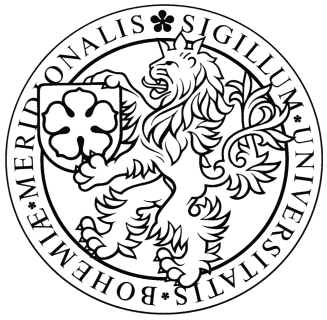
Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta



Analýza historie komunikace xChat

Bakalářská práce

Pavel Ryneš

Školitel: Ing. Jaroslav Kothánek, Ph.D.

České Budějovice 2012

Bibliografické údaje

Ryneš P., 2012: Analýza komunikace historie xChat.
[Analysis communication history of xchat Bc.. Thesis, in Czech.] – Faculty of Science, The University of South Bohemia, České Budějovice, Czech Republic.

Anotace

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

Abstract

Based on the needs of forensic examination of communication history of various communication programs for the police authorities and forensic experts is needed documentation chat history of "xChat". This is especially necessary to analyze the data files containing records of contacts and communication history at a local PC. Based on the contact information to analyze the possibility of obtaining identification information from the portal xChat.

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 eletronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledků 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, 25. listopadu 2012

Podpis

Poděkování

Děkuji vedoucímu práce Ing. Jaroslavu Kothánkovi, Ph.D. za cenné rady, připomínky a trpělivost. Rovněž děkuji rodině za podporu a korekturu textu.

Obsah

1 Úvod a cíle

1.1 Úvod

Osobní počítač s připojením na internet se stal nedílnou součástí každodenního života většiny z nás. Podle údajů z webových stránek Českého statistického úřadu (ČSÚ), v roce 2005 necelá třetina domácností vlastnila počítač a pětina měla přístup k internetu. Za pouhých 5 let osobní počítač s připojením na internet vlastnila více než polovina všech domácností v ČR[1)]. A tento počet bezpochyby nadále stoupá. Jako jednu z činností jednotlivce v oblasti komunikace ČSÚ uvádí chatování[2)]. Z tabulky[3)] za rok 2011 lze vidět, že 31,4% (1,8mil.) jednotlivců starších 16 let, co použili v posledních 3 měsících internet ke komunikaci, chatovalo. Jednou z nejznámějších chatovacích služeb v ČR je portál xChat.

Tato práce má za úkol seznámit se s xChat službou a provést analýzu historie komunikace na úrovni lokálního počítače, následně analýzu možností získání identifikačních údajů z portálu poskytující xChat služby, které by pomohly usvědčit osobu z nelegální činnosti. Sloužit by měla zejména pro policejní orgány a vyšetřovatele, kteří po získání soudního příkazu k zabavení výpočetní techniky, nejčastěji osobního počítače, udělají zálohu disku, kterou následně zkoumají forenzními prostředky.

1.2 Cíle

Nejprve se představí funkce na xChat portálu. Poté se provede analýza lokálních dat, které se na základě "xchatování" vyskytují na pevném disku. Pokusí se získat uživatelské přihlašovací jméno (login), které se posléze identifikuje na webu xchat.cz. Zjištění, co ukládá prohlížeč do historie na základě navštívení a chatování na xchatu. Prověření adresáře Temp, cache prohlížečů a systémových souborů pagefile.sys a hiberfil.sys u systému Windows 7. Práce bude obsahovat softwarový prostředek, který ve zmíněných souborech vyhledá vlastní komunikaci a najde přezdívky uživatele. Nalezené údaje se se budou moci vyexportovat do souborů.

1) Přístup z internetu 4.11.2012, http://www.czso.cz/csu/redakce.nsf/i/kolik_domacnosti_v_cr_ma_pocitac_a_internet
2) Chat - krátká komunikace dvou či více lidí prostřednictvím komunikačního prostředku
3) Přístup z internetu 4.11.2012, http://www.czso.cz/csu/2011edicniplan.nsf/t/500043D798/$File/97011123.pdf

2 xChat

2.1 Co je to xChat?

XChat je poskytovatel veřejné služby, která nabízí nejen možnost poznat nové lidi prostřednictvím chatování, ale jsou zde i další služby, které se mohou využívat v případě volného času - jako například nahrávání fotek do fotoalb, porovnávání profilů s možnosti ohodnocení, pořádání srazů, zanechání názorů na fórech nebo využíváni dalších služeb portálu centrum.cz. Pokud se octnete v těžké životní situaci a nemáte se komu svěřit, nalézá se zde i sdružená linka bezpečí.

2.2 Historie

Prvním projektem byla seznamka vytvořená v roce 1996, která se považuje za první internetovou seznamku v České republice, jejíž autorem byl Martin Michale. V roce 1997 začal spolupracovat s Jiřím Vaníčkem na webových stránkách obohacených informacemi z kultury, regionu a možností inzerce. Tato seznamka dostala název Xland a pomalu se rýsovalo vnoření dalších funkcí – chat. Server představovaly 2 počítače, běžící na Technické fakultě v Liberci a dokázaly pojmout i 100 lidí online. Tým se rozrostl o Pavla Francíka a nyní Xland obsahoval chat, fóra a e-mail. Doména www.xchat.cz se spustila datem 25.srpna 1998 a server byl zřízen u společnosti Cesnet. Na začátku roku 2000 přišel do týmu poslední člen, Jakub Olexa a na jaře téhož roku začala spolupráce s NetCentrem (dnes Centrum.cz). Pro velké neshody se ale od spolupráce odstoupilo již v létě roku 2000, přičemž Centru zůstala doména i databáze se 180 000 uživateli a tuto doménu provozuje dodnes. Původní xChat team od té doby fungoval pod doménou Xko.cz, která ale v roce 2009 ukončila svůj provoz.

2.3 Představení portálu

K využívání služeb xChatu je potřeba mít internetové připojení a prohlížeč. Aby bylo možno chatovat s ostatními, musí se zaregistrovat, avšak pokud je uživateli pod 18 let, podle pravidel registrace potřebuje k potvrzení emailem svého zákonného zástupce, nebo osobu starší 18 let, která za budoucího uživatele vysloví souhlas s všeobecnými smluvními podmínkami. Jediný povinný údaj při registraci kromě nicku a hesla je výběr pohlaví.

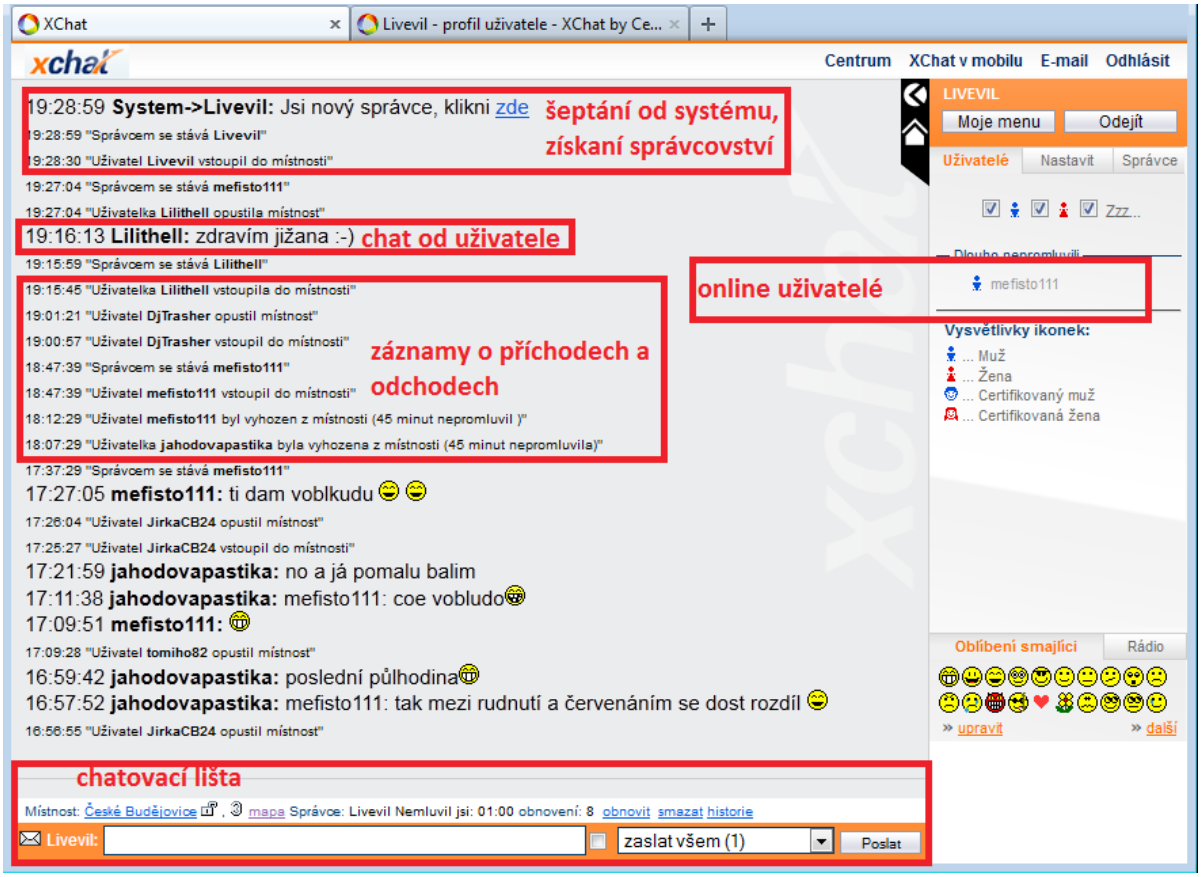
2.3.1. Základní hierarchie chatu

Rozdělení do kategorií je následující:

- Města a kraje
- Seznámení a flirt
- Hudební styl a kapely
- Pokec a klábosení
- Lechtivá erotika
- Film, knihy a počítače
- Volný čas a sport
- Sex a neřesti od 18 let

V každé kategorii se nachází takzvané místnosti, které se rozdělují na stálé (běžící na serveru) a uživatelské, založené člověkem s možností zaheslování. Mnohé místnosti například s erotickou tématikou mají svá dodatečná pravidla, která by váš případný vstup mohla ovlivnit. Jedno z pravidel může být věk, počet nachatovaných hodin nebo například pohlaví. V místnosti je jeden z uživatelů nebo ten, kdo založil onu místnost, určen jako správce, který dočasně zodpovídá za chování zúčastněných uživatelů v místnosti. Pokud by měl nějaké pochybnosti o porušení pravidel, má schopnost kicku[4)] uživatele nebo dokonce celé místnosti. Do místnosti, kde probíhá chat, je možné nahlédnout i jako guest - bez přihlášení, ale přichází se tím o schopnost chatovat.

4) Kick – z angličtiny: kop; v kontextu vyhození z místnosti



Obrázek 1 : Náhled do místnosti a její popis

Existují dva typy zasílání zpráv. První je na takzvané "sklo", tuto zprávu vidí všichni zúčastnění v místnosti, druhý typ je nazýván šepot, který probíhá pouze mezi odesílatelem a příjemcem, přičemž je možnost šeptat přes místnosti. V případě neaktivity trvající 45 minut vás systém vyhodí z místnosti. Doba obnovení skla s novými zprávami od účastníků neni okamžitá, minimální nastavitelná doba je 5 sekund.

2.3.2. Uživatelé

Neaktivní Uživatelský účet. V případě, že se Uživatel nepřihlásí ke svému Uživatelskému účtu (tj. nenavštíví emailovou schránku, nepřihlásí se xChat.cz, apod.) po dobu delší než 6 měsíců je Poskytovatel oprávněn zrušit takový Neaktivní Uživatelský účet.[6)]

Toto pravidlo může ovlivnit možnost vyhledat a identifikovat uživatele. Nicméně bylo nalezeno mnoho uživatelů, kteří mají dobu posledního přístupu i rok starou.

6) Přístup z internetu, část 3. Práva a povinnosti bod 9. Neaktivní uživatelský účet. http://napoveda.centrum.cz/index.php?/Knowledgebase/Article/View/71

Druhy uživatelů

- nově registrovaná osoba
  - ikonky muž, žena 
- certifikovaná osoba (osoba nad 15 let, u které byla prokázána totožnost občanským průkazem)
  - účelem certifikace je důvěryhodnost údajů (jméno, věk) pro ostatní
  - dostane změnu ikonky 
- modrá hvězdička (na 1 rok vylepšený a zpoplatnělý účet s několika výhodami např. sledování uživatelů pomocí sms)
  - k ikonce přibude modrá hvězdička ★ a po dobu platnosti se účet nemaže
- ostatní hvězdičky  jsou administrátoři
- bot

2.3.3. Další služby

- Srazy - velice oblíbenou činností je pořádání skutečných srazů. Sraz může pořádat pouze certifikovaná osoba.
- Fórum - možnost zanechat příspěvky na diskuzních fórech
- Profil - nabídka vyplnění bližších konkrétních údajů o osobě např. Vzhled, Životní styl ...
- Webík - uživatelsky upravitelná zeď, která obsahuje několik grafických prvků
- Změna nicku - nárok na změnu má osoba, jejíž účet disponuje modrou hvězdičkou s minimální dobou 30 dní do jejího vypršení a má nachatováno 100hodin. O žádost na dalši změnu se smí za další 3 měsíce. Jedná se o další věc, která by mohla ztížit identifikaci při vyšetřování.
- Fotoalba - veřejně přístupná všem, soukromá, se znalostí hesla
- Duel - uživatelé porovnávají mezi dvěma náhodnými profily s fotkou, vyberou, který se více líbí a ovlivňují umístění v žebříčku
- Mobilní verze xChatu
- xChat sdružená linka bezpečí - pro uživatele mladší 18 let nebo studenty do 26 let, každý den od 15 do 19 hod.
- Služby portálu centrum.cz

2.3.4. Vyhledávání

XChat disponuje vyhledávačem profilů, filtry, podle kterých je možnost hledat:

- podle pohlaví
- věku
- lokalita
- s fotkou
- právě chatuje
- chce se seznámit s
- za účelem
- ve znamení
- hvězdička
- certifikace
- podle emailu
- ve Fotoalbech podle názvu fotky

V sekci Srazy se nachází kalendář uskutečněných a budoucích srazů. Při detailní prohlídce se získá náhled, kdo tento sraz pořádá a účastníky. Srazy se vztahují ke konkrétní místnosti.

Rozšířený filtr nabízí vyhledávání ve srazech dle:

- budoucí/minulé
- dne
- měsíce
- roku
- místnosti
- města

Pro vyšetřování by mohlo být zajímavé zjistit, kdo se kdy zúčastnil jakých srazů. Tato funkce ale k dispozici není, bude se muset vystačit Google vyhledavačem. V případě, že se zná konkrétní osoba s daným nickem, stačí do vyhledávače zadat:

nick site:http://xchat.centrum.cz/meeting/

Stejně důležité může být prohledání příspěvků týkající se uživatele na fórech:

nick site:http://xchat.centrum.cz/forum

Pozn. místo "nick" se zadá konkrétní přezdívka uživatele, která se chce zkoumat.

3 Analýza PC

3.1 Analýza lokálních dat

K vyhledávání a analýze dat se využilo jednak virtuálního prostředí Wmware Workstation 7, kde se virtualizovalo Windows 7 na oddíle o malé velikosti pro snadnější a rychlejší vyhledávání. A zároveň i vlastního stolního počítače, který mohl rychle prohledávat jak virtuální počítač, tak svoje vlastní datové fondy, případně je porovnat. Aby se nějaké datové fondy vůbec našly, je potřeba "zachatovat si" a vytvořit si tak dohledatelná data.

Jelikož se neví, jaký prohlížeč uživatel používá, byly proto vybrány tři nejpoužívanější, dle říjnových statistik roku 2012, ze serveru nermarketshare.com[4)], a to jsou Internet Explorer, Firefox Mozilla a Google Chrome.

K prvotnímu vyhledávání souborů se využilo programu Google Desktop, pomocí něhož se nejprve indexovaly veškeré vybrané typy souborů. Po naindexování se mohlo začít se samotným vyhledáváním řetězců, například xchat, použitý nick apod. Prohledávání těchto řetězců probíhalo nejen v názvech, ale i v obsahu indexovaných souborů. Výsledky hledání představovaly především cache soubory prohlížečů.

K bližšímu zkoumání vybraných nalezených souborů se vystačilo s forenzním nástrojem AccessData FTK imager 3.0, který byl schopen zobrazit obsah jak v binární podobě, tak v textové, a umožnil vyhledávání řetězců ve znakové sadě Unicode.

Potencionální data na lokálním počítači na základě komunikace na xChatu:

- Cookies
- Ukládání jmen a hesel v prohlížečích
- Historie prohlížeče
- Cache prohlížeče
- Systémový adresář Temp
- Stránkovací soubory
- Otisk fyzické paměti

4) Přístup z internetu 19.11.2012, http://www.netmarketshare.com/browser-market-share.aspx?qprid=0&qpcustomd=0

3.2 Cookies

Portál www.xchat.centrum.cz si ukládá cookies. Co může být zajímavý údaj u cookies, je datum vypršení, které může být i několik let od doby vzniku. V případě, že uživatel nesmazal své cookies, může se jednat o první vodítko povrzující možnou aktivitu.

