Russian IM- applications: «Mail.ru Agent»

Olga Kapinus,
Igor Michailov,
Igor Yurin

Introduction

For the last year we have received several messages from our foreign colleagues, in which they asked for help in the research of history, created by the IM-applications, which had been developed by the Russian manufacturers, such as «Mail.ru Agent», «Rambler ICQ», «IceIM», «QIP», «QIP Infinium», «&RQ», «&ML», etc.

There is practically no information about these programs in English and most widespread foreign programs for forensic researches do not support history formats of IM-applications created by the Russian developers. The given cycle of articles aims at compensating of informational vacuum on methods and means of forensic research of the IM-applications, created by the Russian developers and widely used on the territory of the post-Soviet area as well as by the emigrants, natives of Russia, who live abroad and use IM-applications to communicate with their relatives, friends, acquaintances, who live in the homeland.

1. About «Mail.ru Agent»

«Mail.ru Agent» is an own development of the Mail.ru Company (www.mail.ru). According to the data of the company Mail.ru [1], more than 1 million people use the program «Mail.ru Agent» at the same time.

With the help of «Mail. Ru Agent» the user can use several connection means:

• instant messages;

• free SMS to mobiles;

• voice contact;

• telephone calls all around the world.

The program is constantly developing and increasing its functionality. The program interface is realized in five languages: Russian, English, Ukrainian, Kazakh, and Uzbek. There is unicode support in messages and ICQ protocol support. «Mail.ru Agent» works under Windows 2000, XP and Vista operational systems. There are versions of the program «Mail.ru Agent» for the operating system of Windows Mobile and on Java: «Mail.ru Agent Java». Functionality of different versions of the program «Mail.ru Agent» is described in the Table №1.

Table №1

Functionality of different versions «Mail.ru Agent»

Function	The program version		
	«Mail.ru Agent» for PC	«Mail.ru Agent Java»	«Mail.ru Agent» for PC
Instant messages exchange	X	X	X
Calls to standard phones	X		
Send SMS for free	X	X	X
Voice communication	X		
Online games	X		
New friends search	X	X	X
Smileys	X	X	X
Spam protection	X	X	X
Flesh-rollers exchange	X		
New version notification	X	X	
Video calls	X		
Choose color scale	X		
Function «Alarm»	X	X	X
Files exchange	X		
Spell checking «on the move»	X		
Search in the contact list	X		
Notification about new letters	X	X	X
Birthdays reminder	X	X	X

Sort contacts	X	X	X
Location of contacts in any place of a desktop	X		
Personal photos of the contact	X		
Visibility settings	X		
Information about counterparts	X		
Possibility of usage of different accounts	X		
Contacts from mobile phone	X	X	
ICQ protocol support	X		

Directly distributive of the program «Mail.ru Agent» is available for downloading at: http://agent.mail.ru/en/.

Answers to frequently asked questions, in English, can be viewed at: http://agent.mail.ru/en/help/.

Now there are alternative clients for «Mail.ru Agent» network: «&ML», «QIP Infium», «Miranda IM», etc. «Mail.ru Agent» carries out data exchange under its own protocol - MMP. The description of the given protocol is located at: http://agent.mail.ru/ru/developers/protocol.html.

2. How it looks

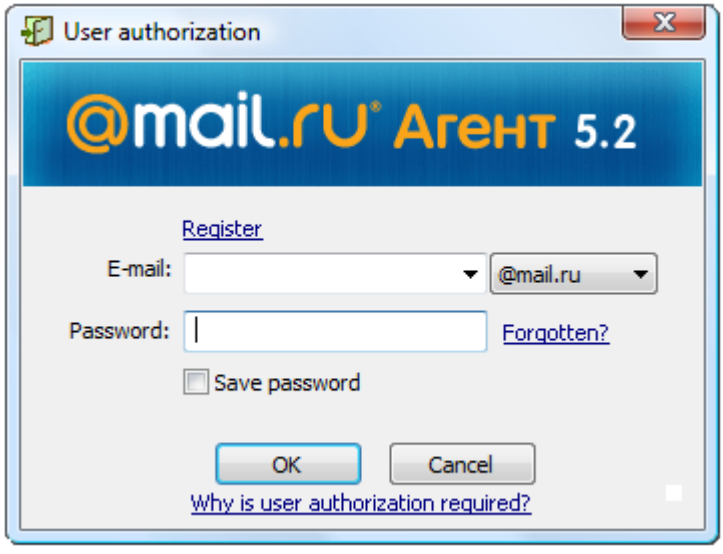

Fig.1. Authorization. [2]

