МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И. ВЕРНАДСКОГО»
ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ
Кафедра компьютерной инженерии и моделирования

Криптография и шифрование

Отчет по лабораторной работе 4
по дисциплине «Информационная Безопасность»
студента 3 курса группы ИВТ-б-о-202
Шор Константина Александровича

Направления подготовки 09.03.01«Информатика и вычислительная техника»

Симферополь, 2023

Голландский лингвист Огюст Керкгоффс в 1883 г **сформулировал главное требование к криптографическим системам, которое остается актуальным и поныне:**

1. Система должна быть физически, если не математически, невскрываемой
2. **Нужно, чтобы не требовалось сохранение системы в тайне; попадание системы в руки врага не должно причинять неудобств**;
3. Хранение и передача ключа должны быть осуществимы без помощи бумажных записей; корреспонденты должны располагать возможностью менять ключ по своему усмотрению
4. Система должна быть пригодной для сообщения через телеграф
5. Система должна быть легко переносимой, работа с ней не должна требовать участия нескольких лиц одновременно
6. Наконец, от системы требуется, учитывая возможные обстоятельства её применения, чтобы она была проста в использовании, не требовала значительного умственного напряжения или соблюдения большого количества правил

Секретность шифров должна быть основана на секретности ключа, но не алгоритма.

Симметричное шифрование – использование одного и того же ключа для шифрования и расшифрования:

- AES
- DES
- RC6
- 3DES
- SEED
- Camellia

Ассиметричное шифрование - использование для шифрования и расшифрования разных, но математически связанных ключей:

- RSA
- DSA
- ECC
- Меркля
- Схема Шнорра

Ход работы

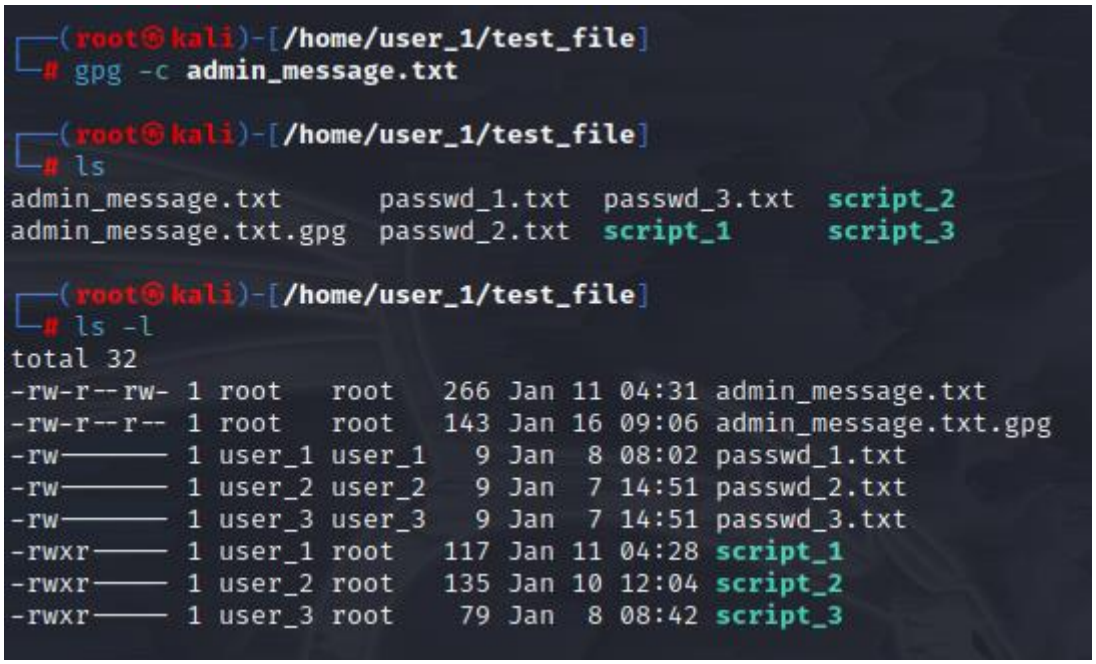
```
┌──(root㉿kali)-[/home/user_1/test_file]
└─# ls
admin_message.txt  passwd_1.txt  passwd_2.txt  passwd_3.txt  script_1  script_2  script_3
```

1. Установить PGP, GPG 2.

```
└─# apt install pgpgpg
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  gnome-bluetooth-common libgnome-bluetooth13
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  pgpgpg
0 upgraded, 1 newly installed, 0 to remove and 811 not upgraded.
Need to get 18.8 kB of archives.
After this operation, 62.5 kB of additional disk space will be used.
Get:1 http://mirror-1.truenetwork.ru/kali kali-rolling/main amd64 pgpgpg amd64 0.13-12 [18.8 kB]
Fetched 18.8 kB in 2s (10.6 kB/s)
Selecting previously unselected package pgpgpg.
(Reading database ... 418938 files and directories currently installed.)
Preparing to unpack .../pgpgpg_0.13-12_amd64.deb ...
Unpacking pgpgpg (0.13-12) ...
Setting up pgpgpg (0.13-12) ...
update-alternatives: using /usr/bin/pgpgpg to provide /usr/bin/pgp (pgp) in auto mode
Processing triggers for man-db (2.11.0-1+b1) ...
Processing triggers for kali-menu (2022.4.1) ...
```

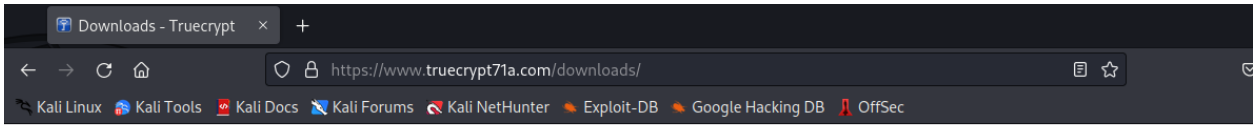
2. Произвести операции шифрования и дешифрования над произвольными файлами. Для шифрования используйте команду . Для дешифрования (В этом случае в директории зашифрованного файла будет создан расшифрованный. Если нужно лишь вывести на экран расшифрованное содержимое используйте)

Шифрование



Дешифрование

3. Установить TrueCrypt. Версия 7.1a



Downloads

July 29, 2015 by admin

We offer the product as is, and do not claim any rights to the name TrueCrypt or TrueCrypt.org – this is not a fork but the distribution of the product under Section II of the TrueCrypt license.

