A Quick Look at Data Encryption

What is Encryption?

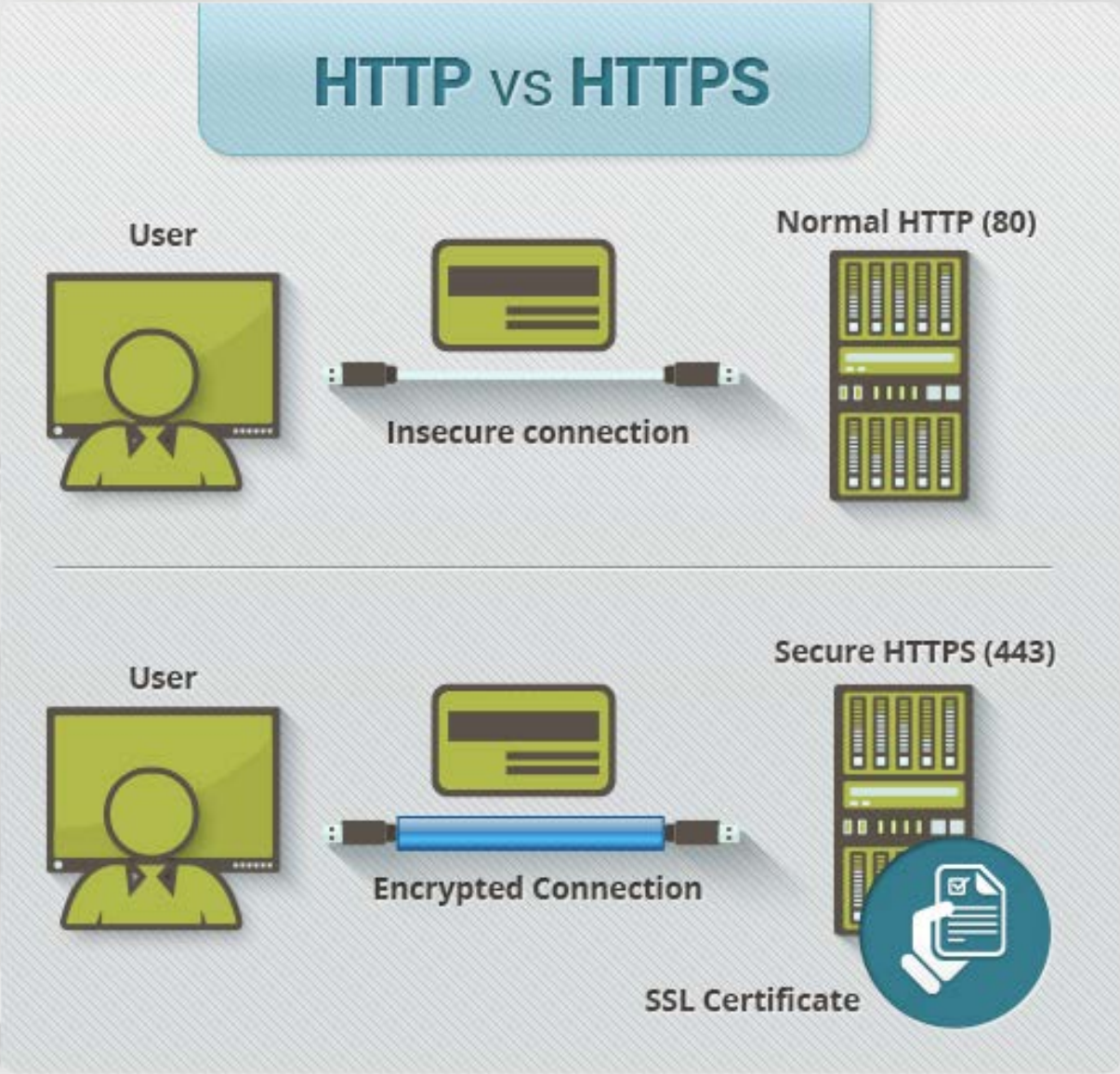
Encryption is one specific element of cryptography in which one hides data or information by transforming it into an undecipherable code.

