ElcomSoft All-In-One iOS Forensic Toolkit: Nun mit Keychain-Dechiffrierung, Windows-Unterstützung und iOS 4.3.4 Akquisition

Moskau, Rußland – 25. Juli 2011 - ElcomSoft Co. Ltd. veröffentlicht ein umfassendes Update von iOS Forensic Toolkit und implementiert iOS-Akquisition auf Windows- und Mac-Plattformen. Das Unternehmen fügt mehrere neue Funktionen hinzu, um iOS Analyse gleichzeitig schneller, einfacher und umfassender zu machen.

Elcomsoft iOS Forensic Toolkit bietet einen nahezu sofortigen forensischen Zugriff auf verschlüsselte Daten, die in iPhone-Geräten gespeichert sind, und bietet Spezialisten die Möglichkeit, auf die geschützten und von iPhone-Geräten gewonnenen Datei-System-Dumps zu zugreifen, auch wenn die Daten mit einem Sicherheits-Chip von iOS 4 verschlüsselt sind.

Die neueste Version fügt Windows-Unterstützung hinzu, unterstützt logische Akquisition neben der physischen Akquisition und kann einen ursprünglichen Passcode in Geräten mit iOS 3.x sofort wiederherstellen. Brute-Force-Wiederherstellung des Passcodes ist für Geräte mit iOS 4.x verfügbar. Darüber hinaus unterstützt Elcomsoft iOS Forensic Toolkit jetzt auch eine vollständige Wiederherstellung der Schlüsselbund-Informationen, indem es Login- und Passwort-Informationen zu Websites und geschützten Ressourcen entschlüsselt, und nimmt ein umfassendes Protokoll aller Operationen auf.

Physische Akquisition als die fortgeschrittenste iOS Forensic-Analysis-Methode

Die Methode der physischen Akquisition verwendet den gedumpten Inhalt des physischen Geräts, um eine umfassende Analyse der Benutzer- und Systemdaten, die im Gerät gespeichert sind, durchzuführen. Vor Elcomsoft iOS Forensic Toolkit war die Entschlüsselung des verschlüsselten Speicherauszugs einfach nicht möglich, mit oder ohne Passcode. Der Prozess wird ohne Brute-Force der ursprünglichen Passcode (einen langwierigen Prozess, der die forensischen Untersuchungen verlangsamte, die auf der Analyse der iPhone Backup-Dateien basierten) möglich. Normalerweise erfolgt eine vollständige Akquisition eines 32 Gb iPhone 4 mit iOS 4.x während weniger als 1,5 Stunden.

Eine Analyse der physischen Akquisition bietet einen Zugriff auf viele weitere Informationen über die Verwendung eines iOS Geräts an, als eine Backup-Datei speichern kann, und bietet Experten eine Reihe von zusätzlichen Leistungen, die durch der Analyse von Backup-Dateien nicht zugänglich sind.

- Zero-Footprint: keine Änderungen am Gerät oder seinem Inhalt vorgenommen werden;
- All-in-One-Lösung;
- Bit-genaue Images: eine physische Akquisition beschäftigt sich mit kompletten System-Dumps, präzise bis zum letzten Bit;
- Typische Akquisition dauert bis zwei Stunden;
- Industrietaugliche Produkte zur forensischen Analyse können verwendet werden, um den entschlüsselten Speicherauszug zu analysieren.

Die neue Version von Elcomsoft iOS Forensic Toolkit kann auch eine logische Akquisition schneller durchführen, indem es nur die tatsächlichen Benutzer-Dateien überträgt und nicht-relevanten Speicherplatz weglässt. Mit der logischen Akquisition wird die Entschlüsselung durch das Gerät selbst (obwohl die Dateien, die Passcode für die Dechiffrierung benötigen, mit dem Image der logischen Akquisition nicht enthalten werden) durchgeführt.

(Fortsetzung auf der nächsten Seite)

Passcode Ist Nicht Nötig (Aber Manchmal Hilfreich)

Elcomsoft iOS Forensic Toolkit implementiert eine Fähigkeit, Passcodes durch Brute-Force-Attacke direkt an iOS 4.x Geräten zu retten, obwohl das nicht immer erforderlich ist.