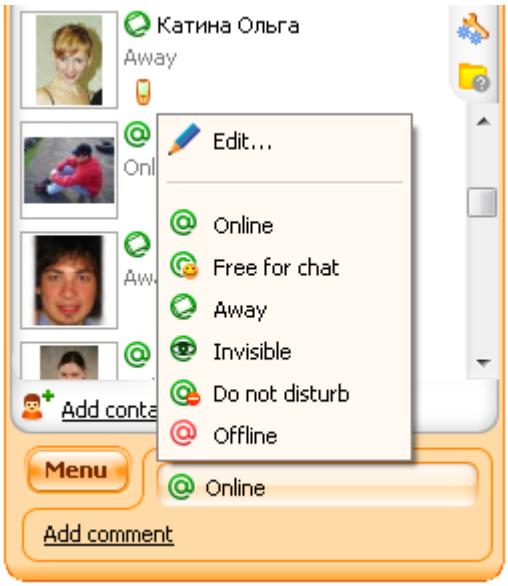

Fig.2. Status change. [2]

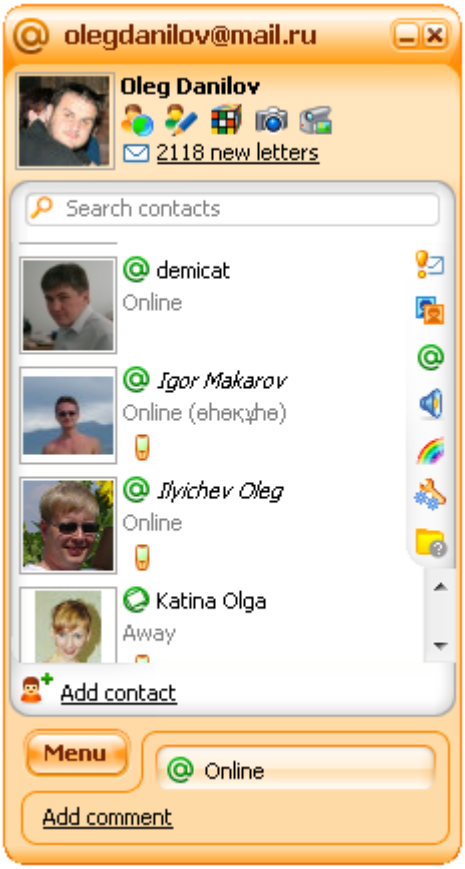

Fig.3. Contact list. [2]

