Täterkommunikation mit Instant Messaging Clients

Prof. Dr. rer. nat. Daniel Hammer
Faktultät Medien und Informationstechnik (M+I)

Badstraße 24,
77652 Offenburg
Tel.: 0781 205-388
E-Mail: hammer@hs-offenburg.de

1965: geboren in Berlin
Studium der Mathematik und Physik in Berlin und Moskau, Promotion auf dem Gebiet der Theoretischen Informatik (deskiptive Komplexitätstheorie)
Wissenschaftlicher Mitarbeiter an verschiedenen Forschungseinrichtungen (Karl-Weierstraß-Institut Berlin, TU Berlin, Uni Greifswald)
Forschungsaufenthalte in Spanien (CRM), Russland (IUM/MCCME) und Israel (Technion)
Tätigkeit in zahlreichen IT-Projekten (Security, Systemintegration) auf dem Gebiet des eBusiness und Online-Providing sowie im öffentlichen Sektor
Seit 2004: Professor für Informatik, insbesondere Sicherheit in Informationssystemen an der Hochschule Offenburg

Forschungsgebiete: Computer & Netzwerk-Forensik, Sicherheit in vernetzten Systemen, Privacy Protection, Security Engineering

---

4.1 Täterkommunikation mit Instant Messaging Clients

Prof. Dr. rer. nat. Daniel Hammer

Abstract
Instant messaging systems allow users to interact in real time over the Internet. Hackers and criminals often use instant messenger programs for illicit purposes and consequently the logfiles and any possible digital evidence from such programs are of forensic interest. The current research project attempts to provide an accurate and reasonable description of some issues where to find evidence and presents possible solutions to those issues.

Das Internet bietet eine Vielzahl von Möglichkeiten zum weltweiten Informationsaustausch. Es hat sich zu einem unverzichtbaren Bestandteil der beruflichen und privaten Alltagskommunikation entwickelt. Im Lauf der Jahre hat dies zu Veränderungen der Kommunikationsgewohnheiten geführt.

Nicht nur die verwendete Technik hat eine rasante Entwicklung genommen und dadurch zu einer enormen Steigerung von Mobilität, Effizienz und Individualisierung beigetragen. Mit dem Einzug dieser neuen Informationswege gehen auch grundlegende gesellschaftliche Wandlungsprozesse und Veränderungen der orts- und raumbezogenen Sozialstrukturen einher.

Im Zug dieser Entwicklung finden Instant-Messengern als Kommunikationsplattform in der Bevölkerung eine immer breitere Anwendung. Verbreitung, Akzeptanz und Funktionalität führen dazu, dass dieses Medium auch zur Täterkommunikation, also zur Vorbereitung und Durchführung von Straftaten, benutzt wird. Somit rückt diese Art des Informationsaustauschs bei Sicherheitsbehörden zunehmend in den Fokus der Ermittler.

Wenn Computer bzw. computergestützte Dienste bei Straftaten involviert sind, werden Computer-Forensik-Experten zur Sicherung gerichtsverwertbarer elektronischer Beweismittel zu Rate gezogen. Hierbei geht es um die Untersuchung, Wiederherstellung und Bewertung digitaler Spuren und Datenbestände auf den Computern der Täter oder sogar in Netzwerken. Die forensische Untersuchung digitaler Spuren, die Straftäter bei der Nutzung von Instant Messengern hinterlassen, ist kein leichtes Unterfangen.

Zunächst gibt es eine Vielzahl solcher Messenger, wobei jeder sein eigenes Portfolio an Funktionen, Formen der Standardinstallation, Änderungs- bzw. Einstellmöglichkeiten durch den Anwender, jeweilige Systemvoraussetzungen und Zusatzbibliotheken mit sich bringt.

Darüber hinaus verfügt jeder dieser Instant Messaging Clients über jeweils spezifische Speicherorte kommunikationsrelevanter Daten. Die jeweils verwendeten Datenformate sind dabei meist ebenso spezifisch wie proprietär.

