VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

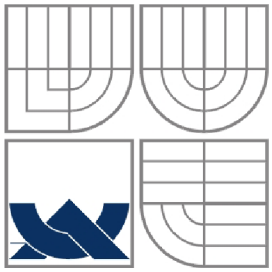
FORENZNÍ ANALÝZA KOMUNIKAČNÍCH NÁSTROJŮ

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

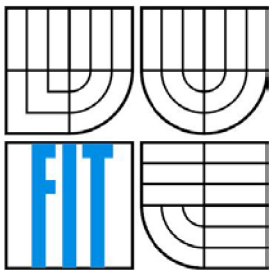
AUTOR PRÁCE
AUTHOR

TOMÁŠ LIPOVSKÝ

BRNO 2014



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

FORENZNÍ ANALÝZA KOMUNIKAČNÍCH NÁSTROJŮ

FORENSIC ANALYSIS OF COMMUNICATION TOOLS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

TOMÁŠ LIPOVSKÝ

VEDOUCÍ PRÁCE
SUPERVISOR

ING. PAVEL OČENÁŠEK, PH.D.

BRNO 2014

Abstrakt

Tato práce se zabývá technikami a postupy forenzní analýzy se zaměřením na internetovou komunikaci. Součástí práce je porovnání existujících aplikací pro forenzní analýzu komunikačních nástrojů, návrh a implementace vlastní aplikace. Vytvořená aplikace umožňuje získání a filtraci vybraných dat z počítače pro pozdější analýzu.

Abstract

This paper deals with techniques and procedures of forensic analysis with focusing on the internet communication. Part of this work is comparison of existing applications for forensic analysis of communication tools, design and implementation of its own application. Created application enables obtaining and filtration selected computer data for later analysis.

Klíčová slova.

Forenzní analýza, komunikační nástroje, internetová komunikace, získávání dat

Keywords

Forensic analysis, communication tools, internet communications, data acquisition

Citace

Lipovský Tomáš: Forenzní analýza komunikačních nástrojů, bakalářská práce, Brno, FIT VUT v Brně, 2014

Forenzní analýza komunikačních nástrojů

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením Ing. Pavla Očenáška, Ph.D.
Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

.....
Tomáš Lipovský
20. května 2014

Poděkování

Tímto bych chtěl poděkovat za trpělivost, nápady a náměty vedoucímu práce Ing. Pavlovi Očenáškovi, Ph.D. a dále všem za nezbytnou podporu při tvorbě.

Obsah

1 Úvod

Oblast informačních technologií se v poslední době značně rozrostla. Z daleka se nejedná jen o osobní počítače a firemní servery. Jde i o výkonné tablety a chytré telefony, které má dnes každý téměř pořád při sobě. Proto i v této oblasti je zapotřebí mít k dispozici způsoby, jakými vyšetřovat případné zneužití informačních technologií.

Forenzní analýza slouží jako objektivní nástroj k určení, zdokumentování a analýzy určitého z pravidla trestného činu. Podobně je tomu i u forenzní analýzy v informačních technologiích (neboli digitální forenzní analýza), která je tvořena zajištěním, identifikací, extrakcí, dokumentací a interpretací počítačových dat [1]

Digitální forenzní analýza (DFA) přestože za svou krátkou historii prodělala určitý vývoj, stále patří ve skupině forenzních věd mezi nejmladší. Nicméně má určité specifické vlastnosti a její výsledky jsou používány nejen k soudním účelům, ale také v oblasti bezpečnosti IT [2]. Elektronické komunikační nástroje jsou nyní dostupné téměř na všech počítačových zařízeních. Mezi nejběžnější komunikační nástroj patří email a různé proprietární i otevřené komunikátory (Facebook Messenger, Skype). Mezi internetovou komunikaci lze řadit i běžné prohlížení webu. Všechny tyto nástroje za sebou nechávají stopy, které lze při spáchání zločinu analyzovat. To může pomoci k objasnění různých typů zločinů nebo i k identifikaci pachatele.

Vzhledem k rozšířenosti informačních technologií a jejího využití se můžeme čím dál častěji setkávat s případy trestných činů v této oblasti. Může se jednat o případy přímo související s využitím těchto technologií, jako je například vykrádání bankovních účtů nebo o běžný trestný čin, kdy pachatel použil informační technologie pouze ke komunikaci se spolupachateli. Naše společnost na toto reaguje a musí činit určitá protiopatření. Ta jsou buď preventivního charakteru, nebo charakteru aktivního potlačení zločinu. Aby bylo možno tuto činnost postihnout, je nutné v průběhu vyšetřování zajistit odpovídající stopy, které musí mít určitou vypovídací hodnotu a zároveň musí mít vztah k páchané trestné činnosti. V tomto konkrétním případě jsou tyto stopy označovány jako digitální. [2] Proto je čím dál více zapotřebí specialistů v tomto odvětví.

2 Nástroje pro digitální forenzní analýzu v internetové komunikaci

V následující kapitole budou popsány existující nástroje digitální forenzní analýzy pro jednotlivé druhy internetové komunikace. Jedná se o analýzu dat, které lze získat ze stolního počítače s operačním systémem Windows. V poslední podkapitole pak bude závěr týkající se testovaných nástrojů.

2.1 Prohlížení webu

V dnešní době je web nezbytnou součástí práce, ale i trávení volného času na počítači. Drtivá většina uživatelů si mnohdy ani neuvědomuje, co vše lze zjistit pouze na základě historie prohlížení internetových stránek. Forenzní analýza může využívat těchto poznatků a proto je mnohdy klíčovým prvkem v některých případech.

Většina webových prohlížečů si do uživatelského profilu ukládá jak soubory s historií navštívených stránek, tak dočasné soubory ze kterých se dá získat mnoho užitečných informací.

Příkladem těchto informací může být u historie především seznam webových stránek, ale také čas jejich navštívení a mnohdy i cesta, ze které se uživatel na webovou stránku dostal. Z mezipaměti (*cache*) prohlížečů, lze pak například získat některé soubory a obrázky, ke kterým měl uživatel přístup.

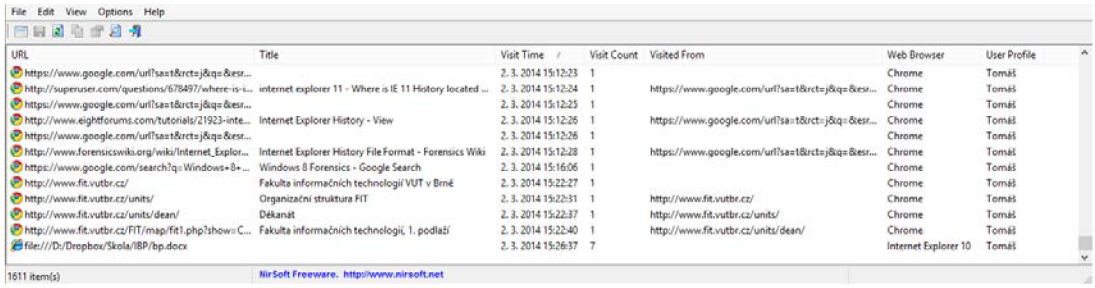
Kde hledat dočasné soubory?

Internet Explorer 11
%USERPROFILE% AppData/Local/Microsoft/Windows/WebCache
Chrome 34
%USERPROFILE% AppData/Local/Google/Chrome/User Data/Default/Cache/
Opera 20
%USERPROFILE% AppData/Local/Opera Software/Opera Stable/Cache
Firefox 29
%USERPROFILE% AppData/Local/Mozilla/Firefox/Profiles/*xxxxxxxx*.default/Cache
V uvedených cestách lze hledat stejná data i pro některé starší verze prohlížečů.

BrowsingHistoryView

(1.43) - freeware

K zobrazení historie z prohlížečů do jednoho seznamu lze použít software BrowsingHistoryView od tvůrce Nirsoft[1] (zobrazí historii z Internet Explorer (až do verze 11), Chrome, Firefox, Safari a SeaMonkey). Program automaticky detekuje cesty k historiím všech prohlížečů a proto je jeho obsluha velmi snadná. Jediný problém je se zobrazením historie Opery. Ta totiž od verze 15 změnila formát ukládání. Tento problém lze obejít změnou cesty k historii prohlížeče Chrome, se kterým má totožný formát. Výhodou BrowsingHistoryView je možnost nastavení parametrů při spuštění a také možnost exportu nalezených dat ve strojově čitelném formátu. Jedná se o URL, titulek stránky, čas návštěvy, počet návštěv, v některých případech i URL stránky, ze které bylo přistoupeno, dále systémový uživatelský profil a nakonec prohlížeč, který byl použit. Obrázek 1 ukazuje získané informace. Z dat uchovávaných prohlížeči umí BrowsingHistoryView získat maximum.



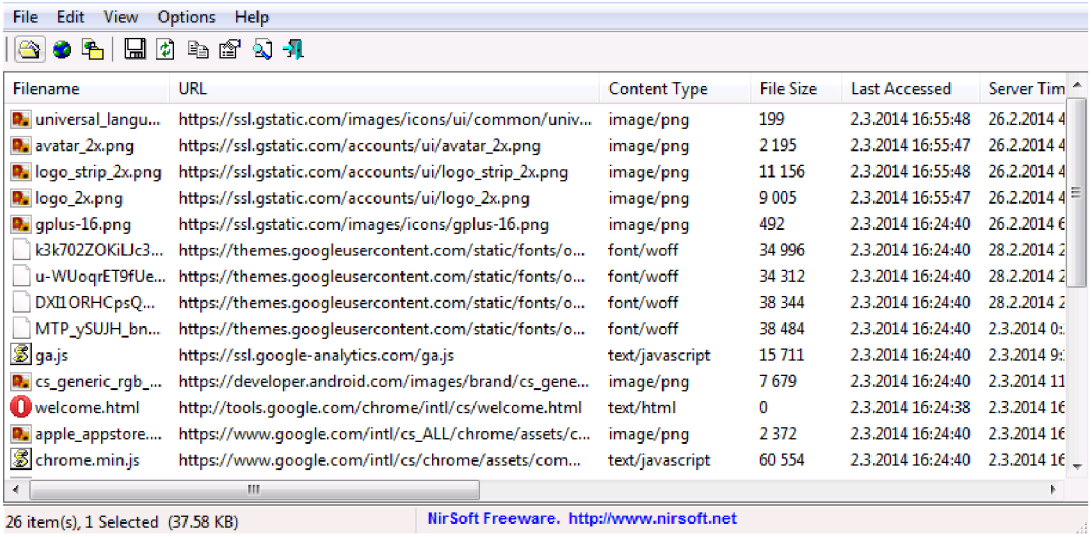
Obrázek 1 Historie všech prohlížečů

OperaCacheView/MizillaCacheView/ChromeCacheView

freeware

Pro zobrazení dočasných souborů je možnost použít sadu programů ChromeCacheView, OperaCacheView, MozilaCacheView také od vývojářů Nirsoft[2]. Tyto programy hledají ve výchozích adresářích nebo umožní přímo zvolit cestu k dočasné paměti (*cache*) prohlížečů. Mimo konkrétní soubor zobrazí v tabulce i čas stažení, posledního použití a poslední modifikace na serveru a spoustu dalších metadat (viz. Obrázek 2). Dočasné soubory lze rovnou kopírovat z původního archivu do nového umístění. V případě prohlížeče Opera se zde vyskytuje podobný problém jako u programu BrowsingHistoryView, tedy ten, že se změnil formát dočasné paměti. Opět ho lze vyřešit použitím nástroje určeného pro Chrome. Všechny programy z této sady je možné nastavovat pomocí parametrů ještě před spuštěním a všechny programy umí export dat do nejrůznějších formátů (XML, csv, xls). Přes velmi jednoduché ovládání jsou tyto programy užitečné a zobrazí všechny potřebné údaje vhodné k hledání důkazních materiálů.

