Luke 8:17 - Misleading implementations that compromise the privacy and information security

ROGERIO WINTER

Agenda

- Luke 8:17
- Questions about theme
- Is the cryptography algorithm a problem?
- Loss and theft
- Bitdefender issues
- TrueCrypt issues
- Others cryptography softwares
- Bitlocker issues
- Conclusions

Presentation goals

- to show vulnerabilities in encryption software
- To present some impacts on cybersecurity
- To propose some mitigation actions

Luke 8: 17 – Bible citation

“For there is nothing hidden that will not be disclosed, and nothing concealed that will not be known or brought out into the open”

Ask about?

- I wonder if the CEO or CIO of company install his/her own crypto software?
- I wonder who install or configure crypto software?
- Paradigms of Cybersecurity: technology, people, process and environment.

Is the cryptography algorithm a problem?

- Clear mathematical foundation
- Large consumption of computer time
- Virtually impossible and uneconomical

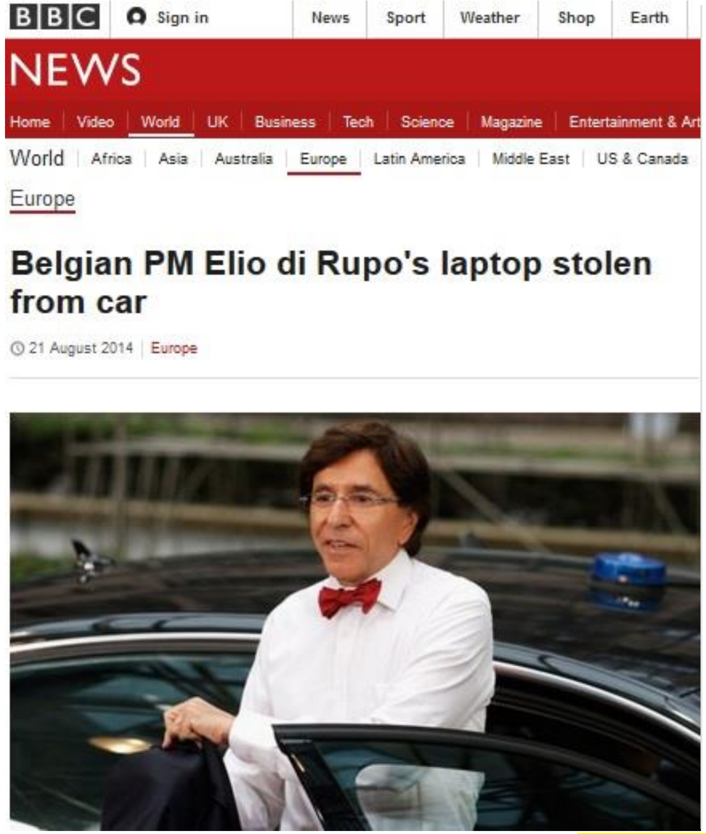
Where is the problem?

People, software implementation or process and environment

Where is the problem?

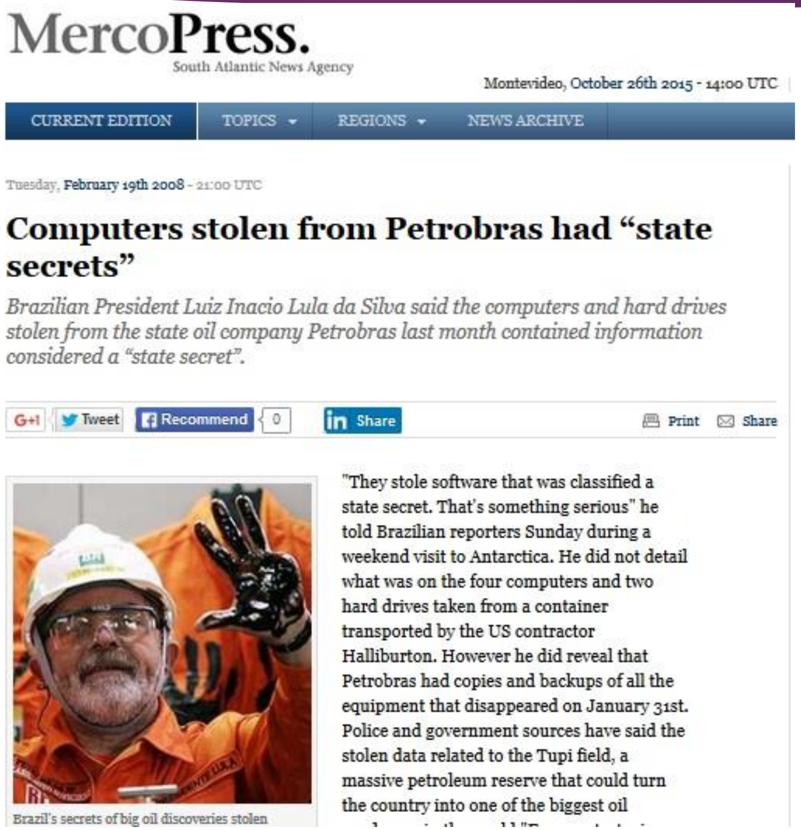
- algorithms are implemented in the software
- Software is a friendly user
- Manager, CEO, CIO are dependent of the technicians
- People are stolen or lose computers

Loss and theft


BBC Sign in News Sport Weather Shop Earth
NEWS
Home Video World UK Business Tech Science Magazine Entertainment & Art
World Africa Asia Australia Europe Latin America Middle East US & Canada
Europe

Belgian PM Elio di Rupo's laptop stolen from car

21 August 2014 | Europe


MercoPress.
South Atlantic News Agency
Montevideo, October 26th 2015 - 14:00 UTC
CURRENT EDITION TOPICS REGIONS NEWS ARCHIVE
G+1 Tweet Recommend 0 Share Print Share

