Digital Forensic Journal

2/2014 **30. prosinec 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 kompletní sadu nástrojů pro pořizování forenzních binárních kopií dat.
DEAT obsahuje prakticky vše, co můžete potřebovat - od sady redukcía kabelů, přes HW write-blockery pro různé typy disků nebo paměťových médií, až po speciální kopírovací zařízení.
DEAT je možné na přání vybavit i dalšími pomůckami a nástroji, které můžete na místě zajištění potřebovat.
DEAT je unikátně vybaveni nástrojem **DEAS** - forenzním bootovacím CD, které je pro účely práce na místě zajištění vytvořeno v laboratoři Znaleckého ústavu RAC.
Pomocí **DEAT** dostáváte kompletní přenosnou sadu HW a SW nástrojů pro forenzní pořizování kopií dat na místě zajištění.

Digital Forensic Journal

2/2014 **30. prosince 2014**

Úvodník

Vážení čtenáři,

předem musím přiznat, že rčení "je těžké začít, ale důležité je vytrvat" se opět potvrdilo. Druhé číslo DFJ se nerodilo jednoduše. Nejde ani tak o to, že by nebylo dostatek námětů, ale čas nás všechny tlačí čím dále tím více. Proto stále méně jej zbývá na "nadstavbové" aktivity, kterými nesporně vydávání časopisu v našich podmínkách je.

V tomto čísle jsme se zaměřili zejména na identifikaci a forenzně správné zajištění dat. Je to téma široké, vzletně by se dalo říci, že nekonečné. I proto se k němu budeme vracet pravidelně. Není to ale jenom samotné zajištění dat, s tím souvisí i další navazující procesy, které jsou více nebo méně na datech závislé.

Pozitivem tohoto čísla je také to, že již máme i externí autory. Navíc autory z privátní sféry. Je to důkaz toho, že digitální forenzní analýza má mezi ostatními forenzními vědami své specifické postavení právě tím, že to není výlučně věda určená pouze pro soudní dvory, ale věda a forenzní praxe, která má velice široké uplatnění v celé naší informační společnosti. Proto aplikacím digitální forenzní analýzy v jiných, než trestně-právních případech, se budeme snažit věnovat patřičný prostor i v budoucnosti. Tlak na řešení problematiky bezpečnostních incidentů roste s jejich enormním množstvím a s výší škody, kterou takové útoky organizacím způsobují. A tady si jen s technickým řešením už nevystačíme (nemluvě o tom, že i s tím je mnoho problémů), je potřeba řešit i ochranu dobrého jména, ochranu spotřebitele, procesní, pracovně-právní a trestně-právní dopady takových aktivit. Digitální důkazy v tom mají nezastupitelné místo.

Dalším pozitivem je rozšiřování naší čtenářské základny. Zejména nás těší zájem, který projevily univerzitní knihovny a velice nás těší zájem našich čtenářů ze Slovenska. Po vydání prvního čísla to považujeme za úspěch. Doufám, že i toto druhé číslo vám přinese užitečné informace. Plánů do budoucna máme hodně, držte nám palce, ať máme na jejich realizaci dostatek času a energie.

Příjemné a užitečné čtení Vám přeje

Marián Svetlík

Obsah

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 2 / Vyšlo 30. 12. 2014 v Praze

Sedm hříchů digitální forenzní analýzy

Co by se nikdy nemělo stát při zkoumání digitálních dat

Jiří Hološka, Ph.D., GCFA
holoska@rac.cz
ICT Security Consultant, Digital Forensic Certified Expert, Incident Response Analyst
Ing. Marián Svetlík st.
svetlik@rac.cz
Soudní znalec v oboru Kriminalistika, kriminalistická počítačová expertíza, vedoucí Znaleckého ústavu společnosti Risk Analysis Consultants, s.r.o.

Anotace:

Článek popisuje chyby a nedostatky znaleckého zkoumání v oboru digitální forenzní analýzy, které jsou bohužel v našem prostředí častým jevem a se kterými se potkáváme v každodenní práci. Na některých konkrétních příkladech ilustruje fatalitu nesprávných postupů a nedodržování základních pravidel digitální forenzní analýzy. Neklade si za cíl popsat veškeré nedostatky nebo je seřadit podle jakýchkoliv kritérií. Všechny jsou však navzájem propojeny právě digitálními stopami, poznáním jejich základních vlastností a elementárními postupy a metodami práce s nimi.

Úvod

V prostředí České republiky nejsou definována prakticky žádná pravidla pro zkoumání digitálních stop. Proto značné množství znalců používá kouzelnou formulaci "zkoumání dle nejlepšího vědomí a svědomí". Pokud k tomu přidáme fakt, že požadavek na zkoumání podle posledních poznatků vědy v daném oboru nemá kdo kvalifikovaně zhodnotit, dostáváme se do situace, kdy se takto provedené "forenzní" zkoumání neblíží (natož aby bylo v souladu) s vědecky ověřitelnými postupy běžně používanými v západní Evropě a USA.

Chyby však nejsou jen na straně znalců, ale i na straně zadavatelů, kteří často nezajistí veškeré dostupné stopy, popřípadě zadávají otázky, které omezují objektivní hodnocení zkoumaných dat. Nezřídka tím fakticky nutí znalce k zodpovězení zavádějících otázek, které přímo vyviňují obviněné osoby nebo i svalují vinu na potenciálně nevinné.

Přestože u nás není přesně a jednoznačně stanoveno, jaké zásady by měly být při digitální forenzní analýze dodržovány, je celkem zřejmé, že zásady legálnosti, nepodjatosti, přiměřenosti, zachování integrity důkazů, opakovatelnosti a přezkoumatelnosti patří k pilířům všech forenzních analýz. Podrobněji je o tom pojednáno např. v článku "Digitální forenzní analýza a bezpečnost informací", uveřejněném v časopise Data Security Magazine č 1/2010, str. 20 - 23 [1].

V následujících odstavcích budou uvedeny a rozebrány konkrétní problémy, se kterými se v poslední době setkáváme a které považujeme za zásadní (aniž bychom je uváděli v nějakém pořadí důležitosti). Pokusíme se také nastínit jejich příčiny a možné způsoby řešení, jestliže taková řešení jsou v našem prostředí a v našich možnostech prakticky realizovatelná.

Základní neznalost nebo ignorování známých postupů manipulace a analýzy digitálních stop

Digitální forenzní analýza je exaktní forenzní věda, která zkoumá procesy a zákonitosti vzniku, existence a zániku digitální informace v prostředí informačních systémů. Jedním ze závěrů, které vyplývají z vlastností digitálních stop, je skutečnost,

že kopie digitální stopy je identická s jejím originálem. Správný postup je tedy zkoumat binární kopii digitální stopy. Tento postup zaručuje, že nemůže dojít ke změně nebo ke zničení původní (originální) digitální stopy a zkoumající osoba má vždy k dispozici jednu nezávislou kopii dat pro případ poruchy na technologickém zařízení a ztráty zkoumané kopie digitální stopy.

Forenzní metodika definuje tři druhy stop a) originální zařízení b) bitovou (identickou) kopii originálního zařízení c) kopii bitové kopie, na které je prováděno zkoumání.

Nicméně tato fakta nebrání některým znalcům zacházet s digitálními stopami natolik neopatrně a neprofesionálně, že původní stopy jsou často již v prvopočátcích znehodnoceny, pozměněny nebo úplně zničeny.

A jestliže původní, originální digitální stopa již neexistuje (počítač byl vrácen původnímu majiteli), nebo je stopa zkoumáním nevratně změněna a neexistuje ověřená binární kopie originálních dat této digitální stopy (policejní orgán nebo znalec nepořídili a nearchivovali identickou kopii digitální stopy), vypovídací hodnota důkazu je z důvodu nepřezkoumatelnosti minimální.

Lze se setkat s posudky, které vykazují elementární neznalost metod forenzního zkoumání. Pro příklad lze uvést posudek, ve kterém znalec zkoumal tři měsíce notebook, který si spustil a přímo na něm prohlížel obsah dokumentů. Tento způsob zkoumání je nepřípustný jak z formálního hlediska, tak i z technického.
Formálně se znalec dopustil manipulace s digitální stopou, kdy jeho akce vedly k nevratným změnám na zkoumaném zařízení. Z technického hlediska se nevratné změny projevily ve změnách časových značek u vytvořených souborů. Dále mohlo dojít ke změně obsahu dokumentů vlivem antivirových a indexovacích nástrojů nebo automatického ukládání souboru po uplynutí přednastaveného času od posledního uložení. Tento stav lze nazvat jako neúmyslné porušení integrity původních dat.

Pokud vynecháme možnost úmyslného zničení stopy, lze obecně tvrdit, že nevhodné nakládání s digitálními stopami vede k nepřezkoumatelnosti posudku. Právě přezkoumatelnost je jedním z hlavních pilířů forenzní analýzy obecně.

Při přezkoumání znaleckého posudku jde o to, že když jsou jinému znalci poskytnuta stejná data a zadané stejné otázky, měl by použitím obdobných postupů dospět ke stejným, nebo alespoň srovnatelným (analogickým) závěrům, a tím potvrdit původní zkoumání.

To, že značná část posudků je ve své podstatě nepřezkoumatelná, je způsobeno právě tím, že nelze zajistit stejné výchozí podmínky, tedy že pro přezkoumání nejsou k dispozici originální data. Tento stav je v drtivé většině způsoben nevytvořením bitové kopie disku nebo jiného relevantního zdroje informací nebo poškozením integrity původních dat.

Poškození integrity dat nastane, když zkoumání není provedeno v režimu, kdy je garantováno maximální zajištění objektivity interpretovaných dat. Jinak řečeno, při zkoumání nebyla zajištěna ochrana originálních dat proti změnám dat samotných nebo jejich metadat.

V zemích, kde jsou metody zkoumání digitálních dat lépe definovány než v ČR, je takovýto postup až trestně postižitelný (zničení nebo znehodnocení důkazů, přičemž z pozice znalce by se nemělo jednat o neznalost nebo nedbalost, protože znalost odpovídajících postupů zkoumání je nutnou podmínkou výkonu profese) a znalecký posudek s těmito vadami je nepřípustný pro soudní jednání.

Neopakovatelnost zkoumání

V praxi narážíme na skutečnost, že posudky, se kterými se v procesu naší práce musíme seznamovat, nelze ověřit, protože postupy v nich uvedené, jestliže vůbec nějaké postupy uvedeny jsou,

Úkolem jistého znalce bylo nalézt na předloženém PC veškeré dokumenty obsahující určitou specifickou informaci (jednalo se o čísla bankovních účtů). Protože znalec nebyl schopen nalézt dokumenty, které byly v době zkoumání již smazané, při revizním zkoumání jsme zjistili neuvěřitelnou věc – dotyčný „takyznalec“ na zkoumaném PC vytvořil v rootu adresář s názvem „NALEZY“. A tam překopíroval své nálezy, které posléze z toho samého počítače vytiskl přes v počítači nainstalovaný MS Word na tiskárně, kterou pro tyto účely k počítači připojil. Doufám, že k tomuto případu není potřebný žádný komentář. Kromě fatální neodbornosti zničil svým diletantstvím v oblasti zásad forenzní práce další potenciální důkazy.

Jistá firma „A“ nebyla spokojena s dodávkou SW vybavení v ceně několika miliónů. Své servery s nainstalovaným systémem dala k posouzení firmě „B“. Protože však byly závěry firmy „B“ zpochybněny, došlo na přezkoumání. S údivem jsme museli konstatovat, že v zásadě sice závěry našeho předchůdce mohly odpovídat skutečnosti, avšak tento (asi ve snaze efektivně využít vše, co ve firmě je) v době mezi skončením svého posuzování a vrácením serverů zpět firmě „A“, operativně využil zkoumané servery pro vlastní potřebu – zřídil si z nich na dobu cca dvou měsíců backupovací servery. Dohra takového „takykvalifikovaného“ posuzování nebyla příjemná. Zdroj - DSM 1/2010

nelze zopakovat. Příčiny, proč nelze opakovat použité postupy, jsou v zásadě pouze dvě:

- postupy, použité předchozím znalcem, nejsou zadokumentovány vůbec nebo jsou zadokumentovány natolik nedostatečně nebo nepřesně, že je nelze spolehlivě opakovat. Nelze tedy určit na jakých základech stojí interpretace dat v daném posudku.
- chybí originální data (digitální stopy)

To, že znalci nedostatečně dokumentují postupy zkoumání, by se dalo vysvětlit jednoduchými ekonomickými propočty. Vzhledem k nízké hodinové sazbě a také vzhledem k nízké pravděpodobnosti nepředvídané události (tedy požadavku na ověření nebo přezkoumání), není ekonomicky zdůvodnitelné konat cokoliv nad rámec minimálně nutných nákladů. Někdy nejasná nebo dokonce chybějící dokumentace postupů zkoumání může být ale i záměrem, vyloučit to nelze.

Celkem běžná situace (dokonce by se dalo říci, že standardní) se dá popsat následujícími kroky. Policejní orgán zajistí počítač. Na počítači je znalcem nalezena a zadokumentována určitá informace – důkaz. Počítač je vrácen původnímu majiteli a k soudu se (s odstupem někdy i několika let) dostane pouze znalecký posudek, který obsahuje tvrzení, že ta určitá informace se nacházela na zkoumaném počítači.

Výše popsaná standardní situace je analogická tomu, jako kdyby se k soudu dostal pouze výňatek přepisu záznamu telefonního odposlechu a původní/originální záznam telefonního odposlechu byl zničen. Ono totiž nestačí zdokumentovat, že jedna osoba v telefonní komunikaci řekla druhé osobě „já ho zítra přerazím“, aniž by byl posouzen kontext takového tvrzení. Úplně stejná situace je u počítačových záznamů. Jestliže neznáme kontext digitální informace (její vznik, existenci a případně zánik), nelze činit jednoznačné závěry.

