Jihočeská univerzita v Českých Budějovicích

Přírodovědecká fakulta

Katedra Aplikované Informatiky

Analýza historie komunikace softwarového prostředku Skype

Analysis of communication history by Skype software

Bakalářská práce

Karel Novotný

Vedoucí závěrečné práce: Ing. Jaroslav Kothánek, Ph.D.

2013

Prohlašuji, že svoji bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích dne

Novotný K. (2013) Analýza historie komunikace softwarového prostředku Skype.
[Analysis of communication history by Skype software, Bc. Thesis, in Czech]. 25 p., Faculty of Science, University of South Bohemia, České Budějovice, Czech Republic.

Anotace

Tato bakalářská práce se zabývá analyzováním historie softwarového prostředku „Skype“. Práce se zaměřuje na analýzu, vyhodnocení způsobů a možností získání datových fondů a následnou realizaci aplikace, která slouží ke sběru a analýze těchto dat.

Abstract

This Thesis deals with analyzing the history of the software product „Skype“. The work focuses on the analysis, evaluation methods and access to data funds and subsequent implementation of an application that is used to collect and analyze this data.

Poděkování

Rád bych poděkoval vedoucímu práce Ing. Jaroslavu Kothánkovi, Ph.D. za jeho odborné připomínky a rady a dále bych chtěl poděkovat svojí rodině za trpělivost a psychickou podporu.

Obsah

1 Úvod

1.1 Zadání

Na základě potřeb forenzního zkoumání historie komunikace různých komunikačních prostředků vzniká potřeba pro orgány policie a forenzních znalců dokumentace chatové historie softwarového prostředku „Skype“. Zde je zejména zapotřebí provést analýzu datových souborů obsahující záznamy o kontaktech a historii komunikace na úrovni lokálního PC. Na základě získaných informacích o kontaktech je dále třeba provést analýzu možnosti získání identifikačních informací z portálu Skype.

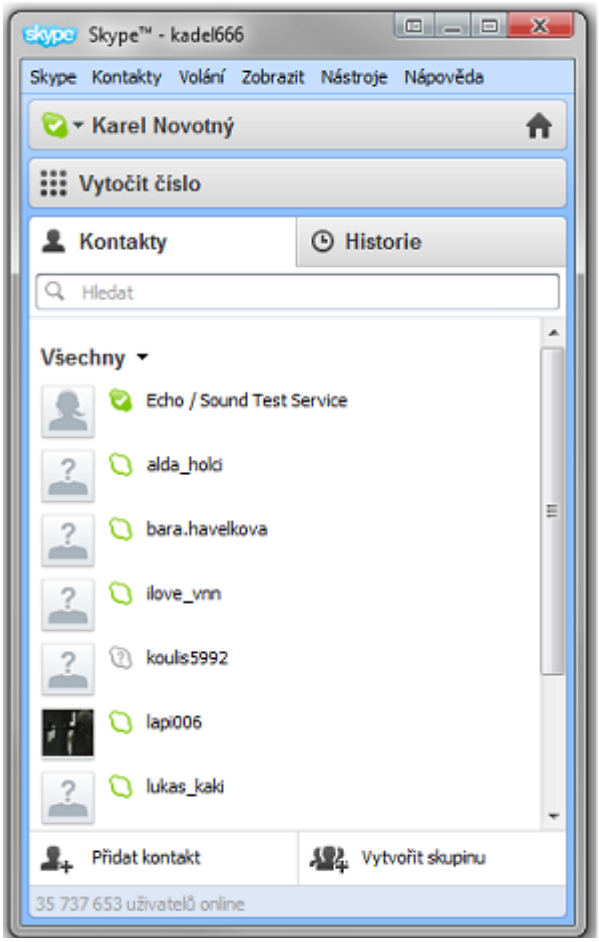
1.2 Cíle

Nejprve bude provedena analýza lokálních dat komunikačního prostředku Skype. Dále bude vyhodnocena možnost získání informací o uživatelských kontaktech a historii jejich komunikace v co možná největším rozsahu a na základě získaných informací bude provedena analýza možností, jak získat identifikační informace o uživatelích z portálu Skype. Na základě těchto analýz pak bude za pomoci jazyka C# napsán software na čtení a získávání informací softwarového prostředku Skype. Software bude moci získávat a zobrazovat kontakty, chatovou komunikaci, informace o uživatelově nastavení, záznamy o přenášených souborech, záznamy hlasové komunikace a video soubory. Na závěr bude otestována správná funkčnost vytvořené aplikace.

2 Softwarový prostředek Skype

2.1 Základní zjištění

Společnost Skype byla založena v roce 2003 Niklasem Zennströmem a Janusem Friisem. Za vývojem aplikace Skype stojí Estonians Ahti Heinla, Priit Kasesalu a Jaan Tallinn (Andreas Thomann. Skype - A Baltic Success Story.). Původní název projektu byl Sky peer-to-peer, který byl později zkrácen na Skype. V roce 2011 byla společnost odkoupena společností Microsoft a nyní tvoří oddělení Microsoft Skype Division. Skype má celosvětově více než 500 milionů registrovaných uživatelů (http://www.skype.com/intl/en-us/affiliate/). Aplikace využívá stejnojmenného protokolu (Skype). Protokol není veřejně dostupný a veškeré oficiální aplikace tento protokol využívající jsou pouze closed-source. Každý účet založený pomocí Skype má své unikátní ID, které slouží zároveň jako uživatelské jméno.



Ilustrace 1: Aplikace Skype

2.2 Základní funkce

Softwarový prostředek Skype umožňuje psanou, mluvenou i video komunikaci a také umožňuje přenos datových souborů.

