

student: Копытов Василий Геннадьевич seminar # 1

1) Сделать chroot для /bin/bash и перенести в новый корень программу ls

```
PS C:\Users\Gregorian> ssh -p 8022 gregorian@localhost
gregorian@localhost's password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.19.0-43-generic x86_64)
```

```
* Documentation: https://help.ubuntu.com
* Management:   https://landscape.canonical.com
* Support:      https://ubuntu.com/advantage
```

Расширенное поддержание безопасности (ESM) для Applications выключено.
0 обновлений может быть применено немедленно.
Включите ESM Apps для получения дополнительных будущих обновлений безопасности.
Смотрите <https://ubuntu.com/esm> или выполните: `sudo pro status`

The list of available updates is more than a week old.

To check for new updates run: `sudo apt update`

Last login: Sun Jun 4 20:11:34 2023 from 10.0.2.2

```
gregorian@gregorian-VirtualBox:~$ mkdir HT1
```

```
gregorian@gregorian-VirtualBox:~$ mkdir HT1/bin
```

```
gregorian@gregorian-VirtualBox:~$ cp /bin/bash HT1/bin
```

```
gregorian@gregorian-VirtualBox:~$ ldd /bin/bash
```

```
linux-vdso.so.1 (0x00007fffabfd3000)
```

```
libtinfo.so.6 => /lib/x86_64-linux-gnu/libtinfo.so.6 (0x00007f40b7a15000)
```

```
libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f40b7600000)
```

```
/lib64/ld-linux-x86-64.so.2 (0x00007f40b7bb8000)
```

```
gregorian@gregorian-VirtualBox:~$ mkdir HT1/lib
```

```
gregorian@gregorian-VirtualBox:~$ mkdir HT1/lib64
```

```
gregorian@gregorian-VirtualBox:~$ cp /lib/x86_64-linux-gnu/libtinfo.so.6 HT1/lib
```

```
gregorian@gregorian-VirtualBox:~$ cp /lib/x86_64-linux-gnu/libc.so.6 HT1/lib
```

(создаем новую директорию)

(создаем папку bin для копирования bin/bash)

(копируем bin/bash)

(вызываем содержание библиотек)

(создаем директорию для первой библиотеки)

(создаем директорию для второй библиотеки)

(копируем файлы первой библиотеки)

(копируем файлы второй библиотеки)

```
gregorian@gregorian-VirtualBox:~$ cp /lib64/ld-linux-x86-64.so.2 HT1/lib64
gregorian@gregorian-VirtualBox:~$ whereis ls
ls: /usr/bin/ls /usr/share/man/man1/ls.1.gz
gregorian@gregorian-VirtualBox:~$ mkdir HT1/usr/bin
```

(копируем файлы второй библиотеки)
(Узнаем, где лежит ls)