[1] http://nirsoft.net
[2] http://nirsoft.net



Obrázek 2 Nalezené soubory dočasné paměti prohlížeče Chrome

2.2 Email

Jako další nezbytný komunikační nástroj v době internetové komunikace je email. Dnes už každý z uživatelů má vytvořenou emailovou adresu, kterou nemusí nutně využívat pouze ke komunikaci, ale mnohdy je vyžadována i jako předmět identifikace při registraci na různých portálech, e-shopech apod.

Abychom mohli získat informace o odeslaných a přijatých emailech, musíme samozřejmě mít přístup k disku, kde jsou uložené. Velmi často uživatelé využívají pro komunikaci emailové klienty, jako je například software Microsoft Outlook, který všechnu poštu ukládá do souboru s příponou .pst nebo .msg, které jsou v počítači uloženy defaultně na cestě: %USERPROFILE% AppData/Local/Microsoft/Outlook/.

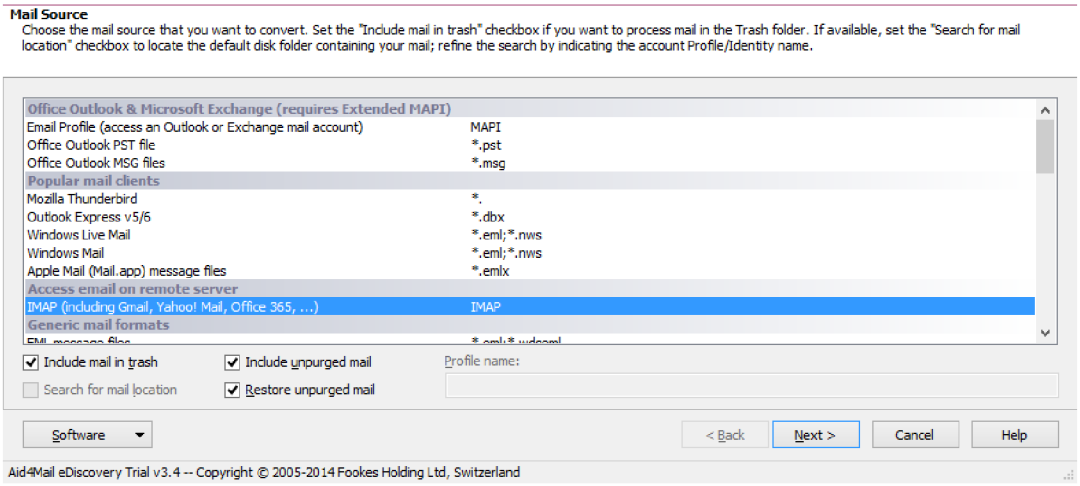
Pokud uživatel nevyužívá podobné aplikace, která data ukládají lokálně na disk, je nutné znát přístupové uživatelské jméno a heslo pro přihlášení ke vzdálenému serveru, jako je například gmail.com.

Jako u ostatní internetové komunikace, i zde jsou nástroje pro forenzní analýzu e-mailu. Tyto programy stahují nebo načítají uloženou poštu. Tu lze pak filtrovat, například podle vytvořených filtračních skriptů a následně ji uložit do mnoha druhů formátů, pro počítačové čtení například jako je formát xml nebo csv.

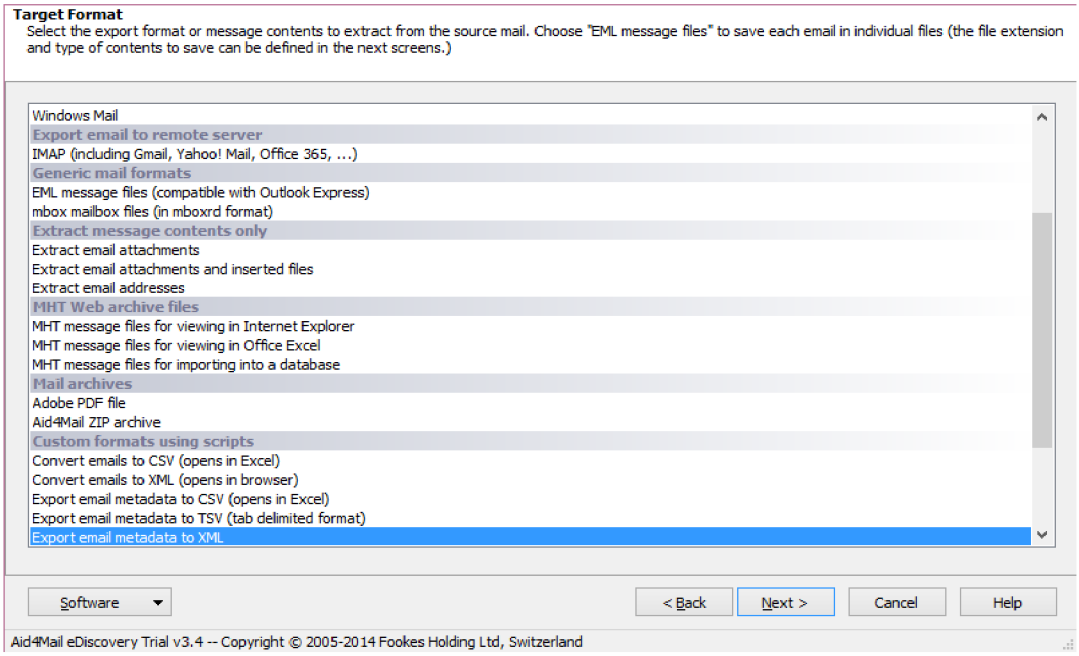
Aid4Mail eDiscovery

(3.4) – trial

Software Aid4Mail[3], který je vytvořen společností Fookes Software umožňuje filtrovat poštu z různých zdrojů. Autoři udávají podporu pro až 40 emailových formátů a klientů, mezi nejznámější, ze kterých lze načíst pošta je Microsoft Outlook nebo Mozilla Thunderbird, ale lze také poštu získat přímo ze vzdálených serverů pomocí služby IMAP (včetně Gmail, Yahoo!, apod.). Výběr zdroje je znázorněn na obrázku 3. Výsledek přefiltrované pošty lze pak uložit do různých formátů (Obrázek 4), které lze vybrat v přehledné tabulce.



Obrázek 3 Výběr zdroje emailových dat



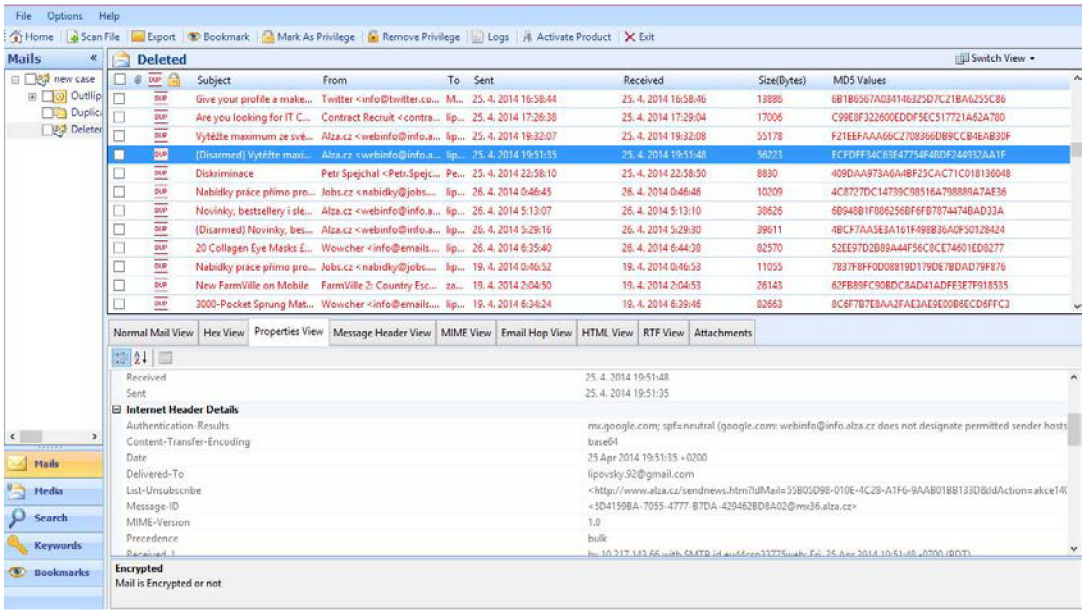
Obrázek 4 Nastavení výstupu

[3] http://aid4mail.com

MailXaminer

(4.0) – demo

MailXaminer[4] od firmy SysTools slouží jako Aid4Mail k analýze emailových zpráv. Umožňuje analyzovat hlavičku, tělo i přílohy zpráv. Program podporuje přes 750 emailových archívů pro pokročilou forenzní analýzu. Dokáže načíst data z Lotus Notes, Mozilla Thunderbird, Microsoft Outlook, Exchange a webových Google Apps, Gmail, Yahoo Mail, IMAP. Všechny nalezené emaily jsou pak v přehledné tabulce zobrazeny včetně hlavičky emailu a všech informací. Rozhraní připomíná Microsoft Outlook (viz. Obrázek 5). Velkou výhodou je, že dokáže obnovit smazané zprávy.



Obrázek 5 Hlavní obrazovka nástroje MailXaminer

2.3 Komunikátory

Internet je možné použít i k zasílání takzvaných rychlých zpráv (instant messaging). Pro rychlé zprávy jsou vytvořeny speciální sítě, ke kterým se lze připojit pomocí webového rozhraní (web-based), nebo pomocí klientů uložených v počítači, ve většině případů lze tento přístup kombinovat. Existují i programy, které přístup k sítím sjednotí například Trillian, QIP. Mezi nejrozšířenější sítě patří Facebook Messenger, Skype, Google Hangout, dále pak ICQ, Yahoo.

Získávání důkazních materiálů v případě klientů ve webovém prohlížeči není jednoduché. Pouze některá data jsou stažena do počítače a navíc se nachází v dočasných pamětech (v mezipaměti prohlížeče nebo operační paměti).

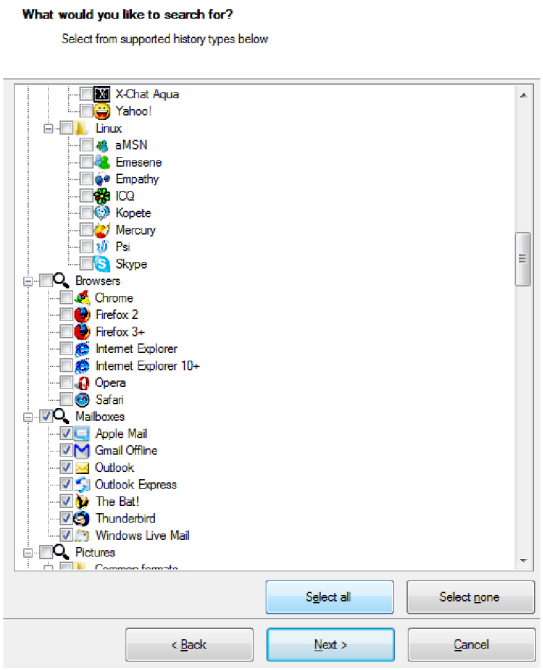
[4] http://mailxaminer.com

Evidence Center Ultimate

(6.2) – demo

Evidence Center[5] od ruské firmy Belkasoft je velmi složitý a komplexní nástroj pro forenzní analýzu. K dispozici je demoverze, která je schopna zobrazit od každého protokolu pouze 20 položek. Tato aplikace neslouží pouze k analýze komunikátorů, ale umožňuje také analyzovat historii prohlížečů, emailové klienty, videa i obrázky. Umožňuje skenování alokovaných i nealokovaných oblastí na disku, takže je velká pravděpodobnost úspěchu.

