Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta
Katedra Aplikované Informatiky

Analýza historie komunikace softwarového prostředku ICQ

Analysis of communication history by ICQ software

Bakalářská práce

Michal Prenner

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

2012

Prohlášení

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 přístupně části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejich 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

Prenner M. (2012) Analýza historie komunikace softwarového prostředku ICQ.

[Analysis of communication history by ICQ software]. - 30 p. (počet stran), Faculty of Science, The University of South Bohemia, České Budějovice, Czech Republic.

Anotace

Tato bakalářská práce se zabývá analyzováním historie softwarového prostředku „ICQ“. 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 "ICQ". 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 této práce Ing. Jaroslavu Kothánkovi, Ph. D., za ochotu konzultace a odbornou pomoc při realizaci práce.

Obsah

1 Úvod a cíle práce

1.1 Úvod

Na základě potřeb forenzního zkoumání historie komunikace různých komunikačních prostředků vzniká potřeba pro orgány policie a forenzních znalců dokumentace chatové historie softwarového prostředku „ICQ“ za účelem získání informací a důkazních materiálů, které mohou pomoci usvědčit již stíhané osoby, případně pomoci osvětlit skutečnosti vedoucí k odhalení osob porušujících zákon. Je zejména zapotřebí provést analýzu datových souborů obsahující záznamy o kontaktech a historii komunikace na úrovni lokálního PC. Na základě získaných informací o kontaktech je dále třeba provést analýzu možnosti získání identifikačních informací z portálu ICQ.

1.2 Cíle práce

V prvé řadě je potřeba důkladné analýzy lokálních dat komunikačního prostředku ICQ. Na základě znalosti zdrojů těchto dat lze vyhodnotit možnosti získání informací o uživatelských kontaktech a historii jejich komunikace v co možná největším rozsahu. Za pomoci získaných informací je potřeba provést analýzu možností získání identifikačních informací o uživatelích z portálu ICQ a souborů uložených na disku v kontextu s těmito údaji. Účelem práce bude vytvořit ucelený a řádně zdokumentovaný výstup datových fondů z lokálních a externích úložišť za pomoci vytvořeného softwaru, který bude automatizovaně vytvářet kompletní a přehledný výstup veškerých dostupných informací. Na závěr práce bude provedeno řádné otestování, ověření výsledků zkoumání a funkčnosti vytvořené aplikace. Rozbor softwarového prostředku ICQ

1.3 Stručný popis

1.3.1 Základní poznatky

Předmětem zkoumání bude program ICQ (zkratka anglického „I Seek You“) ve verzi 7.0 až 7.7 určené pro operační systémy Microsoft Windows XP/Vista/7 sloužící primárně k textové komunikaci přes internet. Tento program pracuje s komunikačním protokolem OSCAR. K tomuto protokolu je veřejně k dispozici pouze neoficiální dokumentace s popisem jeho struktury. ICQ má uzavřený vývoj a vydělává zobrazováním reklam. Ke stažení a používání je zdarma. Programem lze zasílat datové soubory, které jsou následně automaticky ukládány do složky účtu uživatele. Dále je schopen na základě volby uživatele v nastavení ukládat do lokálního úložiště historii veškeré komunikace a seznam kontaktů, se kterými byla prováděna komunikace. Defaultní[1] nastavení ukládání historie se liší v jednotlivých verzích programu.

1.3.2 Vývoj

Program byl vyvinut izraelskou firmou Mirabilis a vydán v roce 1996. Nynější vlastníkem je firma AOL, která v roce 1998 firmu Mirabilis koupila.

1.3.3 UIN

Uživatelé ICQ jsou identifikování devítimístným číslem zvaným UIN, toto číslo se uděluje v pořadí od nuly. Od verze ICQ 6.0 se uživatelé mohou přihlásit zadáním e-mailové adresy, která je zadána při registraci ICQ.

1 Defaultní - Výchozí, přednastavené.

1.3.4 Licence

Registrací ICQ účtu uživatel souhlasí, že četl a že respektuje všechny tyto dokumenty, ve kterých mimo jiné stojí [3]:

- ICQ se nesmí používat, pokud uživatel není starý alespoň 13 let.
- Z oficiální aplikace se nesmí odstraňovat reklamy.
- ICQ protokol může být kdykoli upraven, nebo ICQ síť zastavena bez jakéhokoli varování.
- ICQ se nesmí používat pro jinou než soukromou potřebu (např. firemní komunikace je proti podmínkám používání).
- pokud je chyba v nějakém překladu podmínek do jiného jazyka, AOL za to nenese odpovědnost (tj. souhlasíte s anglickou verzí podmínek).
- ICQ sice nesleduje data uživatelů, ale má právo je prodat.

1.3.5 Základní funkce

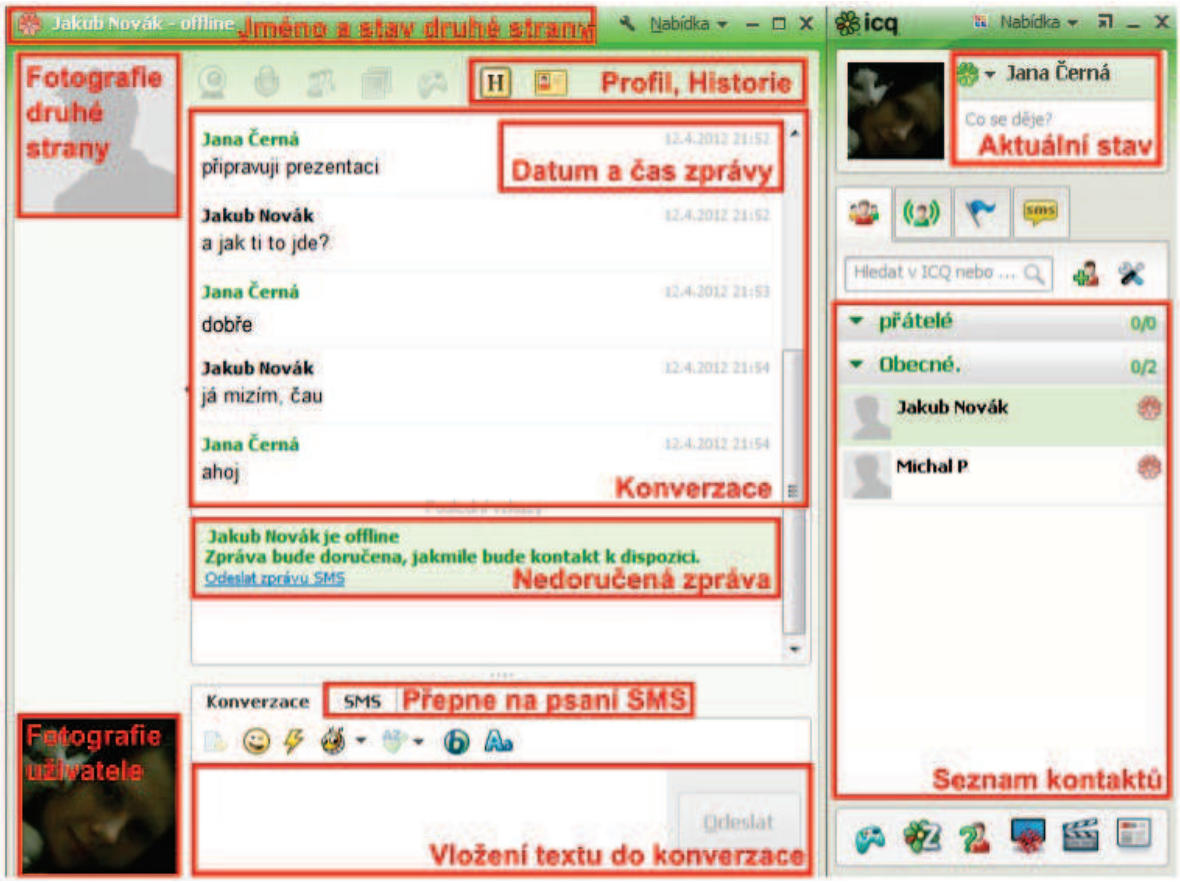
Mezi základní funkce programu řadíme:

- Schopnost přijímat a odesílat textové zprávy v reálném čase.
- Zjistit dostupnost ostatních uživatelů programu.
- Odesílat a přijímat datové soubory.
- Ukládat historii veškeré komunikace.
- Ukládat seznam kontaktů a dělit je do skupin.
- Ignorovat nežádoucí kontakty.
- Provádět hlasovou komunikaci.
- Provádět skupinovou textovou komunikaci.
- Odesílání SMS zpráv.

1.4 Analýza základních funkcí ICQ

1.4.1 Přijímání a odesílání textových zpráv v reálném čase

Přijímání a odesílání zpráv v reálném čase, neboli tzv. Instant Messaging umožňuje uživateli v reálném čase odeslat a přijmout zprávu s jiným, ve stejné době připojeným uživatelem na síti ICQ. V případě nedostupnosti uživatele je zpráva uložena na databázovém serveru provozovatele ICQ a odeslána cílenému uživateli při následujícím připojení na síť. Uživatelé jsou navzájem identifikováni unikátním identifikátorem UIN složeným z devítimístné číselné kombinace, který jednoznačně odlišuje jednotlivé účty. Navenek však uživatel primárně vystupuje pod zvolenou přezdívkou (jménem), také zvanou nickname. Ta už unikátní není. Od ICQ verze 7.0 je veškerá komunikace přeposílána na všechna připojená zařízení na stejném účtu v jednom okamžiku. Lze tedy v případě, že je uživatel připojen na více zařízeních ve stejné době přijmout zprávu na všech zařízeních současně. V případě starších verzí bylo povoleno souběžné připojení pouze jednoho zařízení na jeden účet.