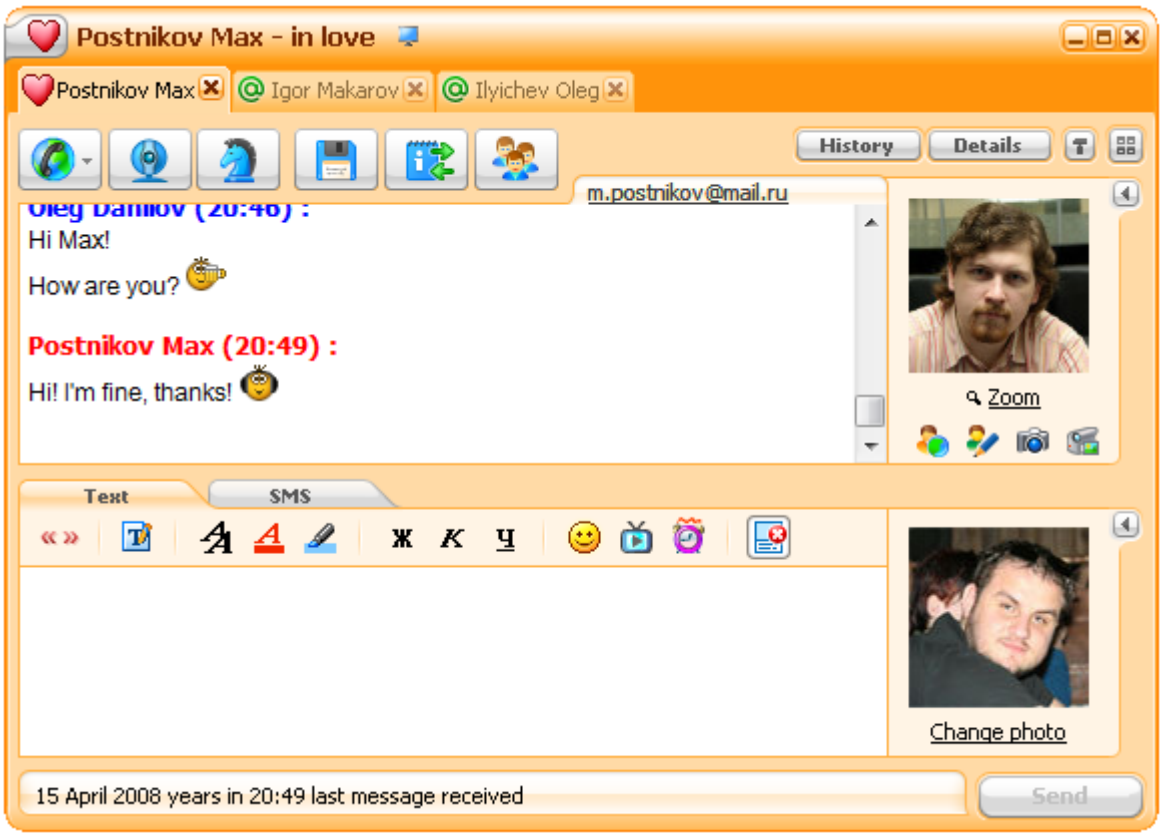

Fig.4. Messages exchange. [2]

3. «Mail.ru Agent» forensic research

Before starting telling about methods of forensic research of «Mail.ru Agent» data, it should be mentioned, that «Mail.ru Agent» is a complicated object for a forensic researcher. It is so, first of all, due to the fact that developers constantly improve protection mechanisms of confidential information of the users of the program «Mail.ru Agent». Methods and means which are nowadays used by a forensic researcher for the analysis of «Mail.ru Agent» data, will, probably, appear inapplicable tomorrow at the new version «Mail.ru Agent» release.

3.1. Storage of program and history settings.

As it has already been mentioned above, «Mail.ru Agent» is an own development of the Mail.ru Company . Message exchange is performed by means of Mail.ru Company's servers. To use «Mail.ru Agent», it is necessary to register an e-mail box on Mail.ru Company's servers, namely: www.mail.ru, www.list.ru, www.inbox.ru, www.bk.ru. The user name /password, used in the program «Mail.ru Agent», always coincide with the name of the e-mail box and its password. The given circumstance can be used to restore password to an e-mail box of the user of the program «Mail.ru Agent» out from:

- the settings of the Mailing Agent used by the user;

- the passwords saved by a browser, which is used by the user;

- and etc.

«Mail.ru Agent» also saves encoded password in the operating system registry (file NTUSER.DAT). The registry path is: HKEY_CURRENT_USER\Software\Mail. Ru\Agent\mra_logins

or HKEY_CURRENT_USER\Software\Mail. Ru\Agent\magent_logins (depends on the version of the program «Mail.ru Agent» used).

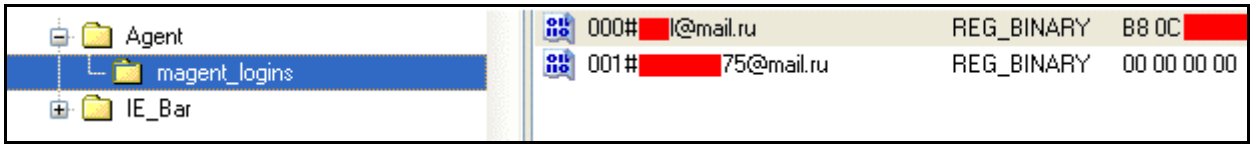

Fig. 5. The password for the account ** l@mail.ru saved by the program «Mail.ru Agent» in the registry of the operating system being analyzed. The password for the account ******* 75@mail.ru has not been saved.

