REMOTE ACQUISITION BOOT ENVIRONMENT (RABE)

BOOTABLE LINUX CD / PXE FOR THE REMOTE ACQUISITION OF MULTIPLE COMPUTERS

DENNIS CORTJENS

UVA | SNE | RP2

NFI

AGENDA

- Introduction
- Research
- Concepts
- Goals
- Implementation
- Testing
- Results / Conclusion
- Future research

Sheets:	20
Duration:	15 minutes
Questions:	after presentation

INTRODUCTION

- large IT infrastructures > companies, data centers, universities
- multiple computers / servers
- time consuming > disassembling each computer
- Netherlands Forensic Institute > 1 project > 3 research projects:
  1. Bootable Linux CD / PXE for the remote acquisition of multiple computers > Dennis
  2. Acquisition server > Eric
  3. Triage software

RESEARCH

- question:

  Can a bootable Linux CD / PXE be build for the remote acquisition of multiple computers and how does it perform compared to the traditional method?

- hypothesis:

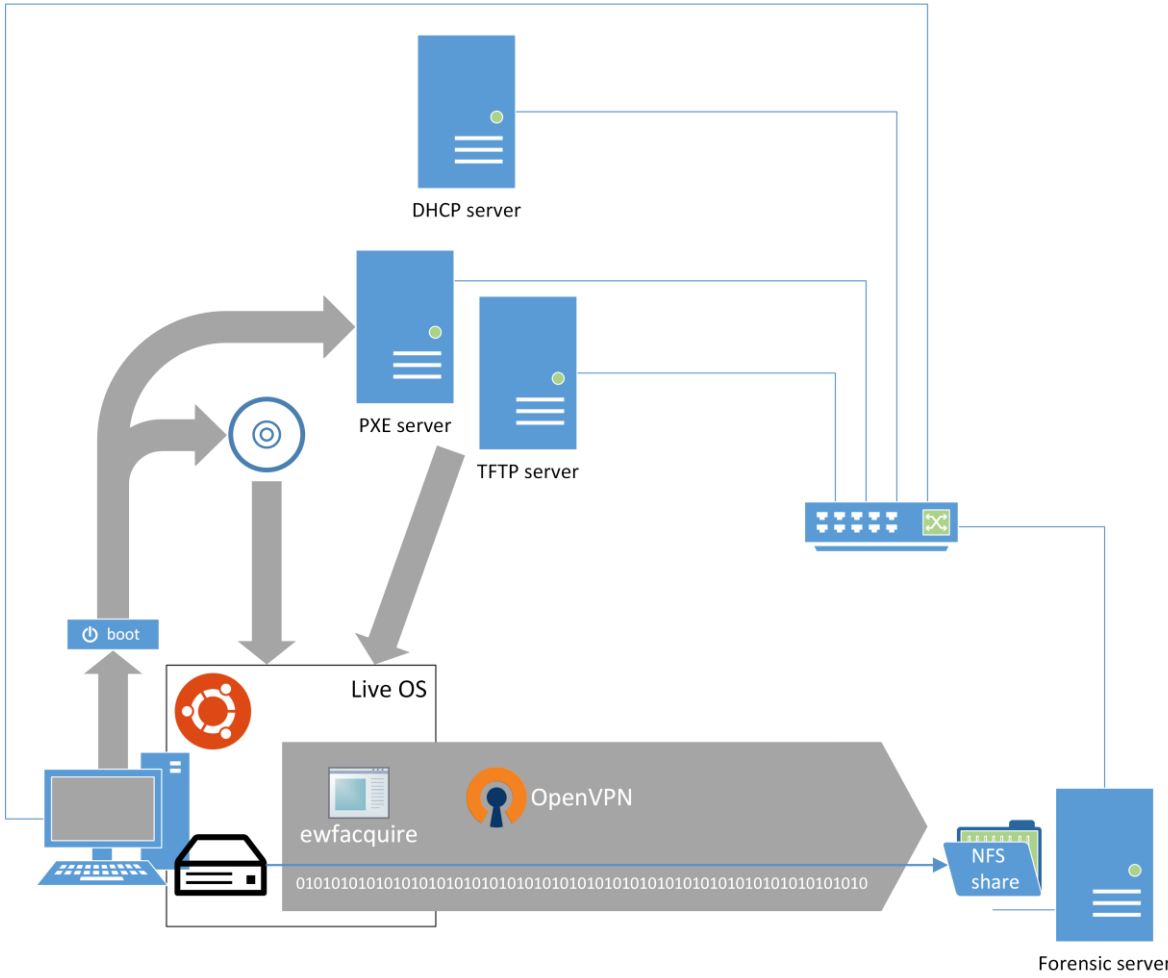
  The remote acquisition of multiple computers (in general) is slower then the traditional method and across the internet it is slower then across a LAN. However, if the acquisition is performed remotely without being on location, it can be done parallel to other activities. This could make it a time efficient solution for partial and sparse acquisition in the future.