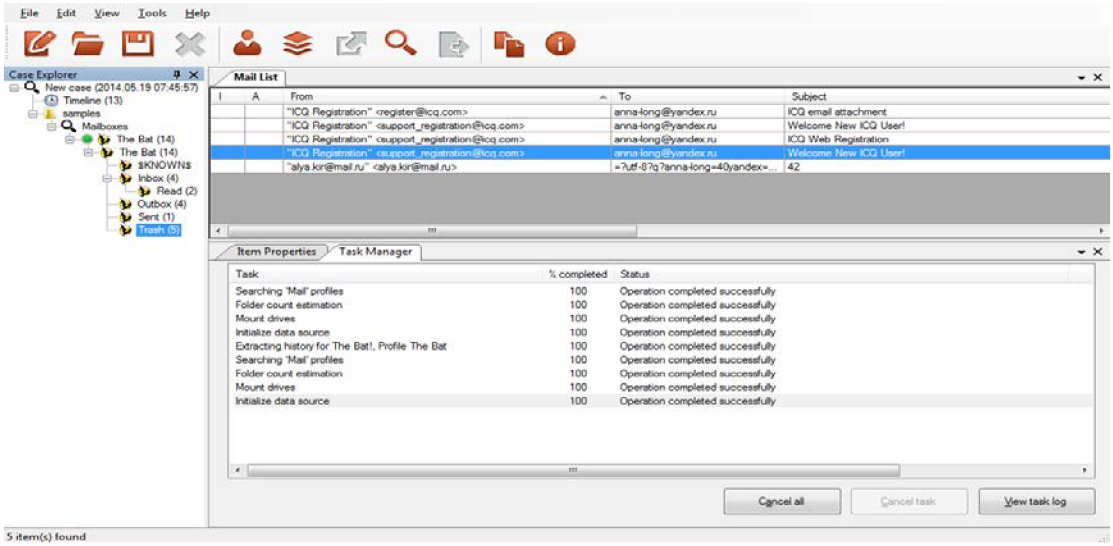
Před spuštěním samotné analýzy si uživatel vybere z dlouhého seznamu aplikací, jejíchž stopy chce na disku najít.



Obrázek 6 Podporované programy

Z komunikátorů program podporuje nejpoužívanější offline klienty jako Skype, Trillian, QIP, umí také najít stopy v dočasné paměti prohlížeče o online klientech Facebook Messenger, Meebo a jiné (Obrázek 6). Evidence Center také umí analyzovat virtuální počítače, registry a zálohy mobilních zařízení Android a iOS.

Výsledky samotné analýzy jsou zobrazeny v přehledném stromu a tabulkách (Obrázek 7), které lze jednotlivě prohlížet a exportovat do 9 různých formátů (txt, csv, pdf, docx).



Obrázek 7 Nalezené výsledky

[5] http://forensic.belkasoft.com

2.3.1 Facebook Messenger

Přístup k síti je umožněn přes protokol Jabber. Oficiální přístup k síti je pouze přes online webový klient (v prostředí PC). V počítači tedy nejsou žádné databáze s historií ani log soubory, které by se dala analyzovat. Veškerá historie komunikace je uložena na serverech Facebooku a lze k ní přistoupit kdykoliv přes webové rozhraní profilu. Pokud je použit neoficiální offline klient, není do něho zpětně stažena historie. Jedinou možností jak získat data z Facebook Messenger (pokud nepočítáme se znalostí hesla k profilu) je analýza živých dat v paměti RAM (případně systémového stránkovacího souboru pagefile.sys a hyberfile.sys).

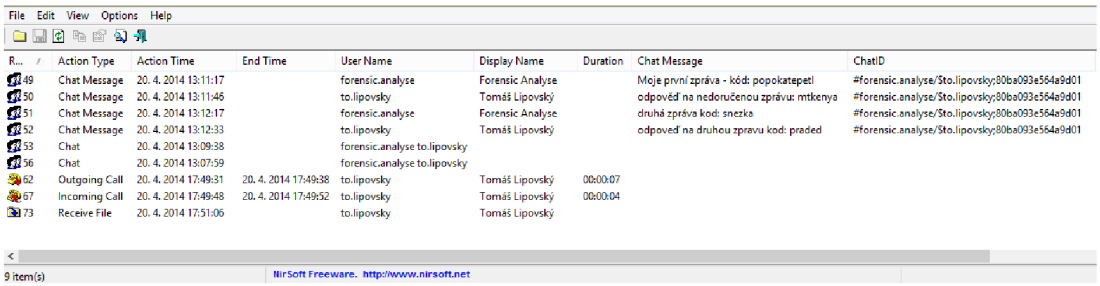
Z testovaných programů byl schopný tyto data analyzovat pouze Belkasoft Evidence Center.

2.3.2 Skype

SkypeLogView

(1.52) – freeware

SkypeLogView[6] je opět od Nirsoftu a je zdarma. Při spuštění má předdefinovanou cestu k profilu, kterou však jde manuálně změnit. Po analýze historie je zobrazena v přehledné tabulce včetně těla zprávy, případně typu záznamu – hovor, soubor, textová zpráva. Na obrázku 8 jsou všechny dostupné informace, které program dokáže získat. Chybí zde například zobrazené kontakty z průběhu hledání a přidávání osob do adresáře, tyto informace jsou jiné programy schopny zjistit. Přes svoji jednoduchost a s přihlédnutím na licencování zdarma se jedná o velmi užitečné nástroj.



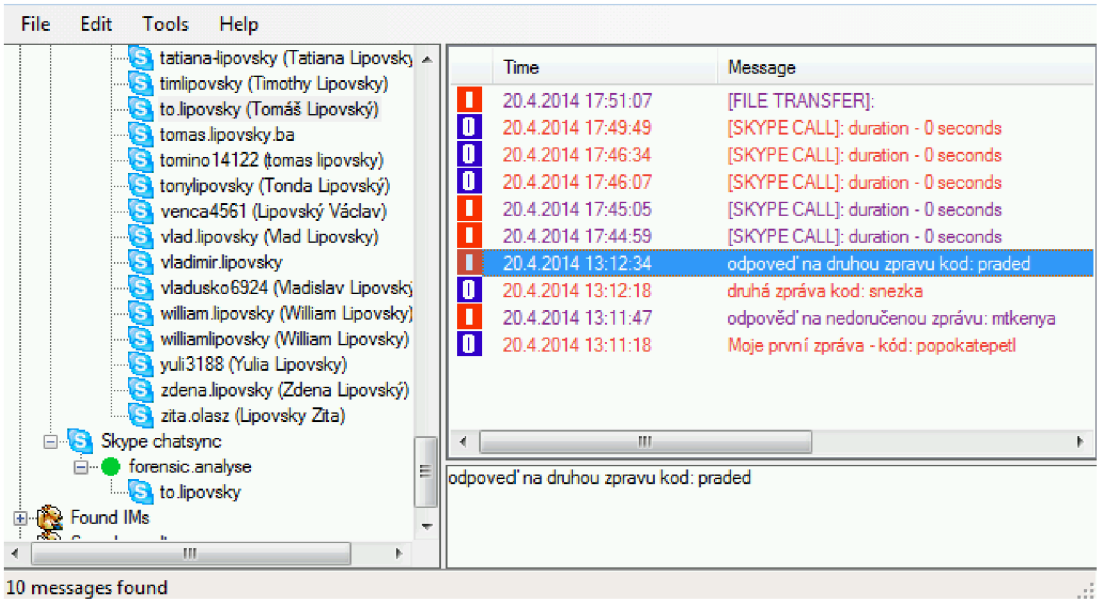
Obrázek 8 Tabulka s výsledky

[6] http://nirsoft.net

Skype Analyzer Pro

(1.04) – trial

Tento program firmy Belkasoft[7] automaticky prohledá celý disk a sám detekuje adresář s historií Skype. Zobrazí jak obsah hlavní databáze skype, ale i synchronizovanou historii komunikátoru. Program vyžaduje, aby v průběhu hledání byl Skype vypnut – dojde k uzamčení jeho databáze. V hlavní databázi jsou obsaženy nejen kontakty daného uživatele, ale i jména lidí, které měl uživatel možnost vidět – například při hledání nebo přidávání nového kontaktu. Na obrázku 9 jsou tyto kontakty v levé horní části (po spuštění byl v testovacím případě hledán kontakt s příjmením „Lipovský“). V pravé části je pak konkrétní konverzace včetně časových značek. Při testovacím hovoru trvajícím pár vteřin program sice hovor zalogoval, ale zobrazuje špatnou délku trvání hovoru – 0 vteřin. V případě více profilů je možnost jednoduše přepínat mezi historiemi. Program Skype Analyzer Pro je velmi přehledný a až na drobnou chybu s délkou hovoru zobrazí všechny dostupné informace které Skype ukládá.



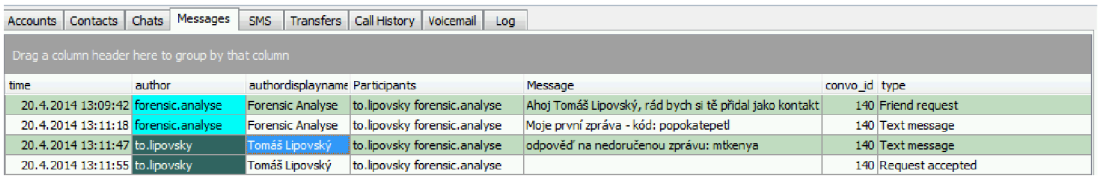
Obrázek 9 Seznam kontaktů a konverzací

[7] http://forensic.belkasoft.com

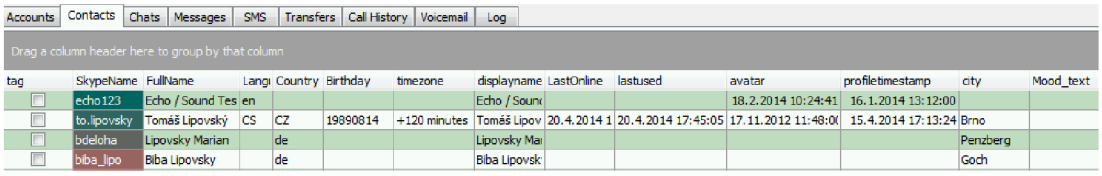
Forensics SkypeAlyzer

(1.2.35) – placený s možností vyzkoušení

Dalším nástrojem pro analýzu Skypu je SkypeAly[8]zer od Sanderson. Po spuštění je třeba provést výběr databáze s historií ručně. Data jsou zobrazena do kategorií. Zobrazí zejména, zprávy (Obrázek 10), adresář kontaktů včetně naposledy hledaných nebo přidaných kontaktů (Obrázek 11), příchozí a odchozí soubory a hlasové hovory. Oproti předchozímu testovanému nástroji nabízí více dat a nemá problém se zobrazením délky hovoru, ale na úkor přehlednosti.



Obrázek 10 Všechny zprávy Skype



Obrázek 11 Seznam kontaktů

2.4 Porovnání

Některé z testovaných aplikací byly velmi jednoúčelové a přes svoji jednoduchost jsou schopny podat dobré výsledky. Tyto programy jsou většinou zdarma. Víceúčelové nástroje, nebo nástroje s většími možnostmi nastavení je ale dobré porovnat.

MailXaminer je komplexní a má spousty funkcí, stejně jako Aid4Mail je placený. U obou programů je k dispozici ukázková verze. MailXaminer je na vyzkoušení pouze jako limitovaná demoverze, Aid4Mail nabízí plně funkční časově omezenou verzi (trial). Velkou výhodou MailXaminer je funkce, která umožňuje obnovit a zobrazit smazané e-maily.

Aid4Mail je jednodušší, ale pro analýzu dostačující. Tato aplikace vyhledané soubory ukládá do předem definovaných souborů, kdežto MailXaminer, kromě exportu, zobrazuje zprávy v přehledných tabulkách přímo v aplikaci.

