4th Interpol Digital Forensics Expert Group
May 2019
Brazil

Forensic Analysis of Crypto-Containers

TrueCrypt, VeraCrypt, PGP disk, Bitlocker, FileVault

Encrypted containers. Transparent encryption.

- Two types: encrypted volume or whole disk encryption (WDE)
- Files are encrypted and decrypted “on the fly”
- Possible secrets can be used for encryption: password, encryption key, recovery key, certificate
- ANY secret is used to reveal symmetric encryption key
- Volume is mounted once after entering the secret
- Volume is dismounted manually or on OS shutdown

Crypto-containers big world…

Most popular crypto containers

TrueCrypt, VeraCrypt
Symantec Encryption/PGP Desktop
Symantec PGP Whole Disk Encryption
Microsoft BitLocker
Apple FileVault

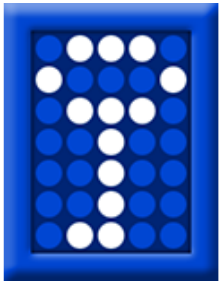
TrueCrypt

Individual ciphers supported by TrueCrypt are AES, Serpent, and Twofish.

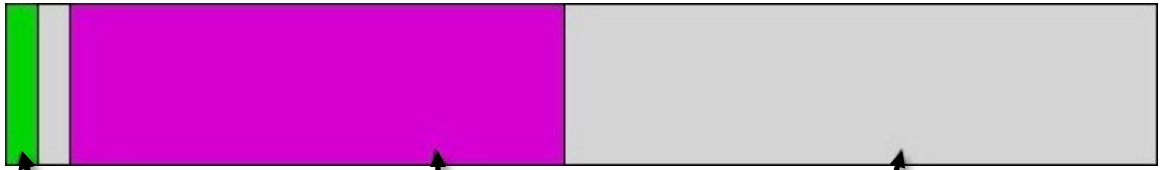
- Create virtual encrypted disk within a file
- Encrypt a partition
- Encrypt the whole storage device (pre-boot authentication)
- Create hidden encrypted volumes

TrueCrypt and VeraCrypt Forensic Acquisition

- If computer is turned on, DON'T shutdown it, even if you cannot unlock it
- If computer is turned off, DON'T turn it on. Extract the HDD if possible. Or boot from USB drive and capture the hibernation file
- If computer is turned off and hibernation is not enabled, you have only one way to get access: brute-force the password by Elcomsoft Distributed Password Recovery
- **Hidden volume** is a volume located within the free space of another TrueCrypt volume. Even when the outer volume is mounted, it is hard to prove whether there is a hidden volume or not.



TrueCrypt Standard Volume

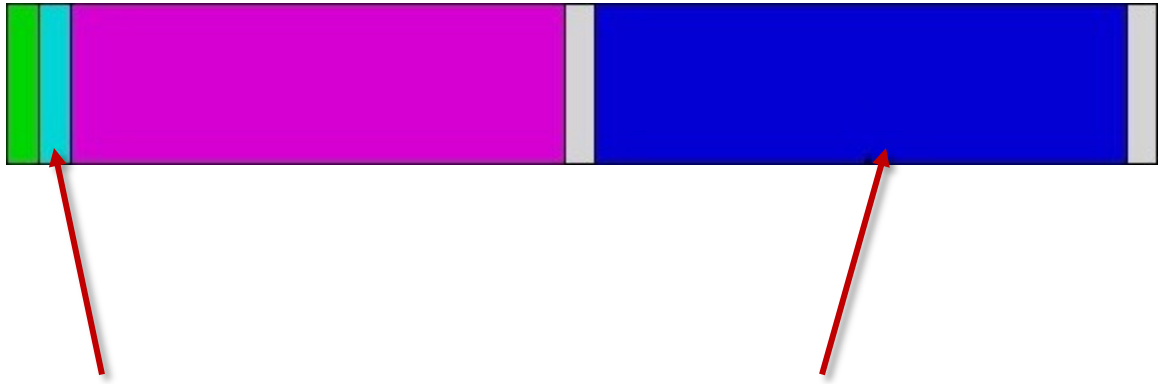


Space occupied by files

Header of standard volume

Free space (**containing random data**)

The standard TrueCrypt volume, after a hidden volume created within



Header of Hidden Volume

Data area of the Hidden Volume

TrueCrypt

As of May 28, 2014 development has been discontinued. Major successors are:

VeraCrypt and **CipherShed**.

Microsoft BitLocker

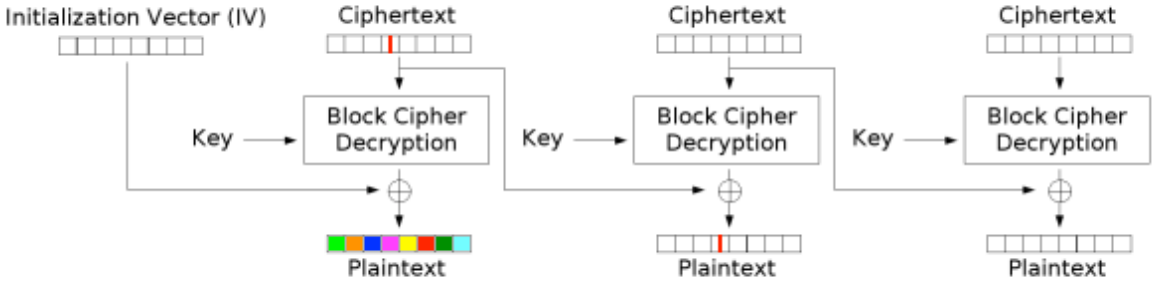
BitLocker is a full disk encryption feature included with Windows Vista and later.

Designed to protect data by providing encryption for entire volumes.

