 11. - 12. září 2013, UTB ve Zlíně, dostupné z http://trilobit.fai.utb.cz/Data/Articles/PDF/37bacb88-3602-4ea7-b9c8-7864970f89e7.pdf

[4] Musil, J., Hodnocení znaleckého posudku, Kriminalistika, ISSN 1210-9150, 3/2010

[5] Svetlík, M., Profesionalita znaleckého zkoumání, Digital Forensic Journal, ISSN 2336-4750, 1/2014, str. 5-14

[6] Svetlík, M., Kolik máme soudních znalců. [online], 5. 3. 2013. Dostupné z: https://msvetlik.wordpress.com/2013/03/05/kolik-mame-soudnich-znalcu/

[7] Hološka, J., Svetlík Jr., M., Kam kráčí digitální forenzní analýza, Digital Forensic Journal, ISSN 2336-4750, 1/2014, str. 29-32

[8] Svetlík, M., Kriminalistická technika, znalectví a forenzní vědy, sborník příspěvků konference „Počítačová kriminalita - juristické, kriminalistické a kriminologické aspekty", Košice, 2014, ISBN 978-80-8152-146-1

Práce s E01 obrazem disku s obsahem šifrovaným pomocí Bitlockeru.

Ing. Jiří Hološka, Ph.D., bezpečnostní specialista ve společnosti PwC

Anotace:

Článek popisuje způsob zpřístupnění šifrovaného diskového oddílu zajištěného ve forenzním obrazu disku E01. Zkoumaný pevný disk obsahuje dva souborové oddíly z čehož jeden je zašifrován nástrojem Bitlocker.

Úvod

Základem digitální forenzní analýzy je zajistit aktuální stav paměťového média a zabezpečit obsah zajištěného média proti náhodné, nebo nechtěné změně.

Reálně je tohoto stavu dosaženo vytvořením bitové kopie, nebo forenzního obrazu disku (E01, AFF, S01). Rozdíl mezi bitovou kopií a forenzním obrazem disku je v použití komprimace u forenzního obrazu disku a CRC kontrolních součtů uvnitř obrazu disku.

Zpřístupnění dat z forenzního obrazu disku je závislé na specializovaných nástrojích, které automaticky převedou komprimovaná data na formát bitové kopie, v odborné literatuře je tento formát označován jako raw image, nebo flat-file image.

Situace se může ještě dále zkomplikovat pokud je paměťové médium chráněno šifrováním.

Zpřístupnění provedeme pod operačním systémem GNU /Linux, konkrétně Debian 6.

Postup

Prvním krokem je nainstalovat nástroje pro práci s E01 obrazy a nástroj Dislocker na dešifrování Bitlockeru.

```
# sudo apt-get update
# sudo apt-get install git ewf-tools libfuse-dev
# git clone https://github.com/Aorimn/dislocker.git
# cd dislocker
# make
# make install
```

Dále je nutné vytvořit tři adresáře které se v linuxové terminologii nazývají mount-pointy.

```
# mkdir /mnt/ewf /mnt/bitlocker /mnt/windows
```

Tyto mount-pointy budou sloužit k přístupu k obrazu disku dat v různých stádiích zpřístupňování šifrovaného souborového oddílu.

Prvním krokem je rozbalení E01 obrazu na formát raw image.

```
# ewfmount test_disk.E01 /mnt/ewf/
```

ewfmount 20140608

Po připojení je možné otestovat výsledný obraz disku pomocí nástroje fdisk, který nám zobrazí rozložení diskových oddílů.

```
# fdisk -l /mnt/ewf/ewf1

Disk /mnt/ewf/ewf1: 128.0 GB, 128035676160 bytes
255 heads, 63 sectors/track, 15566 cylinders, total 250069680 sectors
```

```
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0xca8360ef

Device Boot      Start         End      Blocks   Id  System
/mnt/ewf/ewf1p1   *          2048       206847   102400    7  HPFS/NTFS/exFAT
/mnt/ewf/ewf1p2            206848    250066943   124930048    7  HPFS/NTFS/exFAT
```

První oddíl (ewf1p1) je nešifrovaný a obsahuje informace nutné pro zavedení operačního systému, který se nachází na šifrovaném oddílu.

Druhý oddíl (ewf1p2), obsahuje operační systém Windows a uživatelská data.

U fyzického pevného disku by jednotlivé oddíly souborového systému byly identifikovány jako **/dev/sda1 /dev/sda2**, ale v případě obrazu disku je to pouze jeden soubor (**/mnt/ewf/ewf1**). Proto je nutné začátek šifrovaného oddílu identifikovat pomocí takzvaného offsetu. Offset udává vzdálenost v bytech od začátku disku k začátku vybraného souborového oddílu a lze snadno vypočítat z výše zmíněného výstupu nástroje fdisk.

```
Units = sectors of  1 * 512 = 512 bytes
Device  Boot                              Start
End                           Blocks         Id
System
/mnt/ewf/ewf1p2            206848    250066943   124930048    7  HPFS/NTFS/exFAT
```

Z výpisu víme, že jeden sektor na disku má velikost 512 byte, dále víme, že šifrovaný oddíl začíná sektorem 206848. Offset pro druhý diskový oddíl je 512 * 206848 = 105906176.

Po získání offsetu šifrovaného diskového oddílu je možné tento oddíl dešifrovat, dešifrování se provádí podobným způsobem jako převedení E01 na flat-file.

Pro dešifrování použijeme následující příkaz nástroje Dislocker:

```
dislocker -v -o 105906176 -V /mnt/ewf/ewf1 -p111111-222222-333333-444444-55555-666666-777777-888888 -- /mnt/bitlocker/
```

Parametry:
-o je offset šifrovaného oddílu disku

-V /mnt/ewf/ewf1 udává flat-file soubor s rozbaleným E01 obrazem disku

-p111111-222222-333333-444444-55555-666666-777777-888888 je recovery klíč, který byl vygenerován při zašifrování diskového oddílu.

/mnt/bitlocker/ - je mount point ve kterém bude zpřístupněn dešifrovaný diskový oddíl.

V případě že by obraz disku obsahoval více jak jeden šifrovaný diskový oddíl, bylo by nutné každý jeden oddíl připojit samostatně.