Obrázek 1: Vyobrazení příkladu a popisu komunikace za pomocí klienta ICQ verze 7.x

1.4.2 Zjišťování dostupnosti ostatních uživatelů programu

Díky programu jsme schopni zjistit aktuální dostupnost (status) uživatelů ze seznamu kontaktů zkoumaného uživatele. Tento aktuální stav nelze zjistit z lokálních úložišť. Samotný program tuto informaci upravuje a zobrazuje v reálném čase dotazem na server, který systém ICQ řídí. Není známo, že by tyto stavy jakkoliv zaznamenával. Z tohoto poznatku vyplývá, že tyto informace jsme schopni získat pouze z portálu www.ICQ.com.

1.4.3 Odesílání a přijímání datových souborů

Za pomoci klienta jsme schopni přijmout libovolný datový soubor neomezené velikosti. V případě příjmu je soubor následně uložen do složky uživatele umístěné na adrese: ..*\Documents\ICQ\ReceivedFiles* v podsložce obsahující UIN a nickname odesílatele Např. *\<UIN jméno uživatele\<Jméno souboru>*. Odesílání a přijímání souborů je podmíněno dostupností obou uživatelů. Je tedy možné vycházet z předpokladu, že pokud mezi uživateli došlo k výměně souborů, byly dostupni na síti ve stejnou dobu. Při zasílání a odeslání souboru je ve stejném čase zaslána obou zúčastněným zpráva o přenosu souboru. Tato zpráva je uložena do historie. Tyto zpráva neobsahuje bližší informace o přenášeném souboru. V případě že je uživatel příjemcem a soubor přijme, je soubor následně automaticky uložen do složky uživatele. V případě, že se daný soubor na původním místě disku stále nachází, jsme schopni o něm zjistit veškeré dostupné informace.

1.5 Analýza datových fondů

1.5.1 Základní hierarchie dat

Data jsou ukládána do předdefinované složky umístěné v případě operačních systémů Windows 7/Vista na adrese:

<Oddíl>:\Users\<Jméno uživatele>\AppData\Roaming\ICQ

V případě české verze operačního systému Windows XP na adrese:

<Oddíl>:\Documents and Settings\<Jméno uživatele>\Data aplikací\ICQ

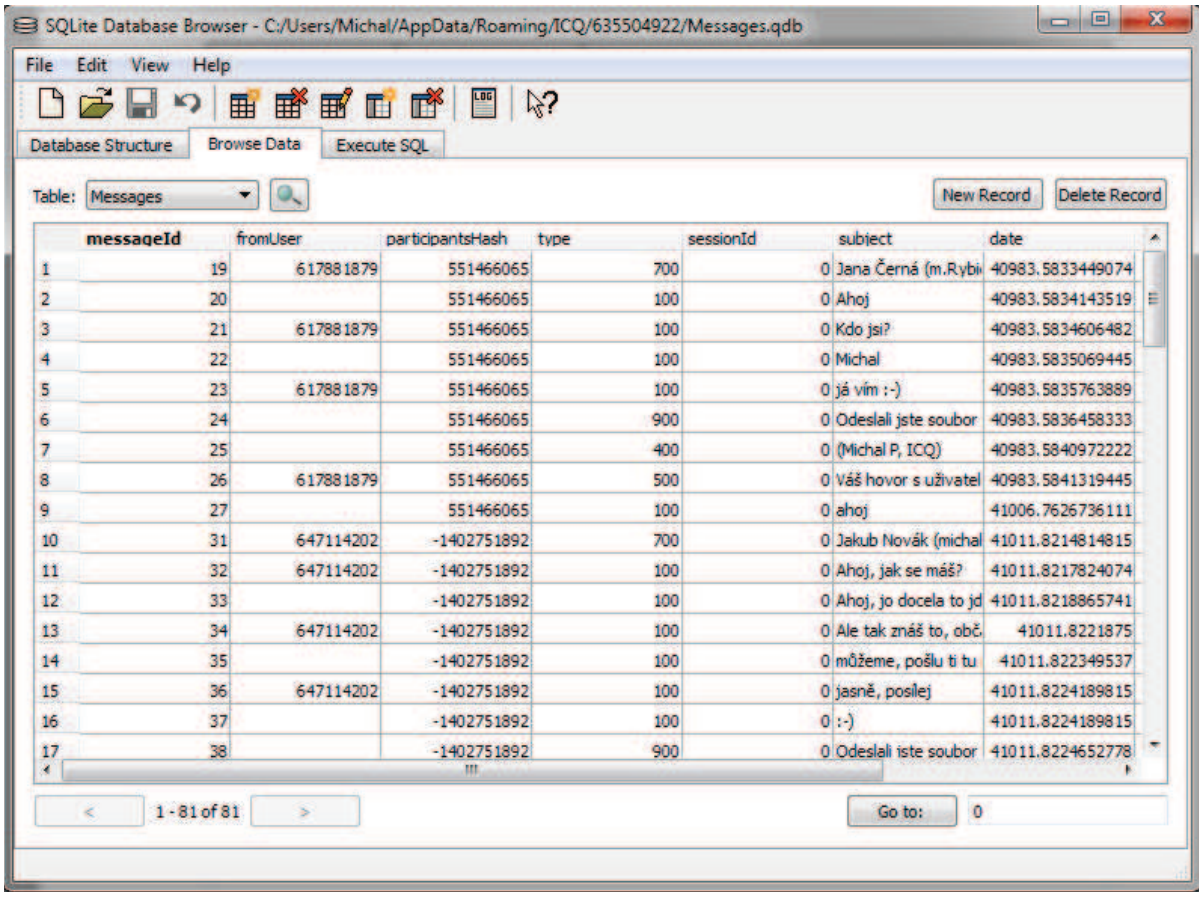
V tomto datovém úložišti lze najít po bližším určení databázové soubory s veškerými potřebnými informacemi. *Oddílem* je myšlen oddíl disku, na kterém program ICQ byl používán. *Jméno uživatele* je označení uživatele systému, pod kterým byl program ICQ používán.

Z lokálních úložišť lze získat tyto data:

- Seznam kontaktů zkoumaného uživatele.
- Historii komunikace (čas a obsah přijímaných a odesílaných zpráv).
- Historii odeslaných a přijatých souborů (velikost, název, datový typ souborů).

1.5.2 Metodika práce s daty

Z koncovky názvu databáze lze v případě verzí ICQ 7.0 až ICQ 7.7, která je označena jako „qdb“ určit, že zkoumaná databáze je typu SqlLite. Databáze byla zkoumána za pomocí volně dostupného softwarového prostředku *SQLite Database Browser verze 2.0b1*. Díky zkoumání za pomoci výše uvedeného programu lze identifikovat funkci a účel jednotlivých datových fondů.



Obrázek 2: Zobrazení využití programu SQLite Database Browser.

1.5.3 Analýza struktury lokální databáze

S užitím výše zmíněného softwaru a s výše uvedenou znalostí umístění databázových souborů v případě verze ICQ 7.0 -7.7 byla zjištěna následující struktura dat. Rozbor databáze Messages.qdb byl vyhotoven v tabulce označené *Tabulka 1*. Rozbor databáze Owner.qdb byl vyhotoven v tabulce označené *Tabulka 2*.

Jméno tabulky	Jméno sloupce	Význam
Messages	*messageId*	Unikátní identifikátor zpráv.
	fromUser	UIN odesílatele zprávy, v případě, že je odesílatelem zkoumaný uživatel, hodnota je nastavena na hodnotu null.
	participantsHash	Hash[2], jehož hodnota je identifikátorem účastnících se uživatelů v diskuzi (tento údaj je důležitý především v případě skupinové konverzace).
	type	Tento údaj blíže definuje typ zprávy. Byly zjištěny následující významy hodnot. 100 – Textová zpráva, 300 – Odeslaná animace, 400 – Odeslaná SMS zpráva, 500 – Oznámení o hlasové komunikaci, 600 – Zmeškaný hovor, 700 – Výzva k přidání uživatele, 900 – Oznámení o odeslání/přijmutí souboru, 1100 – Oznámení o hraní ICQ her
	subject	Samotný text zprávy.
	date	Číselná hodnota značící čas odeslané zprávy (údaj udává počet dnů od 1.1 1990) .
	sessionId, read, data	Tyto sloupce nebylo možné za pomocí zkoumání určit, jejich data nenesou žádnou hodnotu pro forenzní zkoumání.
sqllite_sequence	*name*	Odkazuje na tabulku, ve které je uložen záznam.
	seq	Odkazuje na identifikátor tabulky ze záznamu name odkazující na údaj o provedeném hlasovém hovoru.
Users	*userId*	UIN uživatele uvedeného v listu kontaktů, zároveň slouží jako unikátní identifikátor uživatele.
	name	Uživatelské jméno uživatele (tzv. nickname) příslušného UIN, tento údaj není unikátní.
Participants	*participantsHash*	Suma označující příslušnost do určité skupiny účastníku konverzace.
	userId	UIN uživatele účastnícího se konverzace.