Evidence Center Ultimate jakožto placený nástroj, umožňuje analýzu mnoha typů zdrojů. Tento program pro forenzní analýzu je velmi užitečný a usnadňuje práci, protože není potřeba používat více jednoúčelových programů. Ovšem s mnoha funkcemi se nástroj stává obtížnější k ovládání a použití pro drobné analýzy je zbytečně složitý.

[8] http://sandersonforensics.com

Všechny tři programy umožňují načítání mnoha formátů zpráv, od různých emailových klientů po vzdálený přístup na server a u všech je možnost velkého výběru formátu, do kterého se zprávy vyexportují.

K porovnání jsem měl k dispozici nástroj, který je velice jednoduchý, kde stačí vybrat zdroj, typ formátu, do kterého se vyexportují výsledky analýzy a vše proběhne velice rychle a snadno. Dále nástroj, který je komplexnější a nabízí větší komfort při zobrazování výsledků a vyhledávání mezi nimi. A také program, který je velice obsáhlý a umožňuje všestrannou analýzu skrze celý operační systém. Na základě tohoto zkoušení jsem zjistil, že k běžné analýze není zapotřebí složitých, funkcemi přeplněných nástrojů. Výsledky se ani v jednom z programů moc nelišily a rozdíl vidím pouze v komfortu používání funkcí a zobrazování výsledků.

3 Forenzní analýza

Co je forenzní analýza v informačních technologiích?

Digitální forenzní analýza nebo také Forenzní analýza digitálních dat, patří do široké skupiny forenzních věd. Tyto vědy se aplikují při vyšetřování a dokazování trestných činů. [2] Jak uvádí Ing .Marián Svetlík: „*Obecně jsou tyto vědy charakteristické tím, že se jedná o specifické (forenzní) aplikace „standardních" vědních oborů (např. soudní psychologie) nebo o samostatné forenzní disciplíny (např. daktyloskopie)*. [2]

Michale A. Caloaynnides [3] ve své publikaci také definuje digitální forenzní analýzu jako definovaný soubor technik, nástrojů a postupů použitých pro hledání důkazů na počítačích, které ale mohou být použity i v uživatelův neprospěch.

Ne každá digitální analýza dat musí mít tzv. forenzní charakter. Aby bylo možné tuto analýzu použít v soudním řízení a její výsledky mohly být relevantní, musí splňovat určitá obecná kriteria forenzního zkoumání. Tato kriteria jsou [2]:

- legalita – všechna data, veškeré stopy, dokumenty a jakýkoliv materiál, který je zajištěn, musí být jednoznačně získán pouze legálními způsoby
- opakovatelnost – možnost přezkoumání – při získávání dat a podkladů musí být použito takové činnosti a způsobu práce, aby bylo možno v budoucnu případným opakovacím procesem tato data stejným způsobem znovu získat a tím pádem dospět i k úplně stejným závěrům. Tady bych uvedl praktický příklad, kdy soudní znalec např. využije na zkoumání digitálních videozáznamů pouze a jenom monitor a on jen rozpoznává detaily. Tato činnost je nevhodná, protože je velice subjektivní a nelze ji zopakovat třetí stranou.
- integrita – definuje, že vše co je prováděno s daty a se vstupními informacemi, musí být jednoznačně popsáno a veškerá činnost musí být dokonale zdokumentována, aby nedošlo k neúmyslné či úmyslné manipulaci s důkazním materiálem
- nezávislost neboli nepodjatost osoby, která vykonává forenzní analýzu

Tato výše uvedená kriteria ovšem nejsou nikde v ČR právně zakotvena a vycházejí pouze z tzv. dobrých zvyků (*best practices*) a z obecných zahraničních doporučení. Jen zásada podjatosti je v našem zákonu ukotvena a to v zákonu o znalcích a tlumočnících, a proto musí být standardní součástí znaleckého posudku i vyjádření soudního znalce k podjatosti.

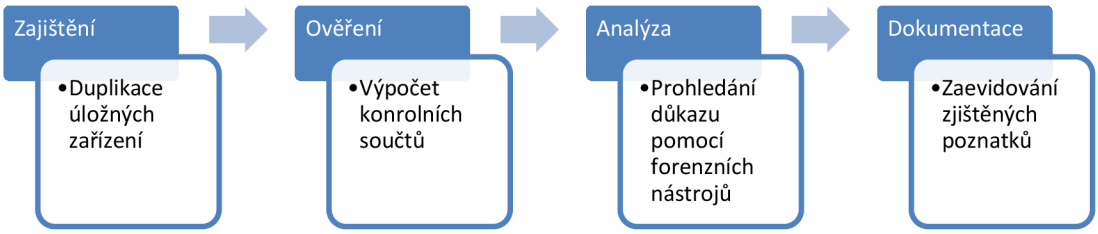
Velice důležitým aspektem při vypracování digitální forenzní analýzy je požadavek na odbornost. Vzhledem k rychlému vývoji informační technologie musí být samozřejmě odbornost neustále doplňována a ověřována. DFA musí být o jasných a transparentních důkazech a nikoli jen o odborných názorech nebo pocitech.

DFA je taky obsažena v systémech reakcí na bezpečnostní incidenty a to podle norem ISO/IEC TR 18044 a tímto se forenzní analýza dostává z oblasti soudních aplikací do preventivních bezpečnostních opatření. Zároveň DFA může být využita při řešení i prevenci incidentů v organizacích a může přinášet důkazy a pomáhat při interních šetřeních a auditech. K tomuto účelu se mohou použít tzv. softwaroví agenti nainstalovaní na počítače a ostatní komponenty informačního systému a pomocí vyhodnocení jejich výsledku je možno následně zjistit a analyzovat všechny procesy v informačních systémech, ale také je možnost aktivně monitorovat důležité informace organizace a předcházet tak bezpečnostním i jiným citlivým rizikům [2].

S Digitální forenzní analýzou souvisí i pojem počítačová kriminalita. Tu lze podle států EU a evropského parlamentu definovat jako**:** *„nemorální a neoprávněná jednání, která zahrnují zneužití údajů získaných prostřednictvím informačních a komunikačních technologií.“* Tuto kriminalitu můžeme charakterizovat třemi možnými způsoby [2]:

- počítač může sloužit jako prostředek, pomocí něhož je páchána trestná činnost, nebo jsou prováděny změny v informačních systémech
- trestný čin může být i vzhledem k počítači, jako k movité věci, např. jeho zcizení nebo poškození
- určité trestné činy mohou být také zaměřeny na software, případně na data uložená v počítači

Každá forenzní analýza se skládá z čtyř hlavních kroků [1] – získání důkazu, ověření důkazu a analýzy důkazu, neméně důležitou částí je pak vytvoření dokumentace (Postup je znázorněn na obrázku 12). V jednotlivých odvětvích forenzní analýzy se pak mohou provést ještě některé další kroky.



Obrázek 12 Obecný postup DFA

Na začátku šetření je doporučeno konzultovat možnosti získání dat z konkrétního systému s odborným znalcem. Systémy mohou obsahovat velká množství dat různého charakteru a ne všechna tato data odpovídají povaze zkoumaného případu. Dále se také musí zhodnotit právní dopady veškerého zkoumání, aby nedošlo k porušení právního řádu a jiných předisů. Je také nutno zvážit, aby tímto zásahem nedošlo k eventuelní ztrátě uložených dat a zvážit i možné komplikace vzhledem k místnímu prostředí.

3.1 Zkoumání na místě činu

Někdy se stává, že na místě činu první nezbytné úkony provádějí lidé, kteří nemají speciální proškolení jak postupovat. Je zapotřebí také zajistit na místě činu bezpečnost personálu. Mimo to není vhodné přímo na zkoumaném místě provádět různé analýzy zajišťovaných dat, tato data je dobré předat k prozkoumání do laboratoře forenzní analýzy[4]. Spolu s těmito daty musí být do forenzní analýzy přiloženo i následující:

- Definovaný speciální software
- Identifikovaná všechna záznamová média a zahrnout do dokumentace odkud byla média vyndána
- Protokol s obsahem výslechu správce systému
- Zápis kolik a jakých PC je zapojeno do počítačové sítě
- Je nutno zajistit kontakty na dodavatele softwarových řešení a servisu.

Zásada, že zkoumaný materiál je analyzován v laboratoři, ovšem nelze vždy splnit, proto je potřeba po zvážení situace rozhodnout, zda při zkoumání na místě nemůže dojít k ohrožení obchodní nebo jiné činnosti firmy, vzhledem k dlouhé době zkoumání.

Před zahájením DFA musí být splněna tato kritéria:

- Ověření právního nároku žadatele a kontrola všech formálních náležitostí k zadanému případu
- Jednoznačná definice předmětu zkoumání
- Specifikace jasně formulovaných otázek na které je potřeba hledat odpověď
- Ověření identity zadavatele
- Jedná-li se o požadavek orgánů činných v trestním řízení, musí být uvedeno i číslo spisu a soudní rozhodnutí opravňující k tomuto zkoumání

3.2 Postup zajištění důkazu

Zajištění důkazu znamená získání dat z počítače podezřelého a je klíčové v budoucí analýze. Nezodpovědné nebo chybné zajištění může znamenat znehodnocení důkazu a takové důkazy mohou být zpochybněny při soudním řízení. To může mít za následek neodsouzení pachatele.

Před zahájením samotného zajištění důkazů je nutná konzultace se znalcem vzhledem k danému prostředí a vytvořit si plán postupu, jež obsahuje [4]:

- Co lze a co nelze z daného systému vhledem k okolnostem zjistit, aby nebylo nic podstatného opomenuto
- Jakými jinými způsoby lze postupovat v případě, že některé informace nelze získat

- Vytvořit si pořadí, tak jak budou jednotlivé důkazy získávány
- Vyhodnotit technickou úroveň obsluhujících uživatelů počítače, protože někteří uživatelé mohou být na vyšší technické úrovni a citlivá a důležitá data ničit
- Vytvořit seznam důkazů, které hledáme (finanční záznamy, fotografie, tabulky, záznamy o komunikaci apod.)
- Zjistit další potřebné informace vztahující se k případu jako jsou: poskytovatel internetu, přihlašovací účty, pravidla tvoření hesel, konfigurační parametry sítě, umístění systémových logů apod. Tyto informace je nutno získat od administrátora systému
- Servery, serverové systémy – zjistit jaké jsou role serverů, všechny protokoly např. protokol událostí, soubory a aplikace
- Zajistit protokoly vnitřních i vnějších síťových zařízení jako např. z firewall brány, směrovačů, proxy serverů, serverů pro síťový přístup NAS a systému pro detekce napadení
- Interní hardwarové součásti, mezi které patří informace o MAC adrese, informace o externích portech, USB apod.
- Je důležité také nezapomenout na přenosná mobilní zařízení jako jsou chytré telefony, MP3 přehrávače, FLASH disky apod.
- Fyzicky zabezpečit důkazný materiál v místě šetření
- Chránit veškerá zařízení před účinky magnetických polí a statickou elektřinou
- Vytvořit si seznam periferních prostředků PC jako jsou různé scannery, tiskárny, čtečky paměťových karet, digitální fotoaparáty, kamerové systémy.
- Zjistit i případné možnosti poskytnutí dalších digitálních důkazů, které nejsou přímo na místě šetření, jako je vzdálené datové úložiště nebo data poskytovatele internetu apod.
- Posoudit i možnost prozkoumání pracoviště pomocí jiných znaleckých metod nejen DFA

Data v počítači jsou uložena ve dvou typech pamětí – nevolatilní/stálá (harddisk) a volatilní/nestálá (operační paměť). Obsah nestálých pamětí se po vypnutí počítače smaže, tudíž je těžší data z těchto typů pamětí získat. Při nalezení počítače na místě je nutné udělat fotografie obrazovky – pokud je počítač zapnutý. Většinou je dovoleno pohnout pouze kurzorem myši, aby technik zjistil, jaké programy jsou spuštěny. Pokud je spuštěn formátovací, nebo destrukční software, je nutné počítač okamžitě vypnout, aby nedošlo k dalšímu odstranění důkazů. Při zapnutém počítači je dobré udělat kompletní obraz disku a operační paměti. Po zkopírování dat z operační paměti je teprve možné spouštět další programy na analýzu běžícího systému. Pokud by technik počítač vypnul, je možné že se tak

ztratí některé důležité důkazy. Již vypnutý počítač lze zařadit do evidence důkazů k bližšímu prozkoumání [5] .