Historical Examples

Jefferson Wheel Cipher (1700's)

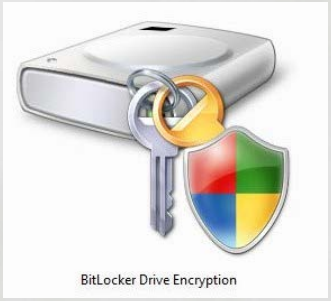
The Enigma Machine (1933-1945)

Everyday Encryption



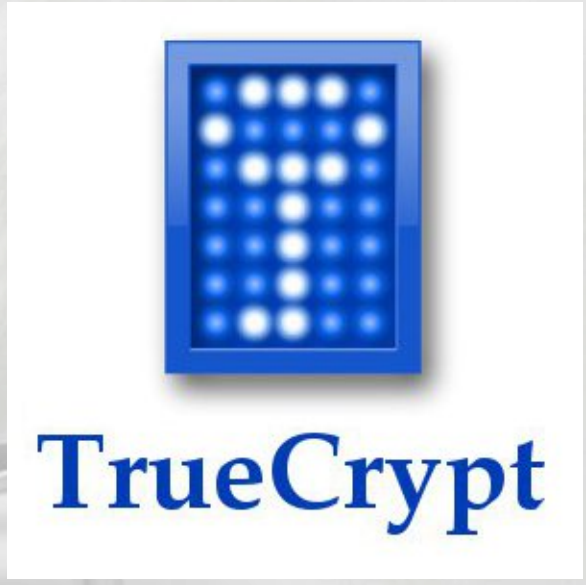
Operating Systems

- BitLocker Encryption
- File Vault 2

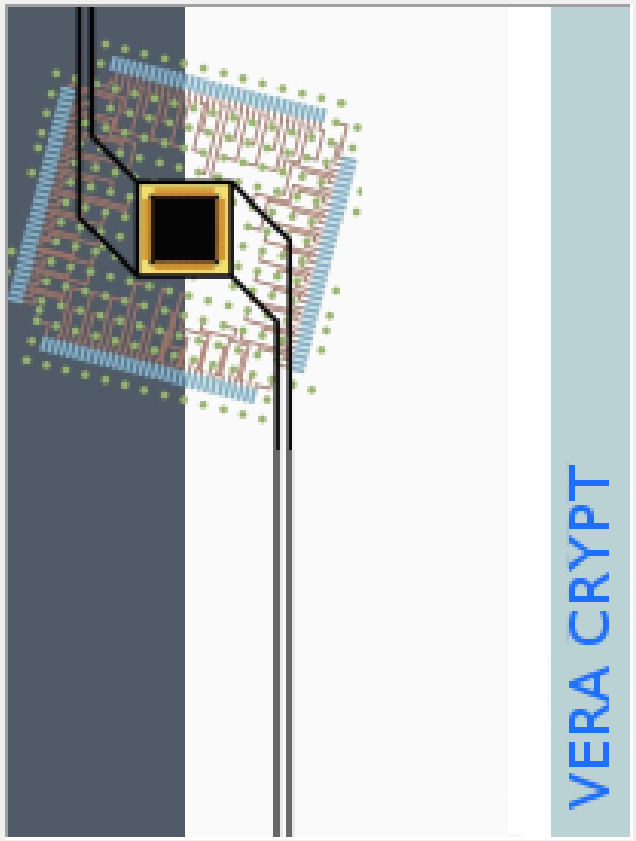


Both Allow Encryption of Removeable Media

Free Encryption Programs



VeraCrypt Volume Creation Wizard



VeraCrypt Volume Creation Wizard

- **Create an encrypted file container**

  Creates a virtual encrypted disk within a file. Recommended for inexperienced users.

  More information

- **Encrypt a non-system partition/drive**

  Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.

