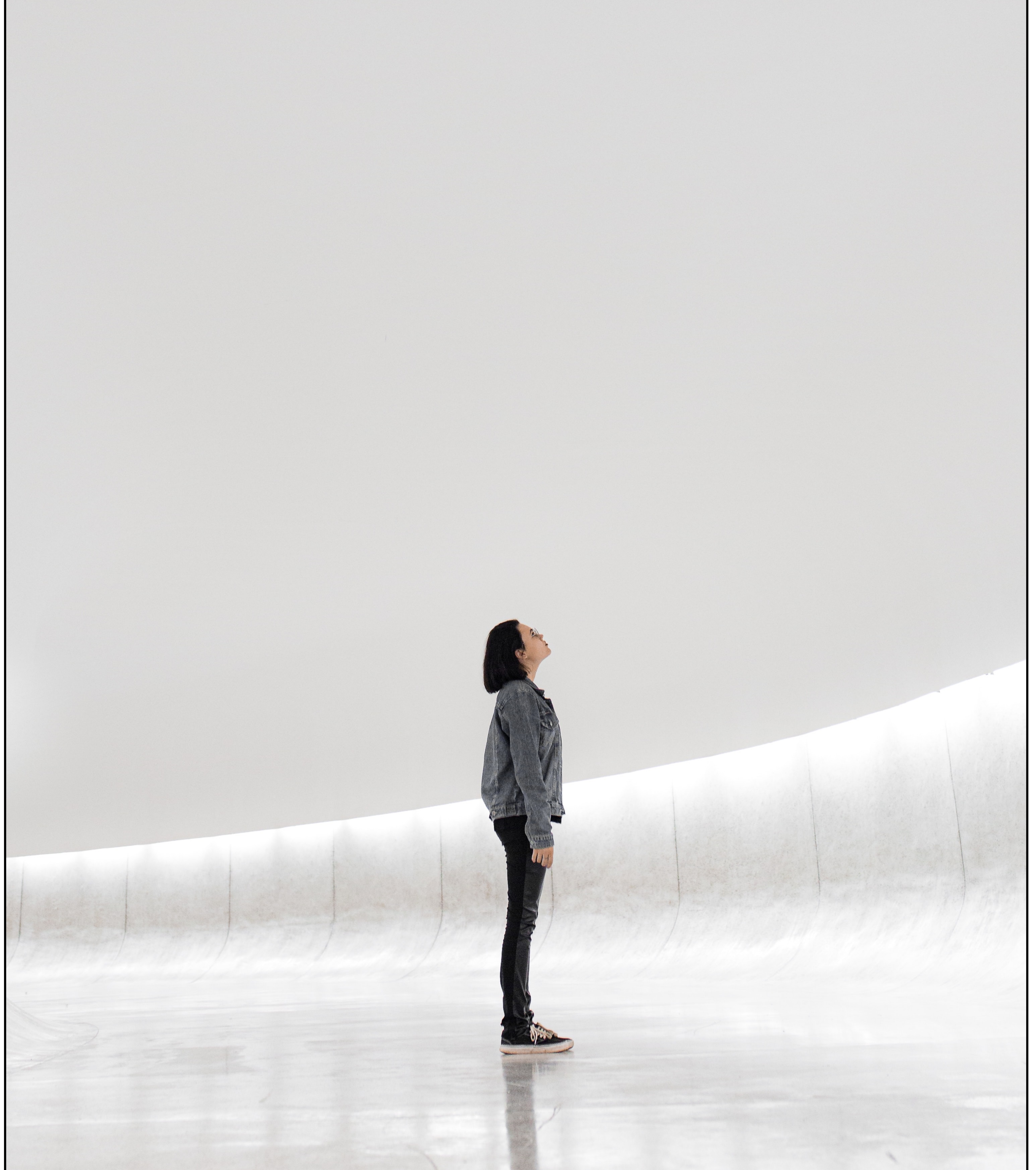
Remote Forensic Investigations

(In the Context of COVID-19)



Xavier Mertens | TF-CSIRT #62 | January 2021
[TLP:White]

Who’s Talking?

- Xavier Mertens (@xme)
- Freelance based in Belgium
- Blueteam
- SANS ISC Senior Handler
- SANS Instructor
- BruCON Co-Organizer

Follow me!

20(20|21)…

… will definitively change our behaviour at all levels.
From a business point of view, most of us are working remotely and this should remain a standard…
This implies our tools and process have to fulfil new requirements…

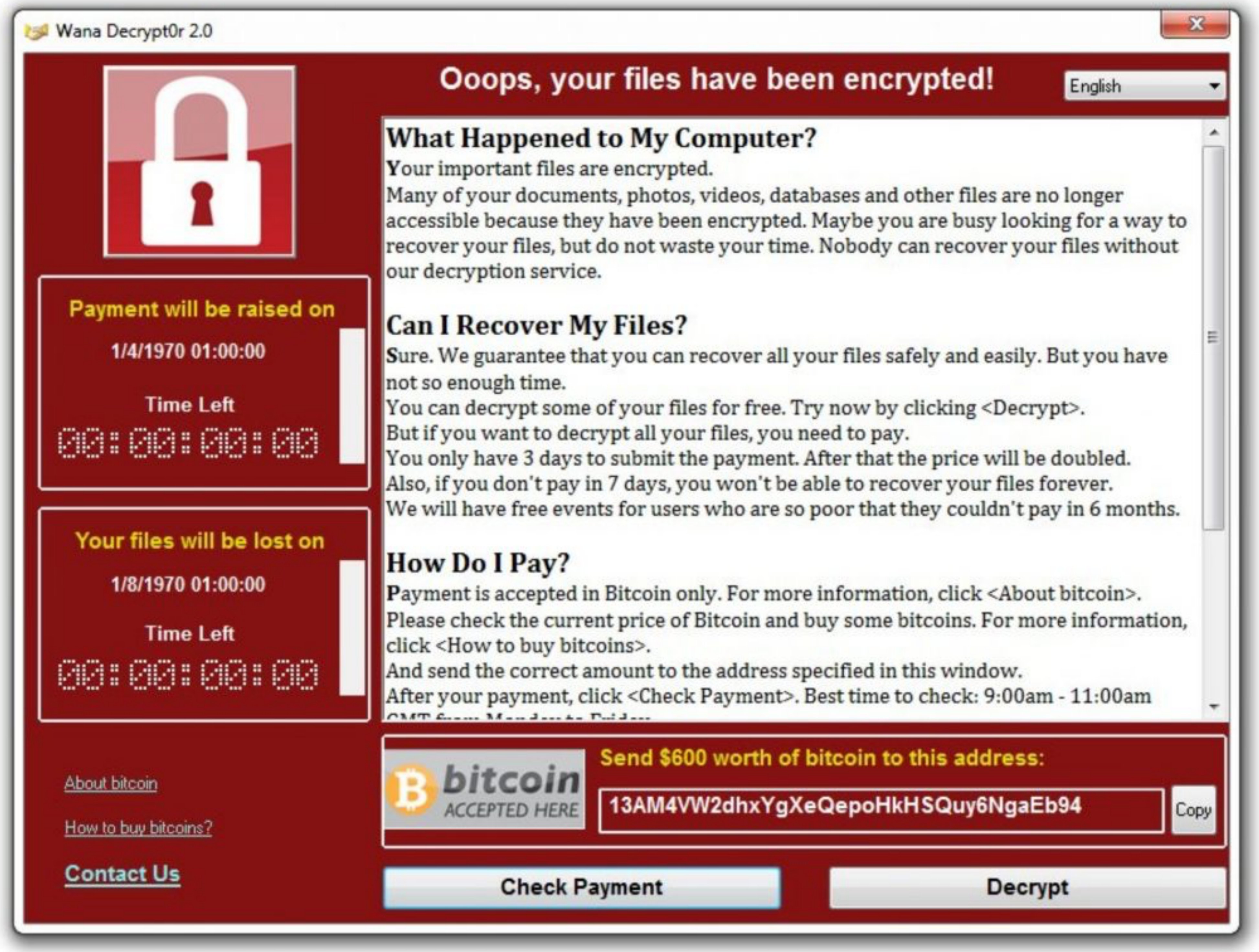
Friday, 10PM

Your Phone Rings…

You're on duty… A customer suspects some malicious activity on a computer. The customer is located 500KM away and asks you to perform investigations as soon as possible.

Many incidents occur at the wrong time.

"Everything takes longer than you think."
(Murphy's law)



What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $600 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

(May, 12 2017 07:44 UTC)

Forensic 101

“The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.” (Wikipedia)

- Collect relevant data from the “suspicious” host in safe way
- Basic artefacts
  - Filesystem
  - Memory
  - Registry
- Useful
  - Application data (browsing history, …)