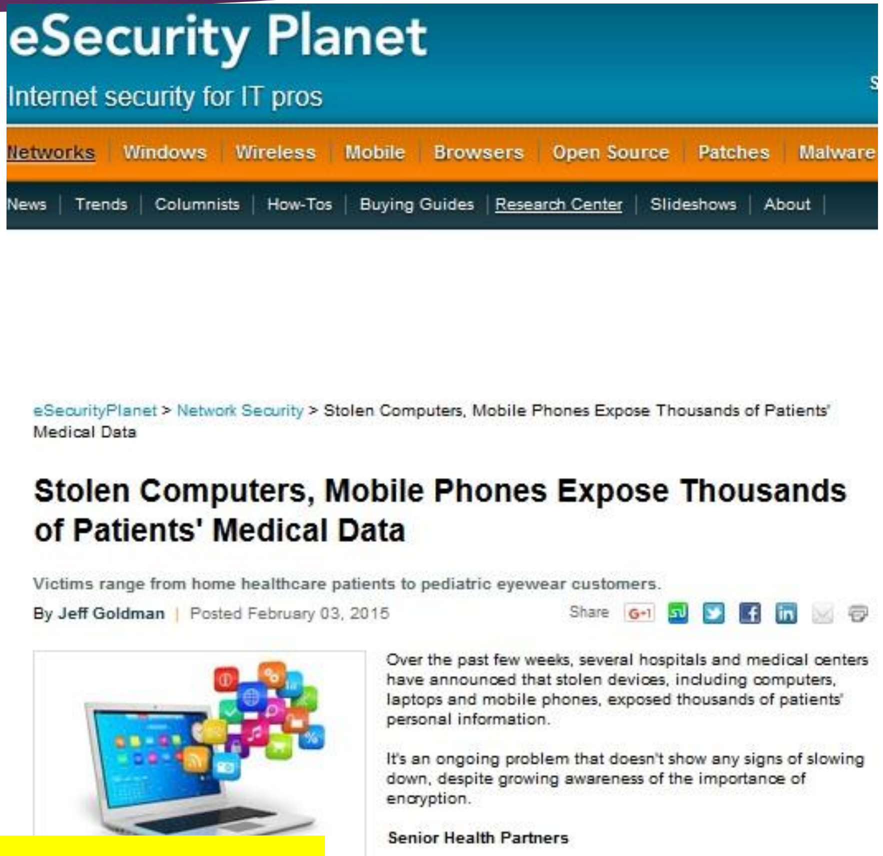
Tuesday, February 19th 2008 - 21:00 UTC

Computers stolen from Petrobras had “state secrets”

Brazilian President Luiz Inacio Lula da Silva said the computers and hard drives stolen from the state oil company Petrobras last month contained information considered a “state secret”.

Brazil's secrets of big oil discoveries stolen

"They stole software that was classified a state secret. That's something serious" he told Brazilian reporters Sunday during a weekend visit to Antarctica. He did not detail what was on the four computers and two hard drives taken from a container transported by the US contractor Halliburton. However he did reveal that Petrobras had copies and backups of all the equipment that disappeared on January 31st. Police and government sources have said the stolen data related to the Tupi field, a massive petroleum reserve that could turn the country into one of the biggest oil


eSecurity Planet
Internet security for IT pros
Networks Windows Wireless Mobile Browsers Open Source Patches Malware
News Trends Columnists How-Tos Buying Guides Research Center Slideshows About
Share

eSecurityPlanet > Network Security > Stolen Computers, Mobile Phones Expose Thousands of Patients' Medical Data

Stolen Computers, Mobile Phones Expose Thousands of Patients' Medical Data

Victims range from home healthcare patients to pediatric eyewear customers.

By Jeff Goldman | Posted February 03, 2015

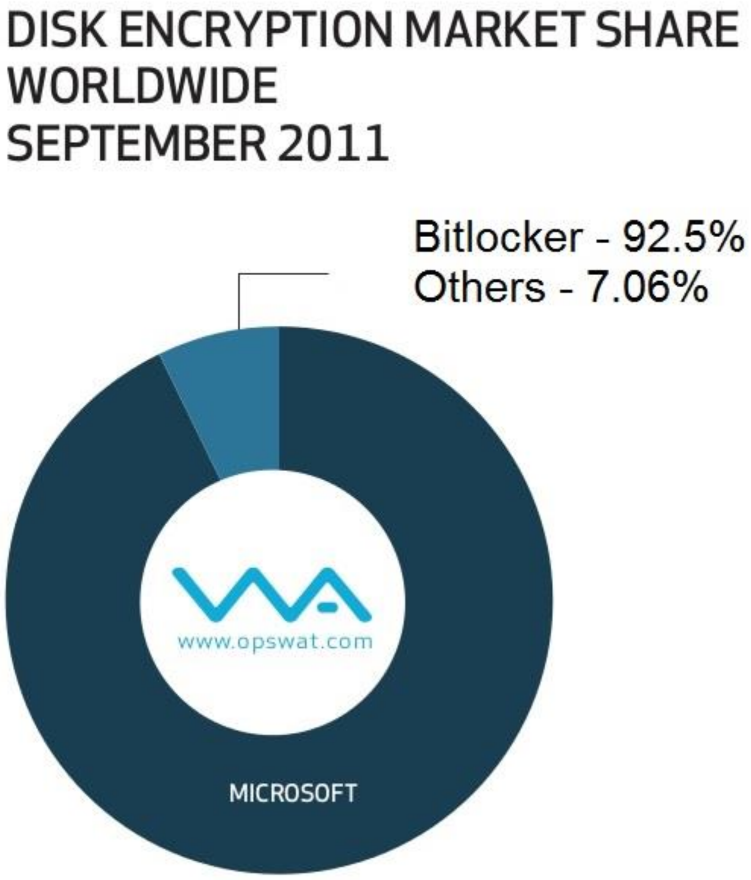
Over the past few weeks, several hospitals and medical centers have announced that stolen devices, including computers, laptops and mobile phones, exposed thousands of patients' personal information.