TrueCrypt 7.1a | Language Packs | Source Code

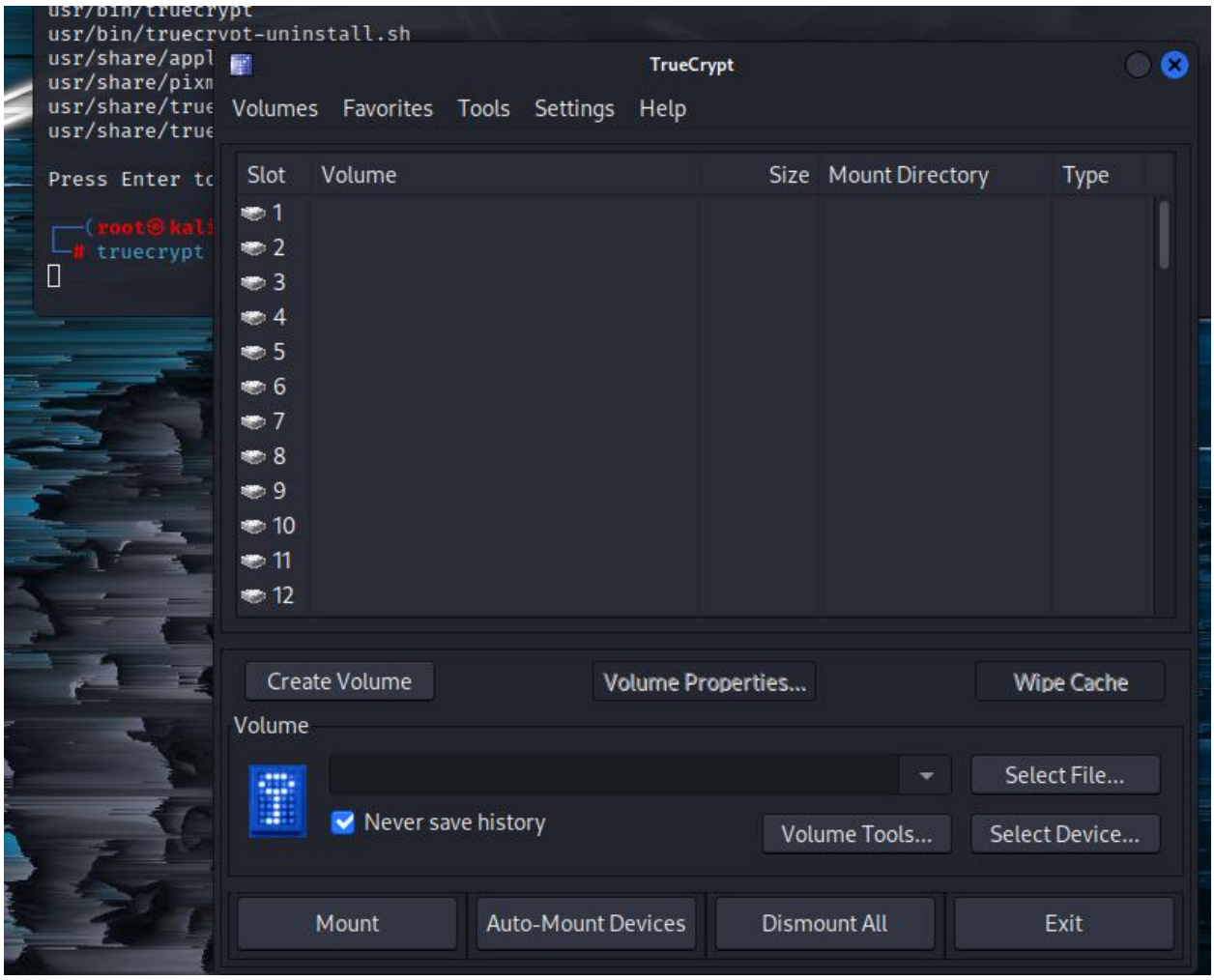
Operating System	Signature	Download
Windows (XP/Vista/7/8)	sig	TrueCrypt Setup 7.1a.exe
MacOS X	sig	TrueCrypt 7.1a Mac OS X.dmg
Linux x86 / gui	sig	truecrypt-7.1a-linux-x86.tar.gz
Linux 64bit / gui	sig	truecrypt-7.1a-linux-x64.tar.gz
Linux x86 / headless	sig	truecrypt-7.1a-linux-console-x86.tar.gz
Linux 64bit / headless	sig	truecrypt-7.1a-linux-console-x64.tar.gz

```
1. The origin of this software must not be misrepresented; you
   must not claim that you wrote the original software. If you
   use this software in a product, an acknowledgment in the
   product documentation would be appreciated but is not
   required.
2. Altered source versions must be plainly marked as such, and
   must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source
   distribution.
```

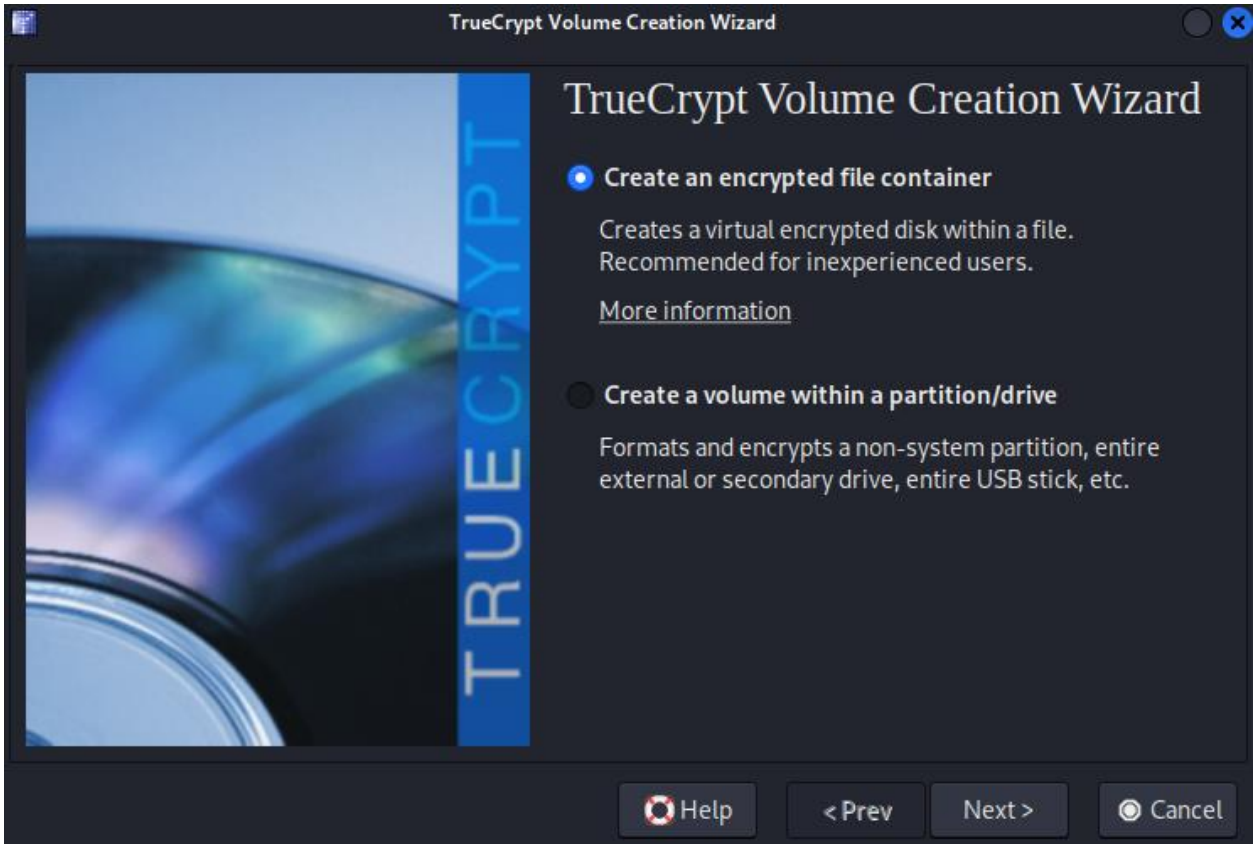
```
Do you accept and agree to be bound by the license terms? (yes/no): yes
```

