Remote Threat Reconnaisance

Vitaly Kamluk

Nicolas Collery

with support of

Leonid Bezvershenko

The Trainers

Principal Security Researcher
Head of GReAT APAC, Kaspersky

- 16 years at Kaspersky
- 2 years with INTERPOL

Author of Bitscout project
Reverse engineer, digital forensic analyst, security researcher, trainer.

kaspersky

Active Defense Executive Director, DBS Bank

Nicolas Collery has been in the security field for over 15 years, focusing on fighting cybercrime. Passionate about forensics, malware analysis, and now simulating attacks focusing on real-adversaries tactics, techniques and procedure to assess capability to prevent, detect and respond.

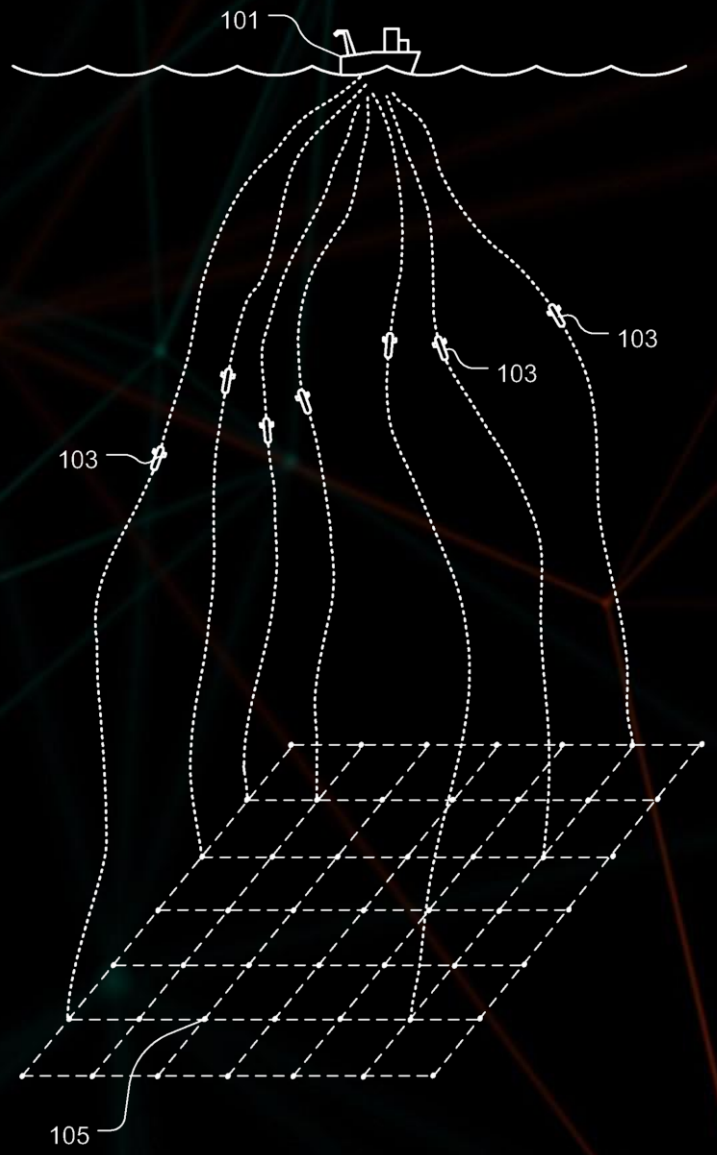
DBS

The Birth of The Idea

Once Upon A Time...

No Flight Zone

My Plan. US8397657B2 but for cyber!



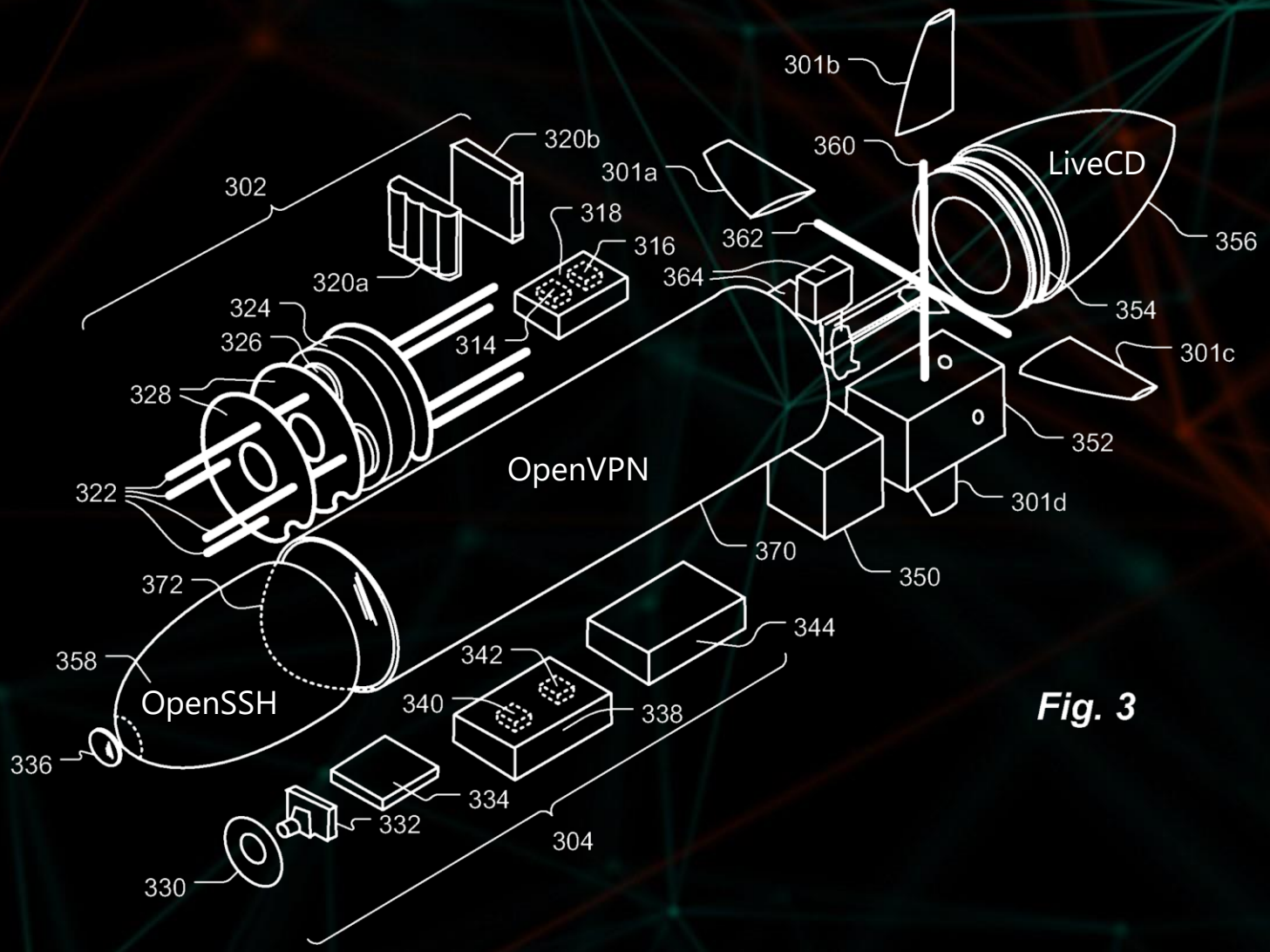
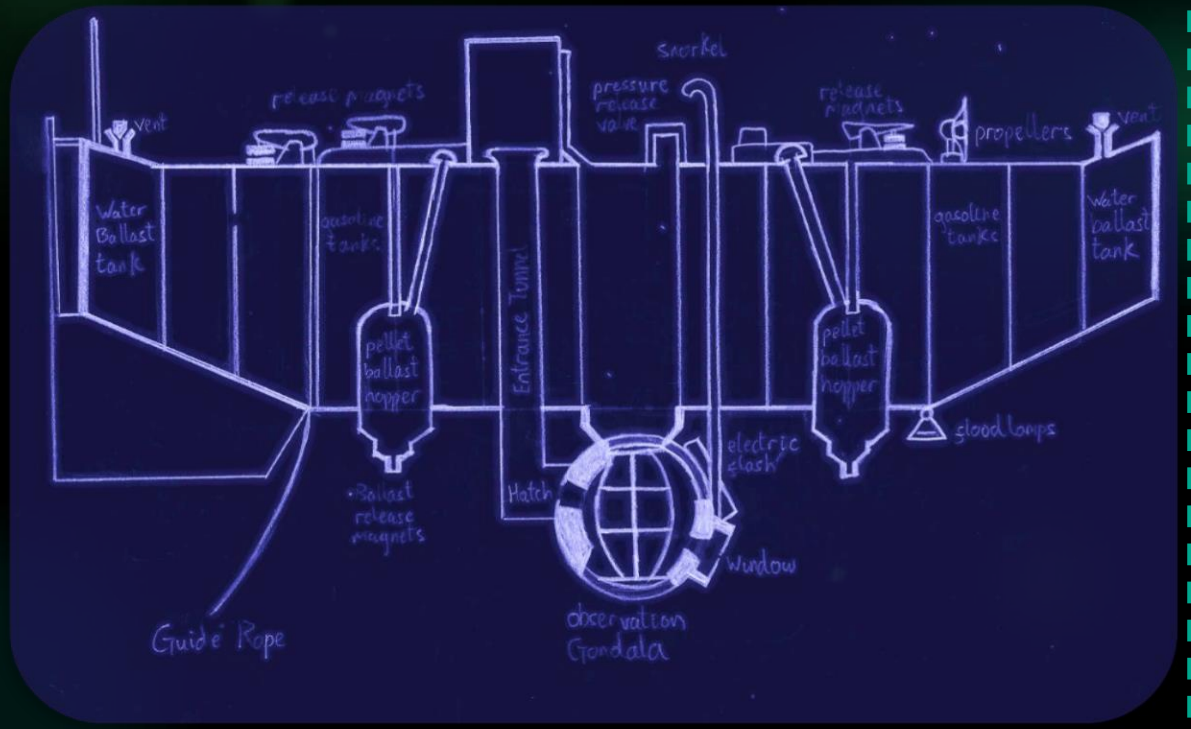


