České vysoké učení technické v Praze
Fakulta informačních technologií
Katedra aplikované matematiky

Semestrální práce

Forenzní analýza v IT

Bc. Ladislav Martínek

3. listopadu 2019

Abstrakt

Tato práce popisuje forenzní technologie v informačních technologiích a především potom forenzní analýzu digitálních dat. V první kapitole je popsána digitální forenzní analýza, je rozdělena na jednolivé typy, jsou popsány jednotlivé kroky a co je předmětem forenzní analýzy. Dále jsou popsány také techniky, omezení a rizika, která jsou při digitální forenzní analýze aktuální. Na závěr první kapitoly jsem popsal základní právní aspekty forenzní analýzy. V další kapitole jsem popsal nástroje forenzní analýzy a vyjmenoval některé softwarové a hardwarové produkty pro provádění forenzní analýzy. Na závěr jsem se zmínil o protikladu a to o anti-forenzní analýze, která není přímo věda, ale při provádění forenzní analýzy je důležité tyto kroky znát.

Klíčová slova Forenzní analýza v IT, digitaní forenzní analýza , informační bezpečnost

Abstract

This thesis describes forensic analysis in information technologies and mainly digital forensic science. The first chapter describes the digital forensic investigation, it is divided into individual types; the steps and the subject of forensic analysis are described. Furthermore, the techniques, limitations, risks that are current in digital forensic analysis are described. At the end of the first chapter, I described the fundamental legal aspects of forensic analysis. In the next section, I described the tools of forensic investigation and listed some software and hardware products for performing forensic analysis. At the end of the text, I mentioned the contradiction, the anti-forensic analysis. It is not directly science, but when do the forensic investigation, it is essential to know the steps of anti-forensic analysis.

Keywords Forensic analysis in IT, digital forensic analysis, information security

Obsah

Úvod

V dnešní době je s digitálními zařízenímy spojena většina našich každodenních činností, ať už to jsou počítače, mobilní telefony, ale v dnešní době i hodinky nebo žárovky, které například ovládáme přes svůj mobilní telefon, a také další domácí spotřebiče. Můžeme například platit bezhotovostně ať už pomocí karty nebo chytrých hodinek. Všechny tyto digitální technologie jsou v našem životě zastoupeny čím dál větší měrou a nahrazují staré postupy, které postupy mnohdy velmi zjednoduší.

Všechna tyto digitální zařízení se však mohou stát terčem útoku. Útoky na digitální systémy se stavájí každodenní rutinou a je tedy nutné umět takové útoky odhalit a bránit se proti nim. Počet útoků na tyto systémy narůstá každým rokem. Nemusí se přímo jednat jen o útoky proti počítačům, ale například i zneužití digitální techniky k páchání trestného činu. Například počítače v bytě, kde proběhla vražda (kumunikace mezi vrahem a obětí na sociální síti).

Pokud se stane nějaký fyzický trestný čin, bude místo činu zkoumáno oprávněnými osobami. Cílem ohledání místa činu je rekonstrukce události a nalezení viníka. Důležitou součástí procesu je sběr důkazů, které představují třeba otisky prstů. Jinak tomu není ani v případě digitálních systémů, kde je nutné zajistit důkazy, například data po škodlivém softwaru. Tyto data jsou velice nestálá a je nutné s nimi náležitě pracovat.

Vědou, která se tímto zabývá je forenzní analýza digitálních dat (angl. digital forensics). V této práci tuto oblast popíši a pokusím se příblížit některé metody, nástroje a postupy. Volně řečeno jde v této oblasti o analýzu dat s cílem zjistit co, kdy, kde a jak se stalo.

Kapitola 1

Forenzní analýza

Forenzní analýza je pojem pro analýzu a vyšetřování, které se provádí za účelem zdokumentování události (nejčastěji v oblasti bezpečnosti). Dále zjištění jejich důvodů, průběhu a hledání viníků a objektivních důkazů, které by případné viníky mohli usvědčit (u soudu)[13].

V knize [4] je digitální forenzní analýza definována jako soubor technik a nástrojů používaných pro hledání důkazů na počítači, které mohou být použity v uživatelův neprospěch. Důkazy nemusejí přímo souviset s počítačovou kriminalitou. Digitalní forenzní analýzu lze aplikovat například při vyšetřování trestné činnosti, vydírání, krádeží, podvodů a padělání.