- previous research:

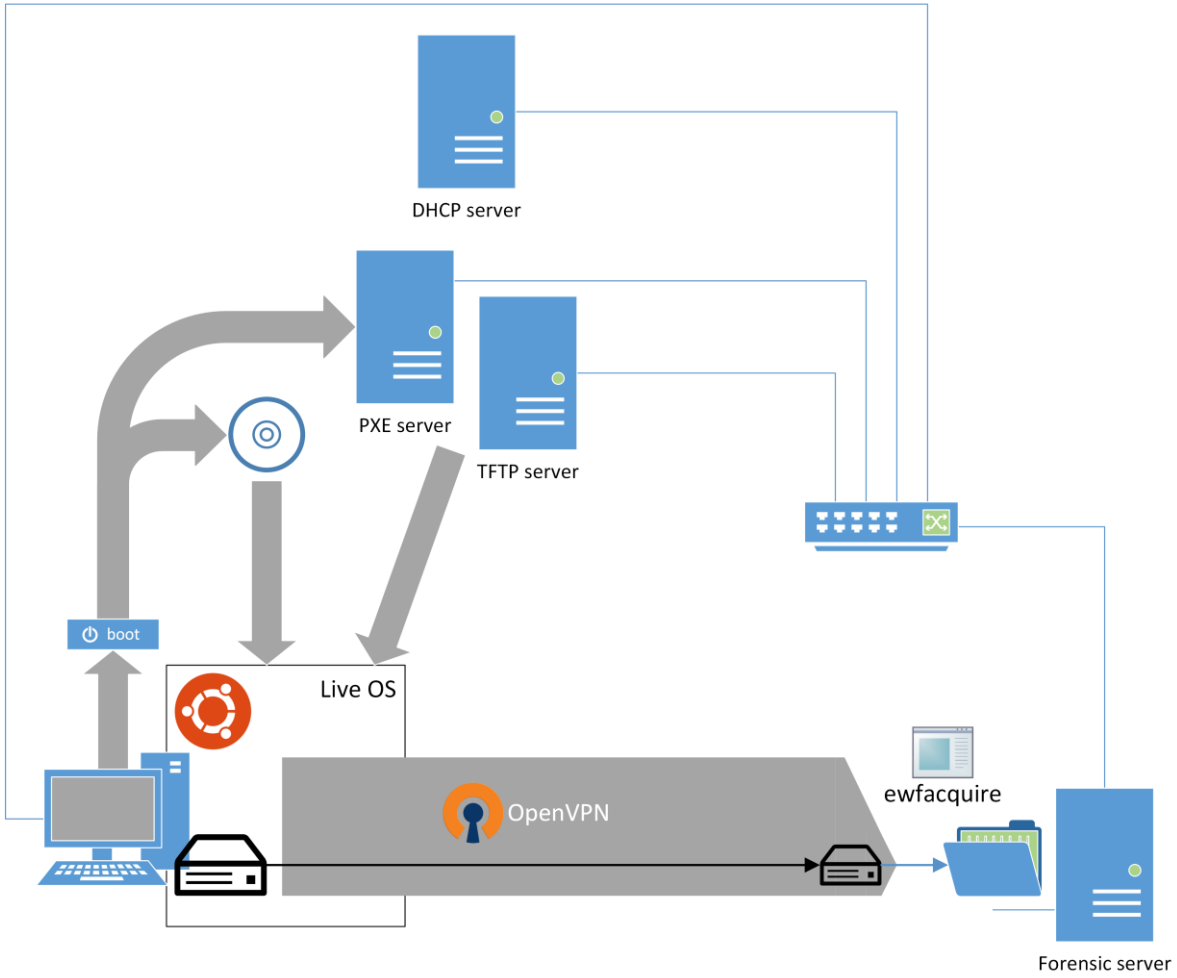
  Automated Network Triage (ANT)