By default, it uses the **AES** encryption algorithm in cipher block chaining (CBC) or XTS mode with a 128-bit or 256-bit key. CBC is not used over the whole disk; it is applied to each individual sector.

Microsoft BitLocker encryption algorithms

Cipher block chaining (CBC)



Cipher Block Chaining (CBC) mode decryption

Microsoft BitLocker encryption algorithms

- AES 128 with CBC
- AES 256 with CBC

AES 128 with CBC is used by default

Symantec PGP Desktop / WDE

Symantec solutions allow creating encrypted volumes with PGP encryption (RSA/IDEA algorithms):

- In a container file
- As an encrypted disk volume
- With full-disk encryption (Symantec PGP Whole Disk Encryption)

Apple FileVault 2

FileVault 2 offers full-disk encryption (FDE). When enabled, the entire contents of the startup drive are encrypted. When computer is powered off, the drive's data is fully unrecoverable without a password.

FileVault 2 uses the **AES-XTS mode of AES with 128 bit blocks and a 256 bit key** to encrypt the disk.

Attacks and Vulnerabilities

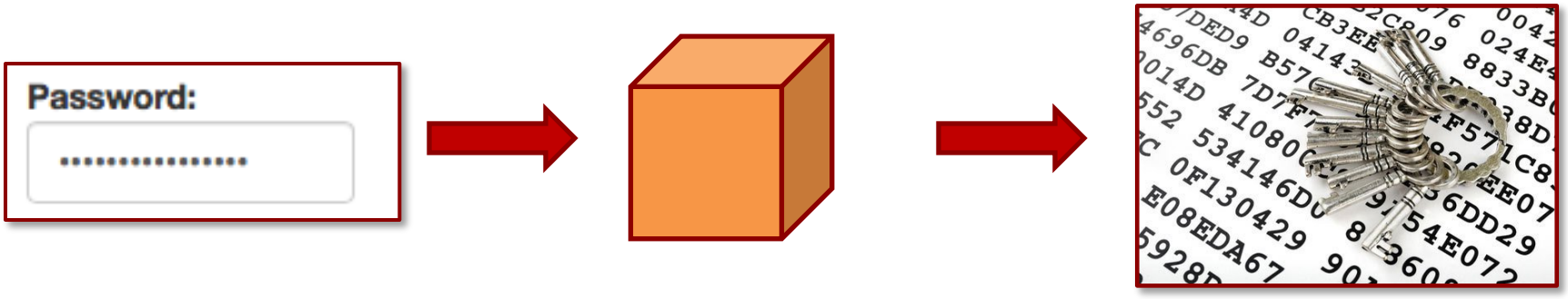
1. **Instant recovery** – weak encryption algorithm, document contains password data
2. **Instant access** – password is not required to data access, vulnerability in encryption algorithm, backdoor presents
3. **Guaranteed time password recovery** – using precomputed passwords/hashes tables (Rainbow Table/Thunder Table)
4. **Specific to document** – for example, attack by known data in WinZip, latest vulnerability in WPA encryption
5. **Dictionary Attack** – brute force with dictionaries that contains most known user passwords
6. **Brute Force**

Unbreakable encryption

Crypto-containers employ the strongest encryption with no known vulnerabilities.

- AES 128/256
- Blowfish
- Serpent
- TwoFish
- RSA
- IDEA…

User password & data encryption keys

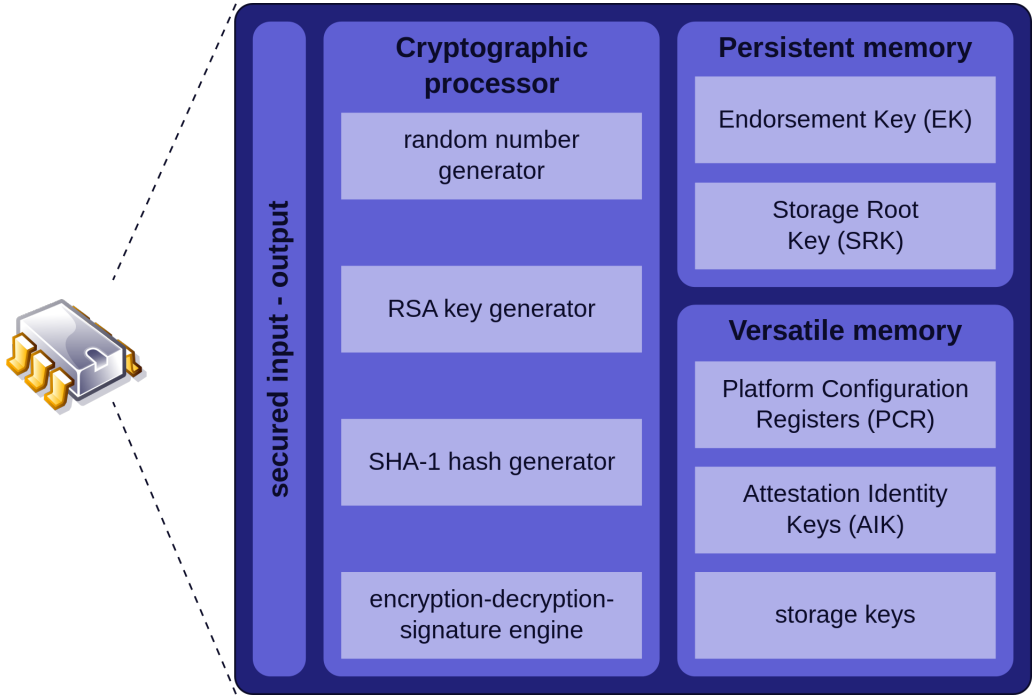


OTFE keys vulnerability by design

Once the encrypted volume is mounted, OTFE keys must exist in PC memory to provide On-The-Fly decryption/encryption functionality