Forenzní analýza v informačních technologiích neboli také forenzní analýza digitální dat (pokud bude dále v textu zmíněna forenzní analýza půjde už pouze jen konkrétně o forenzní analýzu digitální dat) se zabývá výše zmíněnými problémy s využitím digitální dat, jak je popsáno v [11]. Oproti definici výše se zde zmiňují téměř libovolná digitální data a není omezena pouze na počítač. Tato digitální data jsou pak většinou uložena na disku v počítači, ale obecně to může být libovolné digitální médium.

Forenzní analýza se využívá napříč velkým množstvím oborů, například v kriminalistice, interním vyšetřovaní ve firmě, ale může být využita například i při obnově dat nebo občanskoprávním řízení.

Forenzní věda byla vytvořena za účelem řešení specifických potřeb donucovacích orgánů, aby se co nejlépe využila tato nová forma elektronických důkazů, které mohou dopomoci objasntit a vyřešit daný případ. Postupy v digitalní forenzní analýze jsou řízeny směrnicemi a postupy, které je nutné dodržovat.

Jak se píše v [13], počítačová forenzní věda je ve svém jádru odlišná od většiny tradičních forenzních disciplín. Počítačový materiál, který je zkoumán, a techniky, které má provádějící technik k dispozici, jsou většinou produkty soukromého sektoru. Kromě toho, na rozdíl od tradičních forenzních analýz, je běžně vyžadováno provádění počítačových zkoušek prakticky na jakémkoli fyzickém místě, nejen v kontrolovaném laboratorním prostředí. Obecně není

datová forenzní analýza prostorově náročná, ale může být náchylná na drobné nepřesnosti, kterým je nutné se vyvarovat, aby výsledky mohli být použitelné. Digitální forenzí analýza většinou nevytváří přímé závěry, ale poskytuje přímé informace, kterými bývají závěry podloženy.

1.1 Kroky digitální forenzní analýzy

Mezi hlavní kroky forenzní analýzi podle [6] můžeme považovat kroky: zabavení, získávání, validace a identifikace, analýza a vykazování výsledků, které potom podrobněji popíši v následujících sekcích.

1.1.1 Zabavení

Krok zabavení zahrnuje označení prvků, které budou použity v pozdějších procesech. Jsou pořizovány fotografie scény a poznámky. Například počítač je nutné zapečetit, aby nemohlo být napadeno to, že byl obsah modifikován. V [16] je zmíněna zajímavá otázka, na kterou je třeba v tuto fázi odpovědět: Vytáhnout zástrčku ze sítě nebo ne. Ponechání systému online během pokračování může útočníka upozornit, což mu umožní vymazat stopy útoku a zničit důkazy. Útočník může také nechat přepínač, který zničí důkazy, jakmile se systém přepne do režimu offline. Za takových okolností může být nutné nebo vhodné shromáždit důkazy ze systému, když je spuštěn. Pro přijetí jakéhokoliv postupu je nutné kroky vysvětlit. Cílem fáze je zajištění a uchování důkazů.

Jak se píše v [14], není důležité, kde se přesně nachází, ale důležité jsou důkazy, které lze získat. Počítač může být součástí nějakého prostředí, které zahrnuje i vzdálené brány firewall, inteligentní smerovače a rozbočovače, poskytovatele internetu, bezdrátová zařízení, atd... Je nutné shromáždit všechna tyto data a hledat mezi nimi korelace. I tato data mohou být pro hledání důkazů klíčová.

1.1.2 Získávání

Po první fázi je přistoupeno k získávání dat. Součástí této fáze je většinou i fáze duplikace, kdy je kopie dat bezpečně uložena. Data musí být získána beze změny nebo poškození zdroje, který má být analyzován později. Nezákoné zabavení nebo nevhodný postup může ovlivnit platnost důkazů u soudu. Z tohoto důvodu by metody získávání důkazů měly být forenzně spolehlivé a ověřitelné. Získavání může být fyzické nebo logické. Při fyzickém získávání je bitový obraz snímán z fyzického paměťového média, zatímco v logickém získávání je logický obraz zachycen z paměťového média. V obou případech je třeba použít writeblockery, aby se zabránilo úpravě dat na disku. Podle [16] se vždy doporučuje zahájit snímání od nejmenších dat po ta největší data. Pořadí důležitostí je pak:

1. Registry, cache
2. Stav sítě (mezipaměť ARP a směrovací tabulka)
3. Běžící procesy
4. Moduly a statistiky jádra
5. Hlavní paměť
6. Dočasné soubory na disku

1.1.3 Validace a identifikace

Data jsou tedy většinou duplikována na jiné médium. Duplicitní obrázek musí být ověřen jestli je totožný se zdrojem. Například porovnáním hodnoty hash získaného obrazu nebo kopie a původních dat médií nebo kontrolním součtem.