Aby bylo tedy přezkoumání posudku vůbec možné, je nutné uchovávat originální, nezměněné digitální stopy nebo jejich ověřené identické kopie. Alespoň do doby pravomocného rozhodnutí soudem. A jak bylo již řečeno, pro digitální stopy neplatí tvrzení, že „stopa byla zkoumáním spotřebována“. Proto je, při dnešních cenách pevných disků, zachování digitální stopy pouze formální problém.

Přitom úmyslně tady nepoužíváme výraz „archivace“, byť v tomto pojetí by se jednalo o ryze technický pojem, ne pojem právní. Nicméně

problematikou uchování originálních digitálních dat by bylo potřebné se urgentně zabývat, protože stávající situace, kdy se touto oblastí nikdo systémově nezabývá, nejenom komplikuje výkon znalecké činnosti, ale lze si docela dobře představit i dopady procesní, kdy znemožnění opakování nebo přezkoumání znaleckého posudku může být závažnou vadou celého řízení.

Neúplné zajištění stop

Při zajišťování dat není možné ignorovat fakt, že konkrétní zajišťované zařízení muže sloužit pouze jako "čtecí" zařízení a samotná data mohou být uložena jak na interních datových nosičích zajišťovaného zařízení, tak v současnosti stále častěji na lokálních síťových úložištích nebo cloudech. Metody zajišťování je tedy nutné přizpůsobit aktuálnímu stavu na místě.

Příkladem mohou být následující zařízení a technologie:

- Flash disky
- Síťová úložiště
- Cloudová úložiště (jako varianta síťových úložišť)

Zajímavým médiem jsou USB datové nosiče. Při kapacitách, začínajících u USB Flash disků někde v řádech jednotek nebo desítek gigabajtů, až po USB externí disky (ať již klasické nebo SSD), je velká šance, že tato média budou obsahovat obnovitelné dokumenty i dlouho po jejich smazání. Navíc právě charakter těchto médií, jako velice lehce vyměnitelných a lehce přenosných (a také lehce maskovatelných např. ve formě různých přívěšků na klíče, kreditních karet nebo mnohdy i bizarních talismanů), je předurčuje pro uchovávání a přenášení dat, která jsou pro uživatele něčím důležitá, a tedy určitě mohou být důležitá i pro OČTŘ.

Pro zajištění co největšího počtu USB zařízení je vhodné **ihned po zajištění počítače a ještě na místě zajištění** exportovat systémové registry **a provést základní analýzu některých zájmových informací, jako například právě seznamu USB zařízení**, včetně data posledního použití a sériového čísla zařízení. Tato informace je důležitá právě z pohledu **kompletnosti zajištění dat na místě**. Když se počet USB zařízení připojených k danému počítači zjišťuje znaleckým zkoumáním až s odstupem několika měsíců, je prakticky vyloučeno nějaká dodatečná USB zařízení zajistit, tím spíše očekávat, že by na nich ještě byla důležitá data.

Při zajišťování digitálních stop se nelze spokojit pouze se zařízením, které je na první pohled snadno identifikovatelné. V návaznosti např. na zajišťování pracovních stanic je vhodné zkontrolovat zejména síťová úložiště, která mohou sloužit nejenom jako síťové disky pro primární práci s daty/soubory, ale např. i pro zálohování dokumentů, kde mohou být uloženy jejich zálohy, které již dávno na živých produkčních systémech neexistují.

V závislosti na aktuálních podmínkách na místě lze síťová úložiště zajistit fyzicky, pořídit identické kopie datových nosičů nebo pořídit kopie dat pouze na logické úrovni.

Posledním typem paměťového média jsou cloudová úložiště. Tento typ úložišť je možné zajistit zpravidla pouze ze spuštěného počítače a to jen na logické úrovni, tzn. provést kopii platných souborů. Byť technicky mezi síťovými a cloudovými úložišti není zásadní rozdíl, základním věcným rozdílem je fyzické umístění cloudového úložiště (zpravidla mimo dosah uživatelů, ale také často i naší jurisdikce) a vlastnictví technické infrastruktury, která ukládání dat v cloudu umožňuje. Celá infrastruktura cloudu, včetně datových nosičů, je zpravidla ve vlastnictví třetí osoby a datový prostor – možnost ukládat data – je pouze pronajatou službou. To však nic nemění na faktu, že data jsou plně ve vlastnictví pronajímatele.

Nechceme se tady pouštět do diskuse kolem některých nedávných judikátů. Jen zdůrazňujeme, že taková úložiště existují, stále častěji se používají, ať už soukromě nebo i v rámci firemní strategie, a že je potřebné přípravu zajišťovacích úkonů uzpůsobit podmínkám, které se na takovéto typy úložišť vztahují. Nelze totiž vyloučit i situaci, kdy při zajišťovacích úkonech v rámci firmy zjistíte, že

firemní IT je založeno na využívání cloudových úložišť a pracovní stanice jsou realizovány pomocí zařízení s ChromeOS. Tady se hodí uvést jeden konkrétní příklad, který se vztahuje sice k síťovým uložištím, ale pěkně dokresluje i současnou situaci s cloudy.

Policejní orgán zajistil ve firmě počítač paní účetní, protože podle výslechů právě ona pracovala s účetní agendou. Zajištěný počítač předal znalci ke zkoumání s cílem tuto účetní agendu zpřístupnit pro další šetření. Znalec však prohlásil, že na počítači žádnou účetní agendu nenalezl. Protože z výslechů bylo zřejmé, že účetní agenda je značně rozsáhlá (pro ty, kteří vědí, uvádíme, že firma pracovala na SAPu), předal nám zajištěný počítač k opětovnému prozkoumání. Řešení bylo jednoduché - paní účetní měla na ploše link na program SAP, který však byl instalován (celkem logicky) na serveru společnosti, a na počítači paní účetní byl pouze odkaz na tuto serverovou instalaci.

Situace, kdy se zcela zjevně znaleckým zkoumáním prokáže, že existuje nebo existovalo množství paměťových médií, která obsahovala velké množství potenciálně důležitých informací, která nebyla zajištěna a jejichž obsah je z pohledu zkoumání ztracen, není vůbec zřídkavá.

V průběhu zkoumání běžně dochází k nálezu metadat souborů, které by mohly být důležité pro vyšetřovanou věc, avšak jejich umístění odkazuje na externí paměťové médium, či na síťová nebo cloudová úložiště, která však nebyla zajištěna.

Používání nelegálního softwaru

Jistě, zákonem dané hodinové odměny za výkon znalecké činnosti nedávají velký prostor na pořizování forenzních nástrojů jako je FTK, EnCase, Nuix nebo Ultimate Forensic Studio. To ovšem neomlouvá používání nelegálních kopií programů pro znalecké zkoumání. Už jen z morálního hlediska by mělo být zjištění používání takovéhoto programového vybavení diskvalifikačním kritériem takového zkoumání. Ochrana integrity zkoumaných dat je spolu s přezkoumatelností klíčovým faktorem forenzní analýzy, potažmo znaleckého zkoumání. Při použití nelegálního programového vybavení je často nutné obejít licenční ochranu pomocí programů zasahujících do chodu používaného programu. Takový stav vylučuje, aby zpracovatel garantoval správnost výsledků zkoumání.

Obcházení licenčních mechanismů s sebou nese i značné riziko infikování technologického počítače nebo zkoumaných dat virovou nákazou, jelikož pro správnou funkci takzvaných cracků je často nutné vypnout antivirovou ochranu.

Znalec, který pro digitální forenzní analýzu používá nelegální nebo neznámé nástroje, nemůže zaručit integritu zkoumaných dat, a tedy jejich správnost a hodnověrnost. Aniž bychom se na tomto místě pouštěli do právních výkladů autorského zákona a diskutovali o různých variantách využitelnosti programového autorského díla, zásada opatrnosti ve formulaci závěrů, získaných použitím nelegálního programového vybavení, je platná jak pro znalce, tak i pro OČTŘ, když hodnotí závěry, které byly takovým postupem získány.

Žádné nebo jen minimální sebevzdělávání znalců

Vědní obor informačních technologií se vyvíjí neuvěřitelně rychle. Sebevzdělávaní je jedinou cestou zajišťující objektivní hodnocení digitálních artefaktů. Každé dva roky se mění průměrná softwarová výbava osobních počítačů a každých pět let se diametrálně změní technologické možnosti ICT. Tento vývoj je nutné zohlednit i v používaných postupech pro zajišťování a analýzu dat.

Jako příklad lze uvést dlouholeté spory ohledně metod zajišťování dat. V prvních metodikách pro zajišťování dat bylo doporučováno vypnutí počítače odpojením od elektrické sítě. Vlivem větší komplexnosti paměťových médií a složitějších souborových systémů se metodika změnila

a doporučuje se systém vypnout korektním způsobem, aby se předešlo poškození uložených dat. Dnes se ovšem ukazuje, že ani tato metodika již nevyhovuje a samotnému vypnutí systému by měla předcházet fáze on-line zajištění dat z pamětí počítače. Před vypnutím systému je potřeba zajistit obsah operační paměti a zkontrolovat, zda systém nemá aktivní ochranu dat šifrováním.

Vývoj a různorodost informačních technologií se budou nadále rozvíjet, bohužel v ČR není definováno žádné kontinuální vzdělávání znalců. Proto se objevují paradoxní situace, kdy techničtí pracovníci ve firemním prostředí mají po dvou až třech letech praxe lepší technické a znalostní předpoklady pro výkon znalecké činnosti, než znalci s 15 lety praxe.

Důvodem je motivace firem aktivně se účastnit na zvládání bezpečnostních incidentů a podpora vzdělávání v oboru digitální forenzní analýzy se zaměřením na zajišťování digitálních stop a zvládání bezpečnostních incidentů. Tento trend bude dále pokračovat i v návaznosti na začátek platnosti zákona o kybernetické bezpečnosti.

Je zřejmé, že obor IT znalecké činnosti bude muset projít v blízké budoucnosti revizí. Úmyslně zde neuvádíme žádný specifický název oboru, který je podle aktuálního seznamu znaleckých oborů MSp platný, protože ani jeden z nich nevyjadřuje obsah digitální forenzní analýzy. Definice digitální forenzní analýzy, která je uvedena v úvodu tohoto článku, je pouze určitým vysvětlením pojmu a slouží pouze pro lepší pochopení toho, co je dále v článku uvedeno.

Bude zřejmě nutné definovat základní znalosti nezávisle měřitelné jinak, než délkou praxe, ta bohužel nereflektuje hloubku znalostí. Změnou bude muset projít i způsob jmenování znalců. Stav, kdy jsou znalci odmítání pouze z neobhajitelného důvodu nepotřebnosti, bude muset být nahrazen systémem se základem ve znalostech daného žadatele a minimalizovat tak dopad (ne)sympatií hodnotitele žádosti. To je ale problematika mnohem širší a komplexnější, než abychom ji v tomto článku dále rozvíjeli nebo činili nějaké závěry.

Pro ilustraci složitosti této problematiky odkazujeme například na [2].

Jednostranné závěry

Problémem jednostranných závěrů zkoumání je špatné či zcela účelové zadaní otázek položených znalci. Zadavatelé (možná z důvodu šetření) zadávají specifické dotazy na znalce, s jejichž výsledky následně pracují při soudním řízení. Tento stav má paralelu v takzvaném "hledání vražedné zbraně", který spolu s dalšími nepřímými důkazy ve fyzickém světě funguje relativně spolehlivě. Bohužel v digitálním prostředí tento přístup může přinést značně zkreslené výsledky. Krádeže identit jsou známy zejména ve spojitosti s útoky na bankovní služby, ovšem s malou dávkou představivosti je možné krádeže identit použít ke konkurenčnímu boji. Příkladem může být následující situace.

Zabezpečení ICT v malých a středních firmách není top prioritou. Proto provedení útoku a průniku do IT systémů takových firem nebývá v současnosti nijak složité. Z takto kompromitovaných počítačů lze snadno nafingovat průnik do konkurenční (vlastní) firmy včetně nakopírování usvědčujících dokumentů na jejich pevné disky. Pokud bude znalec v tomto případě odpovídat jen na přímo zadané otázky typu „zda na zkoumaných zařízeních existuji dokumenty z firmy XY, s.r.o.“, může mít jeho znalecký posudek fatální následky pro původně napadenou firmu, která teď v očích soudce bude vypadat jako agresor a strůjce nekalých obchodních praktik.

Je nutné dát znalci prostor pro ověření, zda nalezené informace opravdu pocházejí z činnosti, na kterou směřují zadané otázky, nebo zda zkoumaný systém obsahuje programové vybavení umožňující neautorizovaný přístup a využívání systému. Jinak řečeno, umožnit znalci prozkoumat zjištěné skutečnosti ve všech možných souvislostech a nevytrhávat určité informace z kontextu (viz uvedeno výše).

Navíc, když nejsou k dispozici původní digitální

stopy (jak se často stává a jak bylo již rozebíráno výše), nelze nejenom ověřit nebo prozkoumat již podané znalecké posudky, ale nelze již ani zadat zkoumání nové, které by mohlo odhalit jiné, často protichůdné důkazy, které policejní orgán a/nebo dozorující státní zástupce v průběhu vyšetřování mohl opomenout (např. z důvodu neznalosti nebo nízké kvalifikace v oblasti informačních technologií) nebo nevzít v úvahu, a tím narušit objektivitu vyšetřování.