Cesty k zobrazení cookies v prohlížečích:

- Internet Explorer verze 8 neobsahuje vlastní cookie zobrazovací seznam:
  - Nástroje/Možnosti Internetu/Obecné/Historie procházení – Nastavení/Zobrazit soubory
- Mozilla Firefox verze 17.0
  - Nástroje/Možnosti/Soukromí/odebrat některá cookies
  - Následně se vyhledá řetězec xchat
- Google Chrome verze 23.0
  - Nastavení/Ochrana soukromí/Nastavení obsahu/Všechny soubory cookies a data webu
  - Následně se vyhledá řetězec xchat

Při bližším zkoumání se zjistilo, že Mozilla Firefox i Google Chrome si své cookies ukládají do databází. V Mozille Firefox se proto využilo doplňkové stažitelné aplikace SQLite Manager 0.7.7 a tímto nástrojem se dále analyzovaly nalezené cookies databáze. Po nalezení xChat cookie typu _utma[5)] byla zjištěna její doba platnosti a opravdu měla platnost následující dva roky. Cookie typu _utmz[6)] u prohlížeče Google Chrome si ve své hodnotě uchovávala dokonce uživatelské číselné id, které přísluší příhlášenému xChat profilu. Zbylé hodnoty v cookies slouží ve větší míře ke statistice. Měří se počet navštívení, čas posledního navštívení, čas prvního navštivení nebo například průměrný čas, jak dlouho se dotyčný uživatel zdrží na dané stránce.

Internet Explorer své cookies neukládá do databáze, ale do pouhých textových dokumentů typu .txt, které je možno snadno otevřít v Poznámkovém bloku. Kromě časových hodnot uvnitř těchto souborů, se v jednom z nich taktéž nalézalo uživatelské id.

5) Cookie typu _utma sleduje například počet návštívení, první, poslední návštěvu
6) Cookie typu _utmz informuje odkuď návštěvník přišel (pomocí vyhledavače, odkazu atp.)

3.3 Ukládání jmen a hesel v prohlížečích, identifikace uživatele

Vzhledem k faktu, že komunikace probíhá výhradně přes prohlížeč, šance, jak zjistit přezdívku uživatele je možná vytažením jména a hesla z funkce, která po pokusu přihlášení se do inkriminovaného systému, nabízí možnost uložení nebo pamatování si jména a hesla při případném opětovném navštívení. Pouze Internet Explorer potřebuje specializovaný software na zjištění jména a hesla. Nutno podotknout, že v případě použití přihlašovacích údajů se dopouštíme trestného činu, v rámci analýzy je v zájmu pouze login. Zbývající prohlížeče nabízejí zobrazení jmen přímo v prohlížeči. Účelem hledání nemusí být pouze získání xChat loginu, je možno prohlédnout další portály, které dotyčný majitel počítače mohl používat. Kromě Internet Explorer prohlížeče jsme, bohužel, závislí na pohodlnosti uživatele, zda-li si vybral možnost uložit přihlašovací údaje. Utilita pro Internet Explorer umí vyhledat a zobrazit i tzv. autocomplete. Jedná se o našeptávač úspěšných či neúspěšných pokusů o přihlášení na určité stránce.

Mozilla Firefox verze 17.0 nabízí zobrazení přihlašovacích údajů s následující cestou:
Nástroje / Možnosti / Zabezpečení / Zobrazit hesla...
V případě, že uživatel nemá zapnutou ochranu pomocí hlavního hesla, jsme schopni zjistit veškeré uložené přihlašovací údaje.
V Google Chrome verzi 23.0 se přihlašovací údaje dají zobrazit:
Nastavení/Zobrazit rozšířená nastavení/Hesla a formuláře/ Spravovat uložená hesla

Co se týče konkrétních souborů na disku, v kterých jsou uloženy příhlašovací údaje, každý prohlížeč si to vyřešil po svém. Nejsnazší zjištění přihlašovacích jmen je u prohlížeče Google Chrome. Ty si opět ukládá do databázového souboru, konkrétně inspektovaný soubor Login Data v tabulce login obsahoval atribut username_value a jejich hodnoty odpovídaly použitým jménům. Hesla byla z bezpečnostních důvodů šifrována.

Mozilla Firefox si taktéž ukládá jména do databázového souboru signons.sqlite, ale šifruje nejen hesla, ale i jména pomocí šifrovací metody 3DES[7)]. K rozšifrování je potřeba klíč, který obsahuje soubor key3.db, nicméně i tento soubor se nedá číst v plain[8)] textu.

7) Triple DES – bloková šifra DES, aplikovaná třikrát
8) Plain – z angličtiny : prostý, jasný

Internet Explorer si tyto údaje ukládá do registrů, které jsou opět zašifrované 3DES: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2

Obrázek 2 : Zobrazení xchat loginů s pomocí IE Password Decryptor v4.5

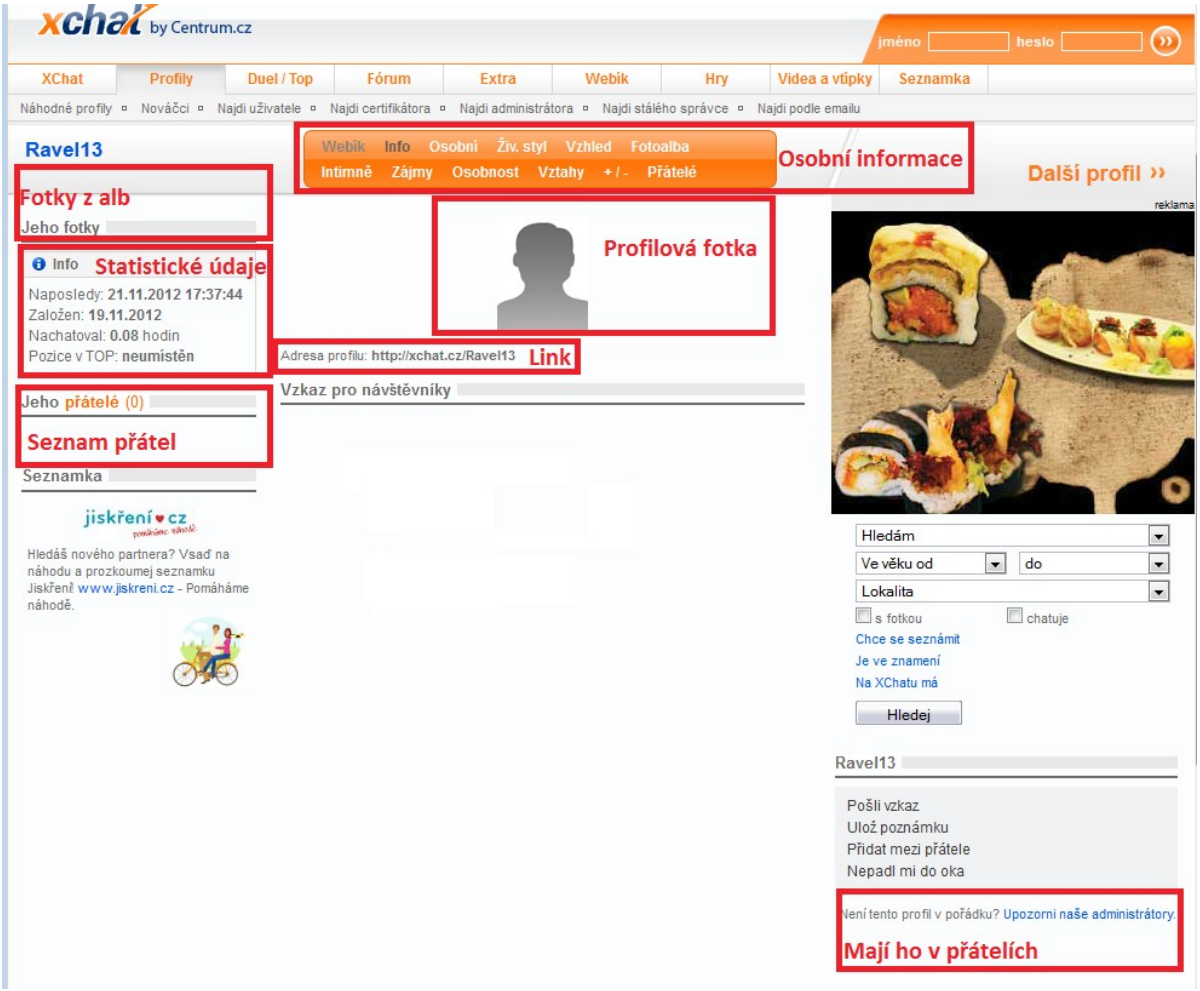
Použitá utilita má freeware licenci a funguje pro prohlížeč Internet Explorer verze 4 až 9. Podmínkou zobrazení záznamů je potřeba, mít otevřený Internet Explorer na dotyčné přihlašovací stránce. Nutno počítat s možnými překlepy, které mohl uživatel provést.