Crypto containers and Trusted Protection Module (TPM)

- International standard for hardware cryptoprocessor (ISO 11889)
- Has unique RSA private key that cannot be extracted
- Can be used to authenticate computer hardware
- **Can be used to securely store symmetric encryption keys**



OTFE keys vulnerability by design

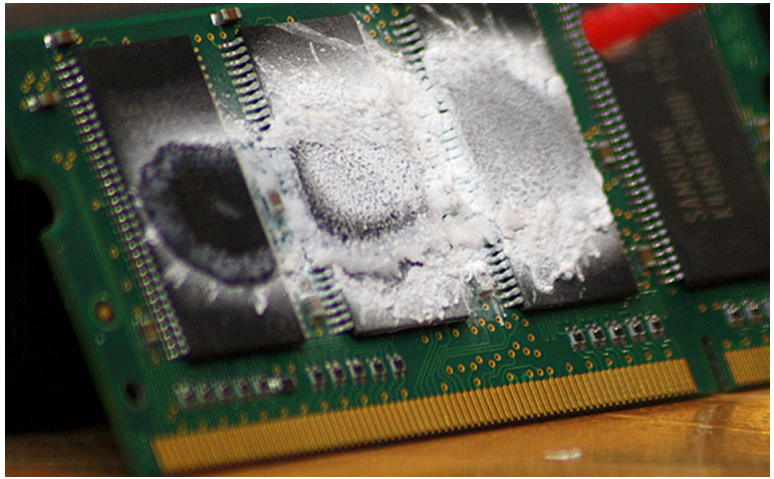
Even if TPM module is used for data protection, OTFE keys are still in memory!

The Cold-Boot Attack

- Computer memory modules (RAM) store all the data after losing power. For seconds or minutes at normal operating temperature
- Freezing memory modules by liquid nitrogen or compressed air increases data life time to hours
- Memory contents can be read either “in place” or by moving modules to another computer

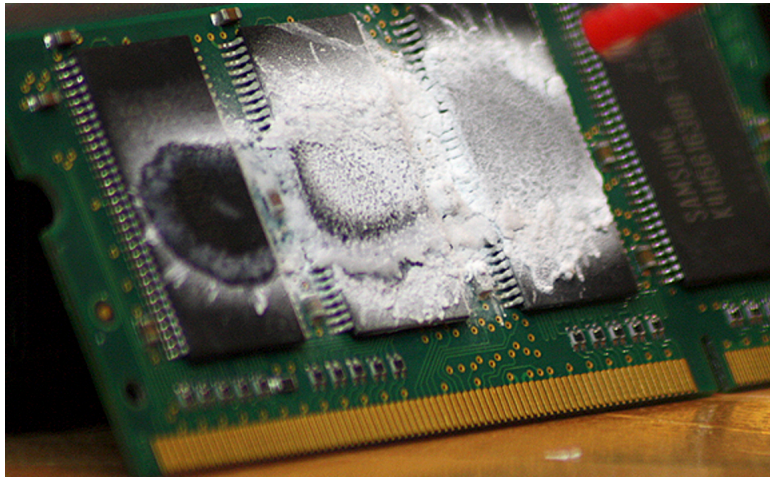
Cold-Boot Attack: when to use

- Computer is powered on
- You cannot unlock the computer and run memory dump
- Computer does not have Firewire or Thunderbolt port
- Firewire memory dump attack failed (keys are located over 2 GB limit)



Cold-Boot Attack: how to

- Disassemble the computer and locate memory modules
- Freeze the modules
- Terminate the computer power (press Power for a long time on laptops)
- **DON'T shutdown OS**
- Boot from Linux USB flash with LiME kernel extension installed
- Dump the memory
- Open the dump in Elcomsoft EFDD to find encryption keys



OTFE encryption keys is enough?

If we have access to OTFE encryption keys, user password is no required to access encrypted data!

Otherwise, it is impossible to find OTFE encryption keys using brute force attack on keys. It can be possible by using a brute force attack on user password.

The Weakness of Crypto Containers

The main and only weakness of crypto containers is human factor. Weak passwords aside, encrypted volumes must be mounted for the user to have on-the-fly access to encrypted data.

No one likes typing their long, complex passwords every time they need to read or write a file. As a result, keys used to encrypt and decrypt data that's being written or read from protected volumes are kept readily accessible in the computer's operating memory. Obviously, what's kept readily accessible can be retrieved near instantly by a third-party tool. Such as **Elcomsoft Forensic Disk Decryptor**.

Three Ways to Acquire Encryption Keys

- By analyzing the **hibernation file** (if the PC being analyzed is turned off)
- By analyzing a **memory dump** file (if the PC turned on and you have administrative access)
- By performing a **FireWire attack** (if the PC turned on, and it's locked by password)

Two ways to get a memory dump

- Using a memory imaging tool or processing the hibernate file by **Elcomsoft Forensic Disk Decryptor 2.x**

- Through a **FireWire attack**. It is possible for FireWire devices to directly access the memory of a computer, even if it is locked!

On one condition

The encrypted disk **must be mounted to the system when you make the dump** (or when the computer has been put to the hibernate state).

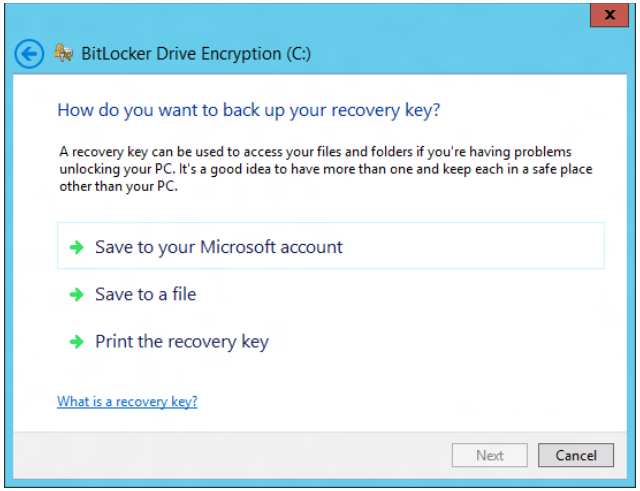
Otherwise, **the encryption keys are not stored in memory.**

One more thing… Clouds & Networks!

