Retrieving Internet chat history with the same ease as a squirrel cracks nuts

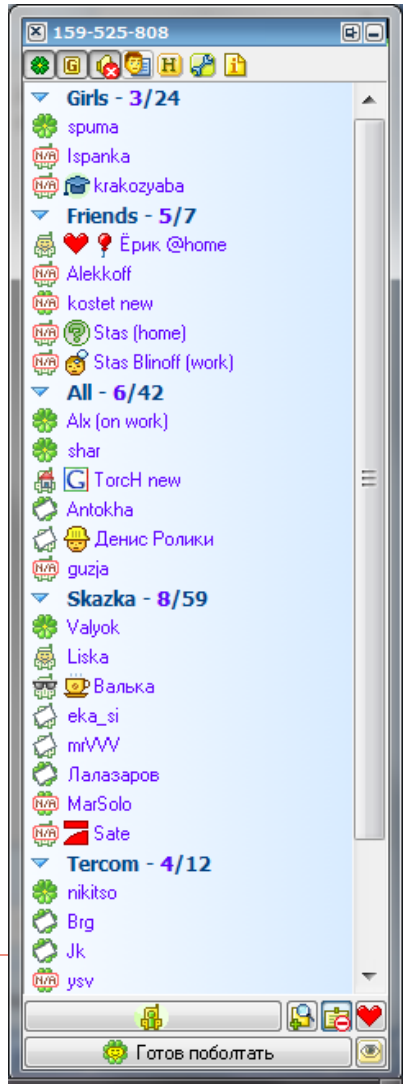
Yuri Gubanov
CEO, Belkasoft
http://belkasoft.com

SANS Forensic Summit
September 21, 2011
London, Great Britain

Belkasoft
forensics made easier

What is Instant Messenger

- Well, you know it
- Simple small program for text exchange
  - Files and images exchange in some IMs
  - SMS, URLs, voice mail or audio calls
  - Twitter and Facebook statuses
- Friends (contacts) list



Retrieving Internet chat history with the same ease as a squirrel cracks nuts

IMs are widely used

- Common means of communication nowadays
- Any country
- Any gender
- Any age
- Any computer skills

Popular IMs

Retrieving Internet chat history
with the same ease as a squirrel
cracks nuts

Forensic IM investigation

- Ways to retrieve information about Instant Messenger communication:
  - Post-factum analysis
    - Existing history file parsing
    - Carving for deleted data
    - Live RAM analysis
  - Real-time analysis
    - Network traffic capture
    - Keylogging

Existing history file parsing

- Locate a file
- Analyze it, knowing its format
  - Format description should be available
- Examples
  - ICQ 7 or Skype – SQLite
  - MSN – xml
  - QQ – OLE container

How a criminal may prevent such analysis?

- Change file location from default
- Move/Rename a history file/folder
- Delete a history file
- Quick format the drive
- Encrypt the drive
- Select "Do not store my history" option in advance

How do I?

- When file location changed from default, using IM means
  - Not all messengers allow for this, most store under a fixed path in a user's folder
  - Search through all the drive(s)!
    - But: possibly too much false positives, e.g. MSN: xml (rather search for MessageLog.xsl but what if it is deleted?)
  - May need to change access rights (some folders may be inaccessible)

How do I?

- When a history file moved/renamed
  - Need to be a computer savvy to know where a history file is stored
  - Search through all the drive(s)!
  - "Paranoid" search
    - Treat all files as history files. E.g. look for Miranda signature "Miranda ICQ DB" in all files.
    - Can be too slow if a messenger has no clear signature like for Miranda
  - Carving is another good approach in this case

How do I?

- When a history file deleted
  - Need to be a computer savvy to know where a history file is stored and not to delete to a recycle bin
  - Recover from recycle bin
  - Recover using file recovery tools
  - Use alternative history sources
    - Example: Skype chatsync. But: format is proprietary and not published
  - What is file is already corrupted/ overwritten?
    - Use carving to retrieve separate messages

What is carving?

- Going through the whole drive
- Disregard file structure
- Byte by byte search for signatures or patterns specific to various data items
  - E.g. instant messages, URLs, emails
- Data may persist very long time after deletion!

Carving

- Example: Skype 3 has "l33l" signature
- Will retrieve both deleted and existing messages
- Works only for history types which have good signatures
  - E.g. old ICQ does not have one
- Note the difference between file and message signature!

How do I?

- When a user Quick formats the drive
  - The same way – use carving
- When a user encrypts the drive
  - Use the software like Elcomsoft's one
- When a user selects "Do not store my history" option in advance
  - Use Live RAM analysis (explained later)

How a criminal prevents carving for deleted data?