Samostatným tématem jsou účelové posudky, které jsou z různých pohnutek neobjektivní, byť se to často těžce prokazuje. Revize posudků je značně ztížena i faktem, že (obecně) jsou si znalecké posudky rovny (když se neprokáže opak) a je jen a pouze na úvaze soudu, jakou váhu tomu kterému posudku přidělí. A to i v případě že např. jeden z posudků je vypracován znaleckým ústavem, kde se problému věnovalo několik specialistů najednou a kde potenciální neobjektivnost je právě díky kolektivní práci výrazně minimalizována.

Vyjadřování se k právním otázkám

Digitální forenzní analýza je o zkoumání počítačových dat a programového vybavení. Forenzní analytik nebo znalec nesmí interpretovat závěry v podobě viny nebo neviny, to přísluší pouze soudu. Nelze odpovídat na otázky legálnosti používání programového vybavení, jelikož to není definováno druhem instalace, ale kupní smlouvou mezi výrobcem, poskytovatelem a uživatelem. Lze v závěrech uvést fakt, že bylo nalezeno programové vybavení obcházející licenční ochranu a/nebo on-line aktivaci programu XY.

Lze pravděpodobně uvést i mnohé další příklady, kdy může docházet k prohřeškům vůči tomuto pravidlu.

Forenzní zkoumání v oblasti digitální forenzní analýzy musí být nezávislé pro obě strany sporu a musí se omezit pouze na interpretaci nalezených dat a objasnění způsobu jejich vzniku, původu, existence nebo případně zániku, a na děje a procesy s tím související.

Závěr

Uvedli jsme sedm hříchů digitální forenzní analýzy, které vnímáme jako nejzávažnější. Nekladli jsme si za cíl je nějak utřídit podle důležitosti, četnosti, závažnosti nebo jakkoliv jinak. Ani jsme neměli v úmyslu je vyjmenovat všechny, spíše jsme se orientovali na problémy snadno napravitelné. Jsou zde ovšem i neméně závažné problémy spojené s interpretací výsledků zkoumání, jejichž náprava však bude muset být podpořena legislativně.

U některých námi revidovaných závěrů znaleckých posudků nebylo možné odlišit, zda byly tyto závěry podloženy exaktním a dokumentovaným zkoumáním nebo se jedná „jenom“ o odborný názor znalce. Je to zčásti díky nedostatečné dokumentaci použitých postupů a metod a jednak díky tomu, že znalec, možná nevědomky, nerozlišuje tyto dva druhy závěrů – objektivní materiální skutečnost a odborný, tedy vlastně subjektivní, názor.

Jestliže tyto dva druhy závěrů znalec explicitně nerozlišuje, nelze toto rozlišení požadovat ani od OČTŘ. Tím mohou vzniknout často i kolizní situace, kdy proti sobě stojí dva závěry dvou znaleckých posudků, přičemž jeden je založen na exaktním zkoumání a jeho výsledkem je potvrzený fakt a druhý je založen na odborném názoru a jeho výsledkem je tedy subjektivní závěr (byť může být zkušenostmi podložen). Jestliže OČTŘ nemůže vzhledem ke složitosti problematiky rozlišit váhu těchto dvou závěrů, může nastat situace, kdy dochází k rozhodování, zda „tato bílá koule je skutečně černou kostkou nebo nikoliv“.

[1] Svetlík, M., Digitální forenzní analýza a bezpečnost informací, Data Security Management, 1/2010, str. 20 - 23, dostupný na adrese http://www.rac.cz/RAC/homepage.nsf/CZ/Clanky/$FILE/DSM-Digitální%20forenzní%20analýza-01-2010.pdf.

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

XRY COMPLETE

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

> CO JE XRY COMPLETE

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

> ŠIROKÉ MOŽNOSTI EXPORTU

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

> XRY COMPLETE OBSAHUJE

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

> PRODEJ A PODPORA V ČR

RISK ANALYSIS CONSULTANTS, S.R.O.
Španělská 2, Praha 2
zu@rac.cz

www.rac.cz

Forenzní logy pohledem vývojáře

Logy jako jeden z klíčových zdrojů informací pro vyšetřování událostí v ICT

Karel Dohnal pracuje ve společnosti AVG Technologies CZ, s.r.o. na pozici Information Security Architect. Jeho hlavním zaměřením je analýza a vyhodnocení rizik pro firemní systémy včetně jejich testování. V případě bezpečnostních incidentů provádí forenzní analýzu. V roce 2013 získal certifikaci CISSP. Programování se věnuje od svých 8 let. Svůj volný čas tráví s rodinou a vařením.

Anotace:

První ze slíbené série článků, které jsou věnovány logům v informačních systémech a jejich využití při digitální forenzní analýze. V tomto článku se autor věnuje některým základním pojmům, základním typům logů, typickým útokům na logy a některým dalším vlastnostem, které je potřebné zvažovat při forenzních analýzách.

Informační vědomí

Ať už v knižním nebo reálném životě, každý detektiv potřebuje pro svůj příběh informace, aby se podařilo případ úspěšně uzavřít a darebákům zajistit odpovídající trest. V digitálním světě, kde jsou informace prchavé, je potřeba mít způsob, jak zajistit jejich stálost. V obecné rovině se ujal anglický pojmem „log“ nebo také „logfile“, či v češtině též známý „žurnál“.

Logem se rozumí soubor obsahující záznam o událostech. Událostí je cokoliv, co se v daném systému stane - např. přihlášení uživatele do systému, otevření souboru, smazání záznamu v databázi, apod.

Asi nejznámějším logem je Event manager v operačních systémech Microsoft Windows, který je nezbytným informačním zdrojem každého administrátora a forenzního analytika. Avšak není jediným. V případě Microsoft Windows lze informace nalézt i v registrech systému (např. historie připojených USB zařízení je uložena v sekci `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\`) [1] nebo v dedikovaných LOG souborech (např. postup instalace Internet Exploreru 11 je uložen v souboru `IE11_main.log` v adresáři operačního systému – většinou `C:\Windows\`).

Moderní programy pro svoji práci a komfort uživatele používají SQLite databáze, které jsou taktéž velmi cenným forenzním zdrojem dat. Například webový prohlížeč Firefox od společnosti Mozilla ukládá seznam navštívených stránek a stáhnutých souborů do souboru `places.sqlite`, který je uložen v adresáři, kam si prohlížeč ukládá profily [2].

Za zmínku stojí i samotný souborový systém, který poskytuje informace o založení, posledním přístupu i modifikaci souboru. Správným výběrem řadícího klíče lze vytvořit časovou osu aktivit uživatele v daném systému a přečtením clusterů disku lze získat buď úplnou anebo alespoň částečnou informaci o obsahu smazaných souborů.

Cíl je vždy stejný – sestavení co nejdetailnější časové osy ve zkoumaném období.

Tvorba logů v aplikacích

Při návrhu aplikace je nutné myslet i na tvorbu logu. Opomenutí této části vede jak k velkým problémům při analyzování nestability a nečekaných výsledků, tak i absenci důležitých informací při forenzním zkoumání.

Na počátku jsou tři možné cesty:

- využití logovacího systému platformy, pro kterou nebo na které je program tvořen,
- využití již existujícího logovacího formátu ve vlastním logu,
- vytvoření vlastního formátu ve vlastním logu.

První možnost je vždy nejjednodušší. Zavoláním patřičné metody a předáním hodnot jako priorita, druh zprávy a textu, dojde k zapsání informace do společného prostoru událostí (v Microsoft Windows jde o Event manager) nebo do dedikovaného systému (například Syslog server). Nevýhodou takového přístupu je zpětné získání informací a jejich případné kolektování a odeslání do tzv. Crash portálů. Z pohledu forenzního analytika jde o ideální přístup, protože všechny informace z celého systému jsou na jednom místě.

Druhá možnost v sobě obsahuje několik dobře nadefinovaných formátů (např. Common Log Format, Extended Log Format, Log4j, Syslog, apod.) s dostupnými knihovnami pro různé programovací nebo skriptovací jazyky, a to jak pro tvorbu, tak i čtení a následnou analýzu záznamů. Nevýhodou je, že každý formát je navržen buď pro obecné anebo příliš specifické použití a navrhovaná aplikace se nemusí do daného rámce vejít. Například zmíněný Common Log Format [5] je primárně určen pro webové služby. Zaznamenává se příchozí IP adresa, identita klienta (pokud je známa), čas příchozího požadavku, URI, návratový HTTP kód a velikost odpovědi. Takový formát je nevhodný pro zaznamenání postupu instalace nebo zaznamenání chyby vzniklé během zpracování. K tomuto účelu se více hodí Log4j formát [6], který byl primárně navržen pro programovací jazyk Java. Zaznamenává jak důležitost zprávy (trace, debug, info, warning, error, fatal), tak i čas, soubor, číslo řádku, ve kterém se událost vyskytla a doprovodný text.

Třetí možnost, vytvoření vlastního formátu, dává v návrhu neomezené možnosti a je nejvíce flexibilní. Lze do něj uložit tolik informací, kolik je potřeba a ve formátu, který vyhovuje dané oblasti použití. Nevýhodou proprietárního řešení je jeho unikátnost a nulová podpora ze strany analytických nástrojů. Takový přístup požaduje od tvůrců vytvoření a udržení dokumentace, což je v praxi nejčastější problém.

V obecné rovině nelze říct, který z přístupů je ten nejsprávnější. Je třeba vždy zohlednit rozsah použití a účel. Pokud je tvořena jednoduchá aplikace pro webový server, potom plně postačují informace vytvořené webovým serverem, který implementuje/podporuje známé formáty. Naopak rozsáhlé aplikace komunikující s dalšími systémy by měly zaznamenat, s jakým systémem komunikují, účel komunikace a s jakým výsledkem. Dobrým forenzním vodítkem je také zaznamenání velikosti dotazu i odpovědi v bytech a čas spotřebovaný k vyřízení požadavku. Tyto údaje mohou pomoci odhalit případný neoprávněný přístup. Pokud je to možné, měly by být použity již definované formáty.

Textové a binární formáty

Logy mohou být v textové nebo binární podobě. Textová je vhodnější pro čtení člověkem, naopak binární dokáže uspořit místo (do jednoho byte lze uložit stav až osmi binárních proměnných) a zrychlit hledání dat díky přirozenější reprezentaci dat pro strojové zpracování. Nevýhodou je nutnost vlastnit nástroj, případně dokumentaci, umožňující přečtení a transformaci do textové a člověkem čitelnější podoby.

V případě síťového přenosu je vhodnější binární formát díky své kompaktnosti. Naopak textový formát lze před přenosem komprimovat (stejně i tak binární, ale většinou s menším kompresním poměrem), avšak komprimace a následná dekomprimace vyžaduje strojový čas, který je v silně zatíženém prostředí komplikací.

Příkladem binárně uloženého logu je registr Microsoft Windows. Jeho jednotlivé části jsou uloženy v binárních souborech v podadresáři `System32\config` a dalších [3]. Široce používaný databázový systém MySQL využívá pro záznam změn taktéž binárního logu [4]. Pro jeho čtení je nutné použít specializovaných nástrojů.

Textový log je výhodné použít v případech, ve kterých se očekává častější čtení a zpracování člověkem. Nejčastěji se s nimi lze setkat při instalačních, odinstalačních procedurách anebo u webových serverů. Nejrozšířenější webový server HTTP od Apache Foudantion umožňuje zápis v již zmíněném formátu Common a Combined Format [5].

Textové logy sami o sobě neimplementují žádnou ochranu proti neoprávněné modifikaci. Jejich integrita je plně ponechána na nastavení ACL na úrovni operačního systému, profesionalitě administrátorů, anebo Log management systému. Z pohledu analýzy je vždy dobré ověřit, že kódování a konce řádků odpovídají platformě, na které byl log vytvořen. Pokud jsou řádky zakončeny znaky `0x0D 0x0A`, což jsou řídicí znaky CR (Carriage Return) a LF (Line Feed) používané na systémech Microsoft Windows a log byl vytvořen na UNIX platformě, kde řádky jsou zakončeny pouze znakem `0x0A` (Line Feed), potom jde o jasný indikátor, že soubor byl během transportu modifikován. Konce řádků (též označované mezi vývojáři jako EOL – End Of Line) patří mezi netisknutelné a v textových prohlížečích se nemusí projevit. Jejich původ je z dob, kdy se pro výstup používaly tiskárny a terminály a bylo potřeba zajistit, aby se tisková hlava nebo terminálový kurzor na konci řádku vrátil na první sloupec (Carriage Return) [7] a válec posunul papír o jeden řádek (Line Feed).

Binární logy sami o sobě ve většině případů neimplementují žádnou ochranu proti neoprávněné modifikaci. Avšak jejich výhodou je, že vnitřní struktura může obsahovat offsetové odkazy, takže při změně velikosti souboru může dojít k narušení vnitřní integrity a log se takzvaně „rozsype“. Tzn.: odkazy vedou na nesmyslné hodnoty a čtecí nástroje zahlásí chybu.
Jedním z možných způsobů zajištění integrity logů je jejich uložení v LMI systémech, které jsou navrženy tak, aby zajistily integritu a pomohly s analýzou [8].

Útoky na logy

Zajímavou formou maskování informace je narušení syntaxe logu a to nikoliv formou přímého zásahu člověka, ale uložením oddělovacího znaku skrz aplikaci. Jako příklad lze použít textový Common Log Format [5], který je ve formátu:

```
127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326
```

Tučně zvýrazněné části jsou informace, které posílá klient (prohlížeč) webovému serveru. Část začínající slovem „GET“ je ohraničena uvozovkami. Pokud dojde k přijmutí následujícího upraveného požadavku:

```
GET /apache_pb.gif" HTTP/1.0
```

do logu se uloží následující řetězec:

```
127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif" HTTP/1.0" 200 2326
```

Červeně označené uvozovky tak narušují původní syntaxi ohraničení požadavku klienta uvozovkami. Pokud na tuto skutečnost nejsou LMI systémy nebo analytické nástroje připraveny, v nejlepším případě zahlásí chybu, v nejhorším řádek mlčky přeskočí (pozor také na konstrukci regulárního výrazu, pokud jde o ruční vyhledávání). Přitom pro forenzní analýzu jsou takové anomálie důležitým prvkem při hledání způsobu průniku do systému.