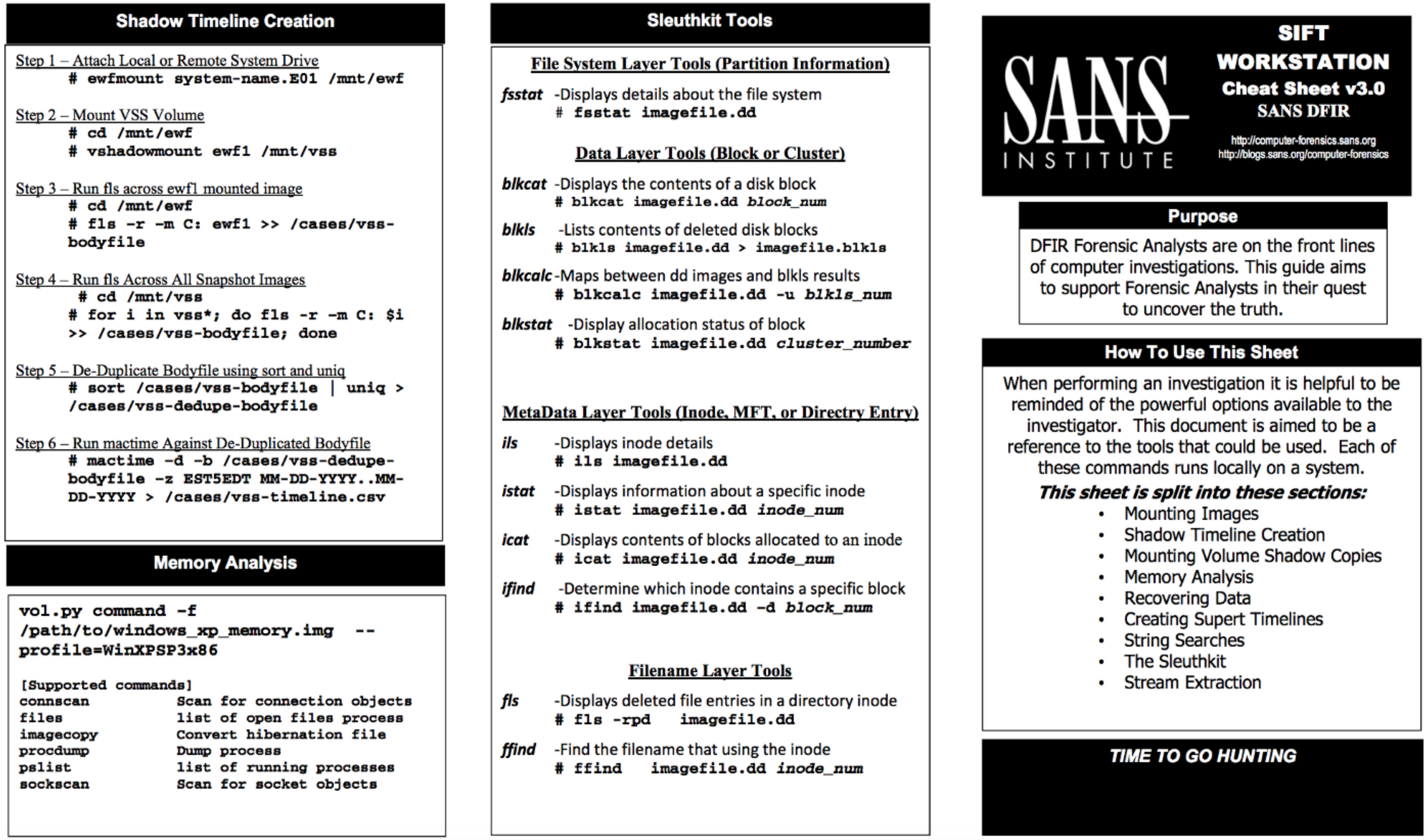
Forensic 101

Toolbox

- Agent-based
  - Encase
  - GRR (Google Rapid Response)
  - MIG (Mozilla InvestiGator)
  - OSQuery, OSSEC
- On-demand
  - SIFT Workstation

SIFT Workstation

The SIFT Workstation is a group of free open-source incident response and forensic tools designed to perform detailed digital forensic examinations in a variety of settings.



Shadow Timeline Creation

Step 1 – Attach Local or Remote System Drive

```
# ewfmount system-name.E01 /mnt/ewf
```

Step 2 – Mount VSS Volume

```
# cd /mnt/ewf
# vshadowmount ewf1 /mnt/vss
```

Step 3 – Run fls across ewf1 mounted image

```
# cd /mnt/ewf
# fls -r -m C: ewf1 >> /cases/vss-
bodyfile
```

Step 4 – Run fls Across All Snapshot Images

```
 # cd /mnt/vss
# for i in vss*; do fls -r -m C: $i
>> /cases/vss-bodyfile; done
```

Step 5 – De-Duplicate Bodyfile using sort and uniq

```
# sort /cases/vss-bodyfile | uniq >
/cases/vss-dedupe-bodyfile
```

Step 6 – Run mactime Against De-Duplicated Bodyfile

```
# mactime -d -b /cases/vss-dedupe-
bodyfile -z EST5EDT MM-DD-YYYY..MM-
DD-YYYY > /cases/vss-timeline.csv
```

Memory Analysis

```
vol.py command -f
/path/to/windows_xp_memory.img  --
profile=WinXPSP3x86

[Supported commands]
connscan        Scan for connection objects
files           list of open files process
imagecopy       Convert hibernation file
procdump        Dump process
pslist          list of running processes
sockscan        Scan for socket objects
```

Sleuthkit Tools

File System Layer Tools (Partition Information)

fsstat -Displays details about the file system

```
# fsstat imagefile.dd
```

Data Layer Tools (Block or Cluster)

blkcat -Displays the contents of a disk block

```
# blkcat imagefile.dd block_num
```

blkls -Lists contents of deleted disk blocks

```
# blkls imagefile.dd > imagefile.blkls
```

blkcalc -Maps between dd images and blkls results

```
# blkcalc imagefile.dd -u blkls_num
```

blkstat -Display allocation status of block

```
# blkstat imagefile.dd cluster_number
```

MetaData Layer Tools (Inode, MFT, or Directry Entry)

ils -Displays inode details

```
# ils imagefile.dd
```

istat -Displays information about a specific inode

```
# istat imagefile.dd inode_num
```

icat -Displays contents of blocks allocated to an inode

```
# icat imagefile.dd inode_num
```

ifind -Determine which inode contains a specific block

```
# ifind imagefile.dd -d block_num
```

Filename Layer Tools

fls -Displays deleted file entries in a directory inode

```
# fls -rpd   imagefile.dd
```

ffind -Find the filename that using the inode

```
# ffind   imagefile.dd inode_num
```

SANS INSTITUTE

SIFT WORKSTATION
Cheat Sheet v3.0
SANS DFIR
http://computer-forensics.sans.org
http://blogs.sans.org/computer-forensics

Purpose

DFIR Forensic Analysts are on the front lines of computer investigations. This guide aims to support Forensic Analysts in their quest to uncover the truth.

How To Use This Sheet

When performing an investigation it is helpful to be reminded of the powerful options available to the investigator. This document is aimed to be a reference to the tools that could be used. Each of these commands runs locally on a system.

This sheet is split into these sections:

- Mounting Images
- Shadow Timeline Creation
- Mounting Volume Shadow Copies
- Memory Analysis
- Recovering Data
- Creating Supert Timelines
- String Searches
- The Sleuthkit
- Stream Extraction

TIME TO GO HUNTING

Requirements

- Easy and quick to deploy
- « Forensically » aware
- Lot of tools preinstalled
- Disk management
- Interaction with users
- Compatible with many systems/networks
- Customers keep control (grant/deny access)
- Low bandwidth usage: process data remotely (just grab evidences)

Bitscout

“A customizable Live OS constructor tool almost entirely written in Bash”

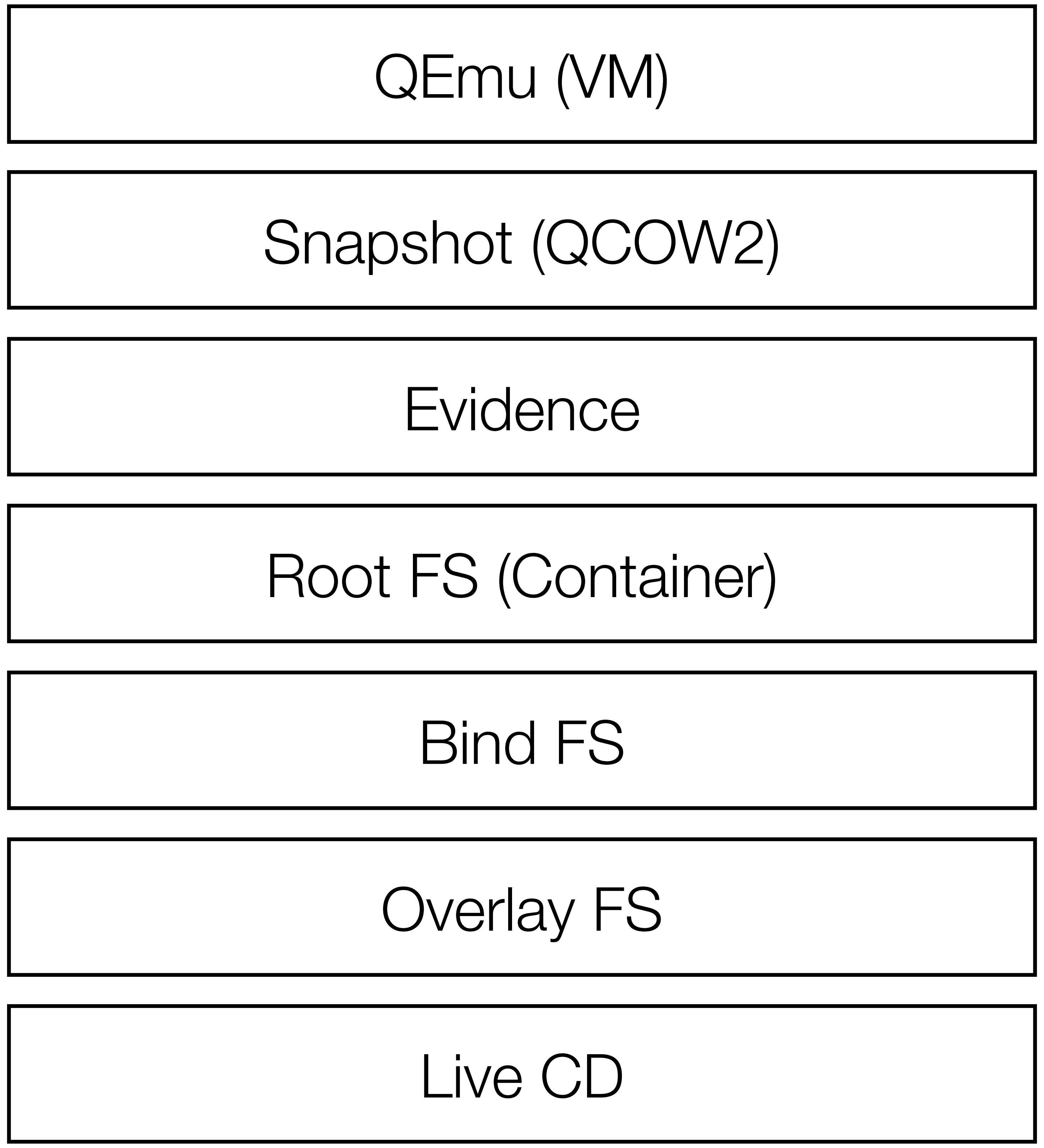
- Live Linux OS
- Simple & customizable at build time
- Extendable at run time
- Minimal system requirements
- Low bandwidth / VPN
- Unprivileged isolated access
- Two roles: “Expert” and “Owner”

BITSCOUT

Bitscout

Key Points

- The “Expert” is root in his/her restricted environment
- Multiple layers
- Access only to authorised resources
- To prevent tampering of evidences



QEmu (VM)

Snapshot (QCOW2)

Evidence

Root FS (Container)

