

ElcomSoft bringt neues Leben der iOS Forensik, fügt physische Akquisition für iPhone 5 und iPad 4



Moskau, Russland – der 17. Juli 2013 - ElcomSoft Co. Ltd. aktualisiert [iOS Forensic Toolkit](#) und ermöglicht eine physische Datenakquisition der letzten Apple-Geräte mit iOS 5 und iOS 6, die einen Jailbreak haben, einschließlich iPhone 4S und 5, iPad 2, 3 und 4, iPad Mini sowie der letzten Generationen von iPod Touch. Die Unterstützung für iPhone 4S und 5 wurde von forensischen Kunden besonders stark gefordert. Durch die Ermöglichung der physischen Datenakquisition der Apple-Geräten von der letzten Generation erlaubt das aktualisierte Elcomsoft iOS Forensic Toolkit eine forensische Analyse dieser iOS-Geräte.

Darüber hinaus automatisiert die neueste Version von iOS Forensic Toolkit die Datenakquisition von iOS-Geräten nach einem Jailbreak und wird die bisher erforderlichen manuellen Schritte los, indem sie die erforderliche manuelle Interaktion minimisiert. Schließlich ist die Datenakquisition von Legacy-Geräten nun komplett mit automatischer Erkennung des Gerätemodells automatisiert.

[Elcomsoft iOS Forensic Toolkit](#) bietet weiterhin die unbeschränkte Unterstützung für ältere iOS-Geräte wie iPhone 4 und frühere, unabhängig von der iOS-Version. Man kann die Passcode von diesen geschützten Geräten wiederherstellen, obwohl eine physische Akquisition in etwas eingeschränktem Modus auch ohne einen Passcode durchgeführt werden kann. Allerdings unterliegt die physische Datenakquisition von letzten iOS-Geräten den bestimmten technischen Einschränkungen. Der Zugang zur Daten von iPhone 4S und 5 sowie den letzten Generationen von iPad kann nur dann gewährt werden, wenn es bereits einen Jailbreak gibt oder wenn der Prüfer in der Lage ist, einen Jailbreak zu installieren. Zu diesem Zeitpunkt können die Geräte ohne Jailbreak und mit einem unbekanntem Passwort nicht zugegriffen werden, was beschränkt die Nutzungsumfang des Tools.

Die Geschwindigkeit der Passcode-Rettung für iPhone 5 Geräte steigert bis 15,5 Passwörter pro Sekunde, was erlaubt, einen typischen 4-stelligen Zugangscode in etwa 10 Minuten zu finden.

Physische Akquisition von iOS 6

Frühere Versionen von [iOS Forensic Toolkit](#) unterstützten bereits iPhone 4S und iPad 2 und 3 mit iOS 5. iOS 6 setzt allerdings neue Sicherheitsmaßnahmen. Bis jetzt war es unmöglich, eine physische Datenakquisition von Geräten mit iOS 6 durchzuführen. Offenbar ist es ElcomSoft noch einmal gelungen, was für die meisten unmöglich war.

Die Vorteile der Physischen Akquisition

Physische Akquisition ist die Methode für den Zugriff auf Informationen, die in iOS-Geräten gespeichert sind. Wenn es eine Wahl gibt, können forensischen Kunden durch die Durchführung der physischen Akquisition mehr Informationen aus dem Gerät erhalten, als durch jede andere Methode wie logische Datenakquisition oder Analyse von Sicherungskopien. Während es schwierig ist, genau vorherzusagen, wie lange es dauern kann, um ein Passwort für eine Offline-Sicherungskopie zu finden, kann man eine physische Datenakquisition im bestimmten Zeitrahmen fertig machen und garantiert die Akquisition des gesamten Inhalts einer 32-GB-Gerät in 40 Minuten oder weniger (je nach Menge der Informationen, die im Gerät gespeichert sind) abschließen. Die physische Datenakquisition bietet viel mehr Informationen, im Vergleich zu Backup-Analyse, durch die Schaffung eines Bit-präzisen Images des Geräts in Echtzeit. Es gibt auch mehr Daten als bei der logischen Erfassung, weil viele Dateien vom Betriebssystem gesperrt sind und nicht zugänglich nach der logischen Akquisition werden.

Andere Methoden der Datenakquisition

Wenn die physische Datenakquisition unmöglich ist, bietet ElcomSoft zusätzliche Möglichkeiten mit einem anderem Programm. Elcomsoft Phone Password Breaker ermöglicht den Zugriff auf Informationen in Offline-Backups, die auf einem lokalen Computer hergestellt werden, oder durch Herunterladen einer Kopie des Backups von Apple iCloud. Elcomsoft Phone Password Breaker ist unter <http://www.elcomsoft.de/eppb.html> verfügbar.

Kompatibilität

Es gibt zwei Versionen von Elcomsoft iOS Forensic Toolkit: für Windows und Mac OS X. Die Möglichkeit der physikalischen Akquisition für verschiedene iOS-Geräte hängt von Jailbreak oder der iOS-Version ab.

Das Tool kann eine physische Datenakquisition für die folgenden iOS-Geräte ausführen, unabhängig von Code-Sperre, Jailbreak oder iOS-Version:

- Legacy iPhone Modelle bis und einschließlich iPhone 4, alle GSM und CDMA-Modelle

- iPad (1. Generation)
- iPod Touch (1.-3. Generationen)

Die physische Akquisition für folgende Modelle kann durchgeführt werden, wenn iOS 5 oder iOS 6 installiert sind und falls Jailbreak entweder bereits installiert ist oder installiert werden kann:

- iPhone 4S
- iPhone 5
- iPad 2, 3 und 4
- iPad Mini
- iPod Touch (4. und 5. Generationen)

Zu diesem Zeitpunkt wurde die physische Datenakquisition unter iOS 6.1.2 und allen früheren Versionen getestet. Neuere Versionen von iOS werden derzeit noch nicht unterstützt, da es kein Jailbreak verfügbar ist.

Über Elcomsoft iOS Forensic Toolkit

[Elcomsoft iOS Forensic Toolkit](#) ermöglicht einen forensischen Zugriff auf verschlüsselte Daten, die in populären Apple-Geräten mit iOS 3 bis 6 gespeichert sind. Durch die Durchführung einer Analyse der physischen Aufnahme der Daten bietet das Toolkit einen sofortigen Zugriff auf alle geschützten 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, der ursprünglichen Klartext-Passwort von iTunes und Gespräche über verschiedene soziale Netzwerke wie Facebook, sowie alle anwendungsspezifischen Daten, die im Gerät gespeichert sind. Das Tool kann auch eine logische Datenakquisition der iOS-Geräte durchführen oder einen forensischen Zugriff auf verschlüsselte iOS Dateisystem-Dumps versorgen.

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, Microsoft Gold Independent Software Vendor Partner, ISV und Intel Premier Elite Partner. Mehr auf <http://www.elcomsoft.de/>