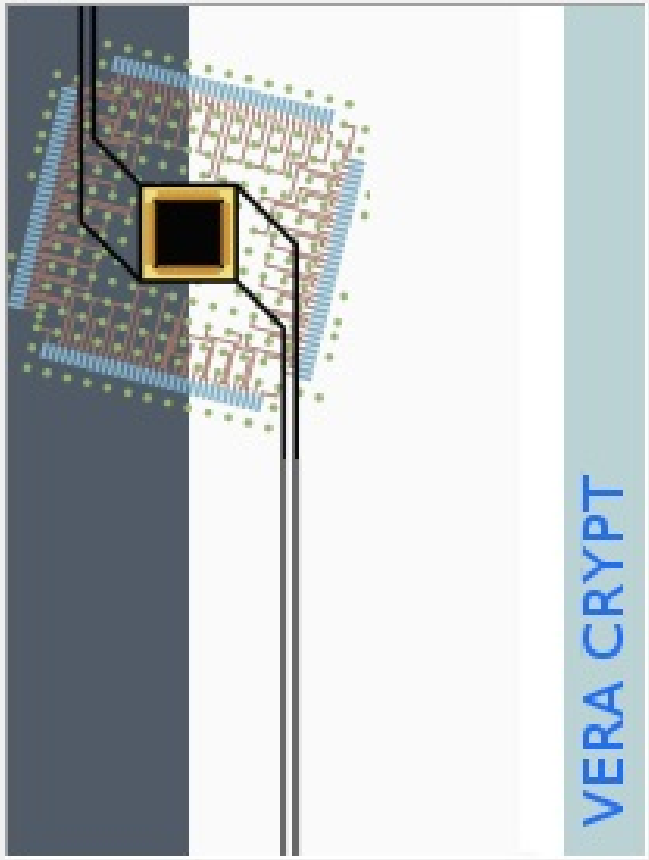
- **Encrypt the system partition or entire system drive**

  Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots. Optionally, creates a hidden system.

  More information about system encryption

Help | < Back | Next > | Cancel

VeraCrypt Volume Creation Wizard



Outer Volume Password

Password: ••••••••••

PKCS-5 PRF: Autodetection

☐ Use PIM

☐ Display password

☐ Use keyfiles

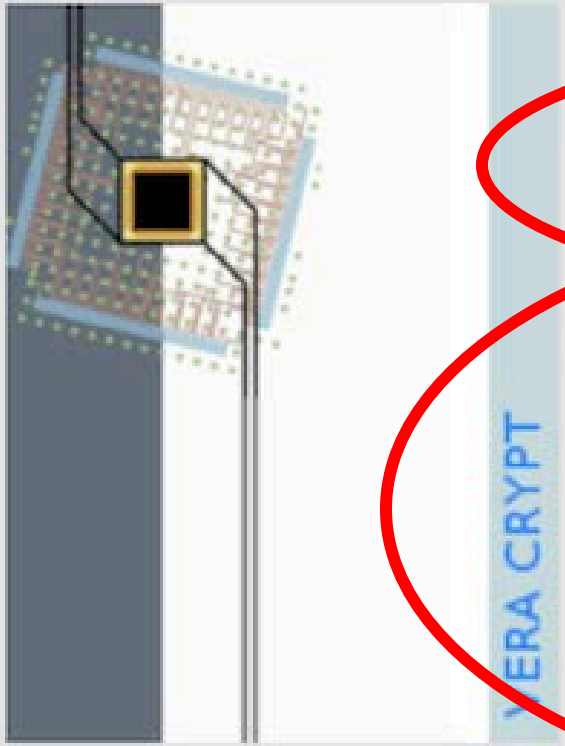
Keyfiles...

Please enter the password for the volume within which you wish to create a hidden volume.

After you click Next, VeraCrypt will attempt to mount the volume. As soon as the volume is mounted, its cluster bitmap will be scanned to determine the size of the uninterrupted area of free space (if there is any) whose end is aligned with the end of the volume. This area will accommodate the hidden volume and therefore will limit its maximum possible size. Cluster map scanning is necessary to ensure that no data on the outer volume will be overwritten by the hidden volume.