The password for the ICQ account used by the user of the program «Mail.ru Agent» is also saved in the registry. The registry path is HKEY_CURRENT_USER\Software\Mail. Ru\Agent\magent_logins2.

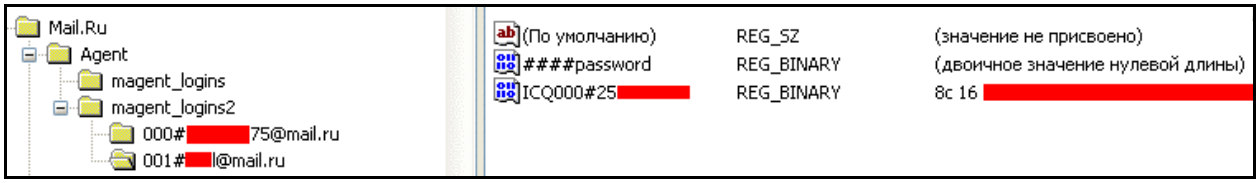

Fig. 6. The password for the ICQ user account ** l@mail.ru saved by the program «Mail.ru Agent».

At present time authors know only two commercial software products which can restore the password saved by the program «Mail.ru Agent» [3], [4].

By means of the research of the operating system registry, namely the registry path HKEY_CURRENT_USER\Software\Mail. Ru\Agent \, one can find out under what accounts work in the program «Mail.ru Agent» was carried out.

As judged by the registry data, shown in Fig. 5 and Fig. 6, one can draw a conclusion that under the researched user profile of the operating system under analysis in the program «Mail.ru Agent» work was carried out under two two accounts: **l@mail.ru and *******75@mail.ru.

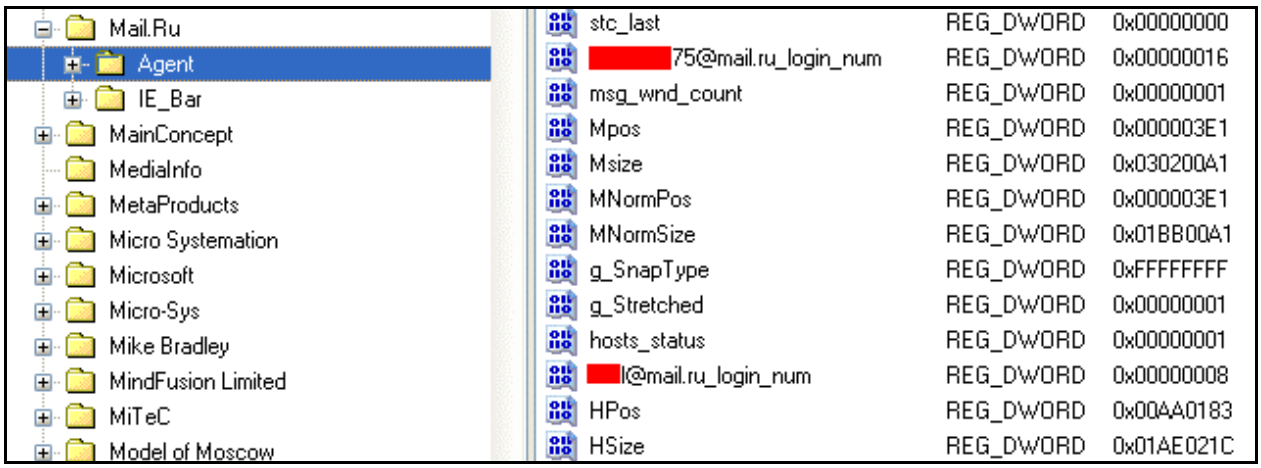

Fig.7. A fragment of the registry of the operating system under research.

The received information about the user's e-mail box (which has been used for «Mail.ru Agent» message exchange) and his/her password can be used for getting of not received messages of the program «Mail.ru Agent» out of his/her e-mail box.

Fig.8. The folder on the e-mail server in which the messages not received by the user and sent by means of the program «Mail.ru Agent» are kept.

