ElcomSoft Tool Helps Analyse Location Data from iOS Devices

Moscow, Russia – June 06, 2018 - ElcomSoft Co. Ltd. updates Elcomsoft Phone Viewer, the company's companion tool for analyzing information extracted with other ElcomSoft tools. Version 3.70 adds support for aggregated location data, combining location information obtained from multiple sources such as system logs and EXIF data into a single timeline. In addition, EPV 3.70 adds the ability to process and view TAR files produced in the course of physical acquisition with Elcomsoft iOS Forensic Toolkit.

"For a long time, we've been doing physical acquisition of 64-bit iOS devices, but offered no tool to analyze information being extracted", says Vladimir Katalov, ElcomSoft CEO. "In this release, we've added support for the TAR images produced as the result of physical acquisition performed with Elcomsoft iOS Forensic Toolkit and third-party forensic tools such as GrayKey."

Background

Since the introduction of the iPhone 5s, Apple's first 64-bit iPhone, forensic experts approached physical acquisition via file system dumps. File system imaging is the only physical acquisition technique available for iPhone and iPad devices equipped with Apple's 64-bit processors. The imaging occurs on the device in order to bypass full-disk encryption. Since the imaging is performed by the device itself, the result of these efforts is always a TAR archive containing an image of the device's file system. The format does not change regardless of the tool performing physical acquisition. Elcomsoft iOS Forensic Toolkit as well as third-party forensic solutions such as GrayKey produce TAR files in the same format and containing identical data.

© 2018 ElcomSoft Co. Ltd.
Microsoft Partner
Gold Application Development
Gold Intelligent Systems
intel Software Partner

The resulting file system image may contain critical evidence that cannot be accessed via any other means such as logical or cloud extraction. One example of such evidence is the list of locations revealing estimated coordinates of the device at any given time or period of time. Combining location data with other bits and pieces can lead to important discoveries, such as finding out the location of the user during a given phone call, or pinning a given picture or video footage to a point on the map.

Up until now, the tools for analysing information inside these TAR images were offered as integral parts of fully-featured forensic toolkits. Experts would be limited to either time-consuming and labour-intensive manual analysis requiring a high level of expertise, or a highly sophisticated and complex forensic suite, with nothing in between.

Elcomsoft Phone Viewer 3.70 offers a perfect lightweight alternative to both the manual analysis and the use of sophisticated forensic packages, providing experts with a tool that is easy to master without day-long training sessions.

Aggregated Location Data

Elcomsoft Phone Viewer 3.70 brings location analysis to a whole new level, adding a new aggregated view to help experts analyse the user's location history based on evidence extracted from multiple sources. The current release extracts and aggregates location information from the system (frequently visited places, GSM and WI-Fi connections), several built-in and third-party applications (from Google Maps to Uber) and geotags in media files.

By accessing location data gathered from such a wide range of sources, experts are no longer limited to evidence collected from just the location logs. Some sources are only available with physical extraction (TAR files), and some data may be limited when analyzing backups. The number of supported sources of location data will be growing in future releases of Elcomsoft Phone Viewer.

© 2018 ElcomSoft Co. Ltd.
Microsoft Partner
Gold Application Development
Gold Intelligent Systems
intel Software Partner

About Elcomsoft Phone Viewer

Elcomsoft Phone Viewer is a lightweight package renowned for its high speed and ease of use, making it easy to learn and quick to master. The Media Gallery makes it easier to browse through thousands of still images and videos on the device, while convenient searching, grouping and filtering help discovering and organizing evidence. Full support for location data allows to quickly identify locations visited by the subject.

Supporting backups produced by popular Apple, BlackBerry and Windows Phone devices, tool offers access to contacts, messages, call logs, notes and calendar, and allows viewing information about the device. The small, inexpensive tool offers a simple and convenient user interface that matches the usage experience of Elcomsoft Phone Breaker, thus requiring no additional learning curve.

Pricing and Availability

Elcomsoft Phone Viewer 3.70 is available immediately. Home and Forensic editions are available, priced for $79 and $399 respectively in North America. TAR support is a feature exclusive to the Forensic edition.

System Requirements

Elcomsoft Phone Viewer supports Windows 7, 8, 8.1, and Windows 10 as well as Windows 2008, 2012 and 2016 Server.

About ElcomSoft Co. Ltd.

Founded in 1990, ElcomSoft Co. Ltd. develops state-of-the-art computer forensics tools, provides computer forensics training and computer evidence consulting services. Since 1997, ElcomSoft has been providing support to businesses, law enforcement, military, and intelligence agencies. ElcomSoft tools are used by most of the Fortune 500 corporations, multiple branches of the military all over the world, foreign governments, and all major accounting firms. ElcomSoft is a Microsoft Partner (Gold Application Development), Intel Premier Elite Partner and member of NVIDIA's CUDA/GPU Computing Registered Developer Program.

© 2018 ElcomSoft Co. Ltd.