A dark blue, irregular ink blot or splash shape is centered on a white background. The blot has a textured, painterly appearance with some lighter blue and white speckles around its edges. Inside the blot, the text "Практическая работа №5" is written in a clean, white, sans-serif font.

Практическая работа №5

```
Файл Действия Правка Вид Справка
arpwatch:!:18557:0:99999:7:::
usbmux:!:18557:0:99999:7:::
tcpdump:!:18557:0:99999:7:::
rtkit:!:18557:0:99999:7:::
_rpc:!:18557:0:99999:7:::
Debian-snmpp:!:18557:0:99999:7:::
statd:!:18557:0:99999:7:::
postgres:!:18557:0:99999:7:::
stunnel4:!:18557:0:99999:7:::
sshd:!:18557:0:99999:7:::
ssllh:!:18557:0:99999:7:::
avahi:!:18557:0:99999:7:::
nm-openvpn:!:18557:0:99999:7:::
nm-openconnect:!:18557:0:99999:7:::
pulse:!:18557:0:99999:7:::
saned:!:18557:0:99999:7:::
inetsim:!:18557:0:99999:7:::
colord:!:18557:0:99999:7:::
geoclue:!:18557:0:99999:7:::
lightdm:!:18557:0:99999:7:::
king-phisher:!:18557:0:99999:7:::
dradis:!:18557:0:99999:7:::
beef-xss:!:18557:0:99999:7:::
enon:$6$iDJVRy8VF9g0KRcI$tgdr6DW/tjrFQyN9MdkV67qig5Sbp2Tjwa0EnEoY8YJvV00BCn
kObl2pCHvr.9aPjdIWYRnRvZt49CxEU3uXb/:18557:0:99999:7:::
systemd-coredump:!:18557:0:99999:7:::
enon@kali:~$ hashid -m '$6$iDJVRy8VF9g0KRcI$tgdr6DW/tjrFQyN9MdkV67qig5Sbp2Tjwa0EnEoY8YJvV00BCnkObl2pCHvr.9aPjdIWYRnRvZt49CxEU3uXb/'
Analyzing '$6$iDJVRy8VF9g0KRcI$tgdr6DW/tjrFQyN9MdkV67qig5Sbp2Tjwa0EnEoY8YJvV00BCnkObl2pCHvr.9aPjdIWYRnRvZt49CxEU3uXb/'
[+] SHA-512 Crypt [Hashcat Mode: 1800]
enon@kali:~$
```

1.1 Определение типа

Файл Действия Правка Вид Справка

```
enon@kali:~$ sudo useradd -m test1
enon@kali:~$ sudo passwd test1
Новый пароль :
Повторите ввод нового пароля :
passwd: пароль успешно обновлён
enon@kali:~$
```