!	**Attention:** To realize getting of the data from the Russian e-mail server, it is necessary to receive the written permit, given out by the Russian judge. Otherwise, the law enforcement officials' actions will contradict the Constitution of Russia and will result in the criminal responsibility of the persons who have carried out illegal getting of the e-mail.

As well as in the case with other IM-applications, history of «Mail.ru Agent» is of most forensic value. For Windows operating systems 2000/XP the program «Mail.ru Agent» saves history on the following path: <drive letter>: \Documents and Settings \% USERPROFILE %\Application Data\Mra \<account> \<the contact's address>. The program «Mail.ru Agent» saves history for the operating system Windows Vista on the following path: <Drive letter>: \Users \% USERPROFILE %\AppData\Roaming\Mra \<account> \<the contact's address>. For each account under which the user carried out work in the program «Mail.ru Agent», a separate folder is created. For example, in the given Fig.8 it is shown that the user carried out work in the program «Mail.ru Agent» under two accounts: ****** ru1983@mail.ru and ****** 7407@mail.ru.

Fig.9. Accounts under which the user carried out work in the program «Mail.ru Agent».

Depending on the program version «Mail.ru Agent» can save history in two equivalent variants:

- all contacts' profiles and the archives of the messages are saved in one folder (see Fig.10);

- for each contact's profile and its archive of messages a subfolder is created (see Fig.11).

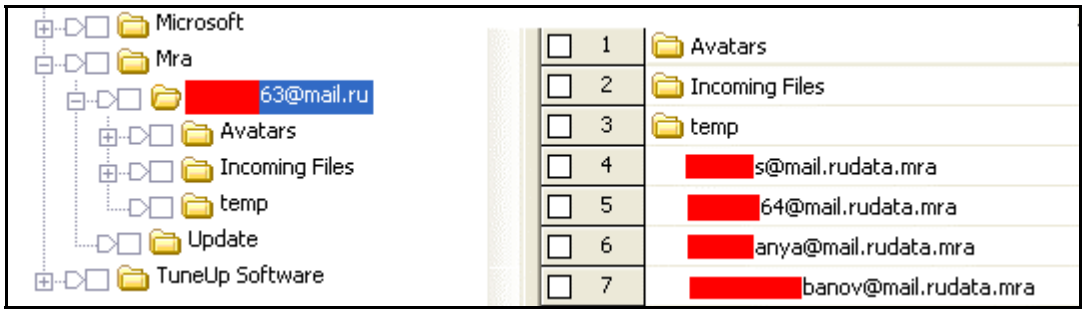

Fig.10. The first variant of history storage by the program «Mail.ru Agent».

Fig.11. The second variant of history storage by the program «Mail.ru Agent».

Sometimes, both variants of history storage are present on the researched disk drive. It means that earlier different versions of the program «Mail.ru Agent» drive were installed on the disk in a successive way or the program upgrade from the old versions on the new one took place.

Folders with history contain the following units of the program «Mail.ru Agent»:

-clist2.txt, clist3.txt or clist4.txt - a file with the contact list;

-data2data.mra - a file with the number of unread messages;

-data.mra - a file with the program settings;

-trash.txt - a file with unsent messages;

- trash.txt.copy - a backup file trash.txt;

-Avatars - the folder with contacts' thumbnail pictures;

-temp - the folder for temporary files storage;

-Incoming files - the folder with the files received by the user and delivered by means of the program «Mail.ru Agent» (The folder location, where files received by means of the program «Mail.ru Agent» are saved, can be changed in the program settings. In the Russian version of «Mail.ru Agent» files are saved in the folder - «My documents».);

-name@server.rudata.mra[1] or numberdata.mra[2] - a file with the contact profile;

-name@server.ruhistory.txt[1] – the archive of the contact's messages (there can be none);

-numberhistory.txt[2] – the archive of the sent SMS-messages;

---

[1] Where «name@server.ru» - an e-mail box name of the contact.

[2] Where «number» - the mobile phone number, which SMS-messages by means of the program «Mail.ru Agent» have been sent to. In a file with history a phone number is stored with "+"sign at the beginning of the number, but in a filename there is no "+"sign at the beginning of the number. Numbers can consist of 11 digits, 10 digits (with the country code omitted) and even of 4 digits (short numbers).