- **Apple FileVault 2** keys can be found in iCloud Apple keychain
- **Microsoft BitLocker** recovery keys can be found in Microsoft Account online
- **Microsoft BitLocker** recovery keys can be found in ActiveDirectory file

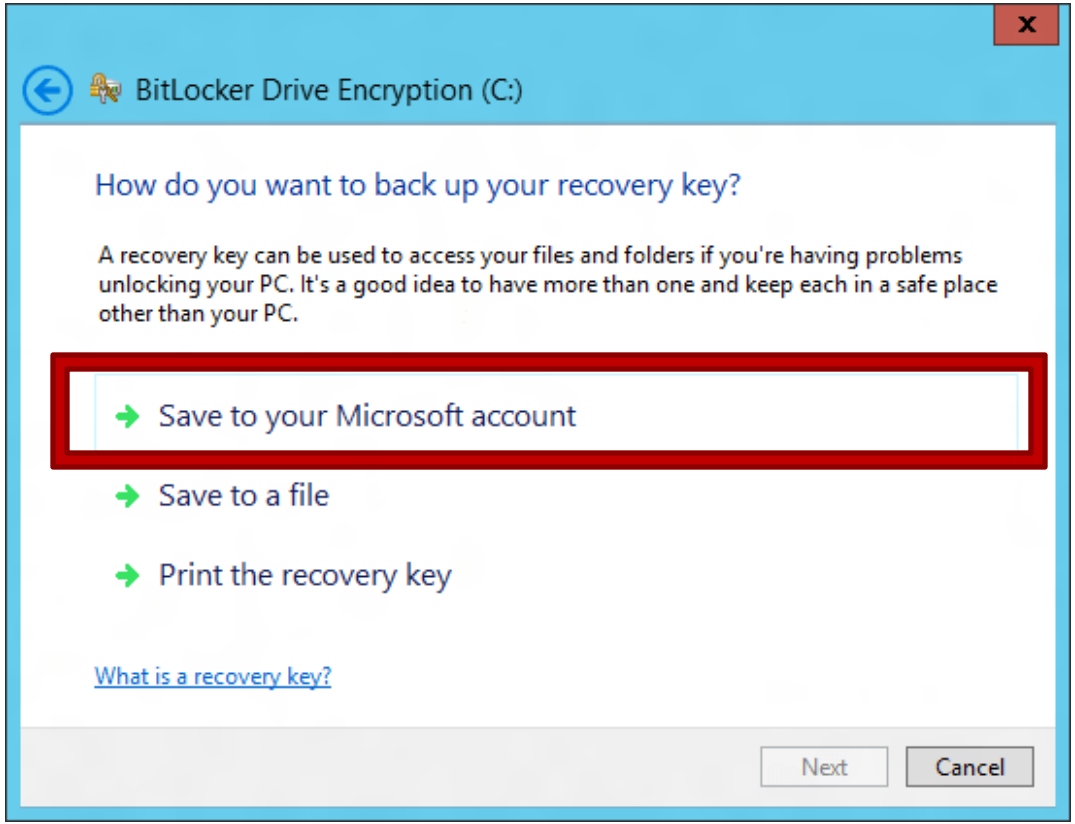
Microsoft BitLocker.
Acquiring recovery keys from Microsoft Account

One of the new features in Windows 8 for BitLocker is the ability to backup your BitLocker recovery key to a Microsoft account. During the process and before the encryption begins, the user is prompted for a location to make a backup copy of the recovery key. Saving to Microsoft account has been added along with saving to a file and printing the recovery key.



The feature even extends to fixed data drives and removable drives!

