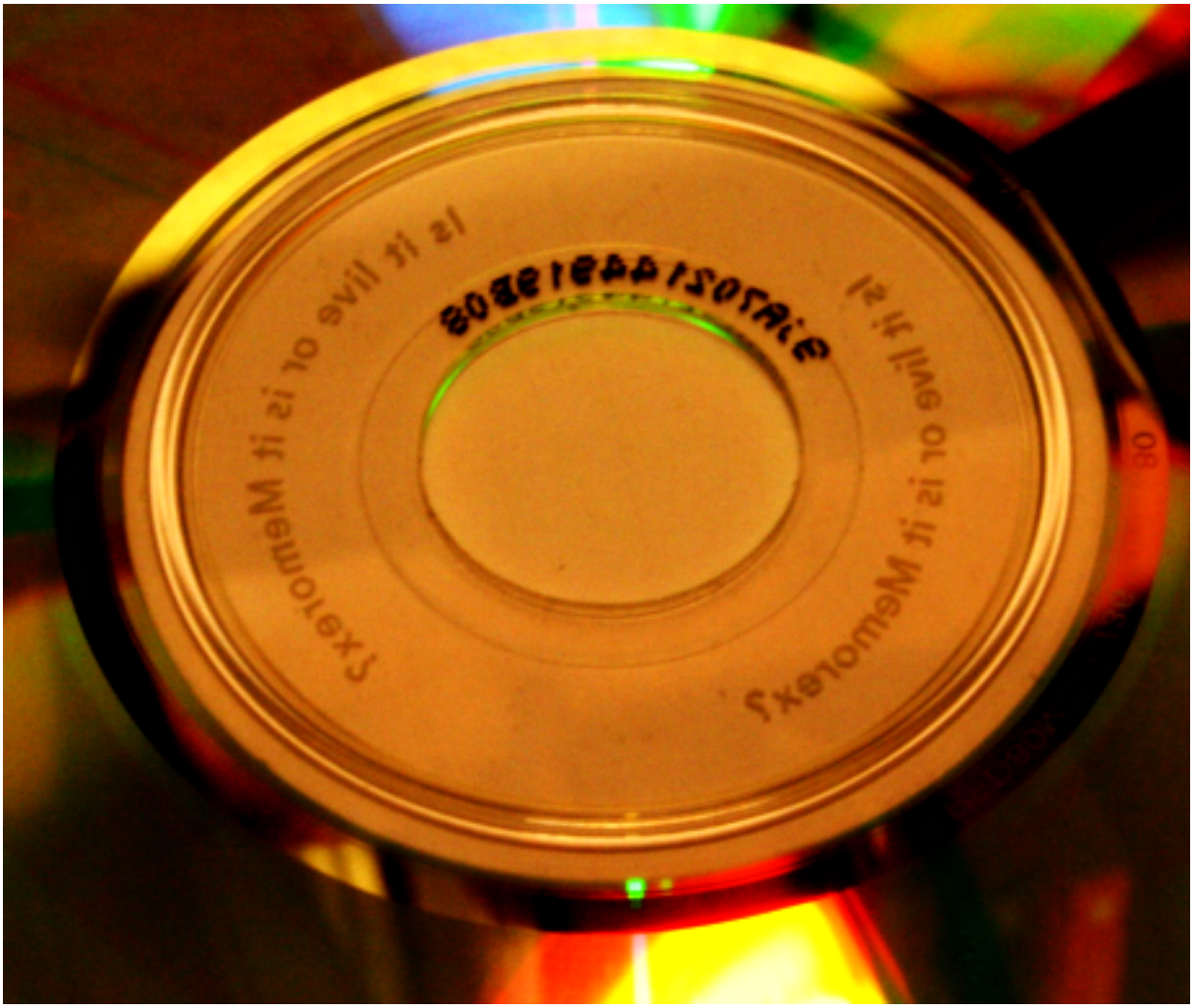
Digital Forensic Journal

1/2014 **15. září 2014**



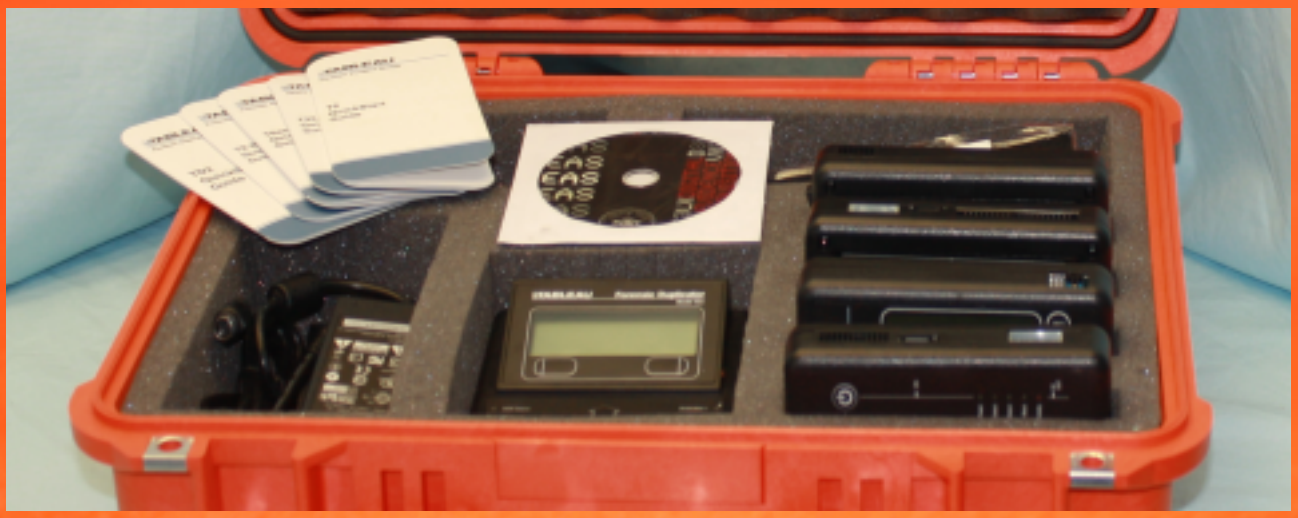
Digital Forensic Journal je odborný časopis věnovaný problematice forenzního zkoumání digitálních dat. Zabývá se nejenom problematikou samotného forenzního zkoumání, ale i dalších oblastí souvisejících s digitálními informacemi, s jejich bezpečností, ochranou, zajištěním a zkoumáním.

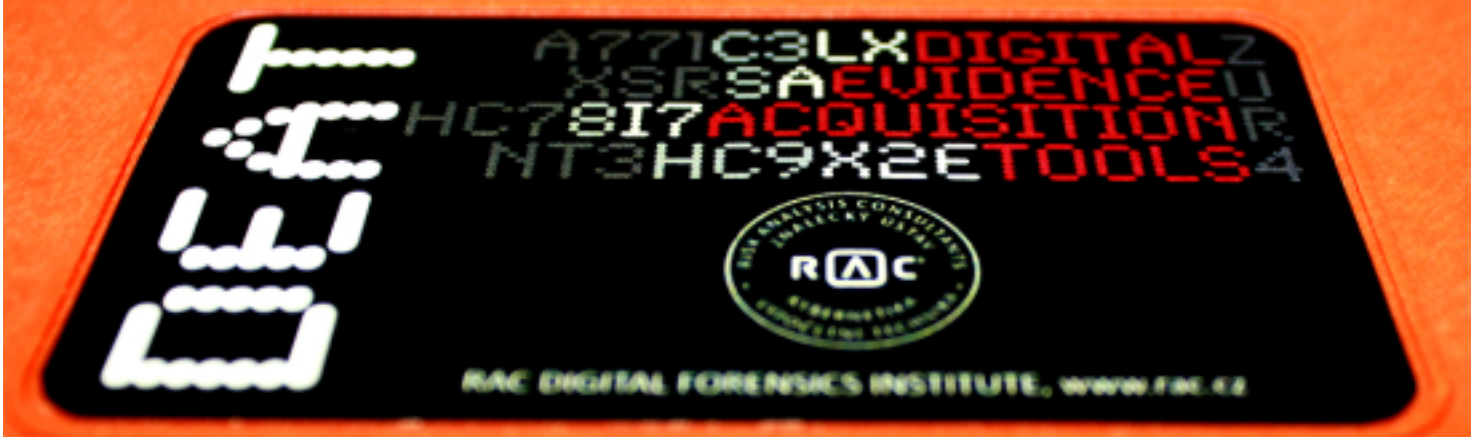
Znalecký ústav RAC konečně přináší český komplet

DEAT

DIGITAL EVIDENCE ACQUISITION TOOLS

DEAT je přenosná sada, obsahující komplet HW a SW nástrojů pro pořizování forenzních kopií dat. DEAT obsahuje prakticky vše, co můžete potřebovat - od sady redukcí a 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, které můžete na místě zajištění potřebovat. DEAT je unikátně vybaven i nástrojem DEAS - forenzním bootovacím CD, které bylo vytvořeno v laboratoři Znaleckého ústavu RAC právě pro účely práce na místě zajištění.





Digital Forensic Journal

1/2014 **15. září 2014**

Úvodník

Dobrý den, vážení čtenáři,

dostává se Vám do rukou první vydání Digital Forensic Journal. Předně bych Vám chtěl poděkovat, že jste jej vůbec začli číst. Svědčí to o tom, že už jenom název Vás něčím upoutal, a to je dobře. Určitě to byl jeden z důvodů, proč jsme jej tak nazvali. Angličtinu v názvu jsme zvolili jenom proto, že prakticky každý český překlad pojmu "Digital Forensics" by byl nesrovnatelně delší a jako název by se tím pádem moc nehodil. Jinak obsah je, a předpokládáme že i do budoucna bude, primárně v češtině, protože je určen pro Vás.
Důvodů, proč jsme se rozhodli k této formě publikace je mnoho, z těch nejdůležitějších namátkou: (a) podobný vydavatelský počin v našem prostředí není; (b) cítíme velkou důležitost tohoto oboru dnes a ještě větší v budoucnu; (c) jsme přesvědčeni, že existuje v této oblasti velmi velký informační deficit jak v odborných kruzích, tak u laické veřejnosti; (d) existuje mnoho zkreslených představ o tomto oboru.
Problematika spojená s kybernetickou kriminalitou a se způsoby jejího odhalování, vyšetřováni a potírání je nesmírně široká. Nebudeme se tedy omezovat pouze a výlučně na otázky digitální forenzní analýzy, ale určitě zařadíme tuto oblast do širších souvislostí. Jak říká klasik, všechno se vším souvisí.
Uděláme vše, abychom Vám jednou za půl roku mohli poskytnout kvalitní a zajímavé informace. Věříme, že se nám to povede a vy se budete k Digital Forensic Journal pravidelně vracet.
Závěrem snad jen tolik, že Digital Forensic Journal je Vám všem bezplatně k dispozici, jen se, prosím, podívejte na následující stranu, kde jsou uvedny podmínky použití. Digital Forensic Journal najdete také ve formátu PDF na stránkách společnosti Risk Analysis Consultants, s.r.o. (www.rac.cz/dfj).

Přeji Vám příjemné a užitečné čtení.
Marián Svetlík

Obsah

RiskAnalysisConsultants
Czech Cyber Crime Centre of Excellence

Digital Forensic Journal je vydáván v kooperaci s Czech CyberCrime Centre of Excellence (C4e, www.c4e.cz) a za podpory Prevention of and Fight against Crime Programme of the European Union European Commission - Directorate-General Home Affairs.

Risk Analysis Consultants, s.r.o.
Španělská 2
120 00 Praha 2
Tel. + 420 221 628 400
Fax + 420 221 628 401
E-mail dfj@rac.cz
Web www.rac.cz
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 1 / Rok 2014 / Číslo 1 / Vyšlo 15. 9. 2014 v Praze

Profesionalita znaleckého zkoumání

Předpoklady výkonu znalecké činnosti a kvality znaleckých posudků

Ing. Marián Svetlík st.
svetlik@rac.cz
Soudní znalec v oboru Kriminalistika se specializací Kriminalistická počítačová expertíza, vedoucí Znaleckého ústavu společnosti Risk Analysis Consultants, s.r.o., viceprezident Akademie forenzních věd, z.s.

Anotace:

Článek se zbývá pozicí a rolí znalce v ČR. Hodnotí situaci v této oblasti zejména z pohledu praktických zkušeností a problematických oblastí, které se při každodenní činnosti vyskytují. Posuzují se také reálné podmínky, které ovlivňují profesionalitu a ve výsledku tím i kvalitu znaleckého zkoumání. Článek je cíleně pojat jako doplnění pohledu prof. JUDr. Jana Musila, CSc. na problematiku hodnocení znaleckého posudku, uveřejněného v č. 3/2010 časopisu Kriminalistika, z pohledu znalce.

Postavení a nezávislost znalce

Jak vlastně, když odhlédneme od definicí v zákoně, chápeme pojem „soudní znalec"? Asi se nespletu, když pod soudním znalcem chápeme odborníka ve svém oboru, který je schopen prozkoumat daný problém tak, aby výsledek jeho práce – znalecký posudek – mohl posloužit jako objektivní skutečnost, jako berná mince, jako něco, co platí. To znamená, aby závěry znaleckého posudku mohly posloužit jako důkaz před soudem. Mnohdy jako klíčový důkaz, který rozhoduje o vině a trestu, jako důkaz, který má hodnotu statisíců, milionů nebo i miliard korun, mnohdy hodnotu osudu člověka. Soudní znalec taky většinou ani netuší, jakou potenciální hodnotu v daném řízení jeho posudek má nebo bude mít. Ani by to vědět neměl. Tím spíše by jeho práce měla mít vysokou úroveň nehledě na to, zda se z jeho odborného pohledu jedná o maličkost, pro kterou by možná ani nestálo sepisovat znalecký posudek nebo o řešení složité problematiky, která by se mohla často srovnávat i se zásadními problémy výzkumu Akademie věd.

Když budu citovat větu profesora Musila *„…v souladu s koncepcí rovnosti zbraní musí být znalecký posudek hodnotitelný a kritizovatelný ze strany všech subjektů, které se podílejí na trestním procesu..."* jednoznačně dospěji k závěru, že znalec, resp. jeho znalecký posudek, musí být zjevně nezávislý na kterékoliv straně procesu.

Obor "digital forensics" má to štěstí, že je to obor exaktní, technický. Ať zkoumáme cokoliv, ať zkoumáme pro kohokoliv, jediným našim cílem je objektivně zjistitelná a nevyvratitelně zadokumentovaná pravda. To je jediný cíl znaleckého zkoumání. Pravda o informacích, jevech, dějích a procesech v prostředcích zpracovávajících digitální data. Nic víc. **Jediným cílem znalecké práce a také jediným posláním je dokumentovat pravdu.** O použití, využití nebo zneužití této pravdy nerozhodujeme. Nechceme s tím mít nic společného, ani bychom s tím nic společného mít neměli. Postavení znalce by mělo být navýsost nezávislé. Nezávislé na tom, pro koho pravdu zjišťuje, a pro co a jakým způsobem je zjištěná pravda použita nebo zneužita. Striktní nezávislost.

Vyjdu opět z citace profesora Musila: *„Institut znalce má v českém prostředí již od 19. století po právní stránce hybridní charakter: v rámci konkrétního řízení… je postavení znalce určováno procesními vztahy, které jsou upraveny v procesních normách… Paralelně s tím však normami veřejného práva byla vytvořena specifická skupina tzv. soudních znalců, … kteří jsou stanoveným postupem jmenováni nikoliv jen*

pro jednotlivé případy (ad hoc), nýbrž trvale… Znalci takto zapsaní mají zásadně povinnost na žádost státních orgánů vypracovat znalecký posudek a nesou právní odpovědnost za jeho správnost; za podání expertizy jim od státu přísluší odměna…. Je možno říci, že znalectví je chápáno jako veřejná služba.“

Státem vytvořená specifická skupina soudních znalců, kteří mají zásadně povinnost vypracovávat pro státní orgány znalecké posudky, a za tuto práci jim od státu přísluší odměna – už jenom takováto formulace nesvědčí o nezávislosti znalců. V tomto pojetí, kdy znalectví je chápáno jako veřejná služba hrazená státem, je znalec zcela zjevně v postavení, které je fakticky v rámci řízení před soudem závislé, a nezávislost znalce je pouze vynucena zákonem, podle kterého znalec musí vykonávat znaleckou činnost podle svého nejlepšího vědomí a svědomí a, jak také uvádí profesor Musil, nese právní odpovědnost za správnost podaného posudku.

