Chat-Analyse mit Belkasoft Evidence Center 3.5

Ausgeplaudert

Alexander Sigel

Chat-Nachrichten gehören ebenso wie Mails, Office-Dokumente und dergleichen zu den für IT-forensische Ermittlungen relevanten Daten. Ein russisches Werkzeug, das in Kürze in neuer Version erscheinen wird, beherrscht besonders viele Formate.

Wer als IT-Forensiker häufiger Chats auswerten muss, braucht entsprechende Werkzeuge. Der Forensic IM Analyzer des russischen Softwareherstellers Belkasoft hilft, den Verlauf der Kommunikation mit populären Instant Messengern zu untersuchen. Er kennt mehr IM-Formate als vergleichbare Tools und ist einfach zu bedienen.

Manche Forensiker nutzen noch das ältere Belkasoft Forensic Studio (BFS), das unter einer gemeinsamen Oberfläche die drei separaten Werkzeuge IM Analyzer, Browser Analyzer und Mail Analyzer bündelt. Es unterstützt alle gängigen Browser, allerdings nur vier Mailbox-Typen.

Jüngstes und leistungsfähigstes, aber auch teuerstes Mitglied der Produktfamilie ist das Belkasoft Evidence Center (BEC), eine integrierte IT-forensische Arbeitsumgebung für Datenspuren unter Windows und Mac. Seit August 2011 ist BEC 3.0 erhältlich. Dem Autor lag die Version 3.5 (eine Vorversion) vor, die im Dezember 2011 veröffentlicht werden soll.

BEC soll es IT-Forensikern im Umfeld von Behörden und Unternehmen erleichtern, Internet-Artefakte, speziell Kommunikationsvorgänge, zu finden. Wie mit dem Vorgänger BFS kann man mit BEC Nutzungsverläufe von Instant Messengern, Browsern sowie Mail-Clients auswerten und nun auch Bilder und Videos. Es ist möglich, Lesezeichen zu setzen und die Ergebnisse in Berichte unterschiedlicher Formate zusammenzufassen.

Manuelle Auswertung nicht möglich

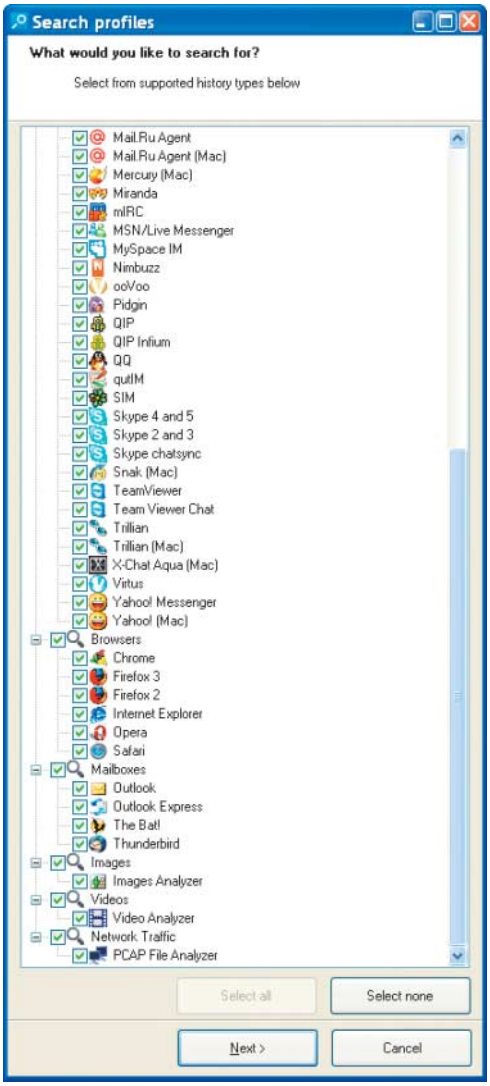
Angesichts der Vielzahl von Kommunikationsprogrammen (es gibt allein mehr als 150 Chat-Programme) würde eine manuelle Auswertung deutlich zu lange dauern. Auch dürfte man für relativ unbekannte Programme unter Umständen einzelne Artefakte oder Einträge übersehen. Man müsste zudem im Detail wissen, wo sie liegen und wie die proprietären Formate jeweils zu lesen sind – und das für alle Versionen.