Help | < Back | Next > | Cancel

VeraCrypt Volume Creation Wizard



Volume Type

Standard VeraCrypt volume

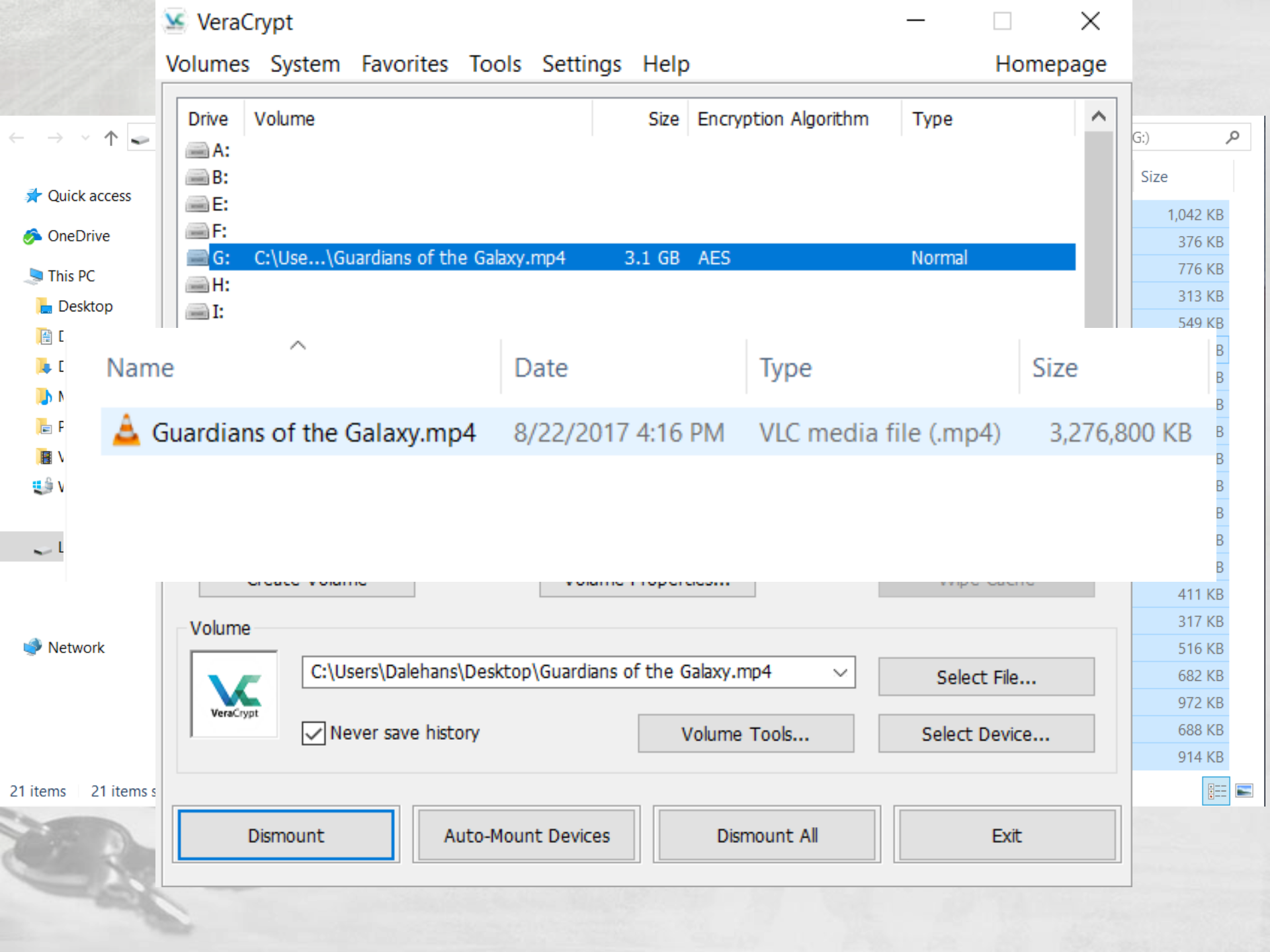
Select this option if you want to create a normal VeraCrypt volume.

Hidden VeraCrypt volume

It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.

More information about hidden volumes

? < Prev Next > Cancel


VeraCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption Algorithm Type
A:
B:
E:
F:
G: C:\Use...\Guardians of the Galaxy.mp4 3.1 GB AES Normal
H:
I:
Name Date Type Size
Guardians of the Galaxy.mp4 8/22/2017 4:16 PM VLC media file (.mp4) 3,276,800 KB
Volume
C:\Users\Dalehans\Desktop\Guardians of the Galaxy.mp4
Select File...
Never save history
Volume Tools...
Select Device...
Dismount
Auto-Mount Devices
Dismount All
Exit
Quick access
OneDrive
This PC
Desktop
Network
21 items
Size
1,042 KB
376 KB
776 KB
313 KB
549 KB
411 KB
317 KB
516 KB
682 KB
972 KB
688 KB
914 KB

Guessing the Password?