Stejně tak pokud by obraz disku obsahoval další nešifrované diskové oddíly bylo by nutné je připojit samostatně pomocí vypočítaného offsetu a příkazu:

```
mount -o loop,offset=123456,ro /mnt/ewf/ewf1 /mnt/windows2/
```

V našem případě máme jen jeden diskový oddíl s daty, který jsme již rozbalili z E01 na flat-file, dále jsme tento oddíl exportovali a dešifrovali. Zbývá připojit souborovou strukturu NTFS do adre-

sářové struktury OS Linux.

Pro připojení souborové strukruty použijeme příkaz mount:

```
# mount -o loop,ro /mnt/bitlocker/dislocker-file /mnt/windows/
```

Ověření

Dostupnost souborů ověříme pomocí příkazu ls:

```
# ls /mnt/windows/
```

```
$Recycle.Bin
Oracle
System Volume Information
Config.Msi
PerfLogs
Users
Documents and Settings
Program Files
Windows
Install
Program Files (x86)
hiberfil.sys
Intel
ProgramData
pagefile.sys
MSOCache
Recovery
temp
```

Výpis souborů zobrazuje root systémového disku s operačním systémem Windows. Konkrétně se jedná o 64 bit verzi systému Windows 7.

XRY COMPLETE

THE ALL-IN-ONE MOBILE FORENSIC SYSTEM FROM MICRO SYSTEMATION

> CO JE XRY COMPLETE

XRY COMPLETE JE ALL-IN-ONE ŘEŠENÍ PRO MOBILNÍ FORENZNÍ ANALÝZU OD ŠVÉDSKÉ SPOLEČNOSTI MICRO-SYSTEMATION, KOMBINUJÍCÍ NÁSTROJE PRO LOGICKOU I FYZICKOU EXTRAKCI DO JEDINÉHO BALÍČKU. XRY COMPLETE UMOŽŇUJE FORENZNÍM EXPERTŮM PŘÍSTUP KE VŠEM METODÁM ZÍSKÁVÁNÍ DAT Z MOBILNÍCH ZAŘÍZENÍ.

> ŠIROKÉ MOŽNOSTI EXPORTU

>> Excel
>> Word
>> Open Office
>> XML
>> Google Earth
>> tiskové sestavy

> XRY COMPLETE OBSAHUJE

>> XRY software a licenční klíč
>> kufřík s organizérem na kabely
>> XRY komunikační jednotka
>> XRY Logical kit kabelů
>> XRY Physical kit kabelů
>> SIM id-Cloner s 12 měsíční licencí
>> 10 SIM karet pro id-Cloner
>> čtečku karet s ochranou proti zápisu
>> 12 měsíční licence
>> XACT hex prohlížeč
>> XRY Reader aplikaci
>> čistící kartáček
>> přístup k podpoře zdarma
>> veškeré upgrade SW zdarma
>> dodání kabelů k novým zařízením zdarma

> PRODEJ A PODPORA V ČR

RISK ANALYSIS CONSULTANTS, S.R.O.
Táborská 5, Praha 4
zu@rac.cz

RAC®

www.rac.cz

Fatal Error

Case Study případu, který skončil osvobozujícím rozsudkem

Ing. Marián Svetlík st., vedoucí Znaleckého ústavu RAC, soudní znalec v oboru Kriminalistika, specializace Kriminalistická počítačová expertíza.
svetlik@rac.cz

Anotace:

Tento příspěvek popisuje vyvrcholení kauzy jednoho soudního sporu, ve kterém se jednalo o přečin neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 odst. 1 tr. zákoníku a ve kterém klíčovým důkazem byla právě digitální data.

Úvod

Přestože rozsudek v případu je pravomocný, celou kauzu budu anonymizovat. Nejde totiž o konkrétní osoby nebo subjekty, ale právě o digitální důkazy, jejich použití v rámci vyšetřování a použití u soudu.

Předesílám a zdůrazňuji už předem, že v tomto příspěvku nejde o to, co se ve skutečnosti v tomto případě stalo nebo nestalo, kdo ze zúčastněných co udělal nebo neudělal, to je záležitostí soudu a jeho rozhodování. Mně jde jenom o to, jakým způsobem se pracovalo s digitálními důkazy.

Rozsudek

Zacituji z rozsudku[1] krajského soudu:

Rozsudek jménem republiky

Krajský soud … projednal ve veřejném zasedání … odvolání obžalovaného … proti rozsudku Okresního soudu … a rozhodl takto:

Z podnětu odvolání obžalovaného se napadený rozsudek podle § 258 odst. 1 písm. a), b), d) tr. řádu zrušuje v celém rozsahu a podle § 259 odst. 3 tr. řádu se nově rozhoduje tak, že se obžalovaný … podle §226 písm. c) tr. řádu

zprošťuje

obžaloby pro skutek spočívající v tom, že v přesně neurčené době… překonal bezpečnostní opatření a získal tak neoprávněný přístup k počítačovému systému, v němž byl obžalobou spatřován přečin neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 odst. 1 tr. zákoníku,

neboť nebylo prokázáno, že tento skutek spáchal obžalovaný.

[1] Pro ty, kdo by chtěl zjistit detaily uvádím, že se jedná o rozsudek Krajského soudu v Hradci Králové, pobočka Pardubice, 14To 312/2015-615

Co k takovému rozsudku nakonec vedlo?

Popíši ve stručnosti celou kauzu, přičemž se tady budu věnovat pouze nezbytně nutné míře detailu a zejména skutečnostem, které se vztahují k digitálním datům (i když digitální důkazy jsou v tomto případě klíčovými).

Následuje popis případu přibližně tak, jak je zadokumentován ve spisu, zejména z pohledu obžaloby.

Případ

Náš případ se týká dvou firem (pro naše účely si je nazveme A a B), které podnikají na regionální úrovni ve stejné nebo velice podobné oblasti služeb a které si tedy zcela zjevně konkurují.

Tento konkurenční boj se projevoval různým způsobem, zejména ale vzájemným přetahováním si obchodních zástupců. Lze si dobře představit, že přechodem obchodního zástupce z jedné konkurenční firmy do druhé vznikne také celá řada problémů v tom, jakým způsobem se vypořádat s klientelou, kterou měl ten který obchodní zástupce na starosti.

Firma B, jak se v určitém období zdálo, získávala na svoji stranu stále více klientů na úkor firmy A a nakonec firma A došla k závěru, že to musí být tím, že firma B nějakým způsobem získává jejich interní obchodní informace. Firma A se tedy rozhodla najmout soukromého detektiva, aby se pokusil zjistit, jestli a případně jakým způsobem se jejich informace dostávají ke konkurenci, tedy k firmě B.