BEC löst dieses Problem: Selbst wenn man sich mit den Artefakten nicht genau auskennt, gelingt es mit nur zwei Mausklicks und ohne aufwendige Konfiguration, relevante und forensisch verwertbare Ergebnisse zu finden. BEC eignet sich daher auch für die Erstsichtung potenzieller Beweise. Vorausgesetzt, es ist kein Verarbeitungsfehler aufgetreten, kann man ziemlich sicher sein, alle verwertbaren Spuren erwischt zu haben. Die Datenmasse reduziert sich auf die erforderlichen Informationen, und man kann sich um die komplizierteren Fälle kümmern. Zwar dauert es auch mit dem BEC, bis Ergebnisse vorliegen, das ist jedoch noch immer ein bis zwei Größenordnungen schneller als ohne das Werkzeug.

Zu BEC gibt es kommerzielle und freie Alternativen. Bei Ersteren sind insbesondere der Paraben Chat Examiner und der Internet Evidence Finder erwähnenswert. Von den kostenlosen Werkzeugen braucht man für jede Aufgabe eines, etwa NirSoft SkypeLogView für Skype.

Verschiedene Formate, verschiedene Quellen

Mit über 50 Messenger-Clients (s. Aufmacher-Screenshot) deckt das Evidence Center mehr ab als andere An-

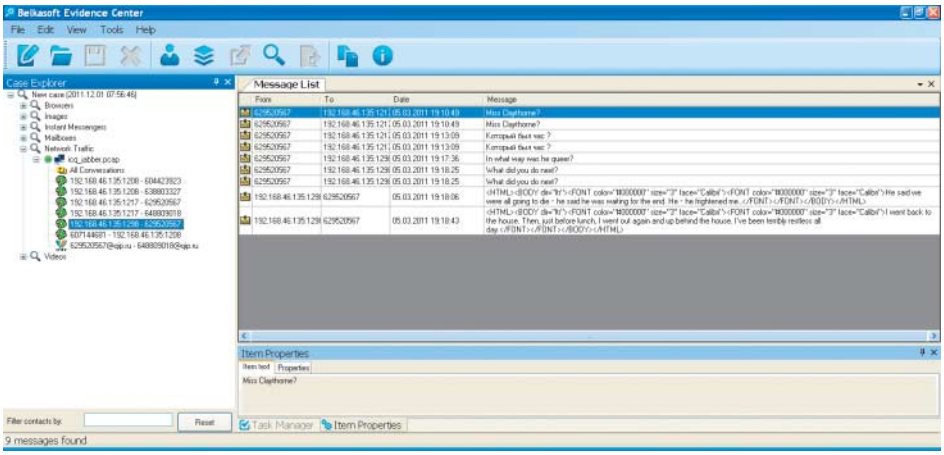


Verschiedene Carving-Verfahren

„Naives“ Carving versucht, auffällige Dateien an einem festen Kopf (Signatur), einer Rumpfsignatur oder einer festen Länge zu erkennen. Fortgeschrittenere Techniken verwenden variable Muster und kontextabhängige Längen. Komplexes Carving kombiniert mehrere Heuristiken und setzt auf anwendungsspezifische variable Suchmuster.

Für IT-forensische Vollständigkeit sollte man keine Sachverhalte wie anwendungsspezifische Besonderheiten in Datei-Artefakten und Seiten-Fragmentierung ignorieren, da sie wertvolle Hinweise enthalten könnten – also bevorzugt ein komplexes Carving durchführen.

© Copyright by Heise Zeitschriften Verlag



Ergebnisse der Rekonstruktion: Chats aus Netzwerkmitschnitten

bieter. Man benötigt nur ein Werkzeug und nicht eines für jeden Messenger. Zugleich ist die Analyse bei BEC umfassend: Die Spuren können dem Dateisystem entstammen, extrahiert von einem Datenträger mit dem Belkasoft Forensic Carver, oder live aus dem Hauptspeicher oder hauptspeicherähnlichen Artefakten (pagefile, hiberfil) sowie (für Chats in den Protokollen Oscar und XMPP) aus Paketmitschnitten des Netzwerks.

Überdies kann das Belkasoft-Werkzeug Windows- und Mac-Images (*dd*, EnCase, SMART) einhängen. Allerdings unterstützt auch das Konkurrenzprodukt Internet Evidence Finder seit Version 4 das Mounten verschiedener Images.

BEC integriert alle genannten Features in einer einheitlichen forensischen Arbeitsumgebung, die Fallmanagement mittels persistenter Speicherung im Backend von Microsofts SQL Server unterstützt und in der Enterprise Edition mehrbenutzerfähig ist.