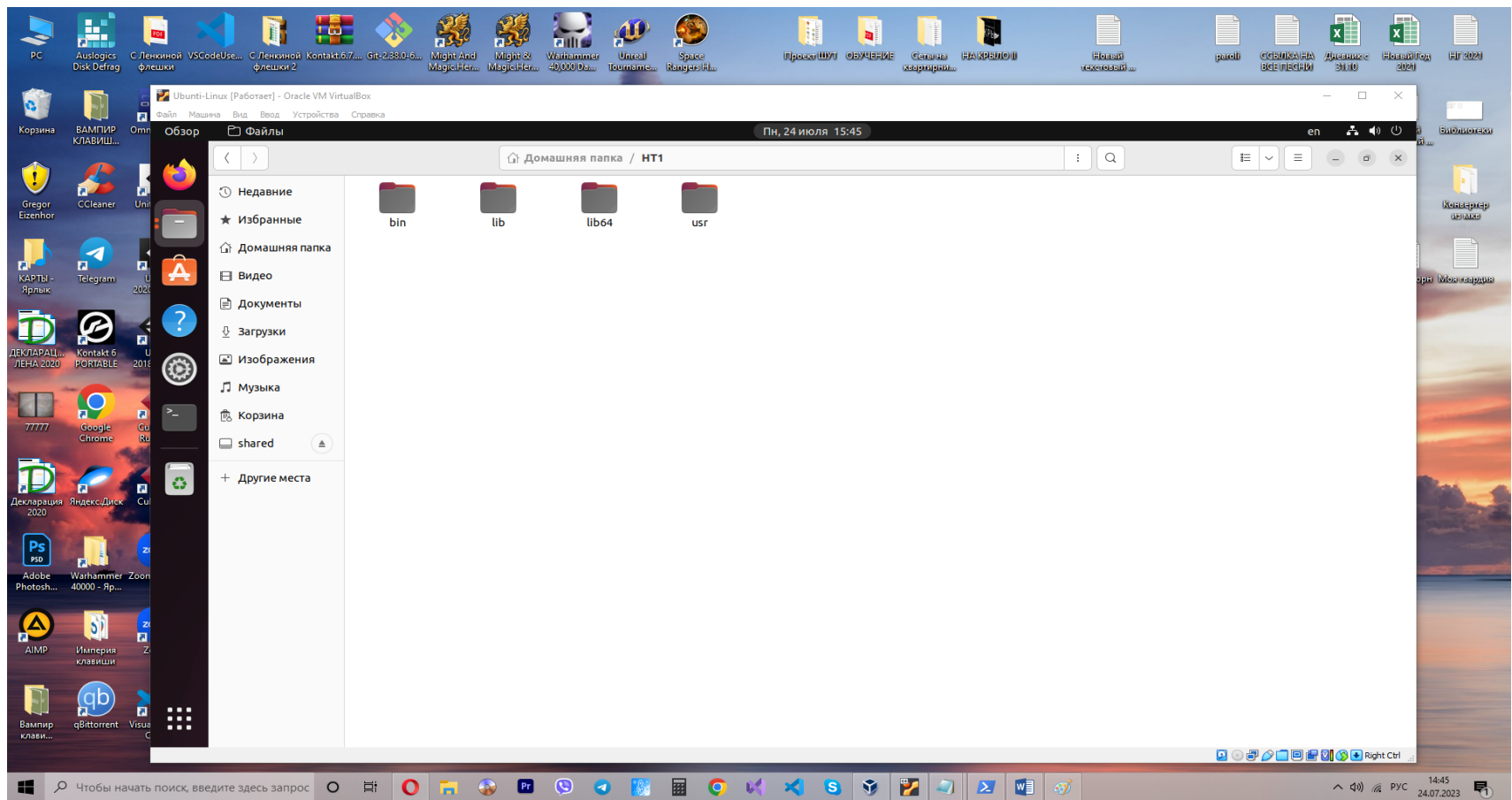
(Создаем новую директорию под ls в HT1)