  Martin B. Koopmans, Joshua I. James | University College Dublin

CONCEPTS – NFS



CONCEPTS – iSCSI

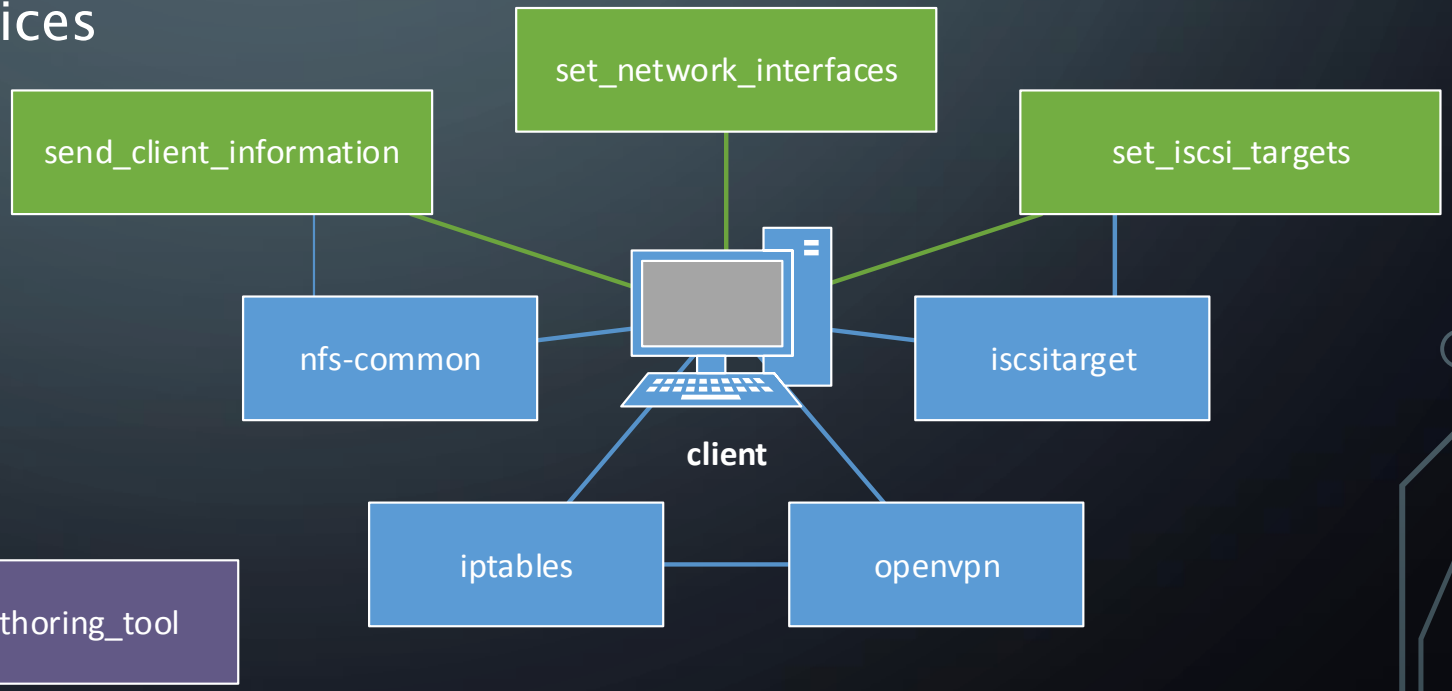


GOALS

- creating a working (iSCSI) concept:
  - live image > optical disc / USB stick / PXE
  - authoring tool > configuring live image
- testing the hypothesis:
  - performance NFS vs. iSCSI
  - remote vs. traditional acquisition
- focus:
  - client side
  - working concept > basic server side