Version 3.5 enthält etliche wichtige Neuerungen. Jetzt kann man die Kommunikationsverläufe auch analysieren, nicht nur – wie in der Vorgängerversion – extrahieren. Eine weitere Neuerung ist die Unterstützung des Apple-Betriebssystems Mac OS X: Man kann zwölf Mac-Messenger untersuchen sowie die Dateisysteme HFS und HFS+ einbinden oder als Image mounten. Die Auswertung deckt neuerdings auch das sogenannte Carving – die Dateirekonstruktion ohne Hilfe des Dateisystems – und Hauptspeicher-Artefakte ab. Carving ist separat für allozierte und nicht allozierte Bereiche einstellbar.

iX-Wertung

- ⊕ umfassende Analyse von Instant-Messaging-Artefakten (Vielzahl unterstützter IM-Clients, Carving, Live-Analyse, Netzwerkanalyse)
- ⊕ praxistaugliche intuitive Benutzeroberfläche, auch für Ungeübte
- ⊖ keine Anzeige bei unvollständiger oder fehlender Spurenverarbeitung
- ⊖ naives und nicht strukturiertes oder auf Datenbank ausgerichtetes Carving

Videos und Bilder aufspüren

Die Hauptspeicher-Analyse schließt auch hauptspeicherähnliche Artefakte wie die Auslagerungsdatei *pagefile* und die Zwischenspeicherungsdatei *hiberfil* ein. Schließlich haben die Entwickler die Analyse um die Suche nach Bildern und Videos erweitert. So kann das Werkzeug nun Metadaten extrahieren, Gesichter und pornografische Darstellungen heuristisch erkennen, außerdem Bilder und Videos nach zahlreichen Kriterien filtern sowie Schlüsselbilder aus ihnen extrahieren. Des Weiteren steht eine Texterkennung (Optical Character Recognition, OCR) zur Verfügung, und der Forensiker kann sich GPS-Daten anzeigen lassen und sie exportieren.

Zudem haben die Entwickler eine Reihe kleiner Verbesserungen vorgenommen: Die Zahl unterstützter Artefakte hat sich erhöht, und bisher schon berücksichtigte Artefakte werden noch gründlicher ausgewertet. Dies betrifft beispielsweise Thunderbird-Mails oder Facebook-Spuren aus dem Internet Explorer und Chats aus dem Hauptspeicher.

Die zum Test zur Verfügung gestellte Vorabversion 3.5 testete der Autor auf den Systemen Win XP SP3 (online) und Win 7 Enterprise x64 (offline). Der zunächst bereitgestellte Build der Entwicklungsversion enthielt versehentlich einen Fehler im Datenmodell. Ebenso zeigte die Hilfeoption im Menü dieser Version nur auf das Online-Handbuch. Das ist jedoch nicht geeignet für einen Offline-Auswertungsrechner und zwischenzeitlich behoben.

Mit und ohne SQL Server

Nach einem Update ließ sich die Testversion problemlos auf den Testrechnern installieren, sowohl mit als auch ohne Fallmanagement über MS SQL. Installiert man ohne MS SQL, benutzt das Werkzeug SQLite im Hauptspeicher. Die Datenmodelle kann man den zugehörigen CreateDB-Anweisungen entnehmen. Die Beispiele (im Sample-Verzeichnis oder von der Download-Seite forensic.belkasoft.com/en/bec/en/download.asp), die die neuen Features demonstrieren sollen, funktionierten zügig und tadellos.

Die moderne Oberfläche wirkt aufgeräumt. Man findet sich rasch zurecht und kann intuitiv die richtige Auswahl treffen.

Besonders beeindruckte, wie einfach man viele Messenger-Artefakte gleichzeitig auslesen, carven, aus Hauptspeicher-Artefakten extrahieren sowie aus dem Netzwerkmitschnitt rekonstruieren kann. Hier hätte auch ein erfahrener Forensiker deutlich mehr Zeit aufwenden müssen und unter Umständen Spuren übersehen können. Praktisch ist die Suche nach Mustern in gefundenen Verläufen anhand regulärer Ausdrücke. Die mächtigen Funktionen zur Bild- und Videoanalyse sind nützlich, weil Dateitausch auch über Messenger und Soziale Netzwerke stattfindet. Alle Ergebnisse konnten wie gewünscht exportiert und in selbst für Nicht-Forensiker verständliche Berichte eingefügt werden.

