

Remote Threat Reconnaissance

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.



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.

kaspersky




The Birth of The Idea

Once Upon A Time...



Hey, Vitaly, can you help me with some malware forensics? We need to find a sample...



Of course, boss! I can definitely do it!

No Flight Zone





Get shot?

Get fired?

My Plan. US8397657B2 but for cyber!

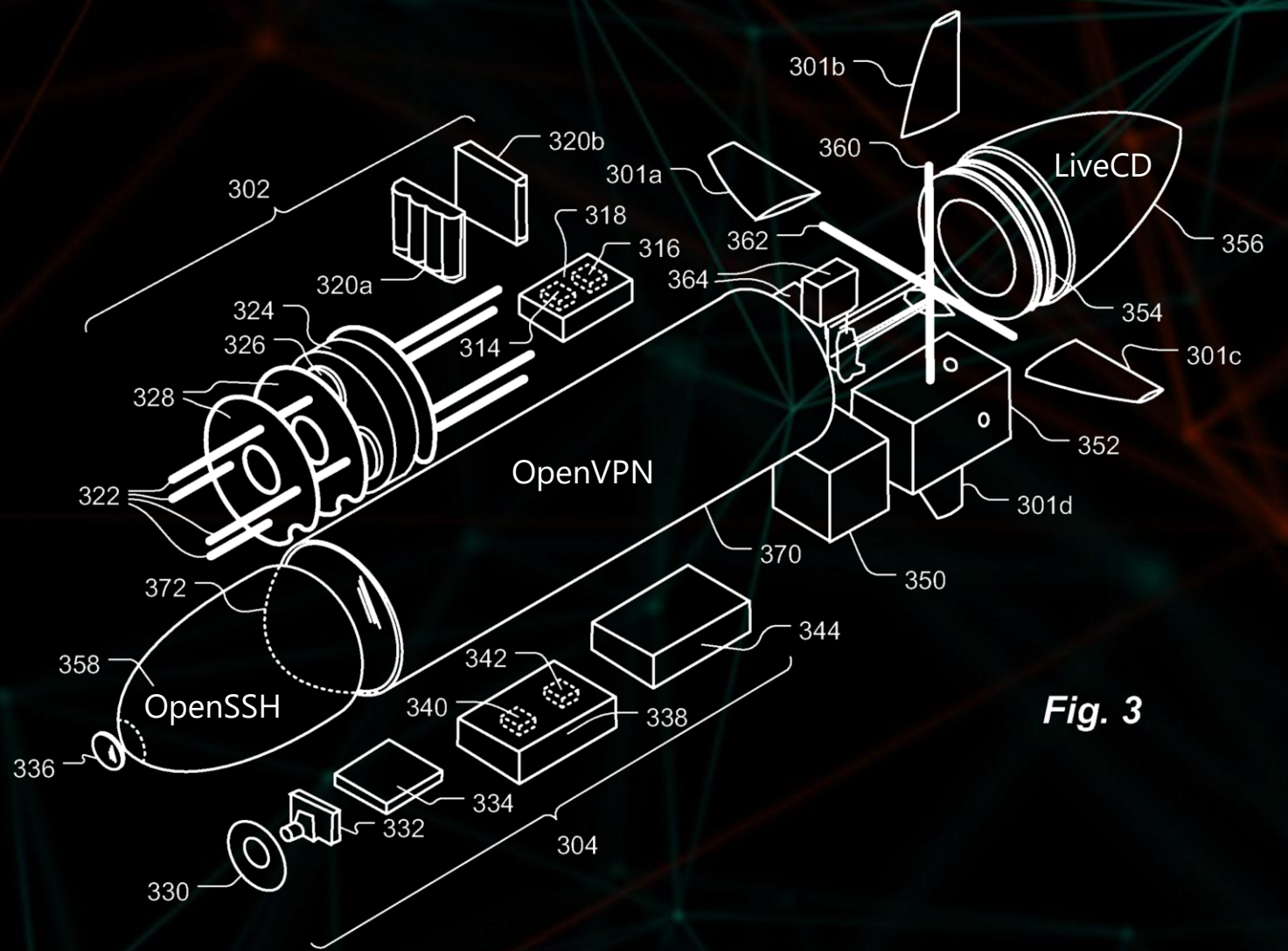
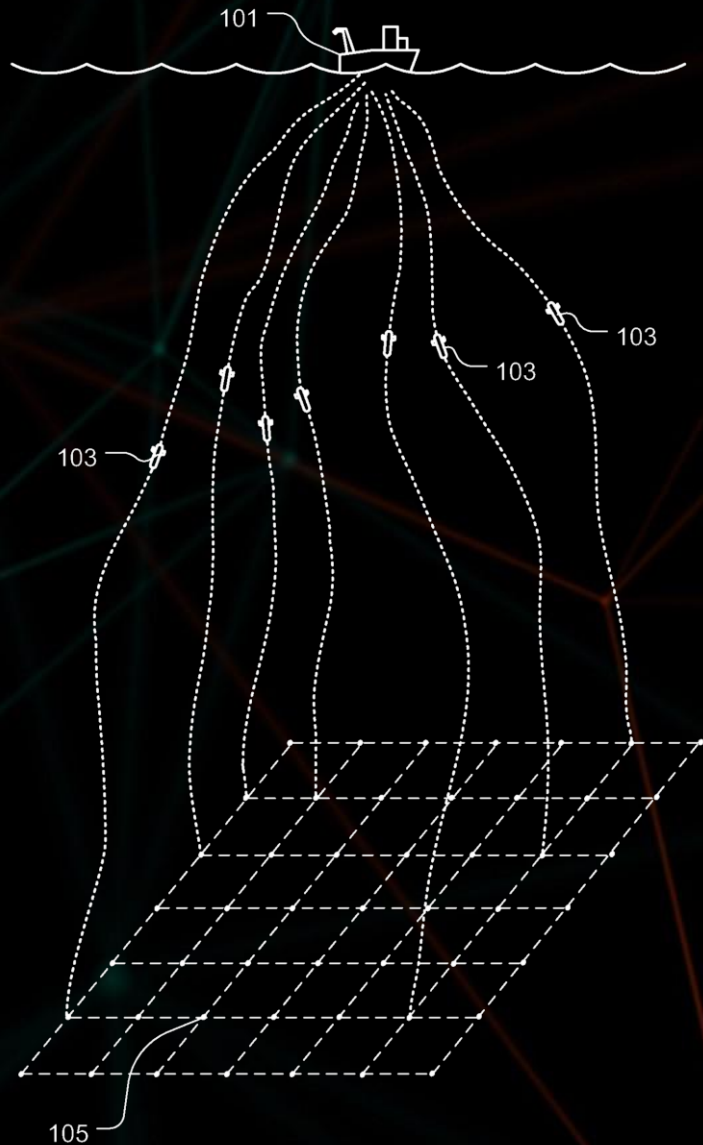
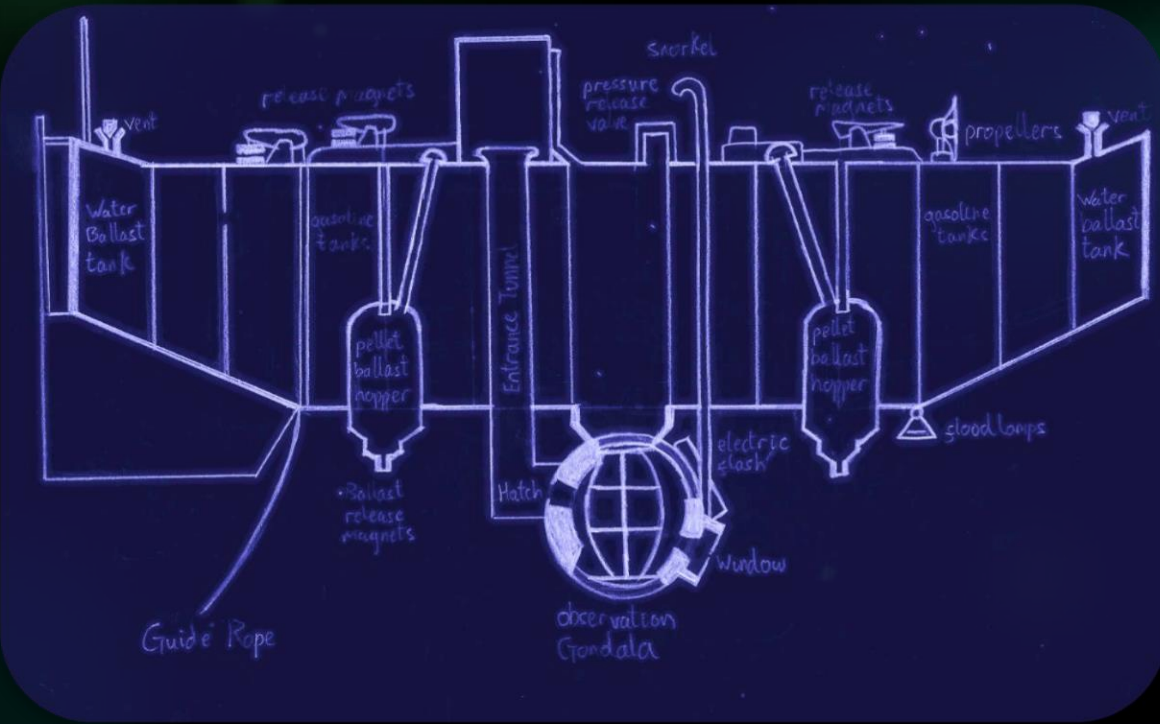
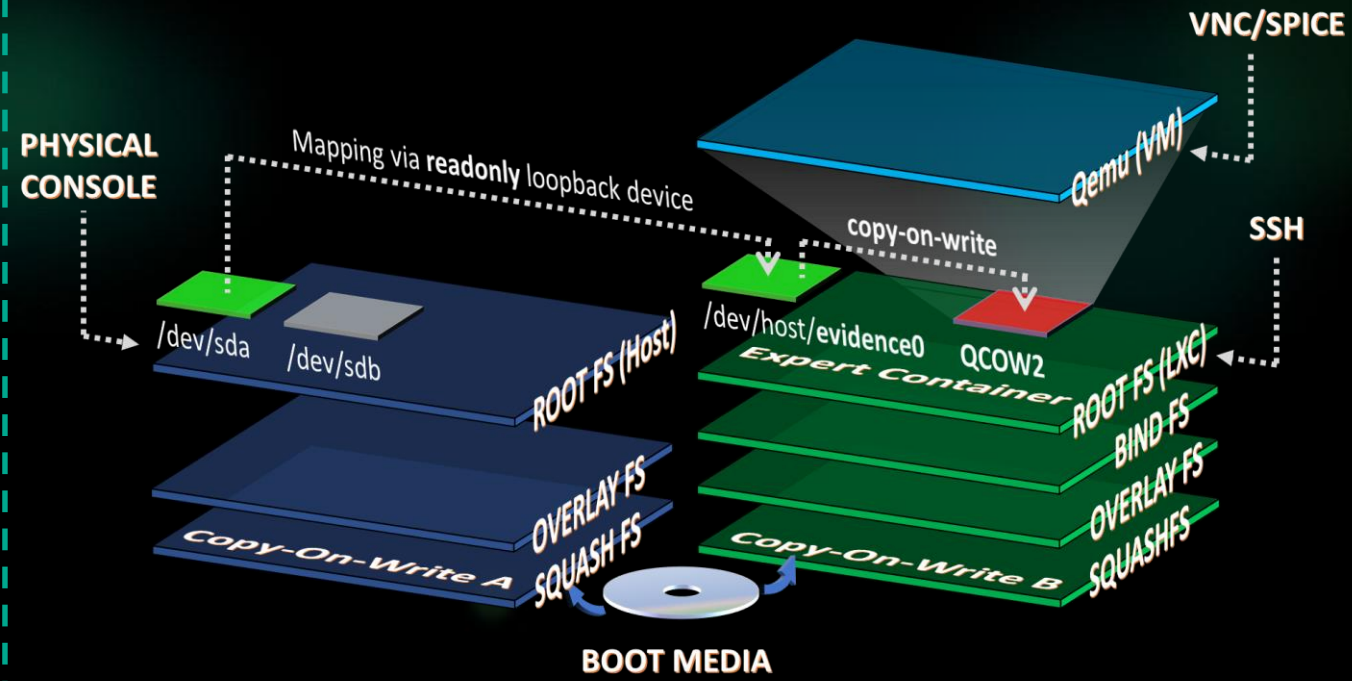