Obtaining encryption key from the Clouds



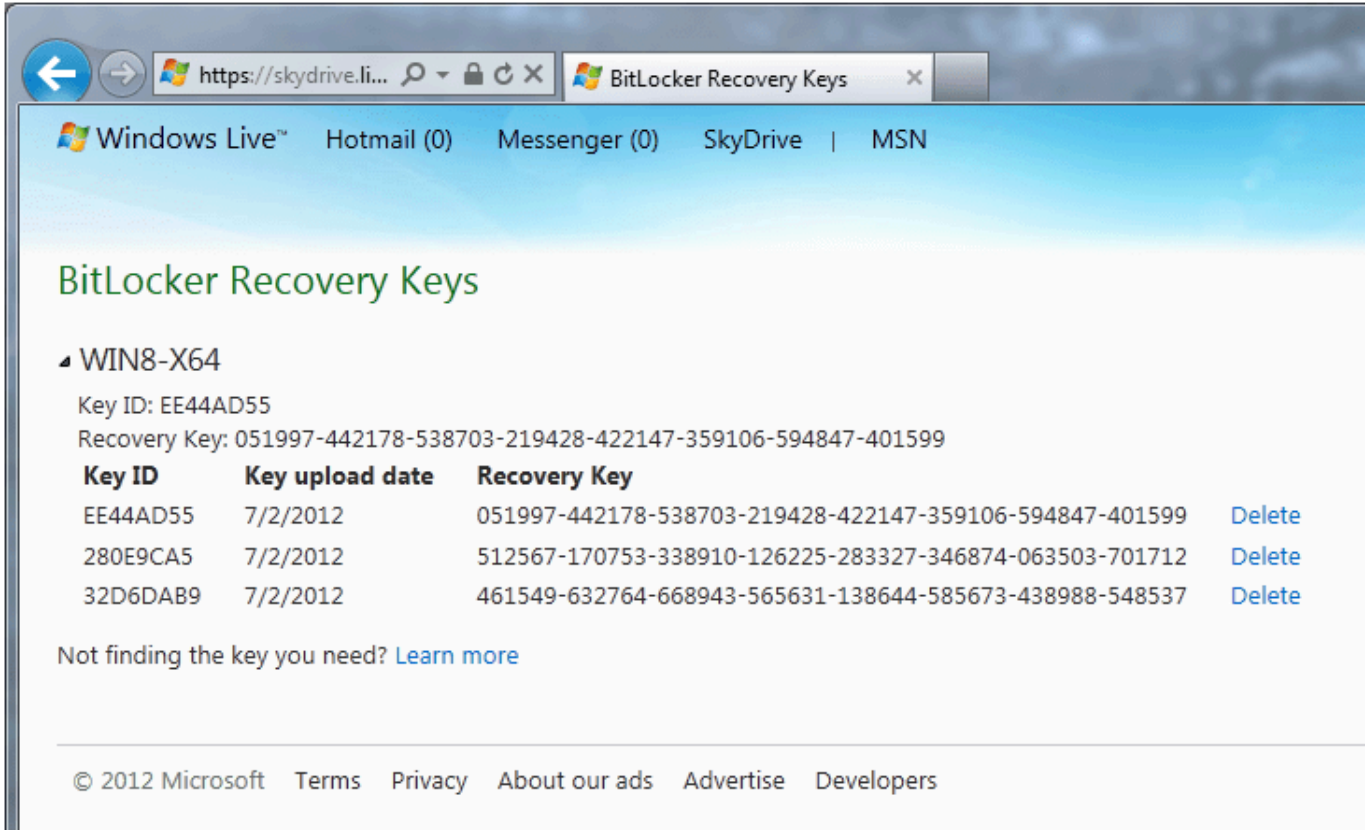
Microsoft BitLocker.
Acquiring recovery keys from Microsoft Account

So, if BitLocker recovery keys saved into a Microsoft account, how can we access it?

Actually, it is pretty simple!

- Go to **http://onedrive.live.com/RecoveryKey**
- Log in with Microsoft account credentials
- **Retrieve recovery keys for all devices that linked with this account**

Obtaining encryption key from Microsoft Cloud

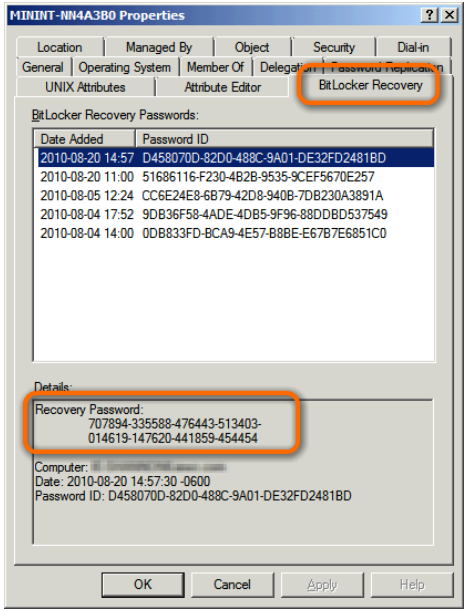


Microsoft BitLocker.
Acquiring recovery key from Active Directory

Microsoft BitLocker Drive Encryption can be configured to back up recovery information for BitLocker-protected drives and the Trusted Platform Module (TPM) to Active Directory Domain Services (AD DS).

C:\Windows\NTDS\ntdis.dat

Use **Elcomsoft Forensic Disk Decryptor 2.x** to acquire this keys from ActiveDirectory file.



Last resort. Brute-force user password

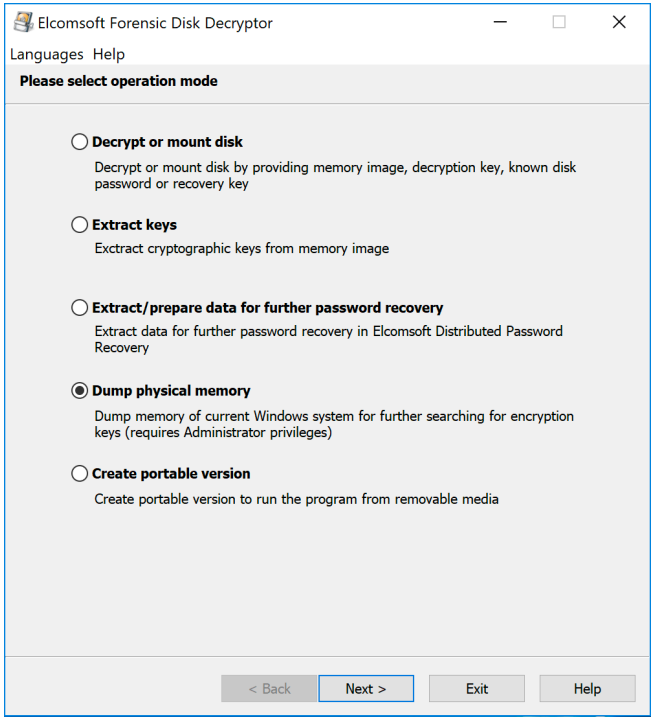
If there is no OTFE keys found in memory or encrypted drive dismounted, only one attack is possible – brute force ☹