Das Toolkit erfordert den forensischen Analytiker nicht, den ursprünglichen Passcode zu kennen. Die vollständige Akquisition eines iOS 3.x Geräts ist ohne den Passcode möglich; außerdem kann Elcomsoft iOS Forensic Toolkit originale Passcodes von solchen Geräten sofort extrahieren.

In iOS 4.x Geräten werden bestimmte Informationen wie Keychains und E-Mails ohne entweder einen Passcode oder eine gültige Escrow-Datei (erhältlich von einem Computer, mit dem das iOS-Gerät synchronisiert wurde) nicht zugänglich. Wiederherstellen eines typischen 4-stelligen Passcodes mit Hilfe von Elcomsoft iOS Forensic Toolkit dauert typischerweise nicht länger als 20 bis 40 Minuten.

Hintergrund

iPhone-Benutzer sammeln große Mengen von hochsensiblen Informationen, die in ihren Smartphones gespeichert sind. Neben den offensichtlichen Angaben wie Bilder, E-Mail- und SMS-Nachrichten speichern iPhone-Geräte erweiterte Nutzungsinformationen wie Geolocation-Daten, angesehene Google-Karten und Routen, Web-Browsing-Verlauf und Anruflisten, Login-Informationen (Benutzernamen und Passwörter), und fast alles was auf dem iPhone eingegeben wurde.

Einige, aber nicht alle diese Informationen werden in iPhone-Backups gespeichert , wenn sie mit Apple iTunes produziert sind. Allerdings ist die Menge der Informationen, die von Telefon-Backups extrahiert werden kann, natürlich begrenzt.

Forensische Experten sind sich der Menge wertvoller Informationen, die in diesen Geräten gespeichert sind, bewusst. Physische Akquisition bietet forensischen Spezialisten einige wichtige Vorteile gegenüber der Analyse von Informationen, die in iPhone-Backups gespeichert werden. Indem die physische Akquisition einen vollen Zugriff auf alle in diesen Geräten gespeicherten Daten gewährleistet, ist sie die einzige völlig verantwortliche Zero-Footprint-Methode, die, zusätzlich zu allen Benutzer-Informationen wie SMS und E-Mail-Nachrichten, auch den Zugriff auf geschützte Informationen versorgen kann, die in Keychains gespeichert sind.

Über Elcomsoft iOS Forensic Toolkit

Elcomsoft iOS Forensic Toolkit ermöglicht einen forensischen Zugriff auf verschlüsselte Daten, die in populären Apple-Geräten mit iOS 3.x oder 4.x gespeichert sind. Durch die Durchführung einer Analyse der physischen Akquisition des Gerätes bietet das Toolkit einen sofortigen Zugriff auf alle geschützte Informationen, einschließlich SMS und E-Mail-Nachrichten, Anruflisten, Kontakte und Organizer-Daten, Web-Browsing-Verlauf, Voicemail und E-Mail-Konten und Einstellungen, gespeicherter Logins und Passwörter, Geolocation-Daten und der ursprünglichen Klartext-Passcodes des Benutzers. Das Tool kann auch die logische Akquisition der iOS-Geräte durchführen oder einen forensischen Zugriff auf verschlüsselte iOS Dateisystem-Dumps versorgen.

Verfügbarkeit und Verteilung

Elcomsoft iOS Forensic Toolkit steht sofort zur Verfügung. Der Zugriff aufs neue Toolkit ist nur Strafverfolgungsbehörden, forensischen Organisationen und gewissen Regierungsbehörden gewährt. Preisauskünfte sind auf Anfrage erhältlich; Sonderkonditionen stehen bestehenden Kunden zur Verfügung.

Über ElcomSoft Co.Ltd.

ElcomSoft Co.Ltd. hat sich zum Ziel gesetzt, Unternehmen und Privatanwendern zuverlässige Applikationen zur Validierung und Rettung von Passwörtern an die Hand zu geben. Seit der Unternehmensgründung 1990 hat sich ElcomSoft einen weltweiten Kundenstamm geschaffen. So wird die Software in den meisten der Fortune 500 Unternehmen, in vielen militärischen Einrichtungen sowie von Regierungen und führenden Wirtschaftsprüfern und Steuerberatern eingesetzt. ElcomSoft ist Mitglied der Russian Cryptology Association (RCA), des Computer Security Institute, der Association of Shareware Professionals (ASP) und ist Microsoft Gold Certified Partner (Independent Software Vendor Partner, ISV). Mehr auf http://www.elcomsoft.de/