Další tvrzení profesora Musila v této souvislosti, že *„trvalá registrace těchto znalců ve veřejných seznamech znalců zajišťuje jejich publicitu a dostupnost pro širokou veřejnost“* je možné chápat ve dvojím významu – jednak je seznamem znalců poskytována lepší služba veřejnosti („dostupnost široké veřejnosti“), ale z druhé strany stát poskytuje znalcům (minimálně v současné době) vlastně téměř zadarmo reklamu jejich specifické činnosti („zajišťuje jejich publicitu“).

Tato relativní výhoda však nedodržuje zásadu rovnosti, neplatí spravedlivě pro všechny znalce, resp. pro všechny znalecké obory a odvětví. Jsou obory, které publicitu, kterou jim dává zápis v seznamu znalců, reálně prakticky nikdy nevyužijí (typicky obor „kriminalistika“, protože tento obor je využíván prakticky pouze OČTŘ v trestních řízeních), a tudíž jejich publicita jim a ani široké veřejnosti žádné výhody nepřináší. Naopak jsou znalecké obory (typicky ekonomické), kde stát přímo požaduje, aby pro určité právní úkony (a těch je značné množství) byly použity znalecké posudky. To pak zápis v seznamu znalců je pro tuto skupinu výhodou významnou, tím spíše, že v soukromě-právních vztazích neplatí státem stanovené sazby za znaleckou činnost, ale platí vztahy smluvní. Tady se zdá být pokřivení principu rovnosti a nezávislosti znalců ještě výraznější.

Podívejme se dále, kdo se podle zákona může stát soudním znalcem. Kromě formálních náležitostí, jako např. že „je způsobilý k právním úkonům v plném rozsahu“, „se jmenováním souhlasí“ a další, dalo by se říct triviální náležitosti (a právníci mi prominou ten výraz o triviálnosti), je jediným odborným kritériem to, že „má potřebné znalosti a zkušenosti z oboru…“.

Znalce jmenuje zpravidla předseda krajského soudu na základě zhodnocení kritérií a podle zvážení potřebnosti takového znalce jmenovat. Výsledek je, že na jmenování není právní nárok a jmenování je výlučně záležitostí rozhodnutí předsedy krajského soudu. Když k tomu přidáme trestní odpovědnost znalce, povinnosti ve vztahu k administrativě znalecké činnosti, termínům, účtování, případným výjezdům a asistencím, hrozbu případné pokuty za přestupky i typu opomenutí, vlastní profesionální odpovědnost, minimální možnost odmítnout podat znalecký posudek, a tím i nepředvídatelnost pracovního zatížení, a nakonec reálné finanční ohodnocení takové činnosti, nelze se divit, že ti nejlepší v oboru (čest výjimkám) se do takové práce nehrnou.

Když to přeženu a zjednoduším, soudní znalci jsou ti, kteří se spokojí s hodinovou sazbou 100 – 350 Kč za vysoce profesionální a specializovanou práci, a to i přes riziko, že míru odbornosti a tedy i výši odměny za zpracování znaleckého posudku ze zákona určuje objednatel, který zcela v souladu se zákonem v problematice není odborníkem, a právě proto tyto odborné činnosti zadává znalcům.

Dá se namítnout, že být soudním znalcem je přece prestižní záležitost. Možná to bylo v době, kdy zákon o znalcích vznikl, v době počátků reálného socializmu roku 1967. Tady je zřejmě to hlavní jádro problému, postavení a celospolečenského chápání výkonu znalecké činnosti a nahlížení na forenzní práci v naší společnosti, jádro toho, proč nejsou u nás soudními znalci ty skutečné špičky v oboru (přirozeně se to netýká všech), kdo se vlastně dává na dráhu soudního znalce a jakou perspektivu mu to skýtá.

Lze si celkem dobře představit, že když se přijímal v roce 1967 zákon o znalcích a tlumočnících, věcný záměr tohoto zákona mohl odpovídat podmínkám, které v té době panovaly. Zákon předpokládal, že pro znalecké vědomosti, resp. pro znaleckou kvalifikaci, budou postačující vysoké lidské vlastnosti a profesní vědomosti, které člověk získá při výkonu své běžné profese a že tyto vědomosti použije i při tak specifické činnosti, jakou je činnost znalecká. Ve skutečnosti ani jiné možnosti zřejmě v té době ani nebyly.

Proto i zákon je koncipován primárně tak, že znalcem je chápána osoba, u které je předpoklad, že je znalý určitého civilního oboru a že tyto vědomosti uplatní i při znalecké činnosti. Navíc, že znaleckou činnost bude vykonávat jaksi nad rámec svého zaměstnání. Jestli znalec něco znalecky zkoumal v rámci své řádné pracovní doby, jeho zaměstnavatel to v té době mohl chápat nanejvýše jako poctu, že jeho zaměstnanec byl pověřen tak důležitým a prestižním úkolem pro socialistický stát. Obdobně je v zákoně chápáno i postavení tzv. znaleckých ústavů. Přední vědecké instituce byly (jakoby navíc, za odměnu) zapsány do seznamu znaleckých ústavů a znaleckou činnost vykonávaly v rámci své standardní výzkumné činnosti, téměř něco jako výzkumnou zakázku státu. Šlo to, dalo by se říct, z „režijních nákladů“. O tom, jestli budou znalcům nebo znaleckým ústavům proplaceny náklady na znaleckou činnost a v jaké výši rozhodoval státní orgán, který o znalecký posudek požádal.

Za bezmála půlstoletí od vzniku tohoto zákona se ale mnohé výrazně změnilo. Jen namátkou:

a) zaměstnavatele již většinou nezajímá, zda jeho zaměstnanec je v seznamu znalců, primárně ho zajímá práce, za kterou mu platí. Schválně si jen tak v mysli udělejte rozvahu, kolik asi stojí hodina práce předního vědce (mzdy, daně a další odvody, nájem, energie, přístrojové vybavení, školení, cestování, konference, stáže, režie apod.). Znalcům tak nezbývá, než skutečně dělat znalectví ve volném čase, kterého je, zejména u vysoce kvalifikovaných lidí, velice poskrovnu;

b) problematika znaleckého zkoumání se ve většině znaleckých oborů mnohonásobně zkomplikovala. Lidské poznání udělalo nesmírný pokrok, objevily se nové vědomosti a poznatky, nové metody, nové technologie. Stejně se změnily i stopy, které jsou předmětem znaleckého zkoumání. Pro jejich zkoumání je potřebné stále složitější přístrojové vybavení, stále složitější metody a postupy dovolují odhalovat další a další skutečnosti, které jsou důležité pro získávání důkazů;

c) kriminální činnost se stala mnohem sofistikovanější, než byla před půlstoletím. Abych nemluvil jen obecně, před 50-ti lety se o kybernetické kriminalitě psaly snad jen trochu naivní romány z oboru science-fiction;

d) co je asi nejdůležitější, jednoznačně se etablovaly forenzní vědy jako samostatné vědní obory. Jako takové již nejsou a nemohou být záležitostí pouze civilně vzdělaných lidí, profesionálů ve svém civilním zaměstnání. Forenzní vědy a jejich praktické aplikace prostřednictvím znaleckého zkoumání vyžadují profesionální vědecký přístup. Znalectví se již nedá dělat jako koníček, jako pocta pro kvalitní zaměstnance/odborníky a také ne jako přivýdělek vedle vlastního zaměstnání.

Profesionalizace znalecké činnosti

Daly by se vyjmenovat i mnohé další skutečnosti, které výrazně změnily (lépe řečeno měly by změnit) chápáni a postavení znalectví a znalců v současné době.

Asi tou nejdůležitější je profesionalizace forenzního zkoumání. Už to není jen interpretace civilní profese pro účely znaleckého zkoumání, znalecké zkoumání se opírá o samostatné forenzní vědní disciplíny. V našem prostředí se jim však systematicky věnuje jenom minimální pozornost.

Druhou skutečností, která je systematicky přehlížena, je náročnost znaleckého zkoumání. Jestliže před půl stoletím bylo znalectví doménou jednotlivců-odborníků, dnes je stále více forenzních oborů natolik složitých a rozsáhlých, že není objektivně možné, aby je vykonával jednotlivec. V mnoha oblastech znaleckého zkoumání již není

možné se dobrat relevantních výsledků bez kolektivního know-how, bez týmové spolupráce. A jestliže někdo tvrdí opak, jestliže někdo tvrdí, že je individuálně schopen na špičkové úrovni obsáhnout např. celé odvětví výpočetní techniky, tak lže. Dá se namítnout, že přece existuje pro znalce možnost přibrat pro dílčí problematiku konzultanta. Papírově ta možnost existuje, reálně ji však ve většině případů nelze využít, protože jednak přibrání konzultanta musí schválit zadavatel posudku a také externista (tedy odborník, který není znalcem, a tedy nemá ani představu o ohodnocení znalecké práce) nebude dělat vysoce odbornou práci za směšnou odměnu a vyšší sazbu za konzultanta zadavatel posudku zpravidla ani nemá možnost schválit.

Náročnost znaleckého zkoumání také naráží na drahou techniku, která je stále častěji pro výkon znalectví nutná a znalec si takovou techniku ze znalečného dovolit nemůže. Tady taky existuje papírová možnost použít zařízení jiné organizace a uhradit náklady na takovou zápůjčku, reálně však opět narazíme na finanční bariéru. Ale nejen to. Zákonodárce vůbec nevzal do úvahy, že znalecké zkoumání není obecně činnost typu „hoď ho do (jakéhokoliv) stroje“. Znalecké zkoumání vyžaduje mnohdy zařízení, která jsou znaleckým úkolům přizpůsobena, specificky nakonfigurována, mají svoje specifické parametry a musí být (pardon, nikdo to nenařizuje, jen to je mezinárodně požadovaný předpoklad) pravidelně certifikované/kalibrované. To se reálně nedá půjčit nebo pronajmout, resp. zadavatel by nikdy nesouhlasil s částkou, která by byla za takový pronájem účtována.

Neexistence formálního statutu forenzních věd způsobuje, že se forenzním vědám, až na výjimky nebo jednotlivce, nikdo systematicky nevěnuje. A když (např. Ústav soudního inženýrství v Brně, Ústav súdneho inžinierstva v Žilině, Ústav kriminalistiky a forenzních disciplín v Karových Varech a některé další menší subjekty), tak to je většinou pouze selektivní výběr oborů, a to zejména těch, u kterých se to z pohledu ekonomické efektivnosti vyplatí. Mnohé subjekty, od kterých by se taková vědecká činnost očekávala (např. Policejní Akademie ČR nebo Kriminalistický ústav Praha PČR) na tyto aktivity v podstatě rezignovaly nebo je nemohou plně realizovat z důvodů přetížení reálným výkonem znalecké práce, kdy na výzkum a vývoj nezbývá dostatek času, prostředků a vědecky erudovaného personálu.

To způsobuje, že v praktickém výkonu znalecké činnosti naši soudní znalci mnohdy tápou a mnohdy porušují elementární zásady forenzní práce. Jen tak mimochodem – ani ty nejzákladnější principy, jako je podrobná dokumentace, přezkoumatelnost, vědeckost, možnost verifikace nálezů, integrita důkazů a další, nejsou celou tu dlouhou dobu nikde zakotveny a v praxi snad jediná závazná formulace typu „znalecké zkoumání se provádí podle nejlepšího vědomí znalce“ je již dávno překonána. Současnému znaleckému zkoumání viditelně chybí solidní teoretická základna. Jak asi může vypadat aplikace forenzní vědy v praktickém výkonu znaleckého zkoumání, když forenzní teorii v tom nejširším pojetí nikdo systematicky nerozvíjí? Jestliže k tomu přidáme požadavek profesora Musila na obsah hodnocení znaleckého posudku *„Hodnocení odborné správnosti znaleckého zkoumání v sobě zahrnuje: - hodnocení teoretických východisek, o něž znalec opírá svůj závěr; -hodnocení empirického základu posudku, tj. kvality a množství zjištěných znaků zkoumaných objektů; - hodnocení použitých odborných metod a postupů; - hodnocení, zda subsumpce konkrétního empirického základu pod obecný teoretický základ je správná.“*, dostaneme se k rozporu mezi požadavky na hodnocení a možnostmi znalce bez vědeckých základů tyto požadavky splnit.

Znalecké ústavy

Jestliže donedávna se působení znaleckých ústavů v zákoně o znalcích nevěnovala nějaká zvláštní pozornost, současná novela opět vrací kolektivní práci zpět do individuálního pojetí a zavádí povinnost zaměstnávat na trvalý pracovní poměr v daném oboru nejméně tři znalce – fyzické osoby. Z jedné strany se dá pochopit účel takového požadavku. Jak správně uvádí profesor Musil při hodnocení kvality podaného znaleckého posudku *„u znaleckých ústavů může vyvstat dodatečná pochybnost např. proto, že se podstatně změnilo jejich*

personální složení, že z ústavu odešli dřívější osvědčení pracovníci". Povinnost zaměstnávat tři znalce – fyzické osoby – pro každý znalecký obor zajistí, že toto riziko bude alespoň částečně eliminováno.

Zákonodárci bohužel již nezohlednili, že tímto požadavkem zavedli do systému práce znaleckého ústavu téměř neřešitelný problém, a zavedli tím interní korupční riziko. Reálná praxe je totiž taková, že většinou před objednáním/pověřením znalce ke zpracování znaleckého posudku je toto se znalcem konzultováno. Když potom znalec – zaměstnanec znaleckého ústavu – přijímá objednávku na znalecký posudek, zjevně se samostatně může rozhodnout (např. podle náročnosti nebo lukrativnosti objednávky) zda ji přijme jako znalec – fyzická osoba a zpracuje a vyúčtuje ji sám nebo ji přijme jako zaměstnanec znaleckého ústavu a nechá ji zpracovat ústavem. Ano, lze namítnout, že o tom nerozhoduje znalec, ale zadavatel posudku. Avšak stačí, aby znalec v rámci konzultací ohledně předpokládaných nákladů jen zmínil, že znalecký ústav bude dražší. Reakce zadavatele, zejména v případě OČTŘ, je nanejvýš predikovatelná.

Z jedné strany je znalec – fyzická osoba – zapsán v seznamu znalců samostatně a zaměstnavatel nemá žádné právo rozhodovat o tom, jestli a který posudek zpracuje (o tom rozhoduje výlučně dožadující orgán), z druhé strany, když pojme svoji práci znalce jako práci pro znalecký ústav, může být za to, že pracoval pro znalecký ústav a sám na sebe nezpracoval jediný posudek, ze seznamu znalců vyškrtnut pro pasivitu. Nejspíše by se takové vyškrtnutí dalo zpochybnit a zdravý rozum říká, že by k takovým situacím docházet nemělo, ale realita je bohužel jiná a riziko je značné. Evidenci znaleckých ústavů totiž vede ministerstvo spravedlnosti a evidenci znalců vedou krajské soudy. Tyto instituce taky nezávisle na sobě provádějí i kontrolní činnost a nikdo je v současné době nezavazuje k tomu, aby zohledňovaly aktivity, které jsou vykazovány v jiných evidencích, navíc když tyto evidence nejsou v působnosti toho kterého kontrolního orgánu. Logicky by to sice mělo vyplývat z povinnosti správních orgánů daných jim správním řádem, ale reálné zkušenosti mluví jednoznačně jinak.