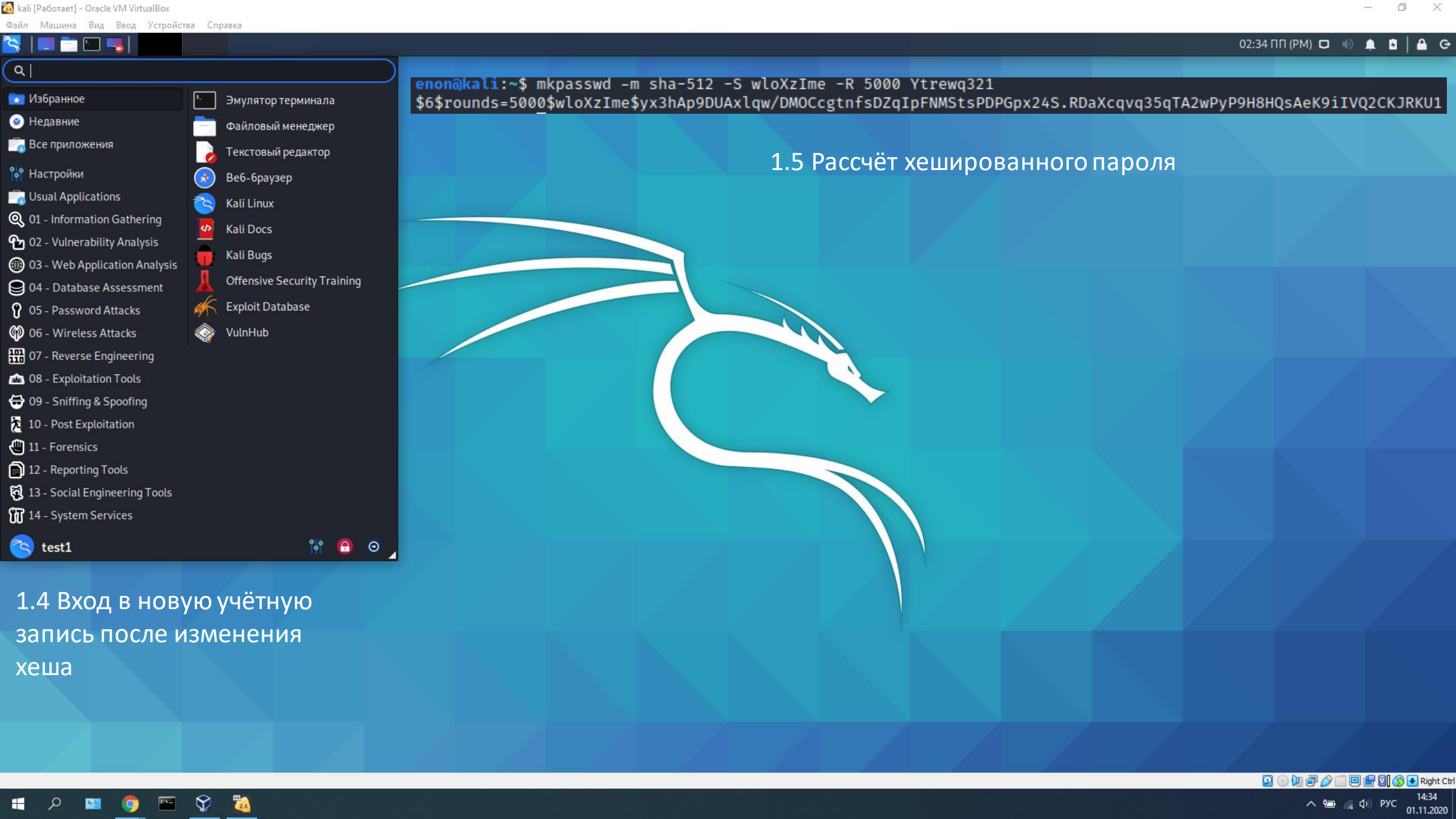
Создать
Пользователя

Пользователь
Создан

1.2 Создание нового пользователя

```
enon@kali: ~  
Файл Действия Правка Вид Справка  
GNU nano 4.9.3 /etc/shadow  
news:*:18557:0:99999:7:::  
uucp:*:18557:0:99999:7:::  
proxy:*:18557:0:99999:7:::  
www-data:*:18557:0:99999:7:::  
backup:*:18557:0:99999:7:::  
list:*:18557:0:99999:7:::  
irc:*:18557:0:99999:7:::  
gnats:*:18557:0:99999:7:::  
nobody:*:18557:0:99999:7:::  
_apt:*:18557:0:99999:7:::  
systemd-network:*:18557:0:99999:7:::  
systemd-resolve:*:18557:0:99999:7:::  
systemd-timesync:*:18557:0:99999:7:::  
mysql:!:18557:0:99999:7:::  
tss:*:18557:0:99999:7:::  
strongswan:*:18557:0:99999:7:::  
ntp:*:18557:0:99999:7:::  
messagebus:*:18557:0:99999:7:::  
redsocks:!:18557:0:99999:7:::  
rwhod:*:18557:0:99999:7:::  
iodine:*:18557:0:99999:7:::  
miredo:*:18557:0:99999:7:::  
arpwatch:!:18557:0:99999:7:::  
usbmux:*:18557:0:99999:7:::  
tcpdump:*:18557:0:99999:7:::  
rtkit:*:18557:0:99999:7:::  
_rpc:*:18557:0:99999:7:::  
Debian-snmpp:!:18557:0:99999:7:::  
statd:*:18557:0:99999:7:::  
postgres:*:18557:0:99999:7:::  
stunnel4:!:18557:0:99999:7:::  
sshd:*:18557:0:99999:7:::  
sslh:!:18557:0:99999:7:::  
avahi:*:18557:0:99999:7:::  
nm-openvpn:*:18557:0:99999:7:::  
nm-openconnect:*:18557:0:99999:7:::  
pulse:*:18557:0:99999:7:::  
saned:*:18557:0:99999:7:::  
inetsim:*:18557:0:99999:7:::  
colord:*:18557:0:99999:7:::  
geoclue:*:18557:0:99999:7:::  
lightdm:*:18557:0:99999:7:::  
king-phisher:*:18557:0:99999:7:::  
dradis:*:18557:0:99999:7:::  
beef-xss:*:18557:0:99999:7:::  
enon:$6$iDJVRy8VF9g0KRcI$tgdr6DW/tjrFQyN9MdkV67qig5Sbp2Tjwa0EoEoY8YJvV00BCnk0bl2pChvr.9aPjdIWYRnRvZt49CxEU3uXb/:18557:0:99999:7:::  
systemd-coredump:!:18557:0:99999:7:::  
test0:$6$r0pBfhxi3Ha9RV$QwOYL2MkWvFVEk7I6cCzCtr3hMrdJeH/tWmlRTbTWIiKmjZKcN8VV3thHLhc/VDzUiIQpUmIXXidfHzICzn9g/:18567:0:99999:7:::  
test1:$6$wloXzIme$yx3hAp9DUAXlqw/DMOCcgtnfsDZqIpFNMStsPDPGpx24S.RDaXcqyv35qTA2wPyP9H8HQsAeK9iIVQ2CKJRKU1:18567:0:99999:7:::  
Save modified buffer?   
Y Да  
N Нет ^C Отмена
```