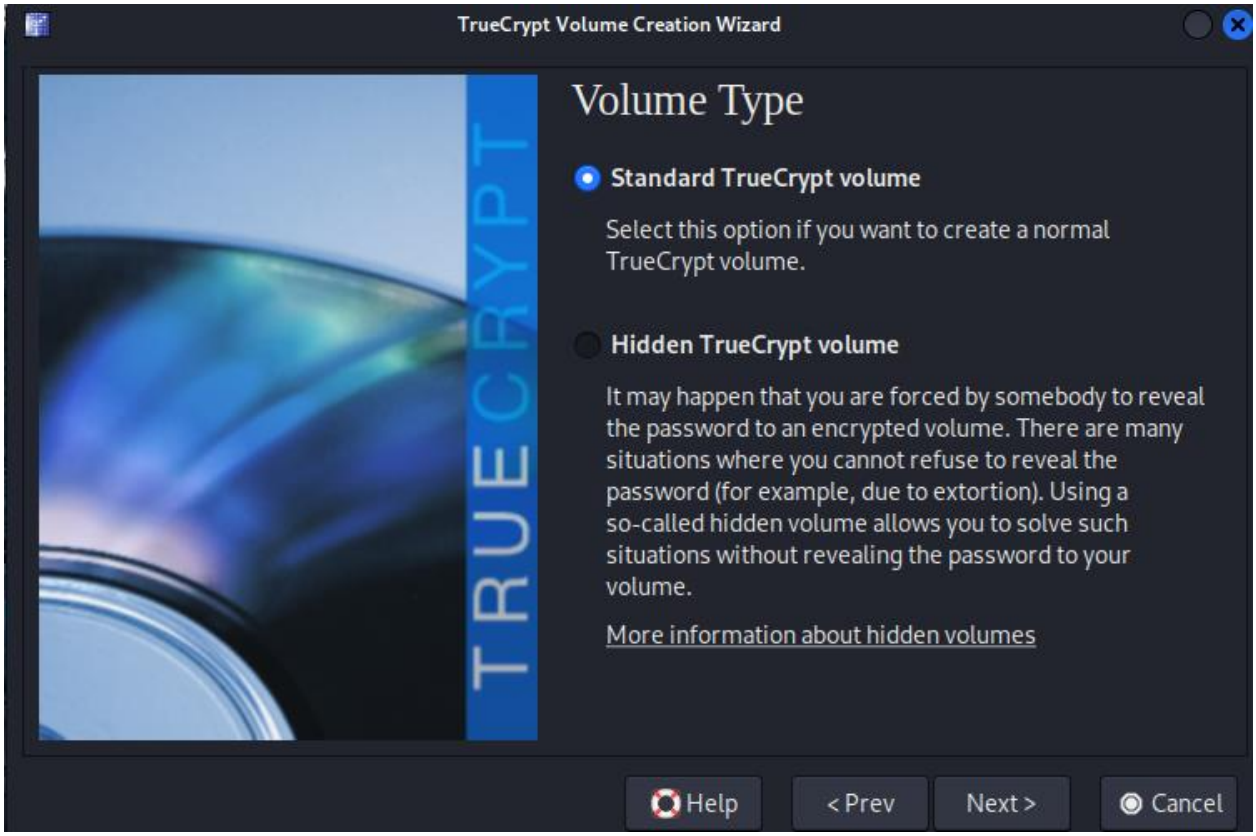
```
Uninstalling TrueCrypt:
```

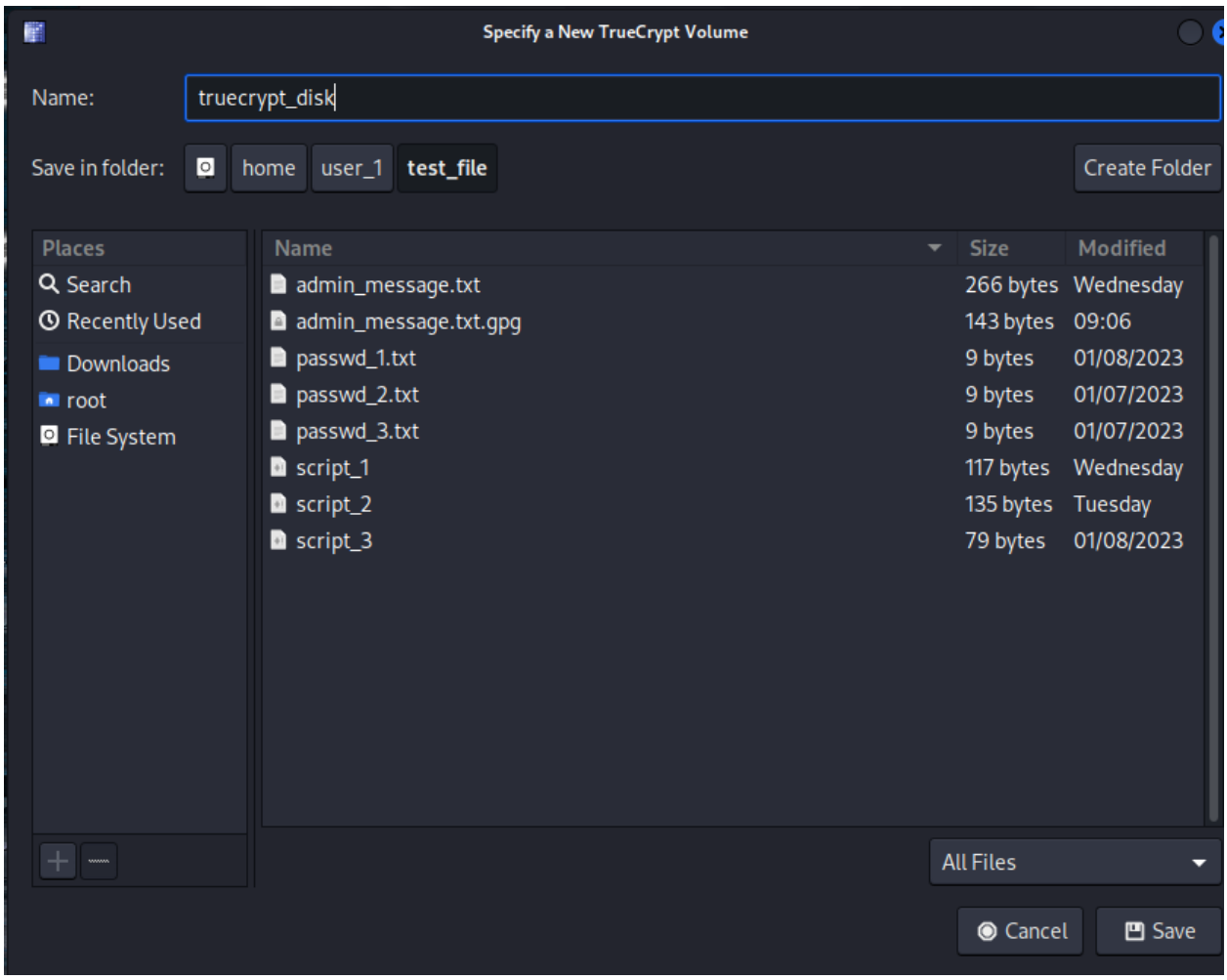
```
To uninstall TrueCrypt, please run 'truecrypt-uninstall.sh'.

Installing package ...
usr/bin/truecrypt
usr/bin/truecrypt-uninstall.sh
usr/share/applications/truecrypt.desktop
usr/share/pixmaps/truecrypt.xpm
usr/share/truecrypt/doc/License.txt
usr/share/truecrypt/doc/TrueCrypt User Guide.pdf

Press Enter to exit ...
```