A 20 character password made up of:

- 6 Upper Case Letters
- 6 Lower Case Letters
- 4 Numbers
- 4 Special Characters

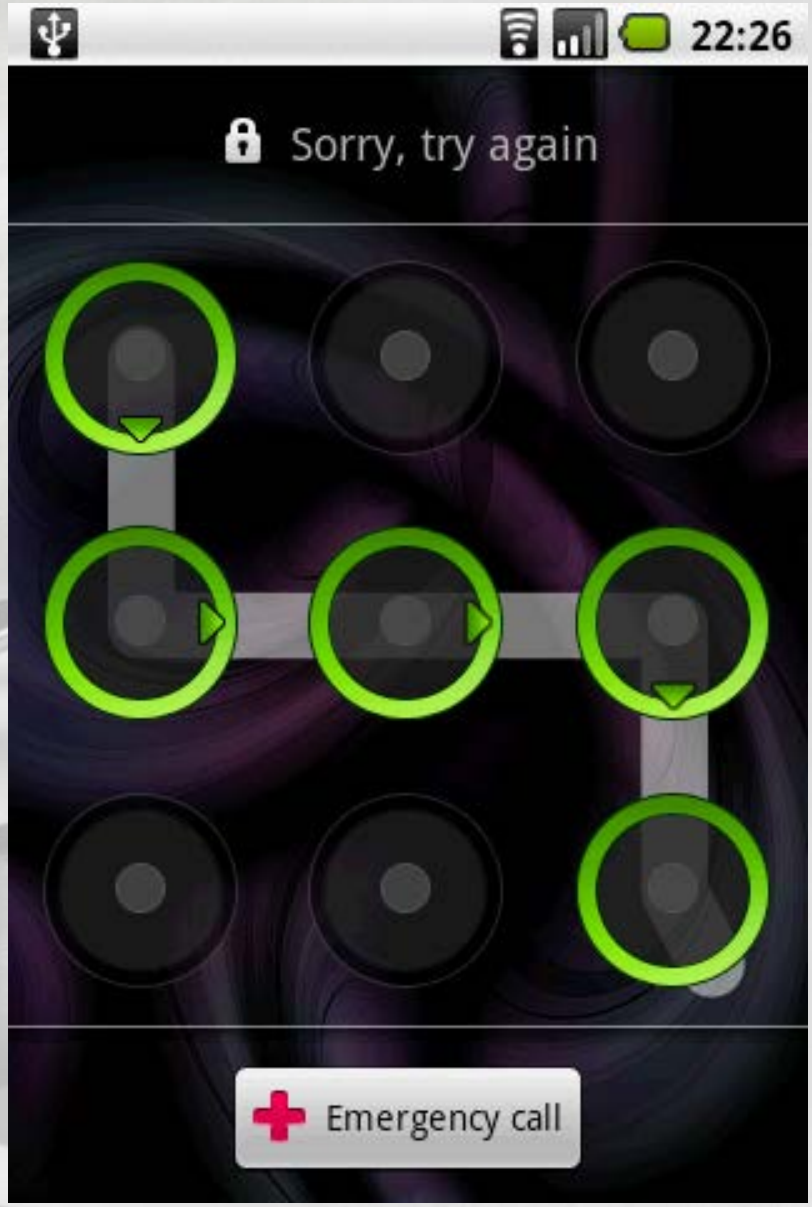
Truecrypt/ Veracrypt Recommends a 20 character password