Paradoxní situace, podobné té výše zmíněné, však provázejí výkon znalecké činnosti i v jiných oblastech. Opět použijí citát profesora Musila: *„Orgán činný v trestním řízení nemůže sám nahradit odborné závěry znalce svými laickými názory. Přesto je však třeba trvat na povinnosti orgánů činných v trestním řízení hodnotit znalecký posudek též z hlediska jeho odborné správnosti."* Z pohledu postavení znalce a znaleckého posudku v trestním řízení a na základě volného hodnocení důkazů je to sice tvrzení obsahující vnitřní rozpor, avšak pochopitelné, protože i znalecký posudek je jen výsledek práce člověka. Pominu tady až schizofrenický problém odborného hodnocení znaleckých posudků soudy, kdy na jedné straně k tomu nemají odpovídající odbornost a na druhé straně se musí spolehnout na vlastní úsudek, vnější charakteristiky znaleckého posudku, rady jiných odborníků nebo reference. Jestliže před desetiletími byla situace v této oblasti co do rozsahu, náročnosti a složitosti znaleckého zkoumání výrazně jednodušší, dnes ani výše zmíněné pomocné parametry zcela objektivně nemusí vést ke správnému rozhodnutí.

K tomuto problému profesor Musil dále sděluje, že *„… nikdo nemůže samozřejmě chtít, aby soudce detailně a hluboce ovládal všechny vědní obory, od chemie a biologie až po lékařství či nukleární fyziku. To je zajisté nemožné. Lze však požadovat, aby trestní soudce měl alespoň elementární znalosti těch disciplín, které se nejčastěji ve znalectví uplatňují, jako je kriminalistika, soudní lékařství, soudní psychiatrie, soudní psychologie. Tento požadavek vznášel již před 120 lety nestor kriminalistické nauky Hans Gross a od těch dob neztratil nic na své aktuálnosti, spíše naopak."* Asi by se s tím dalo i souhlasit, když se jedná o forenzní disciplíny, které jsou postaveny na dnes již dlouhá léta známých principech (například typicky daktyloskopie). Co však v případech disciplín nových nebo těch, které se nevyskytují tak často nebo metody zkoumání jsou natolik složité, že pouze několik jednotlivců je schopno je vědecky zdůvodnit, natož v praxi realizovat? Na rozdíl od profesora Musila jsem přesvědčen, že za 120 let od Hanse Grosse se forenzní vědy transformovaly výrazně, stejně tak se výrazně komplikují i právní vědy (jako primární profese soudců) a výše uvedený požadavek na šíři znalostní báze každého soudce již nemůže odpovídat realitě. Nicméně z druhé strany nikdo nezpochybňuje výlučnou pozici soudců jako

jediného subjektu, který musí v procesu přijmout rozhodnutí. Je pouze na něm, na základě jakých důkazů toto rozhodnutí přijímá.

Hodnocení odborné úrovně a náročnosti znaleckého zkoumání má přímý vliv nejenom na hodnocení materiální pravdy (objektivní skutečnosti) u soudu, ale paradoxně i na ohodnocení práce znalce, protože odměna za výkon znalecké činnosti je plně v kompetenci toho orgánu, který znalecký posudek zadal. Paradoxně tedy ten, kdo objektivně nemá odpovídající odborné vědomosti a právě proto zadává znalecký posudek, je ze zákona povinen kontrolovat a hodnotit jeho odbornou úroveň a náročnost a podle toho přiznávat odměnu za vykonanou práci.

Hodnocení, jako proces zjišťování parametrů hodnoceného objektu, musí mít stanovena hodnotící kritéria, jinak je to nedefinovaný proces založený na individuálním postoji a schopnostech hodnotitele. Stávající stav podle mého názoru postrádá jakoukoliv logiku a vytváří jen další prostředí pro případné korupční jednání, potažmo pro vznik tlaků, které potenciálně mohou ovlivnit objektivitu podaných posudků. Znalec se totiž touto úpravou dostává do podřízeného a závislého vztahu k zadavateli znaleckého posudku.

Znalecké obory

Aby bylo možné přistoupit k diskusi o odbornosti a specificky k implementaci obecných požadavků do oblasti forenzního zkoumání, je ještě jedna obecná problematika, která s tím přímo souvisí. Jestliže máme kvalifikovaně mluvit o odbornosti, musíme si primárně vyjasnit, o jaké odbornosti je řeč, zejména tedy jakých oborů se to týká. Až poté, co bude jasno v oborech, lze mluvit o odbornostech, které těmto oborům odpovídají.

Znalec je podle stávající právní úpravy jmenován pro určitý znalecký obor, případně odvětví. Členění znaleckých oborů je stanoveno ministerstvem spravedlnosti. Na tomto místě je potřeba přiznat, že aktuálně platné členění sice možná odpovídá historickému vývoji, avšak již méně současné realitě. O problémovosti stávajícího členění znaleckých oborů vypovídá mimo jiné i skutečnost, že pro skutečné posouzení toho, jakou odbornost který znalec v reálu zastupuje, bylo nutné zavést další pomocné členění, které se nazývá „specializace“. Jelikož však toto členění nemá oporu v zákoně, je formulováno většinou volně a nekontrolovatelně. Dostáváme se potom do situace, že znalec v oboru elektrotechnika se vlastně specializuje na výpočetní techniku, avšak pouze v oblasti oceňování informačních systémů. Takovýchto a podobných excesů je v seznamu znalců, který je veden krajskými soudy a ministerstvem spravedlnosti, plno. A určitě nelze říct, že to je pouze výjimka, překlep nebo nedopatření úředníka.

Jestliže existuje pouhý seznam znaleckých oborů a odvětví (byť vytvořen historicky) bez jakéhokoliv dalšího obsahu, popisu oboru a odvětví, rozsahu činností, pravidel a zdůvodnění vzniku toho kterého oboru a i kvalifikačních požadavků na znalce, je to pouze orientační vodítko, nemající žádný vědecký nebo zdůvodnitelný základ. Nelze se potom na něj odvolávat ve věcech kompetence znalců, nelze podle takového seznamu zákonem odkazovat na příbuzenství oborů a podobně. Nelze také jednoznačně a transparentně určit procesy, které umožní znalecké obory rozšířit, upravit nebo zrušit. Je zřejmě hodně oborů, kde nutnost podrobného popisu není až tak nezbytná, jsou to obory běžné a obecně známé, avšak jejich forenzní aplikace již tak triviální být nemusí. Jsou ale obory specifické nebo obory, kde jejich specifičnost je právě a jen v jejich konkrétní forenzní aplikaci.

Taxonomie znaleckých oborů je nezbytným předpokladem i pro mnoho ostatních procesů, činností a povinností, které jsou na znalce kladeny. V jednání u soudu je rozhodujícím „arbitrem“ při sporech, které mohou vzniknout v souvislosti s kompetencí znalce, soudce. V dalších, zejména správních procesech, které se znalectvím souvisí, nelze rozhodovací pozici přidělovat státním úředníkům jenom proto, že taxonomie neexistuje. Státní úředník si v lepším případě vytvoří svůj vlastní (mnohdy unikátní) názor, podle kterého postupuje při správním řízení nebo při dalších postupech a procesech, které se znalectvím souvisí.

Z druhé strany je potřebné přiznat, že řešení problému správné taxonomie znaleckých oborů není jednoduchou záležitostí a určitě to je otázka základního vědeckého výzkumu. Ale rezignace na jakoukoliv, byť částečnou snahu o nastavení základních pravidel a parametrů není řešením problémů, které s tím souvisí. Tady se také opět projevuje to, že v ČR není kompetentní orgán nebo instituce, která by se forenzními vědami systematicky zabývala, a tudíž ani elementární problémy nemá kdo řešit, ne to základní otázky existence forenzních věd.

S precizováním znaleckých oborů přímo souvisí i hodnocení kvalifikace znalců. Jestliže máme v ČR v současné době celkem 130 znaleckých odvětví sdružených v celkem 50 znaleckých oborech a k tomu nesčetně různých specializací a bez jakéhokoliv upřesnění, co která konkrétní položka znamená, je posuzování odborné kvalifikace znalců paušálně podle několika málo nejasně a netransparentně nastavených kritérií téměř nerealizovatelné. Veškeré (byť jen potenciální) řídící a kontrolní mechanizmy státu v této oblasti nutně selžou.

V obdobné pozici jsou i znalci, protože si jen stěží mohou plnit povinnosti vzhledem k požadavku neustálého zvyšování své odbornosti a kvalifikace. Jestliže nejsou dány ani rámce, ve kterých je vhodné se pohybovat, může se stát, že vzdělání nebo profesní certifikace, odborně a i finančně náročné, nemusí být soudem nebo správním orgánem uznány jako relevantní. A to nechci v této souvislosti uvádět konkrétní zjevné a až možná absurdní případy, se kterými se potkáváme dnes a denně, není to účelem tohoto článku a ani by se to do rozumného rozsahu článku nevtěsnalo.

Systém výkonu znalecké činnosti

Než se dostanu k otázce kvalifikace znalců, je potřebné se ještě jednou vrátit k názoru profesora Musila. Jestliže přibližně čtvrtinu (přesněji celou poslední 4. kapitolu) svého článku věnuje kritice současného stavu právní úpravy znalecké praxe v ČR a selhávání odpovědnosti státu za organizaci a kontrolu soudně znalecké služby, je s podivem, že i přesto tvrdí, že *„systém, v němž za fungování znalectví nese organizační odpovědnost stát, který má garantovat kvalitu a dostupnost znalecké služby, se v podstatě osvědčil. Je však třeba ho důkladně inovovat a především reálně zajistit prosazení právní úpravy do života.“*

Jestliže má systém závažné nedostatky, je pouze otázkou objektivizovaného zhodnocení, zda je stávající systém vhodný a inovovatelný v našich konkrétních podmínkách, anebo zda nepoužít systém jiný. Jak bylo již uvedeno, současný systém organizace znalecké činnosti je řízen státem. Aby však správně a kvalitně fungoval, je nutné, aby stát vytvořil všechny odpovídající komponenty takového systému. A jestliže v současnosti stát selhává v řízení znalecké práce i podle stávajících pravidel, kde značné množství mechanizmů není nastaveno a regulováno, jak si povede při realizaci inovovaného (náročnějšího) řídicího systému?

Podle dostupných informací (např. Vácha, Kratěna, Zacharov, Znalecká činnost… Praha, ČVUT, 2013) systém centrálního státního řízení znalecké činnosti státem funguje v obdobném rozsahu pouze v několika málo státech Evropy a k obdobnému centrálnímu systému řízení znalecké práce v poslední době přešel pouze jeden z nejbohatších (a ve forenzní oblasti asi nejrozvinutějších) států Evropy – Nizozemí. Je ovšem pravdou, že ani v ostatních západoevropských státech není situace v této oblasti jednoznačně vyjasněná, většina států pozici znalců přímo ani neupravuje nebo využívá kombinaci volné konkurence znalců s profesními nebo jinými sdruženími, které zajišťuji základní požadavky na evidenci a kvalifikaci znalců.

Každopádně dobře fungující systém centrálního státního řízení výkonu znalecké činnosti vyžaduje kromě propracovanosti a komplexnosti samotného systému i velké náklady na jeho realizaci. Bez váhání mohu prohlásit, že v současnosti na takový systém nemáme ani prostředky a ani kapacity. I v případě, že by naši zákonodárci prosadili sebelepší právní normu v této oblasti, na její prosazení do života budou chybět právě zmíněné předpoklady, zejména materiální a lidské zdroje.

Ale jak již bylo naznačeno výše, existují i jiné systémy, které se ve světě, ale i u nás používají. Primárně to je samořízení formou oficiální a zákonem zřízené profesní komory. Pro stát by to bylo výhodné zejména ekonomicky – prakticky veškeré povinnosti, které má v současnosti a které by mu ještě měly přibýt v případě, že by skutečně chtěl odpovědně řídit znaleckou činnost, by takříkajíc spadly na bedra komory. Za to, že by se stát vzdal svého státního dozoru, by znalce postavil do pozice skutečné samosprávné nezávislosti. A s velkou pravděpodobností by i kvalita a odbornost znalců vzrostla právě samořídícími vlastnostmi profesní komory. Určitě více, než naznačují minimální snahy státu v této oblasti něco smysluplného konat. O to větší problém by musela řešit komora – řídit natolik různorodou profesní skupinu by nebyl jednoduchý úkol.

Reálně lze také uvažovat i o modelu, který by rezignoval úplně na řízení výkonu znalecké činnosti a ponechal to vše na znalcích samotných, pouze se stanovením základní právních a procesních požadavků (což se mimochodem od stávající regulace až tak moc neliší). Určitě by obratem vznikaly různá profesní sdružení, asociace nebo spolky a trh by relativně rychle způsobil, že by se jednotlivci nebo skupiny snažili výrazným způsobem kvalitativně vyniknout nad ostatními. Navíc, jestliže profesor Musil tvrdí, že způsobilost znalce je potřebné zakaždým kriticky přehodnocovat i při stávajícím centrálním státním způsobu řízení, a že se může kdykoliv stát, že *„i dodatečně vyvstanou nové skutečnosti, které způsobilost znalce, byť řádně jmenovaného a přibraného, mohou zpochybnit. Může to být např. dříve neznámý fakt, svědčící o vztahu znalce k obviněnému nebo jiným osobám zúčastněným na řízení nebo o jeho poměru k věci. Nelze vyloučit ani případy, kdy řádně jmenovaný nebo přibraný znalec ztratí svou způsobilost, např. v důsledku odhaleného nezákonného či neetického chování nebo zjištěných chyb, jichž se dopustil ve znalecké činnosti. U znaleckých ústavů může vyvstat dodatečná pochybnost např. proto, že se podstatně změnilo jejich personální složení, že z ústavu odešli dřívější osvědčení pracovníci apod. Zvlášť kriticky je třeba posuzovat splnění podmínek u znalců, přibraných do trestního řízení samotnými procesními stranami (§ 89 odst. 2, § 110a tr. řádu).“* Prostě by se ke všem znalcům přistupovalo v podstatě úplně stejně jako doteď, případně jako ke znalcům přibraným ad hoc. Jediné, co by přibylo, je to, že znalec by před soudem asi musel zakaždým obhajovat nebo dokladovat svoji kvalifikaci.

Ve všech případech, ať už zásadní inovací stávajícího systému nebo přechodem na jiný systém řízení výkonu znalecké činnosti, je nutné počítat s určitým ne právě krátkým přechodným obdobím, se stanovením nových oborů a kritérií pro jmenování znalců a také s jejich kompletní přeregistrací.

Jak také uvádí profesor Musil, *„pokládám za vážnou chybu, že se k zásadním otázkám znaleckého dokazování v trestním řízení, a to ani k právní úpravě, ani k obecnému fungování znalecké praxe, nevede fundovaná odborná debata. Existuje jen několik málo nových trestněprocesních prací, které se tímto problémem zabývají; jsou v nich obsaženy i cenné kritické a reformní postřehy, které by však potřebovaly detailnější rozpracování.“* Je jen škoda, že také nevyjádřil názor na příčiny toho, že se fundovaná odborná debata nevede, a jestli i něco existuje, je to právě jen z pohledu trestně-právního, ale ne z pohledu forenzního.

Znalectví a jeho praktický výkon není problém právní. Právo dává znalectví pouze základní rámec pro využití v procesu dokazování. **Forenzní vědy, které jsou interpretovány svojí praktickou realizací právě znaleckým zkoumáním, se pro účely trestně-právní zabývají metodami odhalování a zkoumání kriminalistických stop. Úkolem těchto metod je za využití vědeckých postupů odhalovat objektivní pravdu o skutečnostech, dějích a procesech, které napomáhají objasňovat trestnou činnost a své výsledky prezentovat prostřednictvím znaleckého zkoumání ve formě, která je srozumitelná všem účastníkům soudního líčení.**

Podmínky pro výkon a rozvoj forenzních věd, pro tvorbu a aplikace nových metod znaleckého zkoumání, nejsou upraveny ani zákonem o znalcích, ani odpovídajícími paragrafy trestního řádu. Ty pouze stanovují pravidla a požadavky na výkon znalecké činnosti. **Znalecká činnost je**

pouze interpretací a použitím výsledků forenzních věd v konkrétní praxi. Je jednoznačně nutné konstatovat, že právě podmínky a rozvoj forenzních věd jsou v ČR zanedbávány, pro mnoho oborů ani nikdy nebyly vytvořeny. Neexistuje také prakticky žádný systém přenosu poznatků forenzních věd na znalce – tedy na vykonavatele a praktické realizátory poznatků forenzních věd, ani jakákoliv kontrola správnosti praktického výkonu znalectví.