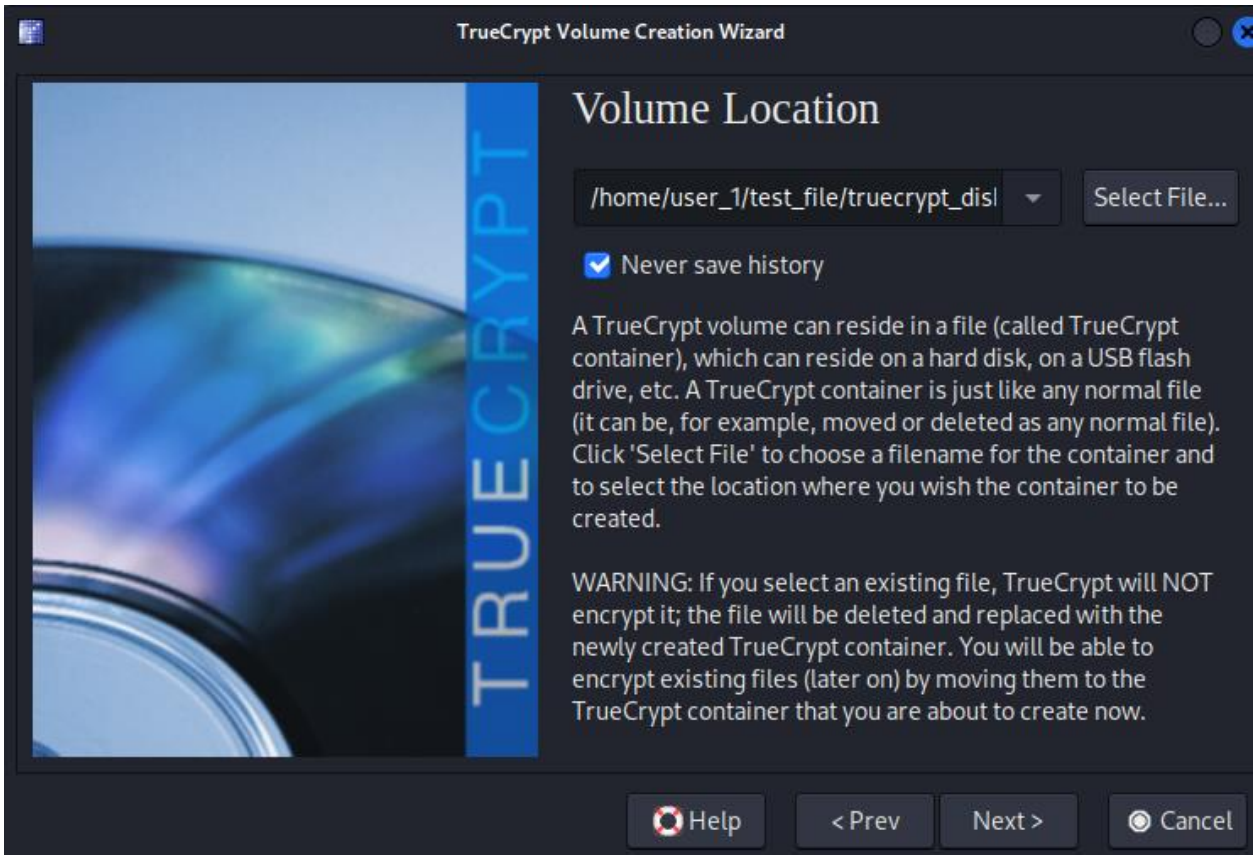

usr/bin/truecrypt
usr/bin/truecrypt-uninstall.sh
usr/share/appl
usr/share/pixm
usr/share/true
usr/share/true
Press Enter to
root@kali
truecrypt
TrueCrypt
Volumes
Favorites
Tools
Settings
Help
Slot
Volume
Size
Mount Directory
Type
1
2
3
4
5
6
7
8
9
10
11
12
Create Volume
Volume Properties...
Wipe Cache
Volume
Select File...
Never save history
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit

4. Создать криптоконтейнер, примонтировать его как виртуальный диск






Specify a New TrueCrypt Volume
Name:
truecrypt_disk
Save in folder:
home
user_1
test_file
Create Folder
Places
Search
Recently Used
Downloads
root
File System
Name
Size
Modified
admin_message.txt
266 bytes
Wednesday
admin_message.txt.gpg
143 bytes
09:06
passwd_1.txt
9 bytes
01/08/2023
passwd_2.txt
9 bytes
01/07/2023
passwd_3.txt
9 bytes
01/07/2023
script_1
117 bytes
Wednesday
script_2
135 bytes
Tuesday
script_3
79 bytes
01/08/2023
All Files
Cancel
Save

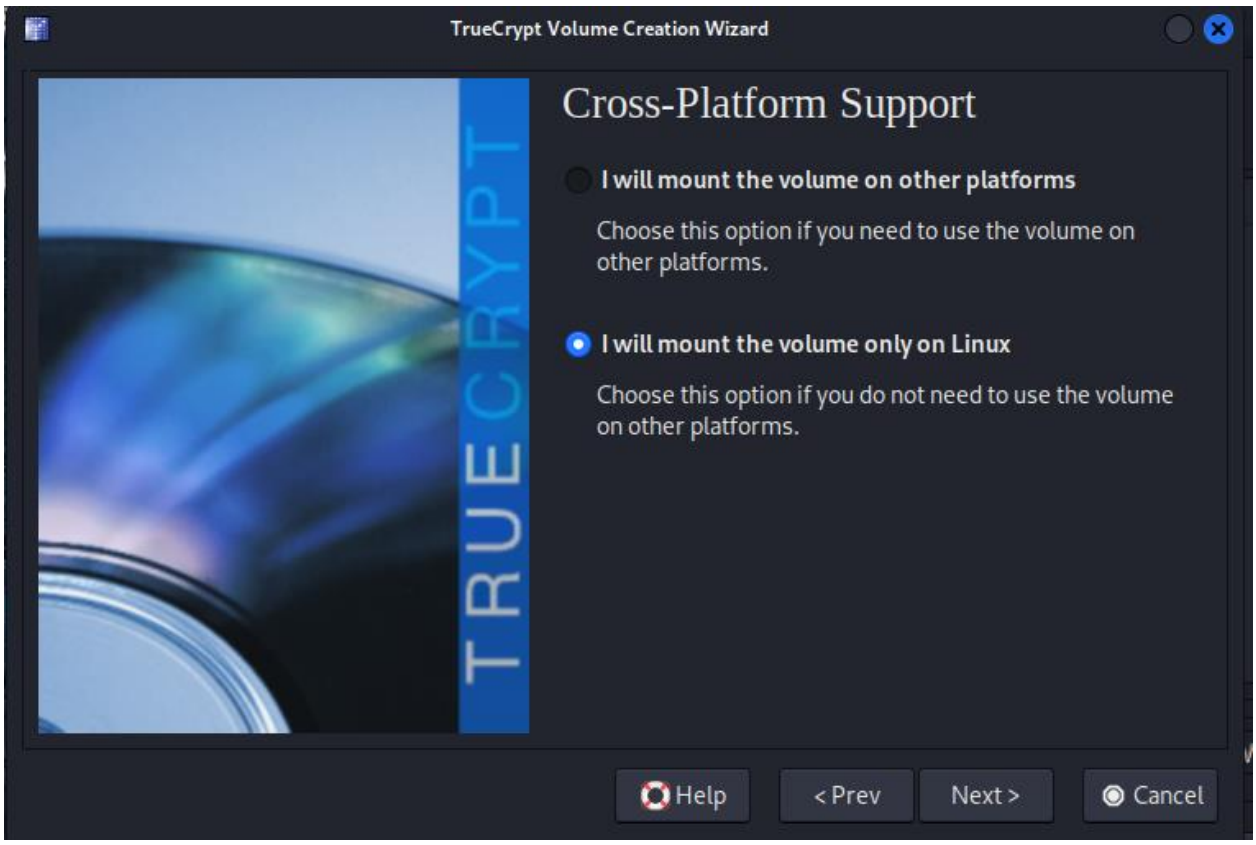

TrueCrypt Volume Creation Wizard
TRUECRYPT
Volume Location
/home/user_1/test_file/truecrypt_disl
Select File...
Never save history
A TrueCrypt volume can reside in a file (called TrueCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A TrueCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.
WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created TrueCrypt container. You will be able to encrypt existing files (later on) by moving them to the TrueCrypt container that you are about to create now.
Help
< Prev
Next >
Cancel


TrueCrypt Volume Creation Wizard
TRUECRYPT
Encryption Options
Encryption Algorithm
AES
Test
FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.
More information on AES
Benchmark
Hash Algorithm
RIPEMD-160
Information on hash algorithms
Help
< Prev
Next >
Cancel


TrueCrypt Volume Creation Wizard
TRUECRYPT
Volume Size
100
M
Free space available: 58.9 GB
Please specify the size of the container to create. Note that the minimum possible size of a volume is 292 KB.
Help
< Prev
Next >
Cancel