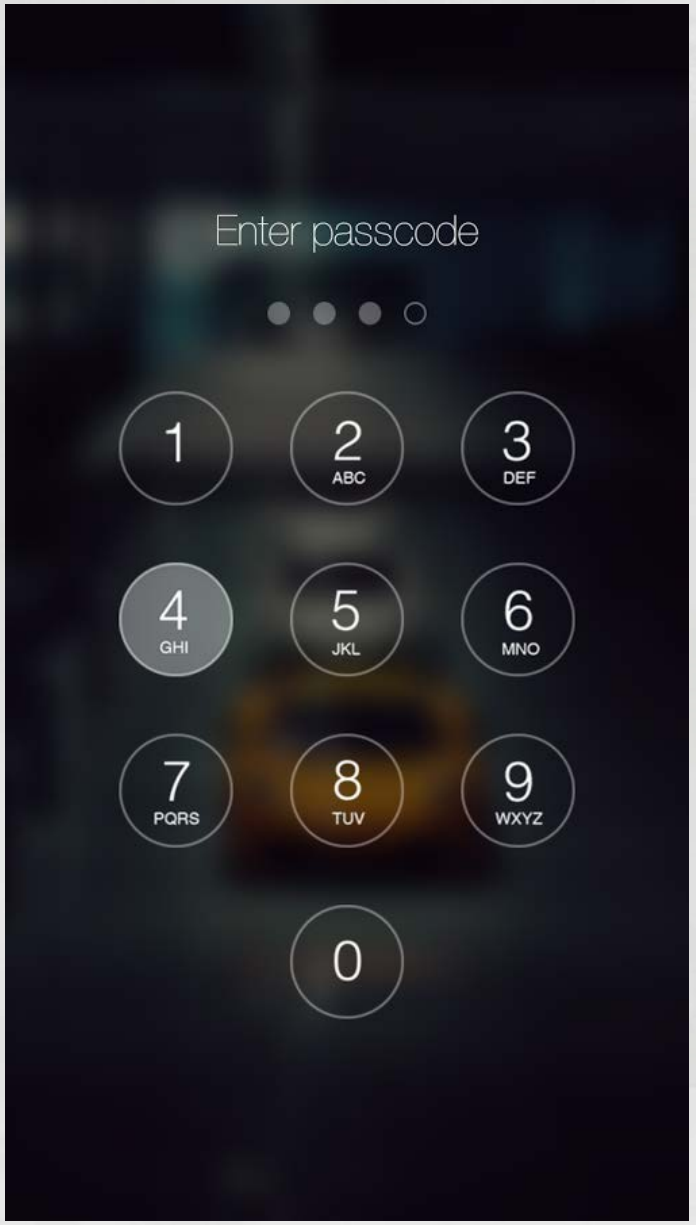
There would be over one octillion combinations.

It would take 1,000 high end computers working in parallel to crack 1,000,000,000,000,000,000,000,000 combinations.

29,122,606,403,101,200.00 Hours

Cellular Phones


22:26
Sorry, try again
Emergency call


Enter passcode
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0

Encrypting

Wait while your phone is being encrypted. 8% complete.

iOS 8

Great OS. Great design.
Now in color.

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

IN THE MATTER OF THE SEARCH OF AN APPLE IPHONE SEIZED DURING THE EXECUTION OF A SEARCH WARRANT ON A BLACK LEXUS IS300, CALIFORNIA LICENSE PLATE 35KGD203	No. ED 15-0451M ~~[PROPOSED~~] ORDER COMPELLING APPLE, INC. TO ASSIST AGENTS IN SEARCH

This matter is before the Court pursuant to an application pursuant to the All Writs Act, 28 U.S.C. § 1651, by Assistant United States Attorneys Tracy Wilkison and Allen Chiu, requesting an order directing Apple Inc. ("Apple") to assist law enforcement agents in enabling the search of a digital device seized in the course of a previously issued search warrant in this matter.

For good cause shown, IT IS HEREBY ORDERED that:

1. Apple shall assist in enabling the search of a cellular telephone, Apple make: iPhone 5C, Model: A1532, P/N:MGFG2LL/A, S/N:FFMNQ3MTG2DJ, IMEI:358820052301412, on the Verizon Network, (the

FBI confirms it won't tell Apple how it hacked San Bernardino shooter's iPhone

Bureau will not tell Apple about the security flaw it exploited to break into the iPhone 5C, in part because it didn't buy the rights to the technical details