3.3.1. Identifikace uživatele

Po zjištění přihlašovacího jména je možno inspektovat profil pomocí vyhledávací funkce na portálu xchat.cz, nebo zadáním následujícího linku do adresního řádku:

http://xchat.cz/nick

Pozn. namísto "nick" se zadá nalezené přihlašovací jméno



Obrázek 3 : Náhled a popis vytvořeného profilu

Identifikovat uživatele můžeme pomocí jeho zveřejněných fotek, seznamu přátel, uvedeného pravého jména, příjmení čí bydliště nebo jiných uvedených informací, které byly uvedeny v časti Představení portálu.

3.4 Historie prohlížeče

Pokud si uživatel zabaveného počítače nechává ukládát historii prohlížeče, a v dotyčném prohlížeči se vyskytují záznamy o xChat webu, jedná se o přímý důkaz využívání jeho služeb a vzniká velká potencionální šance najít nějakou vlastní komunikaci v souborech, které se budou analyzovat v následujících kapitolách. Seznam s historií navštívených stránek nabízí všechny prověřované prohlížeče pomocí klávesové zkratky CTRL + H. Pouze u Google Chrome, po vyhledání řetězce xchat, bylo možno zjistit datum, kdy byl dotyčný na daném odkazu. U Mozilly Firefox a Internet Exploreru se při vyhledání přichází o tento časový údaj a zobrazí se pouze navštívené odkazy.

Vyhledatelné údaje z historie, které ukládají prohlížeče na základě používaní xChat služeb:

- Zobrazené profily
- V případě příhlášení, v některých odkazech i uživatelské id
- Odkazy o pokus o vstup do místnosti
- Odkazy na prohlížené srazy
- Odkazy na fóra
- Datum navštívení

Mozilla Firefox i Google Chrome opět nabízejí volně otevíratelné databáze s obsahem historie prohlížení. Mozilla používá soubor places.sqlite a Google Chrome si vytváří databázové soubory s měsíčním obsahem historie. Též se zde nachází soubor History, který obsahuje veškerou historii. Poslední testovaný prohlížeč Internet Exlorer si uchovává historii v souborech index.dat.

Analýzou obsahu těchto databází a souborů index.dat se nezjistilo nic víc než to, co umožňuje prosté zobrazení historie v prohlížeči.

Adresáře k souborům s historií, v pořadí Internet Explorer, Mozilla Firefox, Google Chrome:

<oddíl>:\Users\<user>\AppData\Local\Microsoft\Windows\History\History.IE5

<oddíl>:\Users\<user>\AppData\Roaming\Mozilla\Firefox\Profiles\9afpej5z.default

<oddíl>:\Users\<user>\AppData\Local\Google\Chrome\User Data\Default

3.5 Temp

Systémový adresář Temp se může spustit příkazem $Temp$ a nachází v následující lokaci:

<oddíl>:\Users\<user>\AppData\Local\Temp

Tento adresář byl prohledán až po vytvoření aplikace, která potvrdila výskyt souboru, v jehož obsahu byly nalezeny řádky ohledně xchatování. Jednalo se o pouhý jeden textový soubor o velikosti 5MB. Jméno souboru se jeví jako velmi podobné generování jmen u cookies .txt souborů. Soubor byl nalezen ve složce adtemp. Při bližší analýze souboru, kromě xChat komunikace, zde bylo možné nalézt i různé hlavičky z jiných webových serverů a dalších záznamů, ne vždy v čitelné podobě.

3.6 Cache prohlížeče

Slouží k dočasnému uložení obsahu navštívených stránek, které se při opětovném zobrazení načtou rychleji. Jedná se především o obrázky, ikony. Nastavení maximální povolené velikosti ukládání na disk a frekvenci obnovování dokumentů má v režii uživatel, stejně tak jejich zakázání.

Cache adresáře prohlížečů:

- Internet Explorer 8.0
  - <oddíl>:\Users\<user>\AppData\Local\Microsoft\Windows\Temporary Internet Files
- Firefox Mozilla 17.0
  - <oddíl>:\Users\<user>\AppData\Local\Mozilla\Firefox\Profiles\<code>.default\Cache
- Google Chrome 23.0
  - <oddíl>:\Users\<user>\AppData\Local\Google\Chrome\UserData\Default\Cache

Pozn. oddíl znamená jednotku, kde se nalézá systém, "user" se nahradí Windows profilem, "code" značí automaticky generovaný Firefox profil, který se skládá z 8 náhodných písmen a čísel s koncovkou .default

Popis cache souborů, v nichž byla nalezena xChat komunikace, analyzovaných prohlížečů:

Internet Explorer cache obsahovala nejvíce souborů, týkající se xChatu. Uložené byly celé stránky s koncovkou .htm, dokonce měly v názvu modchat, což je jeden z parametrů v adresním řádku v případě, že je uživatel přihlášený a vyskytuje se v jedné z místností. Tyto soubory sice jdou otevřít v prohlížeči, ale jejich obsah se, bohužel, nezobrazí. Během doby cca 2 hodin vlastního xchatování se v konkrétní složce Low\Content.IE5\<random>\ nacházely desítky souborů s názvem modchat, vztahující se k naší analýze.
Pozn. <random> představuje název složky, jejíž osmimístný název je tvořen vybranými čísly a znaky 0-9 a A-Z.

Mozilla Firefox cache se může rozdělit na vnější a vnitřní. Vnější tvoří podadresáře 0-9, A-F s dalšími podadresáři, jež obsahují externí soubory. Vniřní cache se skládá z celkem čtyř souborů:

- _CACHE_MAP_ - slouží k indexaci metadat a cache souborů
- _CACHE_001_ - cache soubor ukládající si data v blocích o velikosti 512 bajtů
- _CACHE_002_ - cache soubor ukládající si data v blocích o velikosti 1024 bajtů
- _CACHE_003_ - cache soubor ukládající si data v blocích o velikosti 4096 bajtů

Výše zmíněné cache soubory byly postupně analyzovány v aplikaci FTK Imager 3.0.1 a dále se uvnitř souborů hledaly řetězce xchat. Kromě mapovacího souboru se ve zbylých třech souborech vyskytovaly bloky obsahující xchat.

Google Chrome má řešení velmi podobné, hlavními cache soubory jsou data_0 až data_3 a mapovací soubor index.dat. Cache adresář taktéž obsahuje externí soubory, ikonky, obrázky.

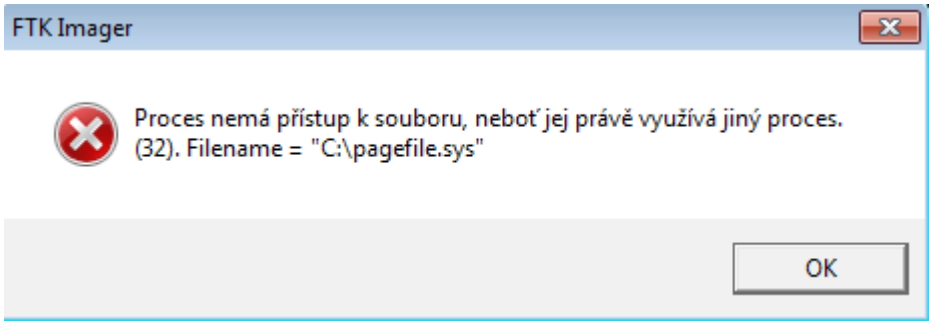
U cache souborů ve všech testovaných prohlížečích byly nalezeny záznamy jak vlastní komunikace, tak zjištění, pokud byl uživatel přihlášený, jeho unikátního, číselného, osmimístného uid.
Zobrazení profilu je funkční i tímto odkazem:

- http://xchat.centrum.cz/whoiswho/profile.php?uid=<uid_number>

3.7 Stránkovací soubory

3.7.1. Pagefile.sys

Soubor pagefile.sys představuje virtuální pamět počítače. Jedná se o skrytý systémový soubor, který v případě potřeby, například při zaplnění fyzické paměti, začne využívat systém. Velikost této paměti bývá zpravidla stejná jako velikost fyzické paměti. Defaultně se tento soubor nalézá přímo v kořenovém adresáři systémového oddílu čili C:\pagefile.sys. V případě, že se bude pokoušet inspektování tohoto souboru na běžícím systému, dostane se pouze odpovědi nemožnosti otevření, neboť jej využívá jiný proces.



Obrázek 4 : Nemožnost čtení stránkovacího souboru

Jednou z možností, jak přistoupit k tomuto souboru, je jeho zkopírování pomocí utility Hobocopy 1.0. Utilita používá řádkový řežim. Technologie, kterou využívá ke samotnému kopírování se nazývá Volume Shadow Copy[9]. Pracuje na principu vytvoření si dočasného otisku souboru, který se posléze kopíruje. Podmínkou je mít povolené zobrazení skrytých a systémových souborů.