1.3 Изменение хеша пароля в shadows



🔍

Избранное

Недавние

Все приложения

Настройки

Usual Applications

01 - Information Gathering

02 - Vulnerability Analysis

03 - Web Application Analysis

04 - Database Assessment

05 - Password Attacks

06 - Wireless Attacks

07 - Reverse Engineering

08 - Exploitation Tools

09 - Sniffing & Spoofing

10 - Post Exploitation

11 - Forensics

12 - Reporting Tools

13 - Social Engineering Tools

14 - System Services

test1

Эмулятор терминала

Файловый менеджер

Текстовый редактор

Веб-браузер

Kali Linux

Kali Docs

Kali Bugs

Offensive Security Training

Exploit Database

VulnHub

```
enon@kali:~$ mkpasswd -m sha-512 -S wloXzIme -R 5000 Ytrewq321  
$6$rounds=5000$wloXzIme$yx3hAp9DUAx1qw/DMOCcgtnfsDZqIpFNMsTsPDPGpx24S.RDaXcqvvq35qTA2wPyP9N8HqSAeK9iIVQ2CKJRKU1
```

1.5 Рассчёт хешированного пароля











1.4 Вход в новую учётную запись после изменения хеша

ФайлДействияПравкаВидСправка

GNU nano 4.9.3/home/enon/group

daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:enon
floppy:x:25:enon
tape:x:26:
sudo:x:27:enon
audio:x:29:pulse,enon
dip:x:30:enon
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:enon
sasl:x:45:
plugdev:x:46:enon
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
systemd-journal:x:101:
systemd-network:x:102:
systemd-resolve:x:103:
systemd-timesync:x:104:
input:x:105:
kvm:x:106:
render:x:107:
crontab:x:108:
netdev:x:109:enon
mysql:x:110:
tss:x:111:

 Видео
 Документы
 Загрузки
 Изображения
 Музыка
 Общедоступные
 Рабочий стол
 Шаблоны
 group
group.sha1

1.6 Изменение данных файла group

[Read 87 lines]