Jestliže kritizujeme některé znalce za nekvalitní znalecké posudky, za nekvalifikovanou práci, za neprůhledné nebo nepodložené postupy nebo závěry, kritizujeme vlastně ty nesprávné (přirozeně kromě lidských slabostí, které se nevyhýbají žádnému člověku). Základní problém je v tom, že znalci obecně nejsou vědci, kteří objevují a vyvíjejí forenzní metody a postupy, znalci pouze lépe nebo hůře aplikují vědecky zdůvodněné a ověřené postupy do praxe výkonu znalecké činnosti. Jestliže neexistuje systém forenzních věd, jestliže není vytvořen systém aplikovaného výzkumu a následně vytvořen systém školení, vzdělávání a praktických cvičení, znalcům nezbývá, jen vykonávat znaleckou činnost „podle svého nejlepšího vědomí a svědomí“, a byť by byli odborníky ve svém oboru a splňovali veškeré formální požadavky, které jim předseda krajského soudu nařídí (třeba i na základě doporučení jeho poradního sboru), a byť budou znát, jaké formální náležitosti má mít znalecký posudek, bez znalosti specifických forenzních postupů a metod nebudou jejich znalecké posudky nikdy odpovídat náročným požadavkům, které jsou obecně na důkazy předkládané soudu kladeny.

Odbornost znalců

Přání (nebo spíše požadavek), aby všichni znalci, kteří jsou uvedeni v seznamu znalců (v současnosti jich je v ČR téměř 10 000, přičemž podle Wikipedie bylo v USA v roce 2010 forenzních specialistů celkem 12 000), byli kromě profesionálů ve svém oboru také vědci, kteří v každém ze svých znaleckých oborů a odvětví zároveň vyvíjejí a ověřují forenzní metody a postupy tak, aby výsledkem jejich práce byl znalecký posudek s maximální důkazní sílou, je nereálné. Je zjevné, že od znalců se to mylně očekává a vyžaduje. Jestliže celý systém od základního výzkumu až po praktický výkon znalecké činnosti neexistuje a na druhé straně je od výkonu znalecké činnosti očekávaná špičková kvalita, jsou taková očekávání lichá.

Lze přirozeně znalcům nařídit, např. novelou zákona, aby iniciativně a samostatně pokryli tento nedostatek, aby sami prováděli forenzní výzkum, přebírali vědomosti a zkušenosti (zejména ze zahraničí), vytvářeli a ověřovali v praxi metody a postupy zkoumání kriminalistických stop, aby znali cizí jazyky (protože v ČR základní forenzní výzkum téměř neexistuje), investovali do přístrojů a technologií, které pro výzkum potřebují, a navíc měli energii a čas na všechny tyto činnosti, povětšinou vedle svého hlavního zaměstnání. Vše výše uvedené jsou však činnosti (a s tím spojené výdaje), které nejsou přímými náklady na zpracování konkrétního znaleckého posudku, tudíž není toho, kdo by je uhradil.

Neustále se zvyšující nároky na znalce jsou, z důvodu neustálého vývoje vědy, technologií, ale i pokročilých způsobů páchání trestné činnosti, nutné. Jenomže každé navýšení požadavků na odbornost nebo na metody a způsoby práce jen navyšuje náklady na znalecké zkoumání, které jsou beztak již výrazně ze strany státu podhodnoceny, takže tudy reálně cesta nevede a jsme prakticky v bezvýchodné situaci.

Závěr

Pokud si hrajeme na vlastním českém písečku, nikoho to asi příliš nepálí, jsme takoví, jaká pravidla máme interně nastavena. V současném světě však zjišťujeme, že skoro všude okolo nás se to dělá jinak. Dovedu si i představit, že současná politika a ekonomická situace neumožňuje mnoho věcí. Ale rezignovat na tak důležitou oblast jako je soudní znalectví, oblast, která zajišťuje moci soudní důkazy pro rozhodování? Asi to není z našeho současného celospolečenského pohledu důležitá oblast, máme mnohem důležitější problémy k řešení, asi všem odpovědným a většině současných znalců vyhovuje, že se znalectví vykonává v zásadě tak, jak bylo stanoveno minulým režimem před půl stoletím. Že

jsou sice nastavena jakási formální pravidla a formální privilegia, která však ve skutečnosti nedovolují nahlédnout pod pokličku samotného výkonu znalectví. Že znalectví je opředeno rouškou tajemství, neboli diplomaticky vyjádřeno „ vysokou odborností“, a že je to vlastně mnohdy black-box, nebo jak se trefně česky říká „věštění z křišťálové koule“. Nikoho nepálí, že to má všechno být naopak? Že znalectví musí být tím nejprůhlednějším a kdykoliv ověřitelným a přezkoumatelným oborem, že použité metody musí být vědecky zdůvodněny?

Dnes snad nikoho netrápí výrok znalce typu „detailním znaleckým zkoumáním bylo zjištěno, že tato černá koule je bílou kostkou“. Znalec řekl, tak to tak je. Znalec prohlásil, že „sklo po detailním znaleckém zkoumání vykazuje všechny charakteristiky čistého krystalického uhlíku“, že “žlutý kov po podrobné analýze je prvek s atomovým číslem 79“. Nikde ani zmínka jak konkrétně k tomu došel. Kde jsme, jestliže znalec v oblasti digitálních technologií s vážnou tváří prohlásí (nota bene písemně do posudku), že „identitu dvou kopií digitálních videozáznamů posuzoval postupným prohlížením obou záznamů na monitoru s vysokým rozlišením“ a všichni se tváří, že je vše v pořádku? Kde tedy jsme s tím našim znalectvím?

Vůbec tím nechci paušalizovat, je mnoho znalců, kteří nespadají do výše uvedených kategorií. Jsem přesvědčen, že většina. Přesvědčení moje, ale i kohokoliv jiného, ale nestačí. Nestačí v tak důležitých věcech, jako je získávání důkazů. Musí existovat systém. Systém, který sice nevyloučí excesy, ale takové výjimky minimalizuje. Zjevně je v celkovém přístupu státu k problému znalectví (říkám „problému“, protože systémem se to nazvat nedá), chyba. Zjevně to stávající řešení sice stanovuje formality (ano, nezbytně nutné), ale o kvalitě mlčí. O pravidlech, která by cíleně působila na kvalitu. O systému, který by vytvářel předpoklady kvalitního výkonu. Ať už by to byly zásady rigidní regulace, typu zřízení specializovaných výzkumných a vzdělávacích institucí, které by zajišťovaly povinné atestace (kdo by ale přednášel, v jaké kvalitě a kdo by to platil a z čeho?), ať už by to byl systém znalecké komory, profesního samoregulačního orgánu typu lékařské, farmaceutické nebo advokátní komory, nebo ať by to byl systém volné konkurence, kdy by existovalo tržní soutěžení typu dobrý znalec – vyšší sazby a ten kdo prohraje, platí vše. Nic takového však není. Jen se udržují kalné vody nevědomosti. Nevědomosti toho, jak se dělají znalecká zkoumání.

Profesionalita ale pláče. Profesionalita soudních znalců je ve stávajícím stavu pouze dobrou vůlí těch vnitřně odpovědných. Profesionalita je pouze koníčkem. Jsou to ty správné základy, na kterých stojí soudní znalectví, rozvoj forenzních věd a získávání důkazů pro rozhodování soudů, na kterých závisí osudy lidí?

Už vidím ty mnohokráte opakované argumenty, že aktuálně platný zákon je vlastně postaven geniálně, že se vlastně osvědčil, a když už vydržel 50 let, není ani potřeba jej měnit. Drobné novely typu vypuštění slova „socialistický“, zavedení pokut a častějších formálních kontrol pro znalce nebo drobná změna sazby za hodinu práce apod. plně postačují. Když se mne ale zahraniční kolegové ptají na hodinovou sazbu, kterou mi stát za znaleckou práci platí, nevěří mi a tváří se, že se úmyslně stavím do pozice chudáka, aby mne litovali. Asi jim budu příště lhát, abych nevypadal jako blbec.

Jen jedna poznámka na závěr – hodinová sazba soudního znalce v ČR je na úrovni necelých 14% z průměru hodinové sazby znalců v EU, a tím je se značným odstupem na nejnižší příčce v Evropě! A jen tak mimochodem, tato hodinová sazba je přesně na úrovni právě zaváděné minimální mzdy v Německu. Co k tomu ještě dodat?

DEAS - Digital Evidence Acquisition Suite

Efektivní a jednoduchý nástroj pro pořizování binárních kopií (obrazů) disků

Jiří Hološka, Ph.D., GCFA
holoska@rac.cz
ICT Security Consultant, Digital Forensic Certified Expert, Incident Response Analyst

Anotace:

Článek popisuje produkt DEAS, který je určen pro jednoduché, efektivní a intuitivní pořizování forenzních kopií dat, tzv. obrazů disků. V úvodu stručně popisuje základní důvody jeho vzniku, dále se věnuje nástrojům, které jej tvoří, a nakonec stručně popisuje způsob jeho ovládání a praktického použití.

Úvod

Jedním z primárnímch úkonů forenzního zkoumání digitálních dat je pořízení identické, tzv. binární, kopie originálního nosiče. Často se této operaci také říká vytvoření obrazu disku (v angličtině "disk image"). Proč tomu tak je?

Prvním důvodem, který vede k vytváření binárních kopií dat pro účely forenzního zkoumání je objektivní skutečnost, že pro digitální data platí, že kopie digitálních dat je identická s origiálem. Z tohoto pohledu je tedy zcela jedno, zda zkoumáme originál nebo jeho digitální kopii.

Druhým důvodem je skutečnost, že digitální data jsou z podstaty extrémně náchylná na změnu. Vyplývá to z faktu, že pro běžnou práci s daty je vyžadována co nejvyšší rychlost jejich čtení a zápisu (tedy změny). Tomu jsou přizpůsobeny používané technologie, které jsou založeny primárně na změně magnetizmu, resp. v současnosti na změně elektrického náboje. Rychlost těchto změn (rychlost zápisu na médium) dosahuje aktuálně 500 MB za sekundu. Pro názornost si to lze představit tak, že přibližně za 1 sekundu lze smazat řádově statísíce souborů nebo za stejnou sekundu důkladně zničit (přepsat) přibližně 10 000 běžných dokumentů.

Abychom se tedy vyvarovali jakékoliv změny originálních dat, ke které může při zkoumání dojít, mimo jiné i neúmyslně, forenzní zkoumání digitálních dat probíhá zásadně na kopiích originálních dat. Toto pravidlo je zakotveno ve všech mezinárodních doporučeních pro forenzní analýzu digitálních dat a i v mezinárodně platných standardech, např. ISO/IEC 27037. Všechny tyto principy a postupy jsou do forenzní analýzy digitálních dat zařazeny z důvodu zajištění integrity důkazů.

Pro správné vytvoření binární kopie dat pro digitální forenzní analýzu je k dispozici i několik ověřených nástrojů. Mezi nejčastěji používané patří např. program "dd" a jeho klony, které pracují pod operačním systémem Linux. Mezi další často používané patří komerční nástroje, např. FTK Imager nebo EnCase a některé další (např. X-Ways Forensic, IXImager a jiné). Každý z uvedených nástrojů má své výhody i nevýhody. Jaká kritéria by takové nástroje měli splňovat? Pokusíme se je naznačit.

Nejdříve vyjdeme s faktu, že zajištění dat formou binárních kopií se provádí jak ve forenzní laboratoři, tak stále častěji i na místě zajištění. Proto jedním z důležitých parametrů nástroje pro práci na místě je jeho rychlost. Rychlost nástroje ovlivňuje hned několik faktorů (když odhlédneme od fyzických parametrů zdrojového a cílového disku). Jsou jimi:

- samotná konstrukce programu (tedy zda programátoři vytvořili program s důrazem na tento parametr);
- použitý programovací nástroj (obecně platí, že čím sofistikovanější vývojové prostředí bylo

použito, tím pomalejší je výsledný produkt);
► využití rychlého interface pro připojení zdrojového a cílového disku;
► použitý operační systém - pravděpodobně nejrychlejšími jsou speciálně vytvořené operační systémy (např. pro program IXImager), jinak obecně platí, že práce programu pod systémem Linux v terminálovém módu je rychlejší než např. pod Windows;
► využití komprese cílového obrazu disku zajistí menší objem ukládaných dat na cílový disk, což může někdy i výrazně zrychlit celý proces (např. když zdrojový disk je SSD a cílový je klasický HDD), navíc následná případná manipulace a analýza může také proběhnout rychleji.

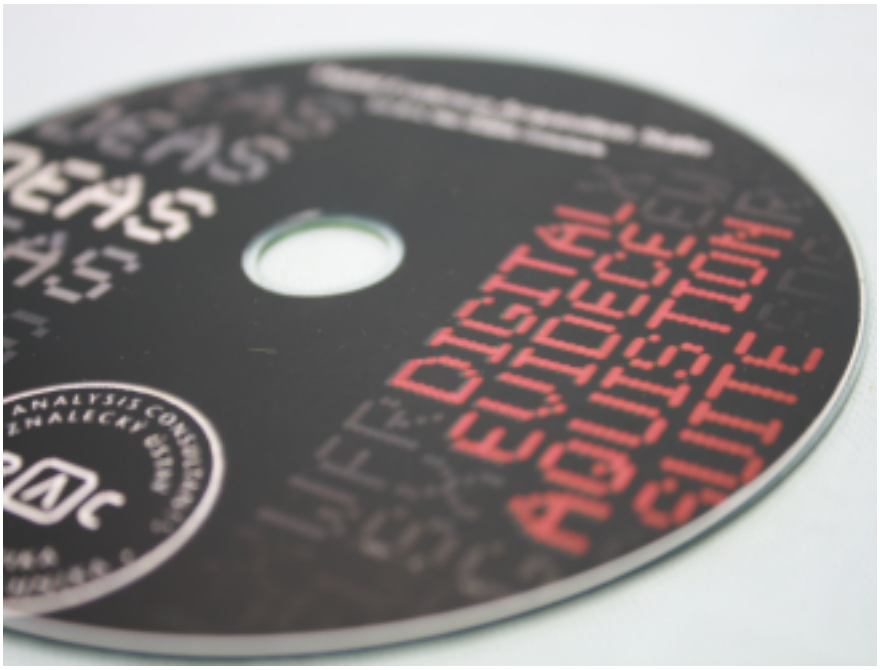
Dalším parametrem, důležitým pro práci těchto programů, je bezpečnost prostředí (operačního systému) z pohledu zachování integrity zdrojových dat. Zkušenosti říkají, že práce pod operačním systémem Linux lépe vyhovuje požadavkům na zajištění integrity zdrojového disku. Dá se dovodit, že nastavení módu "read-only" pro Linux při připojení zdrojového disku do systému by mělo být dostatečnou zárukou zachování integrity dat, kdežto např. pro systém Windows platí, že při připojení zdrojového disku by mělo být vždy použito speciálního modulu (nejlépe hardwarového) pro ochranu zápisu na zrojový disk (nicméně použití takového modulu i pro Linux je výrazně doporučeno).

DEAS

DEAS je nástroj, který vychází z výše uvedených faktorů. Je to tzv. boot CD s operačním systémem Linux a vybranými nástroji pro pořízení forenzních binárních kopií disků. Navíc je pro jednoduchost práce s nástrojem vytvořeno jednoduché a přehledné menu, které vede uživatele způsobem, který eliminuje lidskou chybu. To je důležité zejména proto, že:
► při práci na místě zajištění se výrazně projevuje stresový faktor, který může způsobit chybu i kvalifikovaného operátora (např. záměna zdrojového a cílového disku by nenávratně zničila důkazy);
► jednoduché menu výrazně snižuje kvalifikační nároky na obsluhu programu, není potřeba detailně znát a zadávat řadu parametrů a práci s programem zvládne po vyškolení i technik, který nezná detaily použitého programu nebo operačního systému.