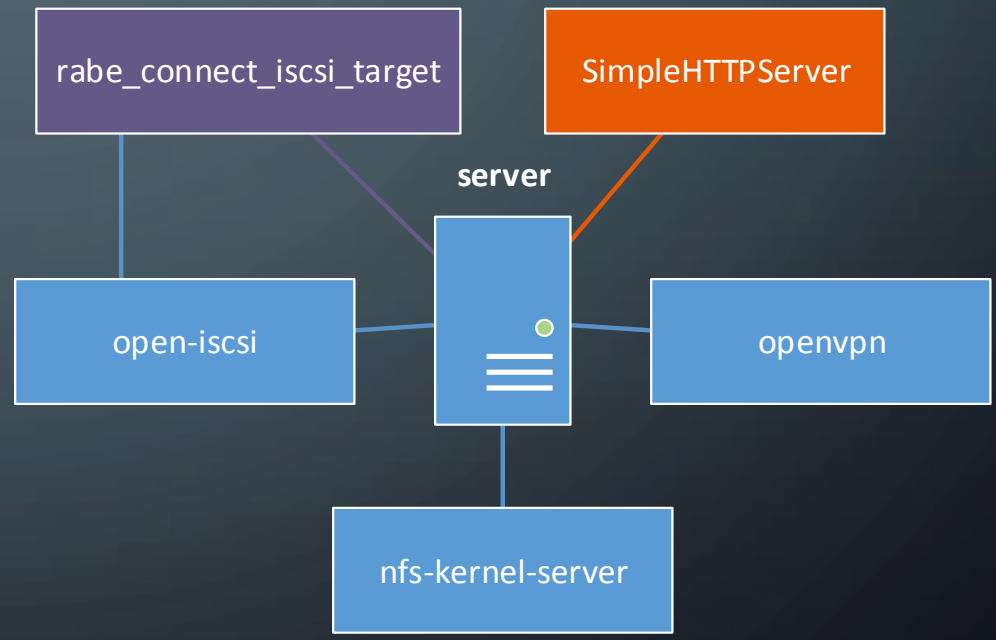
IMPLEMENTATION – Client

- live image:
  - KNOPPIX 7.2.0 vs. Ubuntu Desktop 14.04
  - packages and new services
  - secure connection
  - forensic soundness
- authoring tool:
  - bash script
  - remastering live image

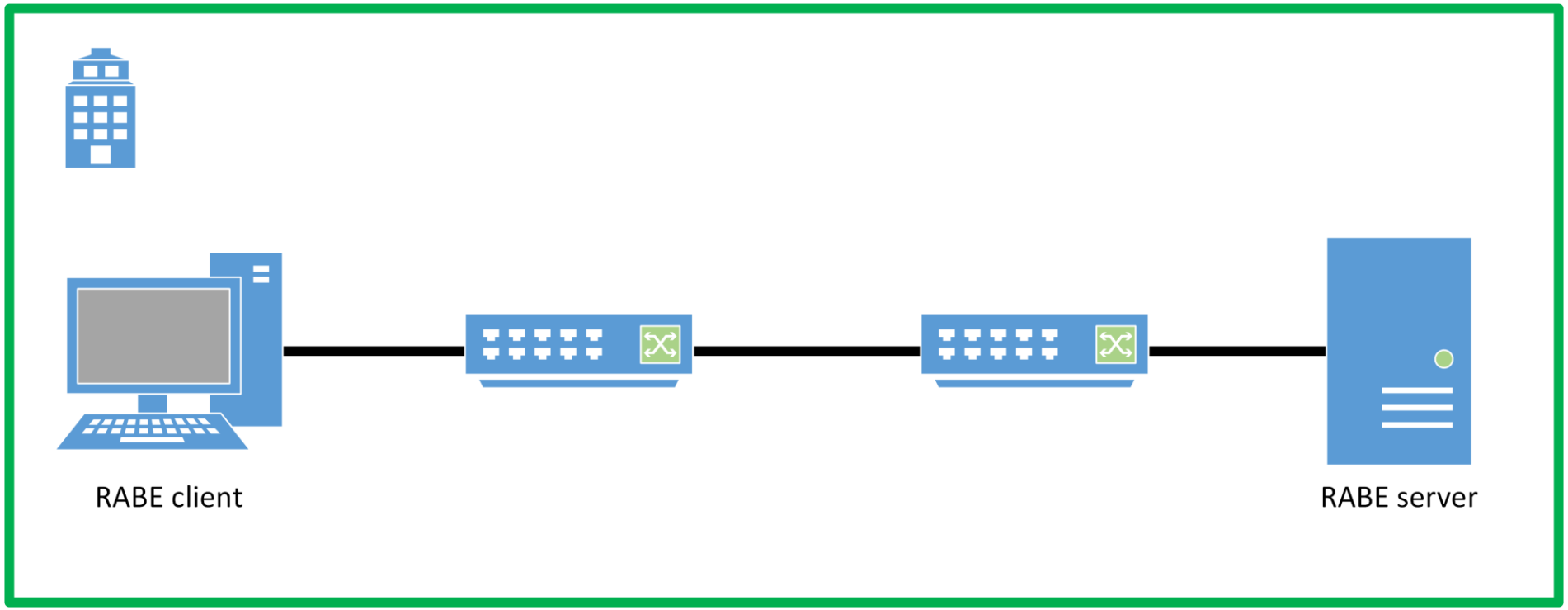


IMPLEMENTATION – Server

- not in initial scope
- needed for working concept
- configuration:
  - Ubuntu Desktop 14.04
  - packages
  - secure connection
  - web service > python
  - bash script > connecting iSCSI targets