- Delete data and use a special program to fill a drive with random bytes
  - File recovery and carving will not give any results
  - White noise detection programs – whom from 10 suspects to choose?
- Never set "Store my history"
  - Live RAM analysis
- Use special SSD drives
  - Live RAM analysis

SSD drives problem

- SSD drives which designed specifically for NTFS
- or SSD drive which supports TRIM
- May completely remove all deleted information in minutes
  - Write blocker devices will not help!
  - See http://www.jdfsl.org/subscriptions/JDFSL-V5N3-Bell.pdf

SSD drives problem

- But:
  - Not all OS supports TRIM
  - TRIM will not work efficiently on highly fragmented drives
    - SSDs cannot be defragmented when using wear leveling
  - TRIM commands compromise disk encryption
  - SSDs are still very expensive and not widely used

What is Live RAM analysis

- Dumping a running computer's RAM memory to a thumb drive using special utilities:
  - win32dd/win64dd
  - Encase
  - FTK Imager
  - etc
- Computer should be seized switched on
- Investigation of dump contents

What if a computer is locked?

- Rebooting will leave most of history in RAM
- Reboot and boot from a thumb drive/CD
  - Will not work if
    - Boot sequence does not allow to boot from thumb drive/CD
    - BIOS is password protected
- Or do a Firewire dump

How to perform analysis

- Use the same technique as carving
- Signatures may differ for messages in memory (but may be the same)
  - E.g. ICQ 7 and Skype 4 have the same signatures in RAM
  - E.g. AIM has a signature "EF FD" repeated 8 times
- Expect to find only a few recent conversations

Analyzing pagefile.sys and hiberfil.sys

- One is swap file (virtual memory) and another is file used for hibernation (if enabled)
  - Most frequently enabled for laptops though I use it on my desktop as well
- Portions of memory used recently are stored in these files
  - The data will survive reboots/switching off
- The same as Live RAM carving but need to decompress beforehand

How a criminal prevents Live RAM analysis?

- Set BIOS password
- Disable boot from anything else than own hard drive
- Disable hibernation and virtual memory
  - Will significantly slow down the computer
- Lock computer
  - Firewire dump still possible
- Switch computer completely off

Real-time analysis

- Two methods available
  - Network traffic capture (so called sniffing)
  - Keylogging
- Both suppose being 'near' to a suspect

Network traffic capture

- A sniffer program captures all network traffic in a local network
- The same hub or switch of LAN, wifi or bluetooth hot-spot
- Sniffer can save intercepted packets in PCAP files
  - E.g. WireShark
- You can analyze these files in real time or later
- IMs use protocols like Oscar (ICQ, AIM…), XMPP (Jabber, GTalk, Facebook…)

How a criminal prevents sniffing?

- There is no way to prevent interception itself (data still goes through ISP)
- Not use public WiFi hot-spots
- Use encrypted communication

Keylogging

- A program running on a user's machine
- Can run in stealth mode, without being shown in Task Manager, Services, etc
- Can send or upload logged information
- Hard to install hidden
- Is not legal in many countries

How a criminal prevents keylogging?

- Disable Windows auto-login feature
- Use strong password for their login
- Have only themselves as a local administrator
- Have robust up-to-date antivirus and do all other stuff all others do against viruses
- Use known anti-spyware tools

The worst setup

- Disable auto-login and use strong password
- Be the only one local administrator
- Remove Administrators and SYSTEM accounts from a 'secret' folders
- Encrypt the drive
- Use SSD which supports TRIM and use Windows 7 OS
- Set BIOS password
- Disable boot from anything else than your hard drive
- Disable history storing in Instant Messenger
- Use Instant Messenger that encrypts traffic
- Disable hibernation
- Disable virtual memory
- Have enough time to perform a quick format before police comes to you
- Have enough time to switch computer off before police comes to you

Still, will not save one from

- Investigating history on another side
- Investigating ISP logs and Instant Messenger server logs

Live demo

- Regular history extraction
- Carving
- Live RAM analysis

Case study

- Is IM investigation important?
- Decide yourself, basing on a cases completed with Belkasoft tools:
  - A country counterintelligence unit found and accused a spy with the help of Skype carving
  - A man was found guilty in a Second Degree Murder with the help of ICQ analysis
  - A spouse was found guilty for adultery in a divorce suit with the help of Yahoo analysis

Questions? Comments?

- Ask me now
- Take my business card
- Attend our FREE webinar on our tools
  - Just send an email to contact@belkasoft.com!

- Site: http://belkasoft.com
- Email: contact@belkasoft.com
- My LinkedIn account: http://ru.linkedin.com/in/yurigubanov