Při rozhodování zda nechat počítač zapnutý může hrát roli i fakt, zda je počítač v roli oběti, nebo podezřelého. V případě oběti (například je uživatel počítače vydírán), může zůstat počítač zapnutý.[6]

Otázkou taky je zda nechat počítač připojený k síti, nebo ne. Je možné, že je na počítači spuštěn software, který po odpojení od sítě začne s destrukcí dat (deadman switch). Pokud ale odpojen nebude, může pachatel provádět zločin dál. Toho lze ale využít ke sledování jeho dalších kroků. I v tomto případě tedy hodně záleží na posouzení konkrétní situace. [7]

Následujícím krokem je pořízení duplikátu pevného disku, případně operační paměti. K tomuto účelu existují speciální nástroje, které za chodu počítače vytvoří bitovou kopii disku včetně neobsazeného prostoru [1]. Vytvoření obrazu je navíc možno několika způsoby. Fyzické vyjmutí pevného disku (a odpojitelných externích medií) a připojení k věrohodnému počítači v laboratoři. V tomto případě je také doporučeno použít speciální adaptér, který je schopen blokovat všechny zápisové operace aby nedošlo k nechtěnému znehodnocení dat [5].

Další možností je připojení se k počítači pomocí sítě. To probíhá tak, že se spustí počítač ze speciálního CD/flash disku, tento odlehčený operační systém umožní ovládání počítače přes síť a zároveň nedovolí zápisové operace na pevný disk.

K zajištění důkazu zařadíme i komunikaci s uživateli počítače. Je totiž možné, že je skrze jejich počítač páchán trestní čin bez jejich vědomí. Mohou tak napomoci vyšetřování poskytnutím přístupových hesel nebo i popsáním jejich běžné práce s počítačem.

3.3 Postup ověření důkazu

Po zajištění důkazů probíhá další analýza výhradně na kopii materiálu. Je proto důležité dokázat, že v průběhu vyšetřování nedošlo ke změně zdrojových dat a tím pádem k znehodnocení důkazu. K tomuto účelu se používá kontrolních součtů (kryptografických hashí) zdrojových dat, které slouží jako takový otisk prstu. Jedná se o hash kód, který představuje jedinečnost dat. Soubory jsou totožné, pokud mají hash hodnoty stejné, i když mohou mít jiné názvy souboru. Takže jakákoli změna v jednom ze souborů, dokonce i změna jednoho písmenka z velkého na malé, vytvoří jiný hash.

Vyšetřovatelé tak mohou porovnávat tyto otisky mezi fyzickým diskem ze zajištěného počítače a obrazem tohoto disku pořízeným za účely vyšetřování. Tímto způsobem je možné porovnat bitové kopie celých disků i jednotlivých soborů. Hashovací funkce je popsána jako matematická funkce „h“, která představuje algoritmus, jež převede

vstupní posloupnost bitů libovolného počtu na výstupní o pevné délce n-bitů. Tento výstup je pak označován jako digitální otisk. Unikátnost digitálního podpisu je v tom, že kontrolní otisk má jedinečnou hodnotu fixní délky, která je vypočtena pomocí hashovaní funkce dle obsahu vstupního souboru.

Pro výpočet kontrolních součtů se nejčastěji používají algoritmy MD5 a SHA, případně kombinaci více hashovacích algoritmů CRC a MD5 pro vyšší kvalitu ověření [1].

V posledních letech však bylo zjištěno, že se mohou vyskytovat v algoritmu MD5 kolize. Pro účely forenzní analýzy jsou však tyto kolize nepravděpodobné. Kolizím se nelze vyhnout, ale vhodnou volbou kombinací hashovacích funkcí je lze eliminovat.

V praxi se při ověřování důkazů používají aplikace na forenzní analýzu, které mají v sobě již tuto hashovací funkci implementovanou.

Vzhledem k tomu, že je tento hashovací mechanismus časově náročný a někdy je zapotřebí vytvořit otisky velkého počtu datových souborů, provádí se proto uložení celé datové složky do jediného souboru archivu a to bez komprese dat a potom se pro tento archiv provede pouze jeden výpočet kontrolního otisku pomocí hashovacího algoritmu.

Není-li možné provést na místě šetření kontrolní otisky, potom je nutné média zajistit a zapečetit tak, jako je to běžné u jiných materiálních stop a tím zabezpečit autentizaci těchto materiálů.

Jakmile je tedy důkaz zajištěný, z pevného disku je vytvořena kopie a je vytvořen kontrolní součet zdroje i kopie – neboli existuje důkaz, že s daty nebylo při vytvoření kopie manipulováno. Není již potřeba pracovat přímo s originálním diskem, ten se uloží na bezpečné místo do sbírky důkazů a dále se pracuje s kopií. Je ale vhodné si vytvořit i druhou kopii, aby se zajistilo, že originál už nebude třeba (například pokud se při vyšetřování omylem zapíší nějaká data do první kopie).

Všechny vypočítané kontrolní otisky je také nutno uvádět v příslušné dokumentaci pořízené v rámci zajišťování digitálních stop. Nepřepisovatelná média typu DVD nebo CD se musí nesmazatelně označit datem, číslem případu a dvěma podpisy, a to zajišťující osoby a osoby nezúčastněné. V těchto kontrolních případech není potom nutné vytvářet kontrolní otisk.

3.4 Analýza důkazu

Poslední část procesu forenzní analýzy je samotná analýza zajištěného důkazu. Analýzu lze rozdělit na „živou“ a „neživou“. Neživá analýza znamená, že technik pracuje pouze s daty, které má k dispozici z diskového obrazu a tento obraz má připojený k důvěryhodnému počítači v laboratoři. Tento typ analýzy je složitější, protože technik musí detailně znát princip daného souborového systému. Naopak živá analýza umožní spustit operační systém

právě ze zajištěného disku (rsp. jeho kopie) a přímo do něho nainstalovat nástroje do analyzovaného systému. Už samotné spuštění systému dá technikovi možnost procházet souborový systém a zobrazí mu všechna metadata o souborech, která jsou k dispozici.

V této části se analýza rozvětvuje na několik částí – tato práce je zaměřena na analýzu internetové komunikace, mimo to lze analyzovat historii otevřených programů, uložených dokumentů, prohlížených souborů jako jsou třeba fotografie atd. Každý program si může (nebo také nemusí) ukládat své dočasné soubory a taky logy jiným způsobem. K prohlížení dat a záznamů (log files) z běžných aplikací (email, internetový prohlížeč, komunikátor) jsou k dispozici specializované nástroje, které zobrazí informace ve formátu čitelném pro technika, viz Kapitola 2. Prohlédnout si dočasné soubory od jiných programů (proprietární firemní software atd.) je trochu složitější. V tomto případě je vhodné zjistit si od výrobce programu vnitřní strukturu soboru a ten pak pomocí HEXa editoru zkoumat, v některých případech je možné zaslat soubor přímo výrobci a ten může data rozšifrovat, v tomto případě je ale důležité zvážit bezpečnostní rizika související s vyšetřováním (data se mohou dostat do špatných rukou).

Většinu těchto částí může provádět současně více techniků, každý se svým obrazem zdrojového disku. Důležitá věc při vyšetřování je také důkladná evidence všech úkonů s důkazy – kdo co kdy kopíroval, otevřel, ukládal a jakým způsobem. Nedůsledná evidence úkonů může znehodnotit celý důkaz [1].

3.4.1 Forenzní analýza Internet Exploreru

Internet Explorer je aplikace k prohlížení webu, kterou denně používá drtivá většina všech uživatelů. Aby mohl analytik rekonstruovat dostatečně přesně data z webového prohlížeče, musí dokonale analyzovat vnitřní datové struktury webu i soubory v mezipaměti prohlížeče v aplikaci Internet Explorer.

Jedním z mnoha problémů jak rekonstruovat data z webového prohlížeče je, že vnitřní datová struktura v mezipaměti prohlížeče je obtížně čitelná. Specializované programy, které analyzují tato data, využívají svých proprietárních řešení. Pracným způsobem, kterým lze tato data číst, je analýza datového souboru. Internet Explorer ukládá řadu souborů s názvem `index.dat` v domovském adresáři každého uživatele. Tento soubor mapuje stránky, které byly uživatelem navštíveny a které jsou uloženy v mezipaměti (*cache*) v náhodně pojmenovaných adresářích, tak aby data při opětovném otevření dané stránky mohla být zobrazena rychleji z lokální mezipaměti. Tento soubor je při forenzní analýze použit k zpětné rekonstrukci uživatelských aktivit na webu a používá se k tomuto účelu analýza hlavičky v datovém souboru `index.dat`.

3.4.2 Forenzní analýza emailu

V dnešní době již je email hlavním prostředkem komunikace a většina počítačových uživatelů používá emailové programy pro příjem, odesílání a zpravování emailu. Tyto programy se však liší jak v ukládání emailu, tak i v možnostech logování emailové aktivity. Některé z nich jsou instalovány do operačního systému, jiné využívají webové prohlížeče, takže nepotřebují instalaci žádného dalšího softwaru do počítače.

Při posuzování emailové komunikace v rámci DFA můžeme zkoumat jak poštovního klienta, tak i část serverovou bez ohledu na operační systém. Program emailového klienta pro přístup uživatelů k emailovým účtům v organizacích většinou definuje správce poštovního serveru.

Při zkoumání forenzní analýzy je mnohem jednodušší zkoumání firemních účtů neboť tyto účty používají standardní názvy stanovené správcem emailových serverů. Opačná situace je při sledování emailových uživatelů internetu, neboť tyto účty nepodléhají žádným předem známým a dedikovaným pravidlům, tím pádem je identifikace majitele emailového účtu obtížnější.

Získávání dat z emailového klienta

DFA při zkoumání emailového klienta používá tyto části [8]:

1) Kopírování emailové zprávy:
   Před zahájením vyšetřování pošty je potřeba zkopírovat a vytisknout emaily, které jsou nějakým způsobem zapojeny do vyšetřování. Pomocí emailového klienta, nebo speciálního forenzního nástroje se emaily zkopírují do bezpečného úložiště a zálohují na rozdílná záznamová media.
2) Prohlížení emailových hlaviček:
   Po otevření emailového záhlaví se zkopíruje a vloží např. do textového dokumentu, takže je možné tato záhlaví později lehce přečíst.
3) Prověřování emailových hlaviček:
   Dalším krokem je posouzení záhlaví emailu a shromažďování informací o emailu podezřelého. Hlavní část informace je hledání původní emailové adresy nebo domény, případně adresy IP. Další užitečná informace zahrnuje datum a čas odeslání zprávy, názvy souboru příloh, případně číslo jedinečné zprávy.
4) Prověřování dalších emailových souborů
   To, jak jsou soubory emailového klienta uloženy, závisí na nastavení klienta a serveru. Například v aplikaci Microsoft Outlook jsou emaily umístěny v souboru PST. S těmito soubory můžeme pracovat i v režimu offline. Také většina emailových programů zahrnuje v sobě i elektronické kalendáře, seznamy úkolů případně poznámky. Tyto informace mohou být také pro DFA velice důležité.