TESTING – LAN



TESTING - LAN

iSCSI:

```
   Written: 9.3 GiB (10000000188 bytes) in 15 minute(s) and 30 second(s) with 10 MiB/s (10752688 bytes/second).
#1 MD5 hash calculated over data:              d1bac32b46721780b314f170058e6db5
   ewfacquire: SUCCESS

   Written: 9.3 GiB (10000000188 bytes) in 14 minute(s) and 15 second(s) with 11 MiB/s (11695906 bytes/second).
#2 MD5 hash calculated over data:              d1bac32b46721780b314f170058e6db5
   ewfacquire: SUCCESS

   Written: 9.3 GiB (10000000188 bytes) in 15 minute(s) and 30 second(s) with 10 MiB/s (10752688 bytes/second).
#3 MD5 hash calculated over data:              d1bac32b46721780b314f170058e6db5
   ewfacquire: SUCCESS
```

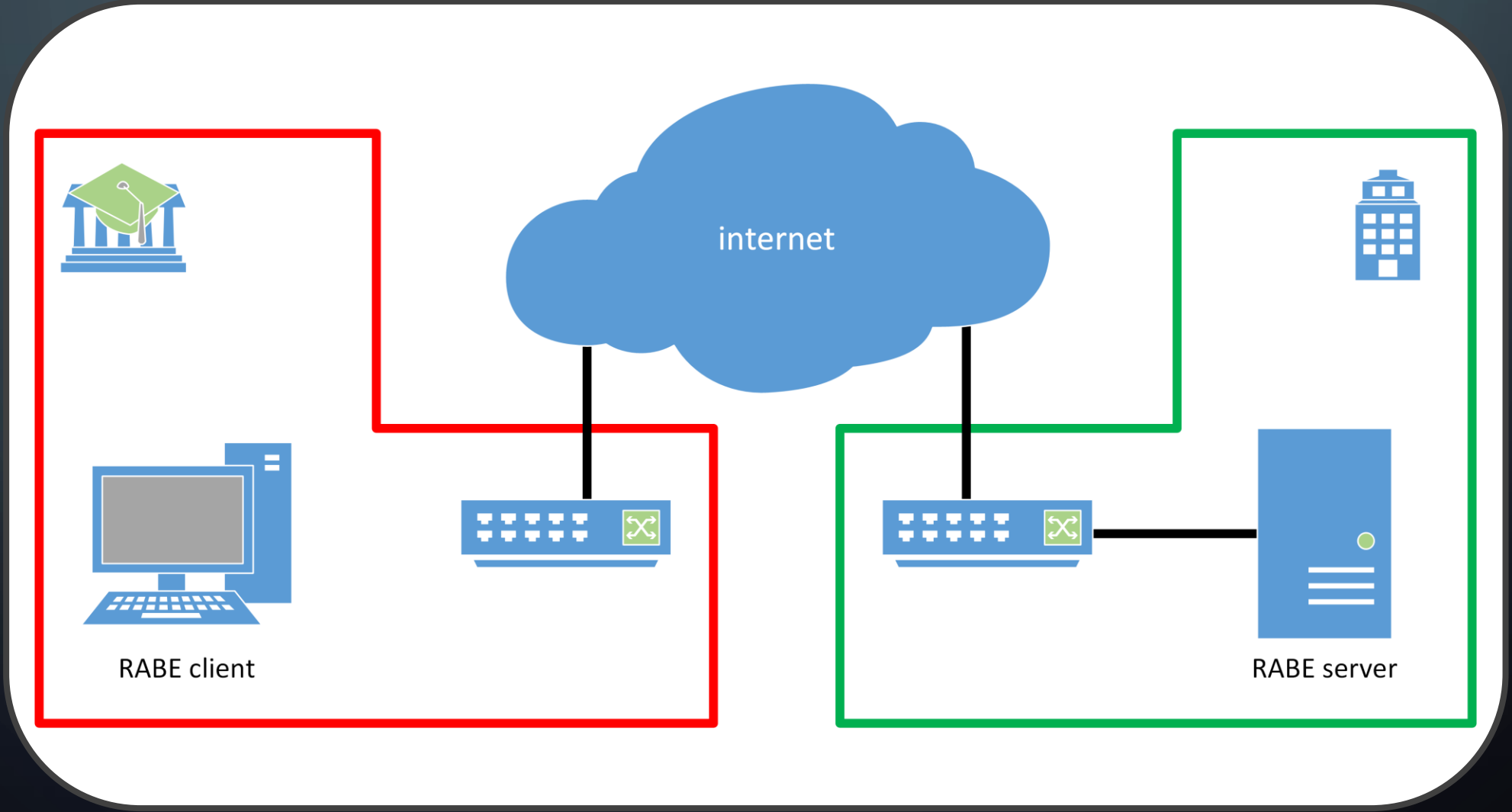
NFS:

```
   Written: 9.3 GiB (10000000188 bytes) in 17 minute(s) and 0 second(s) with 9.3 MiB/s (9803921 bytes/second).
#1 MD5 hash calculated over data:              d1bac32b46721780b314f170058e6db5
   ewfacquire: SUCCESS

   Written: 9.3 GiB (10000000188 bytes) in 15 minute(s) and 38 second(s) with 10 MiB/s (10660981 bytes/second).
#2 MD5 hash calculated over data:              d1bac32b46721780b314f170058e6db5
   ewfacquire: SUCCESS

   Written: 9.3 GiB (10000000188 bytes) in 17 minute(s) and 4 second(s) with 9.3 MiB/s (9765625 bytes/second).
#3 MD5 hash calculated over data:              d1bac32b46721780b314f170058e6db5
   ewfacquire: SUCCESS
```