-ICQ - the folder with history messages received from the users by the ICQ protocol.

The ICQ folder has the following structure:

It contains subfolders of the first level which names designate the ICQ numbers from which the user of the researched computer carried out exchange of short messages. Each subfolder of the first level contains subfolders of the second level, which names designate the ICQ numbers of the users, with whom an exchange of short messages took place. Each subfolder of the second level contains files:

numberdata.mra[3] - a file with the contact profile;

numberhistory.txt[3] - the archive of the contact's messages;

avatar.jpg - the contact avatar;

avatar_small.jpg – the contact avatar thumbnail;

Thumbs.db – a thumbnail file (there can be none). It is created in the subfolder while being browsed by the regular resources of OS Windows.

As it has already been marked above, a format history can be different for different program versions. (see Fig.12 and Fig.13).

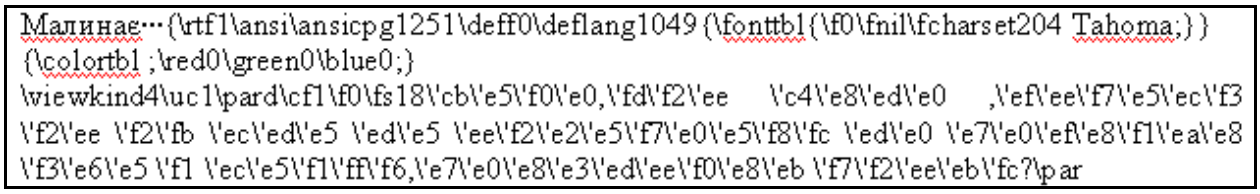

Fig.12. Example of a format of an archive of messages «Mail.ru Agent», version 4.10.

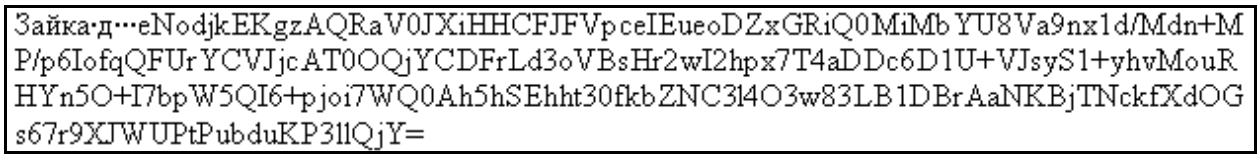

Fig.13. Example of a format of an archive of messages «Mail.ru Agent», version 4.8.

Pay attention, that the messages received before the approval of the user's authorization, are not encoded.

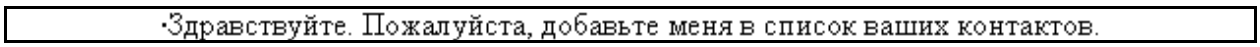

Fig.14. The message received before the approval of the user's authorization.

History of SMS-messages (a file numberhistory.txt[4]), sent to mobile phones, are not encoded. History of SMS-messages of the program «Mail.ru Agent», version 5.2, are saved in the Unicode coding. For the early versions history of SMS-messages of the program «Mail.ru Agent» are saved in ANSI Windows 1251 coding.

[3] Where «number» - the contact's ICQ number (corresponds to the subfolder name of the second level).
[4] Where «number» - the mobile phone number, which SMS-messages by means of the program Mail.ru Agent have been sent to.

3.2. Detection of «Mail. Ru Agent» version.

In some cases version detection of the program Mail.Ru Agent, the files of which are found on the disk drive, may be required (for example, in the case when the program is already uninstalled by the user or history can be found in the deleted mode). After that it will be possible to use the distributive of the appropriate version to review history contents.

Here are some features of the file structure of the folder with history which will allow to detail Mail. Ru Agent version:

a) presence of file clist4.txt - the version 5.2beta;

b) presence of file clist3.txt - versions 5.1,5.2;

c) in the folder root with history there are only clist2.txt, data*.mra, trash.txt * files, and all the rest files are located in the folders with the counterparts' (contacts') names - versions 4.10-5.0;

d) in the folder root with history there are other files, there are no folders with the counterparts' (contacts') names - versions 4.3-4.8.