Další způsob útoku je forma „vyhladovění“. Útočník otevře síťové spojení na server, ale nepošle požadavek. Aplikace tak čeká na data, dokud nedojde k uzavření spojení systémem. Špatná implementace na úrovni aplikace způsobí, že se v logu neobjeví záznam o otevřeném spojení. Je proto nutné zaznamenávat i takové požadavky, které nebylo možné obsloužit.

Některé systémy implementují tzv. rotaci logů. Jde o techniku, kdy je otevřený soubor, do kterého se zapisují události uzavřen a přejmenován z důvodu rychlosti a velikosti souboru a nový soubor otevřen pro zápis. Rotačním kritériem je buď časový úsek (jeden den), anebo velikost souboru (řádově MB). Po definované iteraci dochází ke smazání souboru. Analogie je nahrávání videozáznamu na pásku. Jakmile nahrávací zařízení narazí na konec, začne nahrávat od začátku. Pokud nejsou rotované soubory zpracovány, je pro útočníka jednoduché buď počkat, až se záznamy o aktivitě smažou, anebo vygenerovat dostatečné množství dotazů, které zakryjí ilegální aktivitu. V takovém případě implementace je nutné soubory co nejdříve zpracovat.

Ve většině systémů mají logy předem určené místo, kde se ukládají. Ve většině případů jde o dedikovaný disk nebo prostor. Pokud není implementovaná rotace, nebo odmazávání dat, je pro útočníka výhodné nejdříve vygenerovat takové množství regulérních dotazů, které povedou ke konzumaci zbývajícího místa na disku a teprve potom provést ilegální operaci. Ve většině případů při nedostatku místa pro logy se aplikace neukončí a pokračuje v obsluze požadavků. Taková aktivita nebude nikde zaznamenána.

Centralizované a distribuované ukládání

Při samotném návrhu aplikace a tím i způsobu ukládání logů je nutné vzít v potaz účel, předpokládané zatížení, množství generovaných událostí a potenciální budoucí rozvoj. Obzvláště poslední zmíněné je nejdůležitější. Při špatném rozhodnutí se dostavují komplikace ve formě nedostatečných kapacit nebo naopak příliš složitého kódu.

Centralizované ukládání, kdy všechny logy jsou shromažďovány na jednom místě, je výhodné pro systémy, které jsou geograficky i síťově blízko sebe a během zasílání zpráv nedochází k velkým časovým prodlevám. LMI systémy navíc provádějí zpracování přijatých informací a ukládají do databází podle předdefinovaných klíčů, čímž markantně usnadní vyhledávání. Tento benefit je však také největší nevýhodou. Indexy zabírají místo, musí se udržovat a jejich sestavení je zdrojově náročné.

Centralizované ukládání není vhodným řešením pro systémy, které jsou geograficky odděleny nebo rozprostřeny, což je případ moderních systémů. Firma, která působí celosvětově, potřebuje, aby její webové prezentace a backendové systémy byly co nejblíže k jejím zákazníkům a aby odezva byla co nejkratší. Pokud by systémy běžící v Severní Americe, Asii či Austrálii měly posílat své provozní informace do České republiky, brzo by došlo k zahlcení front díky latenci a ztrátovosti paketů a systém by začal dominově kolabovat. V takovém případě je vždy vhodnější ukládat informace v lokálním datovém centru, případně zpracovat a pouze vybrané informace poslat do centrálního repozitáře pro další analýzy. Takový postup však znamená časovou prodlevu mezi vznikem bezpečnostního incidentu a jeho detekcí.

Centralizovanost a distribuovanost se řeší i v mnohem menších systémech. Pokud je vyvíjena aplikace pro lokální stanici, vývojář či architekt stojí před rozhodnutím, zdali informace posílat do Event managera operačního systému nebo si založit vlastní log a do něj zapisovat potřebné události (viz část Tvorba logů v aplikacích).

Centralizovanost je při hledání souvislostí v celém systému obrovskou výhodou šetřící čas. Avšak z pohledu vývojáře jde o potenciální „Single Point Of Failure“ [9], kdy jeho selháním může dojít k zastavení chodu aplikace. Rozhodnutí by se mělo vždy odvíjet od účelu, zatížení a budoucího rozvoje aplikace.

Synchronizace času a časové zóny

V distribuovaných systémech (ať už geograficky nebo napříč zařízeními ve stejném datovém centru) je důležité mít synchronizovaný čas. K tomu je vhodné vyčlenit jedno zařízení, které se stane hlavním NTP serverem [10] a všechna zařízení vůči němu synchronizovat. Alternativou je využití externích služeb, jako např. `ntp.nic.cz` [11], ale bez garance dostupnosti.

Pokud by se systémový čas na jednotlivých serverech lišil, potom by se lišila i časová razítka záznamů. Následná agregace dat a vytvoření časové posloupnosti musí reflektovat časové posuny, což u zatížených systémů znamená pracovat i s milisekundami.

Dalším důležitým aspektem v případě vytváření vlastního formátu logu je kromě aktuálního času události i uvedení časové zóny, ve které se server nachází nebo vůči které má nastaven čas. Ideální je použít jeden z následujících standardů (nebo pozdějších aktualizací):

- ISO 8601 [12] – příklad: 2005-08-15T15:52:01+00:00

► RFC 822 [13] – příklad: Mon, 15 Aug 05 15:52:01 +0000
► RFC 850 [14] – příklad: Monday, 15-Aug-05 15:52:01 UTC

Závěr

Logy jsou důležité jak pro vývoj, tak i pro následné zkoumání. Měly by být vždy tvořeny s ohledem na použití, kapacitu i předpokládaný vývoj. Kde to situace umožňuje, snažit se logy zasílat do centralizovaného systému, anebo ukládat lokálně s využitím známých formátů a knihoven.

Při návrhu je také nutné myslet i na ochranu dat a rozhodnout se, jak by se měla aplikace zachovat, pokud dojde místo na disku nebo vzdálený systém odmítne logy přijímat.

Aby nedocházelo k různým interpretacím uložených událostí, je nezbytností každého projektu udržovat dokumentaci aktuální.

Bibliografie

[1] USB History Viewing - ForensicsWiki. ForensicsWiki [online]. [12 January 2012] [cit. 2014-11-16]. Dostupné z: http://www.forensicswiki.org/wiki/USB_History_Viewing

[2] Profile folder - Firefox - MozillaZine Knowledge Base. MOZILLA [online]. 1998-2007, [2 September 2014] [cit. 2014-11-16]. Dostupné z: http://kb.mozillazine.org/Profile_folder_-_Firefox

[3] Registry Hives (Windows). MICROSOFT. Registry Hives [online]. 2014 [cit. 2014-11-16]. Dostupné z: http://msdn.microsoft.com/en-us/library/windows/desktop/ms724877%28v=vs.85%29.aspx

[4] MySQL :: MySQL 5.0 Reference Manual. ORACLE CORPORATION AND/OR ITS AFFILIATES. The Binary Log [online]. 2014 [cit. 2014-11-16]. Dostupné z: http://dev.mysql.com/doc/refman/5.0/en/binary-log.html

[5] Common Log Format – Wikipedie. Combined Log Format [online]. 2014 [cit. 2014-11-16]. Dostupné z: http://cs.wikipedia.org/wiki/Common_Log_Format

[6] Log4j - Wikipedia, the free encyclopedia. Log4j [online]. 2014 [cit. 2014-11-17]. Dostupné z: http://en.wikipedia.org/wiki/Log4j

[7] Carriage return - Wikipedia, the free encyclopedia. Carriage return [online]. 2014 [cit. 2014-11-17]. Dostupné z: http://en.wikipedia.org/wiki/Carriage_return

[8] KENT, Karen a Murugiah SOUPPAYA. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST SP 800-92. Guide to Computer Security Log Management. Gaithersburg (USA): NIST, 2006. Dostupné z: http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

[9] Single point of failure - Wikipedia, the free encyclopedia. Single point of failure [online]. 2014 [cit. 2014-11-17]. Dostupné z: http://en.wikipedia.org/wiki/Single_point_of_failure

[10] Network Time Protocol. Wikipedia, the free encyclopedia [online]. 2014 [cit. 2014-11-17]. Dostupné z: http://en.wikipedia.org/wiki/Network_Time_Protocol

[11] CZ.NIC přinese do českých počítačů přesný čas. CZ.NIC [online]. CZ.NIC, z. s. p. o., 2007 [cit. 2014-11-17]. Dostupné z: http://www.nic.cz/page/329/cz.nic-prinese-do-ceskych-pocitacu-presny-cas/

[12] ISO 8601. Wikipedia, the free encyclopedia [online]. 2014 [cit. 2014-11-17]. Dostupné z: http://en.wikipedia.org/wiki/ISO_8601

[13] RFC 822: DATE AND TIME SPECIFICATION. UNIVERSITY OF DELAWARE. STANDARD FOR THE FORMAT OF ARPA INTERNET TEXT MESSAGES [online]. Newark (USA): University of Delaware, 1982 [cit. 2014-11-17]. Dostupné z: https://tools.ietf.org/html/rfc822#section-5

[14] RFC 850. HORTON, Mark R. Standard for Interchange of USENET Messages [online]. 1983 [cit. 2014-11-17]. Dostupné z: https://tools.ietf.org/html/rfc850#section-2.1.4

Architektura ICT pro efektivní provoz FTK5

Správné dimenzování a HW architektura je klíčem pro efektivní práci s FTK5

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

Anotace:

Článek seznamuje čtenáře se zkušenostmi Znaleckého ústavu RAC při instalaci a optimalizaci systému FTK5. Popisuje různé konfigurace infrastruktury ICT pro efektivní provoz FTK5 včetně nedostatků a/nebo výhod jednotlivých konfigurací. Čtenář získá neocenitelné poznatky z praktických testů a použitím popsaných informací ušetří hodně času experimetováním.

Úvod

AccessData Forensic Toolkit je analytický nástroj, využívající lokální a distribuované zpracování dat s úložištěm v podobě centrální databáze. Výkon, respektive rychlost zpracování analýz, závisí na zvolené HW architektuře.

Při volbě architektury je nutné zohlednit zejména průměrnou velikost případů. Poddimenzování by v praxi znamenalo nepoužitelnost, naopak předimenzování by vedlo k finanční nerentabilitě provozu.

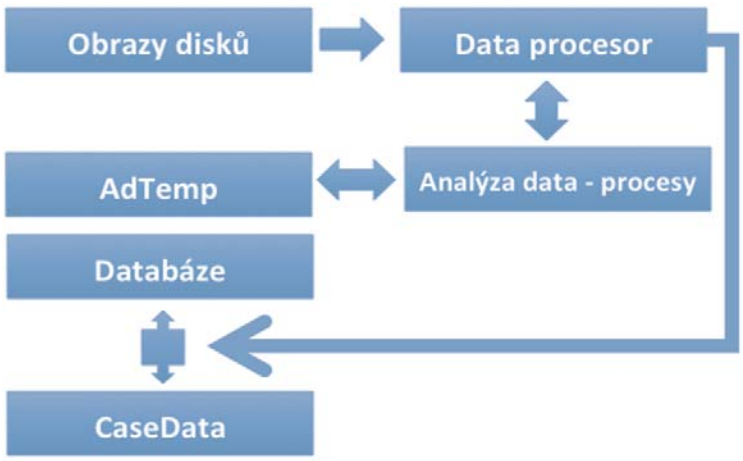
Použitelné architektury:
- Instalace na jednom PC / NTB
- Client - Server instalace
- Client - Server + Paralelní síťové procesory

Dimenzování – dle finančních možností:
- CPU
- RAM
- HDD

Proces zpracování dat v FTK

Obrazy disků jsou načítány data procesorem, který spouští jednotlivá vlákna analytických modulů. Počet vláken je dán nastavením profilu analýzy, definovaným pro daný případ, nebo konkrétní stopu. V průběhu analýz jsou v adresáři AdTemp vytvářeny dočasné soubory. Tyto soubory reprezentují soubory například z rozbalených komprimovaných archivů, e-mailových archivů, databází apod.

Po dokončení zpracování souboru jsou výsledky uloženy do adresáře CaseData, který obsahuje veškeré informace o zpracovávaném případu. Dále jsou informace, jako data pro indexované vyhledávání, uložena v databázi.



Čtení obrazů disků zatěžuje disky kontinuálním čtením velkých objemů dat v řádech stovek gigabajtů až jednotek terabajtů. CaseData a databáze při zpracování dat utilizuje disk zápisem, při prohlížení dat a vyhledávání zase čtením. AdTemp je využíván pouze při zpracování stop, nicméně disk je vytěžován častým zápisem a čtením malých souborů. Při takovémto nehomogenním zatížení není možné I/O operace optimalizovat a je nutné je rozdělit mezi více fyzických pevných disků nebo diskových polí.