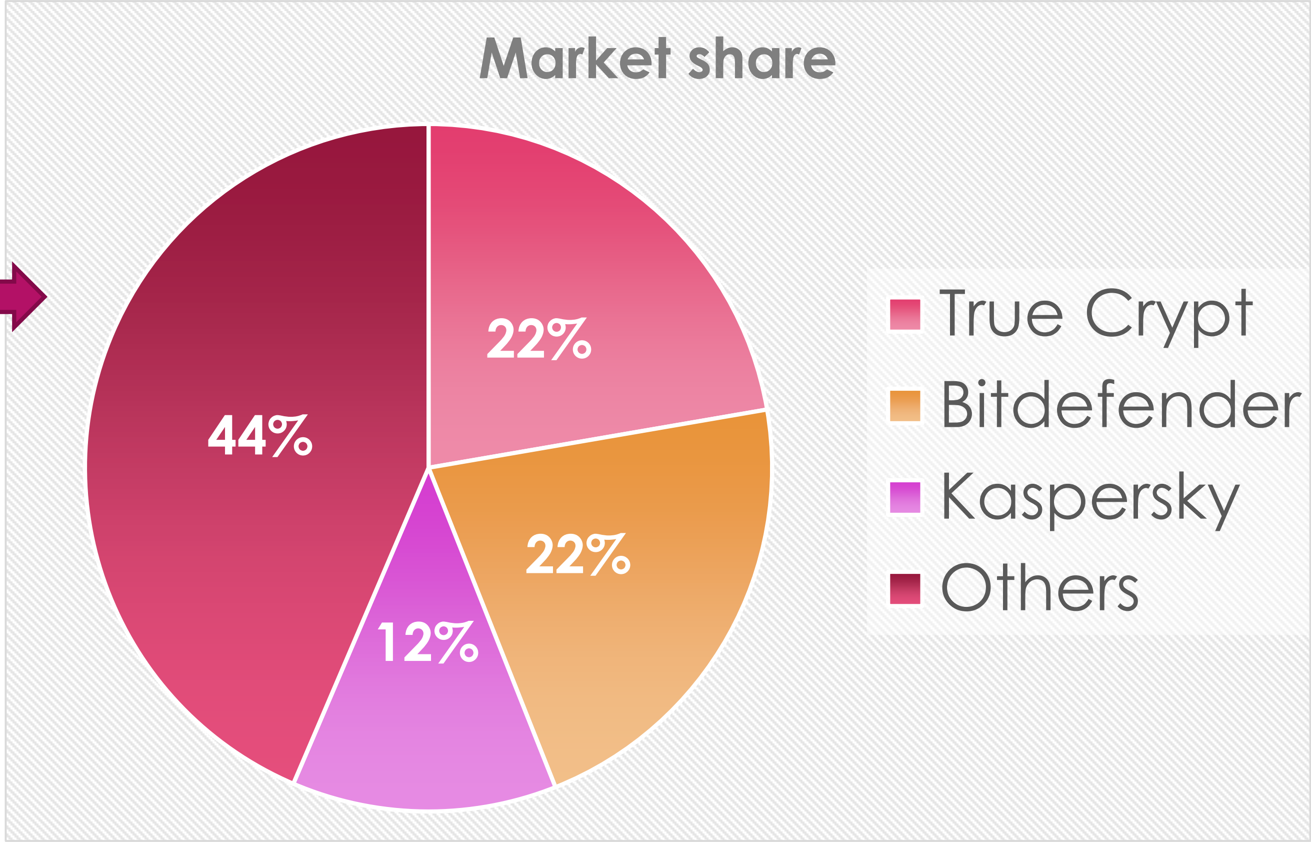
It's an ongoing problem that doesn't show any signs of slowing down, despite growing awareness of the importance of encryption.

Senior Health Partners

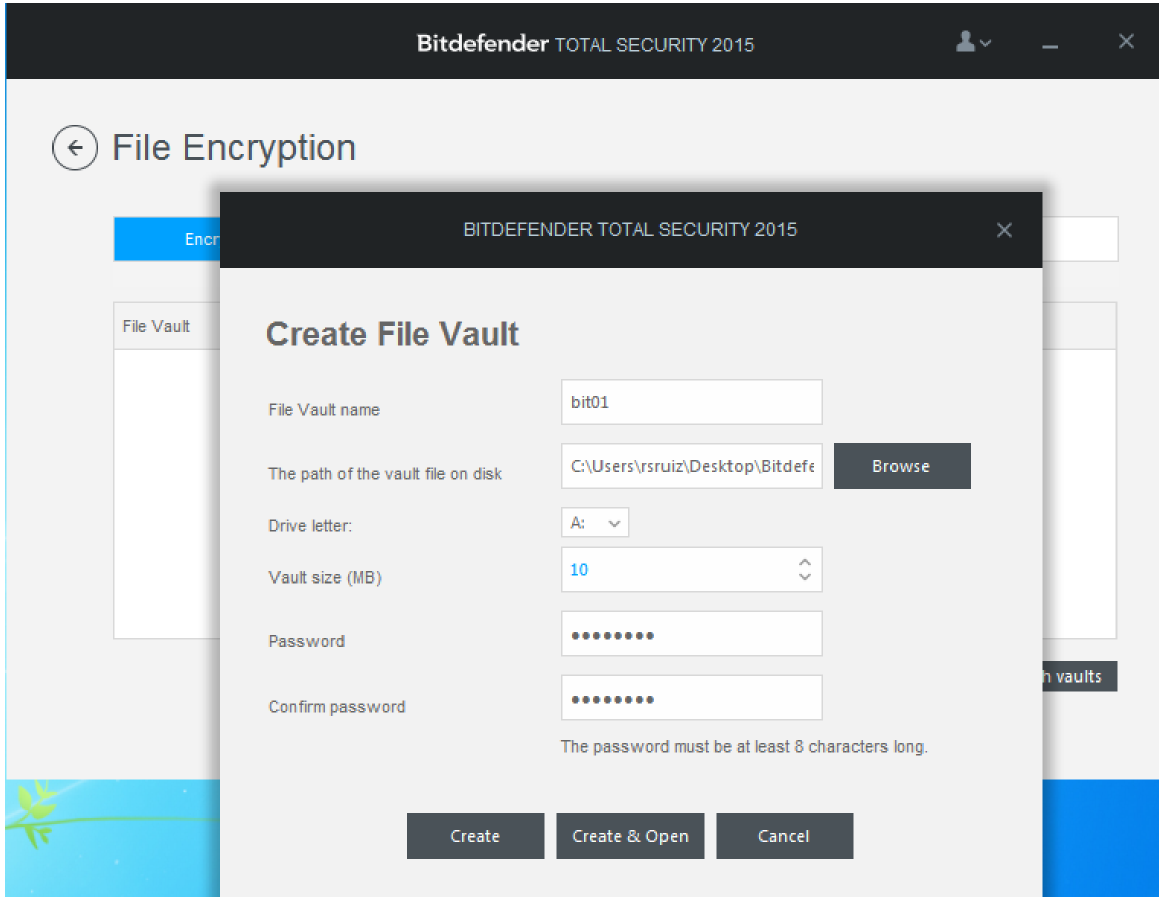
cost significantly ± US$115,000.

Disk Encryption - Market share





Bit Defender Total Encryption - Bitdefender


Bitdefender TOTAL SECURITY 2015
File Encryption
Encr
File Vault
vaults
BITDEFENDER TOTAL SECURITY 2015