Tabulka 1: Rozbor databáze Messages.qdb.

2 Hash – Kontrolní otisk (signatura) souboru.

Jméno tabulky	Jméno sloupce	Význam
Users	*key*	Obsahuje UIN uložených kontaktů. Jeden záznam může být uložen ve více řádcích, každý odkazující do jiné sekce, se kterou program ICQ pracuje.
	section	Obsahuje odkaz na sekci uložení kontaktu.
	data	Data o uložených kontaktech v nezjištěném formátu.
Records		Obsahuje dále nezjištěné informace o přihlášeném uživateli. Z bližšího zkoumání nebylo možné data identifikovat a určit funkci této tabulky.

Tabulka 2: Rozbor databáze Owner.qdb.

2 Rozbor portálu www.ICQ.com

2.1 Stručný popis

2.1.1 Základní poznatky

Portál www.ICQ.com je provozován serverem, který celý systém ICQ řídí. Díky centrálnímu zpracování komunikace na základě protokolu OSCAR, který server využívá, je možné využít ke komunikaci i jiný software od konkurenčních společností pro komunikaci po síti ICQ. Na tomto serveru jsou ukládány uživatelské účty a veškeré informace o profilech uživatelů. Z tohoto poznatku vyplývá, že i po smazání lokálních dat je účet se všemi informacemi o uživateli zachován. Díky webovému rozhraní je možné po zadání příslušného dotazu na např. přezdívku zkoumaného uživatelského účtu zjistit důležité veřejné profilové informace.

2.1.2 Základní funkce

Mezi základní funkce portálu řadíme:

- Řízení systému ICQ.
- Ukládání uživatelských účtů.
- Možnost zobrazit veřejné informace o profilech uživatelů (např. věk, pohlaví, stát uživatele a profilové fotografie).
- Možnost za pomoci online rozhraní komunikovat s lokálně nainstalovanými softwarovými klienty.
- Poskytnout uživatelskou podporu a základní informace o programu.
- Možnost stažení softwarového klienta pro platformy Windows, MAC, Linux a pro Mobilní zařízení.
- Registrace nových uživatelů.

2.2 Analýza funkcí portálu www.ICQ.com

2.2.1 Funkce hledání lidí

Na portálu je k dispozici online aplikace “Hledání lidí”. Bylo zjištěno, že díky této aplikaci lze získat veřejné profilová data o uživatelích. Z níže uvedeného příkladu na *Obrázku 2* ukazující data smyšleného profilu lze vypozorovat, že jsme schopni se znalostí UIN, které lze získat z lokální databáze zkoumaného profilu získat následující data.

- Přezdívku (povinné).
- Pohlaví (povinné).
- Aktuálně.
- Den narození (povinné).
- Adresa.
- Číslo ICQ (UIN) (povinné, na základě UIN je uživatel vyhledán, jedná se tedy o již známou informaci).
- Sítě.
- Web stránka.
- Zájmy.
- Jazyky.
- Kartu „O mě“.
- Fotografii uživatele.

Obrázek 3: Ukázka zobrazení profilových informací na portálu www.ICQ.com

Informace lze získat pouze za předpokladu, že byly uživatelem vyplněny. S jistotou se dají se na výstupu očekávat pouze povinné údaje, které vyžaduje registrace do programu ICQ. Pokud však dojde k registraci z jiného než oficiálního softwarového klienta, jenž síť ICQ využívá, nelze zaručit s jistotou ani tyto informace (např. den narození, pohlaví). Profilové informace se mohou měnit v závislosti na změně, kterou na svém profilu provedl zkoumaný uživatel.

2.2.2 Funkce Web-ICQ

Web-ICQ je online formou klasického softwarového klienta, jehož zkoumání je náplní této práce. Jedná se o klienta spouštěného za pomocí internetového prohlížeče a internetově založeného programu Adobe Flash, který je potřeba mít ve svém počítači předinstalovaný. Web-ICQ lze bez jakékoliv instalace spustit, přihlásit se na svůj účet a uskutečňovat textovou komunikaci se svými kontakty, případně nové kontakty vytvářet. Samotný program obsahuje omezenou funkčnost oproti klasickému klientu. Z mnoha rozdílů je třeba zmínit např. nemožnost ukládání historie, která je předmětem této práce a nemožnost posílat soubory. Program slouží výhradně k textové komunikaci, a jelikož není schopen dlouhodobě uchovávat záznamy komunikace, neposkytuje v současné verzi jakákoliv přínosná data této práci.

2.2.3 Funkce Chat

Portál www.ICQ.com mimo jiné také nabízí možnost skupinového chatu nezávisle na síti klasického ICQ. Rozdělení uživatelů jenž spolu komunikují je tvořené za pomocí tzv. místností, do kterých se uživatelé přihlašují, aby mohli hromadně komunikovat. Tyto místnosti jsou tříděné podle zájmu, místa, životního stylu apod. Tím uživateli nabízí možnost se snadno setkat a komunikovat lidmi podobných zájmů. Tato aplikace je provozována pouze na portále ICQ a jediná spojitost s klasickým systémem ICQ,jenž je předmětem této práce je použití stejných profilových informací. Tedy za pomoci již vytvořeného účtu ICQ, se lze přihlásit do tohoto chatu.

2.2.4 Ostatní funkce

Portál ICQ disponuje dalšími funkcemi, jako je např. podpora a možnost si stáhnout nejaktuálnější verzi programu ICQ, hrát online hry apod. Pro předmět této práce však tyto funkce a informace nejsou přínosné a proto není nezbytné je podrobit bližší analýze.

2.3 Analýza datových fondů

2.3.1 Základní hierarchie dat

Z výše popsané analýzy vyplývá, že za pomocí aplikace „Hledání lidí“ jsme schopni získat veřejné profilové informace uživatelů, se kterými byl zkoumaný subjekt v kontaktu a i informace o zkoumaném uživateli samotném.

Díky těmto znalostem bylo provedeno zjištění o funkčnosti tohoto rozhraní a následné možnosti získání dat. Pro zobrazení informacích o uživateli je potřeba navštívit adresu *www.icq.com/people/<UIN zkoumaného uživatele>*. Z toho vyplývá, že za pomoci znalosti UIN, které jsme schopni zjistit analýzou lokálních dat, jsme schopni jednoznačně najít požadovaný profil a podrobit ho bližšímu zkoumání.

2.3.2 Metodika práce s daty

Informace poskytované serverem lze získat formou HTML[3] kódu. Je tedy nutné po zadání dotazu na portál (v případě jeho dostupnosti) požadovanou stránku stáhnout. Následně z tohoto staženého HTML souboru za pomoci parseru[4] provést identifikaci tagů[5]. Tyto tagy oddělují jednotlivé informace. Na základě jejich znalosti vyfiltrovat nepotřebný kód a získat ucelená data. V případě, že jsou daná data získána, lze stažený soubor nahradit souborem s dalším zkoumaným uživatelem.

---

3 **HTML -** HyperText Markup Language, je značkovací jazyk pro hypertext.

4 **Parser –** Syntaktický analyzátor vstupního souboru.

5 **Tag** – Značka, element.

2.3.3 Analýza struktury externí databáze

Stažený soubor jsme schopni za pomocí libovolného textového editoru otevřít a tím zobrazit potřebný HTML kód, jehož analýzou lze nalézt výše zmíněné požadované informace (*Obrázek4*). Díky tomu lze určit, že všechny pro nás důležité informace jsou umístěna v následujícím formátu:

* Typ hodnoty *

* Hodnota *

V případě, že daný údaj není vyplněn, je hodnota prázdná. Na základě tohoto rozboru staženého HTML souboru, jsme schopni určit typ a hodnotu požadovaných datových fondů, které mohou být důležité pro bližší zkoumání a určení osoby, jenž byla v kontaktu s námi zkoumaným účtem, případně o zkoumaném účtu samotném.

```
<!-- Full Profile -->
<div class="hide" id="fullprofile">
  <!-- Start double information -->
  <div class="d1-1-2-6">
    <div class="d1-1-2-6-1 info_line">
      <div class="info_name">Přezdívka</div>
      <div class="info_value">[ ]</div>
    </div>
    <div class="d1-1-2-6-2 info_line">
      <div class="info_name">Pohlaví</div>
      <div class="info_value">Žena</div>
    </div>
    <div class="d1-1-2-6-3 info_line hide">
      <div class="info_name">Aktuálně</div>
      <div class="info_value"></div>
    </div>
    <div class="d1-1-2-6-4 info_line">
      <div class="info_name">Den narození</div>
      <div class="info_value">7/11/1991 (20)</div>
    </div>
    <div class="d1-1-2-6-5 info_line hide">
      <div class="info_name">Adresa</div>
      <div class="info_value"></div>
    </div>
```

Obrázek 4: Analyzovaný kód staženého HTML souboru

3 Vývoj softwarového prostředku

3.1 Přehled současného řešení

V současné době není vytvořena ucelená vědecká práce řešící forenzní zkoumání softwarového prostředku ICQ do dále uvedené úrovně prováděných analýz a vazeb mezi jednotlivými zkoumanými komponentami.