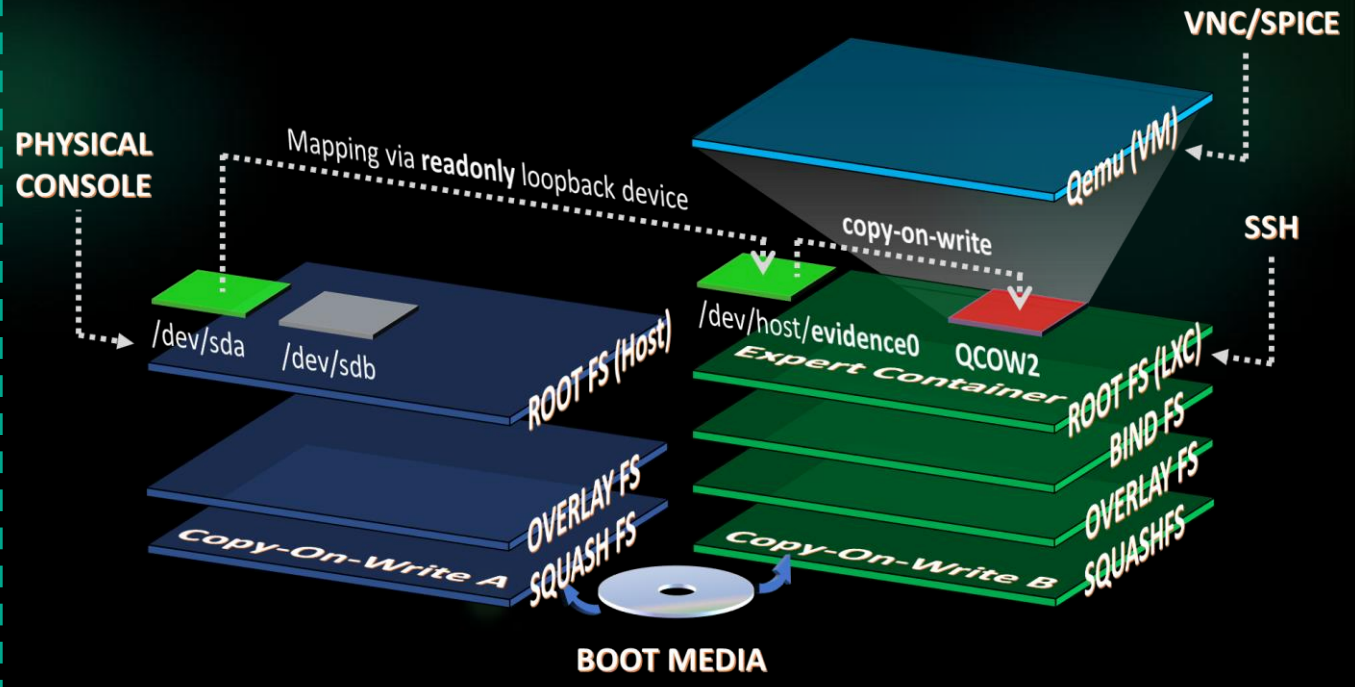
Fig. 3

*Patent US8397657B2 Vertical Glider Robot by Massachusetts Institute of Technology, 2010

The Reality



Bathyscaph



Bitscout

Bitscout: Key Principles

- **Forensically sound live** OS or **revertable** regular OS
- Free and open-source (Linux based)
- Simple and customizable
- Extendable during runtime
- Minimal in RAM and in size
- Capable to work even over very slow or unstable networks
- User owns all VPN certificates, adds own SSH keys
- Extra-safety through unprivileged isolated access
- Leverages original hardware/firmware of the analyzed system

Other Use Cases

A low-bandwidth remote system

An unusual hardware: RAID, SAS, etc.