V případě e-mailu u webových prohlížečů jsou tyto informace zobrazeny jako webové stránky v dočasné paměti prohlížeče. Celá řada emailových poskytovatelů také nabízí služby pro zasílání rychlých zpráv, neboli chat (*Instant Messaging*), které také mohou ukládat svůj obsah zpráv do archivu v nechráněném formátu. Obvykle jsou uloženy ve složkách daného programu, nebo v systémovém profilu uživatele. Některé tyto soubory vyžadují speciální nástroje pro čtení jejich obsahu.

Získávání informací z emailových serverů

E-mail server zaznamenává veškerou emailovou dokumentaci s klienty a tudíž je možné těchto záznamů, které jsou uloženy v logovacím souboru, využít také při zkoumání DFA. K této činnosti je potřeba spolupráce se správcem sítě nebo správcem emailu, který je schopen tato data v těchto souborech vyhledat. Některé emailové servery využívají k záznamu databázi, jiné používají logovací soubor. Tyto emailové protokoly jsou dost často ve formátu prostého textu a lze je číst pomocí základního textového editoru. V některých systémech může být nastaveno i uchovávání kopie emailu klientů, i když tyto zprávy jsou již z jejich schránek odstraněny. Jako příklad mohu uvést Microsoft Exchange Server, který využívá několik souborů v různých kombinacích k poskytování emailové služby. Nejužitečnější pro vyšetřování jsou soubory EDB a STM. Exchange servery mohou také zapisovat do protokolu s názvem Tracking.log., který sleduje veškeré zprávy. Kromě speciálních forenzních nástrojů, tento log poskytuje největší množství informací o zprávách odeslaných a přijatých na serveru Exchange. [4]

3.4.3 Forenzní analýza komunikátorů

Facebook Messenger

Facebook patří mezi nejoblíbenější sociální sítě a jeho popularita za poslední roky prudce stoupla. Současně s tím se samozřejmě objevuje mnoho příkladů, kdy tato síť bývá zneužívána i k trestné činnosti. Různé aktivity jako zasílání rychlých zpráv, komentáře na zdi či sdružování do skupin, mohou vytvářet a vytvářejí spoustu stop v různých paměťových místech.

Části Facebooku mohou být uloženy v rozdílných paměťových modulech jako je operační paměť RAM, mezipaměť prohlížeče, stránkovací soubory, nealokované clustery a systém bodu obnovy počítače. Vzhledem k popularitě Facebooku a tím pádem i k větší možnosti zneužití je potřeba najít při DFA důkazy o Facebookové aktivitě na různých platformách nebo zařízeních.

Pomocí DFA je možno nalézt spoustu Facebookových aktivit jako jsou: vyhledávání přátel, umístění nových zpráv na zeď, komentáře na ostatních zdích, vytváření událostí, odesílání zpráv skupině uživatelů a chatování. Vzhledem k způsobu práce s Facebookem, tedy pomocí webového prohlížeče, jsou stopy po těchto aktivitách dohledatelné pouze v mezipaměti prohlížeče a operační paměti. Získání těchto dat je proto obtížné. Alternativou zůstává přihlášení se na profil Facebooku jako daný uživatel a zjistit data o aktivitách přímo z Facebookového rozhraní, tento způsob je ale reálně téměř nemožný, protože získat přihlašovací údaje vyžaduje spolupráci s vyšetřovanou osobou.

Skype

Tato síť používá svůj proprietární protokol a k dispozici nabízí pouze svůj oficiální klient Skype. Je zde teoreticky možnost použití neoficiálního klienta, ale není zaručena funkčnost komunikace. Historie zpráv je uložena lokálně, ale i na vzdáleném serveru. Při přihlášení k síti je historie synchronizována a tudíž opět stažena do počítače.

Ačkoliv existuje řada softwarových produktů k analyzování činnosti programu Skype, je v některých případech užitečné znát, jakým způsobem lze prozkoumávat soubory protokolů tohoto programu a jaké jsou možnosti získání komunikačních dat. Informace, které jsou obsaženy v těchto souborech, jsou následující:

- Kontakt, se kterým bylo komunikováno
- Datum a čas odeslané zprávy
- Obsah zprávy
- Datum a čas trvání hovoru
- Název odeslaného souboru
- Velikost tohoto souboru
- Datum a čas trvání přenosu souboru
- Informace zda byl hovor odchozí nebo příchozí

Tyto informace jsou uloženy v těchto souborech
%USER_PROFILE%/AppData/Roaming/Skype/%skypename%/main.db
%USER_PROFILE%/AppData/Roaming/Skype/%skypename%/chatsync
Adresář chatsync obsahuje několik binárních souborů .dat, které pravděpodobně obsahují stejné informace jako main.db. Vzhledem k tomu, že neexistuje žádná oficiální dokumentace pro Skype a strukturu jeho protokolu, je nejasné proč Skype ukládá redundantní informaci ve dvou různých formátech [9]. Soubor main.db je databázový soubor SQLite. Tato databáze obsahuje několik tabulek, přičemž tyto tabulky jsou nejzajímavější:

- Messages (uloženy všechny konverzace)
- Callmembers (všichni členové hovoru)

- Call (informace o hovorech)
- Contacts (všechny Skype kontakty)
- Transfers (všechny přenosy souboru)

Windows verze Skype používají další soubor config.xml, který obsahuje konfiguraci Skype a některé další důležité informace. Tento soubor je v běžném XML formátu a lze přečíst jeho obsah. Avšak velkou část tohoto souboru nelze interpretovat vzhledem k nedostatku informací o struktuře. Existují ovšem dvě zajímavé věci uložené v tomto souboru. Jednou je časová značka, která označuje, kdy byl Skype naposledy použit (uložena v atributu <"LastUsed">). A taky všechny kontakty, se kterými bylo korespondováno v tomto čase. Ty jsou uloženy v elementu <"u">.
Pomocí programu na analýzu Skype a jejich výsledku je pak možno reverzní analýzou zjistit a pochopit strukturu binárních dat i jejich popis.

3.5 Evidence a dokumentace nalezeného materiálu

Z této evidence důkazů se pak vytvoří přehlednější dokumentace. Dokumentace je výstupní zpráva pojednávající o zjištěných skutečnostech, způsobu odhalení důkazu. Musí být přesná a dostatečně vypovídající a je psána pro poučené publikum. [9]

Dokumentace musí probíhat také zároveň s analýzou a všechny uchované poznámky by měly být v souladu s politikou DFA. Při provádění forenzní analýzy je doporučený postup dokumentace následující:

- Zapisování poznámek při konzultaci se zadavatelem případu
- Vytváření kopií veškerých povolení, které byly k případu vydány
- Je důležité zachovat všechny počáteční žádosti o pomoc s vyšetřováním
- Zachování veškerých kopií dokumentací, jež jednoznačně potvrzují důkazní integritu
- Vytvoření detailního popisu činností, aby bylo možno podle těchto poznámek činnost opakovat
- V poznámkách je potřeba důsledně uvádět čas, datum a popisy všech akcí a jejich důsledky
- Pečlivé zaznamenání nesrovnalosti, které se při vyšetřování objevili
- Do dokumentace patří i zakreslení topologii sítě, seznamy všech dotčených uživatelů, případně uživatelské smlouvy a taky hesla
- Je také třeba zdokumentovat veškeré změny, které proběhly na systému nebo v počítačové síti, případně vznikly i během vyšetřování

- Zaznamenat také aktuální verzi operačního systému a zkoumaných programů včetně veškerých posledních instalovaných aktualizací
- Do evidence patří i informace, které se týkají i vzdáleného úložiště dat, přístupu k tomuto úložišti, případně informace o veškerých zálohách zkoumaného počítače

Při zkoumání mohou být objeveny i důležité informace, na které se nevztahuje současné právní povolení a které se netýkají právě vyšetřovaného procesu, ale mohou mít důkazní hodnotu. Tyto informace je dobré také zaznamenat a upozornit na ně příslušné osoby, neboť mohou být potřebné k udělení dalšího povolení zkoumání.

Pokud forenzní analýzu provádí soudní znalec, je výsledkem jeho práce znalecký posudek. Znalec je osoba, která je zodpovědná za úplnou a přesnou zprávu o všech svých nálezech, o výsledcích analýz a také o všech zkoumaných digitálních důkazech.

Znalecký posudek v České republice podléhá zákonu o Znalcích a tlumočnících (č 36/1967 Sb.). Dalším použitelným dokumentem může být odborné vyjádření. To nepodléhá zákonu a autorem může být jak soudní znalec, tak fyzická a právnická osoba. V případě použití u soudu je odborné vyjádření považováno za listinný důkaz [6]. Vhodná výstupní zpráva by měla obsahovat následující údaje (seznam vychází z doporučení společnosti Microsoft [10]):

- Identifikace znalce či znalecké laboratoře, která vytváří zprávu
- Jednoznačný identifikátor daného případu nebo jeho podací číslo
- Přesný datum a čas převzetí případu a jednoznačná totožnost osoby, která případ předává
- Datum ukončení a sepsání zprávy
- Detailní informace o znalci, jeho oprávnění i jeho podpis
- Účel, proč byla zpráva sepsána a pro koho je určena
- Seznam všech autorů a spolupracovníků včetně jejich pozic
- Stručný popis činu, na základě kterého musela být vypracována zpráva, popis by měl být srozumitelný netechnickému publiku.
- Seznam dostupných důkazů včetně způsobu jak byly získány
- Detailní popis analýzy včetně způsobu jak byla provedena, grafických výstupů z použitých skenovacích nástrojů a zdrojů a potvrzení na základě kterých se napsané tvrzení dá ověřit
- Závěr shrnující výsledek vyšetřování. Může obsahovat odkazy na některé důkazy, ale bez zbytečných detailů, ty jsou obsaženy v detailním popisu
- Doplňující dokumenty související s vyšetřováním – diagramy sítě, zapojení atd.
- Vysvětlení některých nesrozumitelných pojmů pro netechnické publikum

3.6 Rizika spojená s forenzní analýzou

V průběhu digitální forenzní analýzy nelze vyloučit rizika související s digitálními stopami. Může se jednat o problémy s technikou, selhání zařízení obsahující digitální stoupu. Ale nejčastěji se bude jednat o riziko lidského faktoru, tedy nedodržování předepsaných pravidel a postupů. Toto ohrožení může být způsobeno neúmyslně, ale taky s úmyslem zmanipulovat vyšetřování. Ladislav Vyskočil ve své práci uvádí především tato rizika[11]:

- 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
- a další…

Většině rizik spojených s digitální stopou lze předcházet dodržováním postupů a doporučení a obecných bezpečnostních pravidel.

4 Návrh a implementace aplikace

Cílem aplikace (Forensic Tool) je nabídnout forenznímu technikovi ucelený pohled na data počítače. Konkrétně se jedná o data webových prohlížečů (Internet Explorer, Chrome, Firefox, Opera) a programu Skype. Program by měl být navržen tak, aby umožnil pozdější doplnění získaných dat, například o logy dalších aplikací.

Jedinou podmínkou ke správnému fungování aplikace je operační systém Windows s nainstalovaným frameworkem.NET ve verzi 4.5.

4.1 Návrh

Při návrhu aplikace byla snaha o co nejjednodušší, ale přesto funkční a přehledné uživatelské rozhraní. Z porovnání existujících řešení vyplynulo, že vertikální rozdělení okna aplikace nabízí spoustu místa pro zobrazená data a zároveň stále dostatek prostoru pro ovládací prvky.

Veškerá nastavení související se skenováním počítače jsou soustředěna do levé části okna. Mimo to je zde umístěna také volba pro export dat. Pravá část okna je dále rozdělena horizontálně, je zde umístěna možnost nastavení filtru, přepínání zdrojů dat a samotná data.

Aplikace je navržena tak, aby využívala možností již existujících volně dostupných aplikací (jejich API). Od nich získá surová data a na tyto data dokáže aplikovat filtry. Mimo jiné zajišťuje tento způsob určitou modularitu. Do budoucna tak nebude problém rozšířit možnosti skenování o další aplikace třetích stran.

