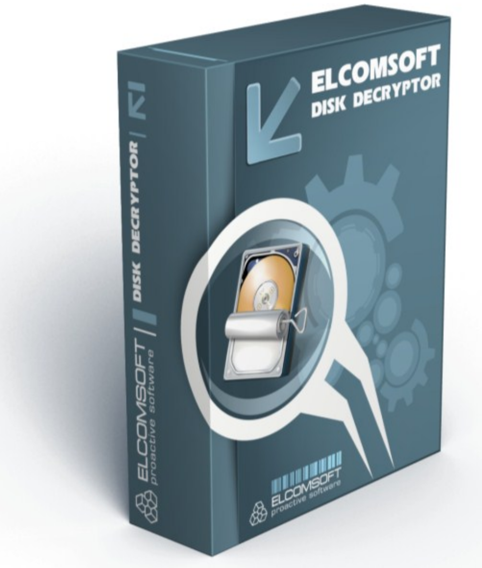
ElcomSoft Provides Forensic Access to Encrypted BitLocker, PGP and TrueCrypt Containers



ElcomSoft Co. Ltd. announces the release of Elcomsoft Forensic Disk Decryptor, a forensic tool providing access to information stored in disks and volumes encrypted with BitLocker, PGP and TrueCrypt. Supporting several acquisition modes, Elcomsoft Forensic Disk Decryptor offers complete access to encrypted information in real time. Recognizing desktop and portable crypto containers and offering zero-footprint operation, the new tool becomes an invaluable tool for investigators, IT security and forensic specialists.

"Our customers asked us for a tool like this for a long, long time", says Vladimir Katalov, ElcomSoft CEO. "We're finally releasing a product that's able to access encrypted volumes produced by all three popular crypto containers."

"*Before Elcomsoft Forensic Disk Decryptor, only Elcomsoft Distributed Password Recovery could handle encrypted disks*", says Yuri Konenkov, ElcomSoft leading crypto analytic. "*It used brute force to break passwords. Today, we're introducing a special tool that uses a completely different approach to decrypting disks protected with PGP, True Crypt, BitLocker and BitLocker To Go. We have also added the ability to brute-force passwords for TrueCrypt and BitLocker To Go containers to Elcomsoft Distributed Password Recovery*."

ElcomSoft also adds True Crypt and BitLocker To Go plugins to Elcomsoft Distributed Password Recovery, enabling the product to attack plain-text passwords protecting the encrypted containers with a range of advanced attacks including dictionary, mask and permutation attacks in addition to brute-force.

About Elcomsoft Forensic Disk Decryptor

Elcomsoft Forensic Disk Decryptor offers forensic specialists a fast, easy way of accessing information stored in three most popular crypto containers. Supporting desktop and portable versions of BitLocker, PGP and TrueCrypt, the new 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.

The complete decryption mode provides full, unrestricted forensic access to all information stored on encrypted volumes. Alternatively, by mounting encrypted containers as drive letters, investigators gain immediate, real-time access to protected volumes. In real-time mode, information read from encrypted containers is decrypted on-the-fly. Elcomsoft Forensic Disk Decryptor offers true zero-footprint operation with no alterations or modifications to original content ever.

Elcomsoft Forensic Disk Decryptor acquires all necessary decryption keys by analyzing memory dumps or hibernation files obtained from the target PC. A memory dump can be obtained from a running PC, locked or unlocked, with encrypted volumes mounted. Memory dumps produced with any forensic product or obtained via a FireWire attack are supported. A FireWire attack requires a free third-party tool, a FireWire (IEEE 1394) cable and another PC to launch the attack from. Decryption keys can also be derived from hibernation files if a target PC is turned off.

"*For PGP Disk, one can greatly speed up the key search if the exact encryption algorithm is known*", comments Yury Konenkov, ElcomSoft's IT security analyst and developer. "*Knowing the exact encryption method is not a given with PGP Disk. Elcomsoft Forensic Disk Decryptor will work either way, but if the algorithm is known, the program will locate the decryption key sooner*."

In either case, the encrypted volumes must be mounted at the time of acquisition or before the computer was hibernated. If an encrypted volume is dismounted prior to acquisition, neither memory dumps nor hibernation files will contain proper decryption keys, and encrypted containers may not be decrypted without knowing the original plain-text password. If such a password is not known, it can be recovered with Elcomsoft Distributed Password Recovery.

Compatibility

Elcomsoft Forensic Disk Decryptor runs on all 32-bit and 64-bit editions of Windows XP, Vista, and Windows 7, as well as Windows 2003 and 2008 Server, and supports BitLocker, BitLocker To Go, PGP Whole Disk Encryption and TrueCrypt.

Pricing and Availability

Elcomsoft Forensic Disk Decryptor is available immediately. North American prices start from $299. Local pricing varies.

About ElcomSoft Co. Ltd.

Founded in 1990, ElcomSoft Co.Ltd. is a global industry-acknowledged expert in computer and mobile forensics providing tools, training, and consulting services to law enforcement, forensics, financial and intelligence agencies. ElcomSoft pioneered and patented numerous cryptography techniques, setting and exceeding expectations by consistently breaking the industry's performance records. ElcomSoft is Microsoft Gold Independent Software Vendor, Intel Software Premier Elite Partner, member of Russian Cryptology Association (RCA) and Computer Security Institute.

# # #

For more information about Elcomsoft Forensic Disk Decryptor visit http://www.elcomsoft.com/efdd.html