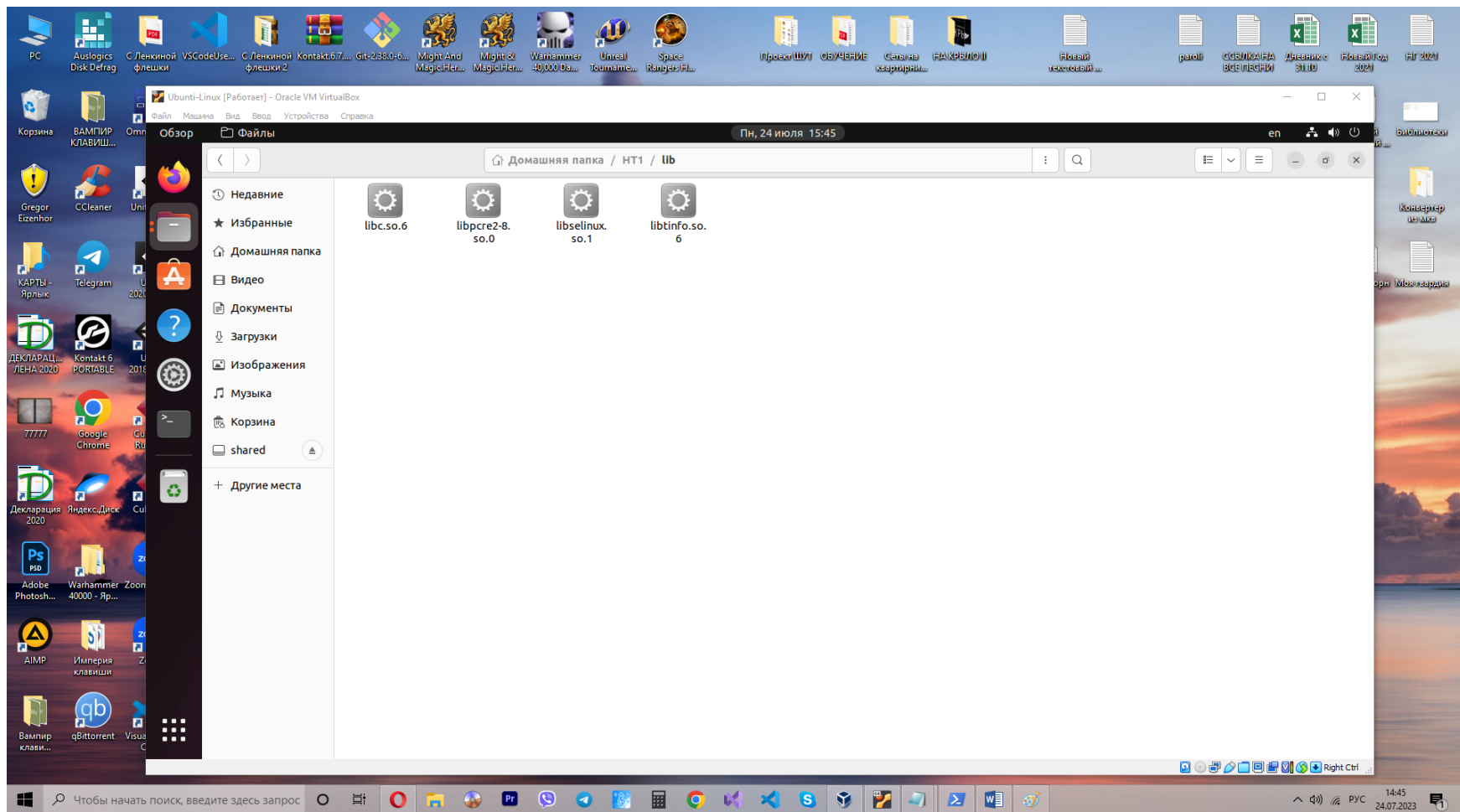
```
gregorian@gregorian-VirtualBox:~$ cp /usr/bin/ls HT1/usr/bin
gregorian@gregorian-VirtualBox:~$ ldd /usr/bin/ls
linux-vdso.so.1 (0x00007ffc75b11000)
libselinux.so.1 => /lib/x86_64-linux-gnu/libselinux.so.1 (0x00007f7aefd98000)
libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f7aefa00000)
libpcre2-8.so.0 => /lib/x86_64-linux-gnu/libpcre2-8.so.0 (0x00007f7aefd01000)
/lib64/ld-linux-x86-64.so.2 (0x00007f7aefdf8000)
gregorian@gregorian-VirtualBox:~$ cp /lib/x86_64-linux-gnu/libselinux.so.1 HT1/lib
gregorian@gregorian-VirtualBox:~$ cp /lib/x86_64-linux-gnu/libc.so.6 HT1/lib
gregorian@gregorian-VirtualBox:~$ cp /lib/x86_64-linux-gnu/libpcre2-8.so.0 HT1/lib
gregorian@gregorian-VirtualBox:~$ sudo chroot HT1 /bin/bash
bash-5.1# ls
bin lib lib64 usr
bash-5.1#
```

(Копируем исполняемые файлы ls)

(Выполняем chroot)

(Проверяем выполнение ls)