Parametry zkopírování daného souboru do vybrané složky:

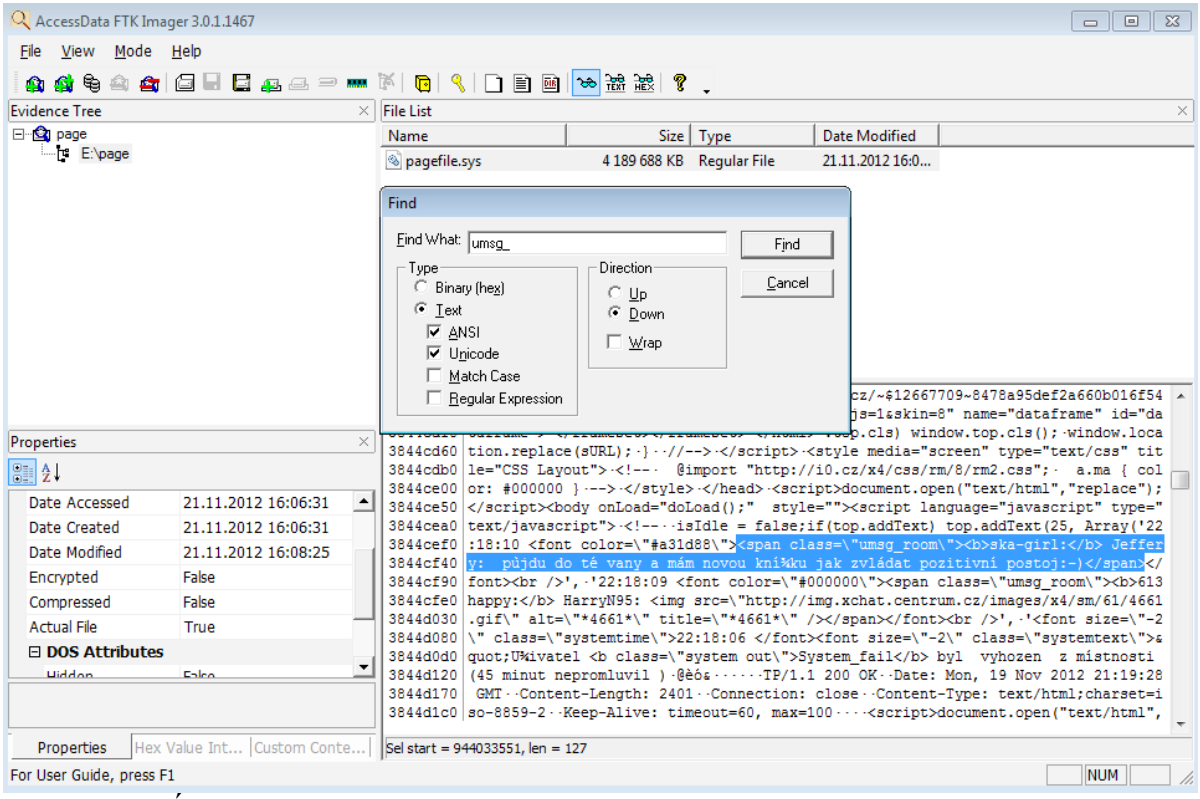
hobocopy.exe_<Složka vstupního souboru>_<Výstupní složka>_<název souboru>

Spodní pomlčka značí mezeru, konkrétní příklad zadaného příkazu:

hobocopy.exe C:\ E:\page\ pagefile.sys

Zkopíroval se soubor pagefile.sys, nacházející se na oddílu C:\, do adresáře E:\page\. K této kopii již proces nepřistupuje a může se dále analyzovat pomocí forenzního nástroje.

9) VSS - Volume Shadow Copy Service je technologie používaná k záloze od Microsoftu



Obrázek 5 : Úryvek nalezené xChat komunikace ve stránkovacím souboru pomocí programu FTK Imager 3.0.1

Stejně tak, jako u cache souborů, se uvnitř stránkovacího souboru hledaly řetězce xchat, následně přezdívky a po získání většího obzoru se přišlo na řetězec umsg_, který obsahoval každý řádek, kde se nalézala vlastní komunikace.

3.7.2. Hiberfil.sys

Podobně jako u pagefile.sys, se jedná o stránkovací systémový soubor, který v systému Windows 7 má obvykle velikost 75% fyzické paměti. Nalézá se taktéž v kořenovém adresáři oddílu. V případě použití funkce hibernace se načte komprimovaný obsah fyzické paměti do zmíněného souboru. Během fáze hibernace se spotřeba pohybuje v jednotkách wattů. Po znovuzapnutí se obsah souboru načte zpět do fyzické paměti a může se pokračovat dále v rozdělané práci. Stejně tak jako u pagefile.sys, systémový proces využívá tento soubor. Postup k inspektování je totožný jako pro výše zmíněný soubor.

3.8 Další možná naleziště

Další způsob nálezu dat může být otisk fyzické paměti. Záloha jako taková se ale musí provést při samotném zabavování počítačové techniky v případě, že je uživatelův počítač zapnutý. Zálohu paměti nabízí i doposud hojně používaný nástroj FTK Imager 3.0.1.

Ve stálých místnostech se mohou vyskytovat i neživí účastníci, jedná se o takzvané boty, kteří mají za úkol například informovat o srazech, zpříjemňovat náladu zúčastněným v místnosti pomocí vtipů, zdravit příchozí a nebo dělat reklamu. Bot není nic jiného, než běžící program, ovšem ne každý ho smí provozovat. Vzhledem k možnostem, co se takovému programu nabízí, je dosti pravděpodobné, že si může neustále ukládat obsah historie skla do logů. Pokud tedy vyšetřovaná osoba vlastní bota (tyto osoby mající boty jsou zveřejněny na xchat webu), má smysl prohledat i botí adresář.

4 Software

4.1 Současné řešení

Doposud není známo nebo nebylo vytvořeno žádné softwarové řešení, které by umělo vyhledat a vyexportovat vlastní komunikaci z dočasných a systémových souborů na základě xchatování.

4.2 Požadavky

Na základě analýzy dat se zvolilo, že nejcennější data jsou výtažky ze souborů, které obsahují vlastní komunikaci – čili opravdové záznamy chatu od uživatele a zároveň i od ostatních účastníků v místnosti. Nalezené záznamy budou sloužit jako důkaz či potvrzení různých aktivit, které mohly provádět podezřelé osoby, jimž byla zabavena počítačová technika. Představa použití programu je taková, že soudní znalec nebo pověřená osoba připojí image[10)] disku počítače podezřelé osoby. K této záloze se přistupuje jako k celé jednotce.

Požadavky aplikace:

- Automatické prohledání vybrané jednotky
- Prohledání vybraných souborů nebo celé složky
- V prohledávaných souborech nalézt řetězce s komunikací
- Nalézt uid přihlášených uživatelů
- Přehledné zobrazení nalezené komunikace v tabulce
- Možnost filtrovat
- Možnost identifikace
- Exportování záznamů do .xls

10) Image – z angličtiny : obraz, podoba; plnohodnotná kopie

4.3 Postup

Aplikace bude napsána v programovacím jazyce Java, ve vývojovém prostředí NetBeans IDE 7.0.1. Při zakládání projektu se využilo připravené šablony Java desktop aplikace. Ta vygenerovala 3 třídy, App.java, View.java a AboutBox.java, které se následně modifikovaly podle potřeb. Prvotní představa grafické stránky, jak bude vypadat aplikace, je taková, že se bude skládat ze základního ovládacího okna s tlačítky, umožnující vyhledávat, a dále zobrazení nového okna s výsledky. Původní verze programu měla být pouhým skriptem bez grafického rozhraní. Nutno dodat, že na grafice programu není postavena funkčnost aplikace, tudíž jí nebyla věnována velká pozornost. Důležitost se bude klást na funkčnost algoritmů a zobrazení správných výsledků.