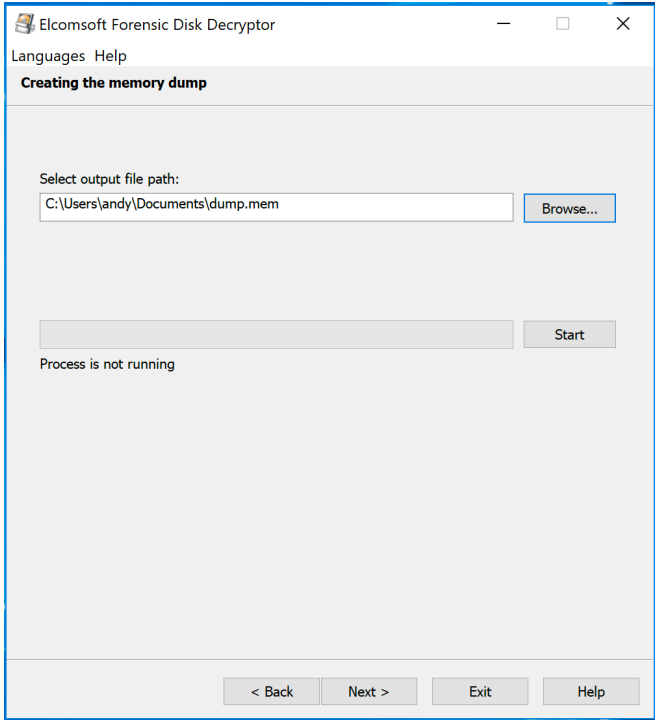
Elcomsoft Forensic Disk Decryptor

- Forensic analysis of encrypted disks and volumes protected with BitLocker, PGP, TrueCrypt and VeraCrypt
- Dump physical memory, even for Bitlocker with TPM
- Extract Bitlocker recovery keys from ActiveDirectory
- Support of Encase, Disk Dump (dd) and Apple (dmg) disk images
- Extract hashes from disk images to brute-force passwords
- Portable version to run from removable media

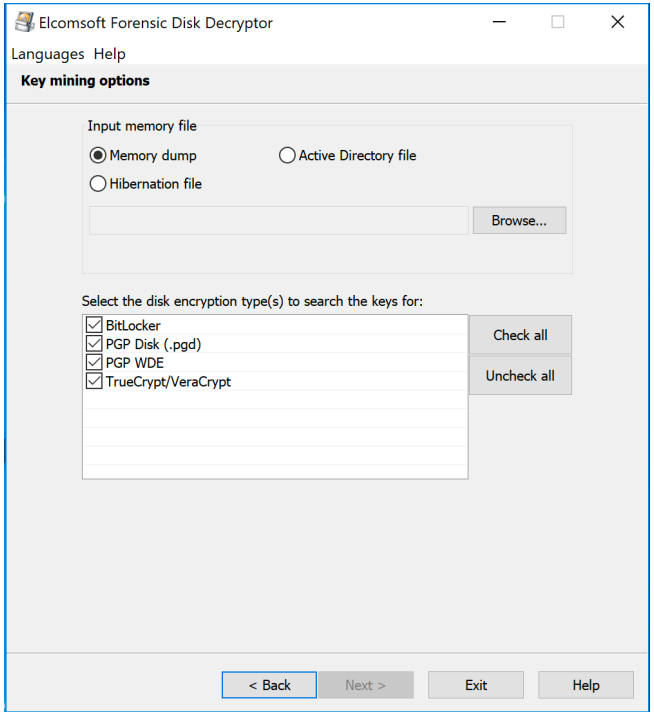
https://www.elcomsoft.com/efdd.html

Obtaining a memory dump using EFDD 2.x.