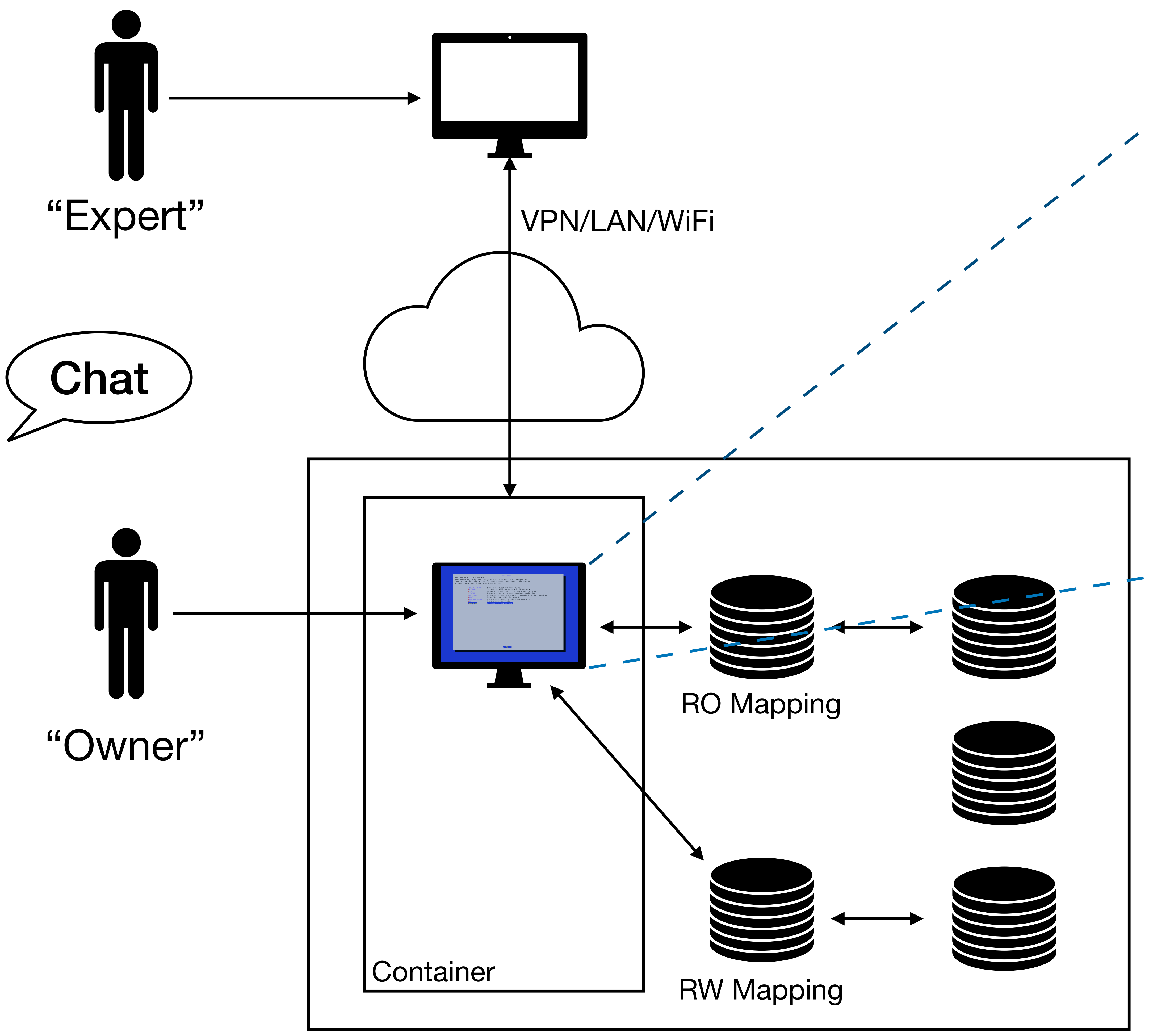
Bind FS

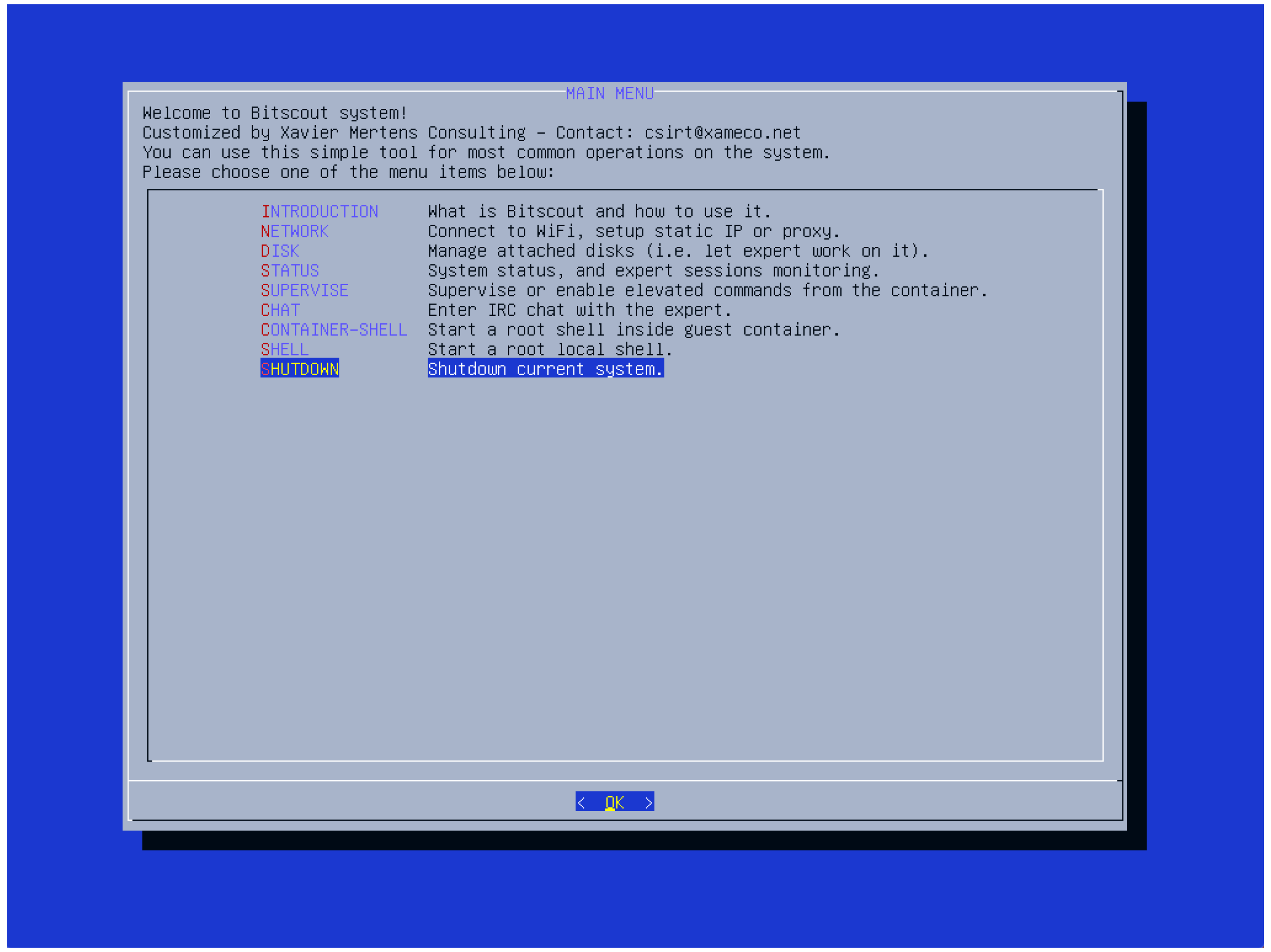
Overlay FS

Live CD

Bitscout

Architecture



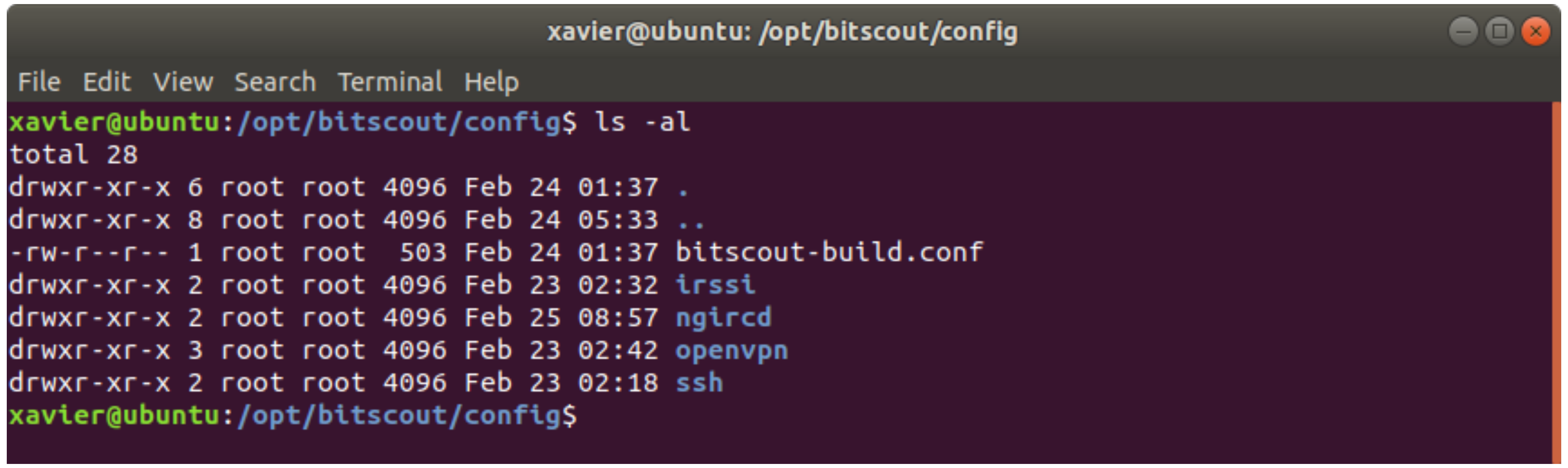


```
Welcome to Bitscout system!
Customized by Xavier Mertens Consulting - Contact: csirt@xameco.net
You can use this simple tool for most common operations on the system.
Please choose one of the menu items below:

          INTRODUCTION     What is Bitscout and how to use it.
          NETWORK          Connect to WiFi, setup static IP or proxy.
          DISK             Manage attached disks (i.e. let expert work on it).
          STATUS           System status, and expert sessions monitoring.
          SUPERVISE        Supervise or enable elevated commands from the container.
          CHAT             Enter IRC chat with the expert.
          CONTAINER-SHELL  Start a root shell inside guest container.
          SHELL            Start a root local shell.
          SHUTDOWN         Shutdown current system.
```