Při návrhu byla důležitá i rychlost aplikace, je totiž možné, že bude zpracovávat desítky tisíc záznamů. Z tohoto důvodu není filtr aplikovaný na všechny získané atributy, ale jen na ty, které má smysl filtrovat. Tyto atributy jsou uvedeny v Tabulka 1 Možnosti filtrace. Vzhledem k použití frameworku .NET, nebude potřeba implementovat žádné speciální třídící algoritmy, o vše se postará standardní knihovna.

Historie prohlížečů	URL, Titulek stránky
Mezipaměť prohlížečů	URL, Název dočasného souboru
Skype	Jméno kontaktu, text zprávy

Tabulka 1 Možnosti filtrace

Jako výstupní formát byla zvolena tabulka Microsoft Excel. Díky své rozšířenosti se jedná o velmi praktické řešení. Veškerá získaná data (s aplikovaným filtrem) budou tímto způsobem uložena.

4.2 Použité technologie

Pro vytvoření programu jsem zvolil programovací jazyk C# jako jeden z rodiny jazyků Microsoft .NET ve verzi 4.5. Výhodou tohoto jazyka je objektová orientace a možnost použít množství knihoven 3. stran například knihovnu pro práci se soubory Microsoft Excel.
Pro návrh uživatelského rozhraní (UI) jsem použil Windows Presentation Foundation (WPF), jakožto nástupce starší technologie Windows Forms. Ve WPF je graf objektů reprezentovaný jazykem XAML (Extensible Application Markup Language), ten umožňuje například propojení dat aplikace s grafickým zobrazením (tzv. databinding) a tato technologie výrazně ulehčuje samotné programování UI.

Jako moduly třetích stran jsem použil ClosedXML[9] a PropertyTools[10].
ClosedXML je volně dostupná knihovna pro práci s tabulkami Microsoft Excel. Je přímo navržena pro práci s objekty a umožňuje pohodlný export našich dat do tabulek Excelu.
PropertyTools je další volně dostupná knihovna takzvaných kontrol – ty se používají ve WPF pro grafické zobrazení dat a pro ovládání aplikace.

Zdroj dat

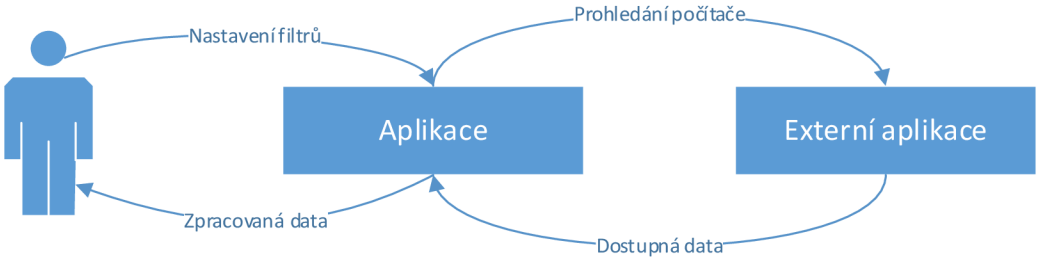
Jako zdroj dat pro navrhovanou aplikaci slouží sada programů společnosti NirSoft [11]. Jedná se o programy BrowserHistoryView, IECacheView, ChromeCacheView, MozillaCacheView a SkypeLogView (viz Kapitola 2.) Přestože lze tyto programy spustit samostatně, neumožňují vzájemné propojení pomocí filtrů.

Díky tomuto řešení je možné rozšířit funkce aplikace o možnost zobrazení dat z dalších zdrojů. Stačí, aby nový program pro skenování počítače umožňoval komunikaci přes příkazovou řádku, nebo aby bylo možné jeho chování definovat parametry a mezi-data uměl uložit do strojově čitelného formátu.

[9] http://closedxml.codeplex.com
[10] http://propertytools.codeplex.com
[11] http://nirsoft.net

4.3 Implementace

Obrázek 13 znázorňuje datové toky v aplikaci. Uživatel nastavuje filtry, které zpracovává aplikace a ta mu také zobrazí zpracovaná data. Druhý tok je mezi samotnou aplikací a externími programy. Aplikace si zažádá o data a odpověď následně zpracuje.

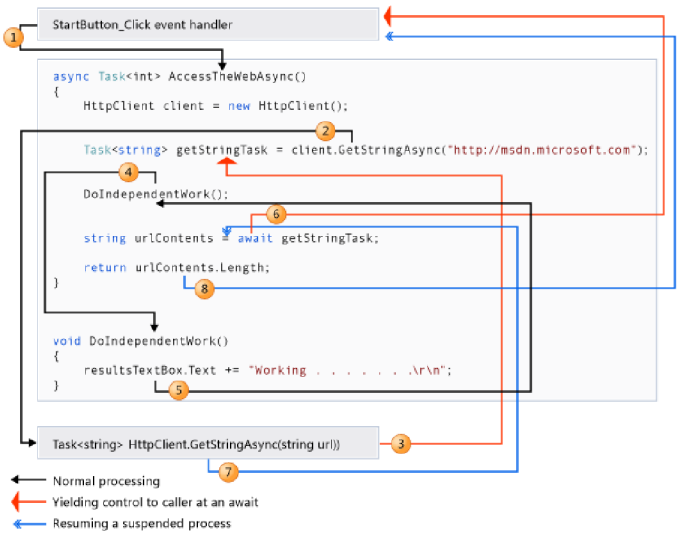


Obrázek 13 Schéma datových toků v aplikaci

Postupně je to ale řešeno tak, že nejdříve aplikace potřebuje získat data od jednotlivých programů popsaných výše. Toho je docíleno jejich asynchronním spuštěním s potřebnými parametry na pozadí. Externí programy předají všechna dostupná data přes dočasné XML soubory, ze kterých si pak aplikace data načte. Uživatel si v tomto kroku zvolí časové rozmezí dat, které chce z počítače získat.

Ve druhém kroku jsou všechna data zobrazena v přehledné tabulce. Na tuto tabulku je možné aplikovat filtr. Interně jsou všechna získaná data stále v paměti, takže je filtrování rychlé i když databáze obsahuje tisíce záznamů. V případě, že uživatel najde hledaná data, může si výsledek uložit do tabulek Excelu a předložit jako důkaz.

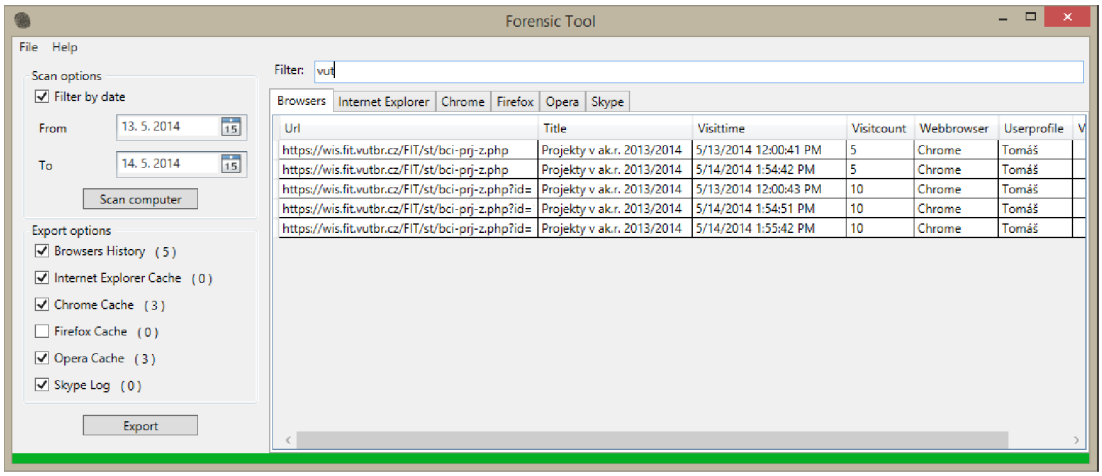
Důležitý faktor je, jak budou data zobrazena. Během implementace vzniklo několik návrhů uživatelského rozhraní a uspořádání výsledných dat. Při testování funkčnosti bylo vybráno to ergonomicky nejvýhodnější uspořádání, tak aby vyhovovalo zamýšlenému účelu.



Obrázek 14 Schéma datového toku await (převzato z[12])

Při implementaci nastal jediný problém, konkrétně bylo potřeba vyřešit asynchronní spuštění externích programů a po dokončení prohledávání počítače zpět načíst výsledky. Zároveň však bylo zapotřebí zachovat uživatelské rozhraní nadále

funkční. K tomuto účelu byla zvolena technologie .NET await/async. Jedná se o vysokoúrovňové asynchronní programování. Program je tedy přehledně strukturován a zdánlivě vypadá jako synchronní, veškerou práci totiž odvede na pozadí kompilátor. Jak vyplývá z obrázku 14, je v metodě AccessTaskWebAsync() zavolána asynchronní metoda GetStringAsync() během jejího zpracování na pozadí je možné provádět další nezávislý kód a až v případě potřeby návratu výsledku z metody GetStringAsync() se použije klíčové slovo await. Pokud mezi tím asynchronní metoda již doběhla, je okamžitě předán její výsledek a aplikace pokračuje dál synchronně, pokud ne tak se v tomto bodě na výsledek počká a zároveň kód odskočí zpět do vlákna, ve kterém běží uživatelské rozhraní (na obrázku znázorněno bodem 6). Po dokončení zpracování asynchronní metody (bod 7) je opět proveden skok z hlavního vlákna na místo await a aplikace může pokračovat běžným způsobem dál. [12]



Obrázek 15 Uživatelské rozhraní navržené aplikace

5 Praktická ukázka analýzy

V této kapitole bude popsán praktický postup analýzy důkazu a jeho evidence. Vzhledem k zaměření této práce se v této kapitole budu věnovat samotné analýze, nebude zde tedy řešen proces získávání a ověření důkazu (viz Kapitola 3). Testovací prostředí je vytvořeno ve virtuálním počítači s operačním systémem Windows 7. Pro ukázku je nainstalovaný software Skype – jako zástupce komunikátoru, Internet Explorer 11, Opera, Chrome a Firefox jako zástupci internetových prohlížečů a Mozilla Tunderbird, Outlook Express jako zástupci emailových klientů. Ukázková sestava reprezentuje počítač běžného uživatele, který působí mimo obor informačních technologií a svůj počítač používá pouze jako komunikační prostředek. Bude zde ukázána živá analýza – tedy v získávání informací bude řešeno přímo ze zajištěného počítače se zapnutým operačním systémem.

Příprava prostředí

Z komunikačních programů bylo odesláno několik zpráv (odchozích i příchozích, případně hlasových hovorů). Přičemž každá zpráva obsahovala unikátní řetězec, který se pak při forenzní analýze budu snažit najít a evidovat.

V internetových prohlížečích byly navštíveny náhodné weby, staženo několik soborů do výchozích adresářů i do uživatelem zadaných. V každém z prohlížečů byla sada navštívených webů jiná, viz následující tabulka.

Z emailových klientů bylo odesláno a přijato několik zpráv včetně příloh.

Cílem této ukázky je najít, analyzovat a evidovat všechny nastražené důkazy. Postup je zaznamenán na přiloženém CD.