Podle [6] je postup následující: Technici opakují proces identifikace pro každou položku v seznamu extrahovaných dat. Nejprve určují, o jaký typ položky jde. Pokud pro forenzní žádost není relevantní, jednoduše ji označí jako zpracovanou a přesunou se dále. Stejně jako ve fyzickém vyhledávání, pokud technik narazí na věc, která je usvědčující, ale mimo rozsah původního příkazu k prohlídce, doporučuje se, aby examinátor okamžitě zastavil veškerou činnost, informoval příslušné osoby, včetně žadatele, a počkal pro další pokyny. Například orgány činné v trestním řízení by mohly zabavit počítač jako důkaz o daňových podvodech, ale technik může najít obrázek z jiné trestné činnosti. Důležité je se pokusit rozšířit pravomoce pro další zkoumání.

Dále také technik může data, která ukazují na zcela nový potenciální zdroj dat. Například mohou najít nový e-mailový účet. V tomto okamžiku je vhodné, aby zkoušející informovali žadatele o svých počátečních zjištěních.

1.1.4 Analýza

Ve fázi analýzy připojí technik všechny zjištěné informace a vykreslí kompletní obrázek pro žadatele [6]. U každé položky v seznamu relevantních údajů technici odpovídají na otázky zmíněné v úvodu a to co, kdy, kde, kdo a jak. Je zde snaha o co nejpodrobnější vysvětlení.

Zkoušející často dokážou vytvořit nejcennější analýzu tím, že se podívají na to, kdy se něco stalo, a vytvářejí časovou osu, která vypráví souvislý příběh [6]. U každého souboru nebo informace je snaha o zasazení na osu tedy o zjištění, kdy byla vytvořena, zpřístupněna, změněna, přijata, odeslána, zobrazena, odstraněna a spuštěna.

Během tohoto postupu by měly být dodržovány vhodné metodiky a standardy (popsané v následující části)[16]. Vyšetřovatel by měl prozkoumat získanou kopii nebo obraz média, nikdy ne originálního médium. Na rozdíl od

fáze zabavení a identifikace vyžaduje fáze analýzy odborníky. Technici musí mít řádné znalosti a musí být řádně vyškoleni.

„*K vyhledávání konkrétních důkazů se používají dva druhy analýz. První je analýza fyzická, která má za úkol najít například nějaký řetězec z obsahu disku a to v rámci všech sektorů disku, který berete jako celek. Logická analýza spočívá v analýze jednotlivých souborů. Mezi Logickou patří například soubory v souborovém systému.*“[11] Podle toho se tato analýza se bude lišit pro různé souborové systémy (Windows, Linux).

1.1.5 Vykazování výsledků

Na závěr je nutné vytvořit zprávu s výsledky. Ve zprávě musí být popsány všechny kroky provedené během šetření. Obsahuje zprávy o předchozích krocích a především získaní dat, jejich ověření a analýzu. Je nutné uvést všechny nástroje a hardwarové prvky. Celý postup musí být opakovatelný nezávislou osobou a také musí být ověřitelná nezaujatost, nestrannost a nezávislost. Výsledky musí jasně prezentovatelné i osobám mimo daný obor.

1.2 Typy forenzní analýzy

Dále můžeme forenzní analýzu rozdělit na nasledující typy, tak jak je uvedeno v [18]. V jiné literatuře je možné narazit i na jiné rozdělení, které je bývají většinou stručnější.

1.2.1 Počítačová forenzní analýza

Identifikace, uchování, sběr, analýza a podávání zpráv o důkazech zjištěných na počítačích, notebookech a úložných médiích na podporu vyšetřování a soudních řízení.

1.2.2 Sítová forenzní analýzas

Monitoring, zachytávání a ukládání provozu na síti. Může sloužit k odvrácení útoků. Sledování abnormálního provozu na síti je jeden z prvních ukazatelů na problém. Analýza této vrstvy zahrnuje analýzu síťových paketů a jednotlivýh síťových protokolů[5].

1.2.3 Forenzní analýza mobilních telefonů

Získávání elektronických důkazů z mobilních telefonů, smartphonů, SIM karet, PDA, zařízení GPS, tabletů a herních konzolí.