DEAS se dodává s následujícími forenzními nástroji pro vytváření forenzních binárních kopií disků (obrazů disků):

FTK Imager - linuxová verze (https://ad-pdf.s3.amazonaws.com/Imager%203_1_4_UG.pdf) je prostředek na vytvoření obrazů a náhledů dat. Rychlý náhled umožňuje vybrat, které součásti má význam zkoumat v aplikaci AccessData Forensic ToolKit (FTK) a které nikoli. FTK Imager také umožňuje vytvoření přesné kopie (forenzní obraz) počítačových dat bez změny orginálu. FTK Imager

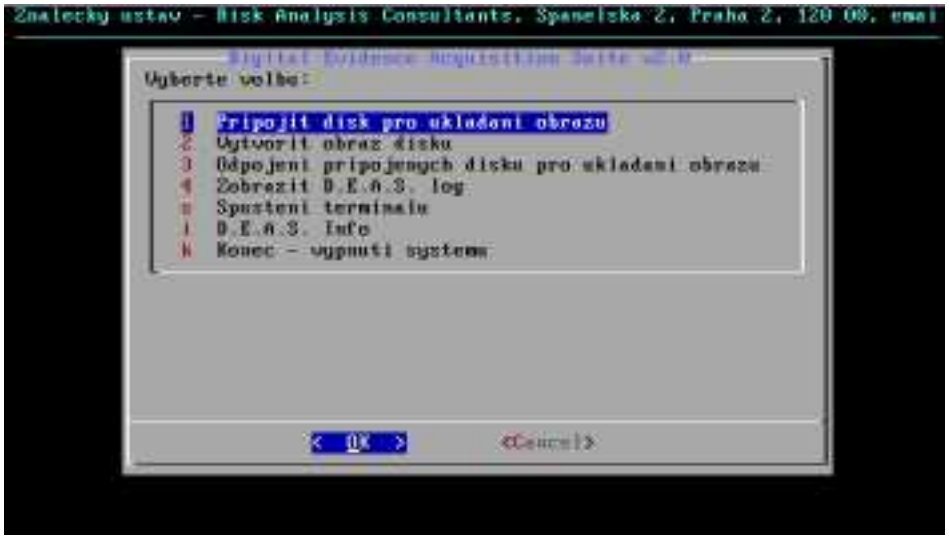


Obr. 1 *CD s nástrojem DEAS*

umožňuje náhled na složky a adresáře na zdrojovém lokálním disku, síťovém disku, disku CD/DVD, vytvoření přesné kopie lokálního disku, disku CD/DVD, adresářů anebo individuálních souborů, export/extrakci souborů a adresářů z obrazu disku, generování hash reportů pro jednotlivé soubory nebo celé obrazy. FTK Imager podporuje také různé formáty dat forenzních kopií disků a konverze mezi nimi.

Libewf (https://code.google.com/p/libewf/) je nástroj pro tvorbu obrazů disků ve formátu EWF (Expert Witness Compression Format), kterými jsou např. často používané formáty obrazů disků (SMART) .s01 nebo (EnCase) .E01 a .Ex01.

Oba použité nástroje jsou ovládány pomocí jednoduchého menu, které umožní uživateli zvolit jeden z nabízených nástrojů (FTK Imager nebo Libewf), zadat zdrojový a cílový disk, zadat několik základních parametrů a informací o pořizované kopii disku. Umožňuje vytvářet komprimovanou kopii zdrojového disku (případně ji ještě ochránit heslem).



Obr. 2 *Ukázka úvodního menu nástroje DEAS*

Menu nástroje je pohodlně a intuitivně ovládatelné pomocí šipek, pouze při zadávání specifických parametrů (např. názvu cílového souboru nebo zadávání konkrétních parametrů nebo pomocných identifikačních informací) je vyžadován vstup z klávesnice. Práce s nástrojem je podrobně ošetřena na uživatelské chyby a tím je výrazně eliminována chyba uživatele. O práci s nástrojem DEAS je veden log, který se ukládá společně s cílovým obrazem disku a dokumentuje činnost uživatele, jakož i parametry, které byly použity při vytvoření daného obrazu disku.

Praktické ověření prokazuje, že v konfiguraci, která je použita v DEAS, je pořizování forenzních binárních kopií disků výrazně rychlejší, než v případě použití nástroje FTK Imager pod Windows, nebo při použití linuxového nástroje "dd" (nebo jeho forenzních variant), který se aktuálně stále používá v policii. Zrychlení, zjednodušení ovládání a zkvalitnění ochrany výsledných obrazů disků použitím nástroje DEAS výrazně přispěje k rychlosti a spolehlivosti práce při zajištění dat na místě.

C4e

Czech CyberCrime Centre of Excellene (C4e) - České centrum excelence pro kybernetickou kriminalitu (www.c4e.cz)

Ing. Marián Svetlík st.
svetlik@rac.cz
Člen řídícího výboru C4e a vedoucí pracovní skupiny "Vzdělávání a školení" (Education and Training)

Anotace:

Článek seznamuje čtenáře s projektem C4e (Czech CyberCrime Centre of Excellence). Popisuje základní cíle a záměry Centra, oblasti klíčových aktivit a podíl jednotlivých partnerů na práci Centra. Popisuje základní náplň jednotlivých pracovních skupin a nastiňuje plánované výsledky jejich dosavadní činnosti. Nastiňuje také budoucí orientaci Centra. Čtenář získá úvodní informaci o existenci a práci C4e a také o rámci a problémech, se kterými se může na C4e obrátit.

Vznik

Vznik Českého centra excelence pro kybernetickou kriminalitu (C4e) byl umožněn díky společnému úsilí širokého spektra českých expertů z akademického sektoru, Policie České republiky, soukromých forenzních laboratoří, Národního bezpečnostního úřadu, justice, státního zastupitelství a ostatních oblastí.

Tito experti byli ochotni spojit svoje know-how směrem k vytvoření skutečného a respetkovaného subjektu v oblasti vzdělávání, výzkumu a vývoje v oblasti kybernetické kriminality, který pokrývá všechny související aspekty, jako je právo, technický vývoj, vzdělávání, a další. Všechny aktivity jsou orientovány zejména na zlepšení celkové kvalifikovanosti všech subjektů zúčastněných na prevenci a vyšetřování kyberkriminality.

Samotný vznik C4e a zahájení jeho činnosti bylo umožněno díky grantu, který byl v roce 2013 poskytnut Evropskou komisí v rámci programu "Prevention of and Fight Against Crime 2007 - 2013 / Illegal use of Internet".

Hlavní snahou C4e je posílit všeobecné povědomí a efektivnost práce v oblasti prevence a vyšetřování kyberkriminality zejména prostřednictvím aktivit jako :

- orgaizace konferencí, workshopů seminářů a školení pořádaných pro partnery a ostatní veřejnost s cílem posílení vzdělání a know-how cílových skupin, zejména policie, státních zástupců a soudců.
- vývoj a tvorba efektivních a dostupných nástrojů a prostředků pro cílové skupiny, zejména pro policii, ale také pro správce kritické infrastruktury.
- tvorba a distribuce návodů, best practises a standardů v oblastech elektronických důkazních prostředků (získávání, analýza, reportování, užití), vyšetřování relevantních případů, provádění digitálních důkazů před soudem.

Úkoly

Základním úkolem C4e je podpořit Českou republiku v boji proti kybernetické kriminalitě.

V ČR absentuje kvalifikovaný ústřední bod know-how v oblasti kyberkriminality. Snahou C4e je koncentrovat nejlepší experty v oblasti kyberkriminality a být ústředním bodem znalostí ve všech oblastech vyšetřování kyberkriminality, např. v oblastech získávání, analýzy, vyšetřování a provádění elektronických důkazních prostředků. C4e tedy směřuje k tomu stát se centrem znalosti, specifickým typem think-tanku.

Všechna tato snaha je realizována v úzké mezinárodní spolupráci. C4e se chce stát jedním z klíčových členů mezinárodní sítě obdobných národních center a navázat a pokračovat v celoevropské iniciativě 2CENTRE (www.2centre.eu). Většina zmíněných výstupů bude tvořena v těsné spolupráci a v koordinaci těmito centry.

Hlavní cíle

Hlavními cíly projektu C4e jsou:

- spojit síly širokého spektra expertů s cílem vytvoření českého znalostního centra v oblastech prevence, detekce, vyšetřování a stíhání všech typů kybernetické kriminality,
- vytvoření a implementace vzdělávacího systému pro naše partnery a sady školení a speciálních vzdělávacích programů a implementace systematického přístupu k vzdělávání a kvalifikaci cílových skupin,
- vytvoření podmínek pro vznik výzkumného a vývojového centra v technologických, metodických a právních oblastech boje proti kybernetické kriminalitě,
- vytvoření centra a zdrojového místa sdílení informací s evropskými a světovými partnery pro všechny cílové skupiny,
- nabídnout služby spolehlivého partnera pro ostatní mezinárodní subjekty plánující vytvoření vlastních národních center. Nabízíme jim výměnu informací a praktických zkušeností s projektovým managementem, vytvořením a provozem centra excelence pro kybernetickou kriminalitu.

Cílové skupiny:

Cílovými skupinami jsou všechny subjekty, které se jakýmkoliv způsobem setkávají nebo účastní boje proti kybernetické kriminalitě, zejména ale:

- policie,
- zpravodajské a bezpečnostní složky,
- bezpečnostní týmy (CSIRT),
- justice,
- akademická sféra,
- veřejnost.

Tým C4e

Řešitelský tým C4e je veden specialisty Ústavu výpočetní techniky Masarykovy univerzity (MU), Ústavu práva a technologií MU a Znaleckého ústavu společnosti Risk Analysis Consultants (RAC).

Tým je dále doplněn o přední odborníky z ČR i z Evropy, z ČR jsou to např. specialisté z Národního bezpečnostního úřadu (NBÚ), Kriminalistického ústavu Praha (KÚP), Justiční akademie (JA) a Policejního prezídia (PP) Policie ČR a mezinárodní tým doplňují odborníci z Velké Británie z De Monfort University a ze společnosti n-Gate. Dále nám pomáhají odborníci z Ústavu matematiky a počítačových věd Univerzity v Litvě a z Ústavu soudního inženýrství v Žilině. V jednání je spolupráce s dalšími partnery, např. s Policejní akademií ČR (PA)

nebo ze Slovenskou technickou univerzitou (STU) v Bratislavě.

práce partnerů je koordinována primárně na Ústavu výpočetní techniky MU a ve Znaleckém ústavu RAC.

Základní oblasti

Zaměření činnosti C4e je rozděleno do tří klíčových oblastí, tzv. pracovních balíčků. Jsou jimi "Výzkum a vývoj", "Právní rámec pro kybernetickou kriminalitu" a "Vzdělávání a školení".

► **Výzkum a vývoj.** Cílem je navrhnout a vyvinout technické a programové prostředky, které by napomáhaly v odhalování kybernetické kriminality. Aktuálně probíhá výzkum a vývoj ve dvou základních směrech, kterými je jednak síťová forenzní analýza a analýza bezpečnostních síťových útoků a jednak implementace metodických doporučení a nejlepších světových praktik a standardů v oblasti Digital Forensic do nástroje pro řízení forenzní laboratoře. Aktuálně je vývoj realizován a

► **Právní rámec** kybernetické kriminality. V této oblasti probíhá aktuálně kromě jiných aktivit práce na komparativní studii regulatorních úprav kybernetické kriminality a kybernetické bezpečnosti napříč celou Evropou, probíhá sběr a vyhodnocení informací, které nám poskytují různé relevantní subjekty z celé Evropy.

► **Vzdělávání a školení.** Tento pracovní balíček se aktuálně zaměřuje do dvou směrů. Jednak na vytvoření a uvedení do praxe celého systému vzdělávání příslušníků Policie ČR v oblasti práce s digitálními důkazy a kybernetickou kriminalitou a jednak na vytvoření uceleného širšího systému různých školení v oblasti kybernetické kriminality, které budou uzpůsobeny různým cílovým skupinám a různým úrovním posluchačů.

Další aktivity

C4e průběžně vyvíjí i mnoho dalších aktivit, které jsou zaměřeny jak na podporu výše uvedených pracovních balíčků, tak do dalších oblastí, které přímo či nepřímo s kybernetickou kriminalitou souvisí.

C4e např. spolupracuje s NATO, naši zástupci byli jako konzultanti pozváni na zatím největší NATO Cyber Security cvičení. Spolupracujeme s NBÚ v oblasti kybernetické bezpečnosti státu a jako jedni z mála v Evropě komplexně (technicky i právně) řešíme např. problematiku vzájemného vztahu CERT týmů a policie při identifikaci trestné činnosti, nastavení regulatorních limitů, cekového rámce takové spolupráce a technických prostředků výměny relevantních informací. C4e bylo i aktivním účastníkem otevření "Národního centra kybernetické bezpečnosti" v Brně, kde v rámci odborné konference zajišťovalo celé druhé odpoledne programu konference. V rámci mezinárodní spolupráce rozjíždíme společné projekty s partnery ze Slovenska v oblasti metodik forenzní práce a vzdělávání expertů v obou státech. Naše aktivní účast a vystoupení na odborných konferencích a obdobných aktivitách v Evropě vytváří dobré předpoklady i pro další efektivní mezinárodní spolupráci. Mimochodem, vydání tohoto časopisu je umožněno také dílčím způsobem právě díky C4e. Některé další konkrétní informace o činnosti C4e jsou na našem webu.

Závěr

Nedávno uběhl rok od založení Czech CyberCrime Centre of Excellence. Možná by se mohlo zdát, že C4e zatím není natolik známé a není až tak vidět výsledky, kterých jsme zatím dosáhli.

Naše koncepce a přístup k problematice boje proti kybernetické kriminalitě však nejsou založeny na zviditelnění ad-hoc aktivit a činností, ale na přípravě a postupné realizaci sady systémových kroků tak, aby celý koncept a následně i jeho výsledky byly založeny na pevných, dobrých a systematických základech.

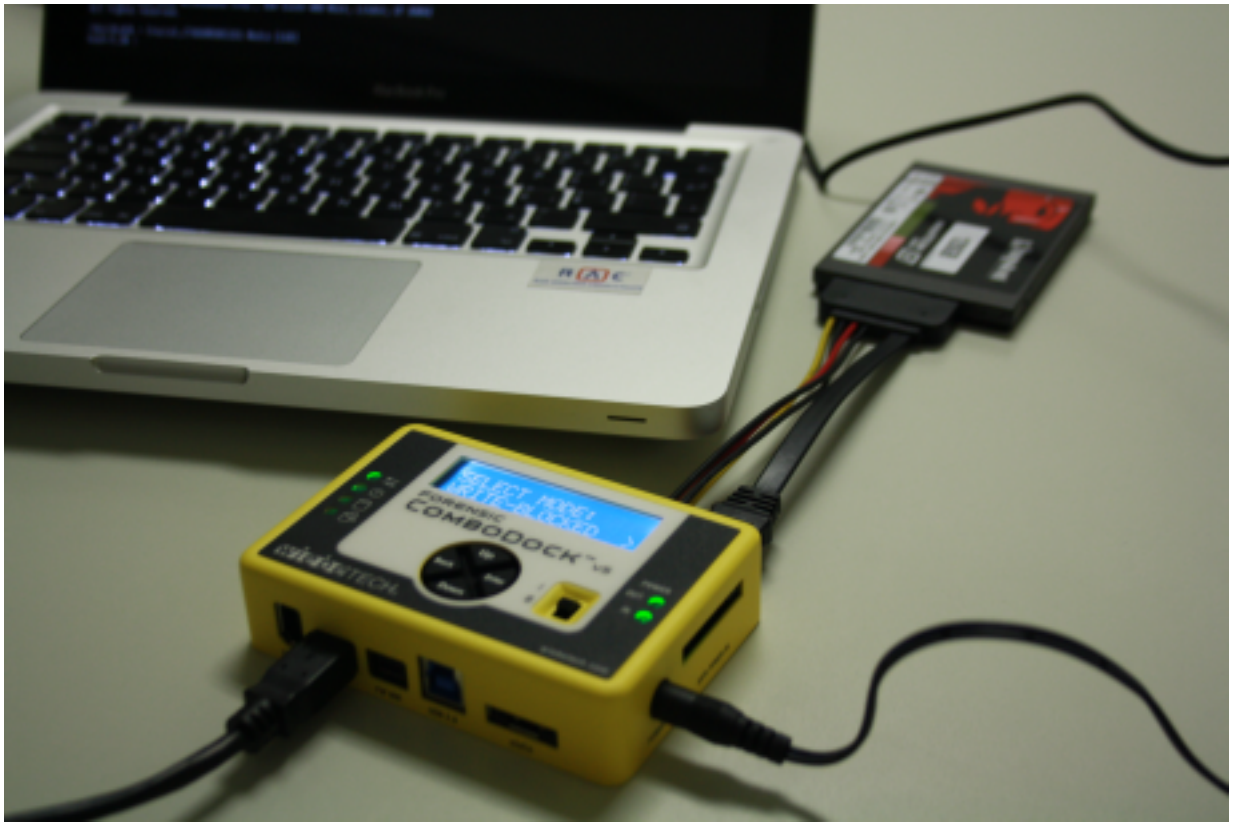
Postupná, koncepční a systematická práce vytvoří dobré předpoklady k dalším krokům a společně s partnery a i všemi zainteresovanými institucemi a organizacemi budeme na takových základech dále rozvíjet problematiku boje proti kybernetické kriminalitě, zkvalitňovat její identifikaci, odhalování, vyšetřování a potírání.