Create File Vault

File Vault name: bit01

The path of the vault file on disk: C:\Users\rsruiz\Desktop\Bitdefe

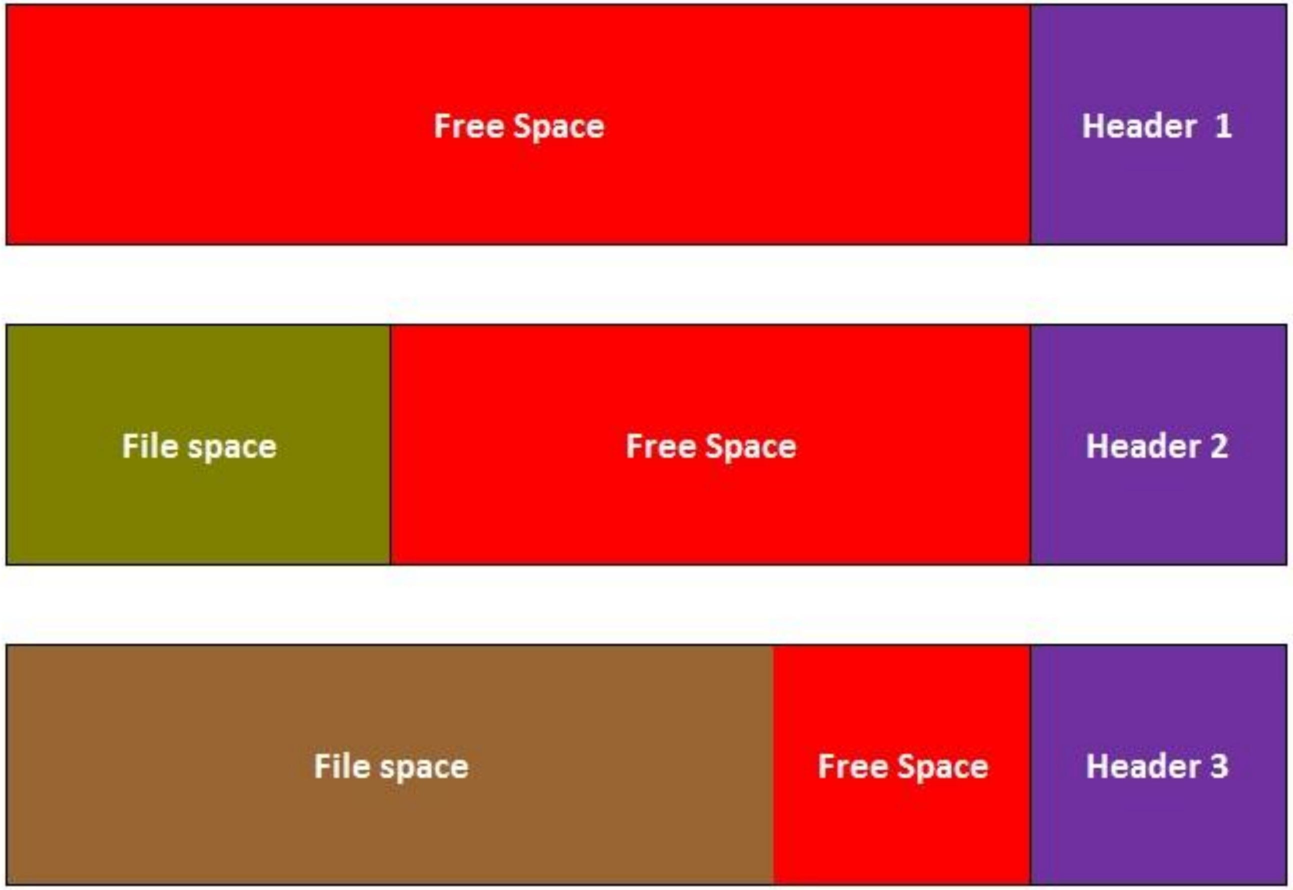
Drive letter: A:

Vault size (MB): 10

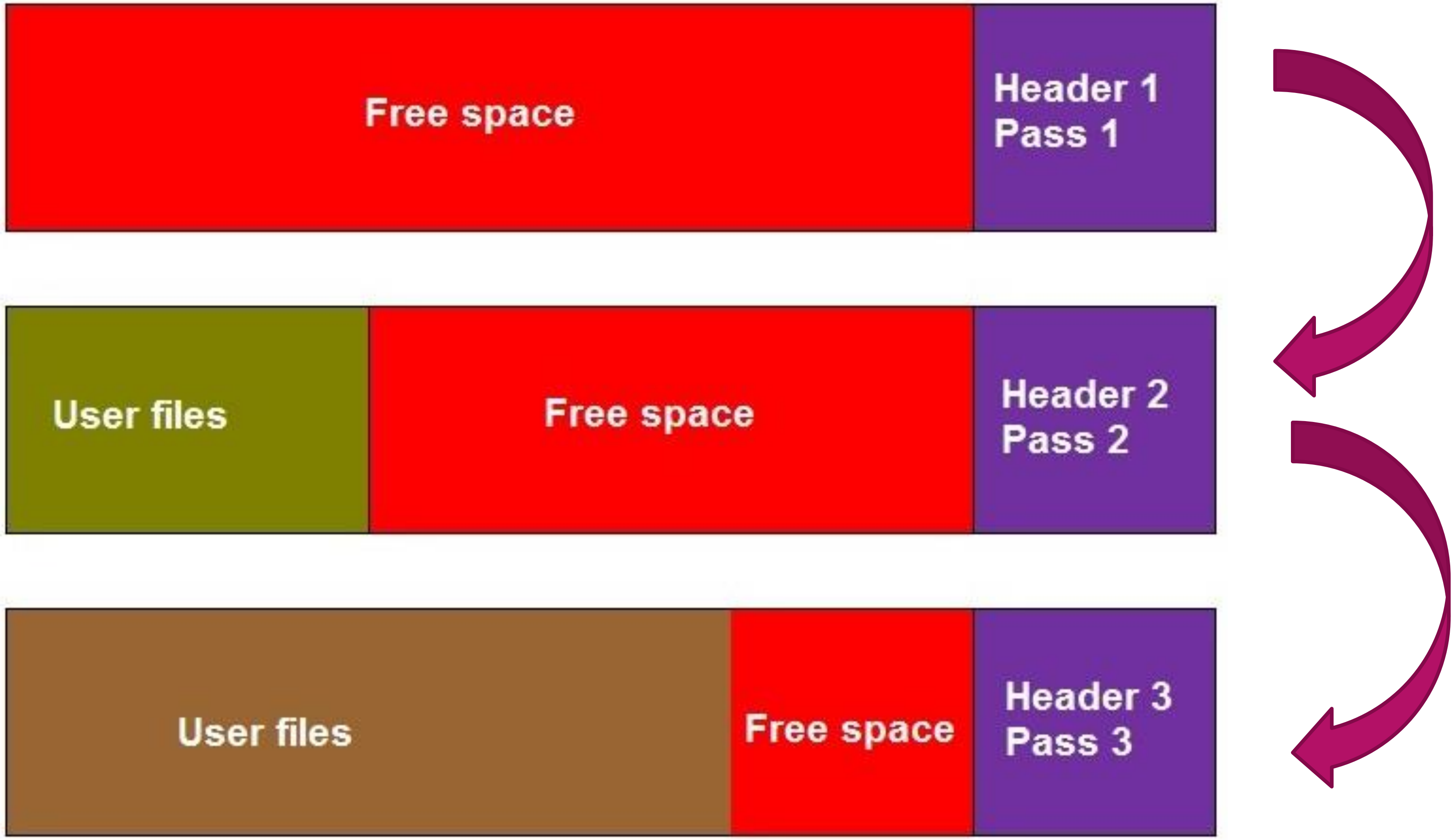
Password: ••••••••

Confirm password: ••••••••

The password must be at least 8 characters long.