1.2.4 Forenzní analýza obrázků

Extrakce a analýza digitálně pořízených fotografických obrazů za účelem ověření jejich pravosti obnovením metadat obrazového souboru s cílem zjistit jeho historii [18].

1.2.5 Digitální analýza videa/audia

Sběr, analýza a hodnocení zvukových a obrazových záznamů. Věda je zavedením pravosti o tom, zda je záznam originální a zda s ním bylo manipulováno, ať už úmyslně nebo náhodně.

1.2.6 Analýza operační paměti

Získání a rekonstrukce dat získaných z operační paměti RAM. Vrstva, která převádí bajty pamětového média na procesy a systémová data a oblast zahrnuje identifikaci probíhajícího kódu a získaní citlivých dat, která nebyla uložena jinde [5].

1.3 Předmět forenzní analýzy

Předmětem forenzní analýzy jsou nejčastěji data, která se nacházení na mediích v podobě souborů a můžou být označovaná jako platná data. Dále data nelatná, které můžou představovat smazané soubory, fragmenty dat (smazané soubory, které byly částěčně přepsány). Dále to pak můžou představovat data v operační pamětí, která jsou nestálá a při vypnutí počítače tyto data zanikají. Data představují kontext programů, bežící kód a proměné. Záznamy běžících aplikací v podobě logů. Aby analýza digitálních dat byla forenzní analýzou, musí splňovat body udedené v kapitole 2 a také nesmí porušit žádné zákony.

1.4 Techniky

Během forenzní analýzy je možné využít některé techniky. Zde jsou ty nejdůležitější podle [2]:

- **Cross-drive analýza** - Metoda je uvedená v publikaci [10]. Cross-drive analýza je forenzní technika, která se snaží vyhledávat informace najednou na více mediích. Tato metoda je velice nová a může přispět k odhalení nových informací, než při analýze každého disku zvlášť.

- **Analýza za běhu** - Technika analýzy běžícího systému pomocí nástrojů systémových administrátorů. Tato technika je důležitá především k získaní dat z operační paměti, dále také pokud je cílový systém šifrován,

může být využit k získaní šifrovacích klíčů, aby disky a data byla použítelná i po vypnutí systému. Může být také obraz disku vytvořen ještě před vypnutím systému.

- **Smazané soubory** - Nejběžnější technikou používanou v počítačové forenzní analýze je obnova smazaných dat. Moderní software mají svoje vlastní nástroje pro obnovu smazaných dat. Data v operačních systémech nejsou při odstarnění fyzicky odstraněna, protože tento proces není fyzicky možný. Data je možné pouze přepisovat (například přepsat nulami nebo náhodnými daty). Tento postup je ale časově náročný, proto není využívaný. Vyšetřovatelům toto umožňuje rekonstruovat data z fyzických diskových sektorů. Pro rekonstrukci smazaných dat uvnitř diskového obrazu se používá tzv. „File carving“, který hledá hlavičky známých souborů [2].

- **Stochastická forenzní analýza** - Je metoda využívající stochastické vlastnosti v operačním systému. Využití pravděpodobnosti a zákonů velkých čísel. Tato metoda se nejčastěji využívá pro vyšetřování krádeže dat.

- **Steganografie** - Jedna z technik využívaná pro ukrývání dat, je ukrytí za pomoci steganografie. S její pomocí se dají data schovat v jiném souboru. Soubor může představovat libovolný formát. Můžem takto ukrýt například důležitou zprávu nebo šifry. Počítačoví forenzní profesionálové mohou odhalit pozměnění originálního obrázku pomocí porovnání jeho haše s hashem originálního obrázku, který ale nemusí být k dispozici. Uložená data můžou být uložena v obrázku, který byl náhodně generován. Vizuálně mohou být obrázky stejné, ale hash se může lišit, protože hashovací funkce by se měla chovat jako náhodné orákulum, které přidělí hash nějaké libovolně dlouhé sekvenci. Tedy při změně jednoho bitu se hash změní radíkálně na libovolnou jnou hodnotu.