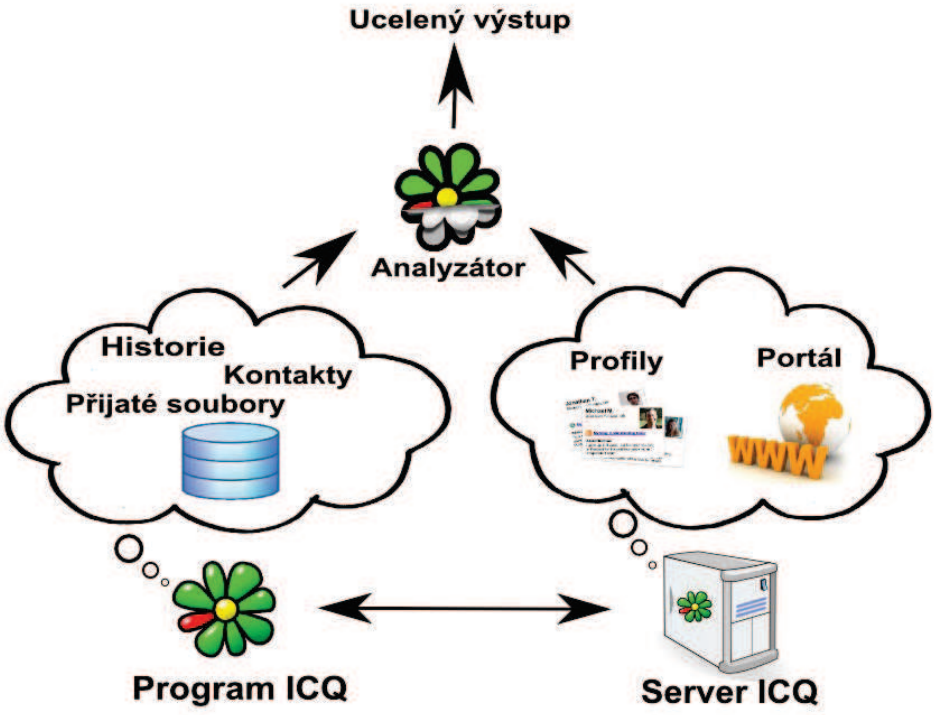
Možnou alternativou je komerční software společnosti Belkasoft *IM Analyzer* schopný získat databázi historie většiny současných komunikátorů. Tento software však pro uživatele nehledá spojitosti a vazby k dalším zdrojům určených pro širší zkoumání a analyzuje pouze základní informace o komunikaci.[0]

Z dalších alternativ nebyl nalezen jiný rozšířený a funkční analyzátor pro zkoumané verze softwarového prostředku ICQ.

3.2 Plán vývoje

3.2.1 Základní postupy

Aplikace bude metodicky napsána v programovacím jazyce Java. Program bude využívat již existující knihovny pro práci s databázemi, soubory, HTTP protokolem a grafickým rozhraním. Samotná tvorba proběhne v prostředí *NetBeans IDE 7.1*. Požadavky pro tvorbu této aplikace jsou založeny na provedených analýzách a znalostí vazeb systému ICQ.



Obrázek 5: Schéma vazeb systému ICQ

3.2.2 Základní požadavky

Aplikace musí být schopna:

- Nalézt datová úložiště programu ICQ.
- Vyexportovat informace z databáze programu.
- Získat umístění přijatých souborů přes program ICQ – tyto soubory zadokumentovat (uložit, vytvořit kontrolní sumu MD5).
- Provést dotaz na portál www.ICQ.com.
- Stáhnout požadovanou stránku.
- Vyfiltrovat požadované informace.
- Vytvořit ucelený výstup všech zjištěných informací.

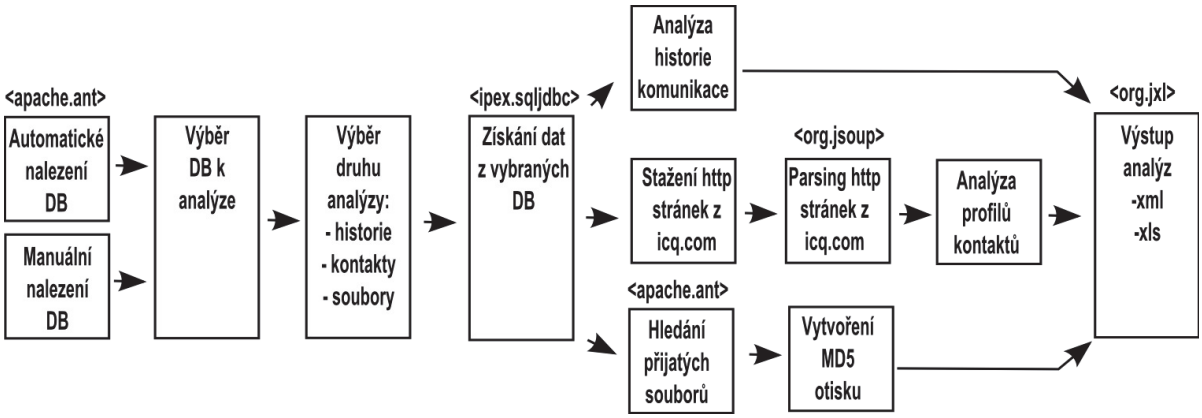
3.2.3 Metodika vývoje

Metodika vývoje programu bude vycházet z agilní metodiky[6] V*ývojem Řízeným Vlastnostmi (Feature Driven Development)* [8]. Jako první krok byly vytvořeny přesně stanovené cíle a požadavky na tvorbu výsledné aplikace. Dalším krokem je určení jednotlivých funkčních celků vycházejících z těchto požadavků. Tyto celky budou promítnuty do následně navrženého modelu aplikace. Poté bude proveden návrh vazeb jednotlivých tříd programu, jejich funkcí a výsledných vlastností tak, aby byly splněny prvotní cíle a požadavky.

3.3 Implementace

3.3.1 Model softwaru

Navržený model slouží jako vodítko při tvorbě aplikace. Jeho jednotlivé bloky a daná funkcionalita z levé strany do pravé by měla nastínit kroky, které bude aplikace vykonávat. Nad bloky, které vyžadují rozšířenou funkcionalitu o dodatečné knihovny, byl uveden název jednotlivých knihoven, které by tuto funkcionalitu měli zastupovat.



Obrázek 6: Navržený model funkcí pro výslednou aplikaci.

6 Agilní – Flexibilní, přizpůsobivé metodiky vývoje kladoucí na důraz efektivitu řešení daného problému, cíle.

V prvním kroku bude uživatelem vybrán způsob nalezení (vložení) databáze. To lze provést automaticky. V tomto případě by program měl být schopen nalézt co nejširší soubor účtů používaných na zkoumaném počítači, k němuž by aplikace měla být schopna nalézt příslušné databázové soubory, ze kterých budou získávány analyzované datové fondy.

Toto hledání bude provedeno rozšiřující knihovnou z balíčku knihoven Apache Ant. Ta umožňuje práci s adresářovou strukturou a vyhledávání souborů. Další možností je v případě, že program nebude schopen požadovanou databázi najít, nebo bude požadavek zadat cestu k databázi ručně, bude uživateli dána možnost i této volby. V případě zvolení manuálního vstupu je potřeba zadat zdrojové soubory pro analýzu kontaktů a souborů taktéž manuálně (pokud tyto funkce budou vyžadovány). Umístění těchto datových zdrojů, neboli návod pro uživatele kde tyto zdroje hledat je podrobně popsán v analýze ICQ a portálu www.ICQ.com, která je předmětem této práce, případně ve zkrácené podobě v manuálu aplikace, který je taktéž přítomen formou přílohy. Při této volbě nebude možné analyzovat více jak jednu databázi najednou, jako v případě volby automatického vyhledání.

V následujícím kroku je za předpokladu, že je zvoleno automatické vyhledání, potřeba vybrat databáze, které jsou zájmem našeho zkoumání. Není tedy nutné zkoumat veškeré databázové účty nalezené na zkoumaném počítači. Účty budou rozlišeny unikátním UIN číslem a následně zobrazeny v seznamu, ve kterém lze vybrat kliknutím myši patřičný účet, případně za podržení klávesy SHIFT, nebo CTRL vybrat účty další.

Poté co byly uživatelem zvoleny databáze, které jsou předmětem jeho zájmu, je nutné zvolit typ prováděné analýzy. Každá z těchto analýz disponuje jiným výstupem a každá se zaměřuje na jiný úsek datových fondů. Tato varianta byla zvolena z důvodů větší rychlosti, přehlednosti a umožnění vybrat si zkoumání dle zájmu uživatele. Uživatel má k dispozici možnost zvolit jednu z těchto analýz: analýzu historie komunikace, analýzu profilů se kterými byl zkoumaný subjekt v kontaktu a analýzu přijatých souborů.

V případě zkoumání historie komunikace budou za pomoci knihoven *SqliteJDBC* otevřeny databáze typu SqlLite pojmenované Messages.qdb, které tyto datové fondy obsahují. Důležitá a dále specifikovaná data budou roztříděna do přehledné tabulky.