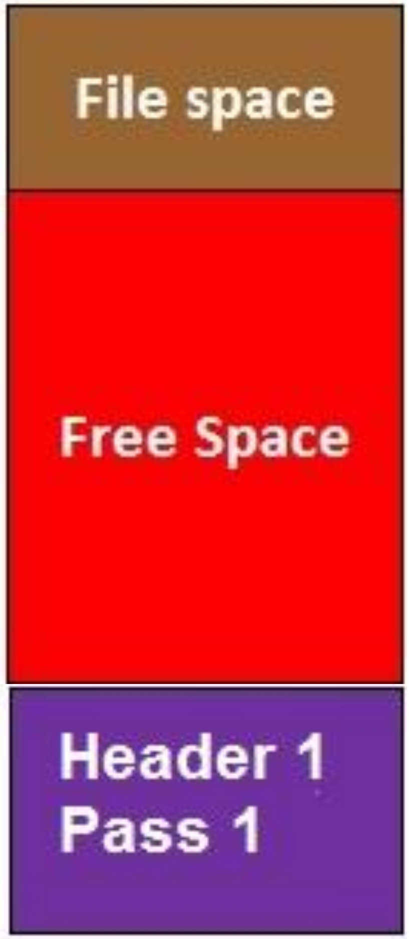
Bitdefender



Change password

Change password

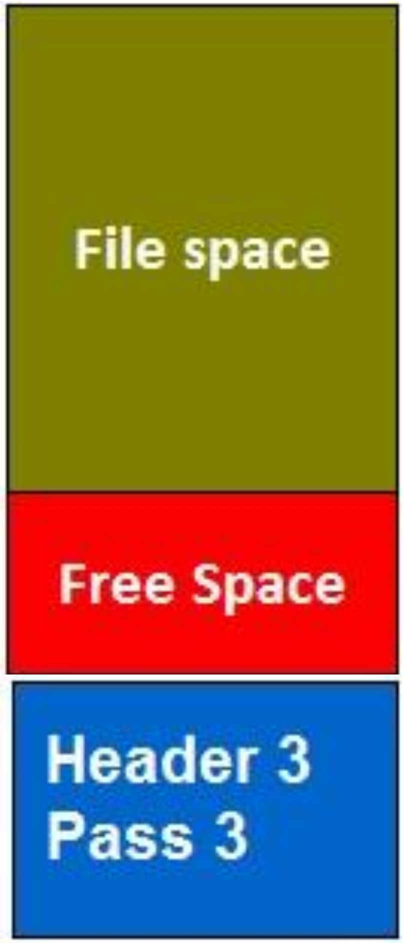
How can we achieve to open file?