Utilizace hardwaru

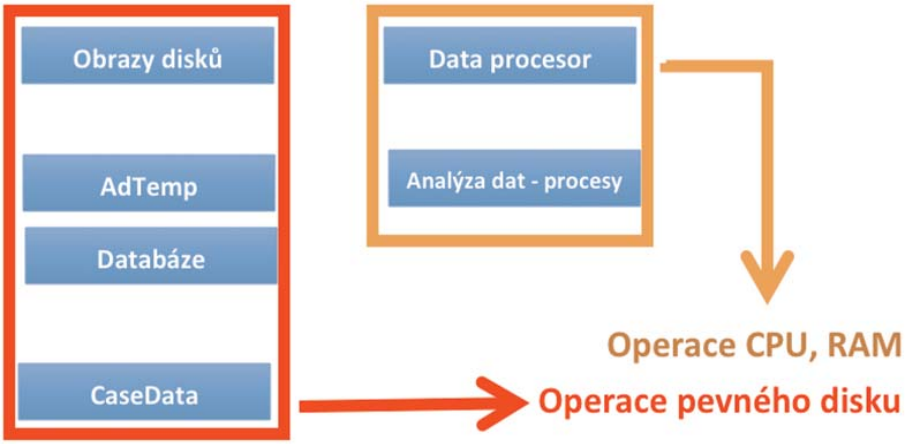
Diskové operace při analýze obrazů disků kladou velké nároky na počet operací čtení / zápis na řadiče pevných disků a samotných pevných disků. Především pro odkládací prostor AdTemp nebo databázi je nejvhodnější použít SSD pevné disky z důvodu jejich krátké vybavovací doby při přístupu k náhodný blokům dat. Samotné SSD disky mají dostatečnou propustnost, nicméně i ta se dá dále vylepšit pomocí zapojení do RAID5 diskového svazku.

Čtení a zápis souborů je jen část prováděných operací. Samotné analýzy spotřebovávají systémové zdroje ve formě CPU a operační paměti.

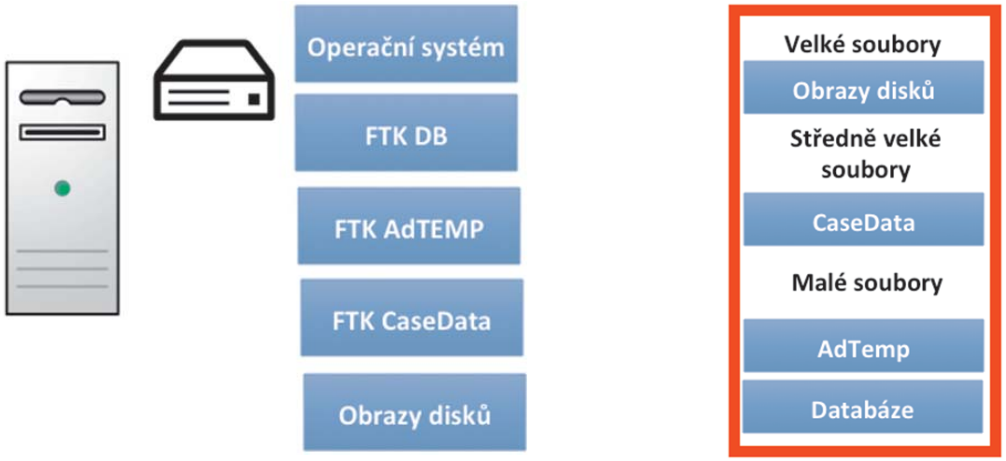
Samotný výkon klíčových komponent neurčuje výsledný výkon sestavy jako celku. Je nutné správně dimenzovat i propojovací sběrnice. Výběr základní desky a řadiče pevných disků dramaticky ovlivňuje výsledný výkon pracovní stanice pro forenzní analýzu. Je nutné posuzovat systém jako celek a dimenzovat ho s ohledem na velké objemy dat.

Jako zcela nevhodná architektura počítačové sestavy pro provozování FTK je instalace všech komponent na jeden pevný disk. Způsob zpracování stop byl již naznačen, stejně tak i charakteristiky zátěže pevných disků generované jednotlivými analytickými moduly.

Situace, kdy je jeden pevný disk vytěžován operačním systémem, čtením obrazů disků, rozbalováním archivů, analyzováním dat, ukládáním mezivýsledků a indexací textových řetězců, vede v lepším případě k prodloužení doby zpracování. V horším případě po týdnu zpracovávání některý z modulů zamrzne a zamezí tak dokončení analýzy. Tato situace je špatná ze dvou důvodů 1) ztráta času, který byl spotřebován na analýzu 2) ztráta času, než si některý z uživatelů všimne, že analýza stále formálně probíhá, ale utilizace systému spadla na minimum a zpracování dat už dále neprobíhá. Při testování této architektury běžně docházelo k zamrznutí výpočtů cca. po 3-5 dnech, další 2-3 dny trvalo, než bylo zpracování dat vyhodnoceno jako ztracené. Důvodem pro toto zpoždění je fakt, že systém, který má zvolenou jednodiskovou architekturu, vykazuje značné výkyvy v zatížení procesorů a operační paměti. Po dobu, kdy systém čeká na dokončení diskových operaci, jsou procesory, zejména vzhledem ke svému velkému výkonu, zátěžovány jen minimálně. Rozložení zátěže na CPU a RAM je tedy jen nárazové a krátkodobé (v řádech hodin). Takovéto chování lze vysledovat v resource manageru systému Windows a je to zjevná známka nevhodné HW konfigurace. Nízká propustnost systému může sloužit i jako indikátor

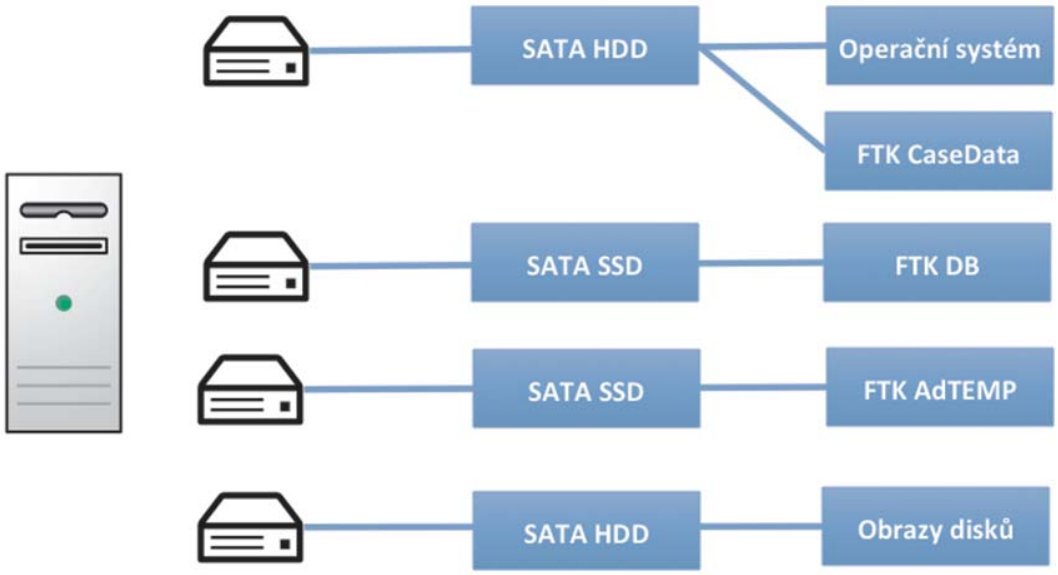


Jedno PC - Nevhodná architektura



Vzhledem k různým charakteristikám zatížení pevných disků, je jediné správné řešení rozdělení zátěže na jednotlivé fyzické pevné disky. Pokud není možné použít extra pevný disk pro ukládání dat případů v adresáři CaseData, lze tento adresář umístit na pevný disk spolu s operačním systémem.

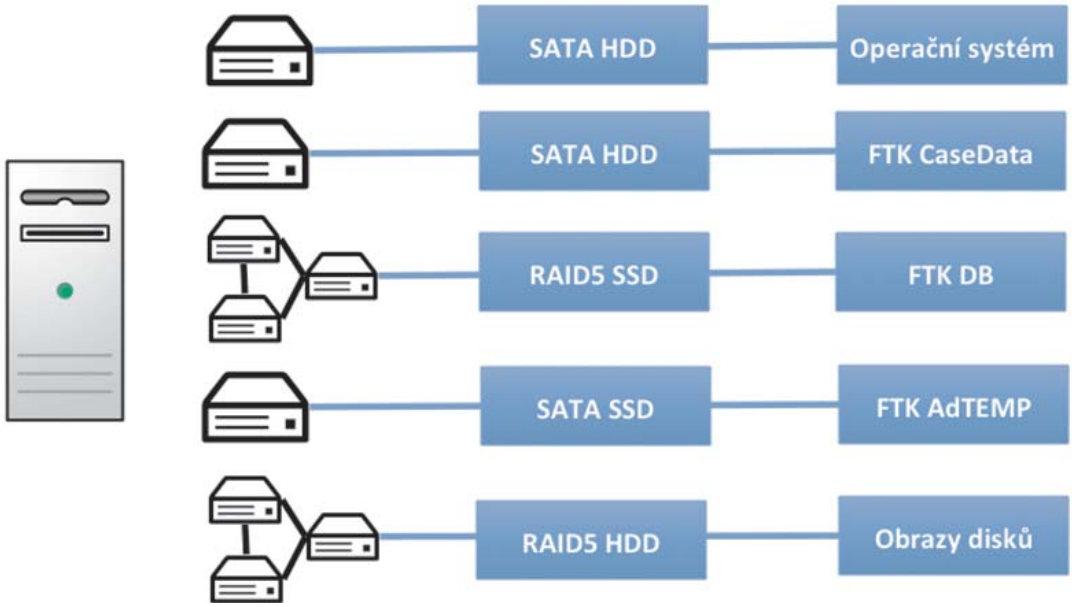
Jedno PC - Minimální architektura



poruchy HW.

Minimální architektura zajišťuje spolehlivý chod u malých případů, kde se zkoumají 2-3 stopy o celkové velikosti 300 - 500 GB (záleží na počtu souborů). U větších případů bude odezva uživatelského rozhraní neúnosně pomalá.

Jedno PC - doporučená konfigurace



Optimální je operační systém provozovat ze samostatného disku. Pro tento účel postačí jakýkoliv metalický disk o 7200 otáčkách a kapacitě 1TB. Disky pro databázi a obrazy disků je vhodné provozovat z RAID5 diskového pole. Tato architektura je použitelná pro případy o celkové velikosti do 750 GB.

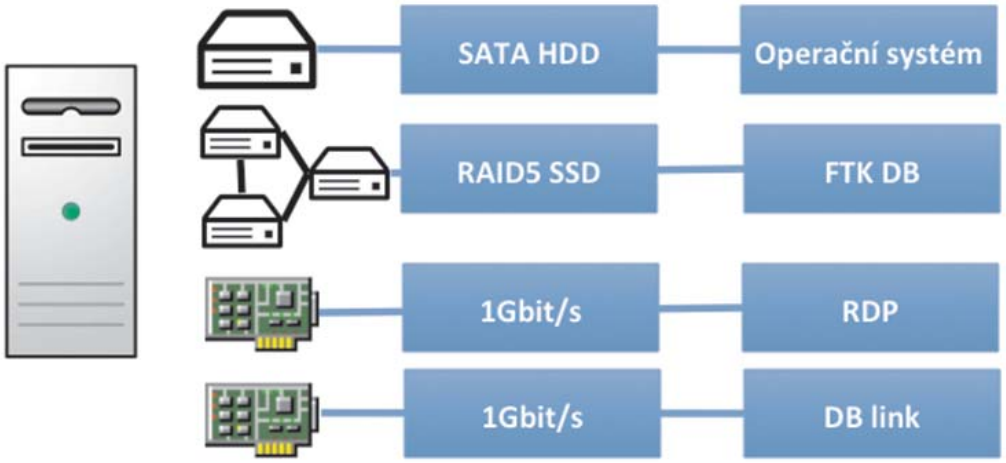
Architektura Klient-Server

Pro případy o celkové velikosti stop větší než 750 GB je nutné použít architekturu klient-server s možným doplněním o distribuované síťové procesory. Architektura klient-server vychází z doporučené konfigurace s tím rozdílem, že databáze a uživatelské prostředí jsou provozovány na oddělených strojích. Rozdělení architektury na dva fyzické stroje s sebou přináší nový problém v podobě přenosu dat mezi databází a klientem. Stejně jako pevné disky, i síťové linky mají omezenou kapacitu a je nutné segregovat jednotlivé datové okruhy na samostatné síťové linky (síťové karty).

Klient-Server - FTK Server

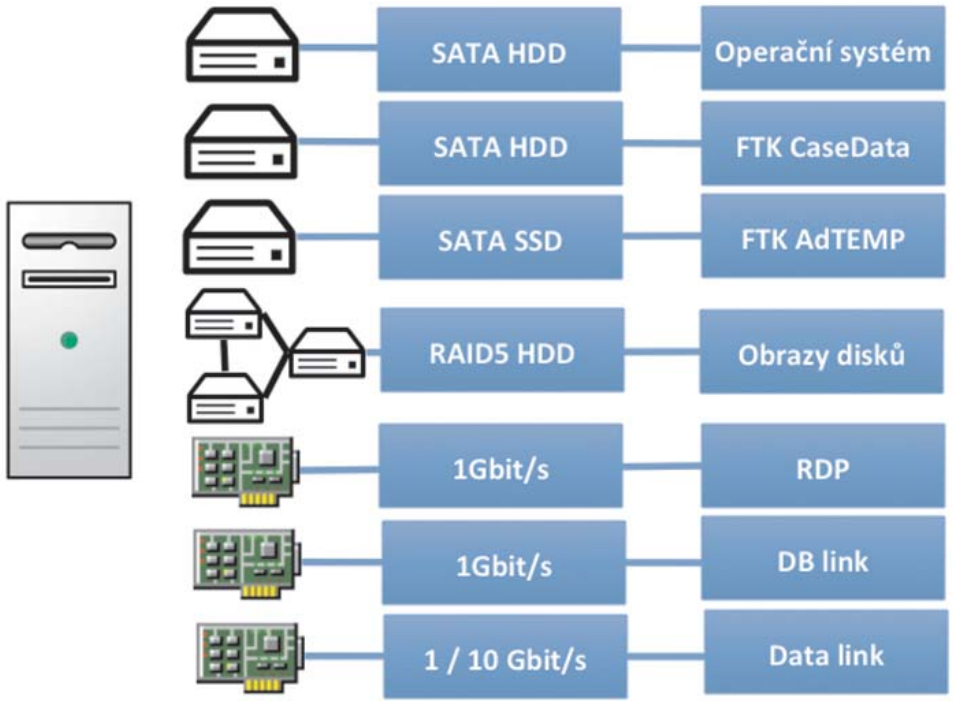
Server, vyjma disku s operačním systémem, potřebuje jeden RAID5 diskový oddíl pro datový adresář databáze. Rozdělení síťového provozu je realizováno pomocí dvou nezávislých síťových karet o rychlosti 1 Gbit/s.

