Persistent Storage Acquisition – Part II

Select Deep Dives

Tobias Dussa

WP8-T1

Webinar, January 2022

Public

Game Plan

- Brief recap of the general concept.
- Discuss more interesting cases:
  - Grabbing data from afar,
  - acquiring encrypted drives,
  - handling VM images,
  - unrolling nested layers of Docker images,
  - last resorts if all else fails.
- Questions/discussion/open mike session.

STOP! A Word of Warning

We cannot and do not provide any legal counseling!

- If you know or suspect that there will be legal steps taken, talk to a lawyer first.
- Depending on your local legislation, there is a very real possibility that you inadvertently destroy evidence.

Quick Recap

The Basics

So there is some sort of persistent storage that you would like to analyze. The objective is to “rescue” as much information as possible.

- Get the data as closely from the actual physical device as possible. The “higher up” you go in the layering, the more likely you will lose interesting information.
- Make sure you have sufficient target storage available.
- Mind necessary information (crypto keys!).

The Basics – Continued

Be extra careful when handling original evidence/data/devices/master copies!

- Double-check your command lines when cloning data.
- Always store master copies safely and securely.
- Write-protect data whenever possible.
- If feasible, verify that data has been copied correctly by running checksums.

Select Interesting Cases

Far From Home

- Situation: The storage of interest is far, far away and only reachable via the Internet.
- No chance to get anything without local help (or a pre-existing login).
- Foremost question:
  - Use running system? May be easier to accomplish, but can result in problematic data.
  - Or have local hands boot a dedicated system? Possibly harder to pull off, but resulting data is clean.
- Either way: Then copy the interesting data home.

Far From Home – Approaches

Critical part: The data transfer. Possible solutions:

- **netcat**: Low-tech, simple, fast, but: plaintext, breaks easily.
- **ssh**: Secure, works well if direct connection is possible, but: harder if jumphosts involved.
- **magic-wormhole**: “Direct” transfer if possible, handshake through relay, encrypted, but: no block device support, better security requires effort.
- **croc**: Like magic-wormhole, can resume broken transfers, but: slower.

Making Sense of Gibberish

- Situation: The block device you are interested in is encrypted (using a decent cipher).
- No chance to get anywhere at all without the key.
- Usually, there are two methods to get to the key:
  - Ask the resource owner – maybe she will give you the passphrase.
  - If the system is running with the targeted device unlocked, a memory dump will very likely contain the master key.
- Then unlock the working copy of the device with the passphrase or master key.
- (Alternative approach if the system is up: Clone the content of the opened device if possible.)

Making Sense of Gibberish – Approaches

Critical part: Pulling the master key out of a memory dump. What tools to use depends heavily on the encryption method used. Examples:

- LUKS volumes:
  - **findaes** to grab master keys,
  - regular **cryptsetup** to open crypto volumes.
- Bitlocker:
  - **volatility** to grab Full Volume Encryption Keys (FVEKs),
  - **bdemount** to open crypto volumes.

Normalizing Drives

- Situation: The storage device you are interested in is a VM image file.
- Depending on the image format and the tools used, this will not work for forensic analysis.
- Solution: Convert the image file into a more palatable format.

Normalizing Drives – Approaches

As in the previous example, the exact tools to use depend on the particular problem and format used. For many (most?) situations, these tools should help:

- **`qemu-img`**: Converting a lot of formats to/from raw disk, managing qemu/KVM snapshots.
- **`vmware-vdiskmanager`**: Flattening VMDK snapshots.
- **`VBoxManage`**: Flattening VDI snapshots.

Unpacking Russian Dolls

- Situation: The storage of interest is a Docker image.
- This is not suitable for direct analysis.
- Solution: Again, unpack the image.

Unpacking Russian Dolls – Approaches

This one is a very straightforward problem for a change. There are tools that will do just that (and, indeed, you *can* theoretically even unroll Docker images by hand):

- **undocker**: Analyzes and unpacks Docker images.
- **dive**: Alternative tool to explore Docker images interactively.

Last Resorts

- Situation: You cannot get the data off the remote system. At all. No chance.
- No way to use your lab equipment and your usual environment.
- Solution: Bring as many tools as practical *to the data* if you cannot bring the data to the tools. Also, make use of whatever tools are already installed.

Last Resorts – Approaches

Obviously, this is an extremely non-specific situation, so here are some generally helpful tools to bring along, preferably *built statically*:

- **`testdisk`**: Analyzes and browses block devices.
- The Sleuth Kit: Entire toolkit to collect forensic information on a block device.

Wrap-Up

Recap

- **netcat**: https://sourceforge.net/projects/openbsd-netcat, http://netcat.sourceforge.net
- **ssh**: https://www.openssh.com
- **magic-wormhole**: https://github.com/magic-wormhole/magic-wormhole
- **croc**: https://github.com/schollz/croc
- **findaes**: https://sourceforge.net/projects/findaes
- **cryptsetup**: https://gitlab.com/cryptsetup/cryptsetup
- **volatility**: https://github.com/volatilityfoundation/volatility, https://github.com/elceef/bitlocker
- **bdemount**: https://github.com/libyal/libbde
- **qemu-img**: https://www.qemu.org
- **vmware-vdiskmanager**: https://www.vmware.com
- **VBoxManage**: https://www.virtualbox.org
- **undocker**: https://github.com/larsks/undocker
- **dive**: https://github.com/wagoodman/dive
- **testdisk**: https://github.com/cgsecurity/testdisk
- The Sleuth Kit: https://github.com/sleuthkit/sleuthkit

Be Flexible

- In forensics, the nitty-gritty details matter.
- The more complex the situation, the more likely it is that you need to come up with creative solutions, **but**:
- You need to be mindful of the bigger picture and always stay on the safe and secure side.
- Get all the help you can!

GÉANT
Networks • Services • People

Thank you

Any questions?

www.geant.org

The research leading to these results has received funding from the European Union’s Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2).