## **Remote Forensic Investigations** (In the Context of COVID-19)



Xavier Mertens | PTS20 | July 2020



# Who's Talking?

- Xavier Mertens (@xme)
- 3rd time speaker @ PTS
- Freelance based in Belgium
- Blueteamer
- SANS ISC Senior Handler
- BruCON Co-Organizer



![](_page_1_Picture_8.jpeg)

![](_page_1_Picture_9.jpeg)

# 

... 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...

![](_page_2_Picture_3.jpeg)

![](_page_2_Picture_4.jpeg)

## 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)

	Ooops, your files have been encrypted!	English	
1	What Happened to My Computer? Your important files are encrypted. Many of your documents, photos, videos, databases and other files accessible because they have been encrypted. Maybe you are busy recover your files, but do not waste your time. Nobody can recover our decryption service.	are no longer looking for a way to your files without	
Payment will be raised on 1/4/1970 01:00:00 Time Left	Can I Recover My Files? Sure. We guarantee that you can recover all your files safely and earnot so enough time. You can decrypt some of your files for free. Try now by clicking <d 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 we Also, if you don't pay in 7 days, you won't be able to recover your f</d 	our files safely and easily. But you have ry now by clicking <decrypt>. eed to pay. After that the price will be doubled. able to recover your files forever.</decrypt>	
Your files will be lost on         1/8/1970 01:00:00         Time Left         21211 21211 21211 2121	We will have free events for users who are so poor that they could How Do I Pay? Payment is accepted in Bitcoin only. For more information, click <br Please check the current price of Bitcoin and buy some bitcoins. For click <how bitcoins="" buy="" to="">. And send the correct amount to the address specified in this window After your payment, click <check payment="">. Best time to check: 9:</check></how>	n't pay in 6 months. About bitcoin>. r more information w. 00am - 11:00am	
About bitcoin How to buy bitcoins?	Send \$600 worth of bitcoin to this addr ACCEPTED HERE Send \$600 worth of bitcoin to this addr 13AM4VW2dhxYgXeQepoHkHSQuy6N	ess: gaEb94	
Contact Us	Check Payment D	ecrypt	

#### (May, 12 2017 07:44 UTC)

![](_page_3_Picture_7.jpeg)

# 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 "compromised" host in safe way
- **Basic artefacts** 
  - Filesystem
  - Memory
  - Registry
- Isetu
  - Application data (browsing history, ...)

![](_page_4_Picture_11.jpeg)

## **Forensic 101** Toolbox

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

![](_page_5_Picture_9.jpeg)

# SIFT Workstation

The SIFT Workstation is a group of free open-source incident forensic examinations in a variety of settings.

<u>Step 1 - Attach Local or Remote System Drive</u> <b># ewfmount system-name.E01 /mnt/ewf</b> <u>Step 2 - Mount VSS Volume</u>	<u>Fil</u> fsstat	le Syster -Display # fsst
<pre># cd /mnt/ewf # vshadowmount ewf1 /mnt/vss</pre>		<u>Data</u>
Step 3 – Run fls across ewf1 mounted image	blkcat	-Display # b1kc
<pre># fls -r -m C: ewf1 &gt;&gt; /cases/vss- bodyfile</pre>	blkls	-Lists c # b1k1
Step 4 – Run fls Across All Snapshot Images # cd /mnt/vss	blkcald	-Maps H # blk
<pre># for i in vss*; do fls -r -m C: \$i &gt;&gt; /cases/vss-bodyfile; done</pre>	blksta	t -Displ # blks
<pre>Step 5 - De-Duplicate Bodyfile using sort and uniq # sort /cases/vss-bodyfile   uniq &gt; /cases/vss-dedupe-bodyfile</pre>	Mata	ata I az
Step 6 – Run mactime Against De-Duplicated Bodyfile # mactime -d -b /cases/vss-dedupe-	ils	-Display # <b>i1s</b>
bodyfile -z EST5EDT MM-DD-YYYYMM- DD-YYYY > /cases/vss-timeline.csv	istat	-Display # ista
Memory Analysis	icat	-Display # icat
<pre>vol.py command -f /path/to/windows_xp_memory.img profile=WinXPSP3x86</pre>	ifind	-Detern # ifir
[Supported commands] connscan Scan for connection objects files list of open files process	fls	-Display
imagecopy Convert hibernation file procdump Dump process pslist list of running processes sockscan Scan for socket objects	ffind	-Find th # ffir

#### The SIFT Workstation is a group of free open-source incident response and forensic tools designed to perform detailed digital