1.5 Omezení

Digitalni forenzní analýza se velice často dotýká velmi citlivých dat. Z tohoto faktu zde můžou plynout určitá omezení. Na zkoumání digitálních mediích se vztahují zákony a předpisy. Takové jsou definovány mezinárodně, ale i vnitrostátně. Nejčastější omezení může být proti monitorování sítě a čtení komunikace jako třetí strana. V zákoně je také přesně předepsáno, co může být předmětem zabavení. „*Právo jednotlivce na soukromí, je jednou z oblastí digitální forenzní vědy, která je soudem stále do značné míry nerozhodnuta*“[1]. Například v Americe je zákon na ochranu osobních údajů v elektronických komunikací velice silný a omezuje schopnosti vyšetřovatelů získávat důkazy. Zde je rozlišováno mezí přenášenou a uloženou komunikací. Sledování přenášené

komunikace je témeř většinou silný zásah do soukromí. Legislativa je jedním z omezeních, se kterým se forenzní technik musí potýkat. Dalším omezením může být například nedostatečný výkon současných počítačů. Výkon nemusí stačit například k prolamování šifer nebo k analýze v reálném čase.

1.6 Rizika

Další částí jsou rizika, které mohou potkat forenzní techniky při práci. Při práci s digitálními daty nelze rizika nikdy vyloučit, ale pokud nějaký problém nastane tak to většinou zkončí nepoužitelnou analýzou. Avšak i při dodržování všech bezpečnostních pravidel není možné úplně vyloučit, je pouze možné tyto rizika snížit na minimum. Problémy můžou být způsobeny vadou techniky, pouruchou zkoumaného zařízení nebo i zvolenou technikou. Může například selhat zkoumaný disk při vytváření bitové kopie. Dalším problémem mohou být rizika, která vzniknou lidskou chybou. Technik například nedodrží přesné postupy a chce si práci usnadnit. Problémy a chyby způsobené lidským faktorem lze například ještě rozdělit na úmyslné, neúmyslné nebo z nedbalosti. V práci [12] jsou uvedena a zmíněna především následující rizika. Většině těchto rizik lze však předcházet dodržováním doporučení, předpisů, zákonů a obecných bezpečnostních pravidel:

- Nezajištění všech digitálních stop
- Neodborné zajištění digitálních stop
- Nesprávné zabalení a ověření digitálních stop
- Nesprávná, nebo neúplná dokumentace
- Znehodnocení zajištěných stop
- Úmyslné zničení dat
- Nemožnost rozšifrovat data

1.7 Právní aspekty

Aby mohla být analýza dat považována za digitální forenzní analýzu a její výsledky použity u soudu jako důkazy, což je cíl digitální forenzní analýzy, musí splňovat konkrétní vlastnosti. Pokud bude analýza dat splňovat tyto vlastnosti je veliká šánce, že její výsledky budou důležitým důkazem u soudu. Kromě nepodjatosti nejsou tyto vlastnosti ukotveny v zákoně a jedná se pouze o doporučení přejatá ze zahraničí. Podle [17] jsou to následující aspekty:

- **Legalita** - Všechny informace (záznamy hovorů, přenos na síti) nebo předměty (notebooky, flesh disky), které jsou využity v digitální forenzní analýze musí být získány legálním způsobem. Získávání dat se musí řídit zákony země, kde je prováděno. Porušním může být například ukradený flesh disk nebo například nelegální nahrávka telefonu.

- **Integrita** - Musí být jednoznačné, co je s daty prováděno, a že nemohlo nebo nemůže dojít k manipulaci. Podle článku [17] porušením může být například jakýkoliv zápis na zkoumaný disk, protože mohou být přepsány sektory, na kterém se mohou nacházet data. V publikaci je uveden konkrétní příklad, ale obecně je už témeř povinností k získaný datům přistupovat pomocí blokátorů zápisu, které jsou popsány v kapitole 2.1.2.

- **Opakovatelnost** - Můsí být použitý takový způsob analýzy, aby byly všechny experimenty opakovatelné. K tomuto je možné využít další hardwarové zařízení a to duplikátor, který je popsán v kapitole 2.1.1. Práce je prováděna na kopii dat a experiment může být posouzen ekvivaletními metodami nebo zopakován stejným postupem. Porušením opět může být přiklad nahoře, tedy že byla pozměněna původní data a nelze již experimenty opakovat. Podle [17] může být porušením například i pokud se mají prozkoumat videozáznamy jestli jsou totožné a technik použije monitor vysokého rozlišení a bude oba videozaznamy pouštět a posuzovat. Je nutné použít objektivní metodu.

- **Nepodjatos** - Nezávislost zkoumaného objektu na subjektu provadějící forenzní analýzu. Tady to může být například pokud technik, který instaloval server poté bude dělat forenzní analýzu nad útokem, který byl na server provedený. I když instalace byla na základě smlouvy o dílo a zkoumání útoku se řídí trestním právem.