Other Use Cases

A remote mobile device

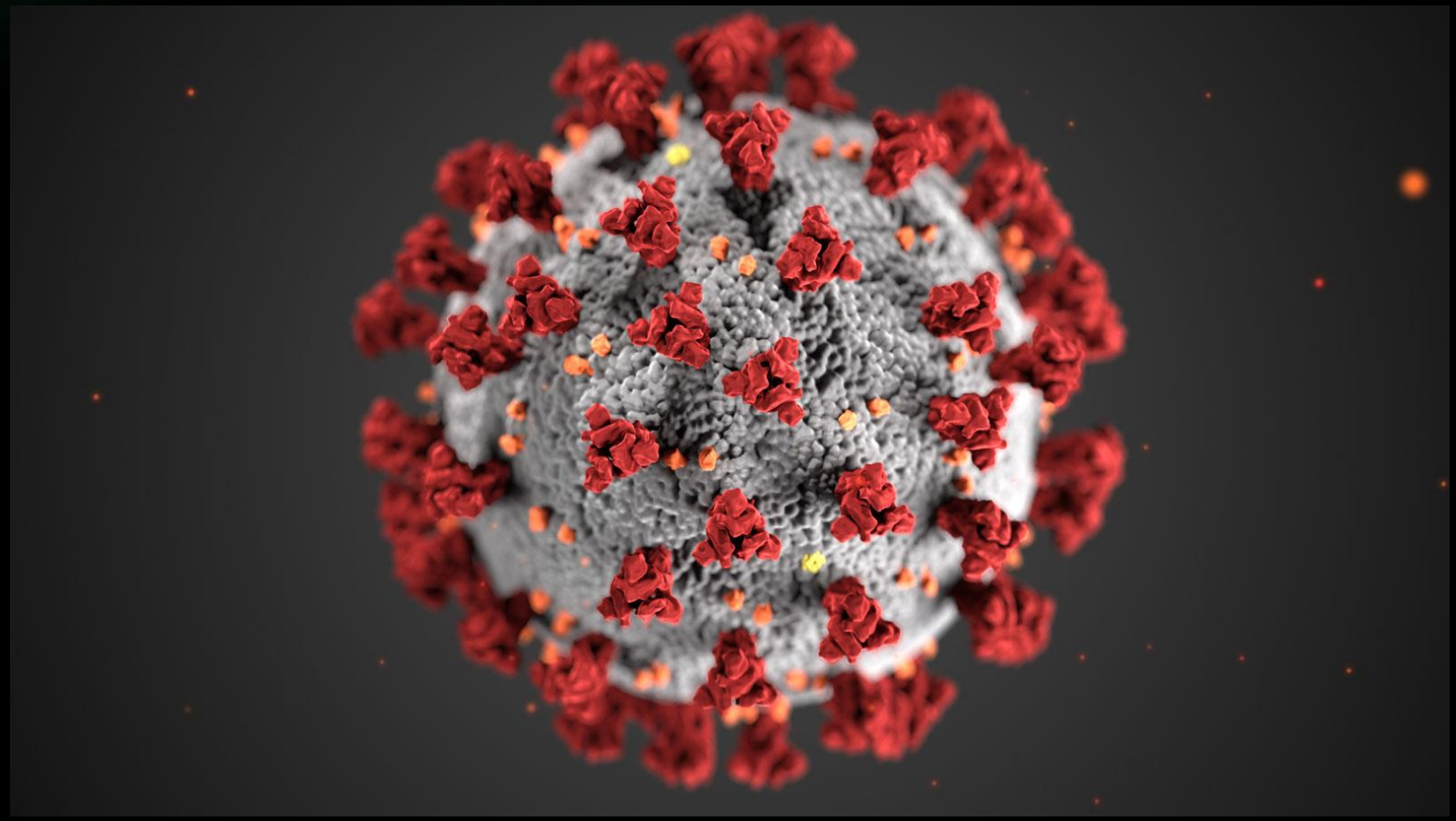
A computer cloud

Other Use Cases

A broken display

A professional spy (APT)