2) Повторить последовательность команд с ip как на семинаре

```
gregorian@gregorian-VirtualBox:~$ sudo ip netns add testns123
[sudo] пароль для gregorian:
gregorian@gregorian-VirtualBox:~$ sudo ip netns list
testns123
gregorian@gregorian-VirtualBox:~$ sudo ip netns exec testns123 bash
root@gregorian-VirtualBox:/home/gregorian# ip a
1: lo: <LOOPBACK> mtu 65536 qdisc noop state DOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
gregorian@gregorian-VirtualBox:~$ sudo ip link add veth0 type veth peer name veth1
[sudo] пароль для gregorian:
gregorian@gregorian-VirtualBox:~$ sudo ip link set veth1 netns testns123
gregorian@gregorian-VirtualBox:~$ sudo ip addr add 10.0.0.1/24 dev veth0
gregorian@gregorian-VirtualBox:~$ sudo ip link set dev veth0 up
root@gregorian-VirtualBox:/home/gregorian# ip addr add 10.0.0.2/24 dev veth1
root@gregorian-VirtualBox:/home/gregorian# ip link set dev veth1 up
root@gregorian-VirtualBox:/home/gregorian# ip a
1: lo: <LOOPBACK> mtu 65536 qdisc noop state DOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
4: veth1@if5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether f2:26:48:69:2d:12 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.0.0.2/24 scope global veth1
        valid_lft forever preferred_lft forever
    inet6 fe80::f026:48ff:fe69:2d12/64 scope link
        valid_lft forever preferred_lft forever
gregorian@gregorian-VirtualBox:~$ ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=0.104 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.071 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=0.075 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=0.073 ms
64 bytes from 10.0.0.2: icmp_seq=5 ttl=64 time=0.071 ms
```

```
64 bytes from 10.0.0.2: icmp_seq=6 ttl=64 time=0.074 ms
64 bytes from 10.0.0.2: icmp_seq=7 ttl=64 time=0.054 ms
^[64 bytes from 10.0.0.2: icmp_seq=8 ttl=64 time=0.072 ms
64 bytes from 10.0.0.2: icmp_seq=9 ttl=64 time=0.079 ms
^[64 bytes from 10.0.0.2: icmp_seq=10 ttl=64 time=0.073 ms
^C
--- 10.0.0.2 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9222ms
rtt min/avg/max/mdev = 0.054/0.074/0.104/0.011 ms
root@gregorian-VirtualBox:/home/gregorian# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=0.109 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=0.080 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=0.081 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=64 time=0.074 ms
^C
--- 10.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3041ms
rtt min/avg/max/mdev = 0.074/0.086/0.109/0.013 ms
```