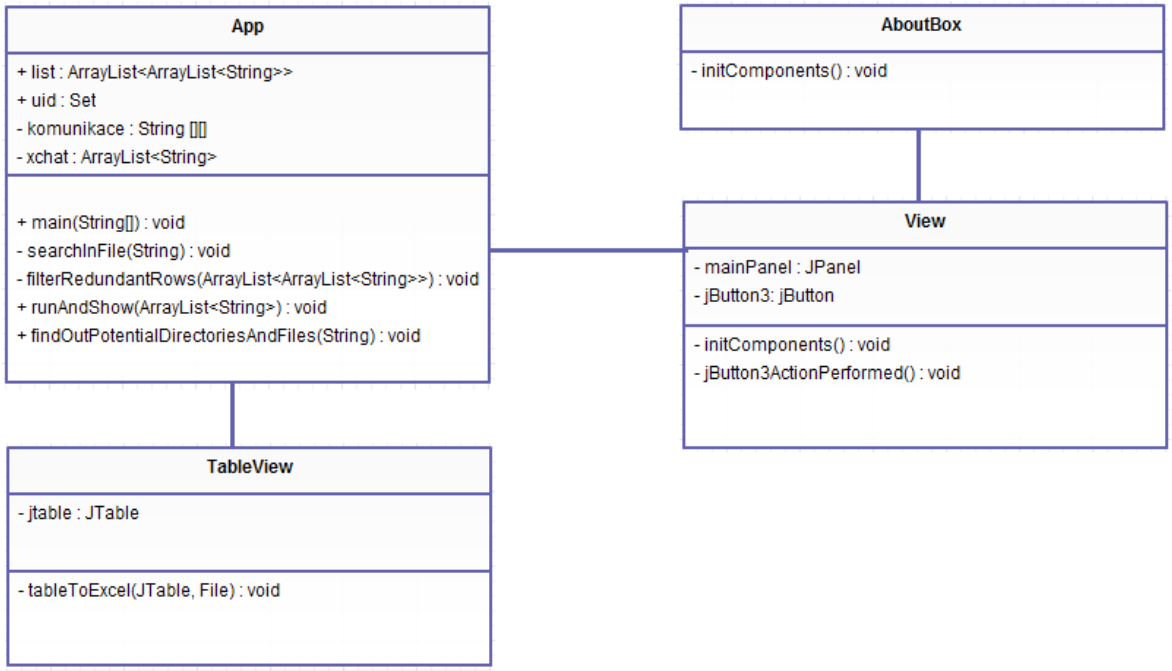
4.4 Návrh řešení

Na základě požadavků aplikace se sestavil základní model algoritmů, popisující funkce aplikace. Tento model bude sloužit jako vodítko, kterého se budeme držet během implementace a dle něj budou vznikat potřebné metody a proměnné. Model probíhá zleva doprava.

Obrázek 6 : Základní model funkcí v aplikaci

4.4.1. Rozdělení a popis tříd

- Třída App
  - bude pracovat se soubory, číst v souborech, získanou komunikaci bude ukládat do kolekce
- Třída View
  - bude zobrazovat základní okno aplikace s tlačítky, podle tlačítka bude spouštět hledací metody v třídě App
- Třída AboutBox
  - tvoří okno s informacemi o aplikaci
- Třída TableView
  - zobrazí nové okno s výslednou kolekcí v tabulce



Obrázek 7 : Výsledný class diagram po implementaci s hlavními metodami a proměnnými

4.5 Implementace

Pro práci se soubory se využije knihovny Commons.IO 2.4 (org.apache.commons.io) a konkrétně třídy FileUtils, která usnadní práci s adresářovou strukturou při prohledávání. Tato třída vlastní metodu listFiles(), a ta na základě parametru cesty k adresáři, uchovává kolekci obsahující všechny soubory včetně podsložek.

V souborech se bude prohledávat řádek po řádce, nesmí se zapomenout na čtení ve správné znakové sadě. Pro zaručení správného zobrazení všech pismen s háčky a čárkami se použije sada Iso-8859-2. Zde se využije několika tříd pro práci se soubory a proudy dat FileInputStream, DataInputStream, InputStreamReader a BufferedReader, které společně tvoří metodu na čtení řádku.

K vybrání jednotky představující zálohu disku bude sloužit ruční vepsání jednotky do JTextField nebo tlačítko, co otevře JFileChooser. Pomocí tlačítka se zobrazí klasické okno s adresářovou strukturou pro výběr chtěné jednotky.

Zahájení automatického vyhledávání bude spočívat ve stisku dalšího tlačítka, které bude mít za úkol ověřit, zda uživatel správně zadal nebo vybral jednotku. Ověření správnosti jednotky se provede pomocí metody listRoots(), kterou vlastní třída File. Tato metoda vrací kolekci kořenových adresářů.

Automatické vyhledávání bude prohledávat veškeré složky a soubory nacházející se na vybrané jednotce a bude porovnávat Stringy řetězců jejich adresářových cest s námi analyzovanými adresáři a soubory obsahující možnou xChat komunikaci.

U Windows 7 jsou to konkrétně řetězce:

- Internet Explorer cache
  - "AppData\\Local\\Microsoft\\Windows\\Temporary Internet Files"
- Mozilla Firefox
  - ".default\\Cache"
- Google Chrome
  - "AppData\\Local\\Google\\Chrome\\UserData\\Default\\Cache"
- Stránkovací soubory
  - "hiberfil"
  - "pagefile"

Tímto globálním hledáním se vyhneme problémům, když se například na dané jednotce vyskytuje více logických oddílů, více systémových uživatelských účtů na jednom z oddílů, nebo v případě počtu nebo jiných než defaultních lokací u stránkovacích souborů. Tyto řetězce budou mít všichni společné. V případě totožnosti nalezené adresářové cesty se tato cesta uloží do kolekce a po prohledání celé jednotky se zavolá metoda na vyhledání xChat komunikace uvnitř nalezených cest.

Po výběru automatického hledání vyskočí informativní okno typu JOptionPane varující před možnou delší dobou vyhledávání. Během vyhledávání poběží symbolické okno s JProgressBar komponentou, ukazující právě probíhající hledání. Při neúspěšném hledání se zobrazí další informativní JOptionPane potvrzující nenalezenou xChat komunikaci.

Nalezená komunikace se zobrazí v novém okně typu JFrame a bude obsahovat tabulku JTable se čtyřmi sloupci: čas, nick, text a typ zprávy. V dolní části tabulky se budou moci filtrovat řádky pomocí zadaného řetězce do JTextFieldu a potvrzujícím tlačítkem. Při potvrzení prázdného řetězce se zobrazí opět všechny nalezené výsledky. Je zde i tlačítko spouštějící JFileChooser, v němž se vyhledá adresář, kam se chce uložit nalezená komunikace. Zadá se název souboru a data z tabulky se uloží do .xsl formátu. Zde se využilo třídy FileWriter a BufferedWriter k převodu obsahu tabulky do souboru. V horní části okna se objeví JComboBox, obsahující množinu nalezených přihlášených uid, při případném vlastnění více nicků. Identifikace profilu dle uid proběhne pomocí tlačítka, které otevře defaultní prohlížeč na stránce profilu. Podle navštíveného profilu je možno dozvědět se opravdovou přezdívku a podle té například filtrovat.

Kromě nabídky automatického vyhledávání v úvodním okně aplikace se bude moci vyhledávat i v konkrétních souborech či složkách. Zde se využití této funkce může hodit v případě vyhledávání například u jiných systémů, kde je jiná adresářová struktura, při zkoumání otisku fyzické paměti nebo jiného souboru. Očekává se, že xChat nebude nijak zásadním způsobem měnit své vnitřní proměnné, podle kterých se hledá.

4.5.1. Popis extrahovací metody v třídě App

Nejprve je třeba přesně zjistit, co konkrétně se vyskytuje v souborech s xChat komunikací. Příklad jednoho z řádků, kde se nachází chatování:

top.addText(25,Array('21:16:50<fontcolor=\"#000000\"><spanclass=\"umsg_whwi\">Livevil: caf
'),1,1)

Z řádku jsme schopni zjistit čas, odesílatele, jeho text a typ zprávy. Tyto čtyři hodnoty budou představovat sloupce v později zobrazené tabulce. Typ zprávy se v programu bude rozlišovat pouze na: Soukromá a Na sklo. V řádcích se dalo rozlišit, zda se jedná o chat na skle nebo v novém šeptacím okně. "umsg_" sekvence se jeví jako společný průnik všech řádků, to, co měly společné - zároveň unikátní, odlišující se od nechtěných řádků. Po nalezení této sekvence v řádku se dále užívá metody split(), kterou vlastní třída String.

Příklad užití metody k získání času z řádku:

line.split("<fontcolor|Array('")[1];

Jako parametr je použit regulární výraz, který značí konec a začátek místa, který nás v řádku zajímá. Rozdělení konce a začátku je znakem | , metoda split() původně vrací pole Stringů, aby se uložila do proměnné pouze námi chtěná sekvence znaků, je třeba zvolit vrácení prvního prvku v poli. Nulté by vrátilo sekvenci před začátkem výrazu.
Podobným postupem se pokračovalo i u zbývajících sloupců. Nalezené hodnoty se ukládají do kolekce ArrayListů.