V případě analýzy profilů program za pomocí knihovny *SqliteJDBC* zjistí z databáze Owner.qdb seznam UIN profilů, se kterými byl zkoumaný uživatel v kontaktu. Jedná se nejen o kontakty, které se již nenacházejí v současném seznamu kontaktů, ale i o všechny

kontakty, se kterými byl zkoumaný uživatel v kontaktu i v minulosti na zkoumaném počítači. Díky znalosti UIN, jsme schopni zadat na dotaz na portál www.ICQ.com a zobrazit veřejně dostupné profilové informace o každém uživateli zvlášť. Tuto HTML stránku lze stáhnout do adresáře programu, jenž je určen pro dočasné soubory. Po stažení je nutné celý kód postupně projít za pomocí knihovny *Jsoup* a získat na základě identifikátorů žádané informace. Tyto informace poté přehledně zobrazit v tabulce stejně jako u předchozího kroku.

Třetí možností analýzy je zaznamenání přijatých souborů, které se nacházejí ve složce ve které ICQ standardně uchovává přijaté soubory. Toto umístění bude vyhledáno na základě znalosti UIN, cesty do které ICQ soubory přijímá a typu operačního systému na kterém byl program používán. Pro vyhledání souborů bude využita knihovna *Apache Ant*. Bude vytvořen kontrolní otisk typu MD5 určený pro ověření, že s přijatými soubory nebylo v průběhu zkoumání manipulováno (v případě jakéhokoliv zásahu a změny v souboru je výsledná suma odlišná). Nalezené soubory a jejich otisk budou taktéž zaznamenány do tabulky.

Po výběru analýzy, s již získanou tabulkou, kterou lze upravit (vyfiltrovat) podle potřeb zkoumání, jsme schopni vytvořit ucelený výstup dvou typů. První možností je vytvoření tabulky typu XLS[7]. V tomto případě bude struktury tabulky zachována a výsledná tabulky bude odpovídat tabulce zobrazené programem. Tento výstup bude tvořen za pomocí knihovny *Jxl*. Další možností je vytvořit výstup typu XML[8]. V případě této volby je potřeba výstup náležitě upravit do odpovídajícího formátu, jehož příslušný popis bude popsán v manuálu aplikace. Umístění a název výstupu bude zadán uživatelem za pomoci dialogového okna pro prohlížení stromové struktury dat. Po provedení uložení bude uživatel navrácen do přehledu obsahující tabulku, jenž byla ukládána.

7 XLS – Přípona souborů typu Microsoft Office Excel

8 XML(eXtensible Markup Language) – Je obecným značkovacím jazykem vyvinutým konsorciem W3C.

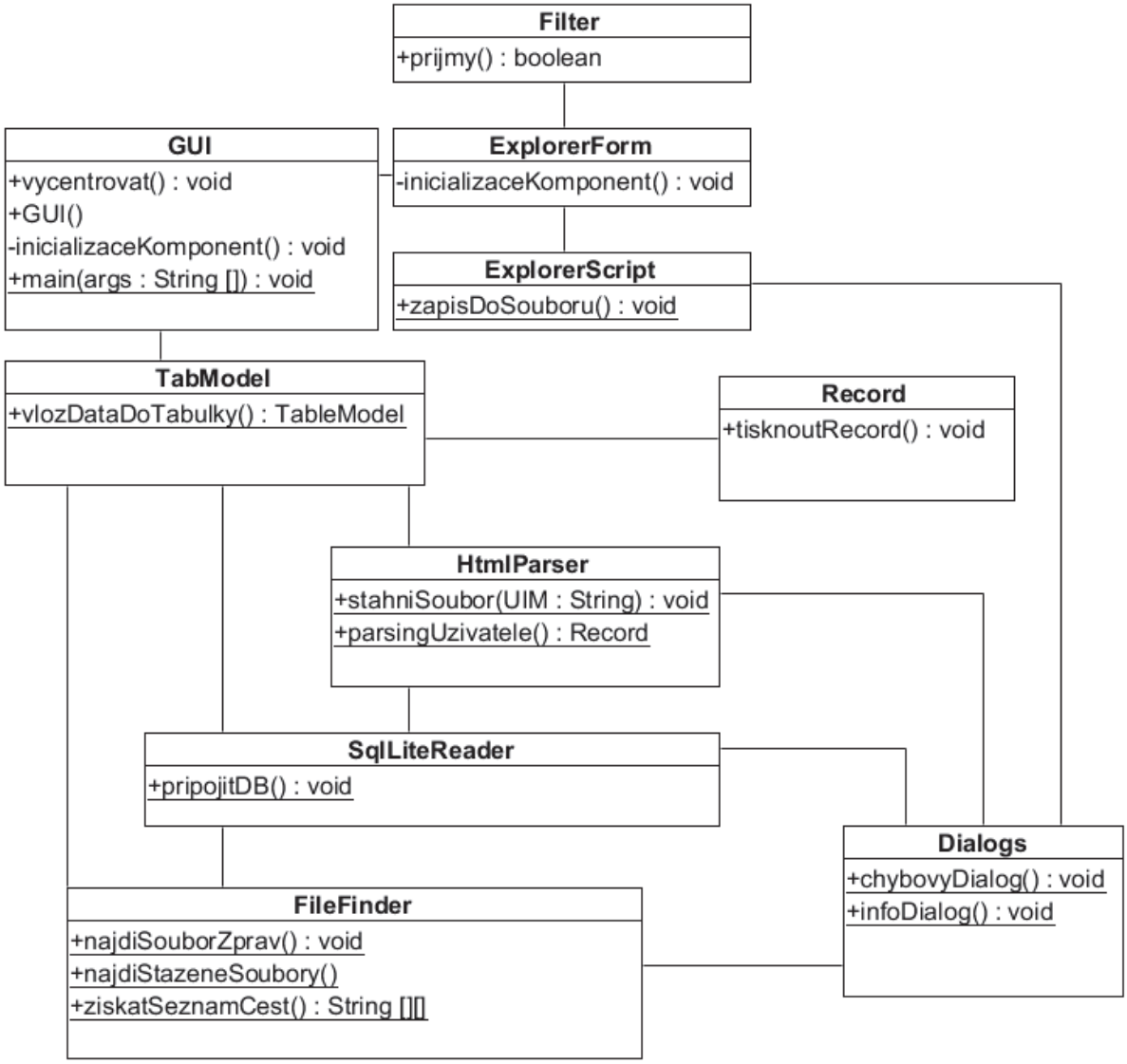
3.3.2 Rozdělení tříd

Program bude psán za využití tříd třech typů. Prvním typem jsou třídy datových objektů reprezentující reálný objekt, jakým je např. záznam. Tyto třídy generují instance[9]. Druhým typem jsou třídy druhu objektu, sloužící k určení příslušnosti do jednotlivých funkčních celků. Tyto třídy negenerují instance. V těchto třídách lze najít většinu algoritmů a výpočtů pro běh programu. Dalším typem jsou třídy formulářové (grafické), jenž mají za úkol vykreslit program do příslušného formuláře (okna) a vytvořit grafické rozhraní, s kterým přijde uživatel přichází do styku. V těchto třídách jsou zpravidla volány metody z jiných tříd a přenášeny informace mezi jednotlivými funkčními celky programu.

3.3.3 Realizace tříd

Na základě výše stanovených požadavků byl vytvořen následující diagram tříd, jenž odpovídá výsledné implementaci. Tento diagram je návrhem konečného modelu aplikace. Obsahuje základní metody a jejich vstupní a návratové hodnoty.

9 Instance – Realizace objektu třídy.



Obrázek 7: Návrh diagramu tříd na základě kterého byla tvořena aplikace.

Třída GUI – Hlavní třída programu. Tato třída je rozšíření třídy *javax.swing.JFrame.* Jejím úkolem je zobrazit základní rozhraní se kterým uživatel přijde do styku. Formulář a jeho prvky jsou umístěny za pomocí funkce Designer prostředí *NetBeans IDE 7.1*. Výsledné okno (*JFrame*) je vycentrováno metodou *centerFrame()* na střed obrazovky uživatele a není možné měnit jeho velikost. Toto okno samo o sobě neobsahuje žádné prvky, se kterými uživatel přijde do styku. Obsahuje několik objektů typu *javax.swing.JLayeredPane*, které reprezentují panel objektů, do kterých jsou přidávány jednotlivé objekty reprezentující převážně text, obrázky, tlačítka a seznam automaticky analyzovaných účtů. Tyto jednotlivé panely jsou zneviditelňovány a naopak zviditelňovány vždy na základě toho v jaké části se uživatel nachází. V případě tabulky je použit panel *javax.swing.JTabbedPane*, který umožňuje přidávat jednotlivé listy oddělené záložkami. Toho je využito v případě zkoumání více účtů. Do těchto panelů jsou následně přidány panely typu *javax.swing.JScrollPane*, z důvodu nutnosti přítomnosti posuvníků v případě, že je tabulka větší a možnosti zobrazení popisů jednotlivých sloupců tabulky. Tento panel již obsahuje výše zmíněnou tabulku se zjištěnými údaji. Metody a algoritmy obsažené v této třídě slouží prioritně ke grafickým úpravám jednotlivých komponent (zobrazení, ukrytí, aktualizace apod.) a k předávání dat formou seznamů mezi jednotlivými komponentami, které jsou případně následně umisťovány do příslušných tabulek a seznamů. V této třídě je využito volání metod získávajících data z databází, webů, pevných disků a jejich následné vkládání do grafických komponent. Případně při volbě ukládání, vyjmutí těchto údajů z existující tabulky a předání k dalšímu zpracování v rámci ukládacího procesu.