File space

Free Space

Header 1
Pass 1

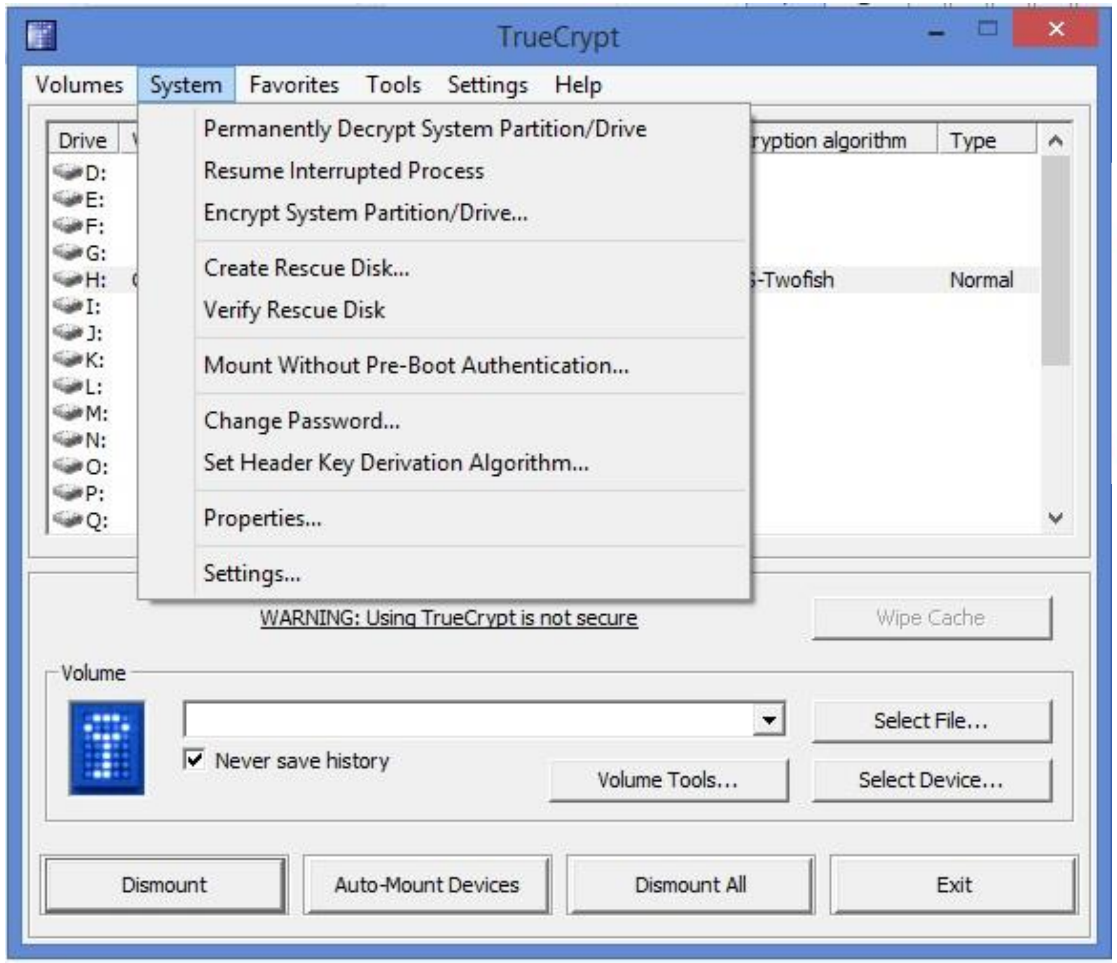


File space

Free Space

Header 3
Pass 3

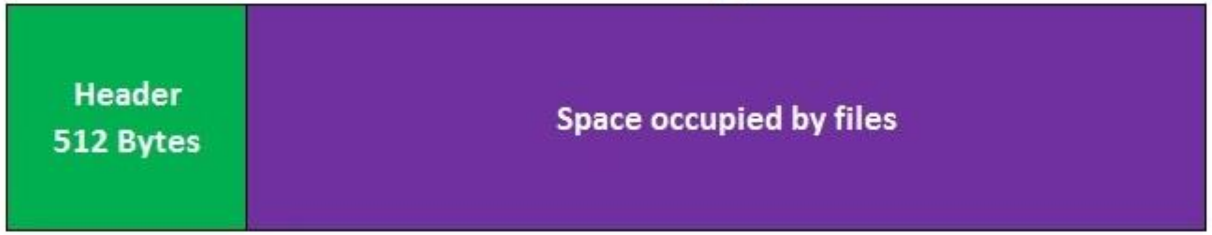
TrueCrypt



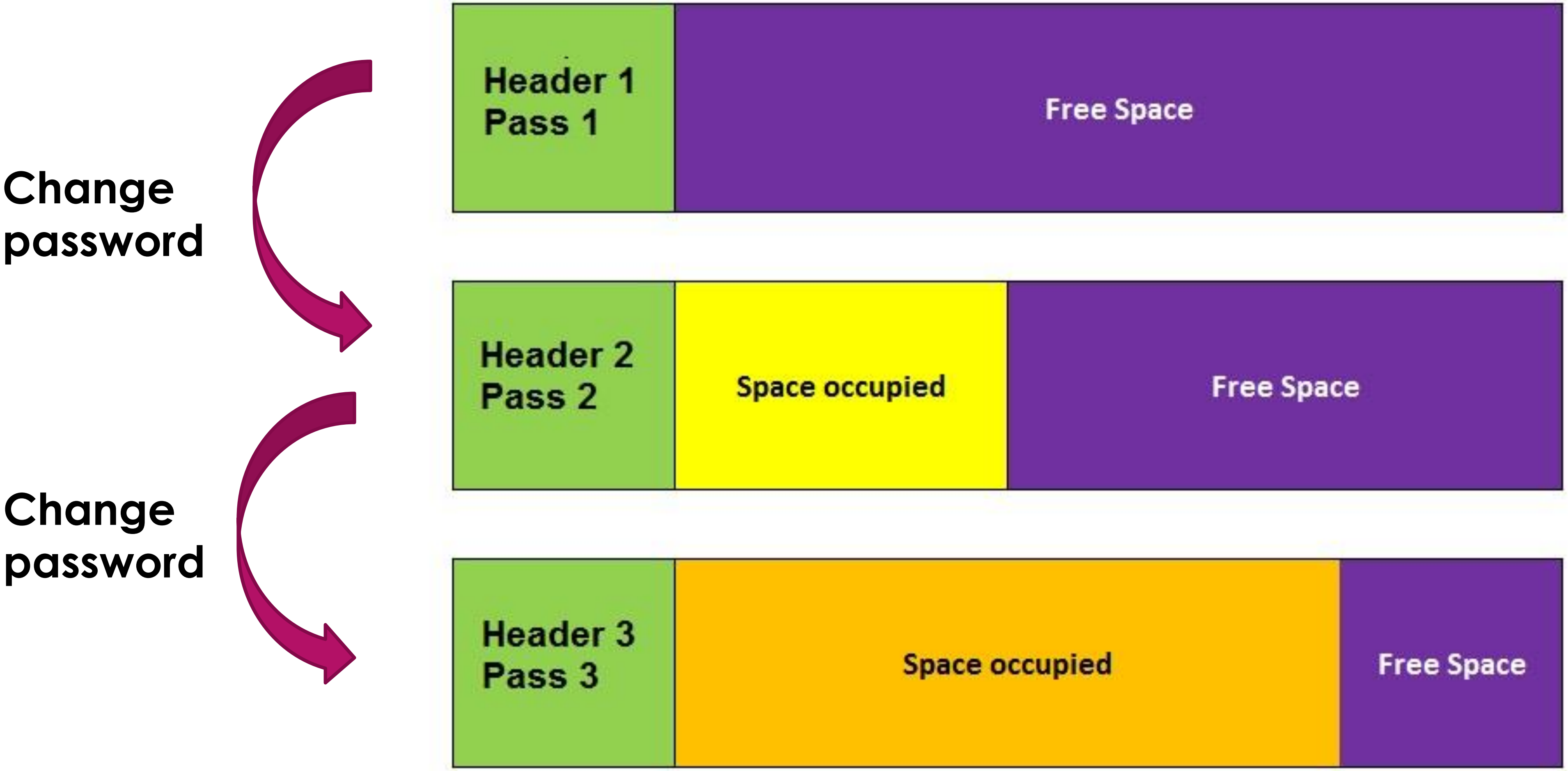
WARNING: Using TrueCrypt is not secure

☑ Never save history