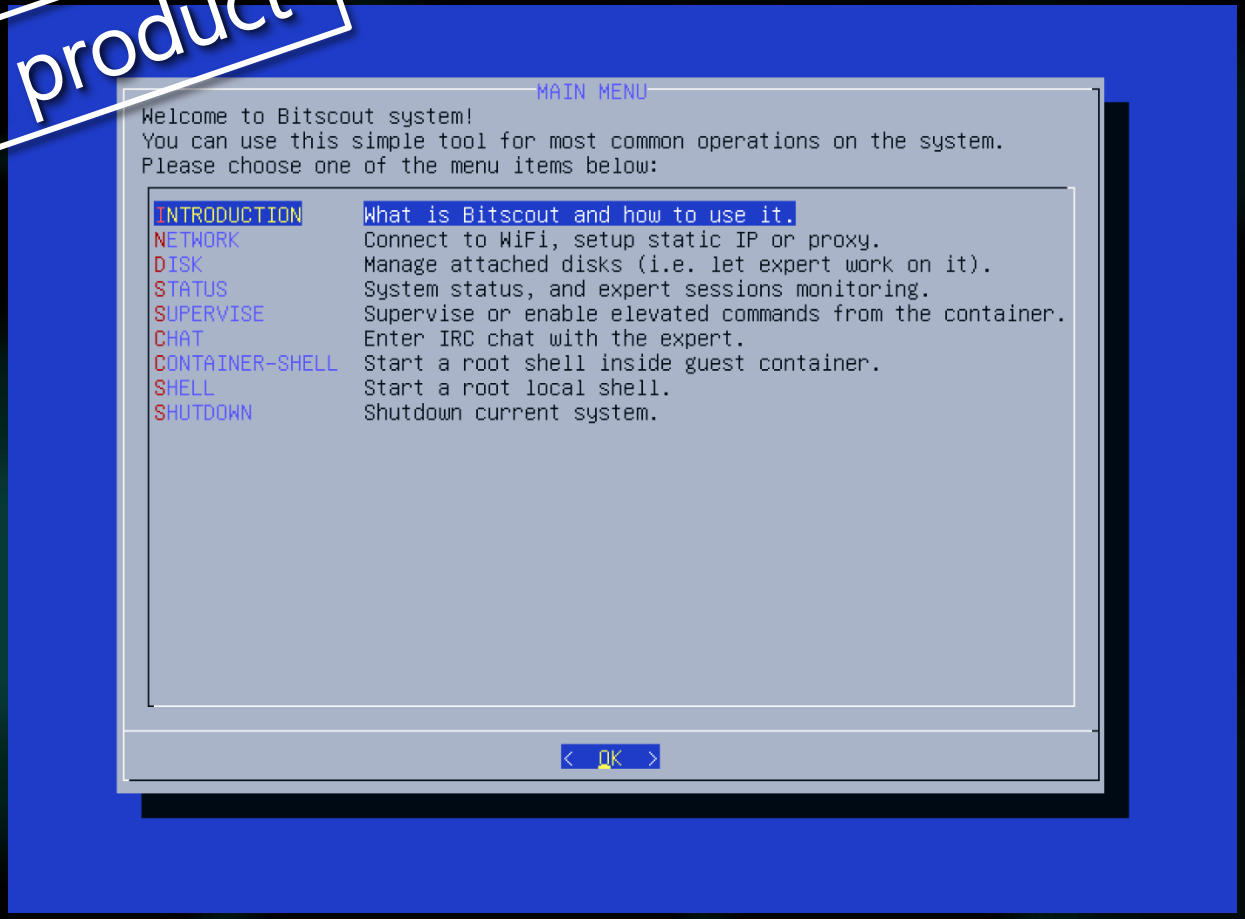
Other Use Cases



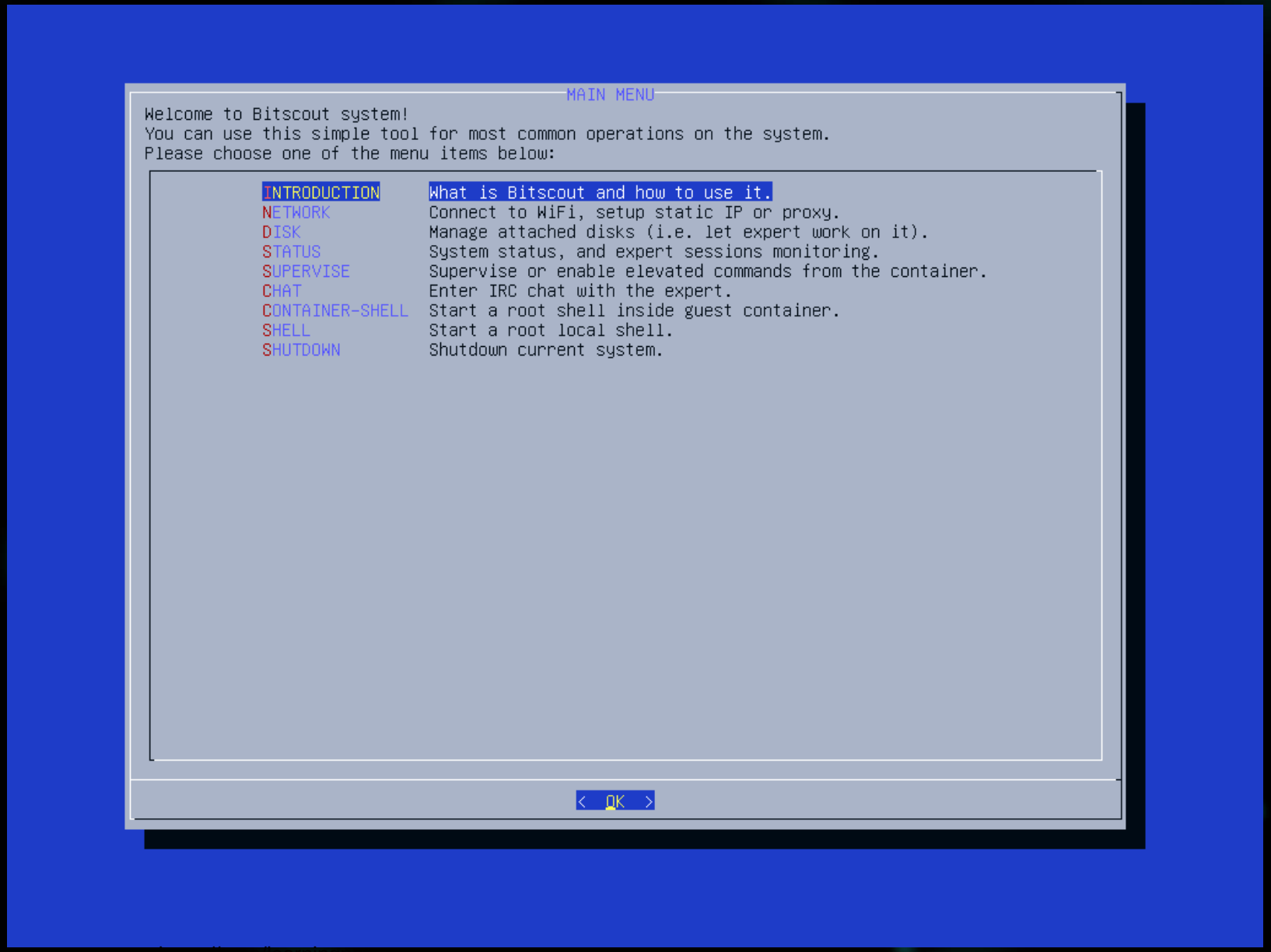
A global pandemic

Say Goodbye to Saturated GUI Fat!