Třída ExplorerForm - Tato třída je rozšíření třídy *javax.swing.JFrame.* Jejím úkolem je zobrazit formuláře, které mají za úkol procházení souborovým systémem. Tohoto formuláře je využito v případě zadávání cesty a názvu souboru, který chceme uložit. Další funkcí je možnost zadání cesty k databázím a zdrojům v případě manuálního zadávání. Samotné procházení je řešeno komponentou *javax.swing.JFileChooser*, která zastává všechny výše zmíněné funkce. Díky variabilitě této komponenty lze snadno změnit typ a vlastnosti tohoto dialogového okna. Pro potřeby funkcí této komponenty obsahuje soubor s výše zmíněnou třídou další třídu rozšiřující *javax.swing.filechooser.FileFilter*, která slouží k vyfiltrování zobrazovaných souborů v okně komponenty *JFileChooser*. Třída ExplorerForm také přijímá data z třídy GUI a volá samotné ukládací procedury, ty data na zvolené umístění pod zvoleným jménem uloží.

Třída ExplorerScript - Třída obsahující algoritmy vykonávající uložení záznamů do souborů. Tato třída přejímá z třídy ExplorerForm cestu a z třídy GUI obsah tabulky, které následně ukládá ve dvou možných variantách. V případě ukládání do formátu XML, rozloží jednotlivé řetězce záznamů mezi předem definované značky. Toto ukládání probíhá na základě vzoru, kterým je předdefinovaný vstupní vzor (dvourozměrné pole) definující logiku vkládání a označení značek. V případě ukládání do formátu XLS je využito knihovny *org.jxl*, která převede obsah tabulky typu *JTable* zobrazované ve třídě GUI do výstupního souboru, který by měl obsahově odpovídat zobrazované tabulce ve formátu pro programy podporující XLS.

Třída Dialogs - Tato třída obsahuje soubor metod volající dialogová okna komponenty *JFrame*. Tyto dialogová okna uživatele upozorní na případné chyby vstupů a běhu programu, aby dali uživateli podvědomí o příčině možné chyby pro eventuální nápravu.

Třída Records – Třída generující potomky reprezentující získané záznamy z analýz různých typů. Záznam reprezentuje objekt obsahující několik textových řetězců. Tato třída je schopna generovat potomky různým typů záznamů s ohledem na počet přenášených informací. Záznamy jsou v aplikaci přenášeny převážně formou seznamů. Každý záznam obsahuje ke každému řetězci adekvátní metodu *Get()*, která ho navrací.

Třída FileFinder – Třída reprezentující vyhledávání souborů na pevném disku s adresářovou stromovou strukturou. Využívá pro tento účel knihovnu *org.apache.tools.ant*. Na základě znalosti umístění a pojmenování databázových souborů, jsou metody třídy schopny najít cesty k databázím na základě určení cest, ve kterých má program hledat. Další funkcí je vyhledání přijatých souborů, které probíhá na stejném principu. Nalezené řetězce s cestami k souborům jsou rozděleny na část obsahující cestu k souboru a část obsahující název souboru. Se znalostí cesty k souboru je následně vytvořen jeho kontrolní otisk využitím funkcí knihovny *org.apache.commons.codec.digest.DigestUtils.md5Hex*.

Třída HtmlParser – Třída, jenž má za úkol analýzu dat z portálu www.ICQ.com. Metody této třídy jsou schopny stáhnout HTML kód do předem připraveného souboru. Stažený soubor lze za pomocí metod určených pro parsování projít a na základě znalosti značek, které značí požadované informace z něho za pomoci knihovny *org.jsoup* tyto informace získat a uložit je jako záznam. Tato třída zároveň řeší situaci, kde při nadměrném dotazování portálu www.ICQ.com dochází k dennímu zablokování funkce „Hledání lidí“.

Tento problém je ošetřen minutovým přerušením běhu programu po každých osmi dotazech. Tato frekvence a potřebná doba byla zjištěna testy.

Třída TabModel – V této třídě jsou tvořeny modely tabulek používaných pro zobrazení ve třídě GUI. Tabulky jsou tvořeny zavoláním metody a předáním záznamů, které bude tabulka obsahovat a na jejichž základě je vytvořen požadovaný model.

Třída SqlLiteReader – Třída jejímž úkolem je práce s databázemi typu SQLite. Tato třída využívá knihovny *ipex.sqljdbc*, které umožňuje práci s těmito databázemi. Na databáze nalezené třídou FileFinder jsou v případě zjišťování historie zpráv zavolány dva dotazy typu SQL[10] na databázi Messages.qdb. Jedním jsou vybrány veškeré zprávy komunikace z tabulky Messages a druhým je provedena vazba s tabulkou Participants. Ta provedená tak, aby bylo možné identifikovat účastníky, kteří sdíleli jednotlivé zprávy. Po provedení dotazu a získání dat z databáze, je třída schopna dopočítat časový údaj, který značí počet dní od roku 1900 tím, že dopočítá dny do roku 1970. Ty odečte od celkového počtu dnů a poté převede časový údaj za pomocí metod pracující s unixovým časem. Ten je počítán právě od roku 1970. Další funkcí je převedení čísla označující typ zprávy na textový výstup z důvodu ulehčení identifikace typu jednotlivých zpráv. V případě, že je volána metoda zajišťující seznam UIN, se kterými byl uživatel v kontaktu. Pro použití ve třídě HtmlParser je položen jeden SQL dotaz na tabulku Users databáze Owner.qdb. Zde jsou vybrány veškeré UIN a profiltrovány v případě duplicitního uvedení v tabulce.

3.4 Testování

Testování aplikace bylo provedeno za pomoci testovacích tříd jazyku Java. Testy jsou navrženy tak, aby pokryly otestování co nejširší možné spektrum vstupů a ošetření chybových hlášení ve všech nestandardních stavech.

Testy nalezení vstupní databáze – Tyto testy byly navrženy za situace nalezení nulového počtu databází a relativně velkého počtu databází (více než třicet). Programem byl ošetřen stav oznamující uživateli, že nebyl schopen automaticky nalézt databáze s odkazem na možnost manuálního zadání.

Testy manuálního vstupu – Účelem těchto testů bylo ověřit správnou funkčnost ručního vkládání databázových souborů a cest pro zkoumání přijatých souborů.

---

10 SQL – Standardizovaný dotazovací jazyk používaný v relačních databázích

Testy nesprávného formátu databáze - V tomto případě byly ověřeny stavy za předpokladu, že zkoumaná databáze nemá formát, se kterým je schopna aplikace bezchybně pracovat.

Testy nedostupnosti portálu www.ICQ.com – Těmito testy byly otestovány varianty, kdy není k dispozici připojení k internetu, portál není dostupný, nebo byl přístup uživatele kvůli nadměrnému počtu dotazů zablokován. V případě teoreticky možného (duplicitní běh aplikace) zablokování aplikace reaguje zprávou nutnosti odložit zkoumání do druhého dne.

Testy ukládání dat – Tyto testy byly provedeny s cílem zajistit chybové stavy, které mohou nastat v případě ukládání souboru jak to formátu XLS a XML.

3.5 Uživatelské testy

Těmito testy byla zjištěna funkcionalita aplikace na několika vzorových konfiguracích systému a na různé verze softwarového prostředku ICQ. Testy byly provedeny na čtyřech počítačových sestavách s nainstalovaným operačním systémem Microsoft Windows XP/Vista/7 a nainstalovaným prostředím Java Runtime Envirovement 7, které je potřebné pro běh aplikace. Na těchto sestavách byly otestovány softwarové prostředky ICQ verze 7.0 - 7.7. Těmito testy byla ověřena úspěšně funkčnost aplikace na cílených systémech a to v jednom případě pro přirozeně používaný program ICQ po dobu 2 let, tak v případě uměle vytvořených vzorků dat, se kterými bylo v průběhu práce a při tvorbě samotné aplikace pracováno.

4 Návrhy pro budoucí řešení

V průběhu vývoje aplikace a na základě poznatků a komentářů z uživatelských testů lze výsledný analyzátor rozšířit nad rámec této práce o následující funkce:

- Podpora neoficiálních softwarových prostředků využívajících systému ICQ
- Podpora pro obdobné komunikátory (Skype)
- Rozšíření možností konfigurace a přizpůsobení aplikace za pomoci konfiguračního souboru
- Přidání možnosti zkoumání mobilních zařízení
- Výstup ve formátu PDF
- Zachytávání probíhající komunikace (sledování síťového provozu, práce s protokolem OSCAR)
- Práce s obrazy (analýza databází získaných z obrazu disku)
    - Podpora operačního systému Linux v rámci zajišťování obrazů disků operačního systému Windows.
- Zjištění a dešifrování hesel k jednotlivým účtům
    - Získání neveřejných profilových informací (práce s protokolem OSCAR, nutná identifikace za pomocí znalosti hesla serveru ICQ)

5 Závěr

5.1 Shrnutí

V bakalářské práci byla provedena a řádně zadokumentovaná podrobná analýza softwarového prostředku ICQ, portálu www.ICQ.com a základní funkčnosti systému ICQ. Na základě této analýzy byly vyhodnoceny možnosti získání co nejširšího spektra datových fondů z výše uvedených zdrojů. Na základě těchto požadavků byl vytvořen návrh analyzátoru, dle kterého byla provedena realizace, jenž byla řádně zadokumentována a otestována.