TESTING – internet



```
TESTING - internet

iSCSI:

    Written: 9.3 GiB (10000000188 bytes) in 2 hour(s), 13 minute(s) and 39 second(s) with 1.1 MiB/s (1247038
#1  bytes/second).
    MD5 hash calculated over data:              0c27b2131c240fa88ceeab132ca326d0
    ewfacquire: SUCCESS

NFS:

    Written: 9.3 GiB (10000000188 bytes) in 2 hour(s), 22 minute(s) and 6 second(s) with 1.1 MiB/s (1172882
#1  bytes/second).
    MD5 hash calculated over data:              d1b749285de3e6ec69537fb1212b4dd0
    ewfacquire: SUCCESS
```

RESULTS / CONCLUSION

- live image & authoring tool
- NFS vs. iSCSI:
  - LAN: iSCSI faster 0.7–1.0 MiB/s (VPN overhead)
  - internet: iSCSI faster 8 minutes and 27 seconds (same speed 1.1 MiB/s)
- hypothesis:
  - correct, but with some side notes
  - speed > network and internet connection limitation
  - takes much longer > ± 29 hours (LAN) / ± 244 hours (internet)
  - partial and sparse acquisition

CONCLUSION / SUMMARY

“ this concept is a theoretical solution for the remote acquisition of multiple computers and will not yet succeed the traditional acquisition method, but could be a solution for partial or sparse acquisition in the near future ”

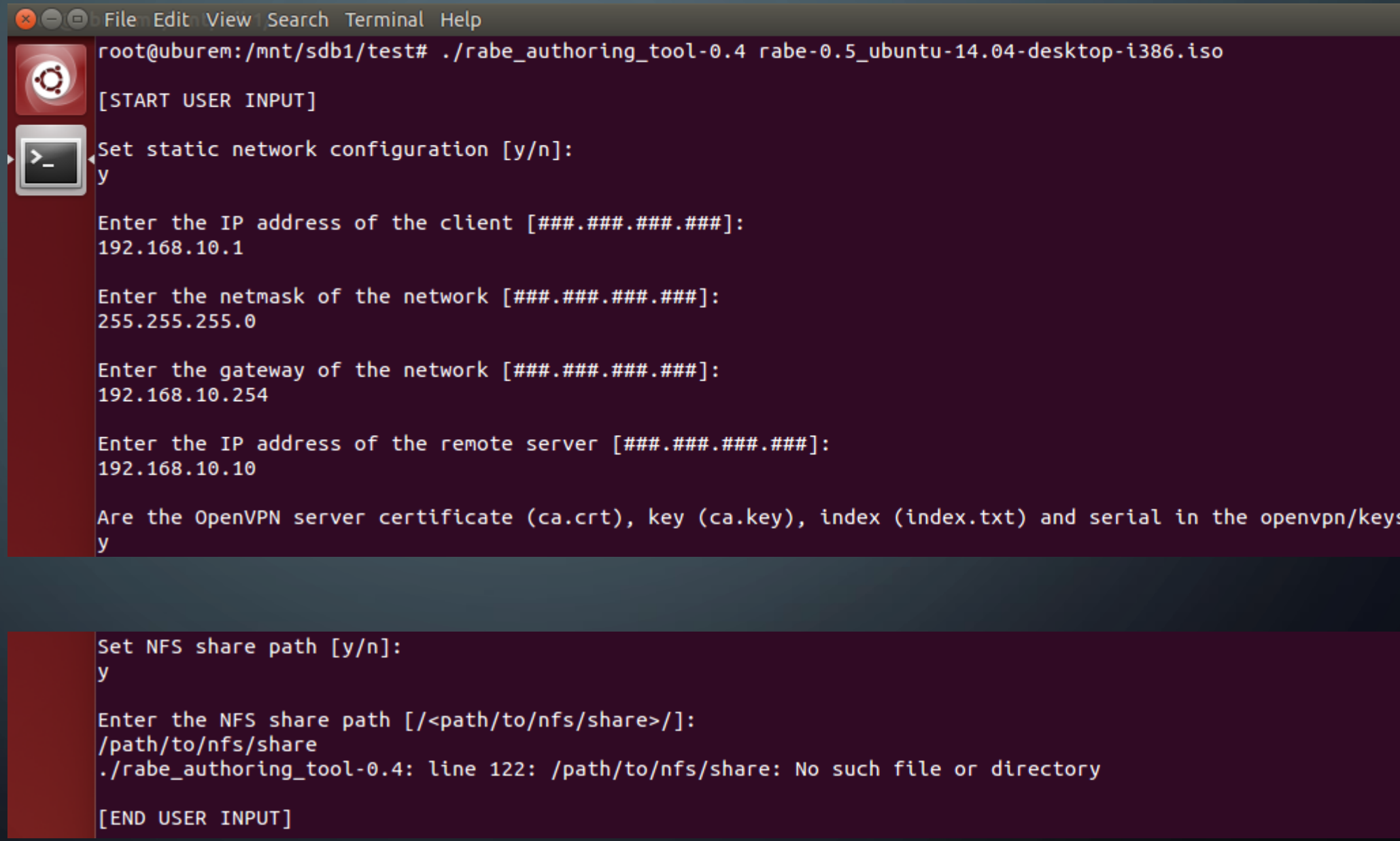
- created working concept
- live image & authoring tool
- concluded on NFS vs. iSCSI
- open framework for future research