Dotyčný soukromý detektiv si na tuto odbornou činnost sjednal svého známého, odborníka na výpočetní techniku, který provedl ve firmě A šetření. Výsledkem bylo konstatování, že někdo nainstaloval do firmy A keylogger, který odesílal na e-mailovou adresu xxx@seznam.cz množství informací z počítačů firmy A.

Aby se zjistilo, kdo schránku xxx@seznam.cz vybírá, odborník na výpočetní techniku ve službách soukromého detektiva poslal do této schránky několik tzv. „trasovacích" e-mailů, které při otevření jejich obsahu zaslaly zpět odesílateli IP adresu počítače, který takový e-mail otevřel. Takto získanou IP adresu identifikovali jako adresu z adresního prostoru poskytovatele internetu, který mezi jinými poskytoval internetové připojení i firmě B. Tyto skutečnosti vedly firmu A k podání trestního oznámení na firmu B za průnik do jejich systému a zneužití jejich interních informací.

Policie na základě tohoto oznámení zajistila vytipované počítače firmy A a předala je ke zkoumání znalci XYZ, který v podstatě potvrdil nález soukromého detektiva ohledně existence keyloggeru.

Policie také zjistila prostřednictvím společnosti seznam.cz IP adresu, ze které byl poslední přístup ke schránce xxx@seznam.cz a potvrdilo se, že to bylo z adresy, která v té době byla poskytovatelem přidělena firmě B.

Na základě těchto informací následně policie zajistila i vybrané počítače (resp. obrazy disků těchto počítačů) ve firmě B

a tyto také předala znalci XYZ ke zkoumání s cílem zjistit, zda se na těchto počítačích nacházejí nějaká data pocházející z činnosti programu keylogger a zda bylo z těchto počítačů přistupováno ke schránce xxx@seznam.cz. Znalec zjistil, že na zkoumaných počítačích byly nalezeny soubory, které „mohly potenciálně souviset s činností" programu keylogger, že jejich struktura se podobá souborům, které byly nalezeny ve firmě A a byla také nalezena informace o přístupu k e-mailové schránce xxx@seznam.cz.

Na základě takto shromážděných informací a důkazů (přirozeně včetně dalších informací, výslechů svědků, listin a pod.) policie obvinila majitele firmy B z výše uvedeného trestného činu a okresní soud dotyčného i za tento trestný čin odsoudil. Na základě odvolání, které podal obžalovaný, jej však krajský soud zprostil obžaloby.

Odvolání

Aniž bychom se pouštěli do právního výkladu detailů, projděme si postupně zejména zásadní technické a odborné problémy, které krajský soud ve svém rozhodnutí uznal a které vedly ke zprošťujícímu rozsudku.

Zásadní námitkou obžalovaného, s níž se krajský soud zcela ztotožnil, je fakt, že ještě v době přípravného řízení došlo ke smazání bitových kopií harddisků ze všech zkoumaných počítačů, a to v době, kdy ještě ani nebyla podána obžaloba a u obžalovaného tak výrazným způsobem došlo ke krácení jeho práva na obhajobu.

Krajský soud ve svém rozhodnutí dále konstatoval, že *„Navíc šlo o zásadní důkaz, na kterém v podstatě stálo celé obvinění a pokud mělo být podkladem pro případné odsouzení obžalovaného, neexistoval jediný důvod pro smazání důkazu tak zásadního významu."* a dále uvádí zásadní vyjádření, že ***„Nelze připustit, aby do pravomocného skončení věci došlo k odstranění v podstatě zásadního důkazu, který by mohl řadu věcí z hlediska objektivity posoudit."***

Na tomto místě je potřebné zdůraznit, že vše, co může napomoct k objasnění věci, je možné považovat za důkaz. Z tohoto pohledu se na obrazy disků lze dívat jako na stopu i jako na důkaz. Digitální stopy, zejména ve formě obrazů disků, jsou stopami komplexními, obsahujícími nesmírné množství velice různorodých informací.

Obhajoba si nechala zpracovat znaleckým ústavem[2] další znalecký posudek, ze kterého jednoznačně vyplývá, že:

► ***Každá aktivita, která je prováděna v prostředí informačních systémů, zanechává v tomto prostředí digitální stopy***. *A je jedno, zda takové aktivity provádí oprávněný nebo neoprávněný uživatel, zda je to aktivita lokálního uživatele nebo činnost uživatele vzdáleného, pracujícího na dálku, např. s využitím internetu, nebo zda je to nějа-*

[2] Znalecký ústav společnosti Risk Analysis Consultants, s.r.o. (www.rac.cz/zu)

ká automatická funkcionalita samotného informačního systému.

► ***Většinu digitálních stop, které takovou aktivitou vznikají, lze identifikovat, zkoumat a interpretovat jejich význam**, příčinu a původ vzniku takových stop, jejich existenci a případné modifikace v čase, jakož potenciálně i jejich zánik či jejich definitivní zničení, ať už je zaviněné (cíleným působením uživatele) nebo nezaviněné (běžnou činností informačního systému).*

► ***Pravděpodobnost možnosti identifikace digitálních stop závisí na mnoha okolnostech**, zejména na tom, zda se tyto stopy zachovají, v jakém čase od doby zjišťované události došlo k zajištění digitální stopy, a mnoha dalších.*

► ***Informační systémy uchovávají ohromné množství různých informací**, jenom část z nich jsou data operačního systému a zpravidla ještě menší část tvoří uživatelská data. Dá se říct, že podstatnou část dat, která se v informačních systémech uchovávají, jsou tzv. metadata, která právě uchovávají informace o chodu informačního systému a o událostech, které v něm probíhají. Tato data vznikají zpravidla bez vědomí uživatele a uživatel je bez speciálních znalostí může jen těžko ovlivnit, měnit nebo jen těžko zcela zamaskovat svoji činnost. Navíc, v závislosti od konkrétního operačního systému, se metadata ukládají na různých místech a mnohdy i v několika nezávislých kopiích nebo modifikacích záznamů o té samé aktivitě, na různých místech a v různých formátech, často se vytvářejí souvislé řetězce informací o informacích.*