^G Помощь

^X Выход

^O Записать

^R ЧитФайл

^W Поиск

^_ Замена

^K Вырезать

^U Paste Text

^J Выворнять

^T Словарь

^C ТекПозиц

^_ К строке

M-U Отмена

M-E Повтор

M-A Отметить

M-6 Копировать

M-] На скобку

^Q Where Was

M-Q Previous

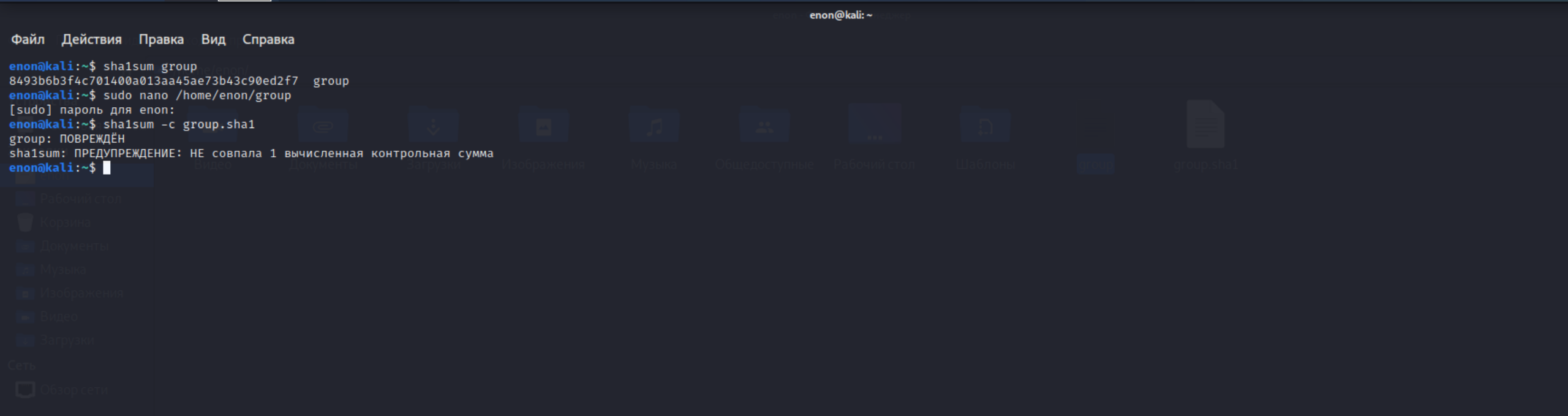
M-W Next

^B Назад

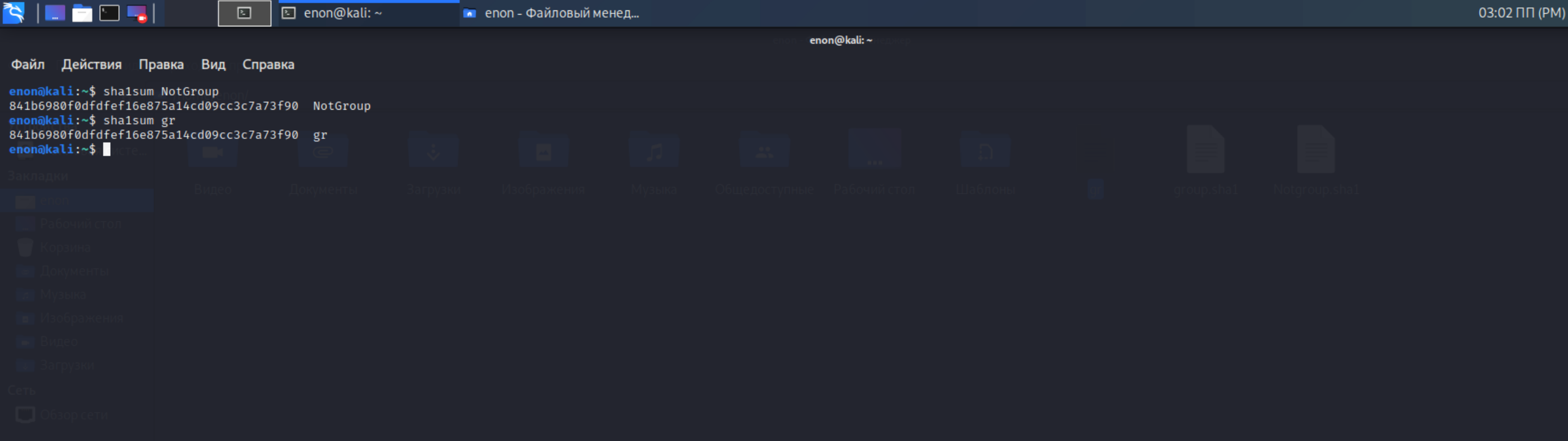
^F Вперёд

^_ Пред. слово

^_ След. слово



1.7 Проверка хеш-суммы после изменения



1.8 Отсутствие изменений в хеш-сумме при смене имени файла


```
enon@kali:~$ gpg --full-generate-key
gpg (GnuPG) 2.2.20; Copyright (C) 2020 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
```

Выберите тип ключа:

- (1) RSA и RSA (по умолчанию)
- (2) DSA и Elgamal
- (3) DSA (только для подписи)
- (4) RSA (только для подписи)
- (14) Existing key from card

Ваш выбор? 1

длина ключей RSA может быть от 1024 до 4096.

Какой размер ключа Вам необходим? (3072) 2048

Запрошенный размер ключа - 2048 бит

Выберите срок действия ключа.