Bitscout

Configuration & Customisation

- Prepare your personal ISO
- OpenVPN setup
- SSH setup (keys)
- IRC (will never die 😛)



xavier@ubuntu: /opt/bitscout/config
File Edit View Search Terminal Help

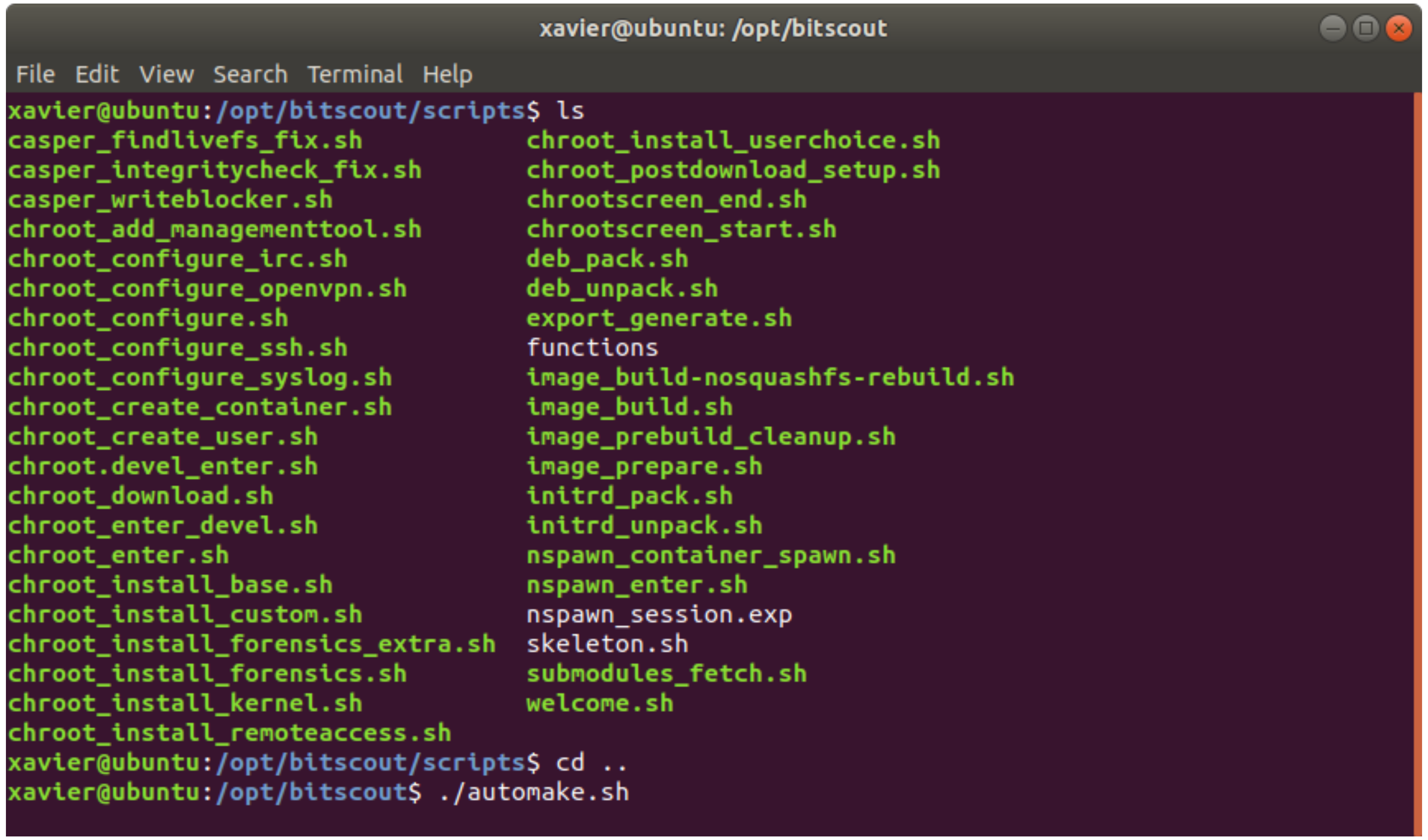
```
xavier@ubuntu:/opt/bitscout/config$ ls -al
total 28
drwxr-xr-x 6 root root 4096 Feb 24 01:37 .
drwxr-xr-x 8 root root 4096 Feb 24 05:33 ..
-rw-r--r-- 1 root root  503 Feb 24 01:37 bitscout-build.conf
drwxr-xr-x 2 root root 4096 Feb 23 02:32 irssi
drwxr-xr-x 2 root root 4096 Feb 25 08:57 ngircd
drwxr-xr-x 3 root root 4096 Feb 23 02:42 openvpn
drwxr-xr-x 2 root root 4096 Feb 23 02:18 ssh
xavier@ubuntu:/opt/bitscout/config$
```

Note: The Expert needs to deploy some servers (VPN, IRC, Syslog, …)

Bitscout

Configuration & Customisation

- Create new Bash scripts
  (Ex: to install your own tools)
- Regenerate the ISO image
  (./automake.sh)
- Make the ISO image available to download for your customers

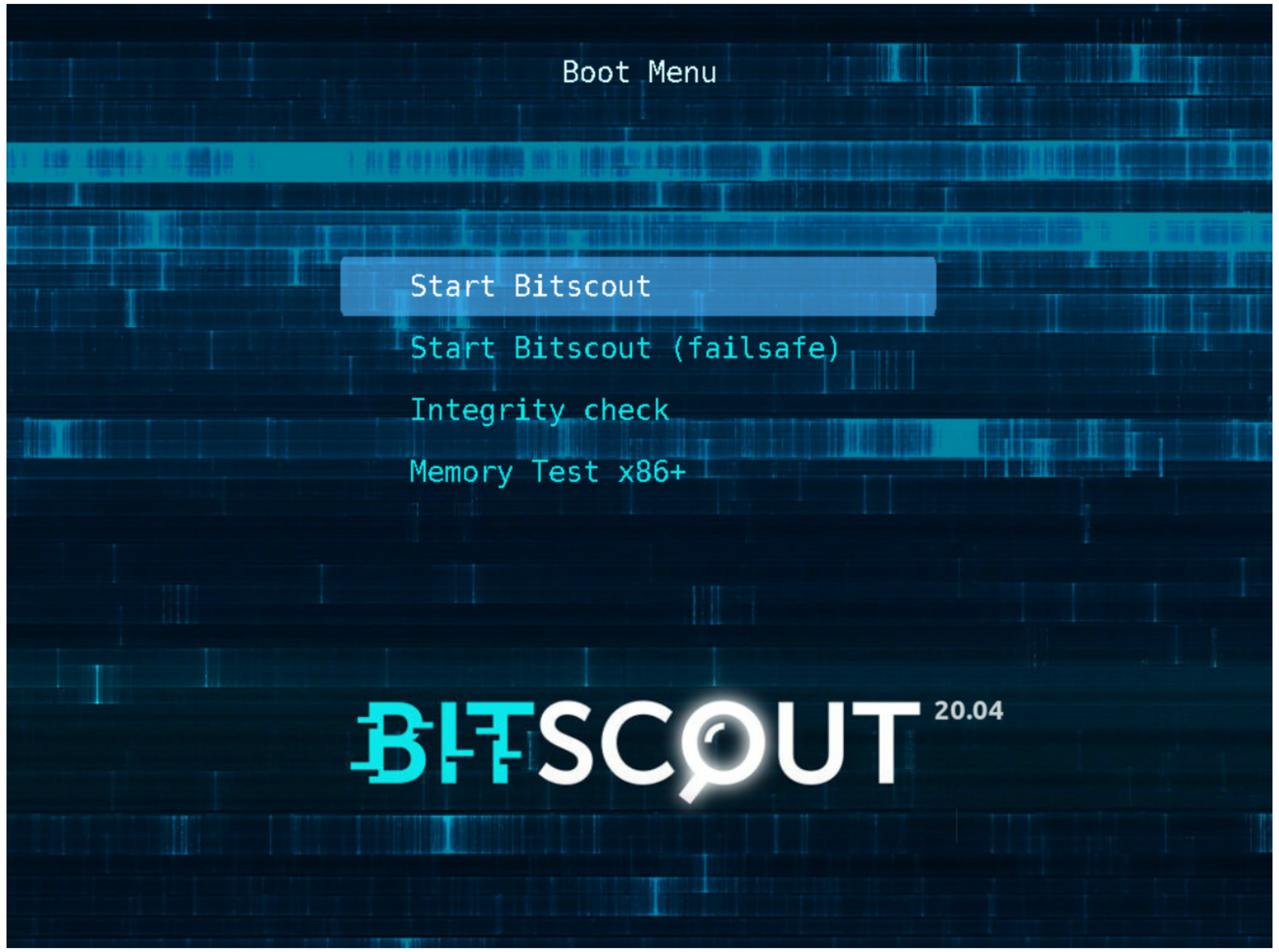

xavier@ubuntu: /opt/bitscout
File Edit View Search Terminal Help

```
xavier@ubuntu:/opt/bitscout/scripts$ ls
casper_findlivefs_fix.sh          chroot_install_userchoice.sh
casper_integritycheck_fix.sh      chroot_postdownload_setup.sh
casper_writeblocker.sh            chrootscreen_end.sh
chroot_add_managementtool.sh      chrootscreen_start.sh
chroot_configure_irc.sh           deb_pack.sh
chroot_configure_openvpn.sh       deb_unpack.sh
chroot_configure.sh               export_generate.sh
chroot_configure_ssh.sh           functions
chroot_configure_syslog.sh        image_build-nosquashfs-rebuild.sh
chroot_create_container.sh        image_build.sh
chroot_create_user.sh             image_prebuild_cleanup.sh
chroot.devel_enter.sh             image_prepare.sh
chroot_download.sh                initrd_pack.sh
chroot_enter_devel.sh             initrd_unpack.sh
chroot_enter.sh                   nspawn_container_spawn.sh
chroot_install_base.sh            nspawn_enter.sh
chroot_install_custom.sh          nspawn_session.exp
chroot_install_forensics_extra.sh skeleton.sh
chroot_install_forensics.sh       submodules_fetch.sh
chroot_install_kernel.sh          welcome.sh
chroot_install_remoteaccess.sh
xavier@ubuntu:/opt/bitscout/scripts$ cd ..
xavier@ubuntu:/opt/bitscout$ ./automake.sh
```