První síťový okruh je vyhrazen pro databázovou linku mezi serverem a klientem. Spojení může být realizováno napřímo, bez použití síťového přepínače. Druhý síťový okruh slouží pro vzdálený přístup k serveru. Tento přístup je využíván zejména pro servisní potřeby.



Klient-Server - FTK Klient

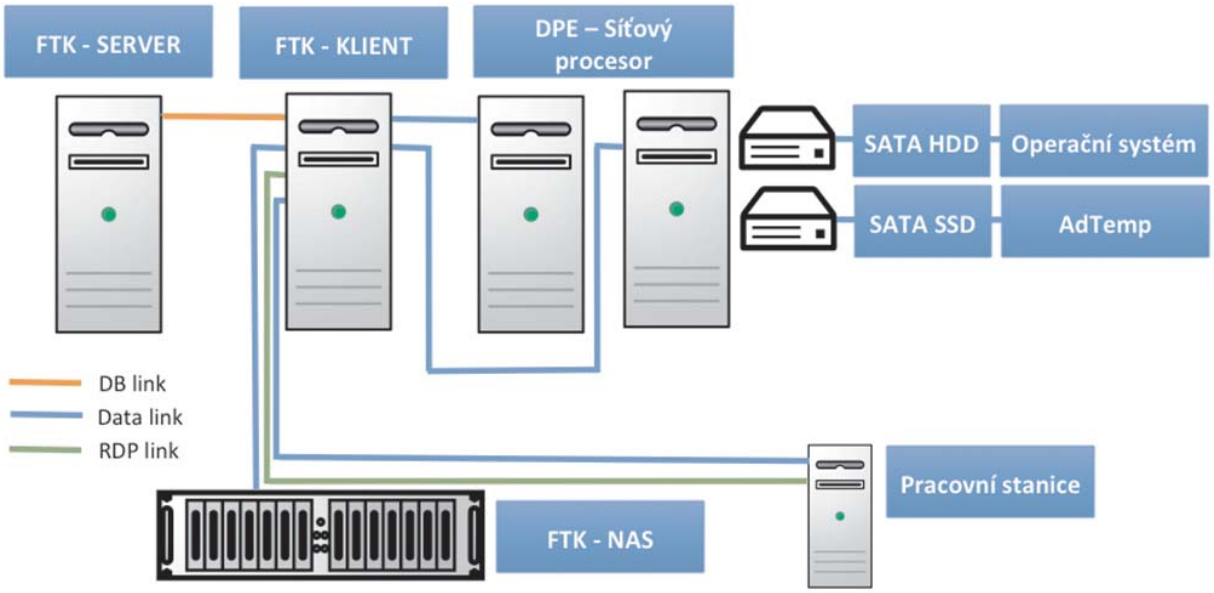
Klientská stanice (klientská ve smyslu uživatelského prostředí FTK) je klíčový bod celé sestavy. Jednak provádí zpracování a interpretaci stop, dále zajišťuje zpřístupnění dat pro paralelní procesory, popřípadě zajišťuje propojení s NAS. Od doporučené sestavy se tato architektura liší jen v počtu a nastavení síťových okruhů. Obdobně jako server, i klient obsahuje vyhrazený síťový okruh pro databázovou linku a linku pro vzdálený přístup (je vhodné obě zařízení umístit co nejblíže k sobě, proto je uživatelský přístup realizován přes RDP), navíc ovšem musí obsahovat vyhrazený okruh pro datové přenosy (kopírování obrazů disků, pracovní stanice -> FTK klient) a v případě napojení na NAS další vyhrazený okruh pro přenos mezi NAS a FTK klientem.



Zpracování obrazů disků je nutné vždy provádět lokálně tzn. z RAID5 pole určeného pro ukládání obrazů. V průběhu testování různých architektur pro FTK byl proveden pokus, kdy lokální úložiště obrazů disků bylo nahrazeno síťovým diskem. Tato změna vedla k nestabilitě při zpracování dat a značnému zpomalení odezvy uživatelského prostředí.

Klient-Server - distribuované síťové procesory

Rychlost zpracování lze do jisté míry ovlivnit počtem takzvaných distributed procesing enginů (DPE), pracujících paralelně ke zpracování dat na FTK klientu. Architektura paralelních síťových procesorů je jednoduchá a hardwarově se podobá FTK serveru. Pro operační systém postačí metalický pevný disk, pro dočasné soubory DPE je vhodné použit SSD disk alespoň o kapacitě 512 GB. DPE vyžaduje síťový přístup k FTK klientovi, a to přístup pro čtení k disku s obrazy disků a přístup pro čtení a zápis do adresáře CaseData. I zde je nutné počítat s vyhrazeným síťovým okruhem pro přenos dat o rychlosti 1 Gbit/s. Jeden nasazený DPE v průměru zrychlí zpracování dat o cca 10 procent.



Realizace zpřístupnění dat z FTK klienta směrem k uživatelské stanici je vždy závislá na konkrétním HW. SMB (Windows sdílení) by mělo být použito pouze pro přístup z pracovní stanice a pro přístup DPE (i zde je vhodnější NFS). Komunikace mezi FTK klientem a NAS je z důvodu nízké latence odezvy nutné realizovat pomocí iSCSI, popřípadě jinou technologii s rychlou odezvou a malou režií při přenosu.

Dále je vhodné, aby přístup pro zápis k datům byl možný jen z pracovní stanic. Přístup FTK klienta k datům je pak realizován pouze v režimu čtení.

Dimenzovaní HW

Dimenzováni počítačových sestav pro chod FTK je značně závislé na dostupných finančních zdrojích. Z důvodu finančních úspor a lepší flexibility je mnohdy vhodnější volit cestu výkonných pracovních stanic, které budou sloužit jako servery, než nákladných U serverů určených k montáži do racku.

V obou případech je však vhodné vycházet ze specifikace v manuálu FTK.

Rozložení pevných disků bylo již vysvětleno. Co se týká RAID řadičů, je vždy vhodné použít HW řadiče, než ty dostupné na základní desce. Nejméně vhodné je sestavovat softwarové RAIDové svazky.

Nově se ve forenzních stanicích začínají prosazovat výkoné PCI-e SSD disky, které mají díky připojeni přímo na sběrnici až dvojnásobnou reálnou propustnost oproti standardním SSD diskům.

Pro CPU obecně platí: čím více jader a vyšší frekvence, tím lépe. Minimální počet jader by měl být 4 a frekvence 3 GHz.

U operační paměti to už tak jednoznačné není. Vzhledem ke správě operační paměti systému Windows se jako nejefektivnější velikost paměti jeví 32 GB RAM. Obecně by mělo platit, že na každé jádro CPU by měly být dostupné 2 GB operační paměti. Vyplývá z toho, že i zmíněných 32 GB musí reflektovat použitý procesor nebo skupinu procesorů.

Doporučené dimenzováni vycházející z doporučení firmy AccessData:

Instalace FTK na jednom PC

	Minimální	Doporučené
CPU	4 jádra	48 jader
RAM	16 GB	96 GB

FTK Server - Databázový server

	Minimální	Doporučené
CPU	4 jádra	8–16 jader
RAM	16 GB	16–48 GB
LAN	1Gbit	10Gbit

FTK Klient - GUI, lokální procesor stop

	Minimální	Doporučené
CPU	4 jádra	8–32 jader
RAM	16 GB	16–64 GB
LAN	1Gbit	10Gbit

DPE - paralelní sítový procesor stop

	Minimální	Doporučené
CPU	2 jádra	4–16 jader
RAM	4 GB	8–32 GB
LAN	1Gbit	10Gbit

Z výše uvedených informací vyplývá, že dimenzování sestav je značně závislé na velikosti dostupného rozpočtu.

Znalecký ústav RAC nabízí obdobné přednášky,
jako byla tato na UTB ve Zlíně, i dalším školám a univerzitám.
Obsah, dobu i rozsah lze domluvit individuálně.

V případě zájmu nás kontaktujte na adrese zu@rac.cz

Přednáška odborníků ZÚ RAC na UTB ve Zlíně

Jednou ze základních podmínek úspěšného rozvoje digitální forenzní vědy a dalšího zvyšování odbornosti a vědomostí v oblasti je zapojení akademické sféry do výzkumu, vývoje a aplikací digitální forenzní vědy. Proto je spolupráce s akademickou sférou jednou z priorit práce Znaleckého ústavu RAC.

Po předběžných jednáních, a ve výsledku na základě pozvání docentky Komínkové Oplatkové a doktora Malaníka, se dne 7. 11. 2014 konala na Univerzitě Tomáše Bati ve Zlíně přednáška specialistů Znaleckého ústavu Risk Analysis Consultants, s.r.o. (RAC) na téma Digitální forenzní analýza.

Přednáška byla rozdělena na tři sekce. V první se studenti seznámili s problematikou soudního znalectví v oblasti výpočetní techniky v podmínkách ČR a se základními předpoklady pro práci s digitálními důkazy.

V druhém bloku byly představeny nástroje, praktické postupy a zkušenosti při zajišťování digitálních stop s ohledem na jejich integritu a důkazní sílu. V předvedeném výjezdovém kufříku RAC DEAT si posluchači měli možnost prohlédnout hardwarové nástroje pro zajišťování digitálních stop.

Třetí blok byl věnován živé demonstraci digitální forenzní analýzy mobilních zařízení. Během ukázky byl proveden export informací z mobilního telefonu na logické úrovni a interpretace získaných dat. Blok byl zakončen prezentací postupu zajišťování dat pomocí nástroje Digital Evidence Acquisition Suite (RAC DEAS)

Na závěr proběhla volná diskuze se studenty, včetně dotazů na možnosti odborné stáže v laboratoři Znaleckého ústavu RAC.

ISO/IEC 27 037
Guidelines for identification, collection, acquisition, and preservation of digital evidence


INTERNATIONAL STANDARD

ISO/IEC 27037

First edition
2012-10-15

Information technology Security techniques Guidelines for identification, collection, acquisition, and preservation of digital evidence

Technologies de l'information Techniques de sécurité Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques

Reference number
ISO/IEC 27037:2012(E)

© ISO/IEC 2012

Koncem roku 2012 byla organizací ISO schválena norma ISO/IEC 27 037. Norma se nazývá "Doporučení pro identifikaci, sběr, zajištění a ochranu digitálních důkazů" a patří do skupiny "doporučení pro nejlepší postupy v praxi".

Norma se zabývá několika oblastmi práce s digitálními důkazy, avšak tyto oblasti nepřesahují rámec prvotních úkonů, týkajících se jejich identifikace, sběru a uchovávání. Nezabývá se dalším zpracováním, využitím, analýzou, prezentací, archivací a ani likvidací digitálních důkazů.

Norma dává základní definice a doporučuje materiální, procesní a personální kritéria pro prvotní úkony. V závěru doporučuje postupy prvotních úkonů pro některé kategorie digitálních zařízení.

Není vůbec jednoduché podat nějaké hodnocení dokumentu, na obsahu kterého se podíleli i odborníci Znaleckého ústavu RAC. Pro vysvětlení je nutné dodat, že v rámci připomínkového řízení, které předcházelo samotnému schvalování normy členy organizace ISO, vznikla poměrně silná odborná skupina, která měla některé zásadní připomínky k připravovanému znění. Společně s kolegy z USA, Velké Británie, Nizozemí a dalšími jsme nedoporučovali schválení a navrhovali přepracování dokumentu. Nebylo nás však dost, tudíž jsme byli přehlasováni a norma byla v roce 2012 schválena v aktuálně platném znění.

Otevřeně tedy říkáme, že tato norma má už od počátku určité obsahové a věcné nedostatky. Je nám jasné, že organizace ISO není natolik operativní, aby byla schopna vydávat nebo aktualizovat normy stejnou rychlostí, jakou se vyvíjejí informační technologie. Nicméně alespoň v době vzniku by normy měly alespoň v základě odpovídat aktuálnímu vývoji v oboru.

Abychom ale jen nekritizovali určité nedostatky, někdy zastaralost nebo nekonzistenci dokumentu, zejména v jeho závěrečných pasážích, norma má jednoznačně i pozitivní aspekty.

► Norma patří do skupiny "best practices" a jako taková má vždy být přizpůsobována a implementována do konkrétního prostředí a podmínek. Tady musíme bohužel konstatovat, že u nás nejsou vytvořeny žádné předpoklady organizační, personální a ani materiální pro výklad a implementaci normy do našeho českého prostředí. A není to jenom do praxe policejní práce, která by měla být jednotná a v souladu s mezinárodními zásadami, ale i do praxe výkonu znalecké činnosti v oboru, a také to platí i pro další skupiny odborníků, kteří s digitálními důkazy přicházejí do styku (aktuálně např. bezpečnostní specialisté, zejména ti, kterých se týká ZoKB).