Fig. 3

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

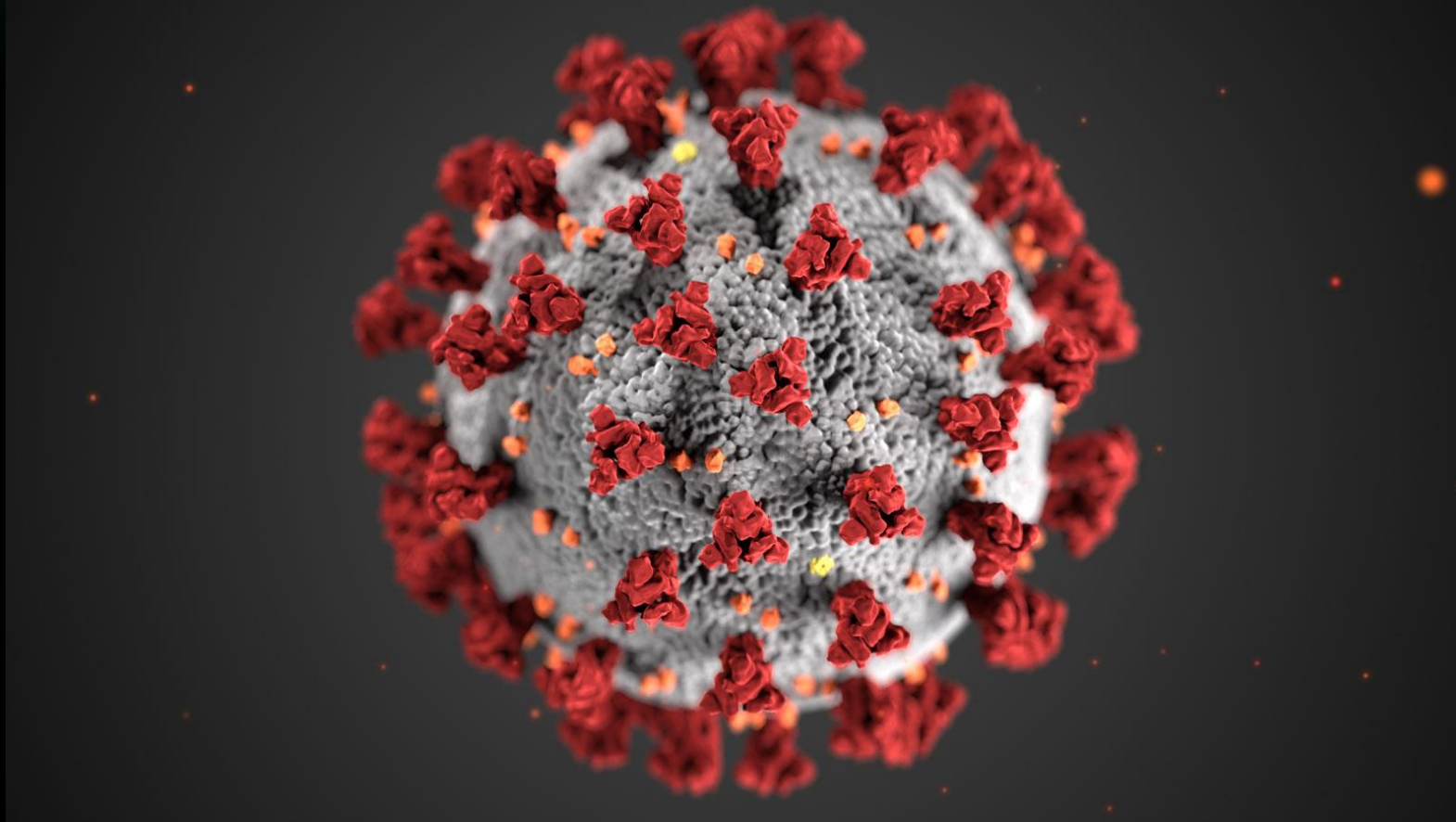


A broken display



A professional spy (APT)