Bitscout

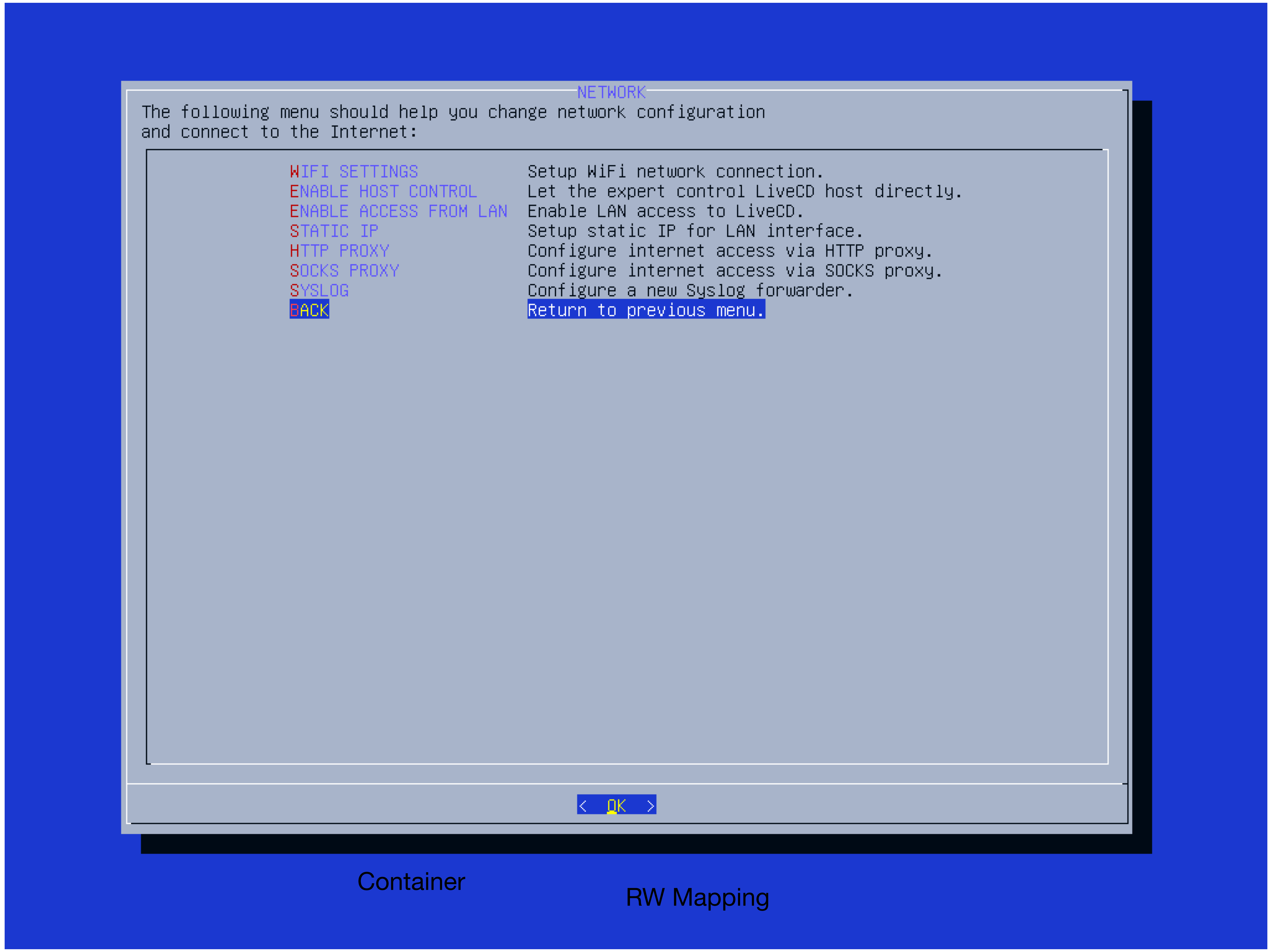
Boot

- Burn a CD
- Or generate a USB stick
- Or add to a datastore and boot a VM (create a temporary VM and assigned the suspicious .vmdk)
- Internet access required!
(DNS & UDP/1194)

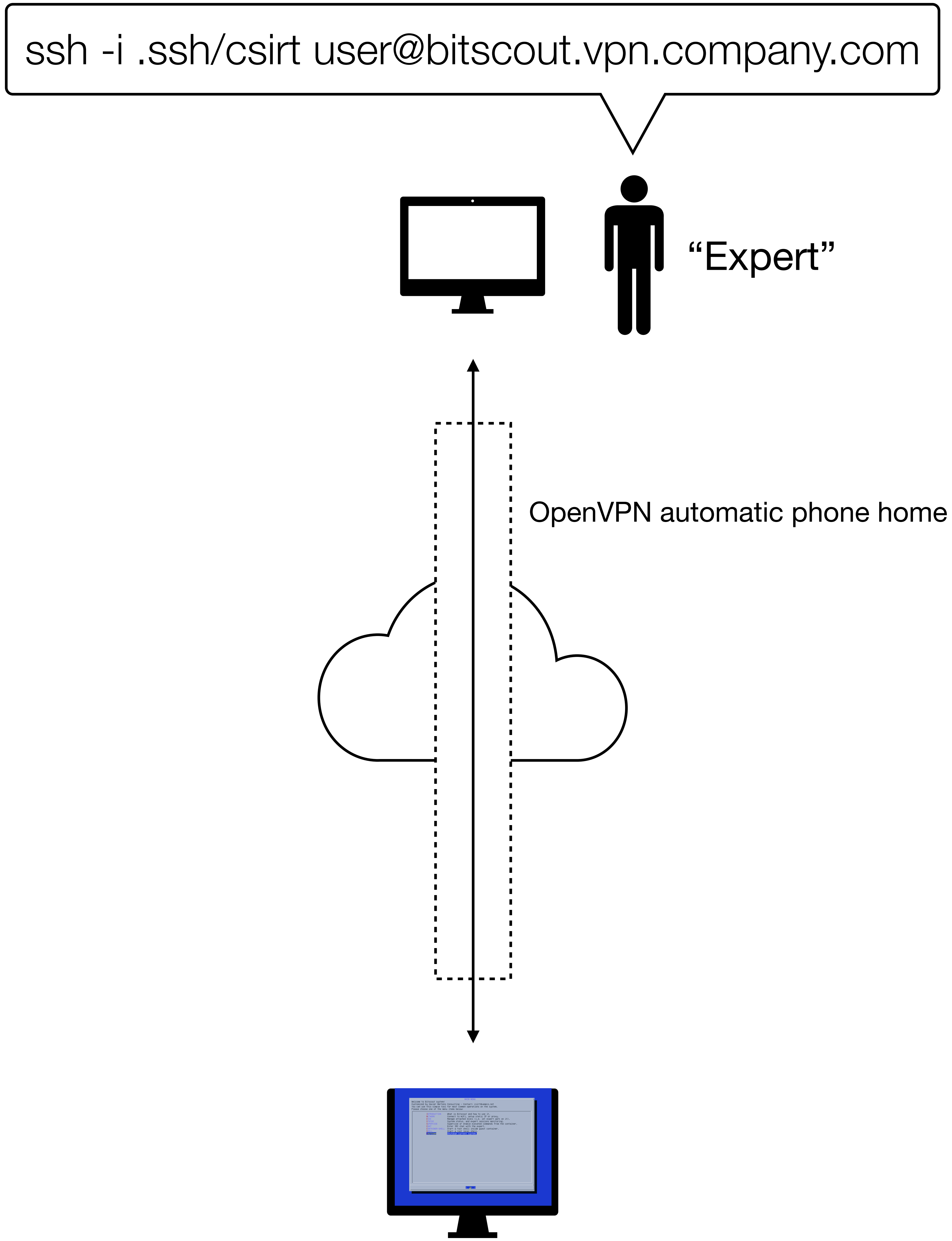


Bitscout

Network Setup



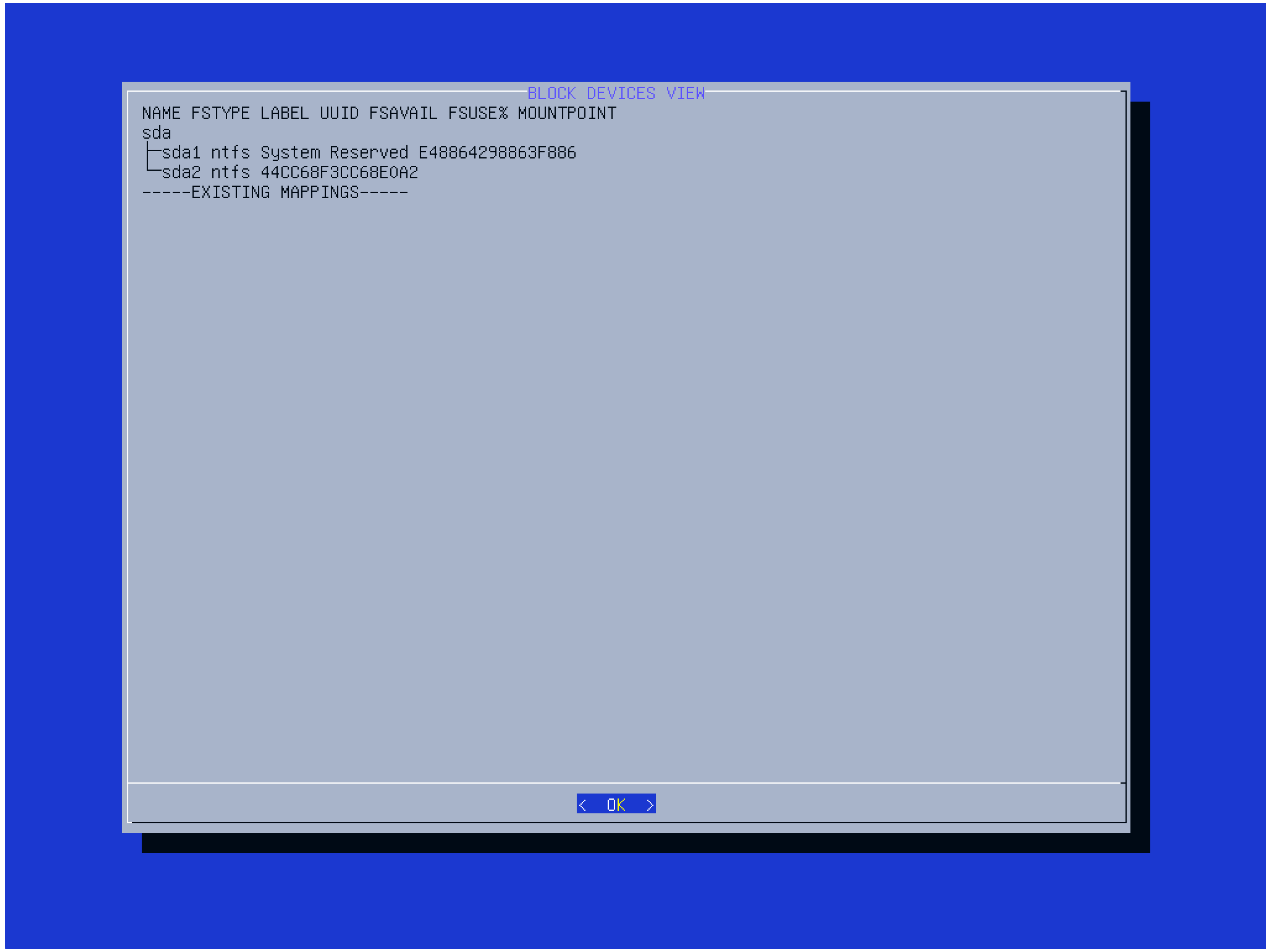
```
                                   NETWORK
The following menu should help you change network configuration
and connect to the Internet:

              WIFI SETTINGS            Setup WiFi network connection.
              ENABLE HOST CONTROL      Let the expert control LiveCD host directly.
              ENABLE ACCESS FROM LAN   Enable LAN access to LiveCD.
              STATIC IP                Setup static IP for LAN interface.
              HTTP PROXY               Configure internet access via HTTP proxy.
              SOCKS PROXY              Configure internet access via SOCKS proxy.
              SYSLOG                   Configure a new Syslog forwarder.
              BACK                     Return to previous menu.

                                   <  OK  >
```



```
ssh -i .ssh/csirt user@bitscout.vpn.company.com
```