Außerdem haben einige Messenger noch Zusatztools und Hilfsmittel wie Toolbars in Browsern, die eine weitere Diversifizierung der digitalen Spuren für jeden Messenger nach sich ziehen. Eigenschaften dieser Datenspuren wie deren Flüchtigkeit und Wiederherstellbarkeit sind zudem oft abhängig vom Kontext des jeweils verwendeten Betriebssystems.

Die hier angesprochenen Probleme sind bisher kaum erforscht, sodass selbst der fachkundige Ermittler nur sehr wenige Anhaltspunkte bei der Beweissicherung und Analyse beweisrelevanter Daten hat. Aufgrund der Spezifik trifft dies nicht nur für die forensische Post-mortem-Datenträgeruntersuchung zu. Bei Instant-Messengern müssen digitale Beweismittel vor allem auf laufenden Computersystemen gesichert werden, da sie nach Beendigung des Messengers oder gar nach einem Neustart des Computers meist unwiederbringlich verloren sind.

Im Labor für IT-Sicherheit und Computer-Forensik der Hochschule Offenburg wurde das Forschungsprojekt Täterkommunikation mit Instant Messaging Clients ins Leben gerufen und damit echtes Neuland in der Forschungslandkarte betreten. Gegenstand ist eine strukturelle Untersuchung von verschiedenen Instant-Messengern auf Computersystemen bzw. in den bei Ermittlungen gesicherten Computersystemen erstellten forensischen Images.

Zentrale Fragen

Folgende Fragestellungen sind in Bezug auf Instant-Messenger für forensische Ermittler am Zielsystem eines Täters von zentraler Bedeutung:

- Wie kann man erkennen, ob Messengerdienste auf einem jeweils vorliegenden Computer genutzt wurden?
- Wie kann man erkennen welche Messengerdienste genutzt wurden?
- Wo speichern Messenger relevante Daten und welcher Art sind diese Daten?
- Wann, mit wem und in welcher Form bestand innerhalb des Messengerdiensts Kontakt?
- Welche Inhalte wurden in welchen Formaten kommuniziert?
- Wurden Daten/Dateien ausgetauscht? Welche? Mit wem? Wann? Speicherort?
  Welche Daten sind sogenannte flüchtige Daten, also nach Abmeldung des Messengers bzw. Ausschalten des Computers nicht mehr vorhanden bzw. aufgrund von Verschlüsselung/ Codierung nicht mehr auslesbar?
- Welche Daten sind nur online aufgrund der Speicherung auf dem Server des Dienstanbieters verfügbar?
- Welche Änderungen zur Standardinstallation wurden vorgenommen (z.B. Protokollierung, Verschlüsselung etc.)?
- Welche Personen wurden seit wann ignoriert?

Untersucht wurden hierzu die Instant-Messenger mit dem größten Verbreitungsgrad

- ICQ
- Yahoo Messenger
- MSN, Windows Live Messenger, Messenger Plus! Live
- Skype

sowie die Multi-Messenger

- Pidgin
- Trillian Astra
- Miranda

in den jeweils aktuellen bzw. am häufigsten genutzten Versionen. Die Applikationen wurden dabei von den Betriebssystemen MS-Windows XP und MS-Windows Vista sowie MS-Windows 7 gehostet.