A standard TrueCrypt volume



TrueCrypt



Change password

Change password

Header 1
Pass 1

Free Space

Header 2
Pass 2

Space occupied

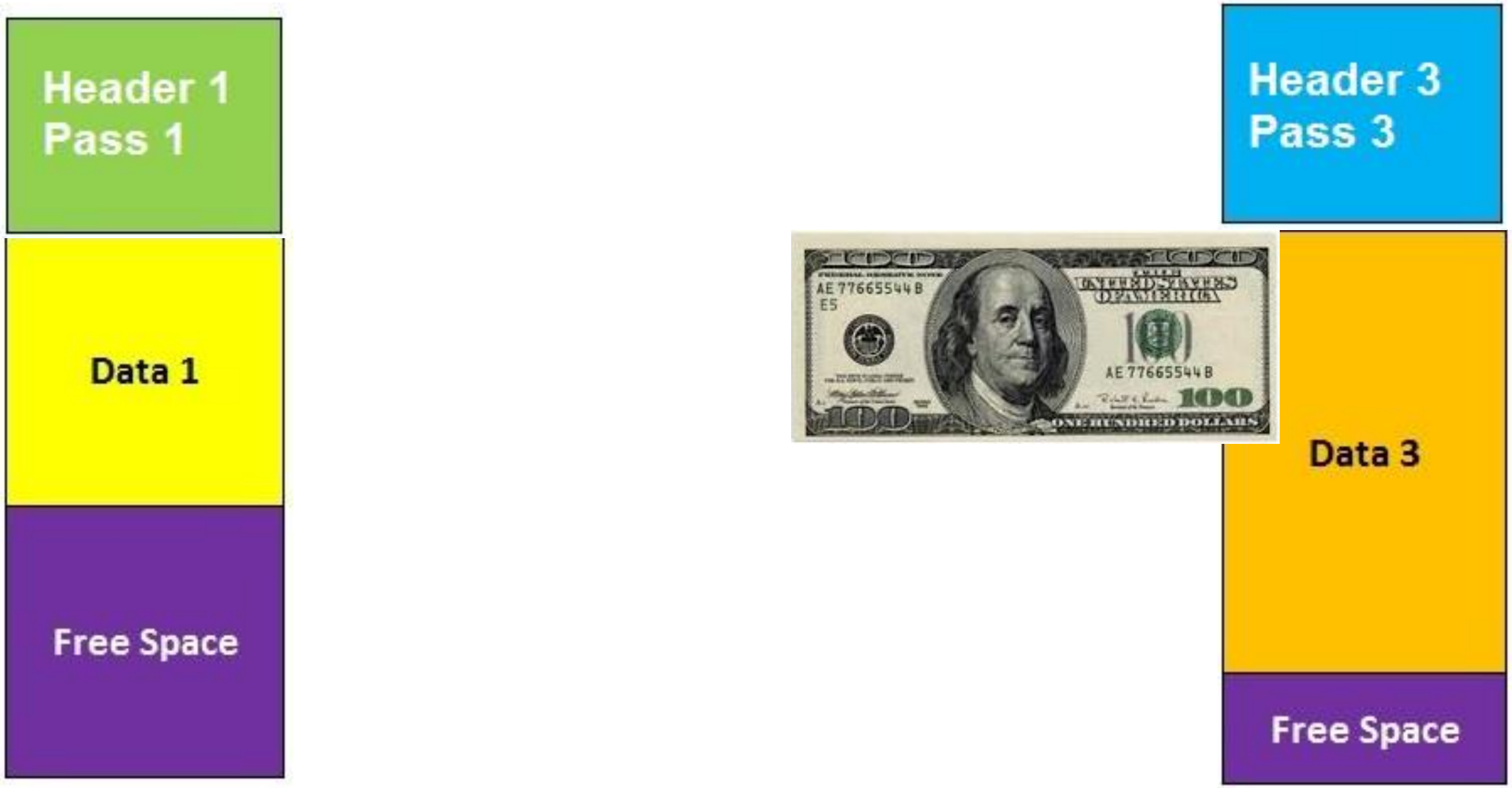
Free Space

Header 3
Pass 3

Space occupied

Free Space

How does this miracle occur?