DOBRÁ PRAXE

Ilustrativní snímek, znázorňující připojení zdrojového disku (v tomto případě SSD disku) k notebooku (obecně k technologickému počítači) za pomocí HW blokátoru zápisu.

Tato konfigurace zajišťuje, že při práci se zrojovým diskem (typicky při pořizování identické kopie zajištěného disku např. z domovní prohlídky) nedojde ke změnám v originálních datech. Použitím HW blokátoru zápisu zajistíme zachování integrity původních dat. Zajistíme tedy, že data, která tímto způsobem pochází z originálního disku, ať už to je jejich samotná binární kopie nebo výsledky dalších analýz nad těmito daty, odpovídají přesně stavu, který byl na zdrojovém disku v době, kdy byl výše uvedeným způsobem připojen k technologickému počítači.

Požadavek na použití blokátoru zápisu při práci se zdrojovými (originálními) daty vychází prakticky ze všech mezinárodních doporučení, která se týkají metod a postupů pro digitální forenzní analýzu.



Jak poskytovat výstupy znaleckého zkoumání

Ing. Marián Svetlík st.
svetlik@rac.cz
Soudní znalec v oboru Kriminalistika se specializací Kriminalistická počítačová expertíza, vedoucí Znaleckého ústavu společnosti Risk Analysis Consultants, s.r.o., viceprezident Akademie forenzních věd, z.s.

Anotace:

Článek se zabývá problematikou velkých objemů a různých formátů dat, které jsou výstupem znaleckého zkoumání v oblasti digitální forenzní analýzy.

Úvod

Ještě si celkem dobře pamatuji na začátky zkoumání digitálních dat v ČR, na první znalecké posudky, kde výstupem zkoumání byla data, nalezená na zkoumaném počítači. Tehdy nebyl problém ten jeden nebo několik málo souborů jako přílohu znaleckého posudku vytisknout.

Za přibližně čtvrtstoletí, co se v ČR systematicky provádí technické zkoumání prostředků digitálních dat, se situace výrazně změnila. Dnes se už nalezené soubory (až na výjimky) netisknou, ale vzhledem k neustálému nárůstu objemů dat se vytváří tzv. elektronická příloha na datovém nosiči. Většinou sice jako datový nosič postačuje jedno nebo několik DVD, ale nezřídka, když už by mělo být těch DVD více než 10 – 20, se výsledky zaznamenávají na jiné vhodné datové nosiče, např. na Flash disky nebo nezřídka i na externí pevné disky.

Problémy

S nárůstem objemů výsledků, které jsou podle zadavatelů znaleckých posudků požadovány, vzniká hned několik dosud neřešených problémů:

1. Ochrana dat. Standardně se pro zápis dat, která jsou výsledkem znaleckého zkoumání, používají nosiče CD nebo DVD. Kromě toho, že to je běžně a obecně známý a relativně levný[1] typ datového nosiče, má také výhodu v tom, že lze na něj zapsat data tak, že jsou ochráněna před přepisem, změnou nebo smazáním, záznam na CD/DVD je v tzv. „read-only" módu. Není tedy nutné je chránit nějakým dalším dodatečným způsobem a objednatel posudku s takovými datovými nosiči může teoreticky pracovat přímo[2]. Nevýhodou takového nosiče je však jeho omezená kapacita, která už nedostačuje současným požadavkům. Další nevýhodou může být nespecifikovaná trvanlivost záznamu[3]. Uvádí se sice něco kolem 5 – 10 let, ale zaručit to nelze a u některých nosičů se záznam postupně degraduje již po třech letech (ověřeno praktickou zkušeností a v závislosti na skutečném výrobci, skladovacích podmínkách, zápisové i čtecí mechanice a dalších faktorech).

S většími objemy dat elektronických příloh znaleckých posudků (nezřídka i stovky GB až několik TB) je jedinou cestou použít takové datové nosiče, které mají vyšší kapacity. V jednodušších případech je možné použít USB Flash disky (pro kapacity řádově max. 64 GB), jinak se i z hlediska ceny jako další vhodný nosič jeví už jenom externí USB pevný disk. Toto řešení má nespornou výhodu v tom, že veškerá data přílohy jsou na jednom nosiči a tedy je ke všem datům pohodlný přístup a zadavatel s daty může pohodlně pracovat, dále je rychlost přístupu k datům nesrovnatelně vyšší, než při čtení dat z CD/DVD. Nemalou úsporu takové řešení poskytuje i v procesu zápisu dat na takový druh nosiče.

Při tomto způsobu řešení záznamu velkých objemů dat však vzniká problém, kterým je ochrana zapsaných dat vůči úmyslným nebo i neúmyslným změnám. Tento druh nosičů totiž nemá jednoduchou[4] možnost nastavit ochranu zápisu zaznamenaných dat. Je sice pravdou, že pro veškerá data elektronické přílohy jsou (nebo spíše by měly být) spočteny kontrolní sumy, pomocí kterých lze ověřit, zda nedošlo ke změně originálních dat, takže takovou změnu lze zjistit, ale v principu jí nelze relativně jednoduchým způsobem zabránit. S takovými daty je tedy nutné pracovat velice opatrně a jakákoliv činnost, i pouhé jejich prohlížení[5], musí být provedeno přísně a výlučně na kopii dat, nikdy ne na datech elektronické přílohy.

2. Struktura dat. Podstatou tohoto problému je způsob, jakým jsou data na elektronické příloze uložena a jaké všechny informace k těmto datům jsou uvedeny a jakým způsobem. V případě, že se jedná o několik desítek, případně i stovek souborů, se způsob a struktura dat nezdá být podstatná a důležité je, že jsou veškeré požadované informace uvedeny. V případě takovýchto relativně malých počtů výsledných souborů lze dožadujícím vyjít vstříc i v případech, kdy požadují zpracovat jiné nebo dodatečné přehledy o datech na elektronické příloze (často se zdůvodněním, že *„jsou zvyklí na jiné uspořádaní dat“* nebo že *„pan státní zástupce – aby nemusel listovat v nějakých excelech – chce, aby informace byly přepsány do wordové tabulky“* nebo s tím, že *„je to potřeba předělat tak, aby na klíčové nálezy bylo možné se dostat maximálně na tři kliknutí myši, protože pan státní zástupce nebo soudce se nebude přece proklikávat celou souborovou strukturou“* a podobně). Jestliže však jsou v elektronické příloze uvedeny tisíce až statisíce souborů, takové dodatečné přeskupení souborů (např. ze struktury „klíčové slovo -> číslo stopy -> původní cesta na stopě“ do struktury „číslo stopy -> klíčové slovo -> původní cesta na stopě“) vyžádá i několik dnů intenzivní práce[6]. Z pohledu zadavatele se to může zdát jako trivialita, z pohledu zpracovatele posudku to je práce, která vyžaduje spoustu času s tím, že při reorganizaci dat na příloze samozřejmě nesmí dojít k jediné chybičce.

Při větších objemech dat začíná hrát podstatnou roli i samotné fyzické omezení rychlosti přenosu dat. Tady bych každému doporučil, aby si to zkusil sám a spustil jen pouhé překopírování např. 100 000 souborů z jednoho fyzického disku na jiný, např. na externí USB disk. Ve většině případů se výsledku dočká tak někdy do druhého dne.

Lze sice v těch nejabsurdnějších případech argumentovat, že znalec svůj úkol splnil a veškerá požadovaná data, která byla nalezena, jsou uložena (někde, byť identifikovatelně) na elektronické příloze. Ano, nicméně od míry spokojenosti klienta závisí i přiznání odměny za zpracování znaleckého posudku. Když totiž zadavatel „zhodnotí“ zpracování posudku z důvodu (pro něj) přílišné složitosti jako nedostatečné, má možnost svým vlastním rozhodnutím krátit znalci odměnu.

3. Formát dat. Různorodost formátů dat je asi největší problém, se kterým se potkáváme při přípravě elektronických příloh znaleckých posudků. Opět platí, že v případě menšího počtu souborů lze vyjít zadavateli vstříc a např. konvertovat je všechny, které jdou (nebo jen vybrané), například do formátu PDF. U (relativně) standardních formátů souborů se to dá vyřešit i jinak a mnozí zadavatelé jsou již postupně schopni se s většinou formátů nějak vypořádat.

Typickým problémem se však stávají e-maily. Mnohdy se setkáváme s protichůdnými požadavky typu *„musí to být tak, abychom sami mohli napříč všemi e-maily hledat (pomocí standardních možností OS Windows) další klíčová slova nebo vazby, nejlépe jak v hlavičce e-mailu, tak v jeho těle a nejlépe i v jeho přílohách, navíc tak, abychom k prohlížení e-mailů nemuseli instalovat žádný dodatečný SW[7]“*. Z pohledu zadavatele se pořád jedná o to samé – e-mail je přece e-mail, každý má hlavičku, tělo a případně přílohu – jak jednoduché! Málokdo z nich si však uvědomuje, že existuje více než 40 různých běžně používaných formátů, které se pro e-maily používají, a není triviálním problémem je poskytnout tak, aby bylo možné splnit všechny zadavatelovy požadavky na pohodlnou, jednoduchou a přehlednou následnou práci s nimi (a nejlépe bez nutnosti si cokoliv dodatečně instalovat).

Příčiny

Existují následující základní objektivní faktory, které způsobují výše uvedené problémy, a které je nutné si uvědomit jak na straně zpracovatelů znaleckých posudků, tak na straně jejich zadavatelů.

Tím prvním je celkový nárůst objemů dat a následně také i výrazný nárůst dat, které jsou pak poskytovány jako výstupy znaleckého zkoumání. Navíc z toho vyplývá, že při zvyšujících se celkových objemech dat je potřebné pro minimalizaci objemů výstupů použít výrazně přesnější specifikaci zadání. Platí jednoduché pravidlo, že čím je požadavek obecnější, tím více dat bude na výstupu. Následně pak se další práce objektivně přesouvá na zadavatele, protože díky stejné přesnosti zadání (při větších objemech dat na vstupu) se následně sám musí probrat velkým objemem výstupních dat[8].

To také souvisí se zažitým procesem přibrání znalce – znalci se položí na začátku otázky, poskytnou se mu podklady (stopy) a znalec poskytne výstupy. Není zvykem průběžně společně se znalcem vyhodnocovat přesnost dotazu a tím i objem nálezů, respektive iterativním způsobem upřesňovat zadání. To by způsobilo množství dalších organizačních problémů, např. by nebylo možné se dopředu domluvit na lhůtě a ceně posudku, muselo by se průběžně upřesňovat zadání, což by mohlo způsobit administrativně-procesní problémy. Požadavek na postupné zpřesňování zadání na základě průběžných výsledků je něco, co v jiných forenzních oborech není zvykem a procesně to není nikde jednoznačně ošetřeno. Naopak, vzhledem k regulaci nákladů na znalečné se preferuje „jednoprůchodové“ řešení, které však v těchto případech způsobuje dodatečné technické, personální, kvalifikační, termínové a tedy i procesní a finanční potíže jak na straně znalce, tak na straně zadavatele. Objektivně se zvyšují náklady na znalečné a, bohužel, dodatečné náklady na straně zadavatele se nekalkulují.

Dalším následným problémem je neustálý vývoj prostředků ICT, jejich neustále se zvyšující složitost. Tomuto se musí přizpůsobovat nejen znalci, ale objektivně i zadavatelé. Jak po stránce technické, tak vědomostní a personální. Zejména z důvodů, které jsou uvedeny v předchozích odstavcích. Objevují se nové formáty a struktury dat, nové druhy informací, které lze z prostředků ICT získat, atd. To vyžaduje nejenom vyšší kvalifikaci zadavatele, aby byl vůbec schopen obsáhnout vše, co je pro jeho potřeby z prostředků ICT možné, nutné a vhodné získat, ale aby byl také schopen s poskytnutými daty dále pracovat.

V neposlední řadě vzniká určitá cílená tendence zadávat požadavky, které nedávají přesné výsledky. Jedná se o snahu získat ze zkoumané techniky forenzně čistě co nejvíc informací a dat, které se vztahují k určitému okruhu zájmových skutečností. Příčin může být několik, z těch nejčastějších to je skutečnost, že zadavatel v době zadání znaleckého posudku neví přesně, co je potřebné nalézt nebo prokázat nebo také zadavatel chce zjistit případné další skutečnosti, které sice ještě nemá přesně zjištěné z jiných zdrojů, ale předpokládá, že v datech by někde mohly být nějaké přesněji nespecifikované informace, které by mu pomohly je potvrdit nebo vyvrátit.

Závěr

Všechny výše uvedené skutečnosti vedou k tomu, že objemy dat, která jsou zadavateli poskytovány jako výstupy znaleckého zkoumání, se objektivně výrazně zvyšují. S tím vzniká nemálo problémů, které jsou pro znalce a i pro zadavatele nové a zatím jednoznačně neřešené a které způsobují nemalé technické, organizační, finanční, komunikační a procesní nedorozumění.

Digitální forenzní analýza je jeden z nejmladších forenzních oborů a vzhledem k dynamice vývoje digitálních technologií vlastně i dlouho takovým oborem zůstane. Neustále se budou objevovat nové skutečnosti, možnosti, ale i problémy. Proto je nutné k tomuto oboru přistupovat jako k neustále se rozvíjejícímu forenznímu oboru a vzniklé problémy vstřícně, trpělivě a se vzájemným porozuměním (tedy jak na straně znalců, tak na straně zadavatelů) řešit.

Poznámky:

---

[1] Ta relativní levnost samotného nosiče je sice objektivní skutečností, avšak když se započte do celkové ceny i proces přípravy dat v dávkách odpovídajících kapacitě nosiče, samotný proces zápisu dat, který není právě nejrychlejší a navíc problémy, které mohou být způsobeny dlouhými nebo nestandardními názvy souborů, které způsobují nekompatibilitu s normami pro zápis dat na CD/DVD, následná manipulace, příprava popisu a polepek, případně identifikačních znaků na popisu nosiče, celková cena pořízení záznamu na CD/DVD nosič už tak příznivá není, zejména když celkový počet těchto nosičů přesahuje již zmíněný počet 10 – 20 ks.