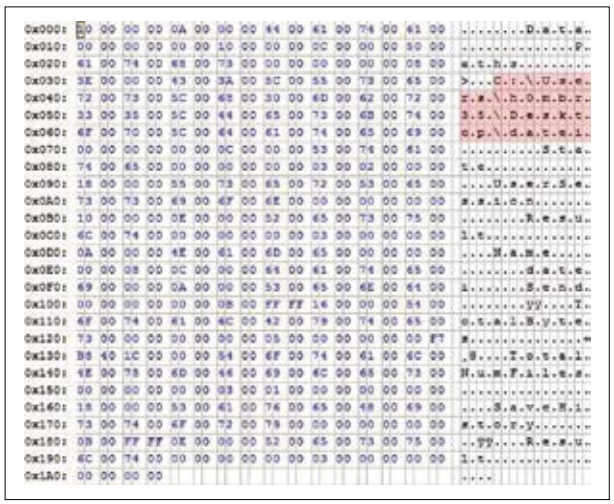

Abb. 4.1-1: *Aufbau einer Transfernachricht Datenpfad rot in ICQ*

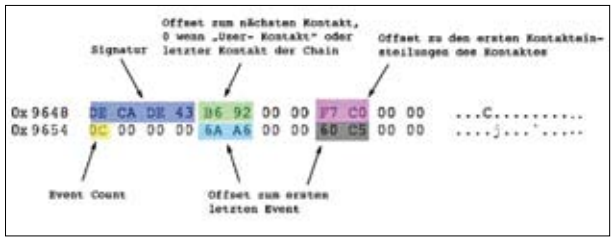

Abb. 4.1-2: *Miranda-2072*

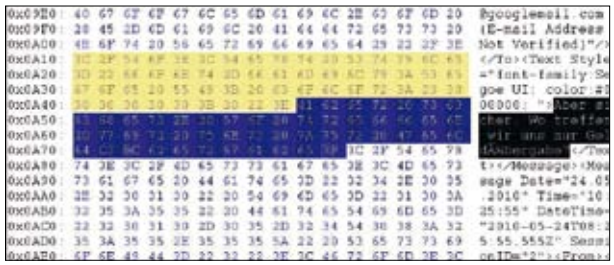

Abb. 4.1-3: *WindowsLive-014*

Abb. 4.1-4: *Yahoo-001*

Zunächst wurden allgemeine Informationen zu den Messengern untersucht. Dazu gehören die genauen Installations- und Konfigurationsdaten im jeweiligen Betriebssystem mit dazugehörigen Hashwerten aller wichtigen Binaries. Dazu wurden bitgetreue forensische Snapshots der Betriebssysteme vor und nach der Installation bzw. der Nutzung des Messengers verglichen. Außerdem wurden alle Änderungen und Schlüssel in der Registry des Systems genauestens ausgewertet.

Des Weiteren wurde ermittelt, welche Log- und Protokolldateien von den Messengern angelegt werden, wo und unter welchem Namen diese Dateien erzeugt und welche Informationen in diesen Dateien gespeichert werden. Da die Dateien meist proprietäre Formate besitzen musste aufwendig untersucht werden, wie sich die in ihnen gespeicherten Informationen darstellen und später interpretiert haben. Hierzu musste die Hexstruktur dieser Dateien Bit für Bit ergründet werden.

Bei der Einrichtung eines User-Accounts ist neben der Festlegung eines Benutzernamens und eines Passwortes die Eingabe von personenbezogenen Daten erforderlich. Zudem kann die Angabe einer E-Mail-Adresse erforderlich sein. Diese Profildaten können für Ermittler von hohem Interesse sein und mussten als Nächstes mit ihren Speicherorten im System ermittelt werden.

Da die Benutzer der Messenger eine Vielzahl von Möglichkeiten haben, z. B. Kennworte zu speichern, sich automatisch anzumelden etc., musste pro Applikation eine Vielzahl von Szenarien durchgespielt werden. Je nach Nutzungs- und Konfigurationsart der Messaging Clients ändert sich die Bitstruktur der angelegten Daten, die es zu finden und zu analysieren galt.

Jeder Kontakt hinterlässt Spuren

Kontakt- und Kommunikationsdaten die im Zug von Chat, Mailversand, Telefonie und Dateitransfer mit Messengern entstehen, sind von höchstem Interesse für Ermittler. Basis aller wissenschaftlichen Untersuchungen ist hierbei das sogenannte Locard'sche Austauschprinzip. Es wurde von Edmond Locard (1877 – 1966), dem Leiter des ersten medizinisch, forensischen Institut der Welt formuliert und später in die digitale Welt des Computerzeitalters übertragen. Es besagt, dass kein Kontakt zwischen zwei Objekten vollzogen werden kann, ohne dass diese wechselseitige Spuren hinterlassen.