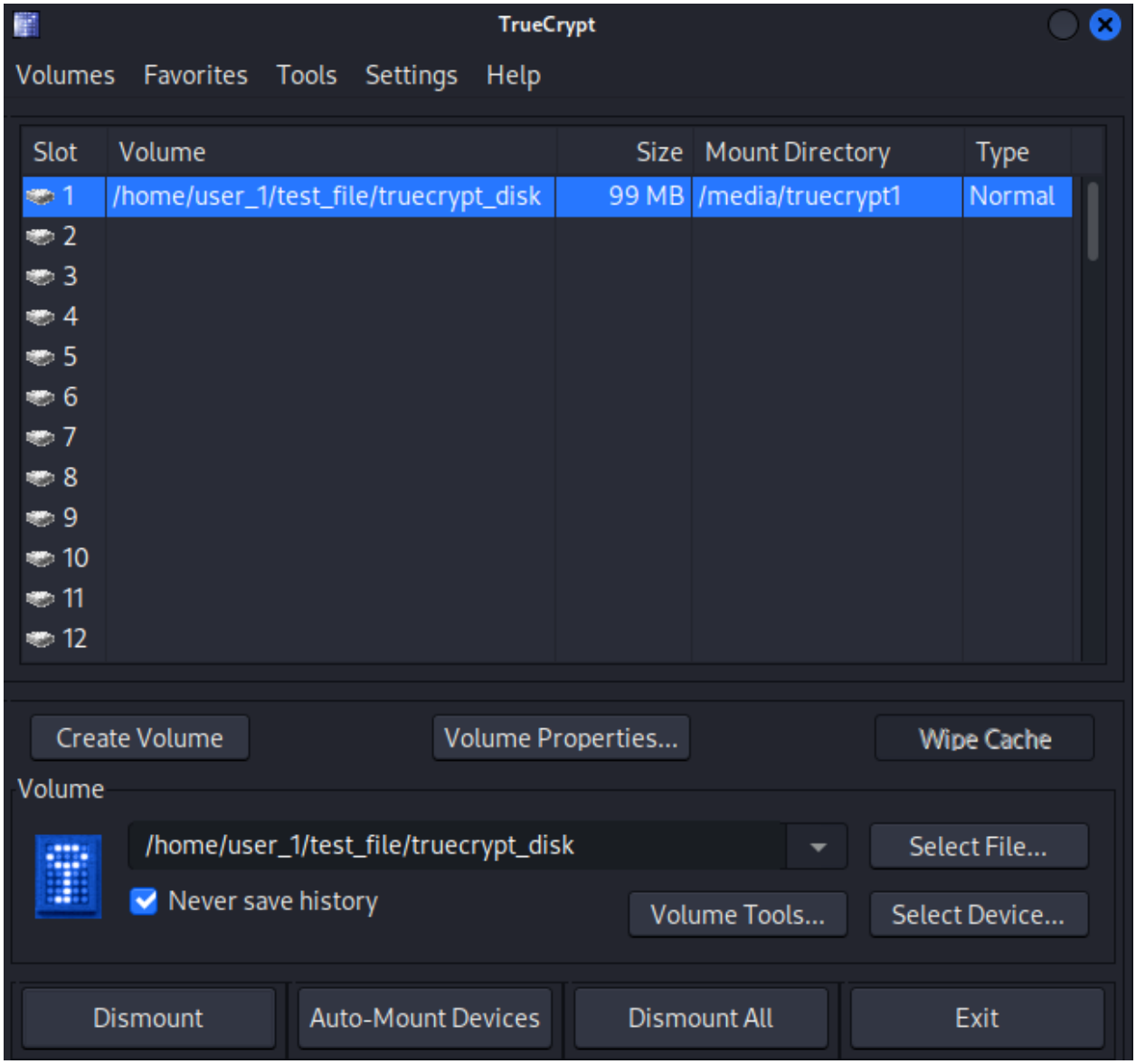

TrueCrypt Volume Creation Wizard
TRUECRYPT
Volume Password
Password:
Confirm password:
Display password
Use keyfiles
Keyfiles...
It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of more than 20 characters (the longer, the better). The maximum possible length is 64 characters.
Help
< Prev
Next >
Cancel


TrueCrypt Volume Creation Wizard
TRUECRYPT
Format Options
Filesystem Options
Filesystem type:
Linux Ext
Volume Format Options
Quick format
In order to enable your operating system to mount your new volume, it has to be formatted with a filesystem. Please select a filesystem type.
If your volume is going to be hosted on a device or partition, you can use 'Quick format' to skip encryption of free space of the volume.
Help
< Prev
Next >
Cancel


TrueCrypt Volume Creation Wizard
Cross-Platform Support
I will mount the volume on other platforms
Choose this option if you need to use the volume on other platforms.
I will mount the volume only on Linux
Choose this option if you do not need to use the volume on other platforms.
TRUECRYPT
Help
< Prev
Next >
Cancel

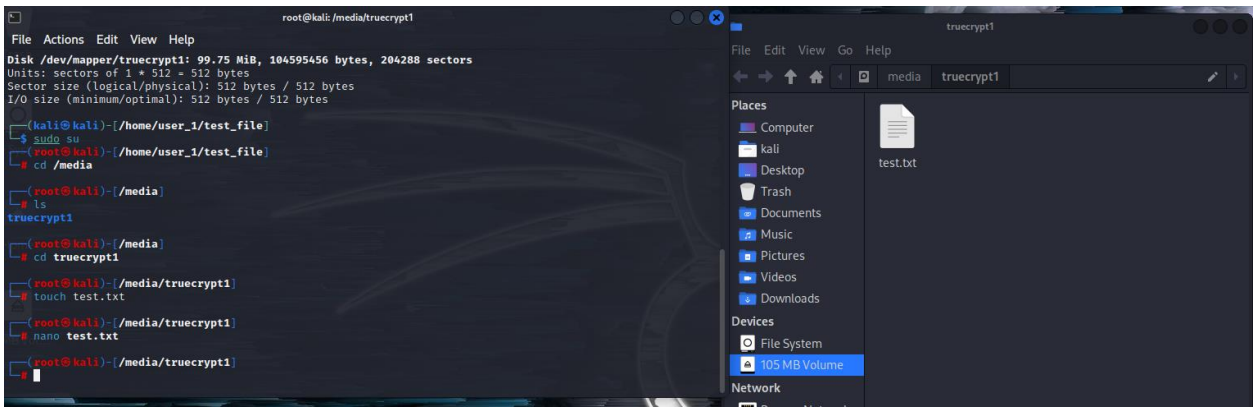

TrueCrypt Volume Creation Wizard
Volume Format
Random Pool: 9F322C916E65E1CD98EED569AD..
Header Key:
Master Key:
Abort
Done
Speed
Left
IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.
TRUECRYPT
Help
< Prev
Format
Cancel

Монтирование

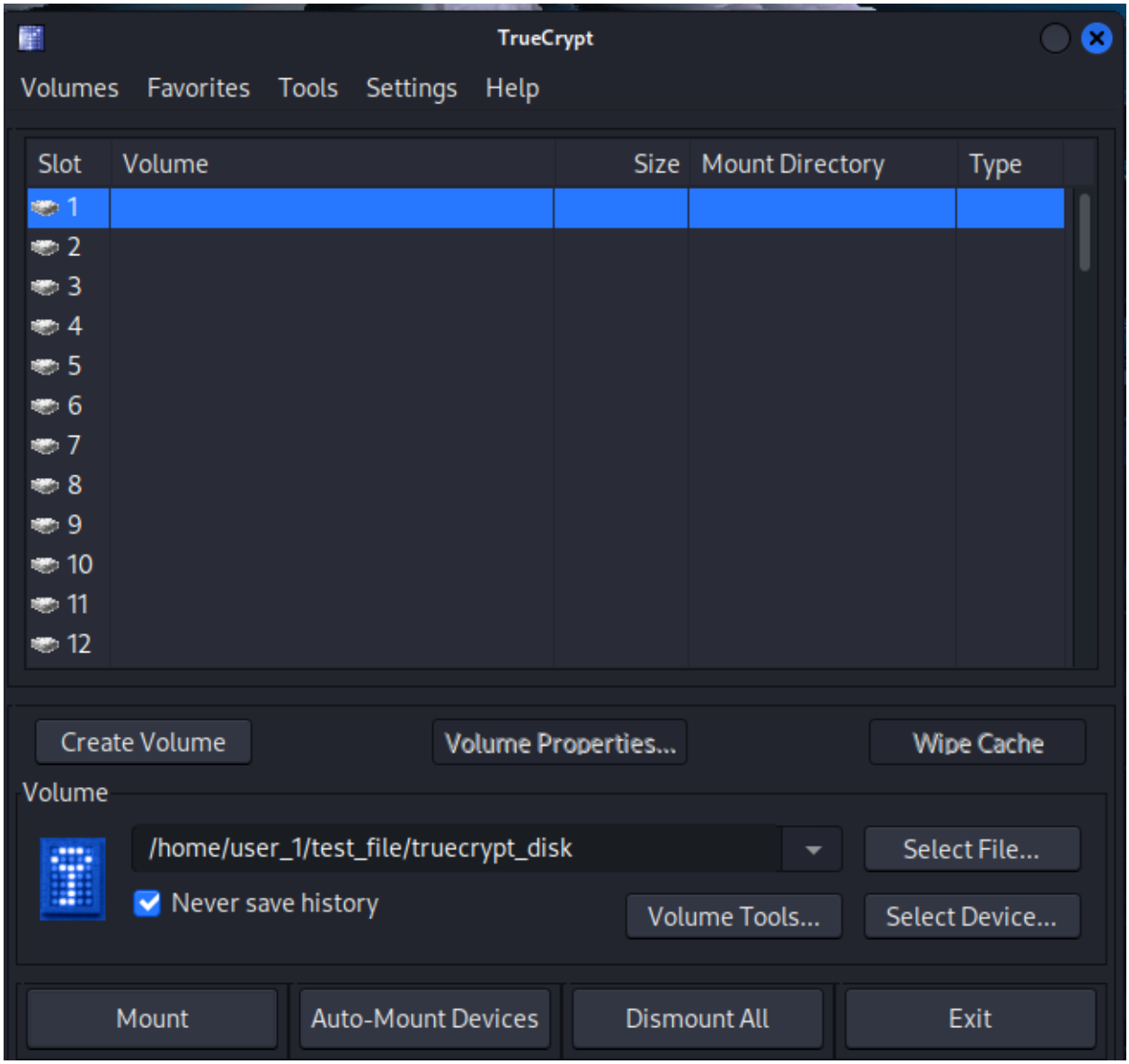


```
┌──(kali㉿kali)-[/home/user_1/test_file]
└─$ sudo fdisk -l
[sudo] password for kali:
Disk /dev/sda: 80.09 GiB, 86000000000 bytes, 167968750 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xb30c6083

Device     Boot Start       End   Sectors  Size Id Type
/dev/sda1  *     2048 167968749 167966702 80.1G 83 Linux


Disk /dev/loop0: 100 MiB, 104857600 bytes, 204800 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/mapper/truecrypt1: 99.75 MiB, 104595456 bytes, 204288 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

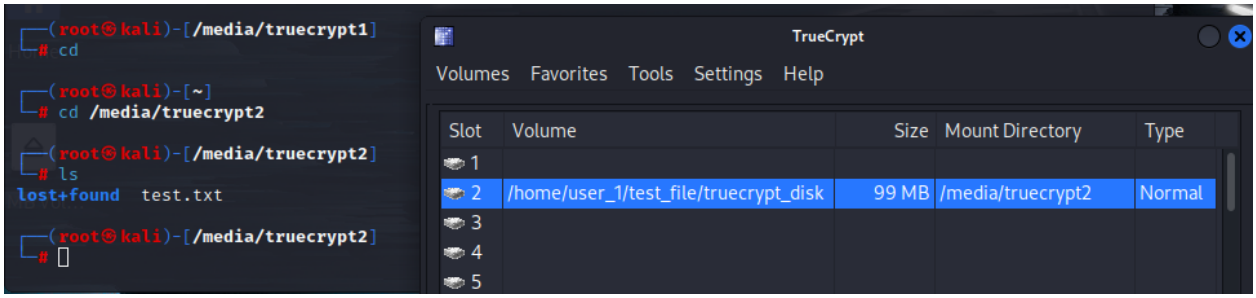
5. Поместить в криптоконтейнер какую-то информацию



6. Отмонтировать диск и переместить криптоконтейнер



7. Повторно примонтировать криптоконтейнер как виртуальный диск. Убедиться, что криптоконтейнер может передаваться и использоваться независимо



8. Установить LUKS/dm-crypt ,