Aplikace uvedených postupů

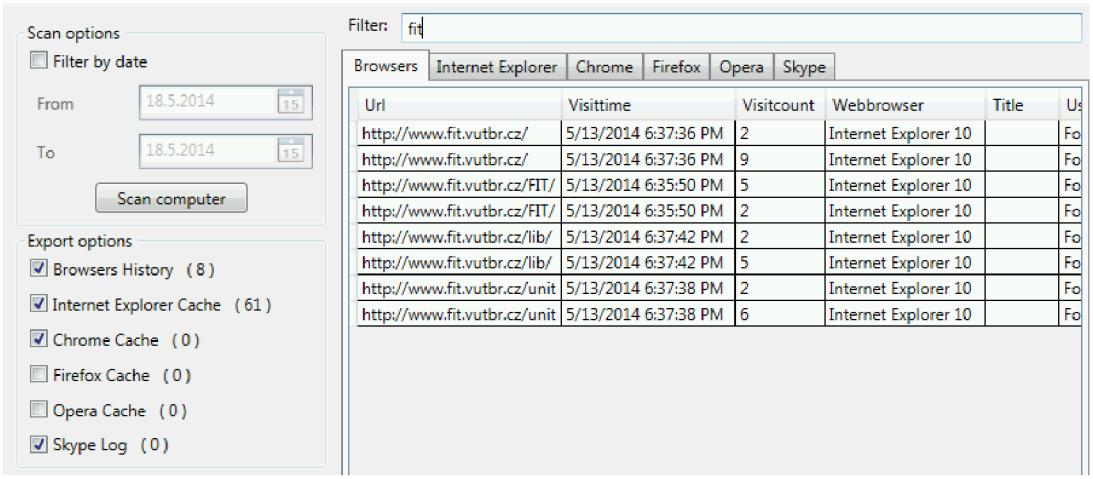
Pro demonstraci použijeme vytvořenou aplikaci. Po spuštění počítače postupně zjistíme, jaké internetové prohlížeče jsou v počítači nainstalovány. Navržený postup je nejdříve hledat spustitelné soubory ve výchozích adresářích, dále pak prohledat celý zbytek disku zda neobsahuje jména hledaných prohlížečů. To je jen pro případ, že by se prohlížeče nenacházeli v typickém umístění, v běžných případech je následně použitý software zjistit umístění sám. V ukázkovém případu byly nalezeny prohlížeče Internet Explorer ve verzi 11, Chrome 34, Opera 20 a Firefox 29. Stejným způsobem zjistíme, jaké jsou nainstalovány komunikátory. Náš demonstrační počítač má nainstalovaný Skype.

To znamená, že budeme moci použít náš program, ten všechny tyto prohlížeče a komunikátory podporuje.

Dalším krokem je nahrání naší aplikace do počítače. Aplikace není třeba instalovat, stačí rozbalit všechny soubory do námi zvoleného adresáře na disku. Po spuštění máme možnost specifikovat časové rozmezí, z kterého chceme získat data. Tato volba není povinná, a proto ji v ukázce nevyužijeme a rovnou klikneme na „*Scan computer*“.

Po vyhledání všech logů jsou tyto data rozčleněna do záložek podle jednotlivých zdrojů. Nyní můžeme použít filtr a tak například zjistit zda, uživatel počítače opravdu navštívil dané webové stránky, rsp. zda o tom existuje záznam. V našem případě budeme hledat stránky podle následující tabulky. Pokud bude o všem existovat záznam, můžeme prohlásit, že jsme správně odhalili, že daný uživatel webové stránky v minulosti navštívil.

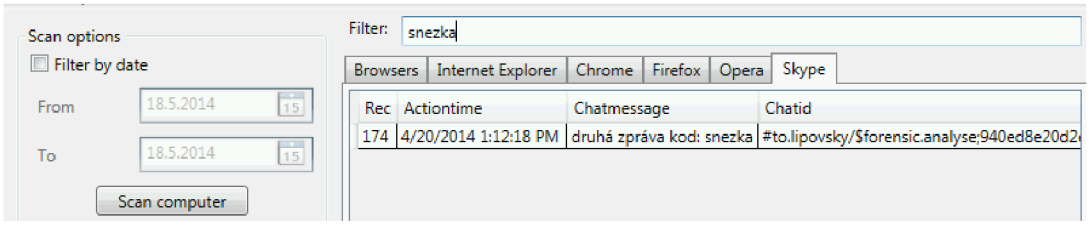
Internet Explorer	Chrome	Opera	Firefox
www.fit.vutbr.cz	www.zive.cz	www.randomsite.com	www.adobe.com



Obrázek 16 Výsledky prohledání PC s aplikovaným filtrem

V našem případě se všechny testované stránky povedly najít, výsledek je patrný z obrázku 16.

Dále budeme hledat záznam v logu Skype. Toto provedeme stejným způsobem jako u prohlížečů, na záložce *Skype*. Nyní budeme hledat, zda konverzace někdy obsahovala slovo „Snezka“. Z obrázku 17 opět vyplývá, že ve své konverzaci toto slovo uživatel použil.



Obrázek 17 Filtr aplikovaný na konverzace Skype

Naše vyfiltrované hledání můžeme uložit do tabulky formátu Excel pro pozdější použití například jako evidenci.

V posledním kroku zbývá pouze vše důkladně zaevidovat. Podle doporučení v kapitole 2.3 bude výstup vypadat přibližně takto:

Znalec	Petr Malec
Identifikátor případu / podací číslo	2014-001
Datum převzetí případu	10. 3. 2014
Případ předal	Jan Zeman
Účel zprávy	V analýze je třeba prokázat, že uživatel předaného počítače navštívil zadané webové stránky a dále zda existuje možnost, že daný uživatel použil při komunikaci slovo „snezka“.
Zpráva vytvořena pro	Okresní zastupitelství Brno
Stručný popis činu	Vyšetřovaná osoba je podezřelá z podávání úplatků. Z vyšetřování vyplývá, že krycí jméno pro předávání je „snezka“. Dále se předpokládá, že vyšetřovaná osoba hledala kontaktní údaje na webu univerzity, informace na zpravodajském serveru a na serveru společnosti Adobe.

Seznam dostupných důkazů

Důkaz	Způsob získání
Historie prohlížeče Internet Explorer	Analýza programem Forensic Tool
Historie prohlížeče Chrome	Analýza programem Forensic Tool
Historie prohlížeče Opera	Analýza programem Forensic Tool
Historie prohlížeče Firefox	Analýza programem Forensic Tool
Konverzace v logu Skype	Analýza programem Forensic Tool

Závěr:

Z provedené analýzy vyplývá, že vyšetřovaná osoba navštívila webové stránky www.fit.vutbr.cz, www.zive.cz, www.randomsite.com a www.adobe.com. Dále byla v počítači nalezena konverzace Skype mezi uživateli forensic.analyse (lokální uživatel) a to.lipovsky (příjemce). V konverzaci se vyskytlo klíčové slovo „snezka“.

Datum ukončení analýzy 5. 5. 2014

Podpis znalce ……..

6 Závěr

Z této práce je zřejmé, že forenzní analýzou se zabývá spousta odborníků IT. Každým dnem vznikají nové nástroje nebo úpravy nástrojů již hotových, tak aby co nejvíce napomáhaly při analýze, nebo samotném vyšetřování. Ve své práci jsem uvedl pouze pár aplikací, které se k analýze dají využít, nicméně většina z nich se liší pouze formou zobrazování výsledků a jiné funkcionalitě. Možnosti testovaných aplikací jsou i tak na dobré úrovni a dokáží získat z logů velké množství užitečných dat.

Profesionální kyberzločinec pravděpodobně dokáže důkladněji zahladit stopy po své komunikaci natolik, aby je forenzní analýza nedokázala rozpoznat. S velkou pravděpodobností ani nebude používat běžné komunikační nástroje. Navíc může používat lepší šifrování jak disku, tak síťového provozu. Proto je stále na čem pracovat, neboť jsou aplikace málo automatizované.

V běžných případech je počítač používán jen jako vedlejší nástroj k páchání jiné trestné činnosti, například běžným administrativním pracovníkem, nebo člověkem mimo obor informačních technologií. V těchto případech by však uvedené metody a postupy měly dostačovat. Vše totiž velmi závisí na použitých nástrojích ke komunikaci, prohlížení internetových stránek, práci se soubory apod.

Z kapitoly o srovnání a kapitoly popisující požadavky na forenzní analýzu je zřejmé, že získaná data jsou při vyšetřování velice užitečná. Pokud je při vyšetřování přístup k datům z počítače oběti, či podezřelého, tak lze velmi snadno rekonstruovat pohyb, jaké aktivity v daný čas na svém zařízení prováděl a to nejen prohlížení a přístup na jednotlivé webové stránky, ale také různou komunikaci prostřednictvím rychlých zpráv nebo emailu.

Možné rozšíření implementované aplikace spočívá v podpoře nových skenovacích nástrojů. V další verzi by také mohly být přidány nové možnosti filtrování – například podporou regulárních výrazů. Bylo by také možné zabudovat automatické generování zprávy.

7 Literatura

[1] BUI, Sonia, Michelle ENYEART a Jenghuei LUONG. Issues in Computer Forensics. In: [online]. 2003 [cit. 2014-10-01]. Dostupné z: http://www.cse.scu.edu/~jholliday/COEN150sp03/projects/Forensic%20Investigation.pdf

[2] SVETLÍK, Marián. Digitální forenzní analýza a bezpečnost informací. *Data Security Management* [online]. 2010, č. 1, s. 20-23 [cit. 2014-05-19]. Dostupné z: http://www.rac.cz/RAC/homepage.nsf/CZ/Clanky/$FILE/DSM-Digit%C3%A1ln%C3%AD%20forenzn%C3%AD%20anal%C3%BDza-01-2010.pdf

[3] CALOYANNIDES, Michael A. *Computer forensics and privacy*. Boston, MA: Artech House, 2001, xvii, 392 p. ISBN 15-805-3283-7.

[4] Forenzní zkoumání digitálních důkazů: příručka vyšetřovatele. *Risk Analysis Consultants* [online]. Praha, 2005 [cit. 2014-04-15]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/883AABB42333CB35C12570FC0034A328/$FILE/Guide%20051230.pdf

[5] *A Simplified Guide To Digital Evidence* [online]. c2000-2014, 22 s. [cit. 2014-04-11]. Dostupné z: http://www.crime-scene-investigator.net/SimplifiedGuideDigitalEvidence.pdf

[6] HOUŠKA, Jan. *Reakce na incidenty a forenzní analýza* [online]. České Budějovice, 2012 [cit. 2014-05-19]. Dostupné z: http://theses.cz/id/dq3g0c/. Bakalářská práce. JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH, Přírodovědecká fakulta.

[7] KADLEC, Josef. *Forenzní analýza unixových systémů* [online]. Hradec Králové, 2006 [cit. 2014-05-19]. Dostupné z: Josef Kadlec. Diplomová práce. UNIVERZITA HRADEC KRÁLOVÉ.

[8] NELSON, Bill. *Guide to computer forensics and investigations*. 3th ed. Boston: Course Technology, c2010, xxv, 682 s. ISBN 14-354-9883-6.

[9] ASHCROFT, John, Deborah J. DANIELS a Sarah V. HART. Forensic Examination of Digital Evidence: A Guide for Law Enforcement. *National Institute of Justice: Special report* [online]. 2004 [cit. 2014-05-19]. Dostupné z: https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

[10] BOIARKINE, Valentine, Ross CARTER, Laura CHAPPELL, Paul CULLIMORE, Thomas QUILTY a Paul SLATER. *Fundamental Computer Investigation Guide for*

Windows [online]. Microsoft, 2007, 60 s. [cit. 2014-05-19]. Dostupné z: http://go.microsoft.com/fwlink/?linkid=80345

[11] VYSKOČIL, Ladislav. *Zajišťování a analýza digitálních důkazů* [online]. Zlín, 2013, 105 s. [cit. 2014-05-19]. Dostupné z: http://dspace.k.utb.cz/handle/10563/24882. Diplomová práce. Univerzita Tomáše Bati ve Zlíně.

[12] Asynchronous Programming with Async and Await (C# and Visual Basic). In: *MSDN* [online]. c2014 [cit. 2014-05-19]. Dostupné z: http://msdn.microsoft.com/en-us/library/hh191443.aspx

Seznam příloh

DVD obsahující:

- zdrojový text této technické zprávy
- adresář s demonstračním postupem analýzy
- spustitelnou aplikaci
- zdrojové kódy aplikace
- programovou dokumentaci