Nadeln im digitalen Heuhaufen

Um dieser digitalen Kontaktspuren habhaft zu werden, muss man sehr tief ins Dateisystem des jeweiligen Betriebssystems einsteigen. Unter Umständen hilft sogar nur eine Analyse des Hauptspeichers der noch laufenden Kommunikationssysteme.

Zwei klassische Ermittlungsfragen sind zum Beispiel: „Hatte Person A mit Person B Kontakt?" bzw. „Wie lauten alle Kontaktpersonen einer gegebenen Person?". Um Beweise für den Informationsaustausch mit Instant-Messenger zweier Kontaktpersonen zu finden, muss man gelegentlich nicht nur Verschlüsselung überwinden. Es ist auch oft sehr schwierig und aufwendig, deren binäre Codierung zu verstehen, um sie zu den entsprechenden Phasen und Inhalten der Kommunikation zuordnen zu können.

Manchmal helfen bei der Spurensuche auch Umwege. Bei Instant-Messengern wird beispielsweise manchmal zur Nutzung der vorhandenen E-Mail-Funktion auf den nach Standard hinterlegten E-Mail-Account des Systems zugegriffen. So kann man vielleicht zwar keine Kommunikationsspuren innerhalb der Dateistruktur des Messengers finden, wohl aber in der des standarddisierten E-Mail-Clients, weil eventuell E-Mails lokal auf dem Computer gespeichert wurden.

Messenger ermöglichen weiterhin, mit Kontaktpersonen Dateien jeglicher Art auszutauschen. Auch hier gibt es eine Reihe nicht-trivialer Fragen zu klären. Gibt es zum Beispiel Hinweise auf die versendeten oder empfangenen Dateien und können Aussagen zur Transferrichtung getroffen werden? Wurden Hashwerte der übertragenen Dateien gespeichert, und wenn ja, an welchen Speicherorten und in welchem Algorithmus?

Um hierauf Antworten zu finden, mussten ebenfalls viele Szenarien durchexerziert, Datenträger Bit für Bit forensisch gesichert und analysiert werden.

Praktische Sicherheitsforschung

Besonders in der Phase der konkreten Zielbestimmung dieses Forschungsvorhabens, aber auch bei der Definition einzelner Nutzungsszenarien der Instant Messaging Clients wurde intensiv mit Spezialisten der Forensic Computer Investigation/Analysis Unit des Bundeskriminalamts zusammengearbeitet.

Dadurch konnte eine höchstmögliche Praxisnähe erreicht und Antworten auf konkrete Fragestellungen des regulären Ermittleralltags und seiner Arbeitsabläufe gegeben werden.

Die im Projekt gesammelten Forschungsergebnisse sind in eine umfangreiche Dokumentation eingeflossen, aus der ein dynamisch erweiterbarer Leitfaden für Ermittler der polizeilichen IT-Forensik in Deutschland entstanden ist. Dieser Leitfaden dient Ermittlern nicht nur als Hilfsmittel und Nachschlagewerk bei der Datenträgeruntersuchung, sondern auch als Anleitung, wie die Sicherstellung aller beweisrelevanten Daten insbesondere bei laufenden Computersystemen erfolgen sollte.

Referenzen/References

[1] Jones: "Information warfare – A European perspective of recent developments?", International Conference on i-Warfare and Security, 2006

[2] Haddon: "Information and Communication Technologies in Everyday Life", Berg Publ., 2004

[3] Morfitt: "Structural Analysis of the Log Files of the ICQ Client Version 2003b", Proc. 4th Australian Digital Forensics Conference, 2006

[4] Locard: „Die Kriminaluntersuchung und ihre wissenschaftlichen Methoden, bearbeitet von Willy Finke", Berlin Kameradschaft, 1930

[5] Sorensen, Yoo and Lyytinen (Herausgeber): "Designing Ubiquitous Information Environments: Socio-Technical Issues and Challenges", Springer, 2010