```
┌──(root㉿kali)-[/home/kali]
└─# apt install cryptsetup
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
cryptsetup is already the newest version (2:2.6.0-2).
cryptsetup set to manually installed.
The following packages were automatically installed and are no longer required:
  gnome-bluetooth-common libgnome-bluetooth13
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  cryptsetup-bin libcryptsetup12
The following packages will be upgraded:
  cryptsetup-bin libcryptsetup12
2 upgraded, 0 newly installed, 0 to remove and 978 not upgraded.
Need to get 0 B/675 kB of archives.
After this operation, 71.7 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
(Reading database ... 419248 files and directories currently installed.)
Preparing to unpack .../libcryptsetup12_2%3a2.6.0-2_amd64.deb ...
Unpacking libcryptsetup12:amd64 (2:2.6.0-2) over (2:2.5.0-6) ...
Preparing to unpack .../cryptsetup-bin_2%3a2.6.0-2_amd64.deb ...
Unpacking cryptsetup-bin (2:2.6.0-2) over (2:2.5.0-6) ...
Setting up libcryptsetup12:amd64 (2:2.6.0-2) ...
Setting up cryptsetup-bin (2:2.6.0-2) ...
Processing triggers for libc-bin (2.36-4) ...
Processing triggers for man-db (2.11.0-1+b1) ...
Processing triggers for kali-menu (2022.4.1) ...
```

9. Создать файл, где будут храниться зашифрованные данные

```
┌──(root㉿kali)-[/mnt]
└─# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda      8:0    0    5G  0 disk
└─sda1   8:1    0    2G  0 part
sdb      8:16   0 80.1G  0 disk
└─sdb1   8:17   0 80.1G  0 part /
sr0     11:0    1 1024M  0 rom
```

10. Создать криптоконтейнер

```
┌──(root㉿kali)-[/mnt]
└─# cryptsetup  luksFormat /dev/sda1

WARNING!
========
This will overwrite data on /dev/sda1 irrevocably.

Are you sure? (Type 'yes' in capital letters): YES
Enter passphrase for /dev/sda1:
Verify passphrase:
```

11. Открыть контейнер

```
┌──(root㉿kali)-[/mnt]
└─# cryptsetup  luksOpen /dev/sda1 SSD
Enter passphrase for /dev/sda1:

┌──(root㉿kali)-[/mnt]
└─# lsblk
NAME    MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINTS
sda       8:0    0    5G  0 disk
└─sda1    8:1    0    2G  0 part
  └─SSD 254:0    0    2G  0 crypt
sdb       8:16   0 80.1G  0 disk
└─sdb1    8:17   0 80.1G  0 part  /
sr0      11:0    1 1024M  0 rom
```

```
┌──(root㉿kali)-[/dev]
└─# cd /dev/mapper

┌──(root㉿kali)-[/dev/mapper]
└─# ls
control  SSD

┌──(root㉿kali)-[/dev/mapper]
└─#
```

Device mapper-это **фреймворк, предоставляемый ядром Linux для отображения физических блочных устройств на виртуальные блочные устройства более высокого уровня**. Он формирует основу диспетчера логических томов (LVM), программных рейдов и шифрования дисков dm-crypt, а также предлагает дополнительные функции, такие как моментальные снимки файловой системы.

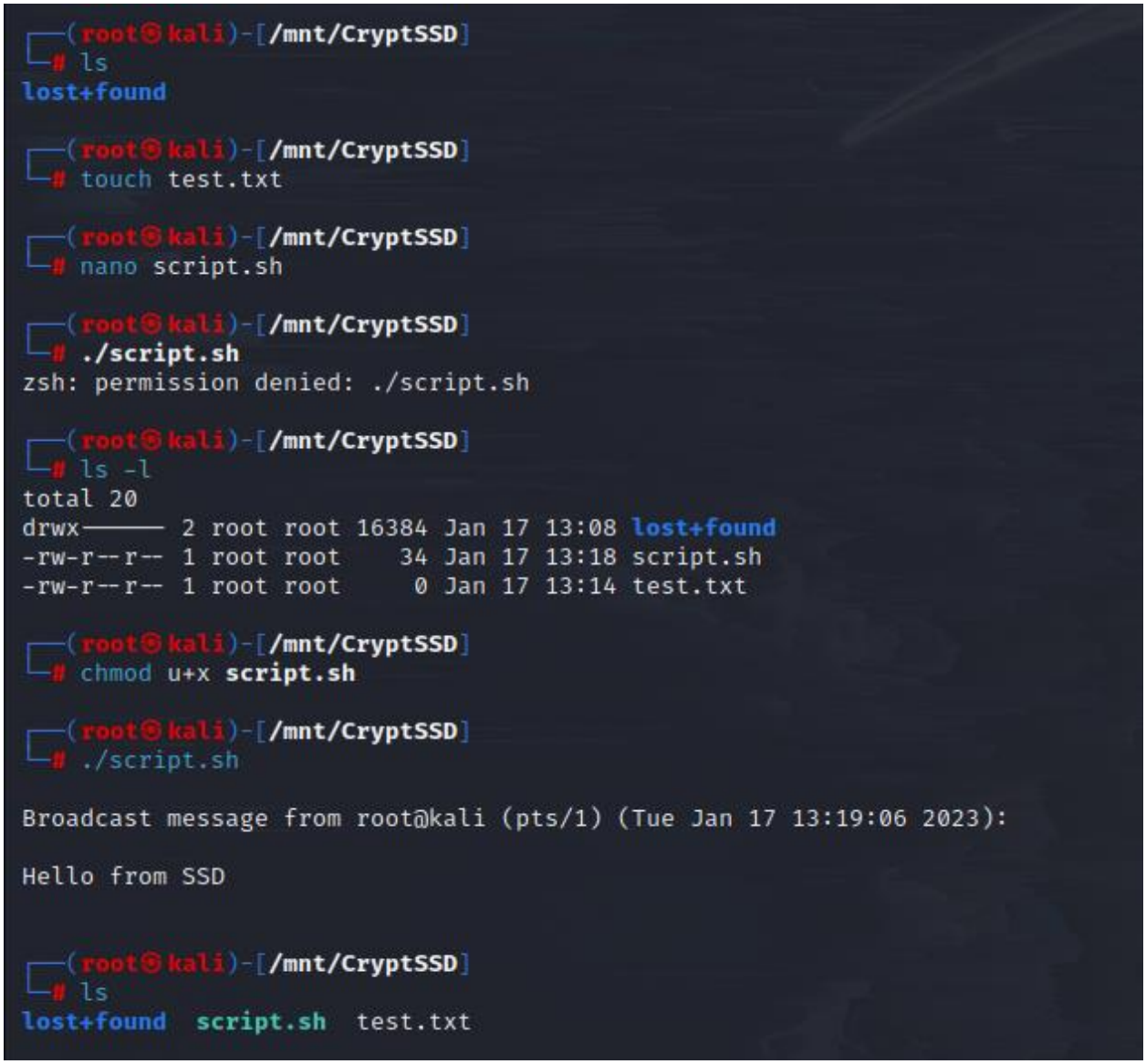
12. Создать в нем файловую систему