2.2.1 Mluvená komunikace

Skype umožňuje jak komunikaci mezi jednotlivými uživateli, tak komunikaci mezi uživatelem a telefonem. Při komunikaci mezi uživateli existuje možnost konferenčního hovoru, kdy spolu hovoří více účtů najednou. Pro komunikaci směrem od telefonního zařízení je nutné získat za poplatek takzvané online číslo, které je unikátní a lze k němu určit konkrétní účet. Ke každému online číslu navíc uživatel získá hlasovou schránku.

2.2.2 Psaná komunikace

Skype podporuje skupinový chat až pro 150 uživatelů.

2.2.3 Video komunikace

Od verze 2.0 Skype umožňuje video hovory a od verze 5.0 navíc skupinové video hovory. Skype také nabízí možnost sdílení obrazovky.

2.2.4 Přenos datových souborů

Zasílání souborů pomocí Skype probíhá jako peer-to-peer, což znamená, že se soubor přenáší přímo mezi dvěma uživateli a není odesílán na server.

2.3 Lokální data

Ke zjištění cílového adresáře pro ukládání historie byl využit komerční software od společnosti Belkasoft – Belkasoft Skype Analyzer a to konkrétně volně stažitelná demo verze (demo verze umožňuje využívat program pouze po dobu deseti dní a navíc zobrazuje pouze omezenou hloubku historie, k odhalení umístění dat je ovšem dostačující). Logová data jsou ukládána do předdefinovaného souboru main.db, který se nachází v adresáři C:\Documents and Settings\[Profile Name]\Application Data\Skype\[Skype User] u Windows XP a nižší a C:\Users\[Profile Name]\AppData\Roaming\Skype\[Skype User] u Window Vista a vyšší. Data jsou ukládána pomocí databázového systému SQLite. Hlasová schránka (voicemail) je defaultně ukládána do C:\Documents and Settings\[Profile Name]\Application Data\[Skype User]\voicemail pro Windows XP a nižší a C:\Users\[Profile Name]\AppData\Roaming\Skype\[Skype User]\voicemail pro Windows Vista a vyšší. Skype od verze 4 k ukládání dat využívá databázový systém SQLite. Dále byl pomocí programu Skype Chatsync Reader, který je volně stažitelný na stránkách „itsecuritylab.eu“, nalezen adresář chatsync, ve kterém se nachází záznamy chatové historie uložené v souborech „.dat“. Ukládání historie je ovšem možné v nastavení programu Skype vypnout.

2.4 Databáze do verze 3

Historie před verzí 4 byla ukládána do speciální databáze, ve které byla data uložena v dnes již nepoužívaném formátu. K získání informací o této databázi byl využit dokument Skype Log File Analysis.

2.4.1 Soubory s daty

Uložené soubory mají vždy příponu ".dbb" a jejich název se skládá z řetězce, který popisuje obsah souboru, a čísla, které udává velikost záznamu (například call256.dbb, transfer512.dbb atd.). Ukládané soubory a údaje v nich obsažené jsou následující:

Hovory (např. call256.dbb)

- Časový údaj
- Uživatelské jméno
- Skype jméno
- Délka hovoru (v sekundách)

Přenos souborů (např. Transfer512.dbb)

- Uživatelské jméno
- Skype jméno
- Cesta k souboru
- Název souboru
- Velikost souboru
- Časový údaj

Zprávy (např. msg256.dbb nebo chatmsg256.dbb)

- Obsah zprávy
- Chat ID
- Časový údaj
- Uživatelské jméno
- Skype jméno

Uživatelské profily (např. user1024.dbb nebo profile1024.dbb)

- Uživatelské jméno
- Skype jméno
- Jazyk (2-znakový ISO kód)
- Město
- Kód státu (2-znakový ISO kód)
- Telefonní číslo
- Pracovní číslo
- Číslo mobilního telefonu
- Profilový obrázek

Hlasové maily (např. voicmail256.dbb)

- Uživatelské jméno
- Skype jméno
- Časový údaj
- Název souboru

2.4.2 Formát souborů

Data v uložená jednotlivých souborech se sice liší, ale struktura souborů je vždy stejná. Soubor vždy obsahuje pouze záznamy z oblasti, podle které je pojmenovaný (například soubor call*.dbb bude vždy obsahovat pouze záznamy hovorů). Číselné údaje jsou vždy uloženy ve formátu little-endian. Záznam vždy začíná hlavičkou, která je složena ze čtyř bytů a má tvar 0x6c, 0x33, 0x33, 0x6c (1331 v ASCII). Za hlavičkou následují čtyři byty, které určují délku následujících dat (údaj je opět ve formátu little-endian). Maximální délka

záznamu je obsažena již v názvu souboru, toto číslo tak bude stejné nebo menší (celková velikost souboru bude maximální délka záznamu + 8 bytů hlavičky). Mezi soubory je možné narazit i na soubory s prázdným záznamem. Takové mají sice hlavičku, ale udáj o velikosti dat je nulový. Soubory nemají žádný indikátor konce záznamu, prázdý prostor za daty je pouze vyplněn byty s hodnotou 0x00. Všechny záznamy týkající se komunikace mají své pořadové číslo, které určuje, v jakém pořadí jednotlivé události nastaly.