5.2 Vyhodnocení

V práci bylo úspěšně dosaženo všech stanovených cílů. Výsledná aplikace odpovídá zadání a požadavkům této práce. Aplikace a podrobná analýza představuje přínos v rámci zjednodušení a zpřístupnění možnosti analýzy historie komunikace a souvisejících datových fondů (profilové informace, informace o přijatých souborech). Mimo jiné je aplikace přínosem v možnosti získávání dat za předpokladu nemožnosti přístupu do klienta ICQ (například v případě zapomenutého hesla). Případně aplikaci lze využít k vlastnímu zálohování komunikace. Na základě zjištění lze prohlásit, že prozatím neexistuje jiné softwarové řešení v takovémto rozsahu zkoumající datové vazby do popsané hloubky.

6 Přehled literatury

6.1 Portály

[0] BELKASOFT. *Forensic and system software tools.* [online]. ©2002-2012 [cit. 2012 02-15]. Dostupné z: http://forensic.belkasoft.com/en/

[1] DAVID CRAWSHAW. *SqlliteJDBC* [online]. ©2012 [cit. 2012-02-15]. Dostupné z: http://www.zentus.com/sqlitejdbc/

[2] ERIC H. JUNG. *Java Excel API* [online]. ©2012 [cit. 2012-02-15]. Dostupné z: http://jexcelapi.sourceforge.net

[3] ICQ LLC. *Icq* [online]. ©1998-2012 [cit. 2012-02-15]. Dostupné z: www.icq.com

[4] ING. JAROSLAV KOTHÁNEK, Ph.D. *Znalecká a detektivní kancelář* [online]. [2010] [cit. 2012-02-15]. Dostupné z: http://www.it-znalec.cz/

[5] JONATHAN HEDLEY. *Jsoup: Java HTML Parser* [online]. ©2012 [cit. 2012-02-15]. Dostupné z: http://jsoup.org

[6] ORACLE. *Java SE Technical Documentation* [online]. ©2011 [cit. 2012-02-15]. Dostupné z: http://docs.oracle.com/javase/

[7] THE APACHE SOFTWARE FOUNDATION. *The Apache Ant project* [online]. ©2012 [cit. 2012-02-15]. Dostupné z: http://ant.apache.org

6.2 Diplomové práce

[8] BC. TOMÁČ HAJDIN. *Agilní metodiky vývoje software*. ©2005 [cit. 2012-02-15]. Dostupné z: http://is.muni.cz/th/39440/fi_m/dp.pdf

7 Přílohy

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

[1] Uživatelský manuál analyzátoru ICQ

Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta
Katedra Aplikované Informatiky

Příloha č.1
Manuál analyzátoru historie komunikace softwarového prostředku ICQ

Příloha k bakalářské práci

Michal Prenner

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

2012

Obsah

1 Úvod

Tento analyzátor je součástí bakalářské práce zabývající se zkoumáním historie softwarového prostředku ICQ. Analyzátor slouží k získání co nejširšího spektra datových fondů z výše zmíněného prostředku určeného primárně pro textovou komunikaci.

Analyzátor je schopen zajistit:

- Zachovanou historii komunikace (účastníci, autor, text, datum a čas, typ zprávy).
- Profilová data uživatelů (veřejně dostupná profilová data, profilová fotografie).
- Analýzu přijatých souborů (seznam, informace o souborech, kontrolní suma).

Z takto zajištěných dat je schopen vytvořit přehledný výstup, který lze dle uvážení upravit a vyfiltrovat. Následně je schopen zobrazená data uložit do formátů XLS a XML.

2 O programu

2.1 Minimální požadavky

Pro spuštění aplikace musí počítač splňovat následující požadavky:

- Nainstalován operační systém Microsoft Windows XP a novější.
- Nainstalované rozhraní Java SE Runtime Environment (JRE) v.7u3 dostupné z *www.oracle.com* a novější.
- Procesor: Pentium 2 266MHz a více.
- Paměť RAM: 128MB a více.
- Místo na pevném disku: 256MB a více.

2.2 Spuštění

Program lze spustit spouštěcím souborem *analyzer.bat*. Tento soubor lze nalézt v kořenovém adresáři programu. V případě nefunkčnosti zavaděče lze program spustit za pomoci rozhraní JRE ze složky *../bin/analyzer.jar*.

3 Provádění analýz

3.1 Hlavní nabídka

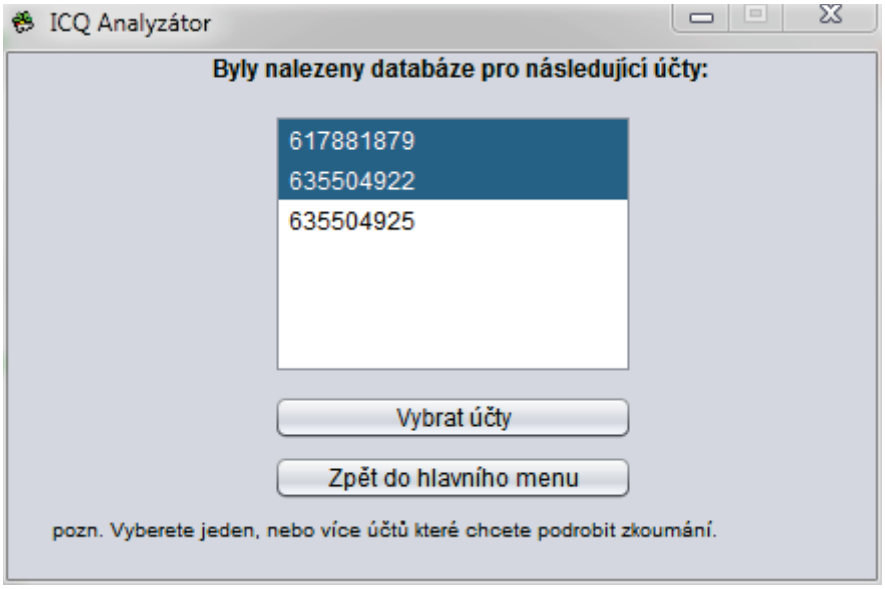
Volbami *Najít databázi automaticky* a *Zadat cestu k databázi ručně*, lze zavádět databázové soubory, ze kterých jsou následně prováděny analýzy a získávány datové fondy. Další položkou v menu tzv. *Nastavení vyhledávání* lze nastavit parametry automatického vyhledávání. Dalšími funkcemi je možností otevření tohoto manuálu a zobrazení stručných informací o programu.

Obrázek 1: Hlavní nabídka.

3.1.1 Automatické vyhledání

Funkce automatického vyhledání slouží k nalezení datových zdrojů v typicky používaných cestách, které softwarový prostředek ICQ generuje. Díky této funkci není třeba složitě manuálně vyhledávat a zadávat databázové soubory. Program automaticky nalezne na oddílu disku zvoleném uživatelem dostupné zdroje a nabídne možnost volby z nalezených účtů, které má uživatel zájem dále analyzovat. Pro postup k analýze je nutné zvolit minimálně jednu databázi ke zkoumání.

Ze zobrazeného seznamu kliknutím levým tlačítkem myši lze vybrat více položek a to za pomoci podržení klávesy CONTROL (CTRL), případně klávesy SHIFT.



Obrázek 2: Volba nalezených databází.

3.1.2 Manuální zadávání

Funkce manuálního zadávání umožňuje uživateli zadat vlastní cestu ke zkoumané databázi.

Při manuálním zadáváním lze zadat následující:

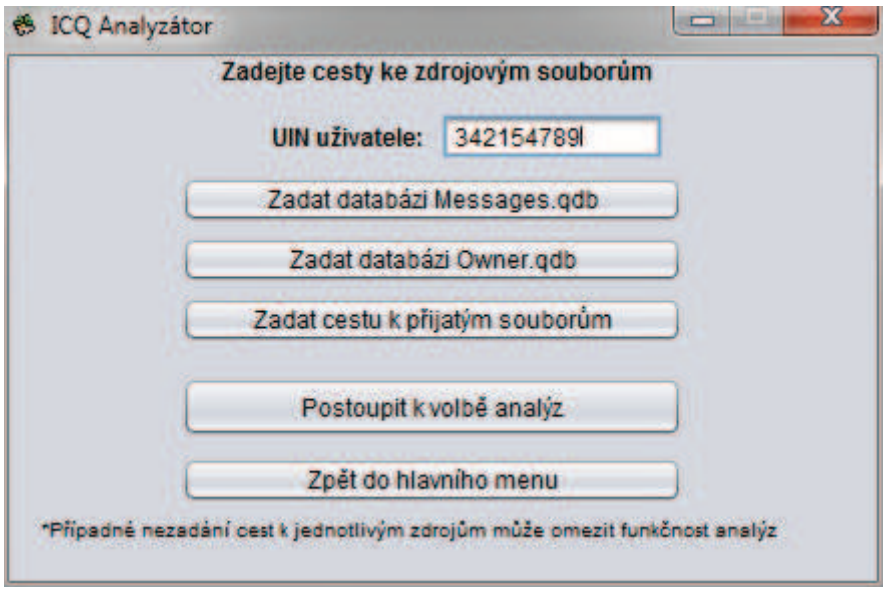
- Cestu k Messages.qdb (umístěné např. *C:\Users\Uzivatel\AppData\Roaming\ICQ*).