0 = не ограничен

<n> = срок действия ключа - n дней

<n>w = срок действия ключа - n недель

<n>m = срок действия ключа - n месяцев

<n>y = срок действия ключа - n лет

Срок действия ключа? (0) 0

Срок действия ключа не ограничен

Все верно? (y/N) y

GnuPG должен составить идентификатор пользователя для идентификации ключа.

Ваше полное имя: istinlih

Адрес электронной почты:

Примечание:

Вы выбрали следующий идентификатор пользователя:

"istinlih"

Сменить (N)Имя, (C)Примечание, (E)Адрес; (O)Принять/(Q)Выход? o

Необходимо получить много случайных чисел. Желательно, чтобы Вы в процессе генерации выполняли какие-то другие действия (печать на клавиатуре, движения мыши, обращения к дискам); это даст генератору случайных чисел больше возможностей получить достаточное количество энтропии.

Необходимо получить много случайных чисел. Желательно, чтобы Вы в процессе генерации выполняли какие-то другие действия (печать на клавиатуре, движения мыши, обращения к дискам); это даст генератору случайных чисел больше возможностей получить достаточное количество энтропии.

gpg: /home/enon/.gnupg/trustdb.gpg: создана таблица доверия

gpg: ключ 735CE2CBBE6D9307 помечен как абсолютно доверенный

gpg: создан каталог '/home/enon/.gnupg/openpgp-revocs.d'

gpg: сертификат отзыва записан в '/home/enon/.gnupg/openpgp-revocs.d/1C8D9401D47147DB9F844C7E735CE2CBBE6D9307.rev'.

открытый и секретный ключи созданы и подписаны.

```
pub  rsa2048 2020-11-04 [SC]
     1C8D9401D47147DB9F844C7E735CE2CBBE6D9307
uid                               istinlih
sub  rsa2048 2020-11-04 [E]
```

enon@kali:~\$

2.1 Создание пары ключей (впоследствии uid сменено на orwell)

enon@kali: ~

Файл Действия Правка Вид Справка

доверие: неизвестно достоверность: неизвестно

sub rsa2048/318584C940DBB1DF

создан: 2020-11-04

годен до: никогда

назначение: E

[неизвестно] (1). misha

gpg> trust

pub rsa2048/57EC564D4E204C48

создан: 2020-11-04

годен до: никогда

назначение: SC

доверие: неизвестно достоверность: неизвестно

sub rsa2048/318584C940DBB1DF

создан: 2020-11-04

годен до: никогда

назначение: E

[неизвестно] (1). misha

Укажите, насколько Вы доверяете данному пользователю в вопросах проверки достоверности ключей других пользователей (проверяет паспорт, сверяет отпечатки ключей из разных источников и т.п.)

1 = Не знаю или не буду отвечать

2 = НЕ доверяю

3 = Доверяю ограниченно

4 = Полностью доверяю

5 = Абсолютно доверяю

m = вернуться в главное меню

Ваше решение? 5

Вы действительно хотите сделать этот ключ абсолютно доверенным? (y/N) y

pub rsa2048/57EC564D4E204C48

создан: 2020-11-04

годен до: никогда

назначение: SC

доверие: абсолютное достоверность: неизвестно

sub rsa2048/318584C940DBB1DF

создан: 2020-11-04

годен до: никогда

назначение: E

[неизвестно] (1). misha

Учтите, что показанная достоверность ключа может быть неверной, пока Вы не перезапустите программу.

gpg>

gpg: signal Interrupt caught ... exiting

enon@kali:~\$ gpg -e -r misha test

gpg: проверка таблицы доверия

gpg: marginals needed: 3 completes needed: 1 trust model: pgp

gpg: глубина: 0 достоверных: 4 подписанных: 0 доверие: 0-, 0q, 0n, 0m, 0f, 4u

gpg: срок следующей проверки таблицы доверия 2020-11-18

enon@kali:~\$ █

2.2 Импорт полученного ключа и зашифровка файла

```

Файл Действия Правка Вид Справка
m = вернуться в главное меню
Ваше решение? 5
Вы действительно хотите сделать этот ключ абсолютно доверенным? (y/N) y
pub rsa2048/F7EFFF3EAAD996E6
    создан: 2020-11-04    годеи до: никогда    назначение: SC
    доверие: абсолютное доверенность: неизвестно
sub rsa2048/F7FA8BB8BE1C2F52
    создан: 2020-11-04    годеи до: никогда    назначение: E
[ неизвестно ] (1). misha1
Учтите, что показанная доверенность ключа может быть неверной,
пока Вы не перезапустите программу.
gpg>
gpg: signal Interrupt caught ... exiting
enon@kali:~$ gpg -e -r misha1 testfile
gpg: проверка таблицы доверия
gpg: marginals needed: 3 completes needed: 1 trust model: pgp
gpg: глубина: 0 доверенных: 6 подписанных: 0 доверие: 0-, 0q, 0n, 0m, 0f, 6u
gpg: срок следующей проверки таблицы доверия 2020-11-18
enon@kali:~$ gpg -d fayl1.gpg
gpg: зашифровано 2048-битным ключом RSA с идентификатором EAF9F0BA7FE948C4, созданным 2020-11-04
"orwell"
Николаев М В Басо 03 20
enon@kali:~$