```
┌──(root㉿kali)-[/dev/mapper]
└─# mkfs -t ext4 /dev/mapper/SSD
mke2fs 1.46.6-rc1 (12-Sep-2022)
Creating filesystem with 520192 4k blocks and 130048 inodes
Filesystem UUID: a1e1f57c-d331-4217-af2c-9f5c632d8896
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912

Allocating group tables: done
Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done
```

13. Создать папку для монтирования

```
┌──(root㉿kali)-[/mnt]
└─# mkdir CryptSSD

┌──(root㉿kali)-[/mnt]
└─# ls
CryptSSD

┌──(root㉿kali)-[/mnt]
└─# mount /dev/mapper/SSD /mnt/CryptSSD

┌──(root㉿kali)-[/mnt]
└─# mount
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
udev on /dev type devtmpfs (rw,nosuid,relatime,size=976128k,nr_inodes=244032,mode=755,inode64)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,nodev,noexec,relatime,size=202876k,mode=755,inode64)
/dev/sdb1 on / type ext4 (rw,relatime,errors=remount-ro)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,inode64)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k,inode64)
cgroup2 on /sys/fs/cgroup type cgroup2 (rw,nosuid,nodev,noexec,relatime,nsdelegate,memory_recursiveprot)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
bpf on /sys/fs/bpf type bpf (rw,nosuid,nodev,noexec,relatime,mode=700)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=29,pgrp=1,timeout=0,minproto=5,maxproto=5
,direct,pipe_ino=12396)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime,pagesize=2M)
mqueue on /dev/mqueue type mqueue (rw,nosuid,nodev,noexec,relatime)
debugfs on /sys/kernel/debug type debugfs (rw,nosuid,nodev,noexec,relatime)
tracefs on /sys/kernel/tracing type tracefs (rw,nosuid,nodev,noexec,relatime)
configfs on /sys/kernel/config type configfs (rw,nosuid,nodev,noexec,relatime)
ramfs on /run/credentials/systemd-sysctl.service type ramfs (ro,nosuid,nodev,noexec,relatime,mode=700)
fusectl on /sys/fs/fuse/connections type fusectl (rw,nosuid,nodev,noexec,relatime)
ramfs on /run/credentials/systemd-sysusers.service type ramfs (ro,nosuid,nodev,noexec,relatime,mode=700)
ramfs on /run/credentials/systemd-tmpfiles-setup-dev.service type ramfs (ro,nosuid,nodev,noexec,relatime,mo
de=700)
binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,nosuid,nodev,noexec,relatime)
ramfs on /run/credentials/systemd-tmpfiles-setup.service type ramfs (ro,nosuid,nodev,noexec,relatime,mode=7
00)
sunrpc on /run/rpc_pipefs type rpc_pipefs (rw,relatime)
tmpfs on /run/user/1000 type tmpfs (rw,nosuid,nodev,relatime,size=202872k,nr_inodes=50718,mode=700,uid=1000
,gid=1000,inode64)
gvfsd-fuse on /run/user/1000/gvfs type fuse.gvfsd-fuse (rw,nosuid,nodev,relatime,user_id=1000,group_id=1000
)
/dev/mapper/SSD on /mnt/CryptSSD type ext4 (rw,relatime)

┌──(root㉿kali)-[/mnt]
└─#
```

14. Положить файлы в криптоконтейнер



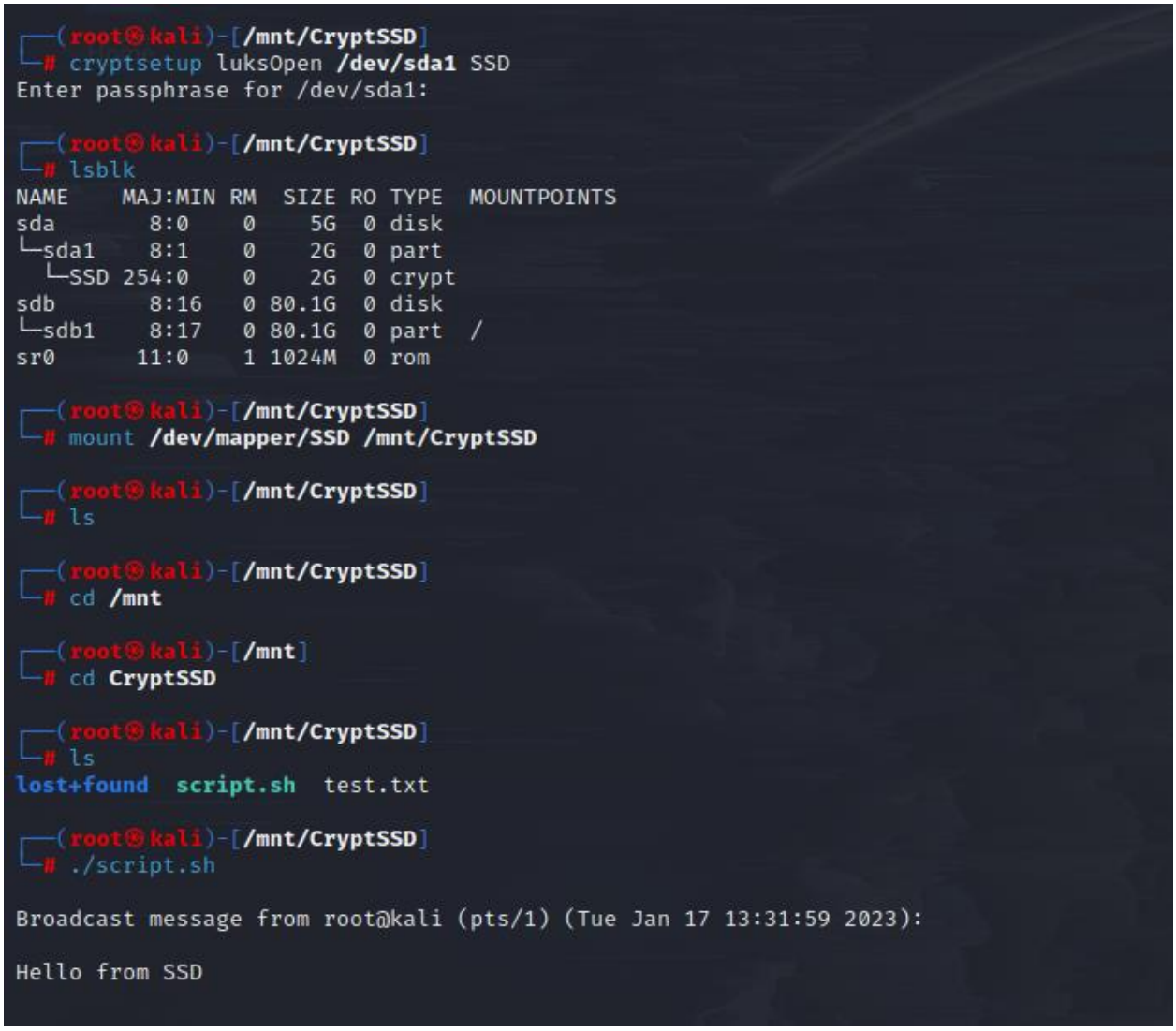
15. Размонтировать