► ***Aby bylo možné při zkoumání digitálních dat zjistit souvislosti a veškeré další skutečnosti, provádí se při zajištění binární kopie datových nosičů**. Taková kopie obsahuje právě veškerá data, která jsou v informačním systému uložena a to dovoluje zkoumat nejenom uživatelská data, ale i metadata a dovozovat tak další souvislosti o dějích a procesech, které jsou důležité pro šetření věci.*

► *Další důležitou skutečností je fakt, že na současné úrovni možností **zpravidla nelze z digitálních stop zjistit konkrétní fyzickou osobu, která prováděla konkrétní aktivity v informačním systému**. Aktuálně je potenciálně možné identifikovat uživatelský účet, po kterým aktivita probíhala, jestliže však jsou uživatelské účty v systému zavedeny a používány.*

I v prostředí digitálních systémů a digitálních stop platí dobře známý Locardův princip[3]. Nestačí pouze konstatovat, že při domovní prohlídce byla nalezena zbraň kalibrem odpovídající vražedné zbrani, ale je nutno zkoumat i veškeré další souvislosti a stopy, aby bylo možné jednoznačně prokázat, zda a jakou souvislost má nalezená zbraň s činem a kdo a jak ji použil apod.

To samé platí i o nálezech dat v informačních systémech. Skutečnost, že se někde nějaký důležitý soubor nachází, ještě není dostačující. Je potřeba vyvrátit potenciální pochybnosti o způsobu, jakým soubor vznikl, případně jakým způsobem se soubor do systému dostal, kdy to proběhlo nebo mohlo proběhnout, dát do souvislostí nejenom existenci

[3] https://cs.wikipedia.org/wiki/Locardův_princip_výměny

informace, ale i procesy spojené s jejím vznikem, případnými úpravami, zpracováním a případně také zánikem.

Mějme na paměti, že vše, co se v systému děje, potenciálně zanechává stopy a je jen otázkou našeho poznání, zda jsme takové stopy schopni včas a korektně zajistit a následně správně odzkoumat a interpretovat.

Je s podivem, že u tzv. „klasických" stop, tedy materiálních, hmatatelných (jako je i výše zmíněná vražedná zbraň), je běžnou praxí, že se zjišťují veškeré možné souvislosti (vlastník, daktylky, DNA, povýstřelovky apod.), ale u digitálních stop to napadne jenom málokoho.

Když předložené digitální důkazy (např. nález souborů odpovídajících práci keyloggeru na počítači firmy B) přirovnáme k případu s vražednou zbraní, vychází nám tvrzení, že nález takových souborů odpovídá tak přibližně střelné zbrani odpovídajícího kalibru. S tím by policie bez dalšího u soudu určitě neuspěla tím spíše, kdyby předložila jako důkaz ne zbraň samotnou, ale pouze prohlášení, že zbraň měla odpovídající kalibr, a zbraň samotnou by zničila.

Okresní soud při argumentaci ohledně zničení obrazů disků ještě v době přípravného řízení dovozuje, že to mohlo být způsobeno novostí problematiky. Taková argumentace se však jednoznačně nezakládá na pravdě, protože základy problematiky vyšetřování trestné činnosti v prostředí digitálních dat byly v Evropě a paralelně i v ČR[4] položeny již v první polovině devadesátých let minulého století (tedy minimálně před dvaceti lety) a jedním ze základních postulátů takové práce bylo právě pořizování obrazů disků jako základní východiskový materiál pro znalecké zkoumání a také základních zásad[5] práce s takto získanými stopami.

Teoreticky bychom mohli i akceptovat takovou argumentaci protože musíme připustit, že u policie existuje značná fluktuace a že tato odbornost není v osnovách policejních škol. Tím se (pravděpodobně nesystémově získané) odborné poznatky šíří v policii značně pomalu. Nelze však takové jednání připustit už z obecného pohledu, totiž že obrazy disků byly vlastně klíčovými důkazy v celém případu a jednalo se tedy o zničení klíčového důkazu. To se nesmí stávat ani v případě, že odborně není policie na takové úrovni, aby pochopila složitosti digitálních stop. Jednou to je klíčový důkaz obžaloby a tedy nesmí být zničen.

Je nutné připomenout, že nahradit komplexní stopu, jakou obraz disku je, pou-

[4] Oficiálně by se dalo považovat za takové datum rok 1998, kdy z iniciativy Kriminalistického ústavu Praha PČR vznikla v Praze evropská pracovní skupina pro forenzní analýzu digitálních dat při ENFSI (www.enfsi. org). Nicméně základy pro vznik evropské skupiny byly položeny v Praze dávno před tím, již počátkem let devadesátých.

[5] Minimálně dále zmíněné pravidlo, že originál a kopie digitální stopy jsou identické a že je nutné udržovat vždy dvě nezávislé kopie digitálních dat právě z důvodu jejich ochrany před nečekaným zničením.

hým jediným znaleckým posudkem, který se zabývá pouze zlomkem informací, které jsou na disku uloženy, je nepřípustné[6].

Složitost digitálních dat, které jsou v obrazu disku uloženy, se nedá podchytit jediným, ani velice podrobným znaleckým zkoumáním. Každé takové zkoumání podchytí pouze zlomek informací a faktů a pouze z určitého úhlu pohledu. I když příklady a přirovnání vždy pokulhávají, dá se to připodobnit tomu, jakoby někdo chtěl nahradit zvukový záznam odposlechu telefonního hovoru pouhým přepisem jenom některých vybraných pasáží a původní zvukový záznam by zničil.

Když si představíte, že v počítači je takových a analogických záznamů, souborů a informací stovky tisíc, lze dovodit, že zničení takového obrazu disku způsobí zničení nepřeberného množství informací, které potenciálně mohou poskytnou další důkazy, které mohou pomoct objasnit, doplnit, upřesnit nebo i vyvrátit určité předpoklady.

Aniž bych podsouval jakýkoliv záměr při vedení vyšetřování tohoto případu, vyvstává ještě otázka, zda vyšetřování bylo vedeno objektivně, tedy zda byly správně a nezávisle postavené vyšetřovací verze. Nabízí se totiž také otázka, proč nebyla zkoumána také možnost, že vše mohlo být naopak, a (jak mimochodem tvrdí i obhajoba) vše mohlo být zinscenováno a důkazy byly firmě B podvrženy ať už přímo firmou A nebo někým třetím. Taková varianta se při konkurenčním boji nabízí zcela přirozeně, avšak z dokumentace, která byla k dispozici při tvorbě tohoto článku, nic nenasvědčuje, že by takováto varianta byla prošetřována. Potvrdit nebo vyvrátit takové tvrzení se však již nepovede, protože obrazy disků - tedy klíčové důkazy - byly policii zničeny.