Bitscout

Disk Management

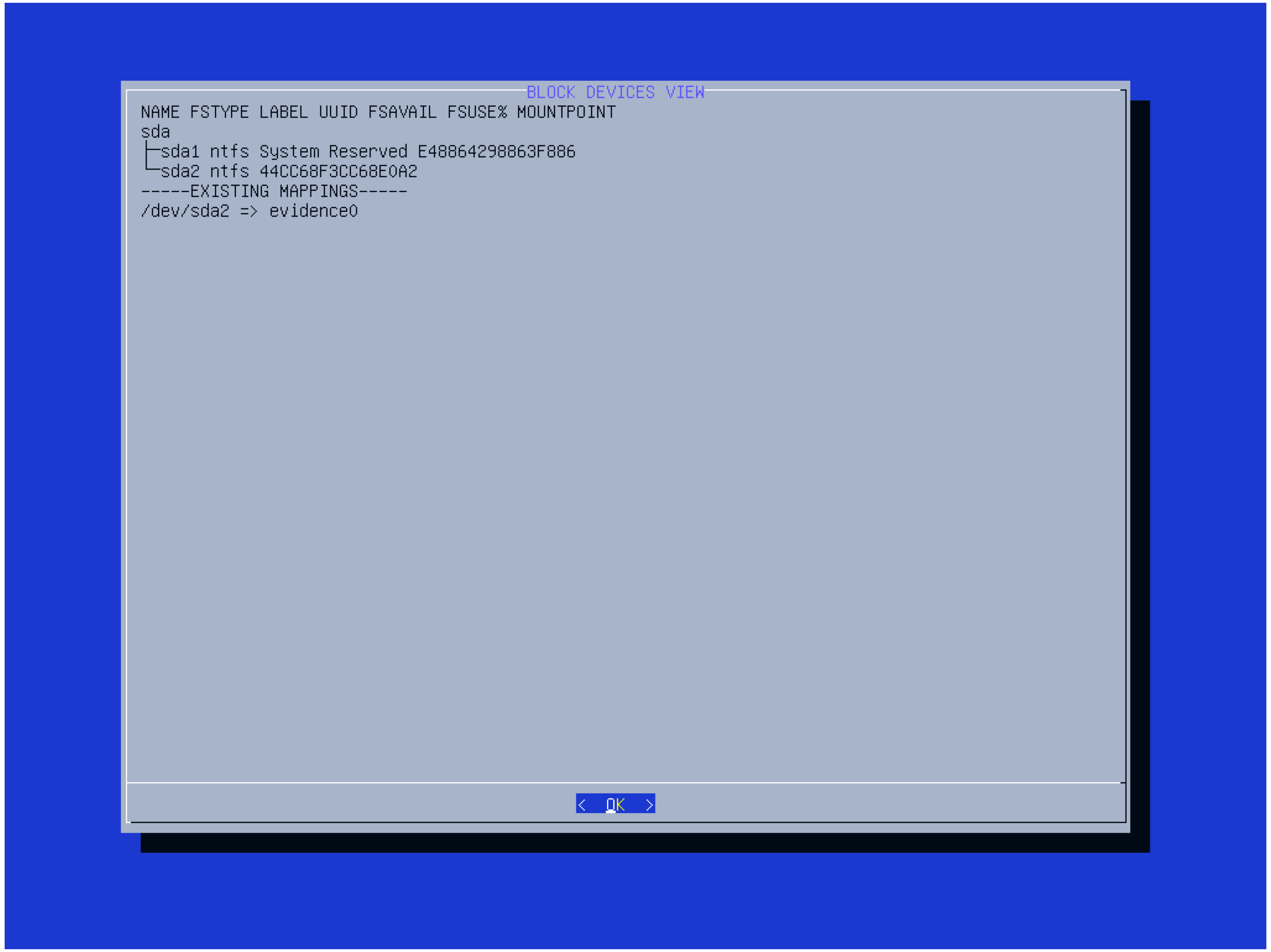


```
NAME FSTYPE LABEL UUID FSAVAIL FSUSE% MOUNTPOINT
sda
├─sda1 ntfs System Reserved E48864298863F886
└─sda2 ntfs 44CC68F3CC68E0A2
-----EXISTING MAPPINGS-----
```

/dev/sda

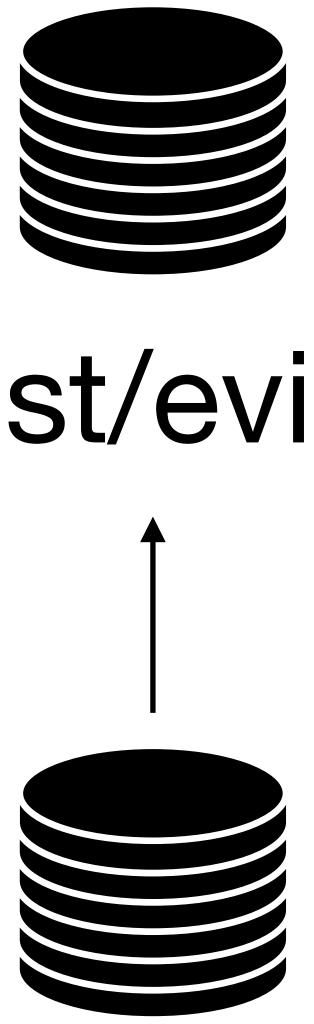
Bitscout

Disk Management



BLOCK DEVICES VIEW

```
NAME FSTYPE LABEL UUID FSAVAIL FSUSE% MOUNTPOINT
sda
├sda1 ntfs System Reserved E48864298863F886
└sda2 ntfs 44CC68F3CC68E0A2
-----EXISTING MAPPINGS-----
/dev/sda2 => evidence0
```