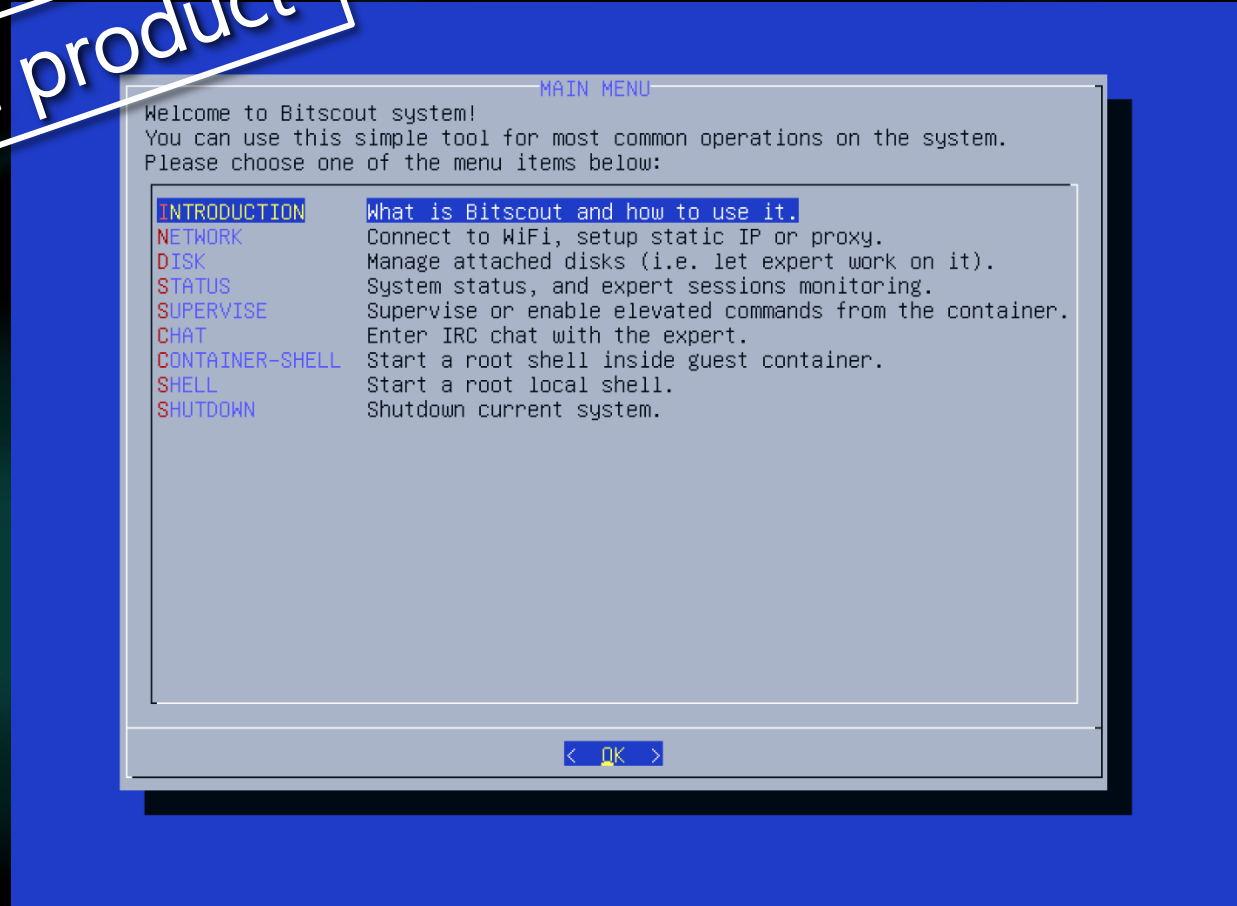
Other Use Cases



A global pandemic

Say Goodbye to Saturated GUI Fat!

GUI-free product



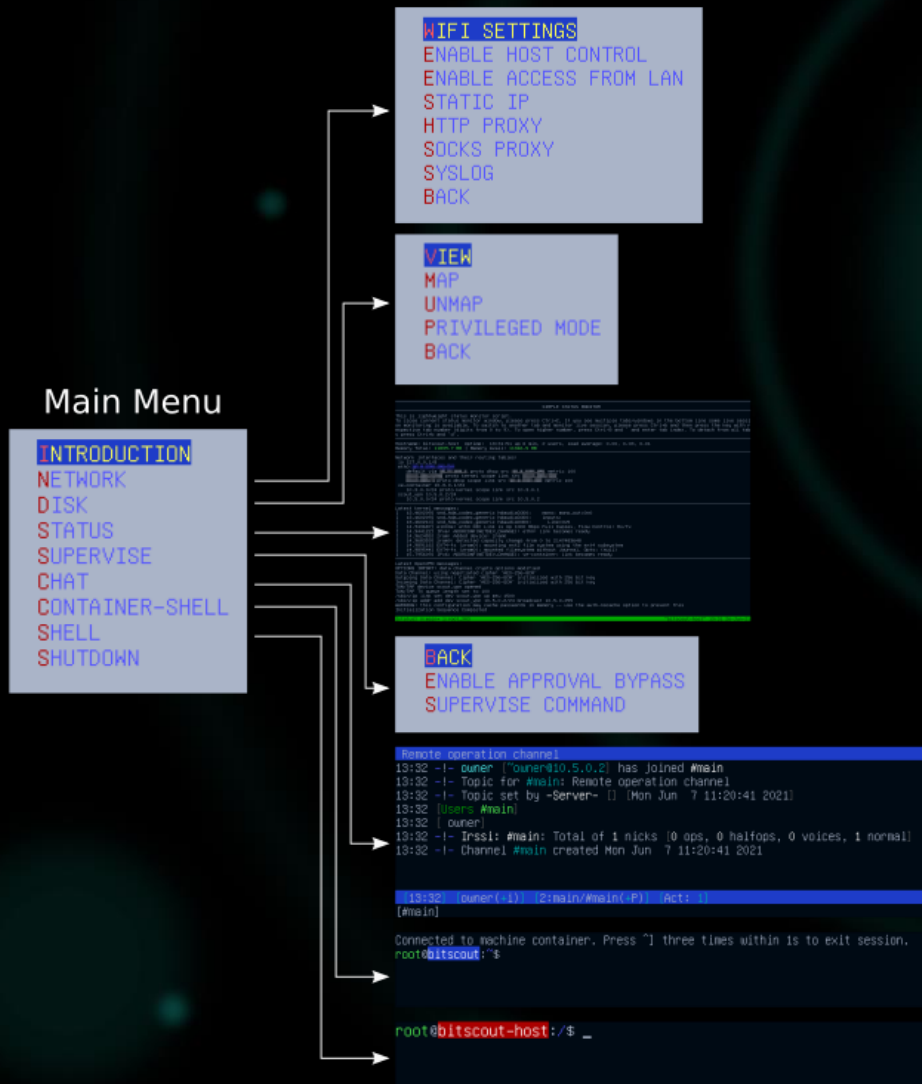
Bitscout Management Tool

```
                                MAIN MENU
Welcome to Bitscout system!
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.

                                < OK >
```