Von Symantecs E-Discovery-Produkt Clearwell ist man es gewöhnt, dass eine grafische Auswertung zeigt, was mit welcher Spur passiert ist und was man im Fehlerfall tun muss, um eine vollständige Verarbeitung sicherzustellen. Ein solches Feature, das vieles auf einen Blick offenbart, würde man sich auch für das Belkasoft Evidence Center wünschen. Seiner Philosophie

© Copyright by Heise Zeitschriften Verlag

der einfachen Bedienung entsprechend verbirgt das Werkzeug jedoch die Komplexität vor den Anwendern. Das kann aber dazu führen, dass diese nur klicken und gar nicht mitbekommen, dass erhebliche „blinde Flecke“ bestehen. Man muss in jedem Fall die technischen Fehler-Logs unter *AppData\Roaming\Belkasoft\Evidence Center\Logs* prüfen.

Zwar ist das nicht besonders übersichtlich, aber man findet so zumindest die Fehlerursache. Mit einem außergewöhnlich langen Pfad im Image gelang es im Test, die Oberfläche der Entwicklungsversion von 3.5 zum Absturz zu bringen. Üblicherweise funktioniert die Fortschrittsanzeige gut. Es gibt sogar einen eigenen Taskmanager. In diesem Fall jedoch lief der Hauptspeicher voll, nachdem die Fortschrittsanzeige über fünf Stunden eingefroren war. Erst dann erschien in der Oberfläche das Fehlerfenster. Hätte man das Logfile gleich geöffnet, wäre die Ursache direkt zu sehen gewesen. Hier hätte ein Hinweis geholfen.

Gut, aber nicht perfekt

Für die Analyse der Webbrowser-Nutzung sind derzeit andere Software-Werkzeuge umfassender als das BEC. Wie bereits erwähnt, liegt die Stärke des Evidence Center bei der Wiederherstellung und Analyse von Chat-Kommunikation. Das Carving beim BEC ist wie bei den Produkten der Konkurrenz nur „naiv“ (siehe Kasten „Verschiedene Carving-Verfahren“), wodurch es unter Umständen Spuren übersehen kann, und es zwangsläufig zu falsch-positiven Einträgen kommt. Insbesondere berücksichtigt das Werkzeug weder Fragmentierung noch datenbankspezifische Artefakte. Für besondere Auswertungen sind im Einzelfall weiterhin andere Spezialwerkzeuge erforderlich. Zum Beispiel kann das Werkzeug Epilog von CCL-Forensics in SQLite-Datenbanken Daten wiederherstellen („carven“).

Wünschenswert wäre eine klarere Beschreibung dessen, was das Werkzeug nicht durchführt. Beispielsweise berücksichtigt es noch keine Spuren in den Volume Shadow Copies (VSC).

Zeitstempel zeigt das BEC derzeit in lokaler Zeit statt in der Weltzeit UTC. Der Hersteller empfiehlt als Workaround, die Zeit des Auswertesystems umzustellen. Dies ist jedoch umständlich und für eine IT-Forensik-Software nicht angemessen. Für eine spätere Version ist immerhin geplant, dass man auch Zeitzonen und -abweichungen angeben kann.

Daten und Preise

Belkasoft Evidence Center 3.5

IT-Forensik-Werkzeug

Hersteller: Belkasoft, St. Petersburg

Website: belkasoft.com

Systemvoraussetzungen: ab Windows 2000; MS SQL Server 2008 R2 erforderlich für Fallverwaltung. Für kleinere Fälle (bis 10 GByte Daten) genügt eine Workstation, für größere Fälle oder die Enterprise Version werden mindestens 4 GByte Hauptspeicher, mehrere Rechenkerne und ein SSD-Laufwerk für den SQL-Server empfohlen.

Preise: Einsteigerversion ohne Fallmanagement und nur für Instant-Messenger-Spuren (ohne Carving etc.) ab 500 US-$; Vollversion mit Fallmanagement und allen Modulen 2000 US-$

Fazit

Trotz einiger Wünsche, die beim Ermittler offenbleiben, hat Belkasoft mit dem Evidence Center ein professionelles Werkzeug vorgelegt, das Konkurrenzprodukten bezüglich Instant Messengern deutlich voraus ist und in angrenzenden Bereichen nützliche Zusatzfunktionen bietet. Es entwickelt sich zunehmend zu einer umfassenden Analyseumgebung, kann und will in Randbereichen aber andere Werkzeuge nicht ersetzen. Ein Upgrade auf die neue Version 3.5 erscheint angesichts der kommenden Änderungen sinnvoll. (ur)

ALEXANDER SIGEL

ist Geschäftsführer des IT-Forensik-Dienstleisters DigiTrace GmbH.

Anzeige

© Copyright by Heise Zeitschriften Verlag