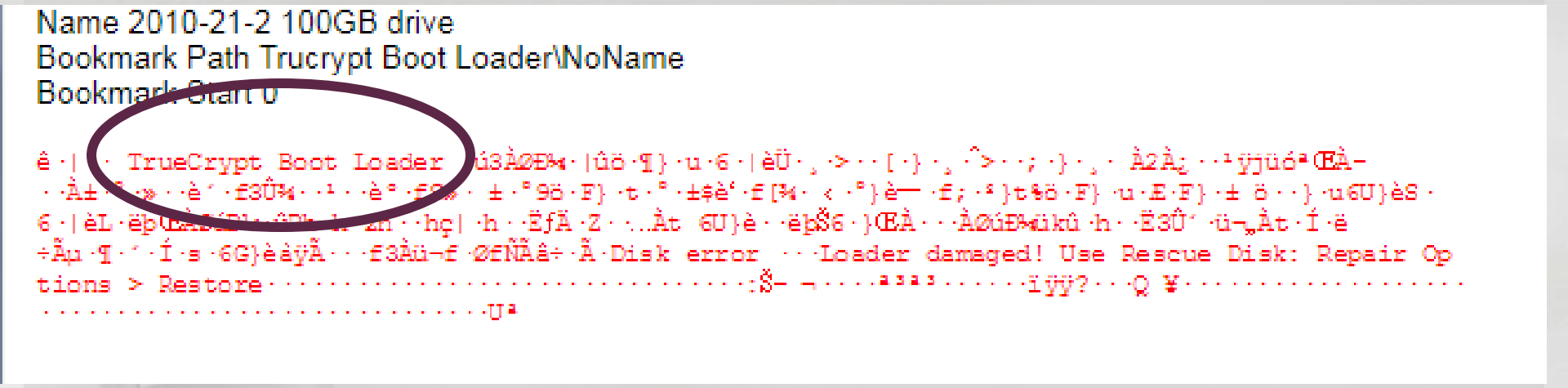
The FBI has offered few details about the hacking tool is paid more than $1m for. Photograph:

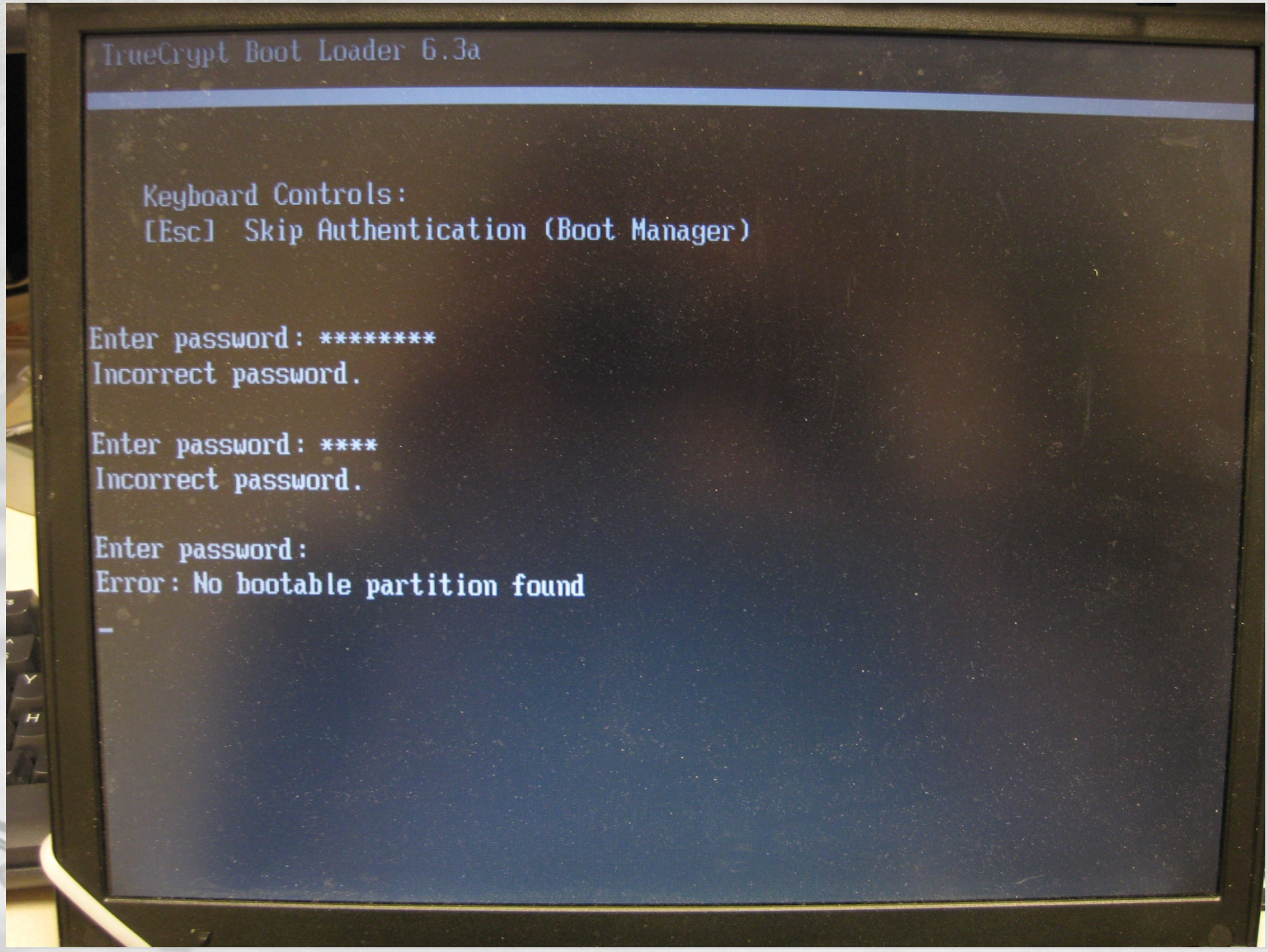
Child Pornography Search Warrant


IBM
T42


ASM P/N39T2584
FRU P/N39T2585
7200RPM 100 0GB
P39T2584
HITACHI
www.hitachigst.com
N13508 E182115 T
LES
RoHS D33373 04-5135(B)
MODEL:HTS721010G9AT00 7200RPM
5V 1.1A DC 100GB ATA/IDE
MADE IN THAILAND BY Hitachi Global
Storage Technologies(Thailand).Ltd. TD
WARRANTY VOID IF ANY LABEL/
SCREW IS REMOVED OR BROKEN 21SEP07
Lenovo P/N:39T2562 (HITACHI P/N:0A26567)
MLC:DA1949
(16383CYL. 16HEADS. 63SEC/T)
195.371.568 LBA'S
11S39T2562Z1ZCYG000JS2
B/A5CA A/B
Don't shock/
push cover
DO NOT COVER
THIS HOLE ⇒
< JUMPER >
DEVICE0
DEVICE1
CABLE SEL.

Name 2010-21-2 100GB drive
Bookmark Path Trucrypt Boot Loader\NoName
Bookmark Start 0




TrueCrypt Boot Loader 6.3a
Keyboard Controls:
[Esc] Skip Authentication (Boot Manager)
Enter password: ********
Incorrect password.
Enter password: ****
Incorrect password.
Enter password:
Error: No bootable partition found


Microsoft
ROOT BEER

Court Ordered Password Disclosure

Should ex-Philly cop suspected of sharing child porn be forced to divulge computer passwords?

Updated: SEPTEMBER 8, 2016 — 1:09 AM EDT

Francis Rawls, a former Philadelphia police sergeant, has been in custody for nearly a year in contempt of court for failing to unlock his encrypted electronic devices.

3rd Circuit Affirms Contempt Judgment For Refusal To Decrypt Devices

Mealey's (March 23, 2017, 10:43 AM EDT) -- PHILADELPHIA — A child pornography suspect was correctly found to be in contempt when he refused to comply with a court order requiring him to provide law enforcement with access to external hard drives, a Third Circuit U.S. Court of Appeals panel ruled March 20, finding that the defendant's rights under the Fifth Amendment to the U.S. Constitution were not violated (United States of America v. Apple Mac Pro Computer, et al., No. 15-3537, 3rd Cir.; 2017 U.S. App. LEXIS 4874). (Opinion available. Document #24-170420-003Z.)

Encrypted Devices

In 2015, the criminal investigations unit of Delaware County, Pa., was investigating Francis Rawls' access to child pornography. While searching Rawls' home, officers seized an Apple Mac Pro computer, an Apple iPhone and two Western Digital external hard drives. All of the devices were protected with encryption software.

Department of Homeland Security (DHS) agents obtained a search warrant to examine the devices. Rawls voluntarily provided his iPhone password. DHS analysts decrypted the Mac Pro. Rawls refused to provide passwords for the external hard drives. The government was unable to unlock the hard drives but in examining the Mac Pro found evidence that child porn images had been downloaded and saved on the hard drives.

Contact Information

Officer Dale Hanson

dale.hanson@minneapolismn.gov

Minneapolis Police Crime Lab

Phone: 612-673-2716