V neposlední řadě je nutné namítnout ještě jednu skutečnost, kterou je právo zúčastněných stran nechat přezkoumat jakýkoliv znalecký posudek, který je ve věci použit jako důkaz. Jestliže však vstupní data, která byla použita pro původní zkoumání, jsou zničena[7], nelze již takový znalecký posudek přezkoumat a tím je omezeno právo jedné ze stran soudního sporu na spravedlivý proces.

V této kauze existuje ještě mnoho dalších detailů, které by stálo za to probrat a vyjasnit. Velké množství nevyjasněných problémů a nesrovnalostí, které by vyžadovaly opětovné prozkoumání původních dat (obrazů disků) již však nelze objasnit. Právě díky

[6] Je tady myšleno to, že když někdo nechá udělat znalecký posudek, tak že takový posudek plně nahradí původní digitálná stopu - obraz disku. Neplatí, že znalecký posudek je důkaz a obraz disku je „pouze" stopa, kterou je možné po zpracování posudku zničit. Zkoumání vybraných dat obrazu disku prakticky nikdy nemůže postihnout veškeré stopy, které jsou v obrazu disku uloženy ani postihnout veškeré souvislosti.

[7] Tady obecně platí jedna výjimka, kdy zkoumané stopy jsou samotným procesem zkoumání spotřebovány (např. biologický materiál pro zkoumání DNA). To ovšem v žádném případě neplatí pro digitální stopy, ty se zkoumáním nespotřebovávají!

zničení původních dat došlo v této kauze k tomu, že při provádění důkazů u soudu již nebylo možné prověřit jednotlivosti, které při tom vyvstaly a nebylo možné ověřit většinu tvrzení obhajoby ani dát odpovědi na dodatečné otázky.

Nechci ty detaily[8] tady rozebírat, jsou až příliš těsně spjaty s konkrétní kauzou a kdyby existovala původní data (obrazy disků), daly by se pravděpodobně mnohé pochybnosti objasnit.

Závěr

Zopakujme si na závěr základní fakta, která z popisu tohoto konkrétního případu vyplývají:

► Každá aktivita v prostředí informačních systémů, zanechává v tomto prostředí digitální stopy[9].

► Většinu[10] digitálních stop, které takovou aktivitou vznikají, lze identifikovat, zkoumat a interpretovat.

► Informační systémy uchovávají ohromné množství různých informací, část z nich jsou data operačního systému, část tvoří uživatelská data a podstatnou část[11] dat, která se v informačních systémech uchovávají, jsou metadata, která uchovávají informace o chodu informačního systému a o událostech, které v něm probíhají.

► Aby bylo možné při zkoumání digitálních dat zjistit souvislosti a veškeré další skutečnosti, provádí se

[8] Jenom pro příklad: celá kauza měla proběhnout v určitém časovém období, avšak doba založení e-mailové schránky xxx@seznam.cz byla určena na dobu 3 měsíce po ukončení kauzy a 4 měsíce poté, co program keylogger měl na tuto schránku odesílat data z firmy A. Určitě lze navrhnout několik hypotéz, které by tuto skutečnost mohly objasnit, avšak mnohem průkaznější by bylo nalézt relevantní vysvětlující informace - důkazy - v zajištěných datech.

[9] To vychází z již zmiňovaného Locardova principu.

[10] Existuje skupina stop, které v systému nezůstávají uloženy. Jedná se např. o tzv. „živá" data, data v operační paměti počítače, která s vypnutím počítače zanikají a proto musí existovat speciální postupy jejich zajištění. Dalším druhem takových dat jsou síťová data - data, která putují po komunikačních linkách a která je potřebné pro zkoumání nejdříve zachytit a uložit. Další skupinou stop jsou stopy, které se z různých důvodů přepisují jinými a mají tedy pouze omezenou dobu platnosti. V závislosti od charakteru jednotlivých stop je nutné stanovit optimální strategii a postupy jejich zajištění.

[11] Poměr objemu jednotlivých druhů dat uložených v počítači se různí v závislosti od mnoha faktorů, jakými je použitý operační systém, doba, kterou je počítač v provozu a mnoho dalších.

při zajištění binární kopie[12] datových nosičů, tzv. obrazy disků, které uchovávají veškerá data, která jsou na nosiči/disku uložena.

► Digitální stopy se vyznačují tím, že pro důkazní účely jsou kopie a originál identické[13].

► Při jakékoliv manipulaci s digitálními daty (např. zkoumání nebo archivace) musí být nastaveny procesy tak, aby nedošlo k jejich modifikaci[14] nebo zničení.

► Z digitálních stop zpravidla nelze provést individuální identifikaci[15] osoby, která prováděla konkrétní aktivity v informačním systému.

► Nelze připustit, aby do pravomocného skončení věci došlo k odstranění jakéhokoliv zásadního důkazu[16], zejména když k tomu nejsou věcné důvody.

► Nelze nedůvodným zničením stop znemožnit právo na přezkoumání[17] již podaného znaleckého posudku.

Nechci jakkoliv znevažovat práci policie, státního zastupitelství a nakonec i okresního soudu v tomto případě. Z průběhu případu však v podstatě vyplývá, že (ve vztahu k digitálním stopám) jediným korektním krokem bylo zajištění digitálních stop[18] (obrazů disků). Jen je měli uchovat až do pravomocného ukončení případu.

[12] Existují výjimky, kdy technicky nebo z procesních důvodů nelze binární kopie datových nosičů/disků zajistit a postupuje se náhradními metodami. Nicméně veškeré takové výjimky je nutné zdůvodnit a zadokumentovat.

[13] Lze tedy pro důkazní účely vytvořit předepsaným postupem libovolné množství kopií digitální stopy, přičemž každá z nich bude mít stejnou důkazní sílu. Nemůže tedy dojít ke ztrátě např. z nepozornosti nebo z důvodů technické závady na nosiči dat. Platí pravidlo, že každá digitální stopa by měla být uchovávána nejméně ve dvou kopiích , které jsou uloženy na dvou technologicky oddělených datových nosičích, čímž se vyvarujeme ztrátě digitální stopy z důvodu technologické závady.