Two Types of Bitscout Shell



```
root@bitscout:~$
```

Bitscout Container Shell

```
root@bitscout-host:/$ _
```

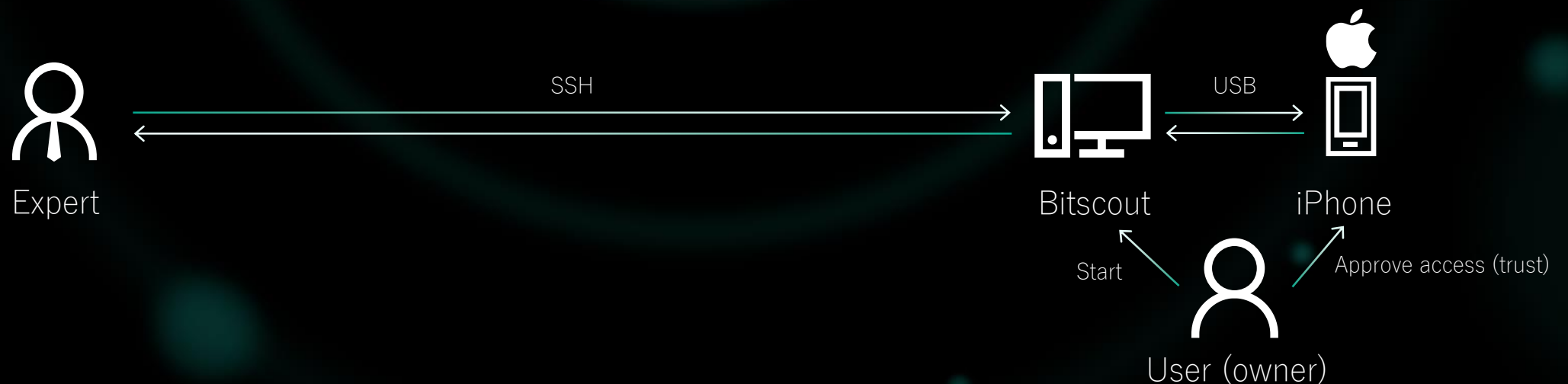
Bitscout Host Shell



Let's Practice!

Exercise: iPhone Forensics Fundamentals

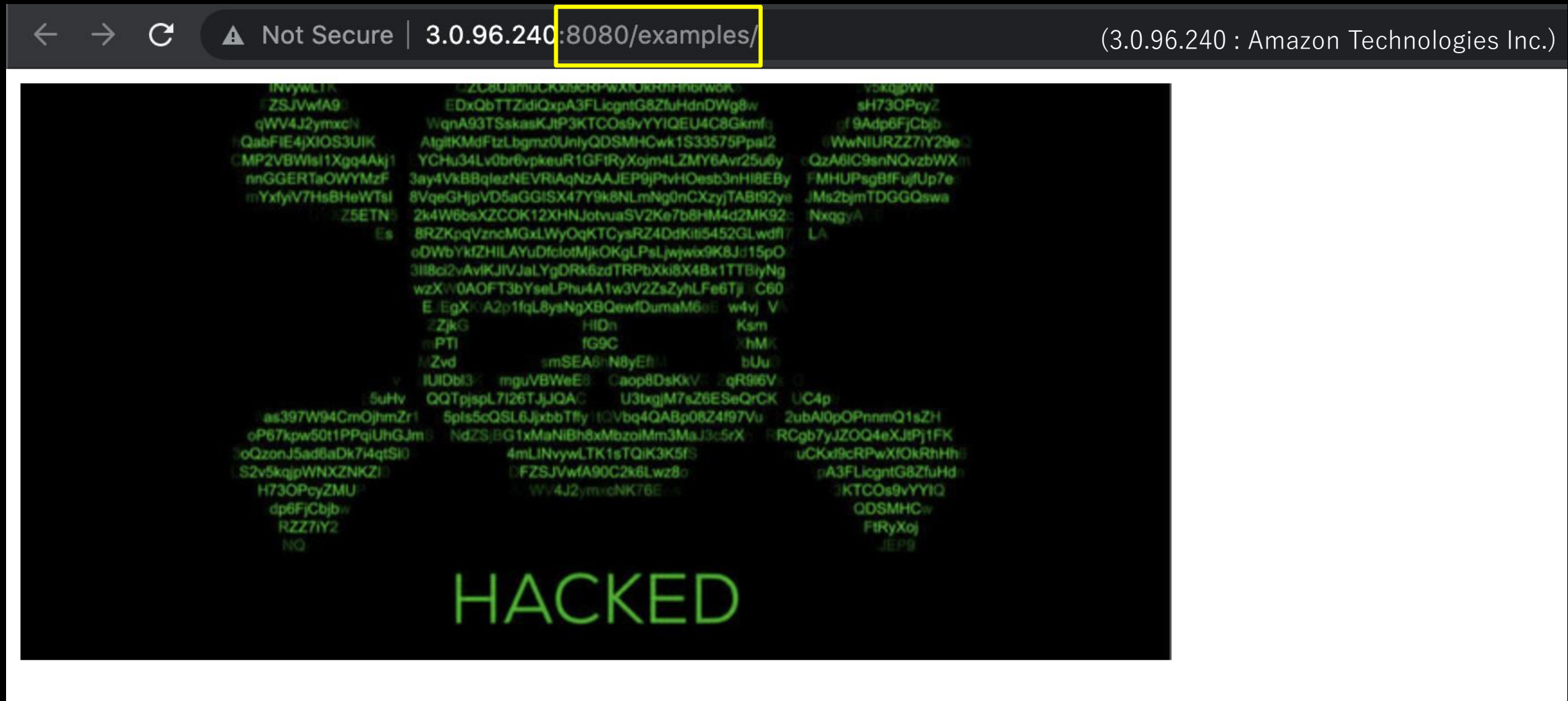
- Connect to remote Bitscout and identify iOS device via USB
- Install libimobiledevice tools and get iOS device name
- Collect full device description (firmware, hardware IDs, etc)
- Request crash dumps, sysdiagnose logs, kernel panic logs
- Get the iPhone screen contents
- Request full system backup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