2.4.3 Časový údaj

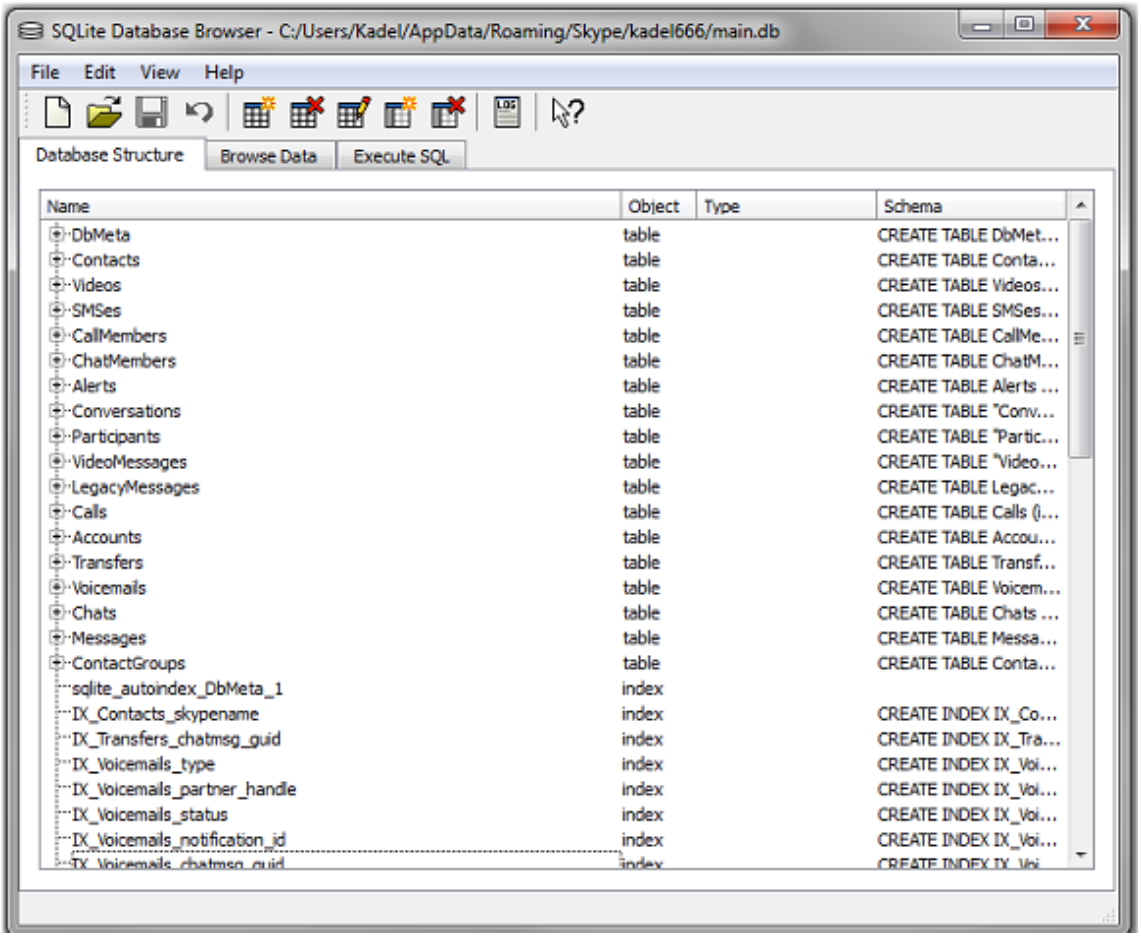
Časový údaj je ukládán ve standardním UNIXovém formátě (počet sekund od 1. 1. 1970). Údaj ovšem není reprezentován 4-bytovým integerem, jak je běžné. Místo toho používá 5-bytový formát, který vypadá následovně:

0000dddd 1ddddddd 1ddddddd 1ddddddd 1ddddddd

Odtržením úvodních nul a odstraněním bitu nejvyššího řádu s hodnotou jedna, získáme 32-bitový údaj, který lze sloučit do použitelného 4-bytového formátu.

2.5 Databáze od verze 4

Databáze je rozdělena do 18 tabulek a to DBMeta, Contacts, Videos, SMSes, CallMembers, ChatMembers, Alerts, VideoMessages, Conversations, Participants, LegacyMessages, Calls, Accounts, Transfers, Voicemails, Chats, Messages a ContactGroups. Data v jednotlivých tabulkách byla detailně prozkoumána pomocí nástroje SQLite Database Browser a bylo rozhodnuto, že podstatná a neredundantní data jsou v tabulkách Contacts, Videos, SMSes, CallMembers, Accounts, Transfers, Messages. Všechny tyto důležité tabulky budou detailně popsány dále.



Ilustrace 2: SQLite Database Browser

2.5.1 Contacts

Tabulka obsahuje seznam kontaktů a jejich informace. Nejdůležitější informací je pole skypename, které udává unikátní a neměnné jméno v aplikaci Skype. Tabulka dále může obsahovat detailní informace o účtech a to jméno, PSČ, datum narození, pohlaví, stát, město, telefonní čísla, e-mailovou adresu a domovskou stránku. Nutno však podotknout, že tyto údaje jsou nepovinné a jejich hodnoty se nemusejí zakládat na pravdě.

- Skypename: textový řetězec udávající skype jméno uživatele
- Fullname: textový řetězec udávající jméno uživatele
- Displayname: textový řetězec, který udává pod jakým jménem uživatele uvidí ostatní
- Birthday: číselný řetězec, který udává datum narození ve tvaru YYYYMMDD (první čtyři číslice udávají rok, další dvě měsíc a poslední dvě den)
- Gender: číslice, která udává pohlaví (1 znamená muž, 2 žena)
- Province: kraj, ve kterém má uživatel trvalý pobyt
- City: město uživatele
- Languages: textový řetězec udávající jazyk (ISO kód 639-1)
- Country: textová řetězec udávající kód státu (ISO kód 3166-1)
- Phone_home/office/mobile: telefon uživatele
- Pstnumber: telefonní číslo, které je použito v případě, kdy kontakt není uživatel Skypu, ale byl uložen jako telefonní číslo (atributy skypename a fullname budou prázdné)
- Emails: e-mailová adresa uživatele
- About: status uživatele
- Homepage: webová adresa uživatele
- Timezone: časová zóna, hodnota je vypočítána jako počet sekund od GMT[6] + 86400

2.5.2 Videos

Tabulka obsahuje především časový údaj a informace o zařízení, kterým byl záznam pořízen.