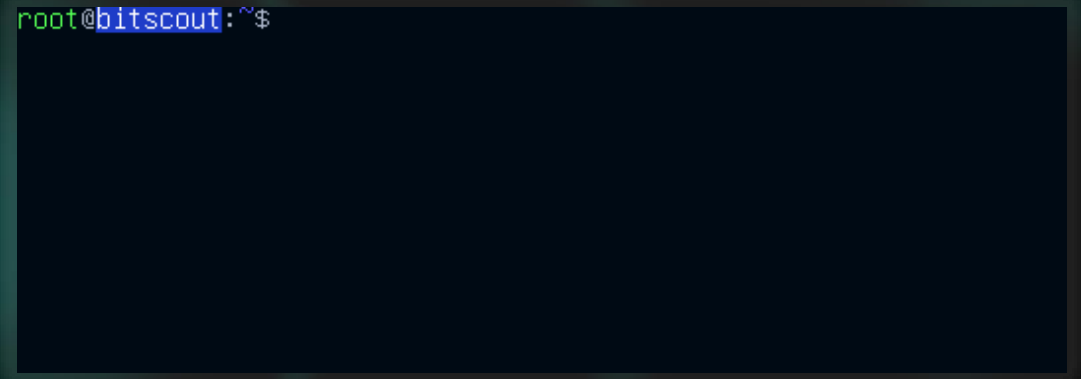
GUI-free product



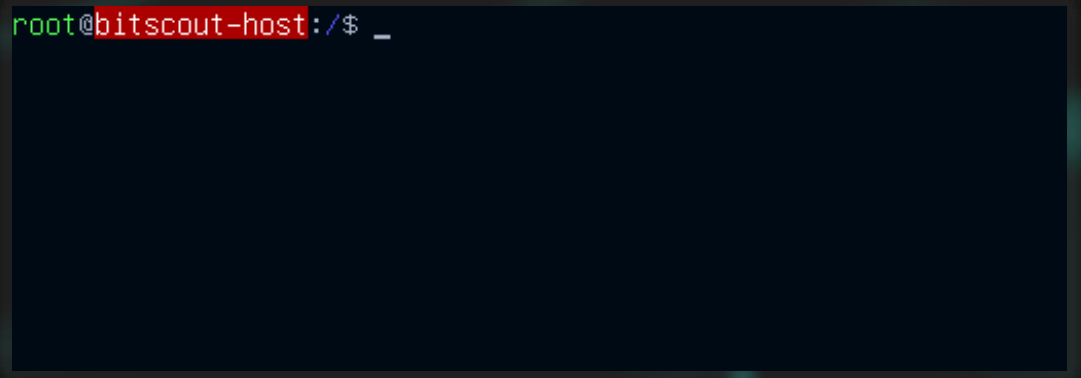
Bitscout Management Tool



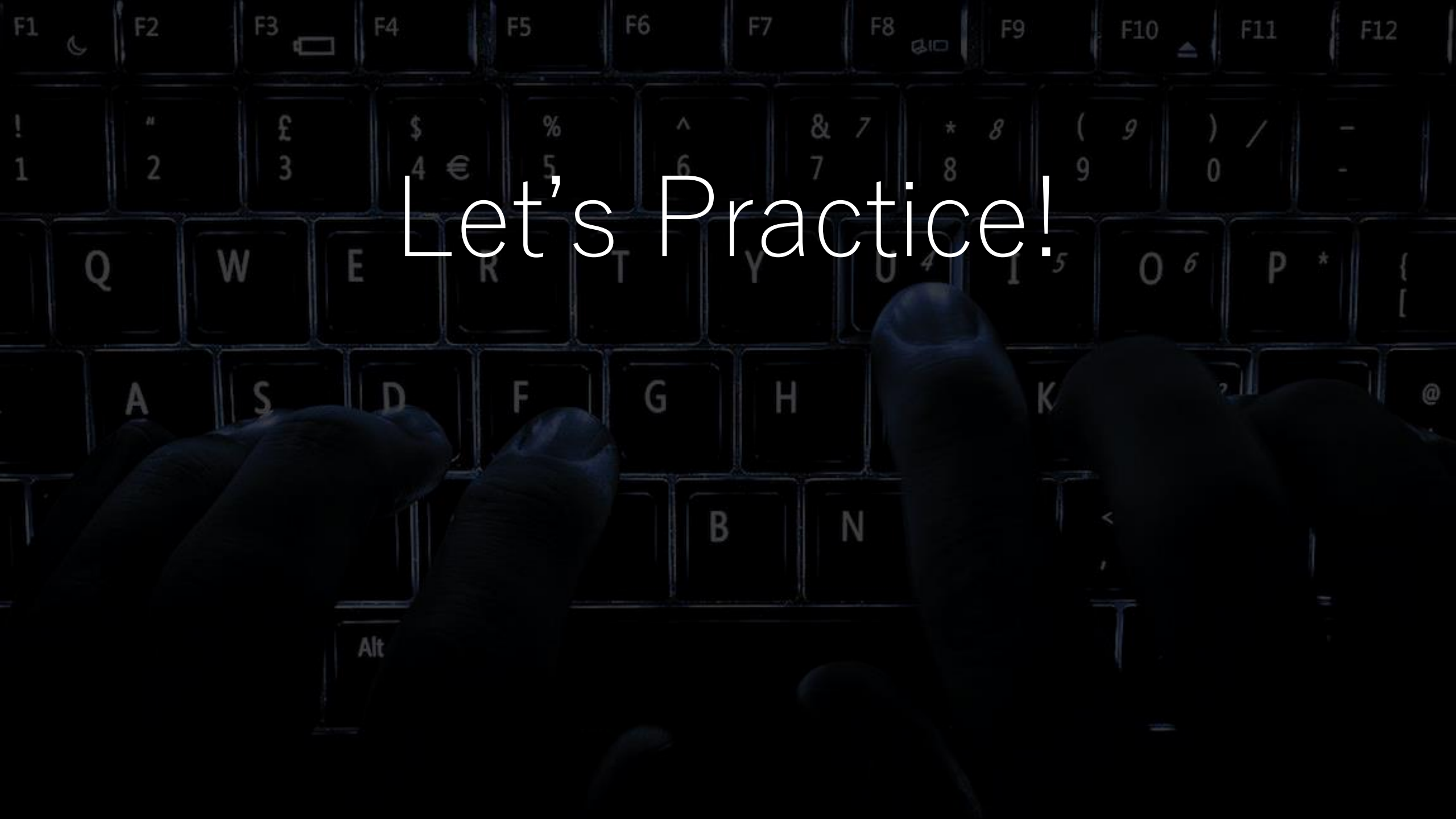
Two Types of Bitscout Shell



Bitscout Container Shell



Bitscout Host Shell


Let’s Practice!

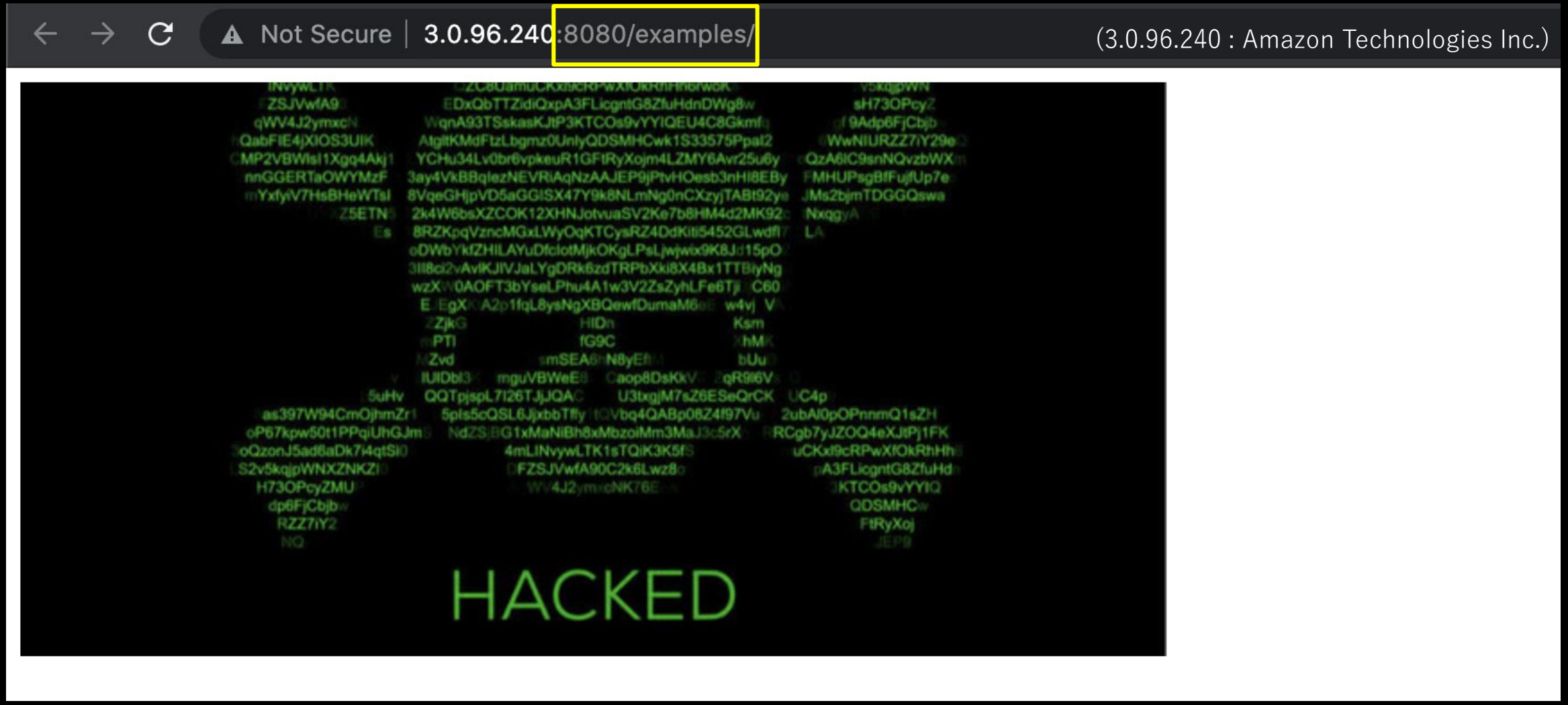
Exercise: iPhone Forensics Fundamentals

- Connect to remote Bitscout and identify iOS device via USB
- Install libimobiledevice tools and get iOS device name
- Collect full device description (firmware, hardware IDs, etc)
- Request crash dumps, sysdiagnose logs, kernel panic logs
- Get the iPhone screen contents
- Request full system backup and scan it with mvt-ios

Exercise: Intro into Cloud Forensics

- We are going to work with cloud of Bitscouts (60+)
- Connect to one server and analyze the breach
- Find all servers in the cloud containing similar filenames
- Run distributed yara scan on all servers
- Collect forensic artefacts from all servers

One of the 62 server owned by company “Lambda inc.” was reported defaced!