← → ↻ Not Secure | 3.0.96.240:8080

Home Documentation Configuration Examples Wiki Mailing Lists Find Help

Apache Tomcat/9.0.52

If you're seeing this, you've successfully installed Tomcat. Congratulations!



Recommended Reading:

- [Security Considerations How-To](#)
- [Manager Application How-To](#)
- [Clustering/Session Replication How-To](#)

Server Status
Manager App
Host Manager

Developer Quick Start

- [Tomcat Setup](#)
- [First Web Application](#)
- [Realms & AAA](#)
- [JDBC DataSources](#)
- [Examples](#)
- [Servlet Specifications](#)
- [Tomcat Versions](#)

Managing Tomcat

For security, access to the [manager.webapp](#) is restricted. Users are defined in:

```
$CATALINA_HOME/conf/tomcat-users.xml
```

In Tomcat 9.0 access to the manager application is split between different users. [Read more...](#)

- [Release Notes](#)
- [Changelog](#)
- [Migration Guide](#)
- [Security Notices](#)

Documentation

Tomcat 9.0 Documentation

Tomcat 9.0 Configuration

Tomcat Wiki

Find additional important configuration information in:

```
$CATALINA_HOME/RUNNING.txt
```

Developers may be interested in:

- [Tomcat 9.0 Bug Database](#)
- [Tomcat 9.0 JavaDocs](#)
- [Tomcat 9.0 Git Repository at GitHub](#)

Getting Help

FAQ and Mailing Lists

The following mailing lists are available:

- [tomcat-announce](#)
Important announcements, releases, security vulnerability notifications. (Low volume).
- [tomcat-users](#)
User support and discussion
- [taglibs-user](#)
User support and discussion for [Apache Taglibs](#)
- [tomcat-dev](#)
Development mailing list, including commit messages

Other Downloads

- [Tomcat Connectors](#)
- [Tomcat Native](#)
- [Taglibs](#)
- [Deployer](#)

Other Documentation

- [Tomcat Connectors](#)
- [mod_jk Documentation](#)
- [Tomcat Native](#)
- [Deployer](#)

Get Involved

- [Overview](#)
- [Source Repositories](#)
- [Mailing Lists](#)
- [Wiki](#)

Miscellaneous


- [Contact](#)
- [Legal](#)
- [Sponsorship](#)
- [Thanks](#)

Apache Software Foundation

- [Who We Are](#)
- [Heritage](#)
- [Apache Home](#)
- [Resources](#)

Tomcat Manager allows deploying new applications

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



Tomcat Web Application Manager

Message: FAIL - No context exists named [#{revshell}]

Manager

[List Applications](#) [HTML Manager Help](#) [Manager Help](#)

Applications

Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	None specified	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/webshell	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Deploy