```

2.3 Успешная расшифровка переданного файла

Действия Правка Вид Справка

напо 4.9.3
ih0

testfile

Устройства

файловая систе...

Закладки

Рабочий стол

Корзина

Документы

Музыка

Изображения

Видео

Загрузки

Сеть

Обзор сети



qr



group.sha1



Istirlin

daniat.neizvestno
@gmail.com
(0xD16A3B6BAE2
0BE7C).pub.asc



key.asc



Notgroup.sha1



testfile



testfile.gpg



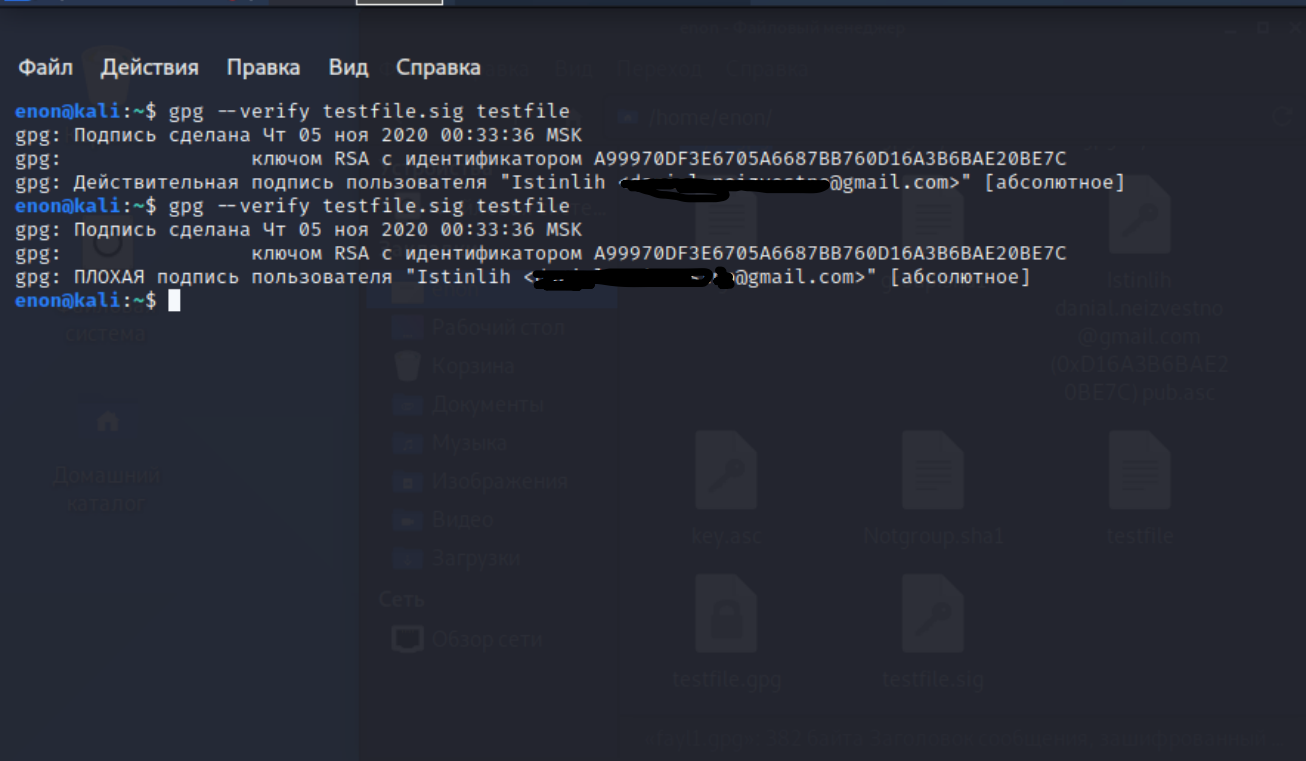
testfile.sig

Full gpg, as I have to make a test file, and I have to make

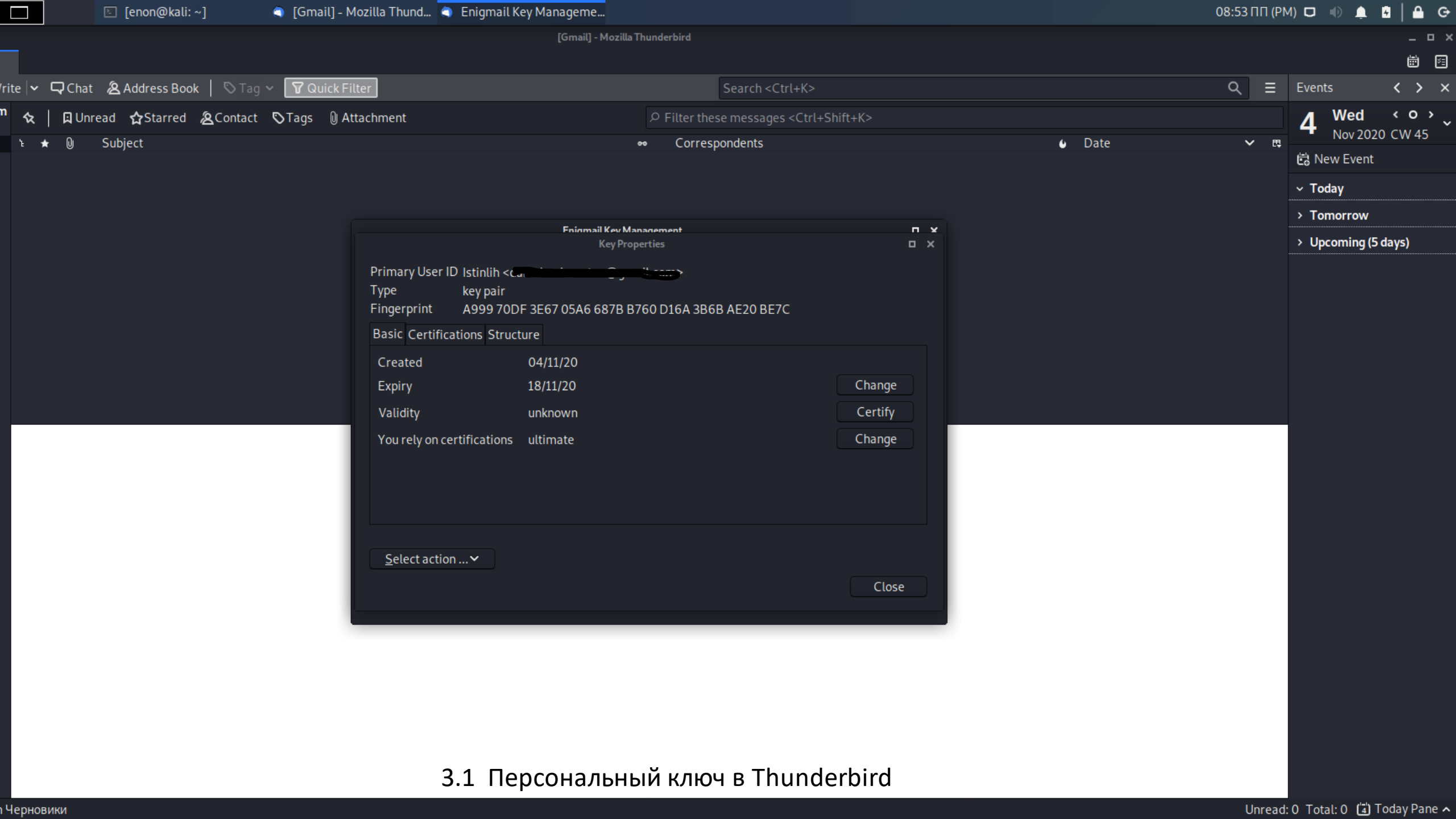
modified buffer?

Отмена

2.4 Изменение подписанного файла



2.5 Проверка подписи до и после изменения



3.1 Персональный ключ в Thunderbird

keys.openpgp.org

この鍵A99970DF3E6705A6687BB760D16A3B6BAE20BE7Cをあなたはアップロードしました。

アイデンティティではない情報だけでこの鍵は公開されました。(どういう意味か?)