[2] I když bych to vřele nedoporučoval. Platí totiž pravidlo, že jestliže mám jeden zdroj důležitých dat (jeden výtisk znaleckého posudku a jednu kopii elektronické přílohy), jakoukoliv činnost s takovými daty bych měl provádět výlučně na kopii i přesto, že CD/DVD nosič je relativně stabilní. Ale jeden nikdy neví. Už jsem viděl, jak se z důvodu skryté vady rozletěl CD nosič v mechanice na desítky kusů a tedy byla zničena nejenom veškerá data na tomto nosiči, ale i CD/DVD mechanika.

[3] Z praxe také víme, že i nosiče CD/DVD, které jsou tzv. značkové, mohou být ve skutečnosti vyrobeny kdekoliv na světě, i v té nejhůře hodnocené továrně někde na jihovýchodě Asie.

[4] Jednoduchost řešení musí splňovat podmínku, že na systémy, které se pro další práci s elektronickou přílohou znaleckého posudku použijí, se neinstaluje žádný dodatečný program nebo ovladač.

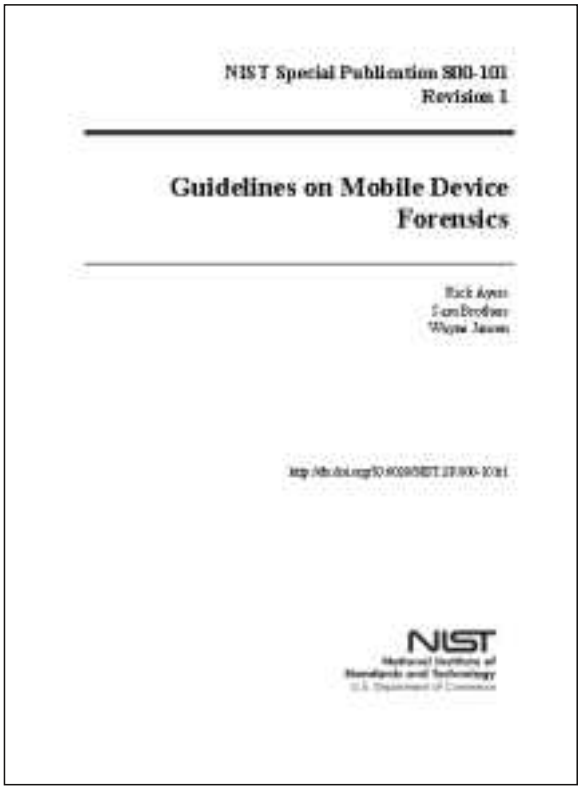
[5] Příkladem může být pouhé otevření souboru MS Excel pro čtení. I v případě, že uživatel neprovede v souboru žádné změny a při zavření souboru na otázku „Uložit provedené změny?“ odpoví „Ne“, systém stejně a bez vědomí uživatele provede změny v hlavičce souboru. Tím dojde k narušení integrity důkazu, kontrolní suma pro daný soubor již bude neplatná a důkaz jako takový bude (může být) zpochybněn.

[6] Odborníci – programátoři samozřejmě namítnou, že se přece dá napsat relativně jednoduchý program, který to provede automaticky. Ano, ale má to dva háčky. Jednak je ten požadavek od každého zadavatele specifický (každý má jiné „zvyklosti“) a nezřídka není zcela algoritmizovatelný („udělejte to jinak, ale jsou tam takové a makové výjimky a navíc se ještě na to podívám a řeknu, co ještě dát dopředu a co dozadu“).

[7] Tady je klíčovým problémem nedostatečné technické vybavení zadavatele a současně nedostatečné základní vědomosti v oblasti ICT, které by jim umožňovaly využívat veškerého potenciálu, který jim informace z prostředků digitálních technologií potenciálně mohou v jejich práci poskytnout.

[8] Dá se odhadnout, že za posledních cca 10 let se celkový objem dat, které dostáváme ke znaleckému zkoumání, zvětšil téměř 1000x a z toho vyplývá, že i objem dat, které následně poskytujeme jako výstupy, narostl přibližně odpovídajícím způsobem.

NIST SP 800-101 Guidelines on Mobile Device Forensics


NIST Special Publication 800-101
Revision 1

Guidelines on Mobile Device Forensics

NIST

Obr. 1 *Titulní strana směrnice NIST SP 800-101*

NIST – National Institute of Standards and Technology – americký úřad pro standardizaci – vydal v květnu 2014 první revizi jejich reportu (Special Publication) č. 800-101 s názvem „Guidelines on Mobile Device Forensics“ (Směrnice pro forenzní analýzu mobilních zařízení).

Dokument na úctyhodných téměř šedesáti stranách (bez úvodních listů, obsahu a příloh – celý má celkem 90 stran) vyčerpávajícím způsobem popisuje problematiku forenzní analýzy mobilních zařízení, přičemž popis je technologicky nezávislý na konkrétních modelech nebo konkrétních technologiích jednotlivých výrobců mobilních zařízení.

V úvodu popisuje základní principy fungování mobilních telefonů a smartfonů, jejich konfiguraci, organizaci paměti a základní strukturu a funkcionalitu. Popisuje základní pravidla zajištění mobilní techniky, způsoby manipulace s ní, balení apod. tak, aby byla minimalizována možnost znehodnocení informací, které jsou v této technice uložené. Dále se věnuje různým principům získávání dat z těchto zařízení pro forenzní účely a upozorňuje na různá specifika a problémy. Věnuje se také zásadám forenzní analýzy a reportování získaných dat, jakož i obecnému popisu a možnostem jednotlivých forenzních nástrojů, které se pro tyto účely používají.

Dokument NIST SP 800-101 není konkrétním návodem, jak a co dělat s konkrétním mobilem a jaké nástroje a postupy pro jeho zkoumání použít. Je to souhrn základních znalostí o jejich funkcionalitě a o základních metodách a postupech forenzní práce s nimi. Z tohoto pohledu je užitečný jako základní návod pro vytvoření vlastních postupů. Konec-konců, takovéto je i určení tohoto dokumentu, jak je uvedeno v jeho „Management Summary“.

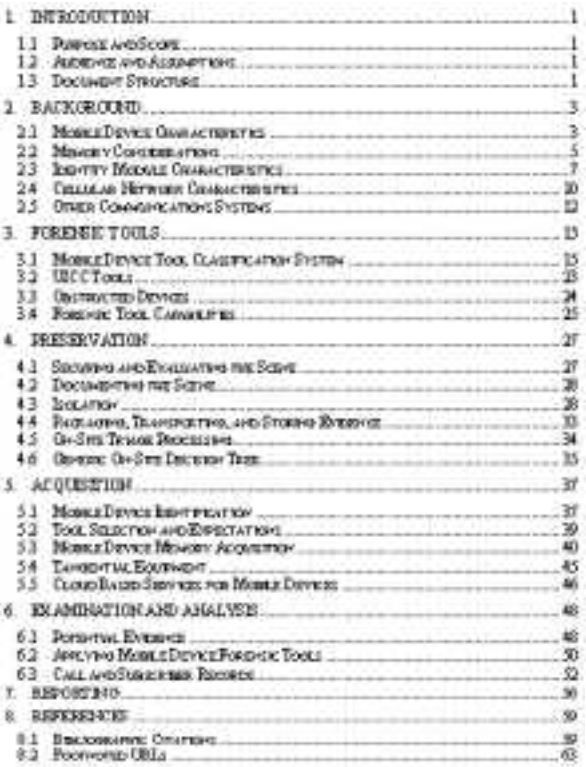
Příkladem tohoto principu může být popis jednotlivých základních metod extrakce dat z mobilních zařízení. Je popsáno základních pět metod, které se při získávání dat z mobilních zařízení používají (resp. obecně připadají do úvahy). Následně je provedena klasifikace forenzních nástrojů, které se pro tyto účely používají. Z uvedeného např. vyplývá, že aktuálně používané u nás nástroje spadají do střední nebo vyšší třídy nástrojů pro získání dat. Poslední dvě zmíněné metody (čtení informací z paměťového čipu mobilu nebo metoda "micro-read", kdy se pomocí fyzikálních principů čte informace přímo z topologie paměťového čipu) vyžadují složité technologické vybavení a speciálně

vyškolený personál a v našich podmínkách jsou prakticky nepoužitelné. Hierarchii metod pro získání dat z mobilních zařízení ilustruje Obr. 3 (ve směrnici to je "Figure 6: Mobile Device Tool Classification System")

Jak vyplývá ze samotného určení dokumentu (cituji: *„Tato příručka poskytuje základní informaci o nástrojích pro forenzní analýzu mobilů a o ochraně, zajištění, zkoumání a analýze a reportování digitálních důkazů v mobilních zařízeních. Tyto informace jsou relevantní pro OČTŘ, pro reakci na incidenty a další typy vyšetřování. Příručka je zaměřena zejména na charakteristiky GSM mobilních zařízení, klasické mobilní telefony, smartphony a tablety s GSM moduly"*), primárními čtenáři by měli být spíše kriminalisté a vyšetřovatelé, protože se dovědí více o informacích, které se v mobilech nacházejí, a o základních principech jejich činnosti a manipulace s nimi.

Samotná expertizní praxe a tedy i výsledky v mnohém závisí na kvalifikačních a technických možnostech a vybavení dané forenzní laboratoře, která právě v oboru zkoumání mobilních zařízení patří k těm dražším. Navíc, jak je i v dokumentu zmíněno, existuje riziko, že forenzní nástroje nemusí přesně nebo správně interpretovat získané informace, protože objektivně vývoj technologií a systémů v této oblasti je rychlejší, než jejich implementace do forenzních nástrojů.

Směrnice NIST SP 800-101 je volně ke stažení z webu:
http://csrc.nist.gov/publications/PubsSPs.html



***Obr. 2** Náhled na obsah směrnice NIST SP 800-101*

***Obr. 3** Klasifikace nástrojů pro získávání dat z mobilů*

Kam kráčí digitální forenzní analýza

Některé postřehy z 10 let znaleckého ústavu v odvětví výpočetní techniky

Jiří Hološka, Ph.D., GCFA, Ing. Marián Svetlík ml.
holoska@rac.cz, svetlikjr@rac.cz

Anotace:

Znalecký ústav Risk Analysis Consultants, s.r.o. shrnuje v tomto článku některé zásadní skutečnosti z desetiletého působení. Informace, které jsou v článku uvedeny, dokladují zejména nesmírný technologický vývoj v oblasti informačních technologií a poukazují na problémy, které je v souvislosti s tímto vývojem nuté akceptovat a hledat nová řešení k jejich překonání.

Bohužel se ukazuje, že taková řešení nelze hledat individuálně, ale pouze společným úsilím všech, kteří se jakýmkoliv způsobem na znalecké činnosti podílí. Ať už to je na úrovni Ministerstva spravedlnosti (jako gestora za znaleckou činnost v ČR) potažmo vlády, tak i na úrovni samotných znalců a znaleckých ústavů, ale i na úrovni zadavatelů (a tedy i uživatelů) znaleckých posudků.

Dynamika vývoje ICT

V žádném jiném odvětví lidské činnosti nepostupuje vývoj kupředu tak překotně, jako v oblasti výpočetních techniky, nebo spíše informačních technologií obecně. Počítače, chytré mobilní telefony a permanentní přístup k internetu postupně mění způsob naší práce a v některých aspektech i způsob našeho života. Podobným způsobem se mění i úloha a míra zapojení těchto technologií při páchání trestné činnosti. Úkolem digitální forenzní analýzy je objasnit skutečnosti a jevy v souvislosti s informačními technologiemi a pomoci úspěšnému uzavření případu. Jak se ale v českých podmínkách tento obor změnil za posledních deset let a jaké výzvy dnes stojí před forenzními laboratořemi a samotnými znalci v oboru informačních technologií?

Abychom byli schopni dobře vnímat rychlost vývoje, začněme krátkým exkurzem do roku 2003. V oblasti mobilních komunikací zaznamenáváme nástup mobilních telefonů s barevným displejem s rozlišením VGA (640x480 bodů, dnes přibližně dvojnásobek obrazových bodů), který nám umožňuje nově využít zasílání multimediálních zpráv MMS, a díky Nokii 7650 už víme, jak vypadá telefon s integrovaným fotoaparátem a operačním systémem (Symbian), byť disponuje pouhými 4 MB vnitřní paměti a v prodejní síti za něj zaplatíte více, jak 20 tisíc korun. Běžný mobilní telefon té doby si ještě musí vystačit s jednobarevným displejem a pamětí na několik set telefonních čísel a přibližně 100 krátkých textových zpráv.

V oblasti osobních počítačů se nejčastěji setkáváme se sestavami vybavenými procesory AMD Duron nebo Intel Celeron s frekvencí kolem 1 GHz a vybavené pamětí RAM 128 nebo 256 MB a pevným diskem o velikosti v řádu desítek GB – kvalitní nové sestavy se pak pohybují přibližně na dvojnásobku uvedených hodnot.

A před jakými úkoly stála digitální forenzní analýza a jaké prostředky využívala? V oblasti mobilních komunikací byla situace poměrně jednoduchá. Mobilní telefony umožňovaly v drtivé většině ukládání pouze telefonních čísel a SMS zpráv – hlavní problém při zajištění těchto dat představovala pouze nutnost zajistit příslušný datový kabel ke konkrétnímu typu zařízení, pokud vůbec bylo vybaveno komunikačním portem. Vzhledem k rozsahu zajištěných dat nebylo jejich další analýzy zapotřebí. Jinak tomu však bylo u klasických osobních počítačů a notebooků. Pevné disky o velikosti desítek GB už obsahovaly takové množství dokumentů, že jejich ruční procházení by bylo zcela neefektivní. Proto už tehdy forenzní

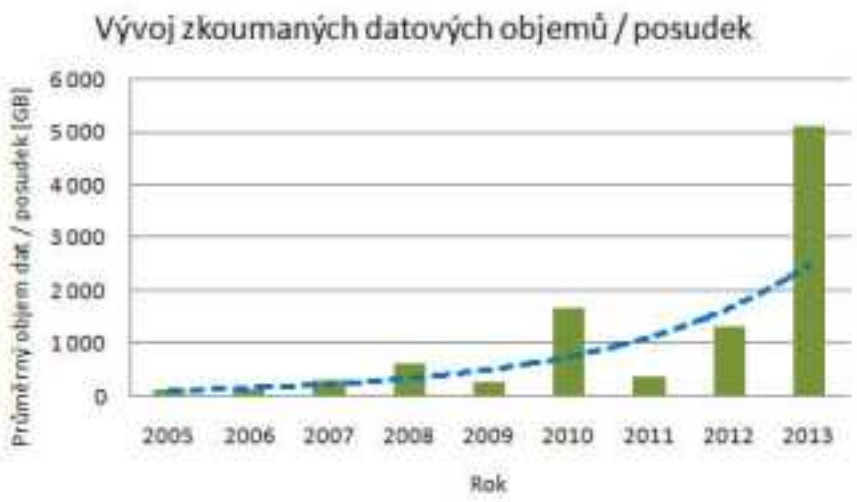
experti znali specializované nástroje pro analýzu dat – populární EnCase, tehdy ve verzi 4, doporučoval jako vhodnou konfiguraci Pentium IV 1,5 GHz a 512 MB RAM, konkurenčnímu FTK 1.5 stačilo Pentium III. Námi používaný technologický počítač s procesorem Athlon 64 XP 3000+ 2,17 GHz a pamětí RAM 512 MB DualChannel tak dostačoval nejen teoreticky, ale i prakticky. Je totiž nutné si uvědomit, že provedení jedné domovní prohlídky v době před deseti roky znamenalo zajištění pouze jednoho, výjimečně 2 ks počítačů a zpravidla jednoho mobilního telefonu. V případě prohlídky jiných prostor situace závisela na počtu podezřelých v rámci organizace, avšak v relativních číslech se počty kusů zajištěné techniky příliš nelišily. Externí paměťová média pak byla reprezentovaná ponejvíce disketami a CD v maximálně desítkách kusů. A zatímco některé aspekty znaleckého zkoumání se od té doby nijak výrazně nezměnily, některé oblasti předznamenávají změny téměř revoluční.

