ELCOMSOFT
DESKTOP, MOBILE & CLOUD FORENSICS

Elcomsoft Breaks the Latest Version of VeraCrypt

Elcomsoft updates Elcomsoft Forensic Disk Decryptor, the company's all-in-one tool for accessing encrypted disks and containers. In this update, the tool adds support for the latest versions of VeraCrypt, enabling experts to extract on-the-fly encryption keys from the computer's RAM to instantly mount or decrypt VeraCrypt-protected disks without running password attacks and bypassing the associated complexity altogether.

Recent versions of VeraCrypt are using a newer, stronger way to keep on-the-fly encryption keys in the computer's RAM. Elcomsoft Forensic Disk Decryptor 2.18 can now extract these on-the-fly encryption keys from the computer's RAM for the latest versions of VeraCrypt.

About VeraCrypt Disk Encryption

VeraCrypt is the most popular successor of the open-source disk encryption tool TrueCrypt. Compared to the original, VeraCrypt offers a lot more customization options. In this update, Elcomsoft Forensic Disk Decryptor adds the ability to extract on-the-fly encryption keys from memory dumps in recent versions of VeraCrypt.

The Weakness of VeraCrypt Encryption

On-the-fly encryption keys are the only weakness of VeraCrypt, enabling investigators to access encrypted disks without brute-forcing the original plain-text password. The binary, symmetric encryption key is stored in the computer's volatile memory at all times while the encrypted disk is mounted. By extracting these keys, experts can instantly mount or decrypt encrypted disks without running password attacks and bypassing the associated complexity altogether.

Until recently, extracting VeraCrypt OTF encryption keys was straightforward. The latest VeraCrypt updates changed the way the encryption keys are handled in RAM, making the extraction of encryption keys extremely difficult. Elcomsoft Forensic Disk Decryptor 2.18 adds support for encryption keys stored by all versions of VeraCrypt including the current 1.24 Update 7. Note that EFDD 2.18 must be used to both analyze and capture memory dumps. RAM dumps created with third-party tools or older versions of EFDD will not allow discovering the encryption keys stored by recent versions of VeraCrypt.

About Elcomsoft Forensic Disk Decryptor

Elcomsoft Forensic Disk Decryptor is a fully integrated solution for accessing encrypted volumes. The tool helps experts gain access to information stored in encrypted BitLocker, FileVault 2, LUKS, PGP, TrueCrypt and VeraCrypt disks or containers. Depending on the container, the tool extracts cryptographic keys from the computer's volatile memory, hibernation and page files, or uses plain-text password or escrow keys to decrypt files and folders stored in crypto containers or mount encrypted volumes as new drive letters for instant, real-time access.

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 Certrified Partner, and Intel Software Premier Elite Partner.