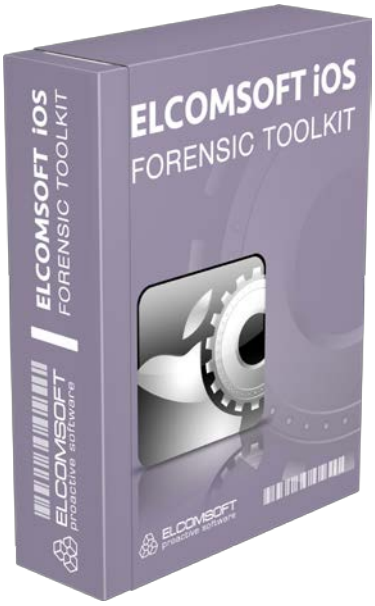
ELCOMSOFT
DESKTOP, MOBILE & CLOUD FORENSICS

ElcomSoft umgeht Apples Secure Enclave-Schutz und greift auf iOS-Schlüsselbund zu



Moskau, Russland – der 20. Juni 2018 - ElcomSoft aktualisiert das iOS Forensic Toolkit (EIFT), ein mobiles, forensisches Tool zur Datenextraktion aus iPhones, iPads und iPod Touch-Geräten. Das Tool wurde mit Version 4.0 generalüberholt und es kann nun Elemente von 64-Bit-iOS-Geräten aus dem iOS-Schlüsselbund extrahieren und entschlüsseln, wodurch der sichere Secure Enclave-Schutz auf Geräten mit oder ohne Jailbreak erfolgreich umgangen wird. Version 4.0 legt zudem einen stärkeren Fokus auf neuere iOS-Geräte und überdies wird der Support für die älteren Apple-Geräte weitgehend eingestellt. Darüber hinaus kann nun auf iOS-Crash-Logs zugegriffen werden.

iOS Forensic Toolkit 4.0 bietet die Möglichkeit, während der physischen Erfassung Schlüsselbund-Elemente zu extrahieren und zu entschlüsseln. Dabei wird der gesamte Inhalt des Schlüsselbunds entschlüsselt, einschließlich Datensätzen, die mit dem 'ThisDevice-Only'-Attribut gesichert sind. Dadurch können wichtige Informationen wie beispielsweise Authentifizierungstoken extrahiert werden. Dies wiederum ermöglicht es Forensikern auf alle Social Media- und Messer-Konten zuzugreifen, die jemals auf dem Gerät verwendet wurden. Das Tool verhindert zudem die Aktivierung der automatischen Bildschirmsperre des iOS-Geräts während die Daten-Extraktion läuft. Damit wird sichergestellt, dass auch jene Datensätze mit den stärksten Sicherheitsattributen erfolgreich extrahiert und entschlüsselt werden.

Der iOS-Schlüsselbund ist eine Lösung von Apple, um Passwörter, Schlüssel, Authentifizierungstoken, Zertifikate, Zahlungsdaten und anwendungsspezifische Anmelde-Informationen sicher zu speichern. Während einige Schlüsselbund-Elemente durch die Analyse einer kennwortgeschützten lokalen Sicherung wiederhergestellt werden können, können mit dem Attribut 'ThisDeviceOnly'-geschützte Datensätze nur auf dem Gerät selbst entschlüsselt werden.

Microsoft Partner
Gold Application Development
Gold Intelligent Systems

intel Software Partner

Der Schlüsselbund ist sicher mit einem hardwarespezifischen Schlüssel verschlüsselt. In 64-Bit-Hardware (iPhone 5s und alle neueren iOS-Geräte) ist dieser Schlüssel zusätzlich mit Secure Enclave geschützt.

*"Jailbreak oder nicht, die Umgehung der Secure Enclave Schutz galt lange als unmöglich. Mit der neusten Version des iOS Forensic Toolkit können nun Schlüsselbund-Elemente von 64-Bit-iOS-Geräten mit Secure Enclave extrahiert und entschlüsselt werden", sagt **Vladimir Katalov**, CEO von ElcomSoft.*

iOS Forensic Toolkit 4.0 bietet die physische Erfassung für alle 64-Bit-Apple-Geräte (iPhone 5s, 6 / 6s / 7/8 / Plus, iPhone SE und iPhone X) verfügbar, auf denen ein Jailbreak installiert werden kann.