2.5.3 SMSes

Nachází se zde časový údaj, text zprávy, číslo z kterého byla zpráva odeslána a údaj o měně, v které bylo za službu zaplaceno.

- Target_numbers: textový řetězec určující, na která a případně ze kterých telefonních čísel byla SMS odeslána
- Body: text zprávy
- Timestamp: čas, kdy byla zpráva odeslána
- Type: číslo, které určuje jestli se jedná o příchozí (1) nebo odchozí (2) zprávu
- Price_currency: kód měny v ISO 4217
- Price: cena zprávy (celočíselný formát)
- Price_precision: přesná cena zprávy na několik desetinných míst
- Status: číslo určuje status zprávy - 6 znamená odeslanou a doručenou zprávu, 5 znamená nedoručenou zprávu, 3 je rozepsaná zpráva

2.5.4 CallMembers

Zde jsou především údaje o uskutečněných hovorech, a to časový údaj, informace o volaném účtu a délce hovoru.

- Call_name: textový řetězec udávající název hovoru
- Identity: skype jméno účastníka hovoru
- Dispname: textový řetězec udávající jméno účastníka hovoru, které se zobrazuje ostatním
- Call_duration: délka hovoru v sekundách (prázdný řetězec značí nepřijatý hovor)

- Start_timestamp: časová údaj určující, kdy uživatel přijal hovor
- Price_currency: ISO 4217 kód měny (hodnota se uloží v případě, že uživatel volal do zpoplatněné sítě)
- Price_precision: přesná cena na několik desetinných míst
- Price_per_minute: hodnota se ukládá ve stejném případě jako Price_currency, udává cenu hovoru za minutu (hodnota je ukládána v celočíselném formátu a je tedy nutné ji patřičně upravit)

2.5.5 Accounts

Informace v této tabulce se týkají všech účtů, které se z daného PC přihlašovaly. Je zde především Skype jméno účtu, časový údaj o posledním přihlášení, informace o časovém pásmu a informace o státu, z kterého bylo přihlášení provedeno. Dále tabulka obsahuje údaje, které vyplňuje uživatel sám, a to jméno, datum narození, město, pohlaví, jazyk, e-mail a telefonní čísla. Struktura tabulky a údaje v ní uložené jsou stejné jako u tabulky Contacts.

2.5.6 Transfers

V tabulce najdeme informace o uskutečněných přenosech dat. Jsou zde údaje o velikosti přeneseného souboru, časový údaj o začátku a konci přenosu, adresa, kam byl soubor ukládán a jméno uživatele, s kterým k výměně dat došlo.

- Partner_handle: textový řetězec udávající skype jméno uživatele, s kterým došlo k přenosu
- Partner_dispname: textový řetězec udávající pod jakým jménem uživatele uvidí ostatní
- Type: číslo 1 znamená příchozí přenos a číslo 2 odchozí
- Starttime: čas začátku přenosu
- Finishtime: čas konce přenosu (pokud je hodnota 0, přenosu byl neúspěšný)
- Filepath: cesta k odesílanému, popřípadě příchozímu souboru
- Filename: název souboru
- Filesize: velikost souboru v bytech (pokud je hodnota 0, jedná se o neúspěšný

příchozí přenos)

- Bytestrensferred: počet úspěšně přenesených bytů

2.5.7 Messages

Tabulka obsahuje informace o veškeré psané komunikaci, jako je chat nebo žádosti o autorizaci. Můžeme zde nalézt časový údaj, jméno partnera při komunikaci nebo text zprávy.

- Chatname: textový řetězec udávající název komunikace (díky němu lze vytvořit spojení mezi konkrétní zprávou a komunikací, ve které byla odeslána)
- Timestamp: časový údaj o odeslání zprávy (počet sekund od 1.1.1970)
- Author: skype jméno uživatele, který zprávu odeslal
- From_dispname: jméno uživetele, které se zobrazí příjemcům
- Chatmsg_type: číslo udávající typ zprávy
- Body_xml: tělo zprávy

2.6 Chatsync

V adresáři chatsync jsou soubory formátu ".dat", které softwarový prostředek Skype vytváří automaticky a do kterých je ukládána chatová historie. Adresář se nachází na stejném místě jako soubor main.db (viz kapitola 2.3). Chatsync slouží zřejmě k synchronizaci záznamů mezi uživateli pokud jeden z nich tyto záznamy nemá z nějakého důvodu přístupné (například je-li přihlášený z jiného počítače). Bez znalosti kódování je ovšem nemožné soubory číst. Po otevření v hex editoru je však možné nalézt alespoň některé informace. Dle Slavomíra Moroze (Nástroj pre analýzu logov aplikácie Skype) je formát souborů následující:

- Prvních pět bytů tvoří hlavička
- Číselné hodnoty jsou uložené jako unsigned integer ve formátu little-endian
- Čtyři byty, které následují po hlavičce udávají čas události. Jedná se o počet sekund od 1. 1. 1970 a hodnotu je potřeba číst odzadu
- Další čtyři byty (offset 0x09) udávají délku souboru od aktuální pozice
- ID komunikace se nachází na pozici 0x34 a je to řetězec ukončený nulovým znakem
- V textové komunikaci se před každou zprávou nachází dvojice bytů s hodnotou 0x03 a 0x02
- Zpráva je uložená v kódování UTF-8 a končí nulovým znakem

Všechny tyto skutečnosti se podařilo úspěšně ověřit a navíc byly zjištěny následující informace:

- 9 bytů za zprávou (od nulového bytu) následují 4 byty, které udávají čas odeslání zprávy
- 4 byty před dvojicí bytů 0x03 a 0x02 jsou pro každého uživatele vždy stejné a je z nich možné poznat, kdo zprávu psal

3 Vývoj softwarového prostředku

3.1 Současná řešení

V současnosti neexistuje žádná vědecká práce, která by uceleně řešila otázku forenzního zkoumání softwarového prostředku Skype v souvislostech a do takové hloubky, která je pro tuto problematiku nutná. Za alternativu lze považovat komerční software společností Belkasoft a Sanderson forensics, které ovšem nenabízejí hlubší pohled na věc a nehledají vazby a spojitosti nutné pro širší zkoumání.

3.2 Vývoj

3.2.1 Základní postup

Softwarový prostředek bude napsán v programovacím jazyce C#. Pro práci s databázemi, soubory a grafickým prostředím bude využito již existujících knihoven. Pro samotné psaní programu bude využito programovacího prostředí Microsoft Visual Studio 2008. Při tvorbě aplikace budou využity znalosti získáné z provedených analýz aplikace Skype.

3.2.2 Základní požadavky

Aplikace musí být především schopna otevřít databázové soubory a vyexportovat v nich uložená data, data dále odfiltrovat, vypočítat kontrolní sumu MD5 a vytvořit přehledný výstup. Dále bude napsána aplikace, která dokáže získávat data ze souborů chatsync.

3.2.3 Metodika vývoje

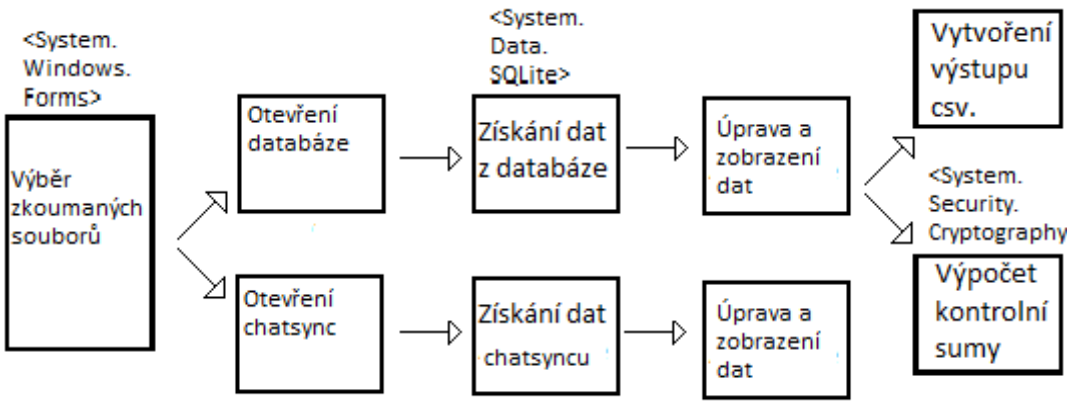
Pro vývoj softwaru bude využita agilní metodika, a to vývoj řízený vlastnostmi. Napřed byly tedy stanoveny jasné požadavky a cíle pro výslednou aplikaci, dále byly cíle rozděleny na jednotlivé funkční celky. Z těchto celků bude vytvořen model aplikace.
Z modelu budou nakonec navrženy třídy a jejich vazby, funkce a vlastnosti tak, aby byly splněny prvotní cíle a požadavky.

3.3 Implementace

3.3.1 Model

Model byl navržen za účelem snazšího vývoje aplikace. Model zobrazuje jednotlivé kroky, které bude aplikace vykonávat. Nad jednotlivými kroky jsou názvy knihoven, které jsou potřebné pro vykonávání některých funkcí.

V prním kroku aplikace otevře formulář vytvořený pomocí knihovny System.Windows.Forms, který se pokusí připojit k databázi. V případě, že zatím neexistuje cesta k databázi, otevře nový formulář, ve kterém uživatel pomocí grafického rozhraní cestu zvolí. Při vybírání souboru je defaultně nastaveno zobrazování pouze souborů s příponou „.db“. Toto nastavení lze ovšem změnit na zobrazení všech souborů pro případ, že přípona bude nestandardně pojmenována. Připojená databáze lze kdykoli změnit pomocí menu. Po připojení databáze dojde ke zpracování dat pomocí třídy SQLiteDatabase.cs, která využívá především knihovnu System.Windows.SQLite a umožňuje práci s jazykem SQLite. Po zpracování dat dojde k jejich zobrazení na datagrid. Veškeré časové údaje jsou upraveny tak, aby zobrazovali čas ve standardním formátu namísto času unixového, ve kterém jsou v databázi ukládány a který zobrazuje počet vteřin, jež uběhly od roku 1970. Datagrid zobrazuje vždy pouze jednu tabulku databáze, kterou lze kdykoliv změnit. Data zobrazená na datagridu lze kdykoli uložit pomocí menu jako soubor .csv. Pro ukládání byl vytvořen přehledný formulář, který se otevře po stisknutí tlačítka „Uložit logy“. Aplikace také umožňuje vypočítat kontrolní sumu MD5. Tato je vždy vypočítána z připojené databáze a její hodnota se jednak zobrazí pomocí messageboxu a navíc se uloží do schránky. Pomocí tlačítka „Chatsync“ lze otevřít nový formulář, který umožňuje otevřít soubory chatsyncu ukládané jako soubory s příponou „.dat“. Po otevření takového souboru je vypsáno ID chatu, čas chatu a text.