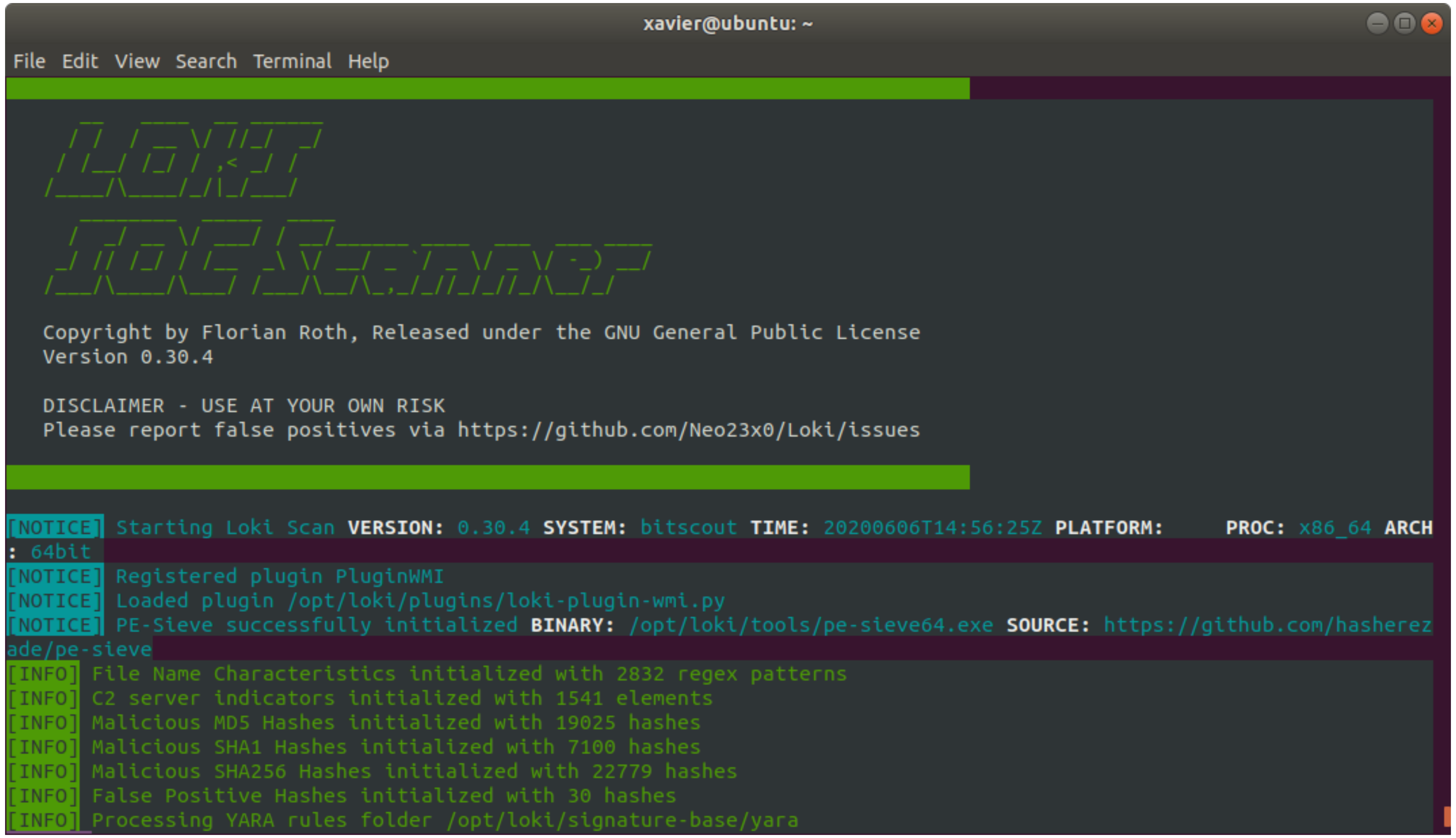
/dev/host/evidence0

/dev/sda

Investigation

Classic Disk Tools

- Mount your filesystems
- Use classic tools
  - Loki
  - BulkExtractor
  - Log2Timeline
  - …[*]



```
      __   ____  __ ______
     / /  / __ \/ //_/  _/
    / /__/ /_/ / ,< _/ /
   /____/\____/_/|_/___/
      ________  _____  ____
     /  _/ __ \/ ___/ / __/______ ____  ___  ___ ____
    _/ // /_/ / /__  _\ \/ __/ _ `/ _ \/ _ \/ -_) __/
   /___/\____/\___/ /___/\__/\_,_/_//_/_//_/\__/_/

   Copyright by Florian Roth, Released under the GNU General Public License
   Version 0.30.4

   DISCLAIMER - USE AT YOUR OWN RISK
   Please report false positives via https://github.com/Neo23x0/Loki/issues


[NOTICE] Starting Loki Scan VERSION: 0.30.4 SYSTEM: bitscout TIME: 20200606T14:56:25Z PLATFORM:     PROC: x86_64 ARCH
: 64bit
[NOTICE] Registered plugin PluginWMI
[NOTICE] Loaded plugin /opt/loki/plugins/loki-plugin-wmi.py
[NOTICE] PE-Sieve successfully initialized BINARY: /opt/loki/tools/pe-sieve64.exe SOURCE: https://github.com/hasherez
ade/pe-sieve
[INFO] File Name Characteristics initialized with 2832 regex patterns
[INFO] C2 server indicators initialized with 1541 elements
[INFO] Malicious MD5 Hashes initialized with 19025 hashes
[INFO] Malicious SHA1 Hashes initialized with 7100 hashes
[INFO] Malicious SHA256 Hashes initialized with 22779 hashes
[INFO] False Positive Hashes initialized with 30 hashes
[INFO] Processing YARA rules folder /opt/loki/signature-base/yara
```

[*] Install and use your preferred tools

Investigation

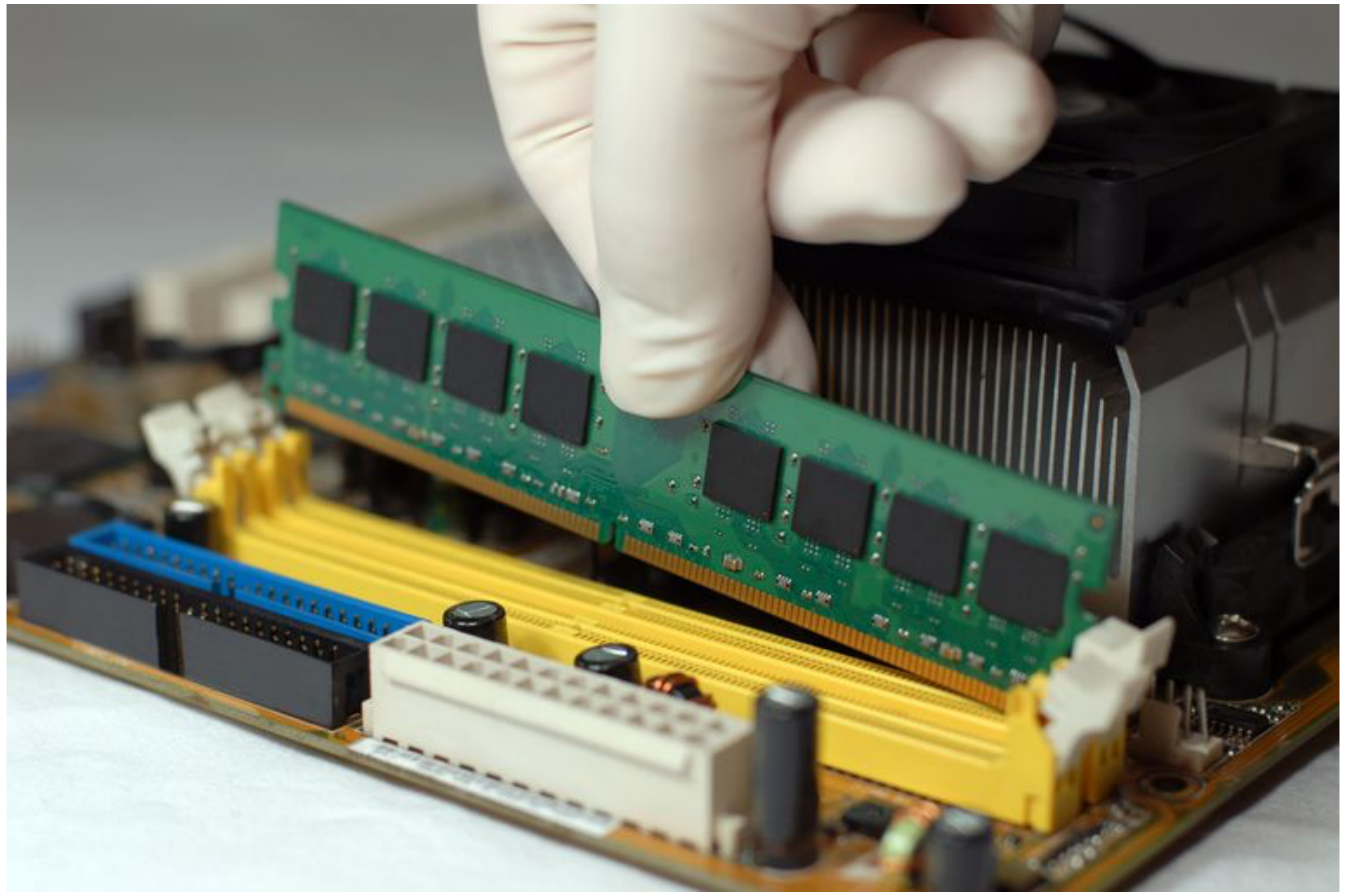
Working with a Live System

- Sometimes, working on a live system is easier
- Again, evidences must be preserved
- QEmu (available on the Live CD) to the rescue!
- Let’s boot the infected/suspicious system in two steps:
    1. Create a snapshot of the mapped disk
    2. Boot the VM using the snapshot as main storage

Investigation

Memory Analysis

- Memory analyzis is a key location for artefacts
- Performing memory acquisition is a pain because
  - Memory size is bigger (32GB is common even for a laptop)
  - Tools not user friendly



(Memory acquisition as seen by end-users)

Need for More Tools?

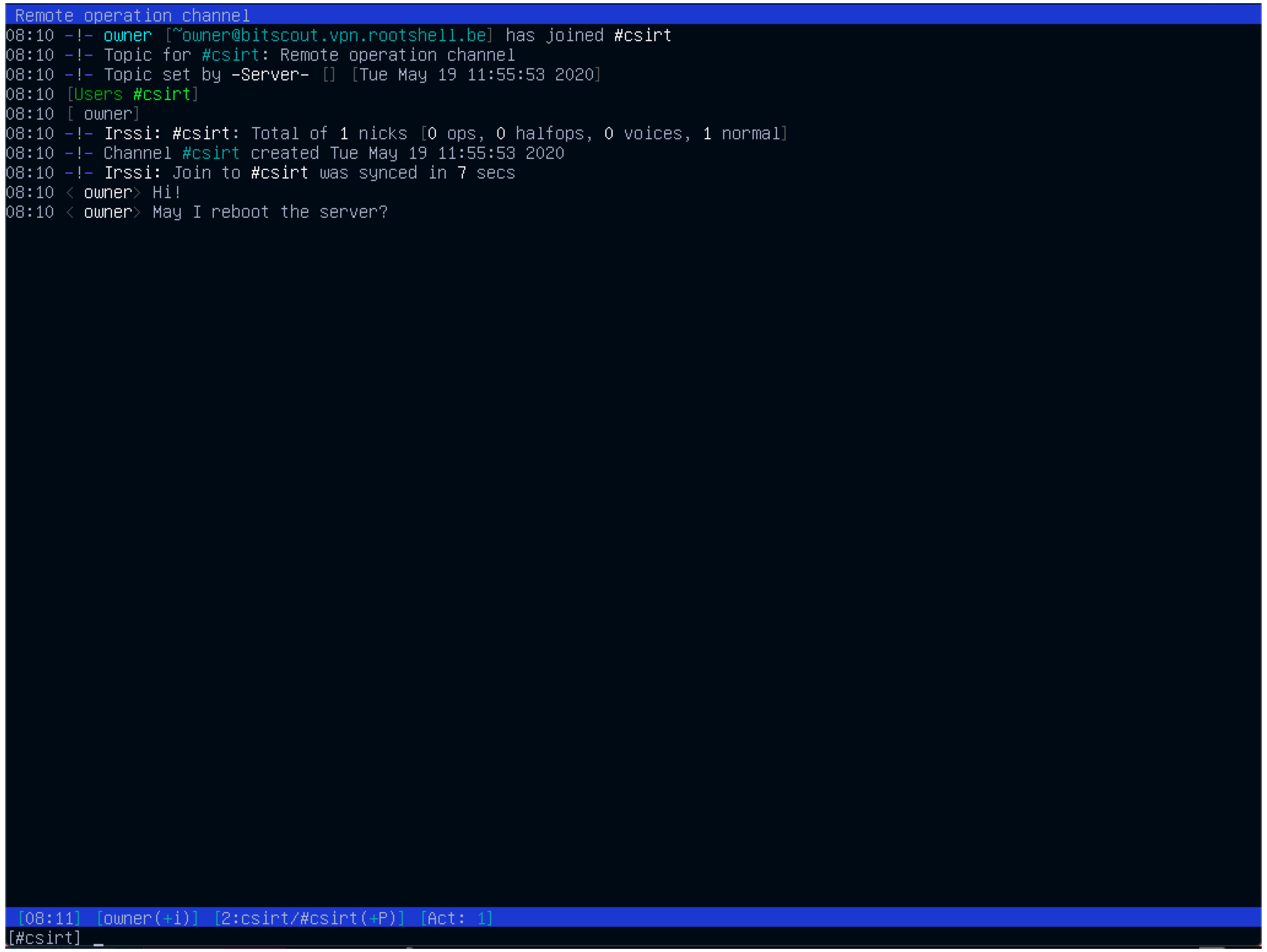
Installation of Extra Tools

- Sometimes, Windows tools are required (ex: Sysinternals)
- QEmu to the rescue again!
- Boot the VM with a SMB share emulated through QEmu
- Copy files on the mount directory
- Enjoy!