- **Dostatečná dokumentace** - Každou forenzní analýzu musí doprovázet podrobná dokumentace, ze které jsou jasné všechny tyto body a celý postup lze podle ní zopakovat. Dále v ní musí být specifikovány závěry, které z forenzní analýzy plynou. Z nedostatečné dokumentace může být celá analýza označena za neplatnou a tedy i důkazy, které by jinak mohli obžalovaného usvědčit.

Kapitola 2

Nástroje digitální forenzní analýzy

Ve forenzní analýze je používáno mnoho nástrojů, které proces usnadňují a pomáhají předejít problémům. Tyto nástroje můžeme rozdělit mezi hardwarové (většinou fyziká krabička) nebo sofwarové (program).

Dále tu na každý takový nástroj máme podle [3] následující požadavky:

- **Použitelnost** - Pro řešení komplexního problému je nutné, aby nástroje poskytovaly dostatečnou vrstvu abstrakce. Data na nejnižším formátu (sektory na disku) je velice těžké analyzovat. Minimálně musí poskytovat abstraktní vrstvy, které jsou uvedeny jako hraniční vrstvy v [5]. Zároveň je nutné, aby nástroj prezentoval data v jasném a přehledném formátu, aby vyšetřovatel mohl data intepretovat správně. [5]

- **Komplexnost** - Musí být schopen zpracovat veškerá data a identifikovat ty důležitá ve všech směrech.

- **Presnost** - Výstup musí být přesný a ověřitelný. Musí poskytovat zpětnou vazbu o míře jistoty (angl. confidence).

- **Determiničnost** - Nástroj musí produkovat stejné výsledky pokud jsou poskytnuta stejná data a stejná sada pravidel.

- **Ověřitelnost** - Výstupy musí být vzhledem k datů ověřitelná. Ověření je prováděno ručně nebo může být provedeno pomocí druhého nástroje.

Další doporučení pro nástroje je read-only (původní data vůbec nemodifikují). Data mohou být snadno zkopírovatelná, sice toto není nutnost, ale pro budoucí verifikaci výsledků je to žádoucí a kopie dat bude vyžadována.

2.1 Hardware

Pro digitální forenzní analýzu existuje také přímo specializovaný hardware. Jde o fyzická zařízení, které pomáhají při forenzní analýze a umožnují zabránit ztrátě dat a i znehodnocení takové analýzy. Vybral jsem dva prvky, které mi přišli při forenzní analýze nejdůležitější. Jsou to duplikátory a blokátory zápisu (angl. write blockers).

2.1.1 Duplikátory

Informace o duplikátorech čerpány z [9]. Duplikátory slouží k vytvoření kompletní kopiích pevných disků, paměťových karet nebo flesh disků. Dále se může jednat o duplikátory na nějakém rozhraní například na ethernetu, kdy může být přesně sledován sítový provoz do a z daného počítače.

2.1.2 Blokátory zápisu

Blokátor zápisu je jakýkoliv nástroj, který umožnuje přístup k zařízení pro ukládání dat pouze v řežimu čtení, tak že není ohrožena integrita datového uložiště [7]. Blokátory fungují tak, že filtrují I/O operace a ty instrukce, které by měli něco zapsat na médium tak zahazují. Je důležité, aby žádná část disku nebyla změněna. Tento typ je také součástí programů popsaných dále. Nemusí se tedy jednat pouze o fyzické zařízení, kde je na blokování speciální čip, ale i o součást programu.

2.2 Software

Téměř veškeré postupy forenzní analýzy jsou stadardizovány a pro provádění forenzní analýzy existuje mnoho programů, které jsou vytvořeny podle těchto standardů. Nástroje pomáhají se vyvarovat chybám, které by mohli výsledky znehodnotit tak, že by výsledky forenzní analýzy nebyly použitelné u soudu. Informace o existujícím softwaru jsem čerpal z [15].

První nástroj je od firmy AccessData. Forensic Toolkit FTK 7 je uznáván jako světový standard pro forenzní analýzu. Tato platforma představuje špičku v oboru analýzy digitálních dat, dešifrování, lámání hesel, a to všechno v intuitivním a přizpůsobitelném rozhraní. Nástroj také umožnuje pracovat s velkými objemy dat, díky distribuované databázové struktuře.