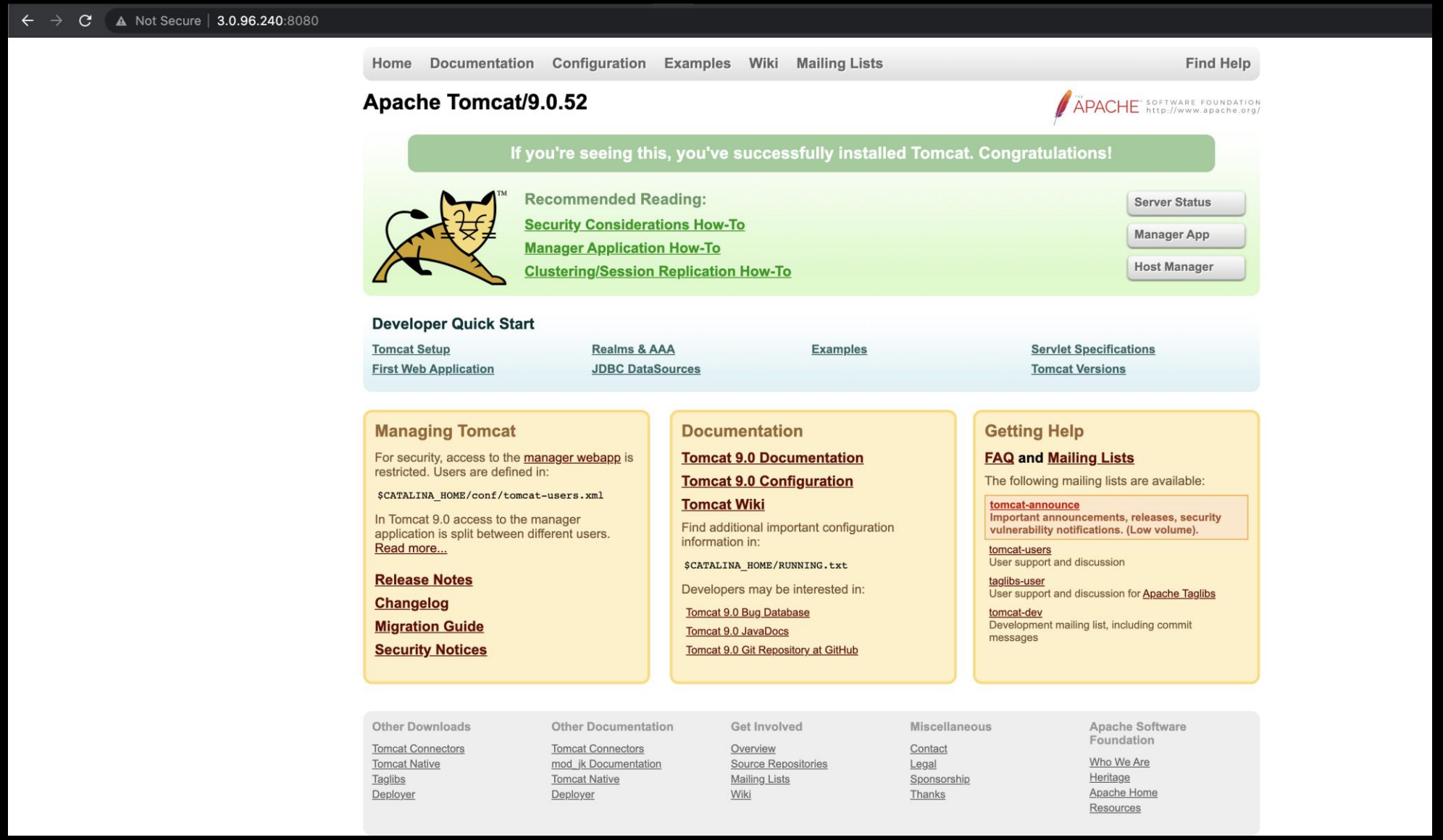


⚠ *Disclaimer: This was a simulation. Nobody was harmed in this process!*

After the “incident” was reported, the cloud administrator took a snapshot of all 62 instances and took them offline.

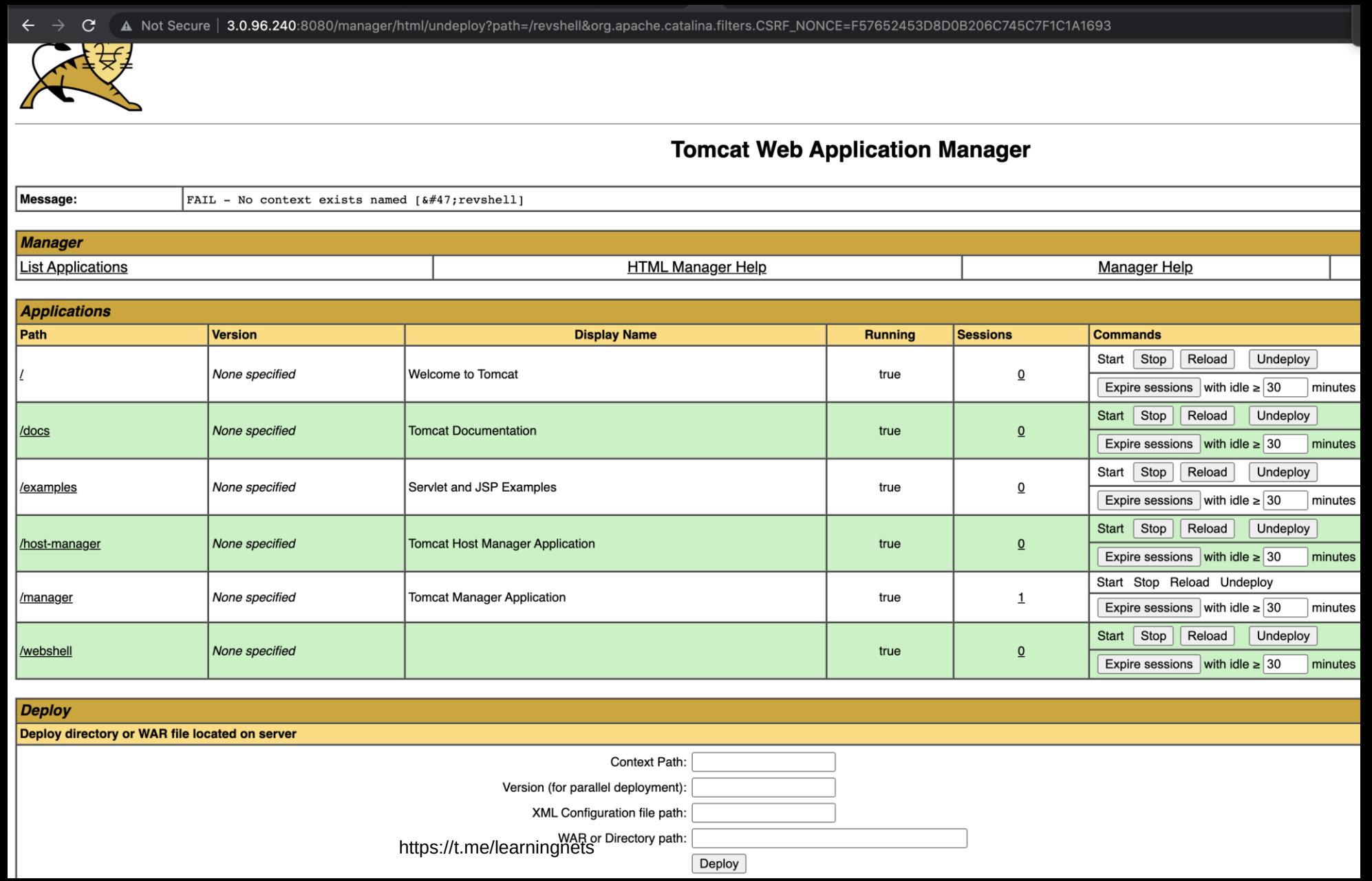
Apparently a Tomcat Manager was accessible (an probably should have not)