FUTURE RESEARCH

- live image:
  - disable auto-mounting
  - reduce size
  - remove GUI
- authoring tool:
  - chroot hopping
- further performance testing

- forensics:
  - disable auto-mounting
  - reduce memory footprint
  - include memory acquisition
  - other tools?
  - preview / triage mode > copy-on-read (Eric)

DEMO

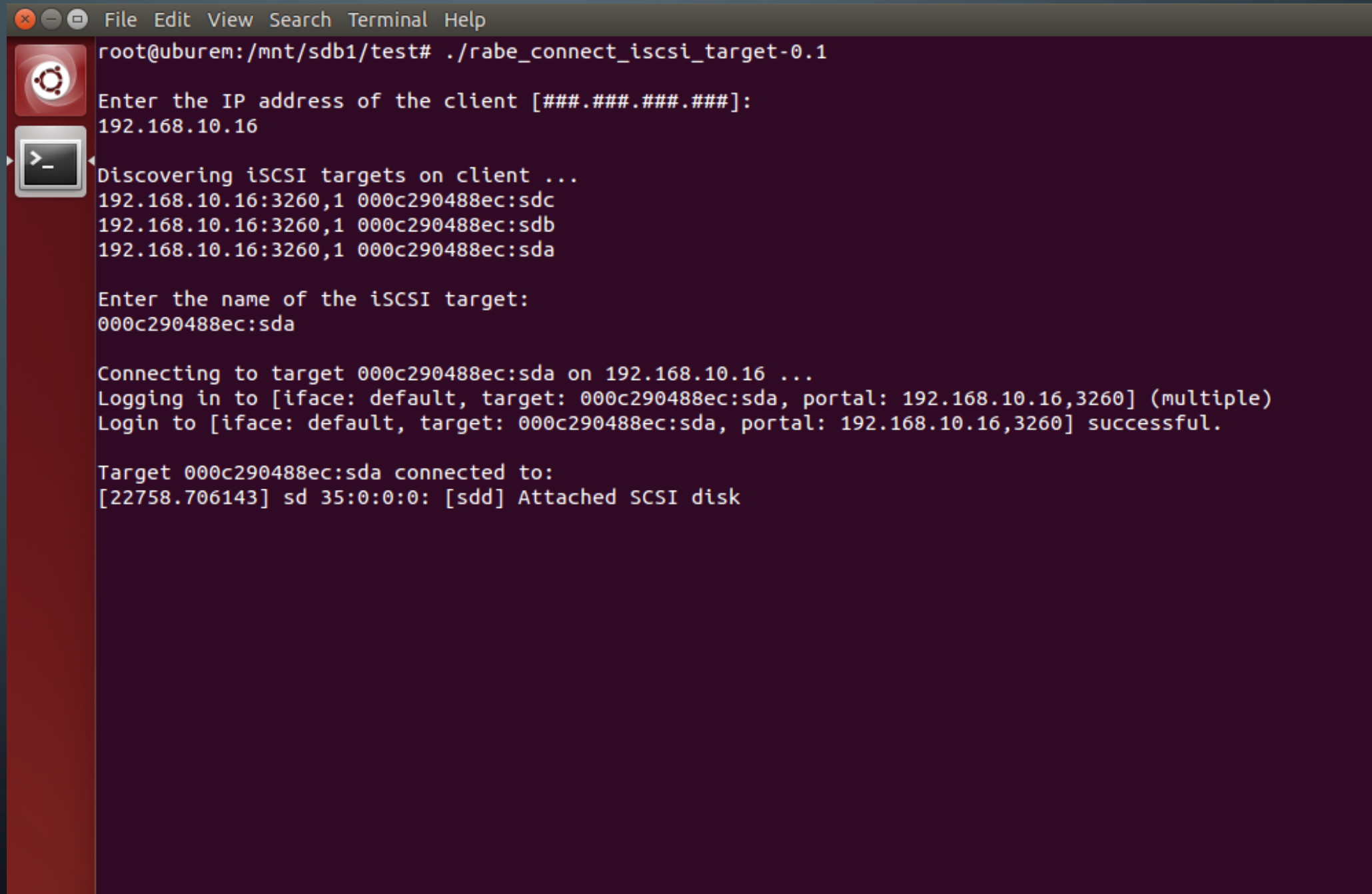

File Edit View Search Terminal Help
root@uburem:/mnt/sdb1/test# ./rabe_authoring_tool-0.4 rabe-0.5_ubuntu-14.04-desktop-i386.iso
[START USER INPUT]
Set static network configuration [y/n]:
y
Enter the IP address of the client [###.###.###.###]:
192.168.10.1
Enter the netmask of the network [###.###.###.###]:
255.255.255.0
Enter the gateway of the network [###.###.###.###]:
192.168.10.254
Enter the IP address of the remote server [###.###.###.###]:
192.168.10.10
Are the OpenVPN server certificate (ca.crt), key (ca.key), index (index.txt) and serial in the openvpn/keys
y
Set NFS share path [y/n]:
y
Enter the NFS share path [/<path/to/nfs/share>/]:
/path/to/nfs/share
./rabe_authoring_tool-0.4: line 122: /path/to/nfs/share: No such file or directory
[END USER INPUT]

```
IP ADDRESS: 145.100.104.61
VPN IP ADDRESS: 10.8.0.6

iSCSI TARGETS:
==============
b8ac6f8b81bd:sda
b8ac6f8b81bd:sdb

DISK INFORMATION:
=================
  *-disk
       description: ATA Disk