► Norma klade určité základní kvalifikační požadavky na odborníky, kteří s digitálními stopami přicházejí do styku, zejména tedy v případě nutnosti provádění prvotních úkonů. Můžeme si jen povzdechnout, že nejsou mnohdy zohledněny při výběru např. znalců v oboru, protože tito také s digitálními stopami pracují. Dodržování základních zásad manipulace s digitálními důkazy by mělo být alfou a omegou jejich znalecké práce. Mnoho i předních soudních znalců nezná ani základní požadavky na zajištění digitálních stop, které jsou v úvodu normy uvedeny. Ať už by se dostali do pozice konzultantů při zajišťovacích úkonech při práci policie, ať tyto úkony provádějí jako znalci samostatně v ostatních případech nebo ať tyto úkony provádějí již jako znalci ve svých laboratořích. Je zjevné, že např. v případě zkoumání celého počítače je nutné provést samotné zajištění dat znalcem v laboratoři a tyto postupy jsou prakticky totožné s postupy, které popisuje tato norma.

► Norma by měla být také určitým východiskem pro práci i dalších subjektů, které např. posuzují práci policejních techniků a expertů, pro práci státních zastupitelů a vyšetřovatelů, kteří fakticky vedou zajišťovací úkony a také jsou ze zákona nuceni hodnotit kvalitu znaleckých posudků v oboru informačních technologií. Ale i manažerů a řídících pracovníků, kteří mají ve své gesci pracoviště, kde se s digitálními stopami pracuje, ať už jsou to pracoviště státní, policejní nebo soukromé.

► Norma položila a sjednotila alespoň elementární zásady a pravidla práce při zajišťování digitálních stop na mezinárodní úrovni. Mnohé z nich (pravděpodobně u nás hlavně v policejní praxi) se jeví jako samozřejmé a dlouhá léta již aplikované do praxe. Nicméně naše zkušenosti říkají, že ani ta policejní praxe není tak ideální. Ale nejenom policisté se setkávají s digitálními stopami. Mnohem horší situace je u dalších subjektů, které také mají nebo by měli mít zajišťování digitálních stop v náplni práce. Pro ně tato norma může být (za podmínky tvůrčí aktualizace na aktuální podmínky technické, kulturní, regulatorní a další) vhodným základním dokumentem a návodem k činnosti.

Závěrem tedy můžeme konstatovat, že uvedenou normu chápeme, i přes některé její zjevné nedostatky, jako užitečný první krok k procesu, který ve svém důsledku povede ke zvýšení povědomí o specifikách práce s digitálními stopami a důkazy, a tím i k postupnému zkvalitnění práce všech, kteří se s digitálními stopami jakýmkoliv způsobem potkávají. Ať to jsou policejní technici a experti, soudní znalci, vyšetřovatelé, advokáti, soudci, ale i bezpečnostní specialisté a správci ICT, členové CERT týmů a všichni další.

RAC Digital Forensic InfoDay vol II.

Úvod

První svého druhu Digital Forensic InfoDay, který se konal v květnu 2014, zaznamenal nebývalý a skutečně neočekávaný ohlas. Téměř stovka účastníků potvrdila, že problematika Digital Forensics je nanejvýš aktuální nejenom pro policejní specialisty, ale i pro další odborníky z dalších státních organizací a institucí. Neméně užitečnou se ale jeví i pro ostatní odborníky, ať už to jsou soudní znalci nebo experti na informační bezpečnost a členové různých CERT týmů.

O formátu RAC InfoDay

Společnost Risk Analysis Consultants, s.r.o. (RAC) organizuje akce typu InfoDay již mnoho let. Základním účelem těchto akcí je podělit se o aktuální poznatky a novinky v daném oboru nebo o zkušenosti s praktickým použitím některého konkrétního produktu. Nejedná se tedy o školení, ale spíše o seminář na dané téma. Standardně jsou akce typu InfoDay orientovány zejména na vybrané produkty z portfolia RAC, kde jsou účastníci (jak aktuální uživatelé produktů, tak i další potenciální zájemci) seznamováni se základní funkcionalitou, určením a použitím produktů, novinkami, výhledem dalšího vývoje a nezřídka i s případovými studiemi, se kterými seznamují ostatní účastníky často samotní uživatelé daného produktu.

Aktuální listopadový Digital Forensic InfoDay se v podstatě přidržel výše uvedeného formátu s tím, že v plánu bylo představit kromě produktů i určité metodické principy práce s digitálními stopami a aplikaci těchto metodik při použití konkrétních nástrojů a produktů.

O průběhu akce

Díky pozitivnímu ohlasu na první, květnový Digital Forensic InfoDay jsme se rozhodli pokračovat v organizaci obdobných akcí. Ve výsledku jsme uskutečnili podzimní Digital Forensic InfoDay vol. II. Tentokráte jsme se sešli v mírně komornějším prostředí Erpet Golf Centra v Praze dne 19. listopadu 2014. A opět byl zájem veliký, účastníků se sešlo přes sedmdesát z celé republiky. Vzhledem k tomu, že na akci byli cíleně zváni pouze specialisté z policie a některých dalších státních institucí a že nám je jasné, že to pro ně není někdy jednoduché se uvolnit ze služebních povinností, jejich zájem nás nesmírně potěšil.

O dopoledním programu

Dopolední programový blok byl věnován zejména práci na místě zajištění. Naši specialisté podrobně vysvětlili důležitost prvotních úkonů při zajišťování

digitálních stop. Zajištění stop, v našem případě digitálních, je totiž klíčové pro veškeré další kroky a významně ovlivňuje nejenom obsahovou hodnotu získaných informací, ale i jejich následnou důkazní sílu.

Na několika příkladech byly ilustrovány i typické chyby, které se při zajišťování digitálních stop vyskytují, a důsledky, ke kterým mohou takové chyby vést. Jako důležité parametry zajištění digitálních stop byly vyzvednuty integrita, komplexnost a přiměřenost.

Právě pro zefektivnění procesu zajištění digitálních stop na místě byly Znaleckým ústavem RAC vyvinuty prostředky, které byly v prvním programovém bloku představeny.

DEAS

Systém DEAS (Digital Evidence Acquisition Suite) byl vyvinut Znaleckým ústavem RAC jako jednoduchý nástroj, který výrazně pomáhá standardizovat a zjednodušovat činnosti při pořizování obrazů datových médií na místě zajištění. Důvodů, které nás vedly k vývoji tohoto systému, bylo několik. Efektivita a spolehlivost činnosti experta/technika na místě zajištění, rychlost pořizování obrazů disků a také metodická správnost těchto postupů.

DEAS je speciálně kompilovaná Linuxová Live distribuce, založená na jádře Debian GNU/Linuxu. Je vybaven vybranými nástroji pro pořízení forenzních binárních kopií disků. Navíc je pro jednoduchost práce s nástrojem vytvořeno jednoduché a přehledné menu. Toto menu vede uživatele způsobem, který minimalizuje lidské chyby. 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
- Libewf (https://code.google.com/p/libewf/) je open-source 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).

Praktické ověření prokazuje, že v konfiguraci, která je použita v DEAS, je pořizování forenzních binárních kopií disků jednodušší, bezpečnější a výrazně rychlejší, než v případě použití nástroje FTK Imager pod Windows nebo při použití linuxového nástroje "dd" (nebo jeho forenzních variant), a 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.

Po představení systému DEAS následovala živá diskuse. To svedčí o tom, že účel vývoje systému DEAS byl odhadnut správně a že o nástroj je mezi odborníky z praxe nebývalý zájem. Diskutovány byly jednotlivé detaily funkčnosti a padlo i několik námětů na další vývoj a rozšíření jeho vlastností a možností.

DEAT

DEAT (Digital Evidence Acquisition Tools) je praktická sestava nástrojů, nářadí, technických zařízení a různých dalších doplňků v praktickém výjezdovém provedení v pevném a odolném kufříku. Základní inspirací pro sestavení DEAT byla doteď prakticky jediná dostupná a používaná sestava writeblockerů - blokátorů zápisu, která se aktuálně dováží z USA od firmy DigitalIntelligence.

Nicméně praktičnost této americké sestavy je značně diskutabilní. Proto jsme se rozhodli udělat mnohem účelnější sadu, která bude obsahovat nejenom blokátory zápisu, ale i další pomůcky a nástroje, které jsou pro práci na místě zajištění digitálních dat nezbytné.

Sestava DEAT nejenom, že obsahuje takové duplikátory a blokátory zápisu, které vyhovují koncovému uživateli (aktuálně Tableau a Wiebetech), ale i sadu dalších nástrojů pro práci s výpočetní technikou a další doplňky, jako např.

dokumentační techniku a další užitečné drobnosti. Navíc, sestava sady DEAT není nijak striktně stanovena, ale významnou vlastností je právě návrh a příprava obsahu na přání a podle konkrétních požadavků a zvyklostí každého konkrétního uživatele.

I následující diskuse a představení jedné konkrétní sestavy DEAT prokázala důležitost praktického výjezdového vybavení. Demonstrovali jsme sadu, kterou jsme postavili na základě našich vlastních zkušeností a pro naše vlastní potřeby a použití při zajišťování digitálních dat na místě výjezdu. V diskusi byla vyzvednuta účelnost dobré výjezdové výbavy. Padlo i mnoho dalších námětů na obsah takového výjezdového kufříku a někteří účastníci hned na místě projevili zájem o sestavení výjezdové sady DEAT podle jejich vlastních požadavků a potřeb.

Instalace FTK

Forensic ToolKit (FTK verze 5) od společnosti AccessData přibyl v posledních letech k základnímu analytickému vybavení speciálních policejních pracovišť. Patří v současnosti k nejrozšířenějším nástrojům digitální forenzní analýzy ve světě a aktuálně už i u nás. Některé nesporné výhody tohoto nástroje jsou však vyvažovány určitými zvýšenými nároky jak na HW vybavení, tak i na způsob instalace a konfigurace pracovního prostředí labolatoří pro digitální forenzní analýzu. Nesprávnou konfigurací a instalací dochází dokonce k výraznému snižování funkčních vlasností a použitelnosti FTK5 v běžné praxi.

Naše vlastní zkušenosti z provozu a několikaleté ověřování a optimalizace konfigurace provozního prostředí pro optimální běh FTK5 byly předmětem další části dopoledního programu. Byly prezentovány jednotlivé způsoby provozní konfigurace ICT, od instalace na jené stanici až po optimalizaci na výkonné provozní prostředí. V rámci prezentace byly doporučeny ekonomicky a funkčně přijatelné konfigurace a poskytnuty i další praktické zkušenosti, jak instalovat a konfigurovat prostředí pro FTK5.

Přednáška o instalaci FTK5 vyvolala snad největší zájem účastníků. Svědčí to nejenom o tom, že bylo předáno hodně praktických zkušeností z provozu a ověřování, které určitě ušetří posluchačům mnoho hodin pokusů a omylů, ale i o tom, že nástroj FTK5 má mnoho zastánců a aktivních uživatelů, kteří chtějí jeho provoz ještě více optimalizovat. Nemalá část účastníků se také zajímala o nevyhnutný HW, aby mohli plánovat jeho pořízení v nejbližším období.

Problematika vhodného dimenzování a konfigurace infrastruktury pro efektivní provoz FTK5 byla jedním z nejvíce ceněných přínosů celé akce. Podrobněji se tomuto tématu věnujeme v samostaném článku "Atchitektura ICT pro efektivní provoz FTK5".

EnCase EnScript

EnCase Forensic od společnosti GuidanceSoftware je pravděpodobně asi nejrozšířenějším nástrojem

pro digitální forenzní analýzu. O práci s EnCase by se dalo určitě hovořit dlouze. Protože však je to aktuálně nejrozšířenější nástroj v rámci policejní praxe, krátká prezentace byla věnována jedné speciální funkcionalitě, která pravděpodobně není až tak často využívána v praxi. Jedná se použití scriptovacího jazyka EnScript. Pomocí EnScriptu lze relativně jednoduše vytvářet nové funkcionality nástroje EnCase nebo například vytvářet speciální procedury, které realizují běžné nebo často se opakující postupy.

Byly předvedeny základní kroky, které umožňují využít jak stávající procedury, které jsou napsány pomocí EnScriptu a dodávají se s instalací EnCase, tak použití procedur vytvořených třetími stranami. V závěru byly představeny kroky, které vedou k psaní vlastních programů - EnScriptů.

Aktuální informací je zpráva, že společností GuidanceSoftware byl uvolněn manuál ke skriptovacímu jazyku EnScript pro EnCase v7, který je volně ke stažení z adresy https://guidance-software.app.box.-com/s/eo6yrgylpg32wu4589n4.

O odpoledním programu

Odpolední blok byl věnován novinkám v oblasti digitální forenzní analýzy na našem trhu. Společnost Risk Analysis Consultants přivedla v roce 2014 na náš trh dva nové nástroje pro digitální forenzní analýzu. Jedná se o analytický nástroj Nuix Investigator společnosti NUIX a nástroj pro získávání dat z mobilních zařízení XRY a jejich následnou analýzu XAMN společnosti Micro Systemation AB.

NUIX Investigator

V odpoledním bloku byl nejdříve představen analytický nástroj Nuix Investigator. Podrobně byly představeny základní přednosti Nuixu oproti

konkurenčním produktům, které jsou realizovány zejména unikátním indexovacím enginem. Další výhodou je robustnost systému, která jej předurčuje ke zpracování velkých objemů dat a řeší tak jeden ze základních problémů konkurence - neschopnost analyzovat na cenově dostupných techologiích najednou objemy dat přesahující jednotky TB.

Nuix, narozdíl od konkurence, je schopen efektivně zapojit do analýzy mnoho procesorů v rámci jednoho stroje, dokonce i integrovat výpočetní výkon mnoha procesorových jader napříč mnoha počítači, a tím je schopen zpracovávat v akceptovatelných časových intervalech i případy o celkovém objemu mnoho desítek TB dat.

Nezanedbatelnou výhodou Nuixu je i promyšlený a intuitivní uživatelský interface a přehledná grafická interpretace nálezů a vzájemných vazeb analyzovaných dat. Zajímavou může být i výhodná cenová politika společnosti NUIX pro policejní účely.