```
┌──(root㉿kali)-[/mnt/CryptSSD]
└─# cd

┌──(root㉿kali)-[~]
└─# umount /dev/mapper/SSD

┌──(root㉿kali)-[~]
└─# mount
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
udev on /dev type devtmpfs (rw,nosuid,relatime,size=976128k,nr_inodes=244032,mode=755,inode64)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,nodev,noexec,relatime,size=202876k,mode=755,inode64)
/dev/sdb1 on / type ext4 (rw,relatime,errors=remount-ro)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,inode64)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k,inode64)
cgroup2 on /sys/fs/cgroup type cgroup2 (rw,nosuid,nodev,noexec,relatime,nsdelegate,memory_recursiveprot)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
bpf on /sys/fs/bpf type bpf (rw,nosuid,nodev,noexec,relatime,mode=700)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=29,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=12396)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime,pagesize=2M)
mqueue on /dev/mqueue type mqueue (rw,nosuid,nodev,noexec,relatime)
debugfs on /sys/kernel/debug type debugfs (rw,nosuid,nodev,noexec,relatime)
tracefs on /sys/kernel/tracing type tracefs (rw,nosuid,nodev,noexec,relatime)
configfs on /sys/kernel/config type configfs (rw,nosuid,nodev,noexec,relatime)
ramfs on /run/credentials/systemd-sysctl.service type ramfs (ro,nosuid,nodev,noexec,relatime,mode=700)
fusectl on /sys/fs/fuse/connections type fusectl (rw,nosuid,nodev,noexec,relatime)
ramfs on /run/credentials/systemd-sysusers.service type ramfs (ro,nosuid,nodev,noexec,relatime,mode=700)
ramfs on /run/credentials/systemd-tmpfiles-setup-dev.service type ramfs (ro,nosuid,nodev,noexec,relatime,mode=700)
binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,nosuid,nodev,noexec,relatime)
ramfs on /run/credentials/systemd-tmpfiles-setup.service type ramfs (ro,nosuid,nodev,noexec,relatime,mode=700)
sunrpc on /run/rpc_pipefs type rpc_pipefs (rw,relatime)
tmpfs on /run/user/1000 type tmpfs (rw,nosuid,nodev,relatime,size=202872k,nr_inodes=50718,mode=700,uid=1000,gid=1000,inode64)
gvfsd-fuse on /run/user/1000/gvfs type fuse.gvfsd-fuse (rw,nosuid,nodev,relatime,user_id=1000,group_id=1000)
```

16. Закрыть volume1.

```
┌──(root㉿kali)-[~]
└─# mount
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
udev on /dev type devtmpfs (rw,nosuid,relatime,size=976128k,nr_inodes=244032,mode=755,inode64)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,nodev,noexec,relatime,size=202876k,mode=755,inode64)
/dev/sdb1 on / type ext4 (rw,relatime,errors=remount-ro)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,inode64)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k,inode64)
cgroup2 on /sys/fs/cgroup type cgroup2 (rw,nosuid,nodev,noexec,relatime,nsdelegate,memory_recursiveprot)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
bpf on /sys/fs/bpf type bpf (rw,nosuid,nodev,noexec,relatime,mode=700)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=29,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=12396)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime,pagesize=2M)
mqueue on /dev/mqueue type mqueue (rw,nosuid,nodev,noexec,relatime)
debugfs on /sys/kernel/debug type debugfs (rw,nosuid,nodev,noexec,relatime)
tracefs on /sys/kernel/tracing type tracefs (rw,nosuid,nodev,noexec,relatime)
configfs on /sys/kernel/config type configfs (rw,nosuid,nodev,noexec,relatime)
ramfs on /run/credentials/systemd-sysctl.service type ramfs (ro,nosuid,nodev,noexec,relatime,mode=700)
fusectl on /sys/fs/fuse/connections type fusectl (rw,nosuid,nodev,noexec,relatime)
ramfs on /run/credentials/systemd-sysusers.service type ramfs (ro,nosuid,nodev,noexec,relatime,mode=700)
ramfs on /run/credentials/systemd-tmpfiles-setup-dev.service type ramfs (ro,nosuid,nodev,noexec,relatime,mode=700)
binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,nosuid,nodev,noexec,relatime)
ramfs on /run/credentials/systemd-tmpfiles-setup.service type ramfs (ro,nosuid,nodev,noexec,relatime,mode=700)
sunrpc on /run/rpc_pipefs type rpc_pipefs (rw,relatime)
tmpfs on /run/user/1000 type tmpfs (rw,nosuid,nodev,relatime,size=202872k,nr_inodes=50718,mode=700,uid=1000,gid=1000,inode64)
gvfsd-fuse on /run/user/1000/gvfs type fuse.gvfsd-fuse (rw,nosuid,nodev,relatime,user_id=1000,group_id=1000)

┌──(root㉿kali)-[~]
└─# cryptsetup luksClose /dev/mapper/SSD
```

17. Открыть, выполняя




┌──(root㉿kali)-[/mnt/CryptSSD]
└─# cryptsetup luksDump /dev/sda1
LUKS header information
Version: 2
Epoch: 3
Metadata area: 16384 [bytes]
Keyslots area: 16744448 [bytes]
UUID: ed923f0a-e92b-459c-bc59-b66c5e2a57c9
Label: (no label)
Subsystem: (no subsystem)
Flags: (no flags)
Data segments:
  0: crypt
        offset: 16777216 [bytes]
        length: (whole device)
        cipher: aes-xts-plain64
        sector: 512 [bytes]
Keyslots:
  0: luks2
        Key: 512 bits
        Priority: normal
        Cipher: aes-xts-plain64
        Cipher key: 512 bits
        PBKDF: argon2id
        Time cost: 4
        Memory: 592564
        Threads: 2
        Salt: 45 9a c7 9c 5b b3 fc 15 ce b4 07 a7 7a 3b 2d d3
                    08 81 10 e2 4f 2c 28 00 3d 8d 10 d7 d2 f2 f2 08
        AF stripes: 4000
        AF hash: sha256
        Area offset:32768 [bytes]
        Area length:258048 [bytes]
        Digest ID: 0
Tokens:
Digests:
  0: pbkdf2
        Hash: sha256
        Iterations: 32637
        Salt: 50 89 06 55 2a 9d 75 ce 92 3e 57 c2 8e 74 f6 67
                    2a 99 65 08 ab d8 dc df 12 12 3d 44 b5 30 00 05
        Digest: 98 ed 4e d0 32 4a 16 25 03 3c 9d 4c 6d 9b 1b b0
                    49 b9 4e 3f b7 4c 26 f8 d1 10 77 51 3c 11 dd 02

Вывод: в ходе данной лабораторной работы я научился пользоваться разными способами шифрования и дешифрования, монтирования и демонтирования. Были изучены такие инструменты, как: gpg, truecrypt и cryptsetup. С помощью gpg было реализовано простейшее шифрование файла. При работе с truecrypt, нам предоставляется графический интерфейс, в котором уже был создан и смонтирован диск, также размер и способ шифрования можно выбрать вручную. В программе cryptsetup работа уже происходит в консоли. Для работы с этой программой я создал виртуальный диск на 5G, создал на нём криптоконтейнер, открыл его, смонтировал и создал на нём несколько файлов, зачтем отмантировал, закрыл криптоконтейнер (произвёл физическое отсоединение). После опять смонтировал криптоконтейнер и убедился, что с данными было всё хорошо. Подводя итоги, можно сделать вывод, что я научился работать с шифрованием дисков.