Ilustrace 3: Model funkcí

3.3.2 Typy tříd

Při vytváření programu byly použity různé typy tříd. Použity byly jednak třídy vytvářející instance, které reprezentují reálný objekt, jako je například kontrolní součet. Dále byly využity třídy grafické, které generují jednotlivé formuláře, s kterými bude uživatel pracovat. A v neposlední řadě byly vytvořeny třídy obsahující především algoritmy a výpočty nutné pro správný běh programu.

3.3.3 Třídy

Třída Zaklad.cs – Částečná třída třídy Form, která vytváří hlavní grafické rozhraní. Třída se stará jednak o zobrazování dat na datagridu a dále o propojení funkcí ostatních tříd. Třída využívá funkce třídy SQLiteDatabase.cs, tak aby mohla používat příkazy jazyku SQLite. Těchto příkazů používá ke zpracování dat z databáze a dále jejich zobrazení na datagrid. Dále třída zprostředkovává volání tříd Ulozeni.cs a KontrolniSoucet.cs, pomocí kterých dokáže informace zobrazená na datagrid ukládat jako soubor „.csv", respektive zobrazit kontrolní součet a uložit ho do schránky. Třída také zobrazuje grafické rozhraní, se kterým uživatel pracuje. Jednotlivé prvky formuláře byly vytvořeny pomocí designeru vývojového prostředí Microsoft Visual Studio.

Třída SQLiteDatabase.cs – Třída zprostředkovává připojení k databázi. Cesta k databázi je určena pomocí speciálního formuláře. Dále třída obsahuje metody, které umožňují komunikovat s databází pomocí jazyka SQLite. Tato třída byla stažena ze stránek www.dreamincode.net jako opensource a pro další práci byla upravena.

Třída Ulozeni.cs – Třída umožňuje ukládání dat zobrazených na datagridu. Pro určení cesty, kam bude výsledný soubor ukládat, využívá speciálního formuláře. Pomocí metody „Ulozit" pak třída umožňuje přepsat jednotlivé buňky datagridu do nově vytvořeného souboru „.csv“.

Třída KontrolniSoucet.cs – Třída se stará o výpočet kontrolního součtu MD5. Třída využívá knihovny System.Security.Cryptography a abstraktní třídy MD5, která obsahuje algoritmus pro výpočet hash kódu MD5. Cesta k souboru, z kterého se kontrolní součet vypočítává je získávána ze třídy SQLiteDatabase.cs a je stejná jako cesta k právě otevřené databázi.

Třída ChatsyncForm.cs – Částečná třída třídy Form, která vytváří grafické rozhraní pro čtení souborů chatsyncu. Umožňuje soubory otevřít a zobrazit potřebná data. Pro získání správných je nejprve celý soubor nahrán po jednotlivých bytech a následně dále upraven pomocí třídy HexString.cs. Jednotlivé prvky formuláře byly vytvořeny pomocí designéru vývojového prostředí Microsoft Visual Studio.

Třída HexString.cs – Třída zpracovává data souborů chatsync. Využívá řetězce bytů získaných ve třídě ChatsyncForm.cs a vyhledává v nich konkrétní byty, které značí např. začátek komunikace nebo časový údaj a dále tyto konkrétní byty upravuje do požadované formy.

Třída Program.cs – Statická třída, která obsahuje metodu Main.

4 Testy

Pro kontrolu správného chodu aplikace bylo využito jednak testovacích tříd jazyku C# a také uživatelských testů.

4.1 Testování

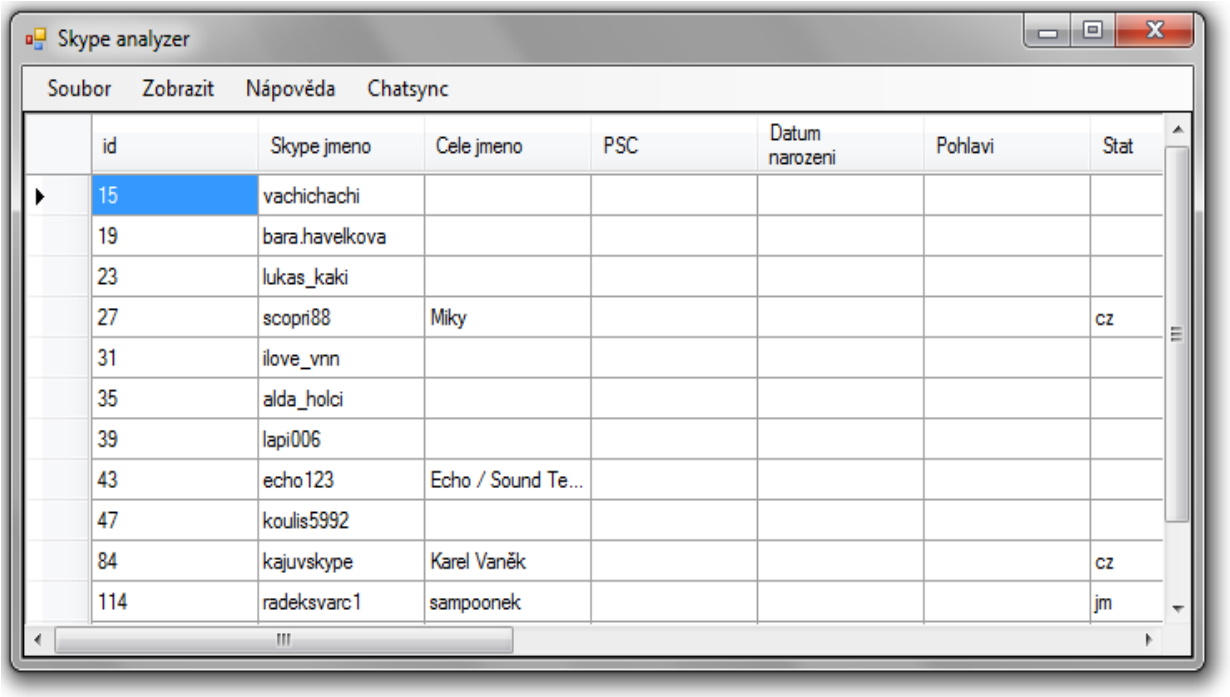
Testy připojování databáze – Cílem těchto testů bylo zjištění stavů aplikace v případě, že je připojována databáze s chybným formátem.