Dalším nástrojem je například Belkasoft Evidence Center 2019 od firmy Belkasoft. Program umožňuje forenznímu expertovi snadno prohledávat, analyzovat, uchovávat a sdílet digitální důkazy zajištěné na paměťových médiích nebo v operační paměti počítače. Nástroj dokáže zajistit důkazy z mnoha zdrojů, jako jsou pevné disky, obrazy paměti, zálohy iOS, Androidu či BlackBerry, nebo obrazy z UFED, JTAG nebo chip-off analýzy [15].

Dalším nástrojem je třeba EnCase Forensic 8 od Guidance Software/-OpenText. Nástroje nejsou levné, ale když vezmeme v úvahu, že pracujeme s daty, která tuto hodnotu mnohdy i převýší, tak se vyplatí investice do nástroje, který pomůže předejít chybám a usnadní digitální forenzní analýzu.

Kapitola 3

Anti-forenzní analýza

Anti-forenzní analýza je soubor technik používaných jako protiopatření k digitální forenzní analýze. V práci jsem se rozhodl toto zmínit, protože znalost těchto technik je určitě důležitá i pro forenzní techniky a naopak. Podle [8] jde rozdělit do následujících kategorií.

- **Schovávání dat** - Nemusí se jednat vždy přímo o snahu, aby data nebyla viděť nebo nebyla na místě kde jsou hledána. Typicky skryté oddíly disku, chybné sektory, skryté složky. Další možností, kdy data jsou viditelná ale nečitelná je šifrování. Zašifrování dat dostatečně silným klíčem je téměř neprolomitelné. Další možností může být například steganografie. Jedná se o ukrytí zprávy. Například využítím nějakého kanálu v obrázku.
- **Vymazání artefaktů** - Zde je jedná například o důkladné smazání prázdného disku. Klasické odstranění souboru nevymaže data z disku fyzicky.
- **Nástrahy a zmatení** - Kde jsou data uložena. Trojské koně, zombii účty nebo například úmyslná záměna informací.
- **Útoky proti nástrojům pro forenzní analýzu** - Jak je zmíněno v [8]. Toto je relativně nová možnost. Je to zapříčeněno standardizací forenzní analýzy, kdy je znám přesný postup, který je prováděn softwarem. Závislost na forenzním softwaru velmi ohrožuje zkoumaná data, forenzní software může být napaden a ovlivněn tak, aby stopu například zahladil.

Závěr

V práci jsem se zabýval forenzní analýzou v IT. Konkrétněji jsem se věnoval forenzní analýze digitální dat, která je čím dál více popularnější tím jak narůstá používání informačních technologií. V první části práce jsem popsal digitální forenzní analýzu. Uvedl jsem kroky digitální forenzní analýzi od zabavení, získávání dat až po tvorbu dokumentace, která je v práci zmíněna několikrát a jedná se o velmi důležitý krok ve forenzní analýze, protože forenzní analýza slouží k hledání důkazů, které je možné použít u soudu a její postup a výsledky musejí být jasně a srozumitelně popsány.

Dále jsem popsal typy forenzní analýzy, tedy na jaké podkategorie lze digitální forenzní analýzu dělit. Dále také co je předmětem forenzní analýzy a jaké jsou techniky získávání dat. V dalších podkapitolách jsem se pověnoval omezením, rizikům a prvním aspektům jako jsou legalita, integrita, opakovatelnost, nepodjatost a dokumentace.

Další kapitolu jsem věnoval nástrojům forenzní analýzy a to jak softwarovým tak hardwarovým. V poslední kapitole jsem jen zmínil anti-forenzní analýzu, která stojí na opačném konci, ale o jejích technikách je dobré vědět, aby mohla být forenzní analýza učinější.

Forenzní analýza digitálních dat spojuje velmi široký okruh témat jak je patrné z textu. K provádění datové forenzní anaýzy je nutné mít znalosti ze síťového provozu, hardwaru a jeho chovaní na okolní podněty. Dále také velké škály programů. Bez daných znalostí nejsme schopni provést analýzu tak aby byl výsledek věrohodný a použitelný. V nejhorším případě by to vedlo ke zničení důkazů.

Obor digitální forenzní analýzy je velice obsáhlý a je možné ho dělit na plno částí, například podle popsaných kapitol. O každé kapitole by mohla být napsána přinejmenších stejná práce. Pro více informací doporučuji citovanou literaturu.