In the case when in the same folder with history there are also folders with the counterparts' (contacts') names and file extensions *history.txt, one can draw a conclusion, that the user carried out replacement of the old (to 4.9) version of Mail. Ru Agent by a newer one (after 4.9).

According to the way of storage of the text of correspondence with the authorized users it is also possible to detect Mail. Ru Agent version:

a) messages are stored in Unicode - version 5.2;

b) messages are stored in Unicode in the view (form), which resembles the structure of the RTF-document - 5.2beta;

c) messages are stored in the view (form), which resembles the structure of the RTF-document - versions 4.10-5.0;

d) messages are stored in the form of lines starting with the signature «eN» - versions 4.3-4.8.

3.3. Ways of history review.

3.3.1. Manual history decoding.

The archive of messages of the format shown in Fig.11, can be decoded (the format of this version of history is similar to rtf format).

{\rtf1\ansi\ansicpg1251\deff0\deflang1049 {\fonttbl {\f0\fnil\fcharset204 Tahoma;}} - coding and font settings

{\colortbl; \red0\green0\blue0;} - background colour setting

\viewkind4\uc1\pard\cf1\f0\fs18

Message text: \'cb \'e5 \'f0 \'e0, \'fd \'f2 \'ee \'c4\... (Here each letter of the alphabet has its corresponding code, for example, letter "a" corresponds with code e0)

' fc? \par - a smiley (smileys are encoded:...\par or …? \par)

}

The following message is located further.

3.3.2. History substitution.

History substitution is the second method to review history of the program «Mail.ru Agent» from the researched disk. To do so, it's necessary for the researcher to:

-install the program «Mail.ru Agent» on the computer («Mail.ru Agent» version installed by the researcher should be similar to «Mail.ru Agent» version which is being researched) and to register on one of Mail.ru company's mail servers;

-start the program «Mail.ru Agent» and send any message (for example, «hello») to the user, history of whom it is necessary to review;

-quit the program «Mail.ru Agent»;

-change the contact profile and a history file, created on the computer of the researcher by the program «Mail.ru Agent», for the contact profile and a history file being researched;

-start the program «Mail.ru Agent» and review the contents of the researched history file.

While using the given method there appears the main problem - where to find the distributive «Mail.ru Agent» of the version which has been installed on the researched computer. This problem can be solved in the following way:

While being installed the program «Mail.ru Agent» places a copy of its distributive at:

- <Drive letter>: \Documents and Settings \% USERPROFILE %\Application Data\Mail. Ru\(for Windows 2000/XP operational systems);

- <Drive letter>: \Users \% USERPROFILE %\AppData\Mail. Ru\(for Windows Vista operational system).

The researcher can often detect the distributive of this program at the address specified above, even after the deinstallation of «Mail.ru Agent».

3.3.3. Usage of the specialized software.

Despite the stated methods of history research of the program «Mail.ru Agent», we consider usage of the specialized software to be the most forensically sound and the fastest method of research. We recommend to use the program Forensic Assistant developed by the National Hi-Tech Crime Unit. RU (www.nhtcu.ru). Forensic Assistant has been developed by the experts who fulfill forensic researches and perfectly understand requirements of the researchers in the field of digital researches. There is a version of the program Forensic Assistant which interface is made in English. The program is being constantly enlarged by new units for the IM-programs analysis.