Testy ukládání výstupu – Testy bylo zjištěno, zda jsou soubory správně ukládány

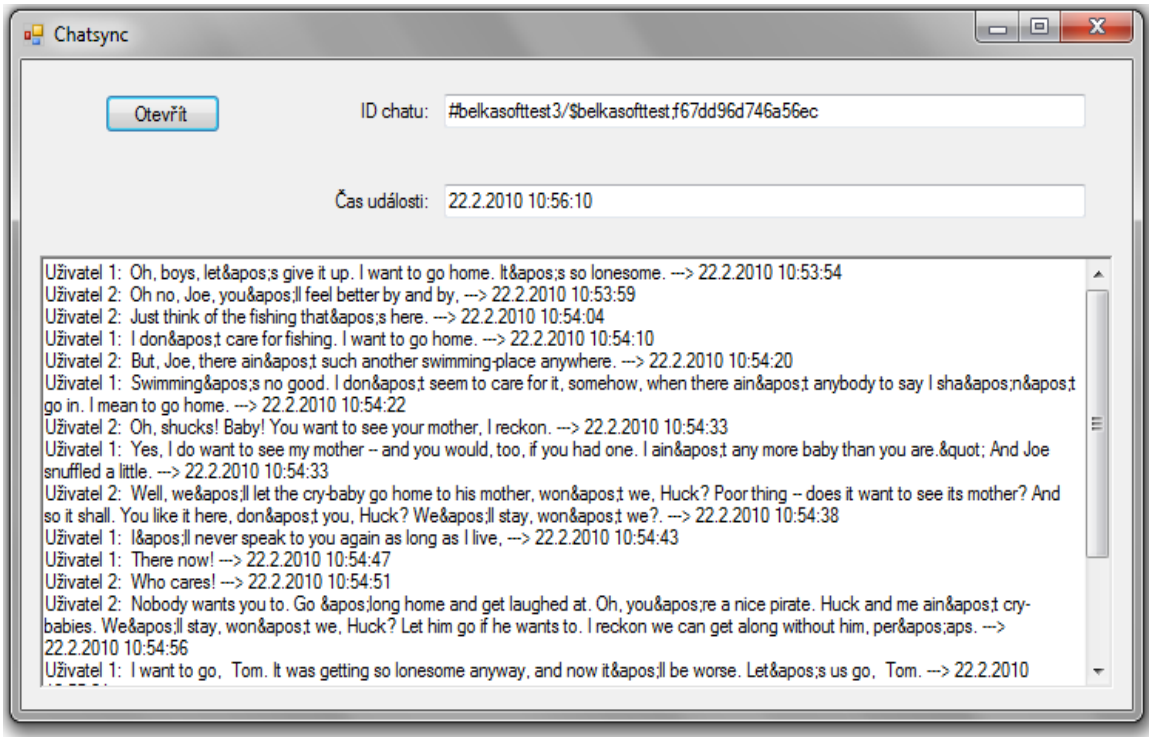
Testy výpočtů – Jde především o kontrolu správnosti výpočtu kontrolní sumy a výpočet časových údaju v souborech chatsync.

4.1.1 Uživatelské testy

Uživatelské testy byly provedeny především za účelem ověření správného chodu aplikace a jednotlivých prvků. Dále jimi bylo ověřeno, že s aplikací dokáže pracovat i osoba neznalá problematiky. Aplikace byla testována na různých verzích operačního systému Microsoft Windows a na několika odlišných počítačových sestavách. Pro testování bylo použito jak uměle vytvořených dat, tak dat vzniklých přirozeně. Testy byla potvrzena správná funkčnost aplikace.



Ilustrace 4: Výsledná aplikace (SQLite soubory)



Ilustrace 5: Výsledná aplikace (soubory chatsync)

5 Uživatelský manuál

5.1 Minimální požadavky

Pro spuštění aplikace musí počítač splňovat následující minimální požadavky:

- operační systém Microsoft Windows XP a vyšší
- procesor Pentium 2; 266MHz a více
- 128MB RAM a více
- 256MB volného místa na disku a více

5.2 Spuštění

Aplikaci lze spustit pomocí spouštěcí ikony Skype_analyzer.exe. Po spuštění aplikace se objeví hlavní formulář aplikace. Zde se nachází čtyři záložky.