Literatura

[1] Digital forensics. [online], [cit. 2019-10-27], Poslední aktualizace 18 September 2019, at 12:03 (UTC). Dostupné z: https://en.wikipedia.org/wiki/Digital_forensics

[2] Počítačová forenzní věda. [online], [cit. 2019-10-27], Poslední aktualizace 7. 10. 2019 v 22:58. Dostupné z: https://cs.wikipedia.org/wiki/Počítačová_forenzní_věda

[3] Brian Carrier: Defining Digital Forensic Examination and Analysis Tools. [online], [cit. 2019-10-27]. Dostupné z: https://dfrws.org/sites/default/files/session-files/pres-defining_digital_forensic_examination_and_analysis_tools.pdf

[4] Caloyannides, M. A.: *Computer forensics and privacy*. 2001, ISBN 15-805-3283-7.

[5] Carrier, B.; aj.: Defining digital forensic examination and analysis tools using abstraction layers. *International Journal of digital evidence*, ročník 1, č. 4, 2003: s. 1–12.

[6] Carroll, O. L.; Brannon, S. K.; Song, T.: Computer forensics: Digital forensic analysis methodology. 2008.

[7] CRU Headquarters: Write Blockers. [online], [cit. 2019-10-29]. Dostupné z: https://www.cru-inc.com/data-protection-topics/write-blockers/

[8] Dr. Marcus K. Rogers: Anti-Forensics pressentation given to Lockheed Martin. [online], 2005, [cit. 2019-10-28]. Dostupné z: https://www.researchgate.net/profile/Marcus_Rogers/publication/268290676_Anti-Forensics_Anti-Forensics/links/575969a908aec91374a3656c.pdf

[9] forensee s.r.o.: FORENZNÍ HARDWARE. [online], [cit. 2019-10-29]. Dostupné z: http://www.firewire-revolution.cz/shop/index.php?route=product/category&path=59_162_232&sort=pd.name&order=DESC

[10] Garfinkel, S. L.: Forensic feature extraction and cross-drive analysis. *digital investigation*, ročník 3, 2006: s. 71–81.

[11] Josef Kadlec: Forenzní analýza. [online], 04 2005, [cit. 2019-10-27]. Dostupné z: https://www.root.cz/clanky/forenzni-analyza-2/

[12] Ladislav VYSKOČIL: Zajišťování a analýza digitálních důkazů. [online], [cit. 2019-10-27]. Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky, Ústav informatiky a umělé inteligence. Vedoucí práce Malaník, David. Dostupné z: http://hdl.handle.net/10563/24882

[13] Michael G. Noblett; MARK M. POLLITT; LAWRENCE A. PRESLEY: Recovering and examining computer forensic evidence. [online], [cit. 2019-10-27]. Dostupné z: https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/oct2000/computer.htm

[14] Palmer, G. L.: Forensic analysis in the digital world. 2002, [cit. 2019-10-29]. Dostupné z: https://pdfs.semanticscholar.org/5f3f/1a95a38d251ef798eb6bc4f5626c27805762.pdf

[15] Risk Analysis Consultants, s.r.o: FORENZNÍ SOFTWARE. [online], [cit. 2019-10-27]. Dostupné z: https://forenzniprodukty.cz/kategorie-produktu/forenzni-software/

[16] Ryan Fahey: Computer Forensics: Forensic Analysis And Examination Planning. [online], [cit. 2019-10-27]. Dostupné z: https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/forensic-science/forensic-analysis-and-examination-planning/

[17] SVETLÍK, M.: Digitální forenzní analỳza a bezpečnost informací. *Data Security Management, ISSN*, 2010: s. 1211–8737.

[18] The Open University: Digital forensics. [online], [cit. 2019-10-27]. Dostupné z: https://www.open.edu/openlearn/science-maths-technology/digital-forensics/content-section-4.3

Příloha A

Seznam použitých zkratek

IT informační technologie

ARP tabulka meziapměti pro uchování linkových tzv. MAC adress. Ty jsou využíváný při směrování

MAC (angl. Media Access Control) MAC adresa jednoznačný identifikátor sítového zařízení

PDA osobní digitální pomocník (malý kapesní počítač)

GPS globální polohový systém

SIM (angl. subscriber identity module) identifikační karta ve standardu 3GPP TS 51.011

RAM (angl. Random-Access-Memory) Operační pamět s náhodným přístupem

iOS je mobilní operační systém vytvořený společností Apple Inc.

UFED je unikátním forenzním nástrojem určeným k extrakci dat z mobilních telefonů, paměťových karet a disků

JTAG Jedná se o architekturu Boundary-Scan pro testování plošných spojů, programování FLASH pamětí apod.

I/O Vstup/výstup