Access to the manager however require authentication

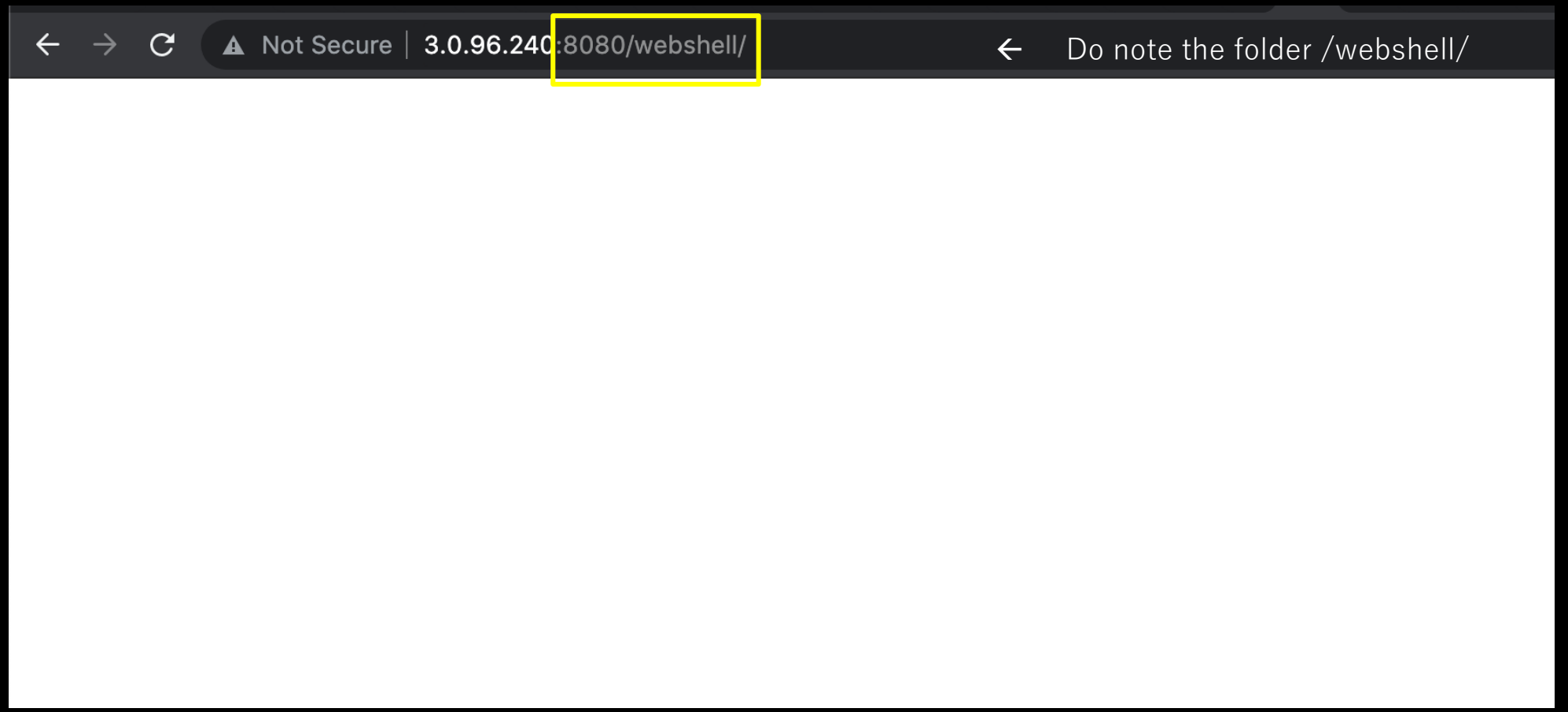


Tomcat Manager allows deploying new applications

Once logged in, new WAR files can be uploaded and started. WAR contains java web applications



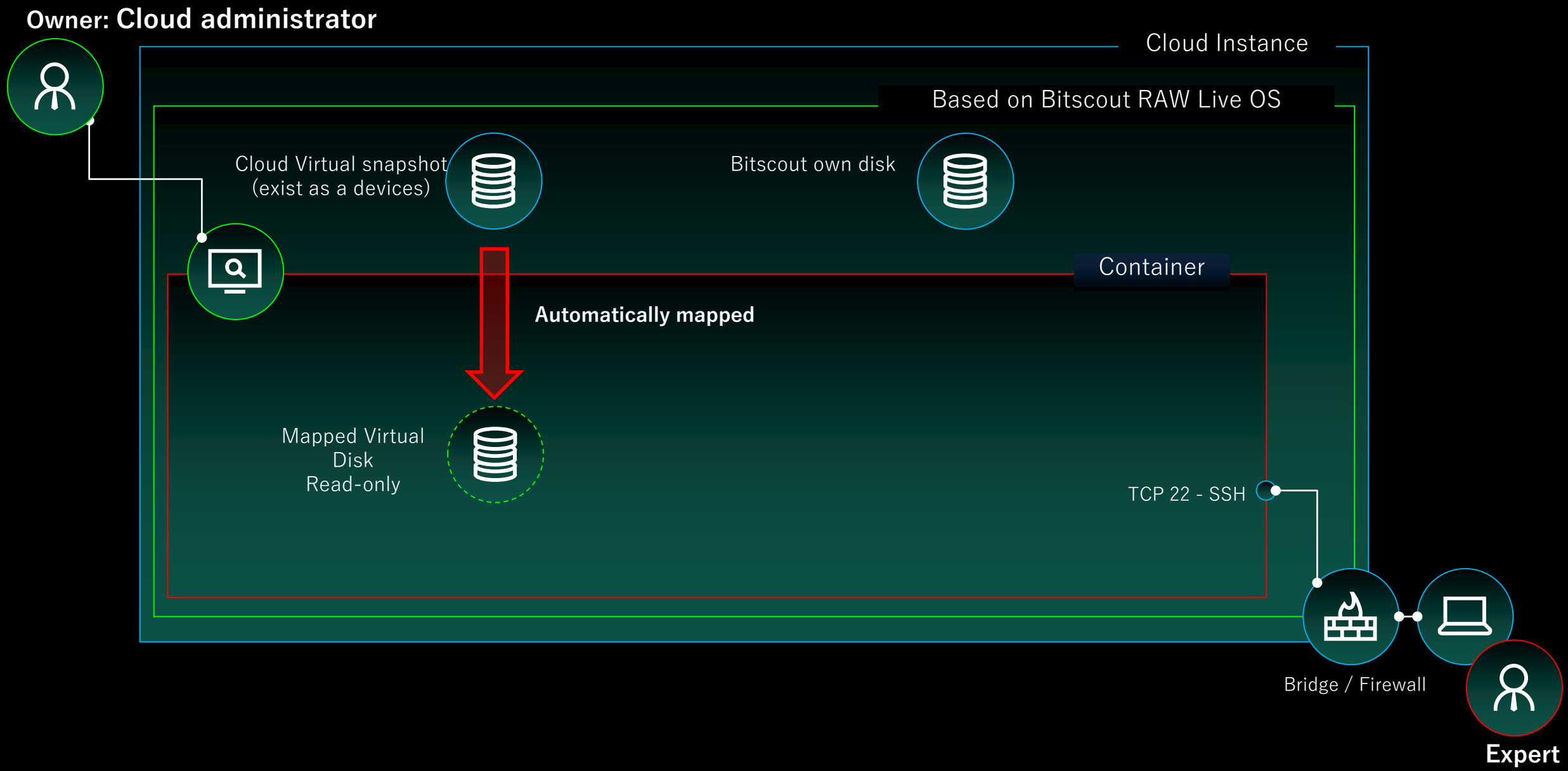
A new application (subfolder) seem to have been deployed!