- Cestu k Owners.qdb (umístěné např. *C:\Users\Uzivatel\AppData\Roaming\ICQ*).
- Cestu k přijatým souborům

  (umístěné např. *C:\Users\Uzivatel\Documents\ICQ\ReceivedFiles*).

Vazby na funkčnost analýz jsou následující:

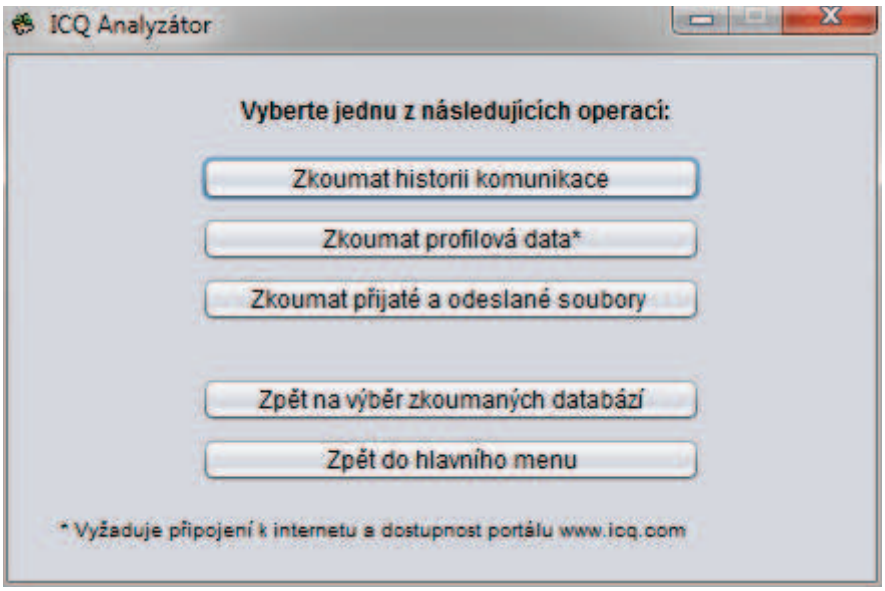
- Zadání cesty k Message.qdb je potřebné pro možnost zkoumání historie komunikace.
- Zadání Owners.qdb pro získávání profilových informacích.
- Zadání cesty k přijatým souborům je nutné pro jejich analýzu.



Obrázek 3: Manuální zadávání cest.

3.2 Zvolení typu analýzy

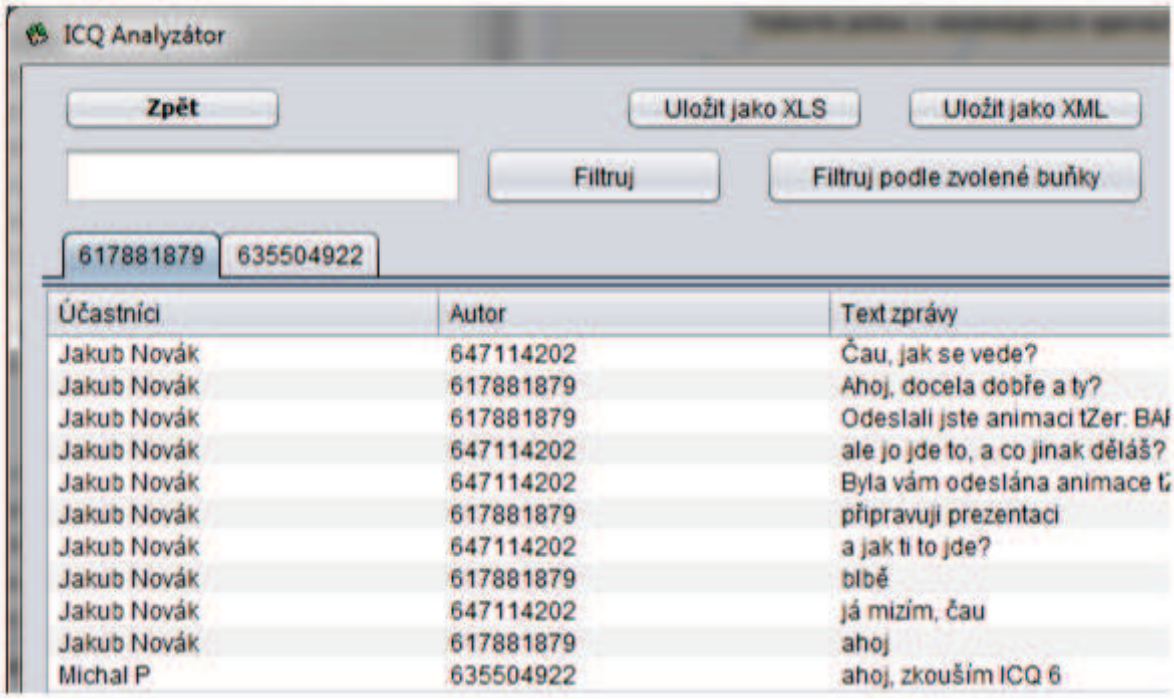
V případě úspěšně vloženého vstupního zdroje dat, uživatel mé na výběr ze tří typů analýz. Po uskutečnění analýzy je uživateli zobrazen přehled ve formě tabulky. V případě analýzy více účtů najednou, lze mezi jednotlivými účty přepínat za pomocí záložek umístěných nad tabulkou.



Obrázek 4: Volba typu analýzy.

3.2.1 Zkoumání historie komunikace

Tento druh analýzy zobrazí zachovanou (nesmazanou) historii komunikace. V této analýze je zachován text samotné zprávy, její autor formou čísla ICQ (UIN), datum a čas, účastníci konverzace (mimo zkoumaného uživatele) a typ zprávy. Typ zprávy odlišuje jednotlivé druhy zpráv a to v případě že zpráva je informace o použití některé z funkcí programu (např. odeslání souboru).



Obrázek 5: Výstup provedené analýzy historie.

3.2.2 Zkoumání profilových informací

K této analýze je zapotřebí připojení k internetu a dostupnost portálu www.ICQ.com. V případě, že není splněno jedno z kritérií, nelze analýzu provést. Tato analýza může trvat v řádu minut z důvodu stahování informací z portálu a nutnými pauzami mezi stahováním, ty jsou nutné z důvodu ochrany proti zablokování ze strany portálu. Výhodou této analýzy je schopnost vyhledat všechny uživatele, se kterými byl na zkoumaném počítači uživatel v kontaktu a to i v případě, že již tento kontakt nefiguruje v aktuálním seznamu kontaktů. K těmto kontaktům jsou získávány z portálu www.ICQ.com veřejně dostupné profilové informace a cesta k profilové fotografii. V případě, že se daná informace na portálu nenachází (nebyla uživatelem vyplněna), je kolonka vyplněna pomlčkou.

3.2.3 Zkoumání přijatých souborů

Tato analýza zaznamená soubory, které zkoumaný uživatel přijal a nepřesunul z původní služky přednastavené softwarovým prostředkem ICQ pro příjem souborů. Krom

informací o souboru je vytvořen kontrolní otisk typu MD5. Tento otisk slouží k zajištění důkazu, že soubor nebyl po provedeném zkoumání dále upravován.

3.3 Filtrování dat

Funkce filtrování dat nabízí uživateli možnost vyfiltrovat pro účel daného zkoumání nepodstatné informace, které analýza byla schopna zajistit.

Možností filtrování jsou následující:

- **Pomocí zvolené buňky –** Na základě zvolené buňky v tabulce vyfiltruje řádky s identickým obsahem buňky v tabulce. V případě že není buňka zvolena, vrátí původní výstup.
- **Pomocí textového vstupu** - Najde na základě zadaného textového řetězce řádky, jejichž buňky obsahují zadaný řetězec. Tento typ filtrování není závislý na dodržení malých a velkých písmen. Filtrování lze provést stiskem tlačítka, nebo stiskem klávesy ENTER.V případě, že není řetězec zadán, zobrazí původní výstup.

4 Výstupy

Za pomocí programu lze získaný výstup uložit jednou z následujících variant. Ukládání probíhá z aktuálně zobrazeného a vyfiltrovaného výstupu, který má uživatel k dispozici. V případě ukládání je nutné zadat cestu a název souboru, který má být výstupem. Koncovku není nutné zadávat.

4.1 Výstup typu XML

Rozloží jednotlivé informace za užití značkovacího jazyka XML. Jednotlivé informace jsou umístěny pod patřičným značkami dle následující logiky ***<typ, název informace> text, obsah informace</typ, název informace>***. Získaný výstup je obrazem tabulky a obsahuje veškeré informace zobrazené tabulky.

4.2 Výstup typu XLS

Výstup typu XLS je obrazem zobrazované tabulky ve formátu používané rodinou programů *Microsoft Excel* a *OpenOffice.org Calc*. Logika i vzhled tabulky odpovídá zobrazované tabulce. V případě, že dochází ke zkoumání více uživatelů, jednotlivé účty jsou rozlišeny záložkami na jednotlivé pracovní listy, obdobně jako u aplikace.