4.6 Testování

Byly provedeny uživatelské testy, které by případně mohly přispět k nalezení nefunkčnosti programu. Na základě těchto testů byly upraveny metody a hlášky.

- Testování správného výběru jednotky
  - Při výběru jiného adresáře než kořenového se tento výběr nepotvrdí
  - Stejné nepřijmutí nastává při ručním vepsání do daného pole
- Testování během hledání
  - Po dobu hledání je zobrazeno informační okno
  - Při nenalezení xChat komunikace je tato skutečnost oznámena
- Testování funkce filtrování
  - Filtr je case sensitive, po zadání řetezce a jeho potvrzení se správně obnoví tabulka
  - Při zadání prázdného řetězce se opět zobrazí původní výsledky
- Při identifikaci profilu je zapotřebí internetového připojení
  - Chybu o nemožnosti zobrazení stránky oznámí daný prohlížeč
- Testování otisku fyzické paměti
  - Za pomoci programu FTK Imager byla provedena záloha operační paměti a následně úspěšně nalezena xChat komunikace

5 Budoucnost

5.1 Návrhy pro možné rozšíření

- Rozšíření pro vyhledávání vlastní komunikace dalších sociálních sítí
- Podpora více typů souborů jako výstup
- Analýza datových fontů jiných systémů (Linux, Macintosh, mobilní systémy)
- Podpora automatického vyhledávání v jiných systémech než Windows
- Práce s databází prohlížeče k zjištění navštívených profilů
- Analýza dat v případě, že vlastník je majitelem tzv. bota
- Podpora dalších prohlížečů

6 Závěr

6.1 Shrnutí

V bakalářské práci se analyzovaly datové fonty, které se na základě používání xChatu mohou vyskytovat na lokálním počítači. V analýze byly probírány datové fonty třech nejpoužívanějších prohlížečů a systémové soubory. Jako nejcennější nález pro policii se jeví vlastní komunikace, která byla v datových fontech nalezena. Z daných fontů je možno zjistit uživatelské unikátní číslo, kterým se může odkázat na konkrétní daný profil, a tím ho identifikovat.

6.2 Zhodnocení

V práci bylo dosaženo všech zadaných cílů. Po analýze datových fontů se vyhodnotilo, jaké údaje je možno získat. Vytvořená aplikace tyto údaje z připojeného otisku disku umí automaticky vyhledat a zobrazit, s možností uložení. Uloženou komunikaci budou dále zkoumat znalci, zabývající se například odhalováním zločinu. Z komunikace je možno se dozvědět spojující linku pachatele a oběti.

Vzhledem k pravděpodobné nepřítomnosti jiného xChat komunikace extraktoru se tato aplikace může považovat za první svého druhu.

7 Použitá literatura

7.1 Portály

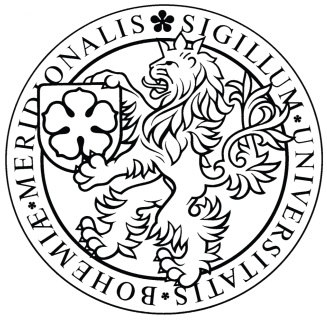
- Oracle Java Documentation. [online]. [cit. 2012-11-25].
  - http://docs.oracle.com/javase/
- xChat portál.[online]. [cit. 2012-11-25].
  - http://xchat.centrum.cz/
- Nirsoft.[online]. [cit. 2012-11-25].
  - http://www.nirsoft.net/
- Ing.Jaroslav Kothánek, Ph.D. [online]. [cit. 2012-11-25].
  - http://www.it-znalec.cz/
- Sleuthkit. [online]. [cit. 2012-11-25].
  - http://www.sleuthkit.org/
- Commons IO. [online]. [cit. 2012-11-25].
  - http://commons.apache.org/
- Stack OverFlow. [online]. [cit. 2012-11-25].
  - www.stackoverflow.com/
- Hobocopy. [online]. [cit. 2012-11-25].
  - https://github.com/candera/hobocopy/
- OSforensics.[online]. [cit. 2012-11-25].
  - http://www.osforensics.com/
- FTK imager 3.1.1.[online]. [cit. 2012-11-25].
  - http://www.accessdata.com/support/product-downloads/
- Vmware.[online]. [cit. 2012-11-25].
  - http://www.vmware.com/cz/
- Java2s. [online]. [cit. 2012-11-25].
  - http://www.java2s.com/
- Google desktop. [online]. [cit. 2012-11-25].
  - http://googledesktop.blogspot.cz/

- Mozilla Firefox. [online]. [cit. 2012-11-25].
  - http://www.mozilla.org
- Google Chrome. [online]. [cit. 2012-11-25].
  - https://www.google.com/intl/cs/chrome/browser/
- Internet Explorer. [online]. [cit. 2012-11-25].
  - http://windows.microsoft.com/en-US/internet-explorer/download-ie
- NetBeans. [online]. [cit. 2012-11-25].
  - http://netbeans.org/

8 Přílohy

- CD se zdrojovými kódy, aplikací a bakálářskou práci ve formátu .pdf
- Manuál k obsluze aplikace

Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta



Manuál xChat Xtractor

Příloha bakalářské práce

Pavel Ryneš

Školitel: Ing. Jaroslav Kothánek, Ph.D.

České Budějovice 2012

Obsah

1 Úvod

Na základě bakalářské práce byla vytvořena aplikace zaměřující se na extrahování xChat komunikace z dočasných a stránkovacích souborů. I přes velkou jednoduchost v ovládání je potřeba vytvořit uživatelský manuál, který vysvětlí jednotlivé funkce.

Xchat Xtraktor umí:

- Nalézt na vybrané jednotce cache adresáře a stránkovací soubory
- Vyhledat uvnitř souborů vlastní komunikaci a množinu přihlášených uid
- Zobrazit nalezenou komunikaci v tabulce

2 O programu

2.1 Požadavky a spuštění

Hardware a software požadavky na běh aplikace:

- Procesor: jednojádrové a vícejádrové
- Operační paměť: minimálně 128MB
- Systém: Windows XP, Vista, 7
- Rozhraní: Java SE Runtime Environment(JRE) version 6u38 a vyšší

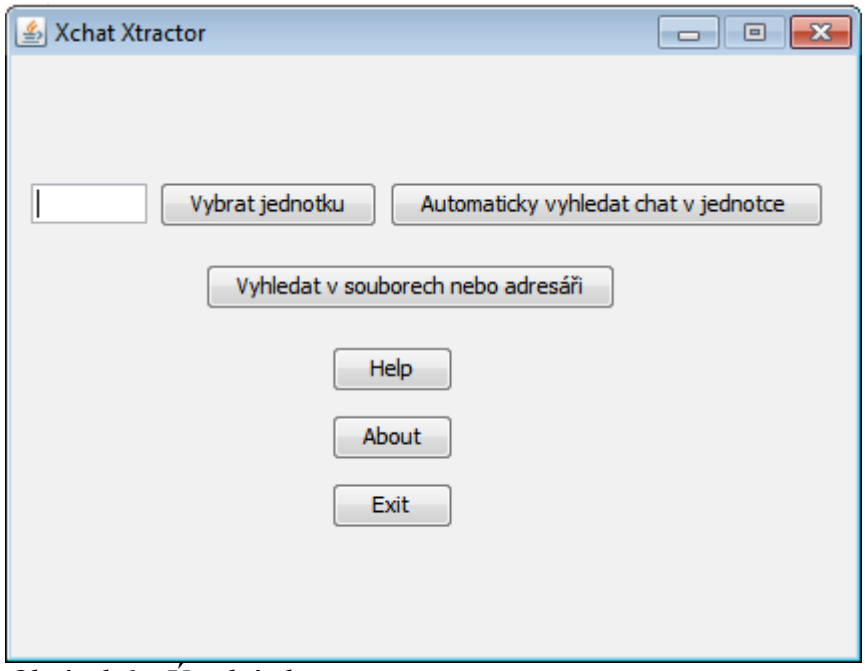
Aplikaci lze spustit souborem XchatSearch.jar. Podmínkou je, aby se ve stejném adresáři nacházela i složka s potřebnými knihovnami lib.

3 Funkce

3.1 Úvodní okno

Aplikace pracuje se dvěma základními typy hledání. První je automatické vyhledávání, jež nejprve prohledává vybranou jednotku a pokouší se nalézt cache adresáře prohlížečů a stránkovací soubory pagefile.sys a hiberfil.sys. Po nalezení cest do těchto adresářů se spustí samotné vyhledávání vlastní komunikace uvnitř souborů a podsouborů. Výběr jednotky je možný dvěma způsoby. První varianta spočívá v ručním vepsání písmene jednotky do formuláře např. "F:/". Druhá je použití tlačítka "Vybrat jednotku", které otevře okno s možným výběrem jednotky. Při správném výběru pouze kořenového adresáře, což představuje načtenou zálohu disku, se vybraná jednotka zobrazí ve formuláři. Nyní se hledání spustí tlačítkem "Automaticky vyhledat chat v jednotce".