We (experts) provided a RAW image and the cloud administrator started 62 instances of the bitscout image provided, attached one snapshot each and started the instances.

The credentials to read-only account was shared with us

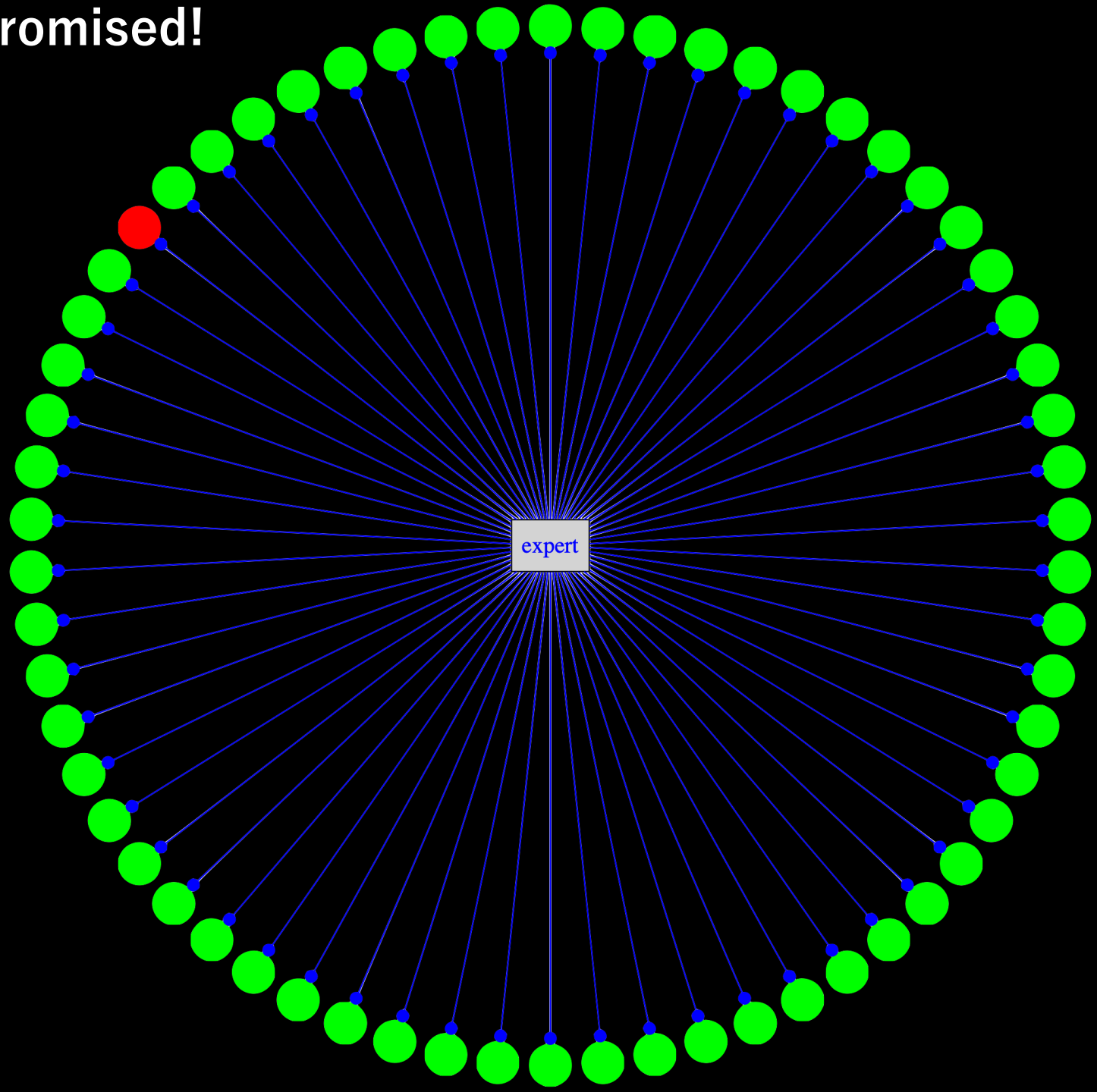
This is how the setup looks like



At least one instance is compromised!

Which instance was compromised?

Are there others instances?
What happened?

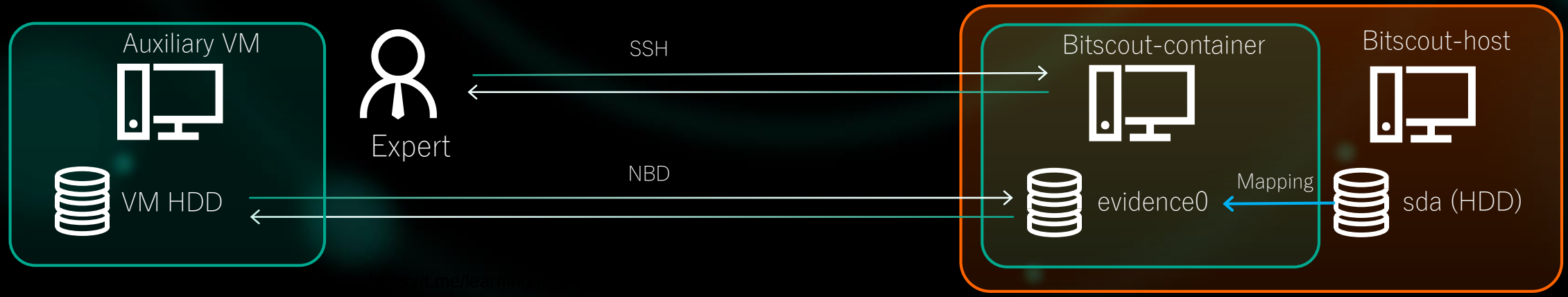


62 instances are suspected, it is a lot!
How can we do this analysis quickly and in parallel?

- Logs
- File system
- Malware artifacts

Exercise: Ransomware Attack Case

- Identify OS disks and “guide” the owner to map them
- Ask for additional USB device and mount as read-write disk
- Acquire disk image (partially just to try)
- List filesystem metadata, count the number of encrypted files
- Export the system disk over NBD protocol
- Import the NBD disk into local auxiliary VM
- Run the decryptor
- Commit changes to the disk to repair the subject system



Thank You!