Oblast, která se téměř nezměnila, je představována především obsahovou a věcnou náplní znaleckého zkoumání. Stejně, jako před deseti lety, i dnes je nejčastějším požadavkem OČTŘ vyhledání dat dle zadaných klíčových slov, zajištění dat z účetního softwaru nebo zajištění elektronické komunikace. Tím zcela zásadním rozdílem je však objem zpracovávaných dat. Trestná činnost, zejména v oblasti finanční kriminality, to je dnes otázka velkého množství subjektů a jednotlivců propojených složitými vazbami. Zajištění prostředků výpočetní a komunikační techniky představuje provedení často i desítek domovních prohlídek a prohlídek jiných prostor. K tomu se přidává i skutečnost, že k běžné výbavě jediného člověka dnes kromě klasického počítače patří většinou notebook, chytrý telefon, tablet a nezměrné množství USB flash disků, paměťových karet a externích pevných disků a internetových úložišť, což představuje objem v řádu stovek až tisíců GB dat na osobu. S ohledem na rychlost stárnutí moderní výpočetní techniky – navíc mezi zajištěnými předměty často nalézáme i starší vysloužilou techniku, která již není používána, avšak stále obsahuje uložená historická data – objem zpracovávaných dat stále narůstá. Není tedy výjimkou, že forenzní pracoviště zpracovává k jedinému případu až desítky TB (desítky tisíc GB) dat.

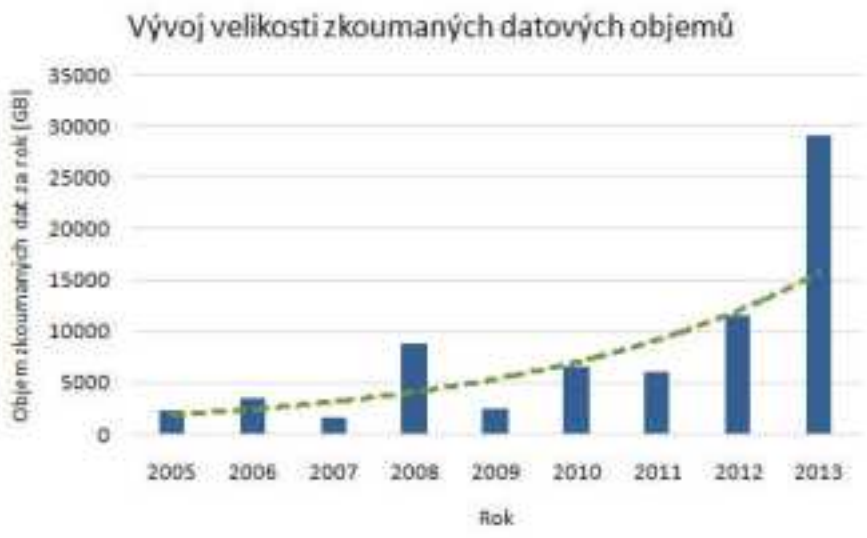
Z grafů sestavených z interní statistiky znaleckého ústavu RAC lze vyčíst trend zvyšování objemu zpracovaných dat v rámci jednoho zkoumání, stejně tak i u absolutního objemu zpracovaných dat za jeden rok, viz. Obr 1 a 2.

Požadavky na výbavu

To samozřejmě přináší i zvýšené nároky na technologické vybavení forenzního pracoviště. Doporučená konfigurace pro provoz i dnes dvou nejpoužívanějších nástrojů se od roku 2003 výrazně proměnila – pro FTK 5 je pro instalaci na jediném zařízení doporučeno využití serveru s 48 jádry a 96 GB RAM, prakticky je ovšem nutné uvažovat s dvěma až třemi servery pro oddělení zpracování dat a samotné databáze. EnCase si zatím dle výrobce vystačí v uvozovkách pouze se čtyřmi jádry a 16 GB RAM, v praxi je však nutno sáhnout po výkonnější sestavě. Zatímco tedy v roce 2003 bylo možno expertní pracovní stanici v dostatečné konfiguraci vč. periferií pořídit za přibližně 40 – 50



Obr 1 *Trend objemu dat na posudek*



***Obr 2** Trend absolutního objemu dat za rok*

tisíc Kč, dnes bychom potřebovali přibližně desetinásobek.

Výpočetní síla hardwaru posléze definuje i čas potřebný ke zpracování dat ve forenzních nástrojích. Společnost Opus One ve výkonostním testu nástrojů FTK a EnCase[1] uvádí, že zpracování jednoho terabajtu dat (cca 1000 GB) trvá mezi 16 až 90 hodinami v závislosti na zvoleném nástroji. Test byl proveden na šestnáctijádrovém stroji (2x Xenon Intel E5-2470) s 96GB RAM a osmi 600GB SAS disky nastavenými do čtyř RAID0 oddílů. Cena tohoto stroje se v lednu 2013 pohybovala okolo 230 tisíc korun bez DPH. Je zřejmé, že při průměrném objemu dat okolo pěti terabajtů na případ[2] se při použití výše zmíněné techniky čas potřebný pro zpracování pohybuje mezi 15 -20 dny. Do tohoto času není započítán čas potřebný pro vytváření bitových kopií paměťových médií, nebo odstraňování problémů s nestabilitou forenzních nástrojů při překročení hranice dvou terabajtů zpracovaných dat, které se zcela běžně vyskytují. Stejně tak zde není započten čas, který znalec potřebuje pro vyhledání a analýzu relevantních informací, dat, souborů apod. (kde právě nastupuje nezastupitelná práce znalce nad daty, které mu forenzní nástroj připraví) a čas na formulaci závěrů a zpracování a administraci samotného posudku.

V návaznosti na rychle se snižující náklady na pořízení digitálních zařízení a zvyšování počítačové gramotnosti mezi běžnými uživateli lze snadno vysledovat i nárůst digitálních artefaktů, které je nutné při forenzní analýze zkoumat. Digitálním artefaktem se označuje pozůstatek datových struktur, které nesou informace o uživatelských aktivitách. Je běžnou praxí, že OČTŘ žádá ve znaleckých posudcích rekonstrukci internetové komunikace jako je Skype, ICQ, Jabber, Viber, WhatsApp apod., nebo historii navštívených internetových stránek, stažených a editovaných souborů, seznam všech USB disků použitých na zkoumaném zařízení. Popřípadě je vyžádána kompletní rekonstrukce uživatelských aktivit v zadaném časovém úseku. Při dnešních trendech, kdy jsou masivně využívána mobilní zařízení s různou úrovní ochrany dat, se tyto jinak snadné úkoly svojí časovou náročností posouvají do kategorie, "možné, ale bude to trvat o měsíc déle". Dodatky ke znaleckému zkoumání, které v průběhu zkoumání upřesňují zájmové informace, často nabourávají časový harmonogram pro zpracování dalších posudků, ke kterým byl znalec přizván.

Predikovatelnost práce

Největší bolestí forenzní analýzy potažmo znalecké činnosti v ČR je nemožnost dopředu plánovat obsazenost znalce nebo znaleckého ústavu v časovém úseku alespoň šest měsíců dopředu. Nikdy totiž není jasné, kdy a kolik případů daný znalec obdrží. To vyžaduje další, předem stěží vyčíslitelné náklady na pokrytí z jedné strany prostojů v případech, kdy znalec nemá zakázky, a z druhé strany další dodatečné, ze zkušeností nemalé náklady na vykrytí lidí a techniky v případech, kdy dochází k přetížení pracoviště. Tedy v době, kdy je nutné operativně navýšit počet lidí, kteří se nějakým způsobem na

zpracování podílejí a pořídit další techniku, specifickou pro ten daný konkrétní případ, přičemž není jisté, zda se pro takto pořízenou techniku najde v budoucnu odpovídající využití (o vyúčtování takových nákladů jako přímých nákladů na zpracování posudku reálně nemůže být ani diskuse).

Čas a peníze

Vidina získání konkurenční výhody žene výrobce elektroniky a vývojáře programového vybavení do někdy až extrémně krátkých vývojových cyklů, to má za následek nekompatibilitu automatizovaných forenzních nástrojů s aktuálními verzemi artefaktů a ty je nutné extrahovat a reportovat ručně. Z toho nutně vyplývá i nutnost neustálého sebevzdělávání znalců – ani zde však není situace jednoduchá. Kvalitní forenzní školení nebo konference se v České republice konají dvakrát až třikrát ročně, bohužel tyto události jsou pro většinu nezávislých znalců cenově nebo jazykově nedostupné, jelikož šestidenní školení se pohybuje v cenové hladině okolo 150 tisíc Kč a konají se výhradně v anglickém jazyce.

Důsledkem výše uvedeného je přesun těžiště znalecké činnosti na ústavní pracoviště, která jsou alespoň částečně schopná pořízení vybavení a odborné vzdělávání znalců financovat z jiných ekonomických činností. Současně s tím, jak se snižuje počet expertů schopných technicky zpracovávat současné objemy dat, zvyšuje se poměrně i čas zpracování jednotlivých posudků na pracovištích, která potřebným technologickým vybavením alespoň zčásti disponují. Na základě vývoje posledních let lze oprávněně předpokládat, že v nejbližších letech se tato situace bude dále zhoršovat. Změnu, jejíž rozsah a dopad na digitální forenzní analýzu lze dnes jen stěží předvídat, bude v horizontu několika let představovat až masový přechod ke cloudovým řešením. Nasazení serverových aplikací nebo cloudových služeb bude každopádně v blízké budoucnosti vyžadovat úpravy stávajících postupů při zajišťování zařízení při domovních prohlídkách a prohlídkách jiných prostor, spočívající ve vytváření obrazů operační paměti a spolupráci s poskytovateli cloudových služeb.

Výše znalečného se v případě přibrání znalce OČTŘ stále pohybuje na úrovni 300 Kč/hod. Podíváme-li se na počet pracovních hodin za rok a na rychlost změn minimálních požadovaných parametrů sestav pro forenzní nástroje, je zcela zřejmé, že soudní znalec v odvětví Výpočetní technika nemá v podmínkách ČR nejmenší šanci pokrýt ze zisku z vlastní činnosti nákup zařízení pro tuto činnost nezbytného. Přitom hovoříme pouze o základním hardwaru – další desítky tisíc korun ročně představují náklady na upgrade forenzního softwaru, nástrojů pro analýzu mobilních zařízení, další ad-hoc vybavení podle specifik jednotlivých případů, spotřební materiál atd. O nákladech na průběžné vzdělávání (nejenom přímé náklady na školení, ale i nezbytné náklady na samovzdělávání, bez kterého nelze v oboru existovat) ani nemluvě.

Závěr

Výše uvedené skutečnosti by měly mít OČTŘ na paměti při přibírání znalce a pokusit se v co nejvyšší míře posoudit možnou relevantnost informací obsažených v zajištěných zařízeních a snažit se, pokud je to možné, omezit absolutní množství zařízení a datových nosičů předávaných ke znaleckému zkoumání. Výraznou pomocí může být rovněž větší konkretizace znění otázek položených znalci – to by měl zadavatel se znalcem vždy konzultovat. Každopádně je však nutné připravit se – zejména u rozsáhlých případů – na výrazně delší lhůty ke zpracování znaleckých posudků.

Poznámky

---

[1] Performance Comparison of AccessData's® Forensic Toolkit® and Guidance Software's EnCase® Forensic software by Joel Snyder.

[2] Interní statistika znaleckého ústavu RAC

NEPŘEHLÉDNĚTE

RAC Digital Forensic InfoDay

V druhé půli listopadu si Vás dovolíme pozvat na již avizovaný seminář RAC Digital Forensic InfoDay.

Seznámíme Vás s některými novinkami a praktickými poznatky z práce s digitálními důkazy.
Aktuálně máme v plánu se věnovat následujícím oblastem:

DEAS
DEAT

Praktické zkušenosti, postupy práce a používané nástroje pro pořizování digitálních kopií dat (obrazů disků) a seznámení s našimi vlastními produkty DEAS (Digital Evidence Acquisition Suite) a DEAT (Digital Evidence Acquisition Tools).

XRY COMPLETE

Představení a některé praktické zkušenosti při zkoumání mobilních zařízení pomocí nástroje XRY společnosti MicroSystemation.

nuix

Nová vlajková loď pro efektivní forenzní analýzy velkých objemů dat. Seznámíme Vás se systémem NUIX a představíme jeho hlavní výhody pro forenzní analýzy digitálních dat, nové možnosti analýzy, interpretace a prezentace výsledků.

Součástí všech bloků jsou praktické ukázky, tipy a triky, doporučení a diskuse k dané oblasti.

Přesný termín a místo konání upřesníme co nejdříve a tyto informace budou včas uveřejněny na našem webu (www.rac.cz).

Budem rádi, jestliže již dnes projevíte zájem o účast a také přispějete k programu svými náměty. Stačí napsat e-mail na adresu **ZU@rac.cz** nebo přímo do redakce na adresu **DFJ@rac.cz**. Na oplátku pak budete mezi prvními informováni o přesném datu, místu i programu a dostanete i dárek navíc.

Již teď počítejte s tím, že v druhé půli listopadu budete potřebovat jeden den na

RAC Digital Forensic InfoDay

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.

Rozhodnutí o publikaci příspěvku je ve výhradní kompetenci vydavatele.

ZNALECKÝ ÚSTAV RAC

LABORATOŘ DIGITÁLNÍCH FORENZNÍCH ANALÝZ

Laboratoř digitálních forenzních analýz Znaleckého ústavu nabízí pestrou škálu služeb pro orgány činné v trestním řízení, justici, advokacii i pro privátní sféru.

Školení

- ***obecná školení forenzní analýzy***
  - aktuální postupy (state of art)
  - ověřené postupy (best practices)
- ***produktové kurzy***
  - AccessData Forensic Toolkit
  - Guidance Software EnCase Forensic
- ***příprava na certifikace***
  - AccessData Certified Examiner (ACE)
  - EnCase Certified Examiner (EnCE)

Služby pro forenzní laboratoře

- ***návrh a realizace pracovišť a laboratoří pro digitální forenzní analýzu***
- ***příprava individuálních kurzů a školení***
  - teoretické i praktické kurzy

Czech Cyber Crime Center of Excellence (C4E)

Hlavním cílem C4E je rozvoj výzkumu, vývoje a vzdělávání v oblasti boje proti kybernetické kriminalitě. C4E je realizováno za finanční podpory Evropské komise konsorciem Masarykovy univerzity, RAC a NBÚ. ZÚ RAC je klíčovým partnerem a zároveň gestorem C4E pro oblast digitální forenzní analýzy. Jako prakticky jediné znalecké pracoviště v republice připravuje metodické a školicí materiály a provádí aplikovaný výzkum v tomto oboru. Kromě specifických forenzních školení připravujeme s Masarykovou univerzitou také ucelený systém vzdělávání pro OČTŘ.

Rozhodnutím Ministra spravedlnosti České republiky č. M-840/2003 ze dne 26. května 2003 byla naše společnost zapsána do prvního oddílu Seznamu ústavů kvalifikovaných pro znaleckou činnost v oboru kybernetika s rozsahem znaleckého oprávnění pro odvětví výpočetní technika se zaměřením na poskytování služeb v oblasti analýzy a posuzování bezpečnostních rizik informačních systémů. Znalecký ústav RAC je první ryze český soukromý znalecký ústav v oblasti forenzního zkoumání ITRS.

Risk Analysis Consultants, s.r.o.
Znalecký ústav
Španělská 2
120 00 Praha 2

tel.: +420 221 628 400
znalecky.ustav@rac.cz

Znalecká činnost v oboru Kybernetika, odvětví Výpočetní technika.

Služby Znaleckého ústavu RAC:

- Digitální forenzní analýzy
- Konzultační a poradenská činnost pro vyšetřovatele, st. zástupce, soudy, advokacii a privátní sféru v oblasti forenzní počítačové analýzy
- Školení v problematice forenzní počítačové analýzy
- Metodická, poradenská a odborná pomoc při vytváření podobných pracovišť
- Dodávky metodik, prostředků technologického, technického a programového vybavení pro speciální a forenzní analýzy
- Ostatní speciální služby, poskytované na základě využití metod, postupů a prostředků forenzní počítačové analýzy

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