ElcomSoft da nueva vida a la ciencia forense iOs, agrega Physical Acquisition Support para iPhone 5 e iPad 4

ElcomSoft Co. Ltd. Actualizaciones iOS Forensic Toolkit tras habilitar la adquisición física de los dispositivos iOS 5 e iOS 6 liberados, incluyendo 4S y 5, iPad 2, 3 y 4, iPad Mini así como las últimas generaciones de iPod Touch. La compatibilidad con iPhone 4S y 5 ha sido muy demandada por los clientes. Tras permitir la adquisición física de las últimas generaciones de los dispositivos Apple, la versión actualizada de Elcomsoft iOS Forensic Toolkit convierte el análisis de estos dispositivos iOS en una tarea factible

Además, la última actualización de iOS Forensic Toolkit automatiza la adquisición de los dispositivos liberados sin necesidad de los pasos de la ejecución manual anteriormente indispensables, reduciendo de esta manera la interacción manual necesaria al mínimo absoluto. Finalmente, la adquisición de los dispositivos legados ahora es completamente automatizada y cuenta con la automática detección de los dispositivos conectados.

Elcomsoft iOS Forensic Toolkit continua proveyendo la compatibilidad sin restricciones para los dispositivos iOs, tales como iPhone 4 y otras versiones, la versión de iOs que usan no es relevante. Se puede recuperar las contraseñas que protegen estos dispositivos legados. Sin embargo, la adquisición física puede efectuarse en el modo limitado y sin necesidad de la clave. A pesar de esta adquisición física para las últimas generaciones de los dispositivos iOS es un sujeto a ciertas limitaciones. iPhone 4S y 5 así como la última generación de los dispositivos iPad pueden ser adquiridos sólo en caso de que hayan sido liberados anteriormente o si el investigador puede liberar el dispositivo por su propia cuenta. Por el momento, los dispositivos no liberados codificados por la contraseña desconocida no pueden ser adquiridos, lo que limita de cierta forma el uso de la herramienta.

La velocidad de la recuperación de la contraseña de los dispositivos iPhone 5 liberados ha sido elevada hasta 15.5 claves por segundo, lo que permite iOS Forensic Toolkit decodificar una contraseña típica de 4 dígitos en unos 10 minutos.

Antecedentes de iOS 6 Adquisición Física

Las versiones anteriores de iOS Forensic Toolkit soportaban iPhone 4S e iPad 2 liberados así como 3 modelos que corren iOS 5. Sin embargo, iOS 6 implementa nuevas medidas de seguridad. Hasta ahora se consideraba que no se podía usar la adquisición física en los dispositivos que corren iOS 6. Aparentemente, ElcomSoft de nuevo ha logrado hacer algo que todos creían imposible.

Las ventajas de Adquisición Física

La adquisición física es una manera preferente de acceder a la información almacenada en los dispositivos iOS. Los clientes forenses tienen la opción de usar adquisición física porque les permite obtener más información del dispositivo que cualquier otro modo, incluyendo la adquisición lógica o análisis de las copias de respaldo. Mientras es muy difícil de predecir cuánto tiempo se va a necesitar para decodificar la contraseña que protege las copias respaldadas fuera de línea, la adquisición física opera en un plazo determinado que garantiza la entrega del contenido completo del dispositivo de 32-GB en 40 minutos o aun menos (dependiendo de la cantidad de la información almacenada). En comparación con el método del análisis de las copias de respaldo, la adquisición física rinde mucho más información creando de esta forma una imagen precisa del dispositivo en tiempo real. También devuelve más datos de adquisición lógica, ya que muchos archivos están bloqueados por el sistema operativo y no son accesibles durante el proceso de adquisición lógica

Dando acceso forense casi instantáneo a la información encriptada almacenada en el último iPhone y dispositivos iPad, Elcomsoft iOS Forensic Toolkit permite el acceso a los volcados de sistema de archivos protegidos extraídos de los dispositivos Apple compatibles incluso si la contraseña del dispositivo original es desconocido.

Otros Métodos de Adquisición

Si la adquisición física no es posible, ElcomSoft ofrece opciones adicionales a través de la adquisición de un producto separado. Elcomsoft Phone Password Breaker, este permite acceder a la información guardada en copias de seguridad fuera de línea producidas por el dispositivo en un equipo local, y la adquisición de una copia del contenido del dispositivo de Apple, iCloud. Elcomsoft Phone Password Breaker está disponible en http://www.elcomsoft.es/eppb.html

Compatibilidad

Las versiones de Elcomsoft iOS Forensic Toolkit para Windows y Mac OS X están disponibles. La compatibilidad para la adquisición física para los distintos dispositivos iOS varía en función del estado de bloqueo, estado jailbreak y la versión de iOS instalada.

La herramienta se puede optimizar la adquisición física de los siguientes dispositivos iOS sin bloqueo y el estado jailbreak, e independientemente de la versión de iOS:

- El legado de modelos iPhone hasta e incluyendo iPhone 4, todos los modelos GSM y CDMA compatibles
- El iPad original
- Las generaciones de iPod Touch 1 al 3

La adquisición física se puede realizar para los siguientes modelos si se están ejecutando iOS 5 o iOS 6 y son jailbreak, o si el código de jailbreak puede ser instalado por el investigador:
- iPhone 4S
- iPhone 5
- iPad 2, 3 y 4
- iPad Mini
- iPod Touch 4ª y 5ª generación

Hasta hoy, la adquisición física ha sido probada en IOS 6.1.2 y en todas las versiones anteriores. Las nuevas versiones de iOS actualmente no son compatibles en dispositivos recientes que no han sido liberados.

Acerca de Elcomsoft iOS Forensic Toolkit

Elcomsoft iOS Forensic Toolkit provee acceso forense a la información codificada almacenada en los dispositivos populares de Apple que corren las versiones de iOS de 3 a 6. Al realizar el análisis de adquisición física del propio dispositivo, Toolkit ofrece un acceso instantáneo a toda información protegida incluyendo los mensajes SMS, los correos electrónicos, historiales de llamadas, contactos, agenda, historiales de navegadores, buzón de voz, las cuentas email y configuraciones, nombres de usuarios y contraseñas almacenadas, historia de ubicación geográfica, las contraseñas de texto plano auténticas de iTunes y las conversaciones realizadas en diferentes redes sociales, tales como Facebook, así como los datos específicos de aplicaciones almacenados en el dispositivo. La herramienta también realiza la adquisición lógica de los dispositivos iOs y provee acceso forense a los archivos codificados del volcado del sistema iOS.

Acerca de ElcomSoft Co. Ltd.

Establecida en 1990 ElcomSoft Co. Ltd es una empresa global, experta reconocida en la industria de computación que desarrolla las herramientas de computadoras forenses de última generación, ofrece un entrenamiento en informática forense y consultas sobre evidencia digital. ElcomSoft ha sido primero en patentar numerosas técnicas de codificación, estableciendo y superando las expectativas constantemente rompiendo los records de rendimiento de la industria. ElcomSoft es Microsoft Gold Independent Software Vendor, Intel Software Premier Elite Partner, miembro de Russian Cryptology Association (RCA) y Computer Security Institute.