[14] Jsou výjimky, kdy stopu nelze zajistit, aniž by nedošlo k její modifikaci (typicky např. zajištění operační paměti počítače). Tyto výjimky však musí být zdůvodněny a podrobně zdokumentovány.

[15] Máme na mysli digitální stopy odlišné od digitálního záznamu biologických charakteristik osoby, jakými jsou např. otisk prstu, záznam z digitální kamery (obličej nebo sítnice oka), zvukový záznam hlasu a pod.

[16] Je jenom málo stop/důkazů, které by vylučovaly možnost dalšího dodatečného zkoumání, proto pro účely doplnění dokazování musí být veškeré stopy a důkazy zachovány minimálně do pravomocného skončení případu. Argumenty, že pro uchování velkých objemů dat nejsou k dispozici dostatečné prostředky pravděpodobně neobstojí už zejména proto, že cena kapacity datových úložišť neustále klesá.

[17] Obecně platí (byť to není pravděpodobně podchyceno zákonem), že pro každý znalecký posudek by melo platit, že musí existovat možnost jej opakovat nezávislým třetím subjektem, resp. měla by existovat možnost jej přezkoumat. K tomu však musí být vytvořeny stejné výchozí podmínky, jako při původním zkoumání, včetně toho, že zůstanou zachovány původní stopy, které byly zkoumány.

[18] Ale ani to zajištění neproběhlo zcela korektně, alespoň z technického pohledu. V případech, kdy se jedná o podezření vzájemné komunikace - tedy v tomto případě počítače z firmy B na počítače firmy A -zajištění dat mělo proběhnout ve stejnou dobu u obou firem.

Problematika vyšetřování v prostředí informačních systémů má množství specifik a navíc každý případ je něčím individuální, osobitý. Nelze dát jednoduchý a univerzální návod, jak s digitálními stopami pracovat, kdy je zajišťovat, jak v nich hledat důkazy a co vše je v nich možné najít.

Při zajištění dat mnohdy záleží na vteřinách, na přesném načasování momentu zajištění, protože důležité důkazy se mohou vyskytnout pouze v určitou dobu nebo při určité činnosti. Bez detailních odborných vědomostí může každý další analogický případ skončit podobně tomu, který byl popsán v tomto článku.

Je asi každému jasné, že ne vždy lze při vyšetřování podchytit a objasnit veškeré skutečnosti kauzy. Nelze však připustit, aby možnost došetřit, resp. objasnit veškeré sporné problémy nebylo možné provést a bez pochybností vyjasnit ještě před rozhodnutím soudu právě díky klíčové chybě, která se vyskytla v tomto případě.

Forenzní analýza SQLite databází

Často opomíjená oblast forenzní analýzy - pokračování z minulého čísla

David Makeev, Nikita Timofeev, Oleg Afonin, Yuri Gubanov - Belkasoft.

(do českého jazyka se souhlasem autorů přeložil Marián Svetlík jr.)

Anotace:

SQLite je populární databázový formát využívaný většinou mobilních i desktopových aplikací. V SQLite formátu ukládají data různé aplikace pro iOS i Android, stejně jako celá řada desktopových i mobilních webových prohlížečů (vč. Chromu a Firefoxu) a instant messengerů (např. Skype, WhatsApp).

Úvod

Forenzní analýza SQLite databází je často opomíjena a omezuje se pouze na jednoduché zobrazení databáze v příslušném prohlížeči. Kromě tzv. freelistů, o kterých jsme hovořili v první části článku, lze k vytěžení SQlite databází použít i Write-ahead logy, jejichž obsahem jsou nové či změněné stránky, které nebyly dosud uloženy do hlavní databáze.

Proč jsou Write-ahead logy tak důležité

Zatímco freelisty nám umožňují přístup ke smazaným stránkám databáze, Write-ahead logy (WAL) mohou být pomyslnou cestičkou k těm záznamům, které doposud nebyly provedeny v hlavní databázi. Pojďme se ale nejprve podívat, jak vlastně WAL fungují.

SQLite databáze historicky používaly k ochraně proti možným chybám zápisu žurnálování. Mechanismus, který to zajišťoval, se nazýval Rollback žurnál. Pokaždé, kdy se SQLite engine chystal provést zápis na stránku, byl původní obsah této stránky zazálohován do separátního žurnálového souboru. Proběhla-li operace zápisu bez chyb, engine následně tento žurnálový záznam odstranil. Pokud ale došlo během zápisu k jakékoliv chybě nebo byla operace přerušena, žurnálový soubor zůstal uložen na disku. Při dalším startu databáze engine těchto souborů využil a obnovil databázi do původního stavu sloučením hlavní databáze a žurnálových souborů.

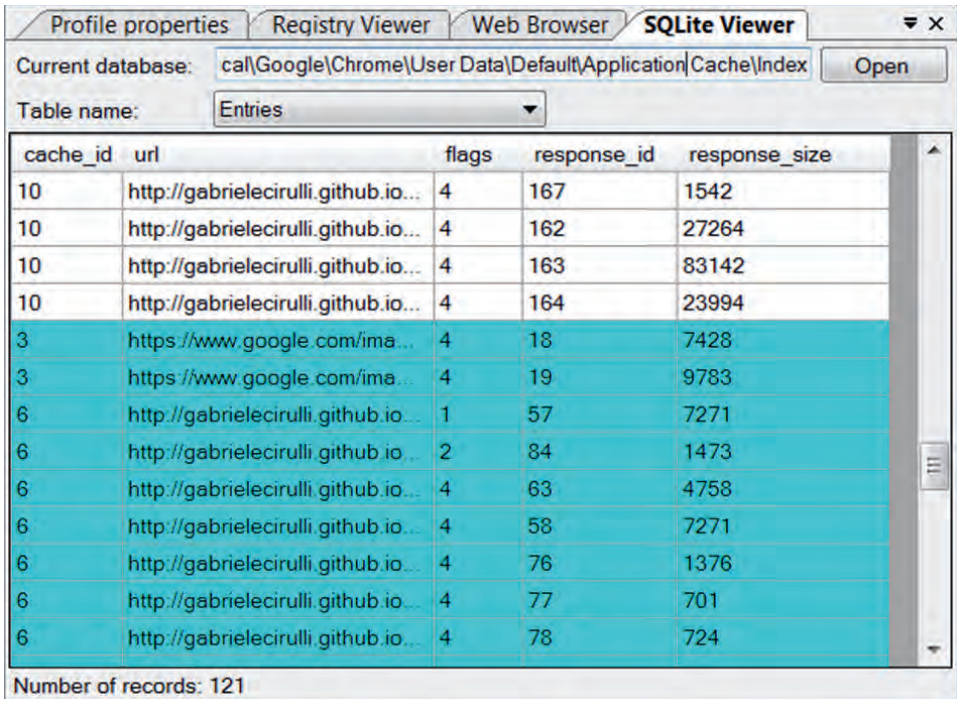
Rollback žurnály jsou však dnes již historií, neboť už od verze 3.7.0 používá SQLite jiný princip žurnálování – WAL. V podstatě se jedná o podobný princip, jako v případě Rollback žurnálu, pouze se zcela obrácenou logikou. Nově vytvořená nebo změněná data se nezapisují do hlavní databáze. Namísto toho se po určitý čas ukládají do separátního souboru WAL. Pro nás je zajímavá skutečnost, že ve WAL mohou být tato data uložena poměrně dlouhou dobu, a to až do provedení příkazu Checkpoint. Do té doby nečte engine nová data z hlavní databáze, ale právě z WAL. Chekpoint se pak provádí automaticky poté, co veli-