3) Повторить последовательность команд с unshare как на семинаре.

```
gregorian@gregorian-VirtualBox:~$ sudo unshare --net /bin/bash
[sudo] пароль для gregorian:
root@gregorian-VirtualBox:/home/gregorian# ip a
1: lo: <LOOPBACK> mtu 65536 qdisc noop state DOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
root@gregorian-VirtualBox:/home/gregorian# ls -l /proc/$$/ns
итого 0
lrwxrwxrwx 1 root root 0 июл 24 21:48 cgroup -> 'cgroup:[4026531835]'
lrwxrwxrwx 1 root root 0 июл 24 21:48 ipc -> 'ipc:[4026531839]'
lrwxrwxrwx 1 root root 0 июл 24 21:48 mnt -> 'mnt:[4026531841]'
lrwxrwxrwx 1 root root 0 июл 24 21:48 net -> 'net:[4026532323]'
lrwxrwxrwx 1 root root 0 июл 24 21:48 pid -> 'pid:[4026531836]'
lrwxrwxrwx 1 root root 0 июл 24 21:48 pid_for_children -> 'pid:[4026531836]'
lrwxrwxrwx 1 root root 0 июл 24 21:48 time -> 'time:[4026531834]'
lrwxrwxrwx 1 root root 0 июл 24 21:48 time_for_children -> 'time:[4026531834]'
lrwxrwxrwx 1 root root 0 июл 24 21:48 user -> 'user:[4026531837]'
lrwxrwxrwx 1 root root 0 июл 24 21:48 uts -> 'uts:[4026531838]'
root@gregorian-VirtualBox:/home/gregorian# exit
exit
gregorian@gregorian-VirtualBox:~$ sudo unshare --pid --net --fork --mount-proc /bin/bash
root@gregorian-VirtualBox:/home/gregorian# ls -l /proc/$$/ns
итого 0
lrwxrwxrwx 1 root root 0 июл 24 21:51 cgroup -> 'cgroup:[4026531835]'
lrwxrwxrwx 1 root root 0 июл 24 21:51 ipc -> 'ipc:[4026531839]'
lrwxrwxrwx 1 root root 0 июл 24 21:51 mnt -> 'mnt:[4026532323]'
lrwxrwxrwx 1 root root 0 июл 24 21:51 net -> 'net:[4026532325]'
lrwxrwxrwx 1 root root 0 июл 24 21:51 pid -> 'pid:[4026532324]'
lrwxrwxrwx 1 root root 0 июл 24 21:51 pid_for_children -> 'pid:[4026532324]'
lrwxrwxrwx 1 root root 0 июл 24 21:51 time -> 'time:[4026531834]'
lrwxrwxrwx 1 root root 0 июл 24 21:51 time_for_children -> 'time:[4026531834]'
lrwxrwxrwx 1 root root 0 июл 24 21:51 user -> 'user:[4026531837]'
```

```
lrwxrwxrwx 1 root root 0 июл 24 21:51 uts -> 'uts:[4026531838]'
gregorian@gregorian-VirtualBox:~$ ls -l /proc/$$/ns
итого 0
lrwxrwxrwx 1 gregorian gregorian 0 июл 24 21:55 cgroup -> 'cgroup:[4026531835]'
lrwxrwxrwx 1 gregorian gregorian 0 июл 24 21:55 ipc -> 'ipc:[4026531839]'
lrwxrwxrwx 1 gregorian gregorian 0 июл 24 21:55 mnt -> 'mnt:[4026531841]'
lrwxrwxrwx 1 gregorian gregorian 0 июл 24 21:55 net -> 'net:[4026531840]'
lrwxrwxrwx 1 gregorian gregorian 0 июл 24 21:55 pid -> 'pid:[4026531836]'
lrwxrwxrwx 1 gregorian gregorian 0 июл 24 21:55 pid_for_children -> 'pid:[4026531836]'
lrwxrwxrwx 1 gregorian gregorian 0 июл 24 21:55 time -> 'time:[4026531834]'
lrwxrwxrwx 1 gregorian gregorian 0 июл 24 21:55 time_for_children -> 'time:[4026531834]'
lrwxrwxrwx 1 gregorian gregorian 0 июл 24 21:55 user -> 'user:[4026531837]'
lrwxrwxrwx 1 gregorian gregorian 0 июл 24 21:55 uts -> 'uts:[4026531838]'
gregorian@gregorian-VirtualBox:~$ sudo unshare --pid --net --fork --mount-proc /bin/bash
root@gregorian-VirtualBox:/home/gregorian# ls -l /proc/$$/ns
итого 0
lrwxrwxrwx 1 root root 0 июл 24 21:56 cgroup -> 'cgroup:[4026531835]'
lrwxrwxrwx 1 root root 0 июл 24 21:56 ipc -> 'ipc:[4026531839]'
lrwxrwxrwx 1 root root 0 июл 24 21:56 mnt -> 'mnt:[4026532323]'
lrwxrwxrwx 1 root root 0 июл 24 21:56 net -> 'net:[4026532325]'
lrwxrwxrwx 1 root root 0 июл 24 21:56 pid -> 'pid:[4026532324]'
lrwxrwxrwx 1 root root 0 июл 24 21:56 pid_for_children -> 'pid:[4026532324]'
lrwxrwxrwx 1 root root 0 июл 24 21:56 time -> 'time:[4026531834]'
lrwxrwxrwx 1 root root 0 июл 24 21:56 time_for_children -> 'time:[4026531834]'
lrwxrwxrwx 1 root root 0 июл 24 21:56 user -> 'user:[4026531837]'
lrwxrwxrwx 1 root root 0 июл 24 21:56 uts -> 'uts:[4026531838]'
```