- Soubor: umožňuje otevřít SQLdatabázi pomocí otevíracího formuláře (otevřít lze pouze databáze verze 4 a vyšší), uložit data zobrazená na datagridu jako soubor „.csv“ pomocí ukládacího formuláře, vypočítat kontrolní sumu z právě otevřeného souboru a zavřít aplikaci
- Zobrazit: umožňuje zobrazit jednotlivé tabulky právě otevřené databáze
- Chatsync: otevírá nový formulář, pomocí kterého je možné číst soubory chatsync
- Nápověda: umožňuje otevřít manuál aplikace

5.2.1 Otevření souboru SQLite databáze

Novou databázi je možné otevřít tlačítkem Soubor a Otevřít logy. Zde si uživatel může pomocí otevíracího formuláře zvolit soubor, který chce prohlížet. Defaultní cesta k souborům je C:\Documents and Settings\[Profile Name]\Application Data\Skype\[Skype User] pro Windows XP a nižší a C:\Users\[Profile Name]\AppData\Roaming\Skype\[Skype User] pro Window Vista a vyšší. Možné je ovšem i otevření databáze na jakémkoliv jiném umístění. Pokud je otevřena chybná databáze objeví se příslušné chybové hlášení.

5.2.2 Uložení zobrazených dat

Pomocí tlačítka Soubor a Uložit logy je možné uložit data zobrazená na datagridu. Po stistknutí příslušného tlačítka se otevře ukládací formulář, pomocí kterého je možné zadat cestu, kam se soubor uloží. Soubory jsou ukládány ve formátu „.csv“.

5.2.3 Kontrolní suma

Po stisknutí tlačítka Soubor a Kontrolní suma je vypočítána kontrolní suma MD5 z právě otevřené databáze. Tato suma se zobrazí na messageboxu a zároveň je uložena do schránky (pozor na přepsání dat, která se ve schránce nacházela).

5.2.4 Chatsync

Stisknutím tlačítka Chatsync se otevře nový formulář umožňující zkoumat soubory chatsync. Nový soubor je možné otevřít stisknutím tlačítka Otevřít. Defaultní cesta k souborům je C:\Documents and Settings\[Profile Name]\Application Data\Skype\[Skype User]\Chatsync pro Windows XP a nižší a C:\Users\[Profile Name]\AppData\Roaming\Skype\[Skype User]\Chatsync pro Window Vista a vyšší. Po otevření souboru je automaticky zobrazeno ID chatu, čas chatu a samotný rozhovor, který obsahuje jednak text a také čas odeslání zprávy.

6 Návrhy pro budoucí řešení

Vzhledem k průběhu vývoje aplikace a výsledkům uživatelských testů bylo zjištěno, že je možné aplikaci vylepšit nad rámec této práce.

- Podpora operačního systému Linux
- Podpora starších verzí databází (3 a nižší)
- Možnost získávání dat z mobilních zařízení
- Podpora jiných formátů výstupu
- Automatická detekce jednotlivých souborů databáze
- Automatická detekce jednotlivých souborů chatsync

7 Závěr

V bakalářské práci byla provedena analýza softwarového prostředku Skype. Tato analýza byla řádně zdokumentována a na jejím základě byly navrženy možnosti, jak získávat data potřebná pro forenzní zkoumání. Na základě navržených možností byla napsána aplikace, která byla otestována a zdokumenována.

7.1 Vyhodnocení

Všech vytýčených cílů bylo v práci úspěšně dosaženo. Aplikace splňuje všechny předem určené požadavky. Aplikace společně s analýzou dat představují zjednodušení v rámci potřeb čtení historie komunikace a získávání dalších datových fondů a znamenají zpřístupnění těchto možností i lidem neznalým problematiky. Aplikace tak může sloužit i pro osobní účely, například při potřebě číst historii i bez přístupu do samotného klientu Skype nebo při potřebě zálohovat vlastní data.

8 Použitá literatura

[1] Andreas Thomann. Skype - A Baltic Success Story ©2006 [cit. 14-11-2012] (https://infocus.credit-suisse.com/app/article/index.cfm?fuseaction=OpenArticle&aoid=163167&coid=7805&lang=EN)

[2] Skype and/or Microsoft ©2012 [cit. 14-11-2012] (http://www.skype.com)

[3] Belkasoft – Forensic and system software tools ©2002 – 2012 [cit. 14-11-2012] (http://forensic.belkasoft.com/en/)

[4] Ing. Jaroslav Kothánek, Ph.D – Znalecká detektivní kancelář [cit. 14-11-2012] (http://www.it-znalec.cz/)

[5] Sanderson forensics ©2012 [cit. 14-11-2012] (http://www.sandersonforensics.com)

[6] Luboš Ptáček - Analysis and detection of Skype network traffic ©2011 [cit. 14-11-2012] (http://is.muni.cz/th/143199/fi_m/ms_thesis.pdf)

[7] Bc. Tomáš Hajdin – Agilní metodiky vývoje software ©2005 [cit. 14-11-2012] (http://is.muni.cz/th/39440/fi_m/dp.pdf)

[8] Dream.In.Code ©2010 [cit. 14-11-2012] (http://www.dreamincode.net/forums/topic/157830-using-sqlite-with-c%23/)

[9] Ronald C Dodge, JR. - Skype Fingerprint ©2008 [cit. 14-11-2012] (http://csdl2.computer.org/comp/proceedings/hicss/2008/3075/00/30750484.pdf)

[10] Skype Log File Analysis (http://cryptocomb.org/Skype%20Log%20File%20Analysis.pdf)

[11] Slavomír Moroz - Nástroj pre analýzu logov aplikácie Skype (http://is.muni.cz/th/325335/fi_b/BP.pdf)

9 Přílohy

[1] CD obsahující aplikaci, zdrojové kódy a elektronickou kopii této práce