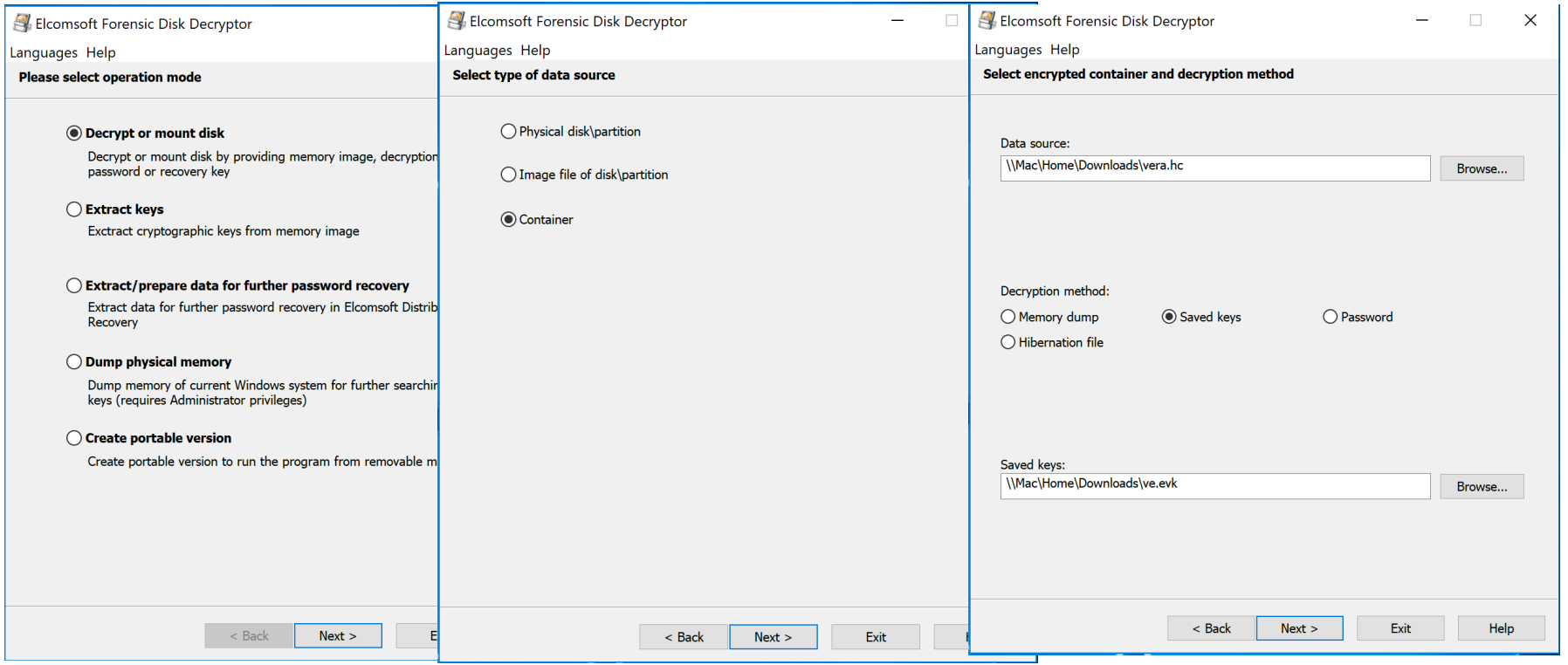




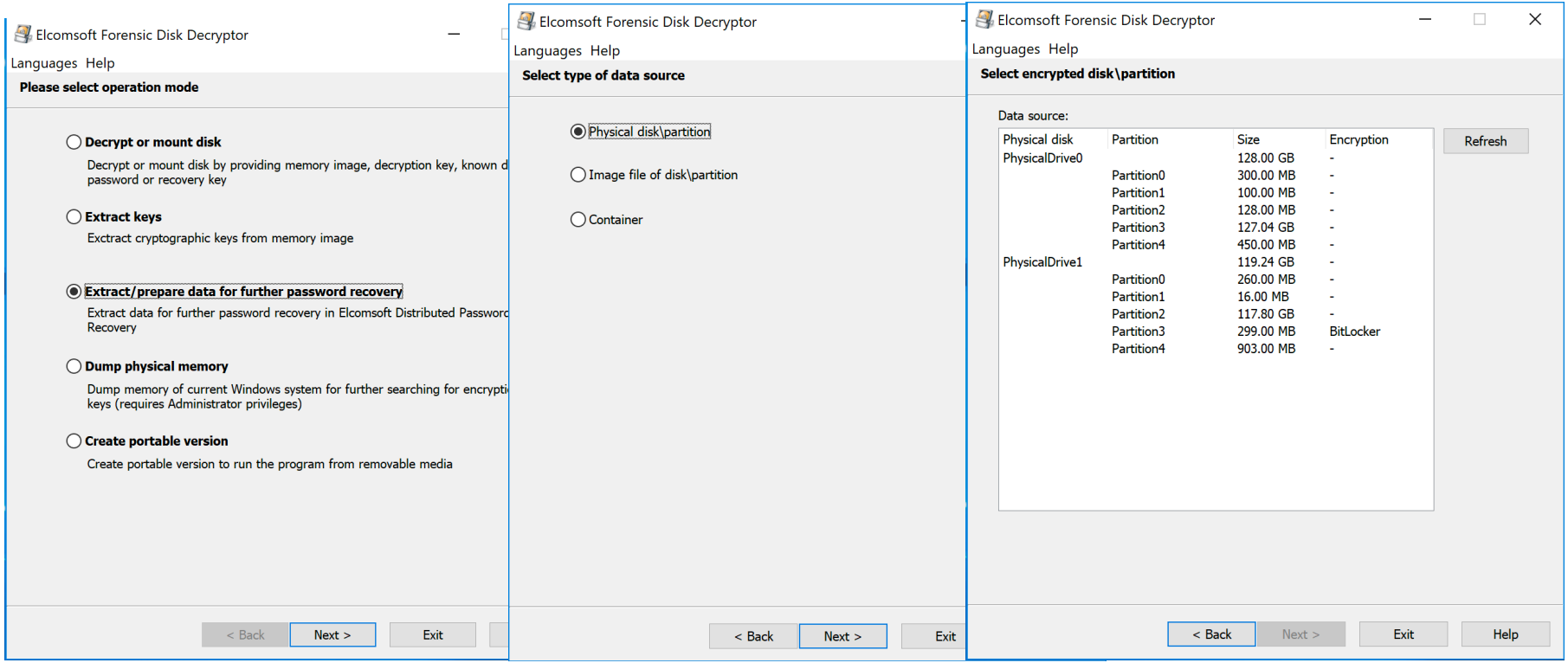
Finding and Extracting OTFE keys from the memory dump



Decrypt or Mount Encrypted Container



Prepare data for Brute Force



FireWire attack

The FireWire attack method is based on a known security issue that impacts FireWire / i.LINK / IEEE 1394 links. One can take direct control of a PC or laptop operating memory (RAM) by connecting through a FireWire. After that, grabbing a full memory dump takes only a few minutes. What made it possible is a feature of the original FireWide/IEEE 1394 specification allowing unrestricted access to PC's physical memory for external FireWire devices.

Direct Memory Access (DMA) is used to provide that access. As this is DMA, the exploit is going to work regardless of whether the target PC is locked or even logged on. There's no way to protect a PC against this threat except explicitly disabling FireWire drivers. The vulnerability exists for as long as the system is running.