Header 1
Pass 1

Data 1

Free Space

Header 3
Pass 3

Data 3

Free Space

CipherShed, VeraCrypt, TCNext, GostCrypt

CipherShed
Secure Encryption Software

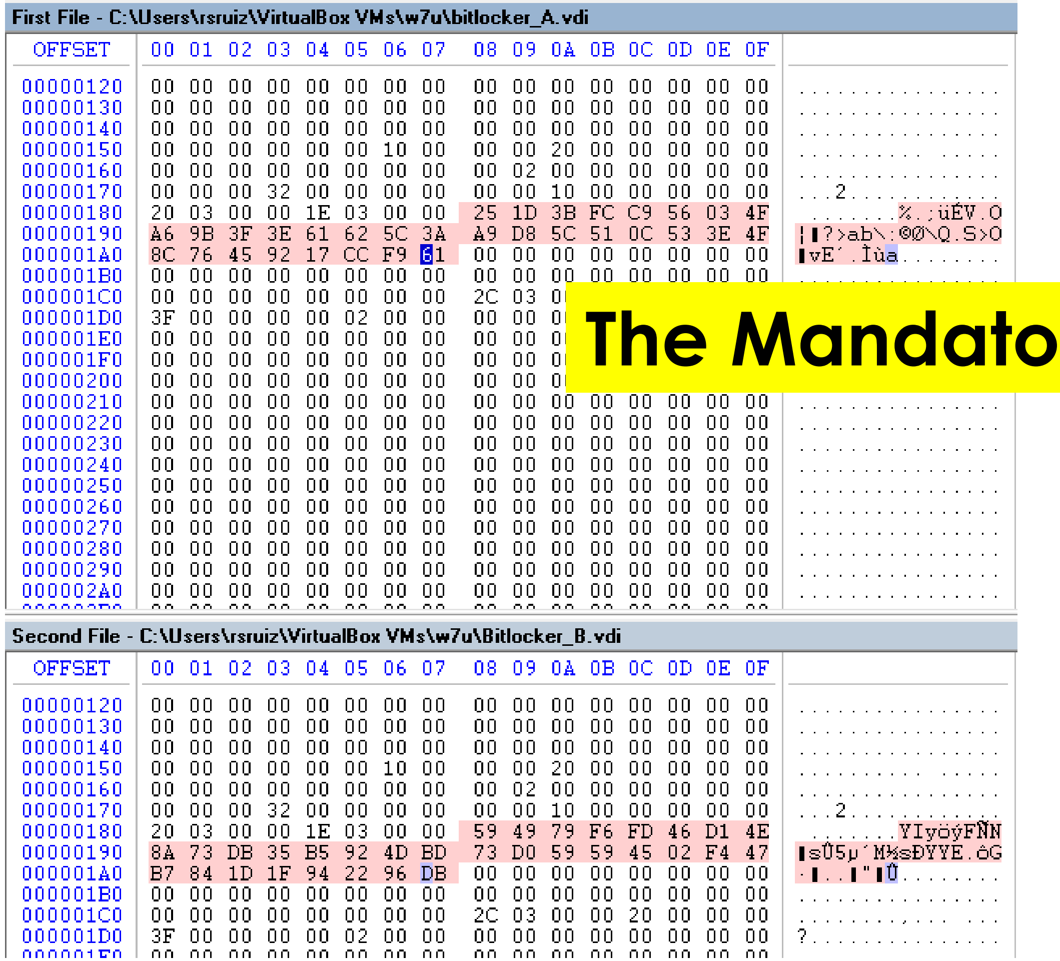
Vera
VeraCrypt

- **Same vulnerabilities exposed in TrueCrypt and BitDefender.**

TCnext

GOSTCRYPT

BitLocker - Microsoft



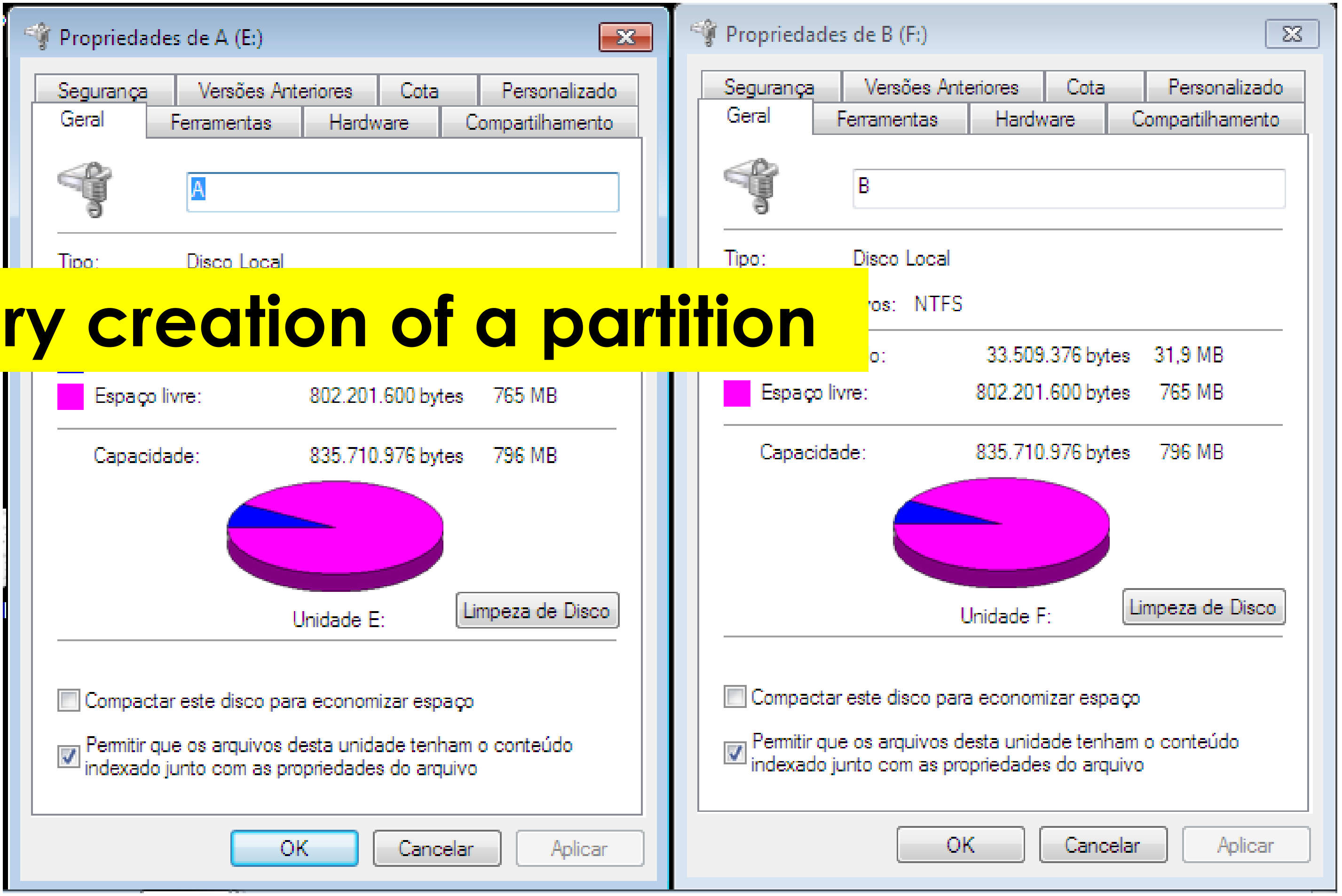
First File - C:\Users\rsruiz\VirtualBox VMs\w7u\bitlocker_A.vdi

```
 OFFSET    00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F

00000120   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000130   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000140   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000150   00 00 00 00 00 00 10 00  00 00 20 00 00 00 00 00   ................
00000160   00 00 00 00 00 00 00 00  00 02 00 00 00 00 00 00   ................
00000170   00 00 00 32 00 00 00 00  00 00 10 00 00 00 00 00   ...2............
00000180   20 03 00 00 1E 03 00 00  25 1D 3B FC C9 56 03 4F   ........%.;üÉV.O
00000190   A6 9B 3F 3E 61 62 5C 3A  A9 D8 5C 51 0C 53 3E 4F   ¦▌?>ab\:©Ø\Q.S>O
000001A0   8C 76 45 92 17 CC F9 61  00 00 00 00 00 00 00 00   ▌vE´.Ìùa........
000001B0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001C0   00 00 00 00 00 00 00 00  2C 03 0
000001D0   3F 00 00 00 00 02 00 00  00 00 0
000001E0   00 00 00 00 00 00 00 00  00 00 0
000001F0   00 00 00 00 00 00 00 00  00 00 0
00000200   00 00 00 00 00 00 00 00  00 00 0
00000210   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000220   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000230   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000240   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000250   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000260   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000270   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000280   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000290   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
000002A0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
```

Second File - C:\Users\rsruiz\VirtualBox VMs\w7u\Bitlocker_B.vdi

```
 OFFSET    00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F

00000120   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000130   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000140   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000150   00 00 00 00 00 00 10 00  00 00 20 00 00 00 00 00   ................
00000160   00 00 00 00 00 00 00 00  00 02 00 00 00 00 00 00   ................
00000170   00 00 00 32 00 00 00 00  00 00 10 00 00 00 00 00   ...2............
00000180   20 03 00 00 1E 03 00 00  59 49 79 F6 FD 46 D1 4E   ........YIyöýFÑN
00000190   8A 73 DB 35 B5 92 4D BD  73 D0 59 59 45 02 F4 47   ▌sÛ5µ´M½sÐYYE.ôG
000001A0   B7 84 1D 1F 94 22 96 DB  00 00 00 00 00 00 00 00   ·▌..▌"▌Û........
000001B0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
000001C0   00 00 00 00 00 00 00 00  2C 03 00 00 20 00 00 00   ........,... ...
000001D0   3F 00 00 00 00 02 00 00  00 00 00 00 00 00 00 00   ?...............
```

The Mandatory creation of a partition



Propriedades de A (E:)

Segurança | Versões Anteriores | Cota | Personalizado
Geral | Ferramentas | Hardware | Compartilhamento

A

Tipo: Disco Local

Espaço livre: 802.201.600 bytes 765 MB

Capacidade: 835.710.976 bytes 796 MB

Unidade E:

☐ Compactar este disco para economizar espaço

☑ Permitir que os arquivos desta unidade tenham o conteúdo indexado junto com as propriedades do arquivo

Propriedades de B (F:)

Segurança | Versões Anteriores | Cota | Personalizado
Geral | Ferramentas | Hardware | Compartilhamento

B

Tipo: Disco Local

os: NTFS

o: 33.509.376 bytes 31,9 MB

Espaço livre: 802.201.600 bytes 765 MB

Capacidade: 835.710.976 bytes 796 MB

Unidade F:

☐ Compactar este disco para economizar espaço

☑ Permitir que os arquivos desta unidade tenham o conteúdo indexado junto com as propriedades do arquivo

BitLocker - Microsoft

- Password - 100 characters including all characters of the ASCII table – 100^95
- one recovery key 48 digits (0-9) - 10^48
- Some recovery key, independent of changes
- **100^95 >> 10^48**

A final weakness of Bitlocker lies in their implementation

Microsoft – LM Hash

$$95^{14} \approx 2^{92} \quad \longrightarrow \quad 69^{7} \approx 2^{43}$$

A final weakness of LM hashes lies in their implementation

My advice

- Use TrueCrypt, Bitdefender, CipherShed, VeraCrypt, TCNext, and GostCrypt carefully. Do-it-yourself password when you create the container
- In Bitlocker, the strength of your password is limited to 48 numerical characters

Conclusions

- software are implemented insecurely
- open , free or paid softwares have a similar problems
- Information security cannot be based solely on advertising
- We need to improve our software test

Thank you so much

- My contacts
  - **rogwinter@gmail.com**
  - **Twitter: @rogwinter**
  - **Linkedin**
  - **www.facebook.com/apocalypseantivirus**