kost WAL dosáhne určité hladiny (defaultně je to 1 000 stránek) – to je možno změnit buď přes API databáze nebo přímo ručně SQL příkazem PRAGMA wal_checkpoint;

Nyní už pravděpodobně tušíte, proč o WAL hovoříme v souvislosti s digitální forenzní analýzou. Vezmeme-li například uloženou historii z chatu nebo z prohlížeče, může být tisícovka záznamů velmi důležitým zdrojem informací. Celá chatovací konverzace nemusela totiž nikdy spustit Chekpoint, výsledkem čehož je skutečnost, že změny z WAL nebyly nikdy provedeny.

Je nutno konstatovat, že většina nástrojů k prohlížení SQLite záznamů se před přístupem k databázi pokusí nejdříve WAL provést a data z WAL tak zahrnout do výstupu. Z pohledu forenzního a zachování integrity vstupních dat nutno konstatovat, takový způsob však není ideální.

V případě použití Belkasoft SQLite Viewer k vytěžení informací z WAL nebo Rollback žurnálů je databáze parsována stránku po stránce na low-level úrovni. Výhodou takového přístupu je skutečnost, že k dispozici jsou následně jak stránky z původní hlavní databáze, tak jejich dosud neprovedené kopie s novým či změněným obsahem z WAL (nebo obráceně v případě Rollback žurnálů). Stránky z WAL jsou pak v prohlížeči odlišeny zvýrazněním:



Belkasoft Evidence Center je komplexní forenzní nástroj, který se osvědčil v mnoha zemích. Kromě jiných funkcí přichází také s nativním SQLite parsováním, což umožňuje forenznímu expertovi spolehlivou extrakci dat z SQLite databází včetně výše zmíněných informací z freelistů. Tuto funkcionalitu si můžete vyzkoušet v rámci trial verze na http://belkasoft.com/trial.

Celý článek v angličtině si můžete přečíst na http://belkasoft.com/en/sqlite-analysis

Problém MessageID ve forenzní analýze

Upozornění na možný omyl forenzní analýzy e-mailů

Ing. Marián Svetlík st., vedoucí Znaleckého ústavu RAC, soudní znalec v oboru Kriminalistika, specializace Kriminalistická počítačová expertíza.
svetlik@rac.cz

Anotace:

Článek ve stručnosti podává úvodní informace do problematiky identifikace podvržení e-mailů. Jedná se o častou problematiku, kdy dochází k podvržení identity odesílatele e-mailu a tím uvedení adresáta v omyl, často s velice významnými i trestněprávními dopady.

Úvod

V zásadě se jedná o to, že lidé obecně věří tomu, co jim do e-mailové schránky dojde. Neuvědomují si, že z principiálních důvodů a podstaty SMTP protokolu (povšimněte si, že SMTP znamená Simple Mail Transfer Protokol), na kterém je posílání e-mailů založeno, je velice jednoduché padělat identifikaci odesílatele a vlastně padělat kompletně nejenom obsah e-mailu, ale i kompletní obsah celé hlavičky[1], o které se domníváme, že „je generován systémem" a tedy musí být věrohodný.

To, co vidíme v našem e-mailovém klientovi, je pouze tzv. „standardní" část hlavičky e-mailu, standardně pouze povinné položky hlavičky, jako „Odesilatel", „Adresát", „Datum", „Předmět" a „Tělo" zprávy. Abychom si uvědomili nebezpečnost důvěry v informace, které jsou v hlavičce e-mailu uvedeny, musíme vědět, že obsah hlavičky tvoří textové informace (stejně jako i tělo zprávy), které lze velice jednoduše podvrhnout. Protože to je volný text, lze do hlavičky napsat úplně cokoliv, nejenom podvrženou adresu odesilatele. Posílání e-mailů je založeno na protokolu SMTP, který pochází ještě z dob počátků internetu (1982), je to skutečně velice „simple" protokol.

Problém MessageID

Jednou z rozšířených a nepovinných položek hlavičky e-mailu je položka nazvána „MessageID". Poměrně často se stává, že tato položka je používána jako hodnověrná informace, která slouží k identifikaci odesílajícího mailového serveru. Není to však pravda.

Položka MessageID byla vytvořena a je používána primárně k účelům zřetězení e-mailů proto, aby nám e-mailový klient umožnil zobrazit tzv. strom celé komunikace (tj. sloučit do jednoho stromu veškerou komunikaci k danému subjektu nebo k provotnímu e-mailu, který inicioval celou další komunikaci). *V žádném případě položka MessageID není vytvořena pro účely prokazování zdroje nebo původu odeslané zprávy*, byť v případě, že e-mail hodnověrně není podvrhem, lze z této položky odesílající mailový server obecně identifikovat. Ale není to pravidlem a tedy nelze na takovém jevu stavět závěry.