       product: ST3250824AS
       vendor: Seagate
       physical id: 0.0.0
       bus info: scsi@0:0.0.0
       logical name: /dev/sda
       version: 3.AD
       serial: 9ND0CZDL
       size: 232GiB (250GB)
       capabilities: partitioned partitioned:dos
       configuration: ansiversion=5 sectorsize=512 signature=8d4b79a1
  *-disk
       description: SCSI Disk
       physical id: 0.0.0
       bus info: scsi@6:0.0.0
       logical name: /dev/sdb
       size: 29GiB (31GB)
       capabilities: partitioned partitioned:dos
       configuration: sectorsize=512 signature=e2ed4f7e
```

DEMO


File Edit View Search Terminal Help
root@uburem:/mnt/sdb1/test# ./rabe_connect_iscsi_target-0.1
Enter the IP address of the client [###.###.###.###]:
192.168.10.16
Discovering iSCSI targets on client ...
192.168.10.16:3260,1 000c290488ec:sdc
192.168.10.16:3260,1 000c290488ec:sdb
192.168.10.16:3260,1 000c290488ec:sda
Enter the name of the iSCSI target:
000c290488ec:sda
Connecting to target 000c290488ec:sda on 192.168.10.16 ...
Logging in to [iface: default, target: 000c290488ec:sda, portal: 192.168.10.16,3260] (multiple)
Login to [iface: default, target: 000c290488ec:sda, portal: 192.168.10.16,3260] successful.
Target 000c290488ec:sda connected to:
[22758.706143] sd 35:0:0:0: [sdd] Attached SCSI disk

QUESTIONS?