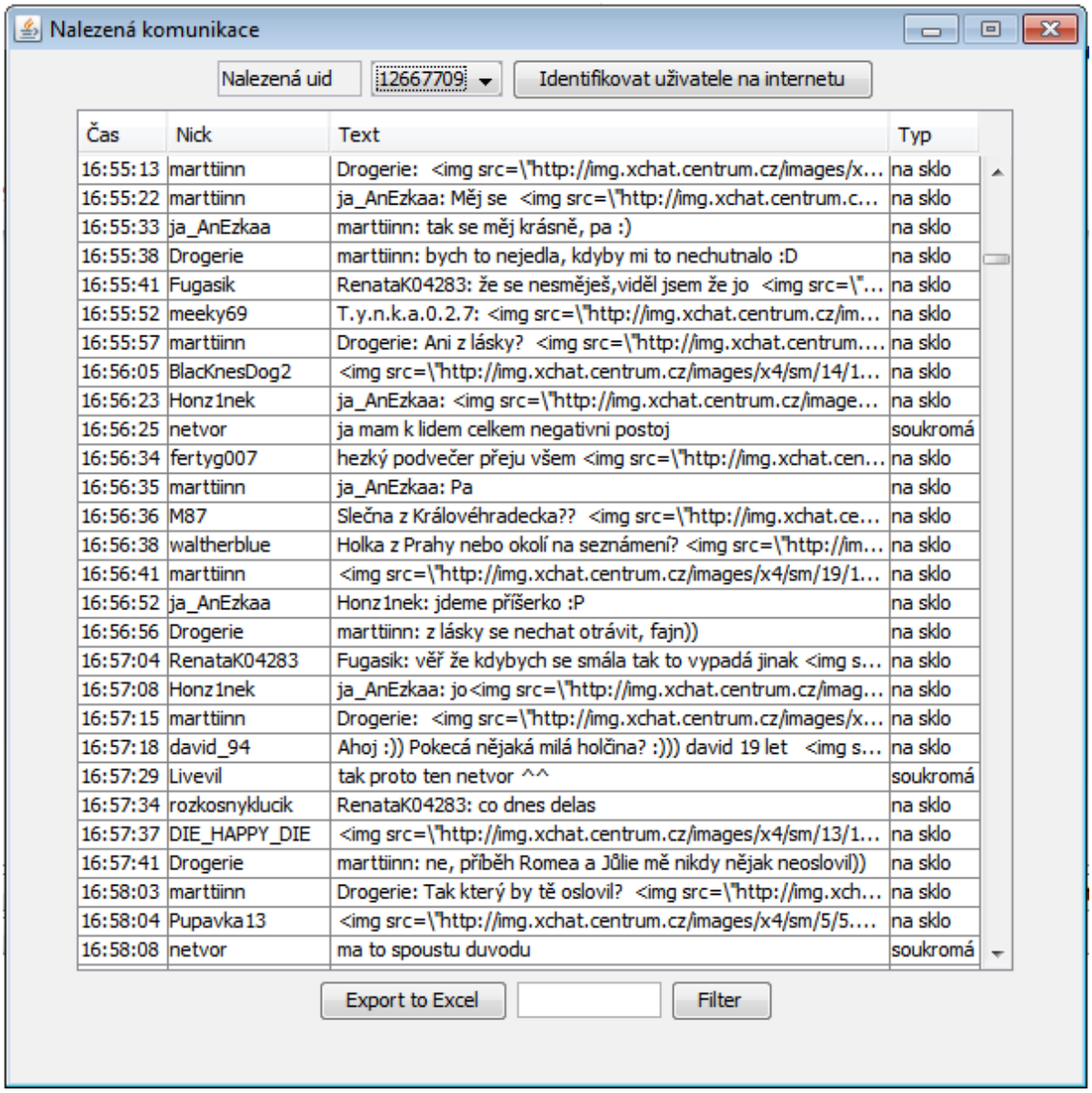
Druhý typ je manuální vyhledávání. V případě volby prohledat konkrétní soubory nebo adresář, jenž by mohl obsahovat vlastní komunikaci, zvolí se tlačítka "Vyhledat v souborech nebo adresáři".



Obrázek 1 : Úvodní okno

3.2 Okno s výsledky

Výsledné okno obsahuje tabulku s nalezeným xChatem. Nad tabulkou se zobrazí množina nalezených uid, uid představuje unikátní profil na xChatu. Po výběru čísla je zde tlačítko "Identifikovat uživatele na internetu", které otevře defaultní prohlížeč na daném profilu. Pod tabulkou figuruje tlačítko "Export to Excel", které zobrazí okno s cestou, kam se chce obsah tabulky uložit a samozřejmě vlastní pojmenování souboru. Filtr je case sensitive, po zadání řetězce do formuláře a stisku tlačítka "Filter", se zobrazí řádky obsahující zadanou sekvenci. Při stisku tlačítka Filter s prázdným řetězcem se opět zobrazí všechny výsledky.



Čas	Nick	Text	Typ
16:55:13	marttiinn	Drogerie: <img src=\"http://img.xchat.centrum.cz/images/x...	na sklo
16:55:22	marttiinn	ja_AnEzkaa: Měj se <img src=\"http://img.xchat.centrum.c...	na sklo
16:55:33	ja_AnEzkaa	marttiinn: tak se měj krásně, pa :)	na sklo
16:55:38	Drogerie	marttiinn: bych to nejedla, kdyby mi to nechutnalo :D	na sklo
16:55:41	Fugasik	RenataK04283: že se nesměješ,viděl jsem že jo <img src=\"...	na sklo
16:55:52	meeky69	T.y.n.k.a.0.2.7: <img src=\"http://img.xchat.centrum.cz/im...	na sklo
16:55:57	marttiinn	Drogerie: Ani z lásky? <img src=\"http://img.xchat.centrum....	na sklo
16:56:05	BlacKnesDog2	<img src=\"http://img.xchat.centrum.cz/images/x4/sm/14/1...	na sklo
16:56:23	Honz1nek	ja_AnEzkaa: <img src=\"http://img.xchat.centrum.cz/image...	na sklo
16:56:25	netvor	ja mam k lidem celkem negativni postoj	soukromá
16:56:34	fertyg007	hezký podvečer přeju všem <img src=\"http://img.xchat.cen...	na sklo
16:56:35	marttiinn	ja_AnEzkaa: Pa	na sklo
16:56:36	M87	Slečna z Královéhradecka?? <img src=\"http://img.xchat.ce...	na sklo
16:56:38	waltherblue	Holka z Prahy nebo okolí na seznámení? <img src=\"http://im...	na sklo
16:56:41	marttiinn	<img src=\"http://img.xchat.centrum.cz/images/x4/sm/19/1...	na sklo
16:56:52	ja_AnEzkaa	Honz1nek: jdeme příšerko :P	na sklo
16:56:56	Drogerie	marttiinn: z lásky se nechat otrávit, fajn))	na sklo
16:57:04	RenataK04283	Fugasik: věř že kdybych se smála tak to vypadá jinak <img s...	na sklo
16:57:08	Honz1nek	ja_AnEzkaa: jo<img src=\"http://img.xchat.centrum.cz/imag...	na sklo
16:57:15	marttiinn	Drogerie: <img src=\"http://img.xchat.centrum.cz/images/x...	na sklo
16:57:18	david_94	Ahoj :)) Pokecá nějaká milá holčina? :))) david 19 let <img s...	na sklo
16:57:29	Livevil	tak proto ten netvor ^^	soukromá
16:57:34	rozkosnyklucik	RenataK04283: co dnes delas	na sklo
16:57:37	DIE_HAPPY_DIE	<img src=\"http://img.xchat.centrum.cz/images/x4/sm/13/1...	na sklo
16:57:41	Drogerie	marttiinn: ne, příběh Romea a Jůlie mě nikdy nějak neoslovil))	na sklo
16:58:03	marttiinn	Drogerie: Tak který by tě oslovil? <img src=\"http://img.xch...	na sklo
16:58:04	Pupavka13	<img src=\"http://img.xchat.centrum.cz/images/x4/sm/5/5....	na sklo
16:58:08	netvor	ma to spoustu duvodu	soukromá

Obrázek 2 : Výsledné okno

4 Výstup

4.1 Excelovský soubor

Výsledný soubor tvoří právě zobrazené záznamy v tabulce. Koncovku souboru při ukládání není nutné zadávat. Universální soubor s koncovkou .xsl se může zobrazit jak v programu Microsoft Excel z balíku MS Office tak v Calc od Open Office.