Other Features

Chat between Owner & Expert

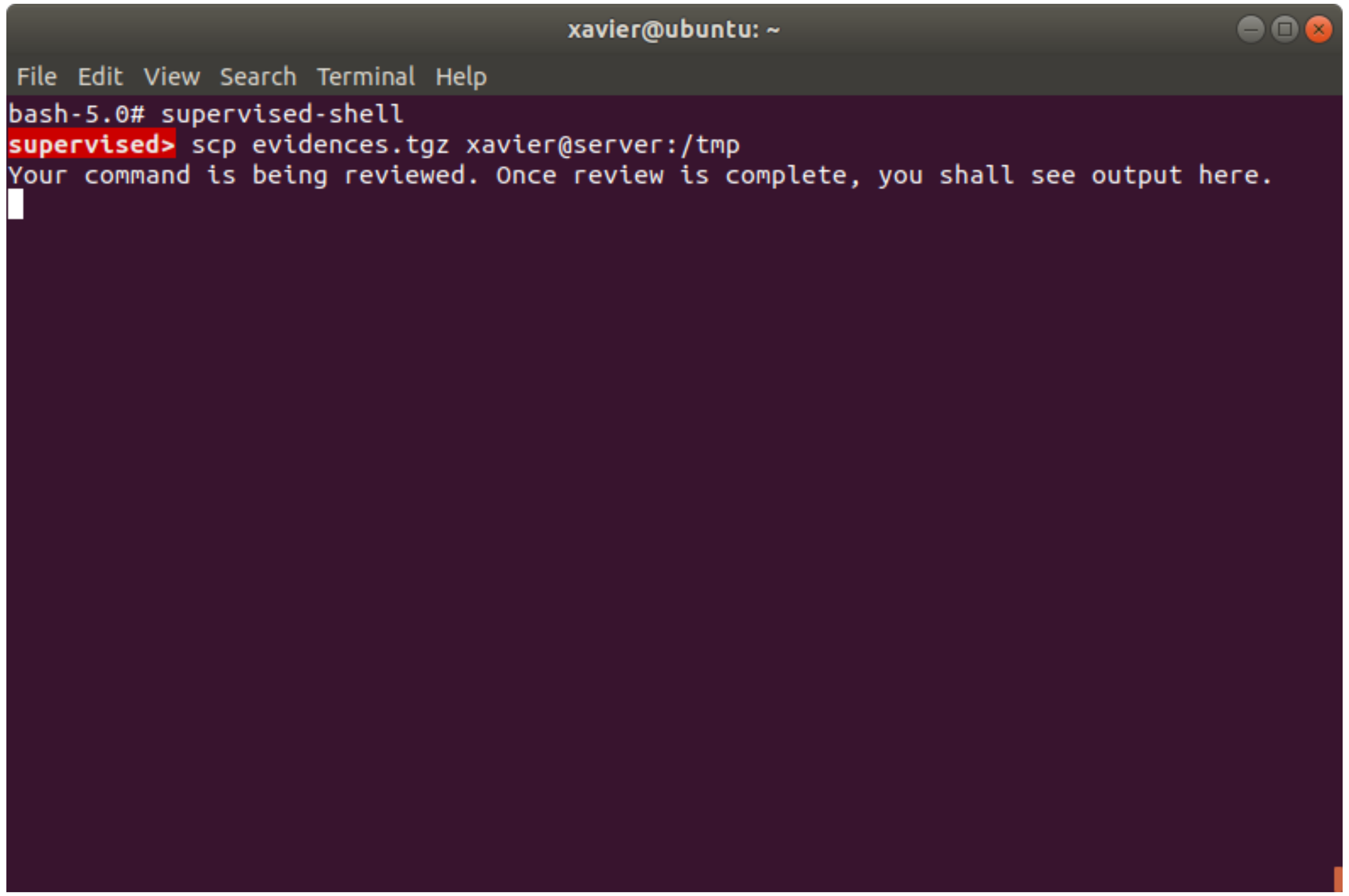
- Communication is key!
- Safe channel through the VPN
- IRC server operated by the Expert (Docker)



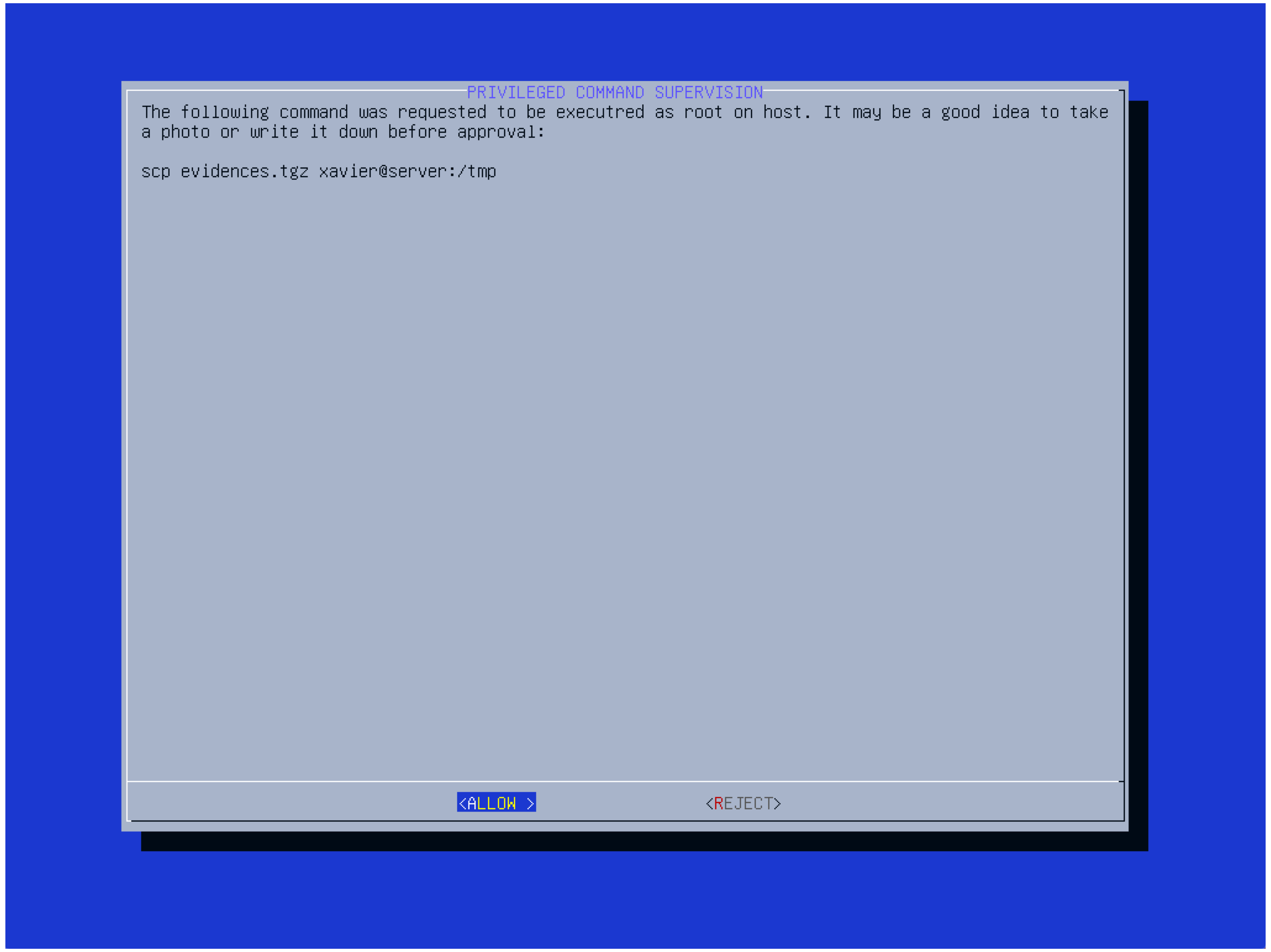
```
 Remote operation channel
08:10 -!- owner [~owner@bitscout.vpn.rootshell.be] has joined #csirt
08:10 -!- Topic for #csirt: Remote operation channel
08:10 -!- Topic set by -Server- [] [Tue May 19 11:55:53 2020]
08:10 [Users #csirt]
08:10 [ owner]
08:10 -!- Irssi: #csirt: Total of 1 nicks [0 ops, 0 halfops, 0 voices, 1 normal]
08:10 -!- Channel #csirt created Tue May 19 11:55:53 2020
08:10 -!- Irssi: Join to #csirt was synced in 7 secs
08:10 < owner> Hi!
08:10 < owner> May I reboot the server?




 [08:11] [owner(+i)] [2:csirt/#csirt(+P)] [Act: 1]
[#csirt] _
```

Other Features

Sensitive Command Approval



```
bash-5.0# supervised-shell
supervised> scp evidences.tgz xavier@server:/tmp
Your command is being reviewed. Once review is complete, you shall see output here.
```



PRIVILEGED COMMAND SUPERVISION

```
The following command was requested to be executred as root on host. It may be a good idea to take
a photo or write it down before approval:

scp evidences.tgz xavier@server:/tmp
```

Data Transfer

The Power of SSH

- Transfert data to Expert’s system

```
On Expert’s system:
# nc -l -p 5555 >evidence0.dd.gz
# ssh -i .ssh/csirt -R 5555:127.0.0.1:5555 user@bitscout.vpn.rootshell.be

On BitScout:
# cat /dev/host/evidence0 | gzip -9 -c | nc 127.0.0.1:5555
```

- Define a proxy to download through the VPN

```
On Expert’s system:
# ssh -i .ssh/csirt -R 3128:192.168.254.8:3128 user@bitscout.vpn.rootshell.be

On BitScout:
# export http_proxy=http://127.0.01:3128
```

Bitscout

Credits

- Bitscout is developed and maintained by Vitaly Kamluk (@vkamluk)
- I’m a simple contributor to the project
- Want to try it / use it? https://github.com/vitaly-kamluk/bitscout

Thank You!

Q&A

! or ?