Deploy directory or WAR file located on server

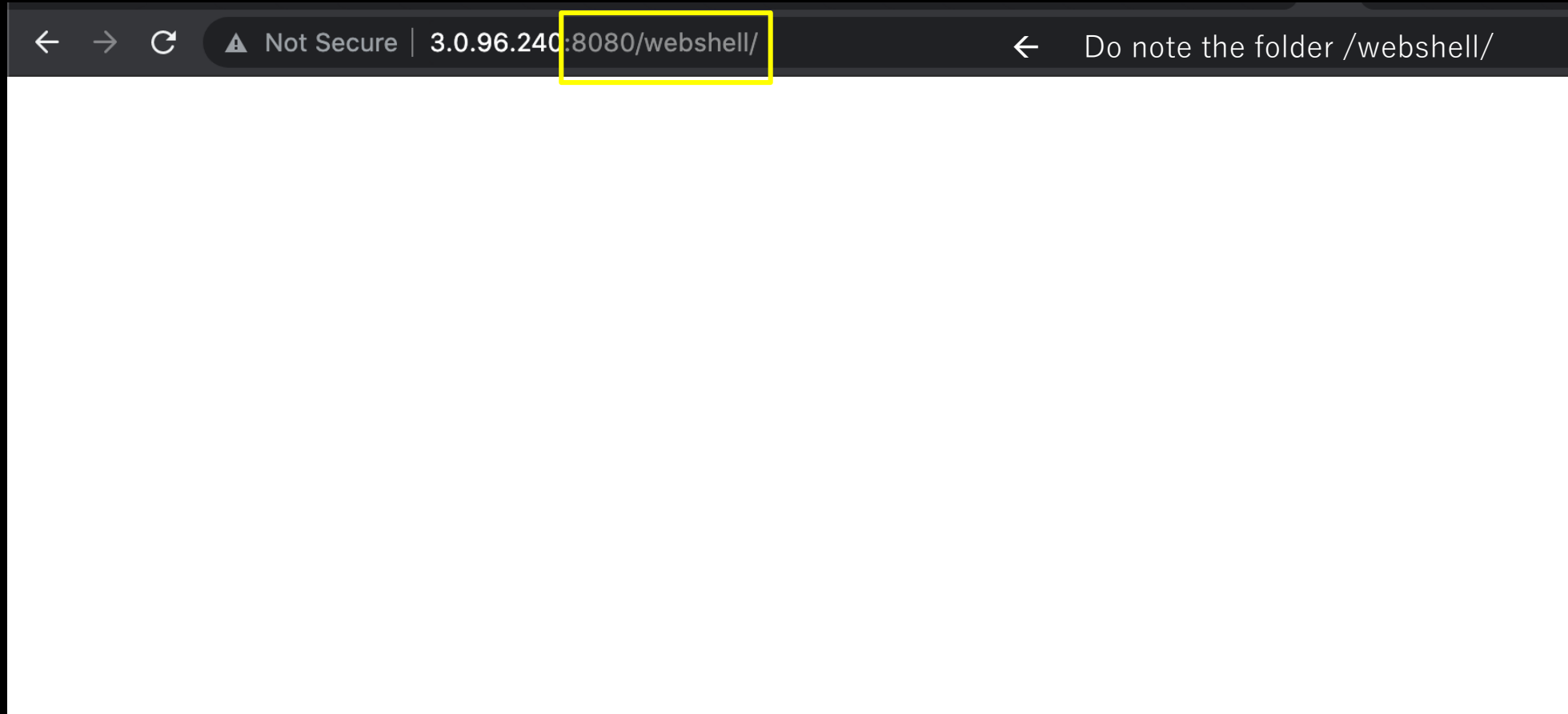
Context Path:

Version (for parallel deployment):

XML Configuration file path:

WAR or Directory path:

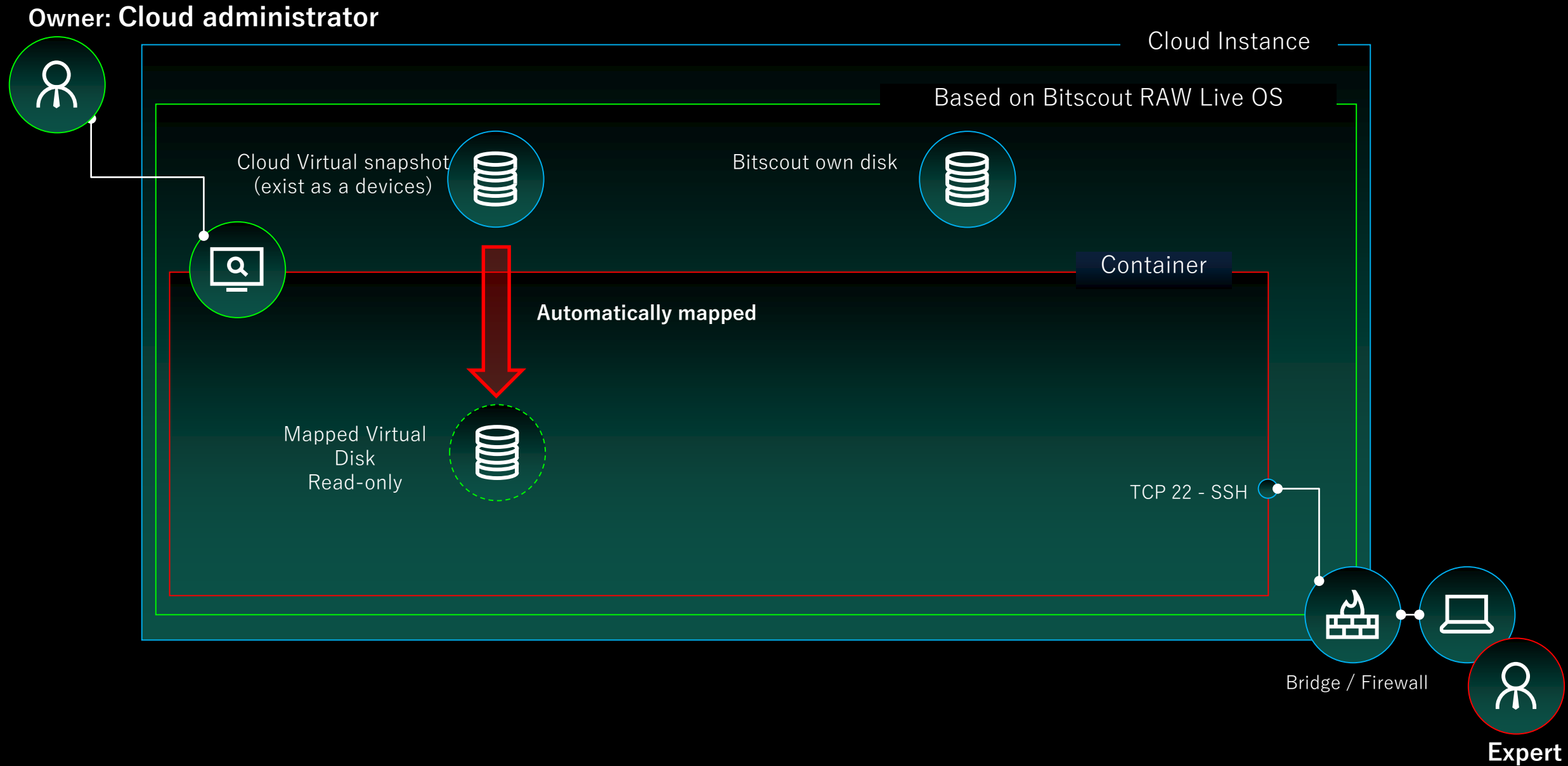
A new application (subfolder) seem to have been deployed!