Obtaining a memory dump using Inception FireWire exploit

Inception Metasploit

http://breaknenter.org/2014/09/inception-metasploit-integration/

https://github.com/carmaa/inception

Obtaining a memory dump using Inception FireWire exploit

>incept dump

```
incept dump

 _|  _|      _|    _|_|_|  _|_|_|_|  _|_|_|    _|_|_|  _|    _|_|    _|      _|
 _|  _|_|    _|  _|        _|        _|    _|    _|    _|  _|    _|  _|_|    _|
 _|  _|  _|  _|  _|        _|_|_|    _|_|_|      _|    _|  _|    _|  _|  _|  _|
 _|  _|    _|_|  _|        _|        _|          _|    _|  _|    _|  _|    _|_|
 _|  _|      _|    _|_|_|  _|_|_|_|  _|          _|    _|    _|_|    _|      _|

v.0.4.0 (C) Carsten Maartmann-Moe 2014
Download: http://breaknenter.org/projects/inception | Twitter: @breaknenter

[*] Dumping from 0x0 to 0x40000000, a total of 1 GiB:
[============================================================] 1024 MiB (100%)
[*] Dumped memory to file memdump_0x0-0x40000000_20140830-174305.bin
[*] BRRRRRRRAAAAAWWWWRWRRRMRMRMMRMRMMMM!!!
```

Step 1. Obtaining memory dump

if the PC being analyzed is turned on, you have access to it, and the encrypted container is mounted, make a memory dump at first.

If the PC is turned on, but it locked by password, and this PC have FireWire interface, use cold-boot/FireWire attack to make memory dump.

If the PC is turned off and it in hibernate mode, then save the hibernate file, do not turn it on.

If the PC is turned off and do not have a hibernate file for analysis, use Forensic Disk Decryptor to prepare data for brute force attack.`

Step 2. Find OTFE keys

Use **Elcomsoft Forensic Disk Decryptor** to find and extract OTFE keys from memory dump

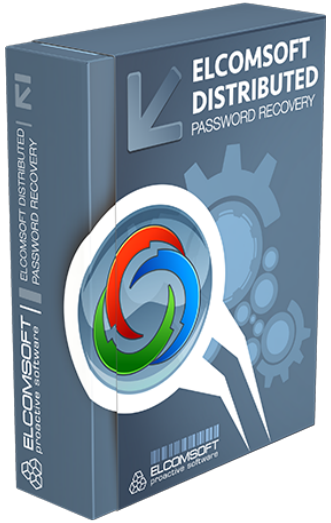
If no OTFE keys found, use **Elcomsoft Distributed Password Recovery** to find user password for encrypted container access

Step 3. Make analysis of encrypted container

Use **Elcomsoft Forensic Disk Decryptor** to mount or extract data from the encrypted container

Elcomsoft Distributed Password Recovery

Elcomsoft Distributed Password Recovery is a high-end solution for forensic and government agencies, data recovery and password recovery services and corporate users with multiple networked workstations connected over a LAN or the Internet.



https://www.elcomsoft.com/edpr.html

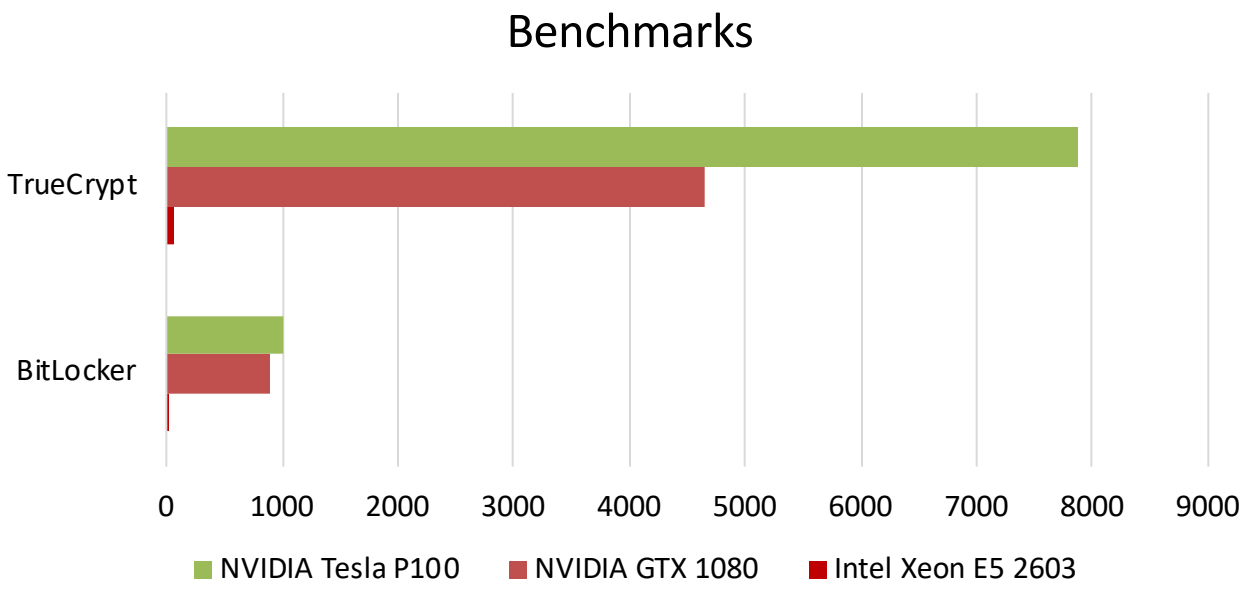
Why we recommend Elcomsoft Distributed Password Recovery

Elcomsoft Distributed Password Recovery allows for massively parallel operation, and **scales linearly to as many as 10,000 workstations**.

Elcomsoft Distributed Password Recovery employs a revolutionary, patented technology to **accelerate password recovery when a compatible NVIDIA or AMD graphics card** is present in addition to the CPU-only mode.

With Elcomsoft Distributed Password Recovery **supporting Amazon Cloud EC2 compute instances**, users can get as much speed as they need the moment they need.

Elcomsoft Distributed Password Recovery



Forensic analysis of crypto-containers

TrueCrypt, PGP disk, Bitlocker, FileVault

Andrey Malyshev, ElcomSoft s.r.o.

https://www.elcomsoft.com
Facebook: ElcomSoft
Twitter: @elcomsoft