Fokus auf aktuelle Geräte

In früheren Versionen von iOS Forensic Toolkit wurden Geräte unterstützt, die so alt waren, wie das iPhone 3G, das 2008 veröffentlicht wurde. Die Unterstützung solch zahlreicher Geräte führte jedoch mit der Zeit zu einer überladenen Benutzeroberfläche.

In der aktuellen Version konzentriert sich ElcomSoft auf die aktuelle Generation von Apple-Geräten: Das iOS Forensic Toolkit unterstützt alle 64-Bit iPhone-, iPad- und iPod Touch-Modelle, beginnend mit dem iPhone 5s. Durch die Beschränkung auf die aktuellen Geräte-Generationen wurde eine optimierte Benutzeroberfläche geschaffen, die einen präzisen, forensischen Workflow ermöglicht.

Zugriff auf Absturzprotokolle

iOS Forensic Toolkit 4.0 bietet die Möglichkeit, Absturzprotokolle von iOS-Geräten mit oder ohne Jailbreak zu extrahieren. Der Zugriff auf Absturzprotokolle erfordert ein gekoppeltes Gerät oder Zugriff auf eine gültige Sperrdatei.

Absturzprotokolle können wichtige Hinweise enthalten, die nicht in einem lokalen Backup enthalten sind, aber möglicherweise aus dem Gerät extrahiert werden können. Aus forensischer Sicht können Crash-Logs von Vorteil sein, da sie eine Liste der installierten und deinstallierten Apps enthalten.

Sobald ein Forensik-Experte einen Crash-Log-Eintrag entdeckt, der von einer App erstellt wurde, die nicht mehr im System vorhanden ist, kann davon ausgegangen werden, dass die App mindestens bis zu dem im Crash-Log-Eintrag angegebenen Datum und Zeitpunkt auf dem Gerät installiert war.

Preise und Verfügbarkeit

Elcomsoft iOS Forensic Toolkit 4.0 ist ab sofort für Mac OS X und Windows verfügbar. Bei einer Bestellung werden beide Versionen mitgeliefert. EIFT 4.0 ist ab 1.499 EUR zuzüglich Mehrwertsteuer erhältlich. Bestehende Kunden erhalten das Update je nach Lizenzablauf kostenfrei oder mit Rabatt.

Kompatibilität

Windows- und MacOS-Versionen von Elcomsoft iOS Forensic Toolkit sind verfügbar. Die Unterstützung der physischen Erfassung für die verschiedenen iOS-Geräte hängt vom Sperrstatus, dem Jailbreak-Status und der installierten iOS-Version ab. Für einige Geräte, auf denen einige Versionen von iOS ausgeführt werden, ist die logische Erfassung die einzige verfügbare Methode.

iOS Forensic Toolkit unterstützt die meisten Geräte mit iOS 7 bis iOS 11.

Über die ElcomSoft Co. Ltd.

Die im Jahr 1990 gegründete ElcomSoft Co. Ltd. entwickelt dem neuesten Stand der Technik entsprechende forensische Computer-Tools, bietet kriminaltechnisches Computer-Training und Beratungsdienstleistungen für Computerbeweismaterial. Seit 1997 hat ElcomSoft Unternehmen, Rechtsschutzbehörden, Militär und Geheimdiensten Unterstützung gewährt. ElcomSoft-Tools werden von den meisten der Fortune 500-Unternehmen, einer Vielzahl militärischer Einheiten überall auf der Welt, ausländischen Regierungen und allen großen Wirtschaftsprüfungsgesellschaften genutzt. ElcomSoft ist Microsoft Certified Partner und Intel Software Partner. Für weitere Informationen besuchen Sie bitte unsere Website: http://www.elcomsoft.de/