メールアドレスでの検索で鍵が利用できるようにするために、そのメールアドレスがあなたのものであることを検証することができます。

daniel.noizawa@gmail.com

検証を出願中です。

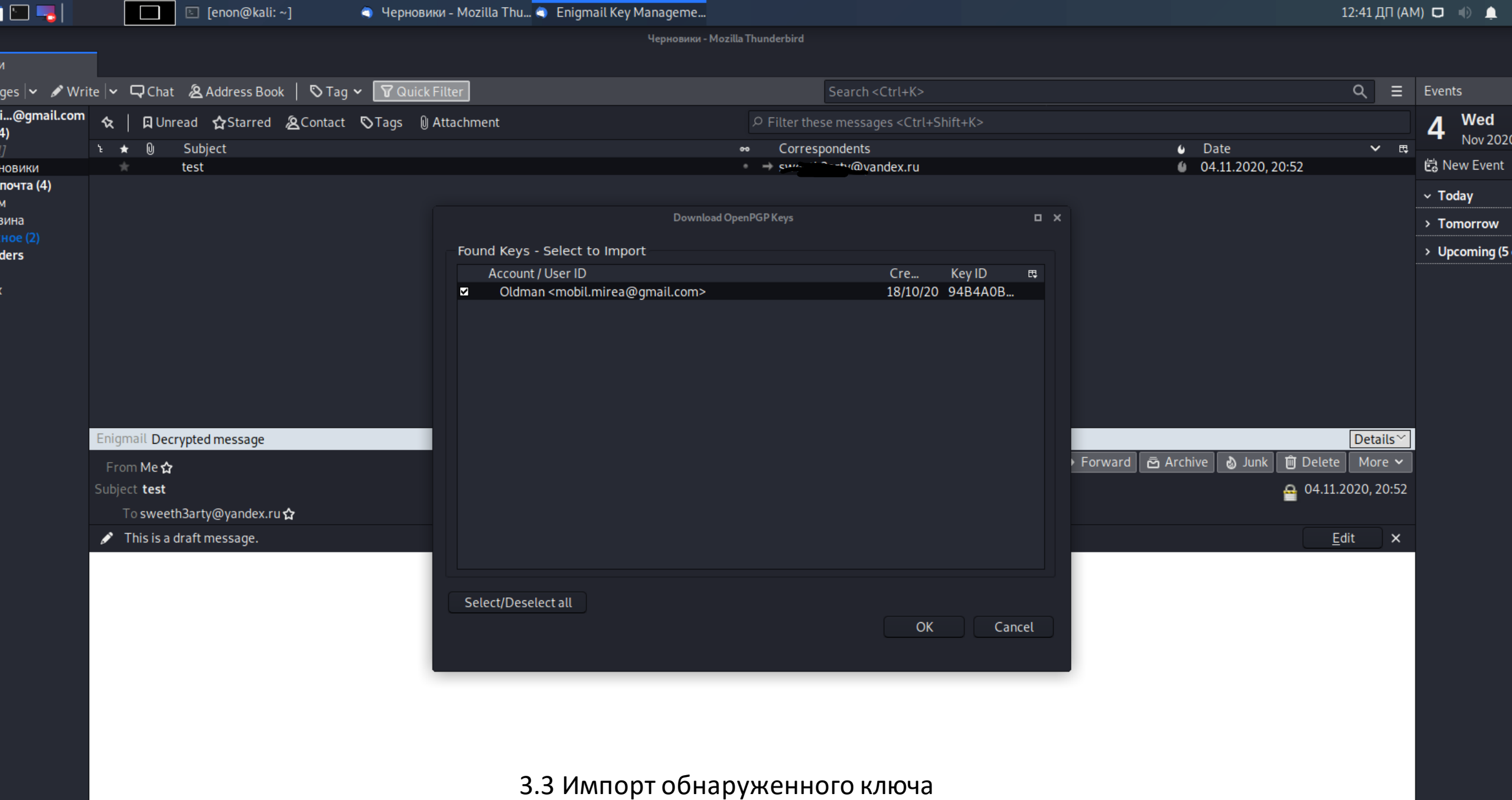
注意: 迷惑メール防止のために、プロバイダは15分ほどメールを遅らせることがあります。しばらくお待ちください。

Hagrid vUNKNOWN、以下でビルドされました 149a698

Sequoia-PGPで動いています

背景の画像はSubtle Patterns からCC BY-SA 3.0のもとで取得されました。

3.2 Загрузка в репозиторий ключа



3.3 Импорт обнаруженного ключа