Pravidlo pro tvorbu MessaageID říká, že hodnota musí mít tvar e-mailové adresy, tj. před i za znakem „@"je syntaxe znaků, která odpovídá pravidlům tvorby e-mailové adresy a že hodnota MessageID by měla být globálně unikátní. Z toho důvodu se za znak „@" obyčejně uvádí validní doménové jméno mailového serveru. Složitější to je se znaky před znakem „@", ty si v rámci své působnosti vytváří každý mailový server podle svých vlastních pravidel. Ve výsledku pak můžeme dostat hodnoty MessageID např. ve tvaru:

<38D1C1FD-3C35-4568-925C-FC46CAC0DE8A@sendinghost.com>

nebo také:

<41B5F981.5040504@sendinghost.com>

Protože neexistují obecně platná pravidla pro ověřování hodnoty MessageID (je to hodnota proprietální pro každý mailový server), nelze se při identifikaci odesílajícího mailového serveru na hodnotu MessageID spoléhat[2]. Z toho také vyplývá, že pro forenzní analýzu a pro utváření závěrů zkoumání, které by vycházely pouze z hodnoty MessageID, je položka MessageID absolutně nevhodná. Zopakujeme ještě jednou, že hodnota položky MessageID je, jako každá jiná položka hlavičky e-mailu, zadávána jako otevřený text a lze ji, jako každou jinou položku hlavičky e-mailu, lehce podvrhnout.

Jedinou cestou, jak zvýšit hodnověrnost hodnoty MessageID, je ověření její validity přímo prostřednictvím odesílajícího mailového serveru, tj. zaslat dotaz na provozovatele odesílajícího serveru, zda konkrétní hodnota MessageID je validní a zda odpovídá některému konkrétnímu e-mailu, který byl daným mailovým serverem zaslán. Bez takového ověření validity hodnoty MessageID je nutné závěry, které jsou položeny na neověřené hodnotě MessageID považovat za neplatné.

Závěr

Identifikace odesílajícího serveru e-mailové zprávy pomocí hodnoty položky MessageID z hlavičky e-mailu se může jevit jako dobrý a jednoduchý způsob potvrzení odeslání e-mailu z daného serveru. Takové závěry však nejsou položeny na správných předpokladech.

Hodnota MessageID je v hlavičce e-mailu uváděna z jiných než identifikačních důvodů a pravidla tvorby hodnoty této položky nepředepisují, aby obsahovala identifikaci odesílajícího serveru. To, že hodnota MessageID je udávána v otevřeném textovém formátu a že takovou informaci MessageID obsahuje, může naopak dobře posloužit ke zvýšení hodnověrnosti podvrženého e-mailu. Bez zpětného ověření validity každé konkrétní hodnoty MessageID u provozovatele odesílajícího e-mailu jsou veškeré závěry, které by byly na hodnotě MessageID postaveny, lehce vyvratitelné.

Literatura

[1] http://martin.vancl.eu/odeslani-e-mailu-z-cizi-adresy-bez-znalosti-hesla

[2] Satheesaan Pasupatheeswaran, *"Email 'Message-IDs' helpful for forensic analysis?"*, Originally published in the Proceedings of the 6th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 3rd 2008

Pokyny pro autory

Digital Forensic Journal je odborný časopis, který se věnuje problematice forenzního zkoumání digitálních dat.

Přijímáme články jak specializované, které se věnují konkrétním technickým problémům, tak i informacím v širších souvislostech z oblasti obecných otázek znaleckého zkoumání.

Věnujeme se doporučením a metodickým pokynům, pozornost věnujeme také použití digitální forenzní analýzy v trestně-právních otázkách ale i v procesu šetření bezpečnostních incidentů ICT. Nevyhýbáme se tématiky bezpečnosti ICT ve vztahu k šetření bezpečnostních incidentů, jakož i dalších oblastí použití digitální forenzní analýzy.

Rukopisy jsou přijímány elektronicky na adrese dfj@rac.cz ve všech běžných datových formátech.

Struktura příspěvků je dána v zásadě podle toho, jak jsou uvedeny příspěvky v aktuálním čísle, tedy název, autor (pozice a kontaktní e-mail), anotace a samotný obsah článku. Doporučujeme členit kapitoly a podkapitoly nanejvýše do tří úrovní. Rozsah článku není v principu omezen, doporučujeme nepřesáhnout 10 stran. Obrázky a grafiku vložte do textu příspěvku, aby bylo zjevné jejich umístění v textu a navíc přiložte jako samostané soubory v dostatečné kvalitě.

Případné obsahové nebo technické připomínky redakce k příspěvku budou individuálně projednány s autorem. Příspěvky v zásadě neprocházejí jazykovou korekturou, autor odpovídá za obsah a za věcnou a gramatickou správnost příspěvku.

Příspěvky, které nebudou splňovat výše uvedené základní požadavky, nebudou publikovány.

Rozhodnutí o publikaci příspěvku je ve výhradní kompetenci vydavatele.

Tableau TD2u Forensic Duplicator

Nový TD2u duplikátor s rozhraními

- USB 3.0
- SATA
- SAS
- IDE

Každý TD2u KIT obsahuje

- TD2u forenzní duplikátor
- TP5 univerzální kompaktní adaptér
- 3M > molex-4 napájecí kabel
- SATA signální kabel
- univerzální SAS/SATA signální a nápájecí kabel (3x)
- 3M > SATA napájecí kabel
- IDE signální kabel
- USB-A > mini USB-B kabel
- utěrku na displej

Podpora množství rozhraní

Již čtvrtá generace duplikátorů Tableau provádí imaging dat ve vysokých rychlostech, které přesahují až 15GB/min při současném vypočítávání MD5 a SHA-1 hashí. TD2u umožňuje zajištění digitálních stop ze zařízení s rozhraním USB 3.0, SATA a IDE/PATA. Dále může uživatel vytvářet obraz SAS disků za použití stejného TDP6 modulu, který se používá u TD1 a TD2 duplikátorů.

Nabitý funkcemi

TD2u dokáže vytvořit jednu (1:1), dvě (1:2), nebo tři (1:3) kopie zdrojových disků. Mezi základní funkce patří disk-to-disk (klon) a disk-to-file (image) duplikace, formátování, mazání, výpočet kontrolních sum MD5 a SHA-1, HPA/DCO detekce a odstranění a kontrola prázdného disku. TD2u vytváří výstupy ve formátech DD, .e01, .ex01 a .dmg. Stejně jako u všech produktů společnosti Tableau, firmware TD2u je upgradovatelný skrz Tableau firmware update (TFU) funkci.

Prodej a podporu v ČR a SR zajišťuje:
Risk Analysis Consultants, s.r.o.
Táborská 5
Praha 4
zu@rac.cz
www.rac.cz

Digital Forensic Journal
ISSN (Print): 2336-4750
ISSN (On-line): 2336-4769