XRY a XAMN

Odpoledním vzácným hostem Digital Forensic InfoDay byl zástupce společnosti Micro Systemation AB (MSAB), výrobce nástrojů pro získávání dat z mobilních zařízení a jejich analýzu, Jonas Andersson.

Jonas ve své více než dvouhodinové prezentaci podrobně seznámil účastníky s nástrojem XRY, který je speciálně navržen pro získávání dat z mobilních zařízení, mobilů, tabletů a dalších podobných zařízení. Samostanou částí jeho prezentace bylo také představení analytického nástroje XAMN, který analyzuje data získaná pomocí XRY a kromě jiných užitečných vlastností umožňuje vysledovat souvislosti a vazby v datech z různých analyzovaných zařízení.

Zajímavou částí jeho prezentace bylo také představení jejich zařízení KIOSK, které bylo vyvinuto speciálně pro jednoduché použití a základní analýzu dat z mobilních zařízení pro účely masového a rychlého použití a pro přehledovou analýzu bez speciálního zaškolení obsluhy.

Po prezentaci následovala neformální diskuse jak k představeným nástrojům společnosti MSAB, tak i k dalším obecnějším otázkám digitální forenzní analýzy.

Závěr

Rádi bychom poděkovali všem účastníkům za hojnou účast a podnětnou diskusi, ve které zaznělo mnoho užitečných námětů k dalšímu rozvoji naší práce a vývoji nástrojů. Všechny zájemce o prezentace z akce můžeme odkázat na webové stránky společnosti RAC, kde jsou prezentace zpřístupněny, viz odkaz: http://www.rac.cz/rac/homepage.nsf/CZ/pdfid2014-2

Listopadový RAC Digital Forensic InfoDay vol II byl organizován v rámci projektu Czech CyberCrime Centre of Excellence for training, research and education a s podporou Prevention of and Fight against Crime Programme of the European Union European Commission - Directorate-General Home Affairs

Školení v oblasti digitálních důkazů

Systém vzdělávání nelze nahradit dílčími vědomostmi

Ing. Marián Svetlík st.
svetlik@rac.cz
Soudní znalec v oboru Kriminalistika, kriminalistická počítačová expertíza, vedoucí Znaleckého ústavu společnosti Risk Analysis Consultants, s.r.o.

Anotace:

Znalecký ústav Risk Analysis Consultants, s.r.o. se systematicky věnuje nejenom výkonu znalecké činnosti, ale zaplňuje i mezeru, která u nás už dlouhou dobu existuje v oblasti vzdělávání. Článek popisuje aktuální aktivity v oblasti školení a představuje připravovaný ucelený systém vzdělávání specialistů v oblasti práce a analýzy digitálních stop a důkazů, jak pro privátní sféru, tak pro OČTŘ.

Úvod

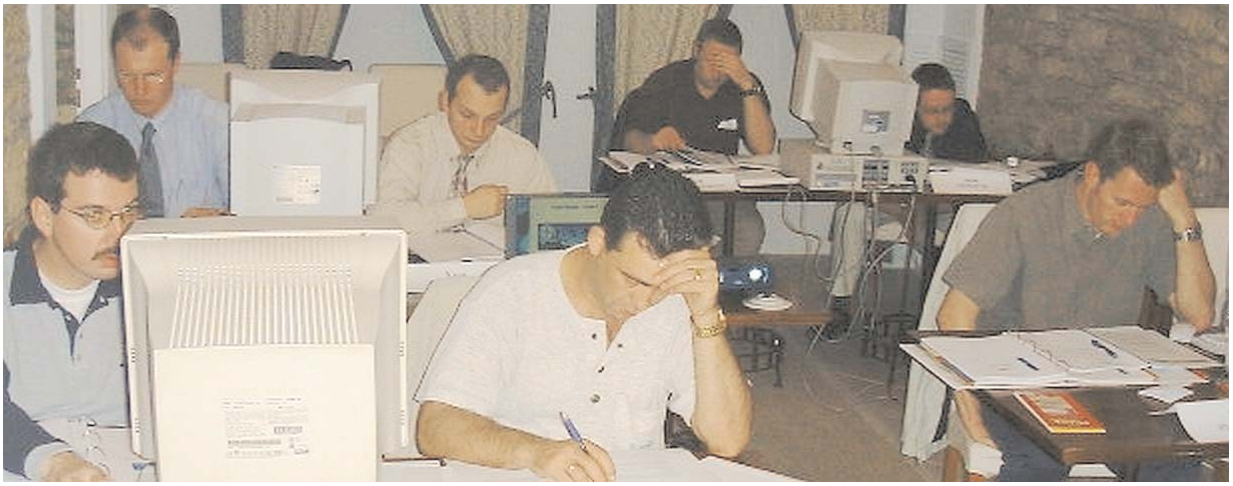
Znalecký ústav RAC dlouhodobě pracuje na přípravě a realizaci různých školení v oblasti digitální forenzní analýzy. Jsme prakticky jediní v ČR, kteří se vzdělávání v tak specifické oblasti věnují.

Ve standardní nabídce máme několik úvodních školení do digitální forenzní analýzy. Další, specifičtější školení, připravujeme většinou podle individuálních požadavků.

V minulosti jsme realizovali již mnoho speciálních školení různého specifického zaměření. Ať to už byla školení v rámci zvyšování profesní kvalifikace, speciální týdenní kurzy bezpečnostních techniků a specialistů interních vyšetřovacích týmů velkých společností, nebo jen cílené a krátkodobé kurzy na jednu speciální nebo dílčí problematiku digitální forenzní analýzy nebo v oblasti jiných specifických činností přímo či nepřímo souvisejících.

Zajišťování dat je klíčové

Vědomi si zásadní důležitosti procesu zajištění digitálních stop (jak je i na několika dalších místech tohoto čísla DFJ uvedeno), připravili jsme speciální kurz, který je zaměřen právě na tuto činnost.



Praxe ukazuje, že forenzně správně zajistit digitální stopy je dnes již nutností nejenom pro OČTŘ, ale kvalitně zajištěné digitální stopy hrají důležitou úlohu i při moha jiných (např. interních) procesech v privátní sféře.

Nezřídka je také nutné zajistit digitální stopy velice rychle a bohužel policejní procesy jsou na nutnost okamžitého zajištění dat příliš pomalé. Proto je snaha i soukromých společností tyto činnosti provádět a provádět je odborně na vysoké úrovni a speciálně k tomu proškoleným personálem.

Třídenní intenzivní školení "Forenzní zajišťování digitálních dat" s množstvím praktických cvičení a certifikační zkouškou na závěr je výsledkem požadavků zejména (možná zdánlivě i paradoxně) privátní sféry.

Odborné úrovni tohoto školení jsme věnovali velkou pozornost. Nejenom technické vědomosti a zručnost v ovládání speciálních zařízení a programového vybavení, ale také procesní a základní právní souvislosti jsou obsahem tohoto školení.

Náročný tříhodinový závěrečný test, navíc doplněný o praktickou úlohu, kterou absolvent musí splnit do jedné hodiny, neprobíhá bezprostředně po absolvování kurzu. My požadujeme, aby získané vědomosti měli u absolventů trvalý charakter. Proto certifikační zkouška probíhá s odstupem tří až devíti měsíců od ukončení kurzu a praktický úkol, který je součástí zkoušky, není ani jeden z těch, které byly v rámci kurzu demonstrovány a řešeny. Absolventi tak získají dostatek času ověřit si v praxi vědomosti, které získali v průběhu školení. S odstupem času se při zkoušce ukáže, co ze školení si zapamatovali, jaké praktické dovednosti si osvojili a jak jsou to všechno schopni aplikovat na, pro ně zcela nové, reálné situaci. Za získání osmdesáti bodů ze sta v testu a za správně provedený praktický úkol získá absolvent certifikaci "Cetrified Digital Forensic Acquisition Expert (CDFAE)".

Systémový přístup

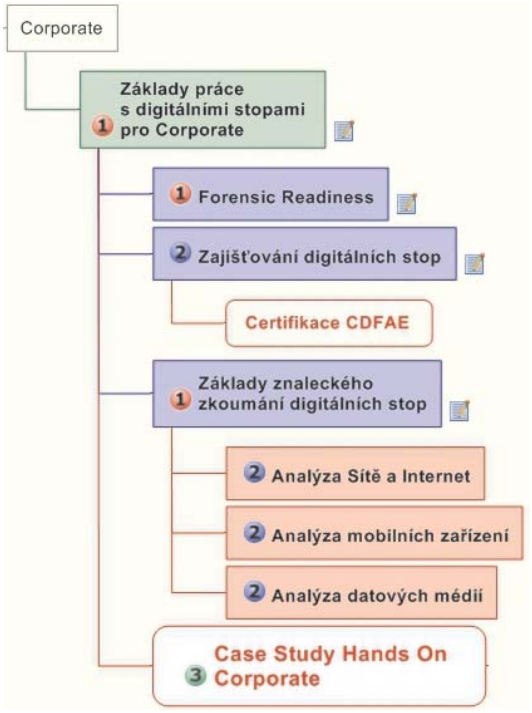
Jedna specifická problematika a speciální kvalifikace však nestačí. Jistě není nutné zdůrazňovat, že problematika digitálních stop a důkazů je mnohem širší.

Komplexní vzdělání v této oblasti bylo cílem i naší další práce. Aktuálně finalizujeme celou strukturu vzdělávacího procesu pro oblast práce s digitálními stopami a důkazy.

Struktura komplexu školení je rozdělena do čtyř základních kvalifikačních rovin a pro dvě klíčové skupiny posluchačů.

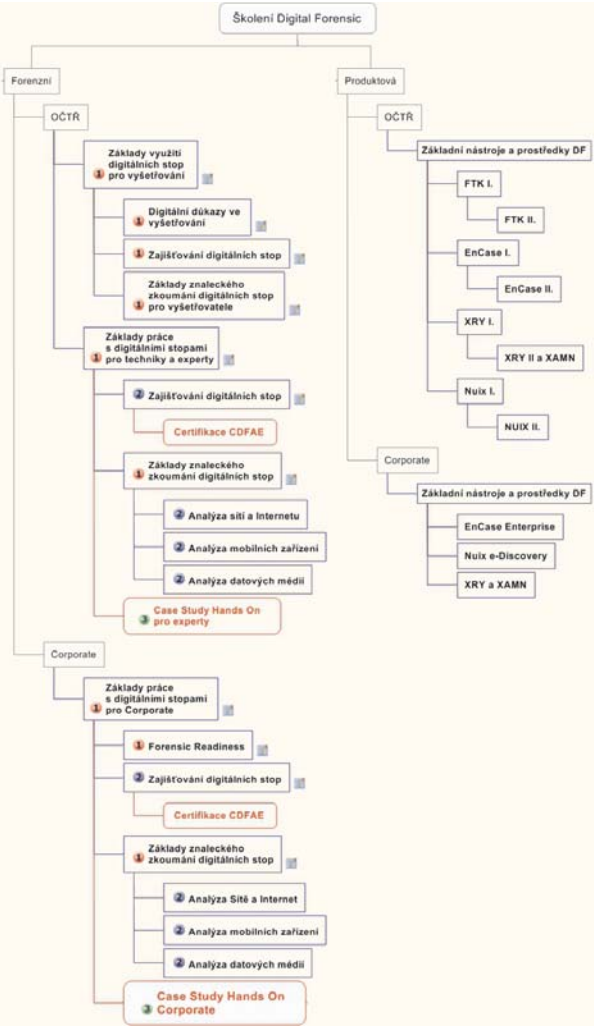
Z pohledu náročnosti se jedná o následující úrovně:
- Přehledový úvod do problematiky
- Základní vědomosti
- Pokročilé vědomosti
- Speciální vědomosti

Vzhledem k rozdílnostem a specifikám práce jsou kurzy dále rozděleny pro:
- OČTŘ a obdobné státní instituce (zaměření na trestní řízení)
- Privátní sféra (zaměření na interní šetření a šetření bezpečnostních incidentů)



Příkladem rozdílného přístupu k oběma skupinám posluchačů může být zaměření speciální skupiny školení - produktových školení. Pro OČTŘ je předmětem školení produkt EnCase Forensic (speciálně určen pro forenzní zkoumání), pro privátní sféru je náplní ekvivalentního kurzu produkt EnCase Enterprise (speciálně určen pro reakce na bezpečnostní incidenty v organizaci a jejich šetření).

Pro ilustraci struktury školení podle náročnosti lze uvést schéma školení - Digitální stopy a důkazy pro privátní sféru (viz schema na předchozí stránce - stupeň 1 - zelená, 2 - modrá, 3 - červená, 4 - bílá) a zatím kompletní strukturu ilustruje následující diagram vpravo.



Závěr

Celkově jsme již připravili v této struktuře bezmála desítku školení a dalších přibližně deset je v procesu přípravy. V průběhu roku 2015 budou vypsány termíny úvodních kurzů a podle aktuální situace budou přibývat další. Kurzy pro OČTŘ budou poskytovány ve speciálně výhodných cenových relacích.

Další informace o systému vzdělávání v oblasti práce s digitálními stopami a důkazy a podmínkách účasti získáte na adrese zu@rac.cz a budou průběžně zveřejňovány na webu www.rac.cz.

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.

Tableau TD2u Forensic Duplicator

Nový TD2u duplikátor s rozhraními

- USB 3.0
- SATA
- SAS
- IDE

Každý TD2u KIT obsahuje

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

Podpora množství rozhraní

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

Nabitý funkcemi

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

Prodej a podporu v ČR a SR zajišťuje:
Risk Analysis Consultants, s.r.o.
Španělská 2
Praha 2
zu@rac.cz
www.rac.cz

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