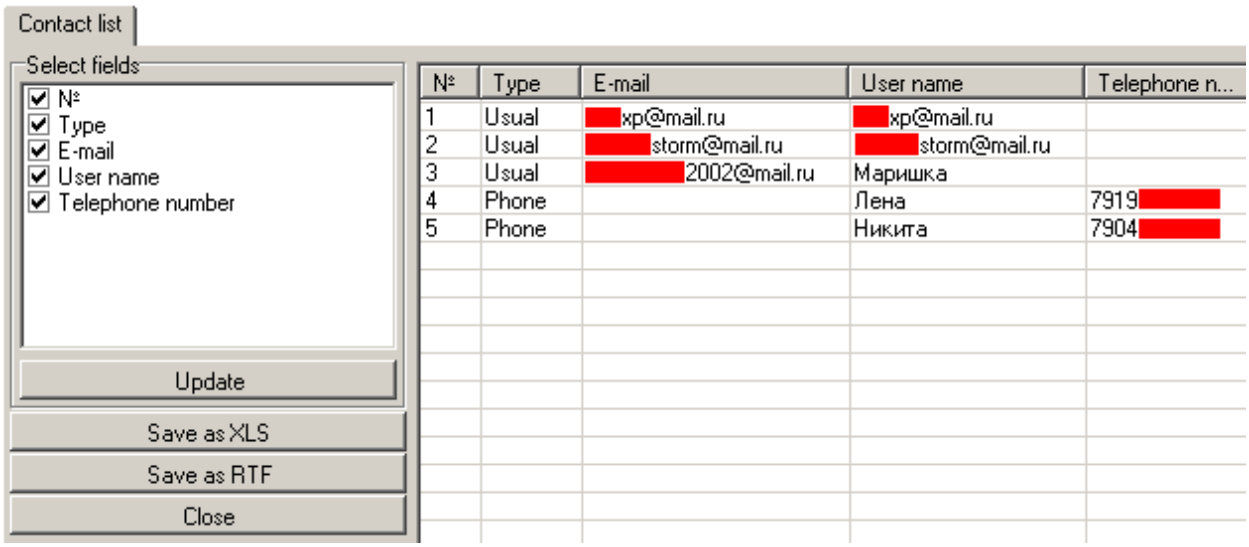

Fig.15. The contact list displayed for the researched profile by the program Forensic Assistant.

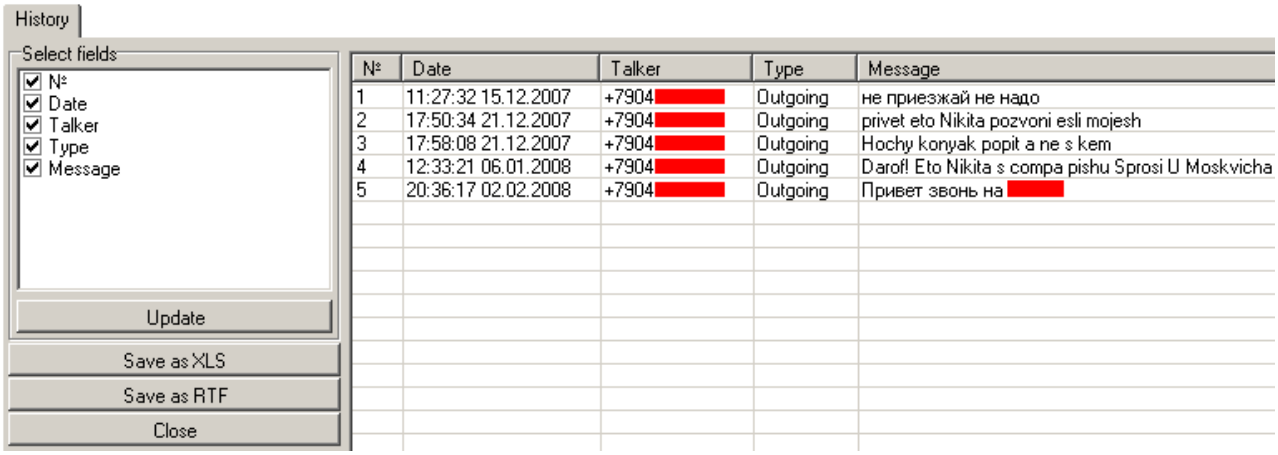

Fig.16. History displayed by the program Forensic Assistant.

Conclusion

Thereon we want to bring to a close the first article devoted to forensic research of the Russian IM-applications. We hope that the information stated in it will be useful for our foreign colleagues and will contribute to disclosure of crimes.

REFERENCES:

1. http://agent.mail.ru/
2. http://agent.mail.ru/en/
3. http://www.nhtcu.ru/
4. http://www.passwords.ru/aimpr.html

Igor Yurin

Director of National Hi-Tech Crime Unit.RU

info@nhtcu.ru

http://www.nhtcu.ru ,

Olga Kapinus,

Igor Michailov (igor_michailov2006@yahoo.com)