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

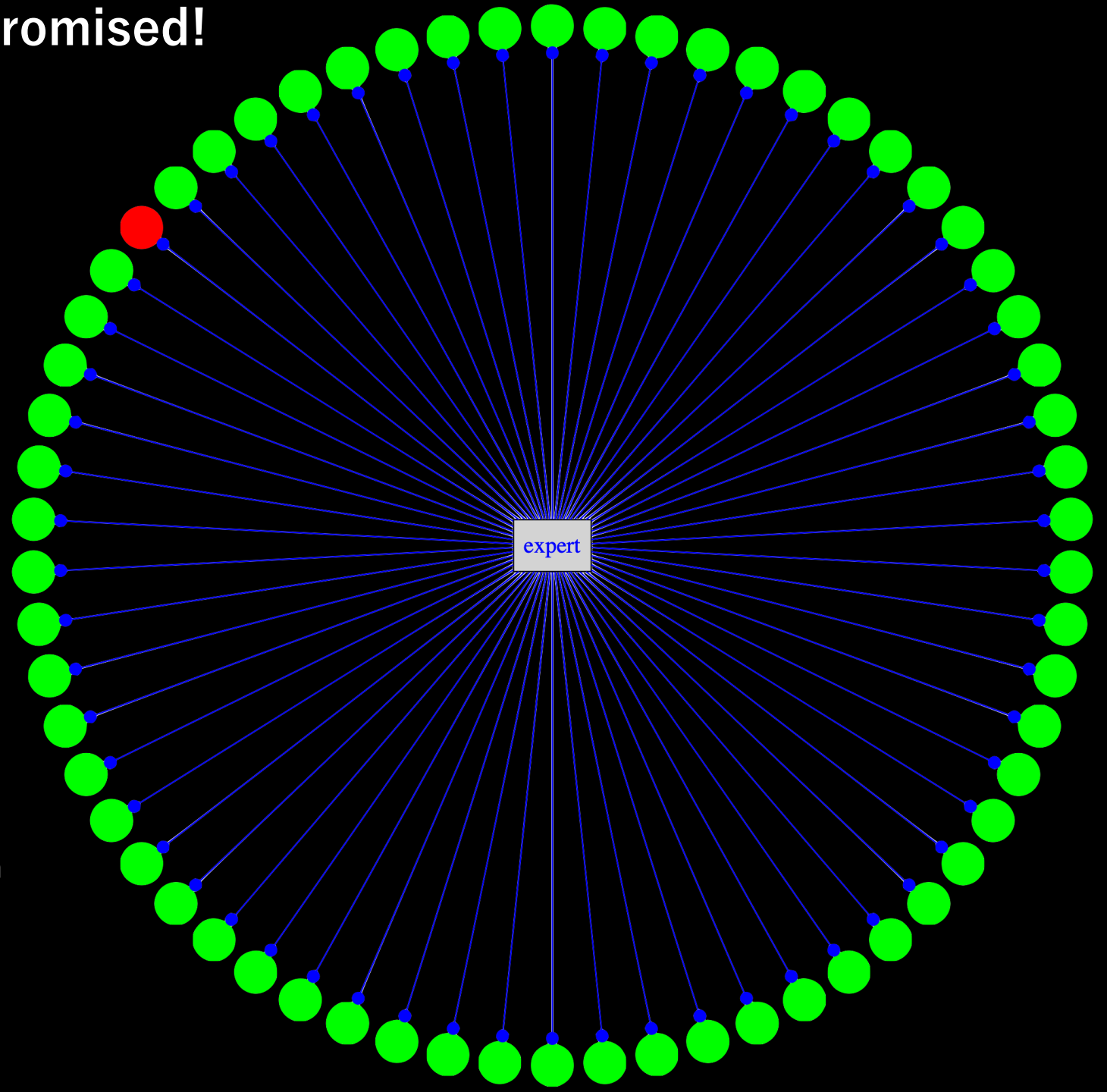


At least one instance is compromised!

Which instance was compromised?

Are there others instances?

What happened?

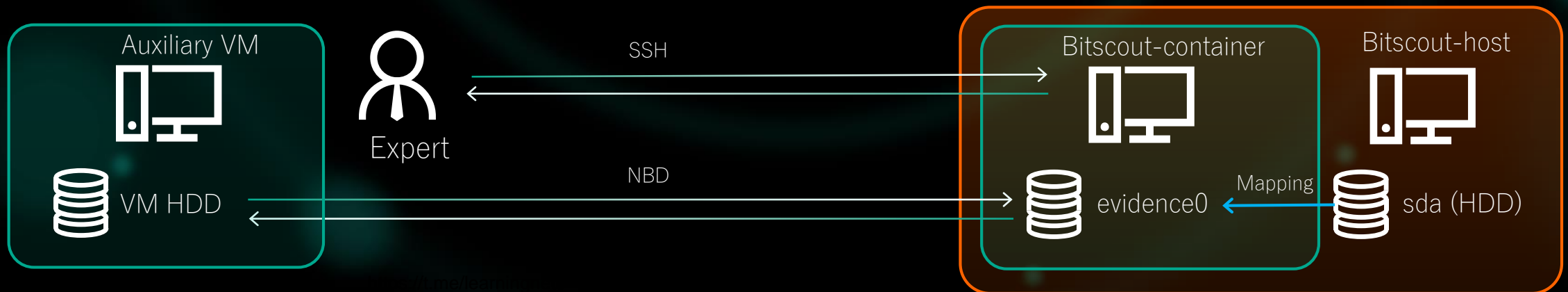


62 instances are suspected, it is a lot!
How can we do this analysis quickly and in parallel?

- 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!