ELCOMSOFT
PROACTIVE SOFTWARE

Forensic Disk Decryptor 2.0 Provides All-in-One Solution for Accessing Encrypted Volumes

Moscow, Russia – January 31, 2018 - ElcomSoft Co. Ltd. releases a major update to Elcomsoft Forensic Disk Decryptor, a forensic tool for extracting information from encrypted disk volumes. The new release makes the toolkit a fully integrated, all-in-one solution for accessing encrypted FileVault 2, PGP, BitLocker and TrueCrypt volumes. The updated toolkit gains the ability to mount or decrypt encrypted volumes using plain text passwords, escrow keys, or cryptographic keys extracted from the computer’s volatile memory image. In addition, a new Microsoft-signed zero-level memory dumping tool is now supplied with the toolkit, allowing experts to image computer’s RAM on Windows computers.

Elcomsoft Forensic Disk Decryptor offers real-time access to information stored inside encrypted containers. Supporting all major full-disk encryption products and delivering zero-footprint operation, the tool is truly invaluable tool for conducting digital investigations.

The tool can be truly indispensable for an investigation if the user’s computer was seized in a powered-on state. Elcomsoft Forensic Disk Decryptor offers a truly forensically sound solution for mounting or decrypting encrypted volumes if a text password or escrow key is available by mounting the volume or decrypting the data for offline analysis. While full decryption may take hours depending on the size of the volume and the amount of data, the mounting works in real time and offers immediate access to essential evidence.

As a last resort, if there is no access to password or any of the keys, one can extract the password hash from the encrypted volume for further password recovery in Elcomsoft Distributed Password Recovery, which will perform a high-performance attack on a local network or Amazon cloud.

Integrated Solution for Accessing Encrypted Volumes

In previous versions, the toolkit was limited to mounting or decrypting volumes with binary cryptographic keys extracted from the computer’s memory image or hibernation file. The ability to use plain-text passwords or escrow keys for accessing data stored in the encrypted containers was sorely missing.

Elcomsoft Forensic Disk Decryptor 2.0 adds the ability to mount encrypted volumes or to perform full decryption for offline analysis by using plain-text passwords, escrow or recovery keys, as well as the binary keys extracted from the computer's memory image. FileVault 2 recovery keys can be extracted from iCloud with Elcomsoft Phone Breaker, while BitLocker recovery keys are available in Active Directory or in the user's Microsoft Account.

Built-In Kernel Level Memory Dumping Tool

Elcomsoft Forensic Disk Decryptor can scan the computer's volatile memory image to look for cryptographic keys that are used for accessing data stored in encrypted containers. By extracting and using these keys, the tool can decrypt the content of the encrypted volume without running a lengthy attack on the original plain-text password.

Before this release, Elcomsoft Forensic Disk Decryptor was relying on live memory images created with other tools. The lack of proper forensic-grade memory imaging tools on the market urged ElcomSoft to develop its own solution.

Elcomsoft Forensic Disk Decryptor 2.0 comes with a forensic-grade memory imaging tool that uses zero-level access to computer's RAM in order to create the most complete memory image. ElcomSoft's RAM imaging driver works in kernel mode and carries a Microsoft digital signature, making the driver fully compatible with all 32-bit and 64-bit versions of Windows from Windows 7 and up to the latest Windows 10 Fall Creators Update.

Automatic Detection of Encrypted Volumes and Encryption Settings

Elcomsoft Forensic Disk Decryptor 2.0 offers fully automatic detection of encrypted volumes and encryption settings, including TrueCrypt. Experts will only need to provide path to the encrypted container or disk image, and Elcomsoft Forensic Disk Decryptor will automatically detect and display encrypted volumes and details of their encryption algorithms.

EnCase .E01 Support and Portable Version

Elcomsoft Forensic Disk Decryptor 2.0 now fully supports EnCase images in the industry-standard .EO1 format, as well as encrypted DMG images. In addition, Elcomsoft Forensic Disk Decryptor can be used to create a portable installation on a user-provided USB flash drive. The portable installation can be used to image computer's volatile memory and/or mount or decrypt encrypted volumes.

About Elcomsoft Forensic Disk Decryptor

Elcomsoft Forensic Disk Decryptor provides instant access with on-the-fly decryption of encrypted data stored in popular crypto containers. Supporting desktop and portable versions of BitLocker, PGP and TrueCrypt, the tool can either decrypt all files and folders stored in a crypto container or mount the encrypted volume as new drive letter for instant access.

Plain-text passwords, escrow or recovery keys as well as cryptographic keys extracted from memory dumps or hibernation files can be used to instantly unlock encrypted volumes. It is essential that the memory dump is obtained from a live system, locked or unlocked, with encrypted volumes mounted. Memory dumps produced with most recognized forensic products are supported. Decryption keys can also be derived from hibernation files if the target PC is suspended. In either case, the encrypted volumes must be mounted at the time of acquisition or before the computer was hibernated.

Compatibility

Elcomsoft Forensic Disk Decryptor runs on all 32-bit and 64-bit editions of Windows 7, 8, 8.1 and 10, as well as the corresponding Windows Server versions. The tool supports all legacy and current versions of BitLocker, PGP and TrueCrypt (and its successors) including BitLocker-to-Go and PGP Whole Disk Encryption up to and including the updated BitLocker with XTS-AES. Encrypted volumes and full disk encryption are supported for PGP and TrueCrypt.

Pricing and Availability

Elcomsoft Forensic Disk Decryptor is available immediately. North American prices start from $599 with a 30% introductory discount available until February 28, 2018. Local pricing varies.

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.