#### Sleuthkit Tools

#### m Layer Tools (Partition Information)

ys details about the file system tat imagefile.dd

#### a Layer Tools (Block or Cluster)

ys the contents of a disk block at imagefile.dd block\_num

contents of deleted disk blocks s imagefile.dd > imagefile.blkls

between dd images and blkls results calc imagefile.dd -u blkls\_num

lay allocation status of block stat imagefile.dd cluster\_number

#### ver Tools (Inode, MFT, or Directry Entry)

ys inode details imagefile.dd

ys information about a specific inode at imagefile.dd inode\_num

ys contents of blocks allocated to an inode t imagefile.dd inode\_num

mine which inode contains a specific block nd imagefile.dd -d block\_num

#### Filename Layer Tools

ys deleted file entries in a directory inode -rpd imagefile.dd

he filename that using the inode nd imagefile.dd inode\_num

![](_page_6_Picture_20.jpeg)

#### SIFT WORKSTATION Cheat Sheet v3.0

http://computer-forensics.sans.org http://blogs.sans.org/computer-forensics

SANS DFIR

#### 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

![](_page_6_Picture_38.jpeg)

7

# 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
- Low bandwidth usage: process data remotely

![](_page_7_Picture_11.jpeg)

# Bitscout

- 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"

#### "A customizable Live OS constructor tool almost entirely written in Bash"

![](_page_8_Picture_11.jpeg)

![](_page_8_Picture_12.jpeg)

## **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

![](_page_10_Figure_1.jpeg)

Welcome to	Bitscout system!	THEN HENO			
Customized You can us Please cho	by Xavier Mertens e this simple tool ose one of the men	Consulting – Contact: csirt@xameco.net for most common operations on the system. u items below:			
	INTRODUCTION NETWORK DISK STATUS SUPERVISE CHAT CONTAINER-SHELL SHELL SHUTDOWN	What is Bitscout and how to use it. Connect to WiFi, setup static IP or proxy. Manage attached disks (i.e. let expert work on it). System status, and expert sessions monitoring. Supervise or enable elevated commands from the container. Enter IRC chat with the expert. Start a root shell inside guest container. Start a root local shell. Shutdown current system.			
L					

![](_page_10_Picture_3.jpeg)

## **Bitscout** Configuration & Customisation

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

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

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\$

xavier@ubuntu: /opt/bitscout/config

![](_page_11_Picture_8.jpeg)

![](_page_11_Picture_9.jpeg)

## **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	
File Edit View Search Terminal Help <avier@ubuntu: bitscout="" opt="" scripts<br="">casper_findlivefs_fix.sh casper_writeblocker.sh chroot_add_managementtool.sh chroot_configure_irc.sh chroot_configure_openvpn.sh chroot_configure_ssh.sh chroot_configure_ssh.sh chroot_create_container.sh chroot_create_user.sh chroot_devel_enter.sh chroot_devel_enter.sh chroot_enter_devel.sh chroot_install_base.sh chroot_install_forensics_extra.sh chroot_install_forensics.sh chroot_install_remoteaccess.sh chroot_install_remoteaccess.sh cavier@ubuntu:/opt/bitscout/scripts</avier@ubuntu:>	<pre>s\$ ls chroot_install_userchoice.sh chrootspostdownload_setup.sh chrootscreen_end.sh chrootscreen_start.sh deb_pack.sh deb_unpack.sh export_generate.sh functions image_build-nosquashfs-rebuild.sh image_puild.sh image_prebuild_cleanup.sh image_prepare.sh initrd_pack.sh nspawn_container_spawn.sh nspawn_enter.sh nspawn_session.exp skeleton.sh submodules_fetch.sh welcome.sh</pre>
hroot_install_remoteaccess.sh avier@ubuntu:/opt/bitscout/scripts avier@ubuntu:/opt/bitscout\$ ./auto	s\$ cd omake.sh

![](_page_12_Picture_5.jpeg)

## **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)

![](_page_13_Picture_5.jpeg)

## Bitscout **Network Setup**

NETWORK The following menu should help you change network configuration and connect to the Internet:			
	WIFI SETTINGS ENABLE HOST CONTROL ENABLE ACCESS FROM LAN STATIC IP HTTP PROXY SOCKS PROXY SYSLOG ACK	Setup WiFi network connection. Let the expert control LiveCD host directly Enable LAN access to LiveCD. Setup static IP for LAN interface. Configure internet access via HTTP proxy. Configure a new Syslog forwarder. Return to previous menu. Return to previous menu.	
		<mark>K <u>O</u>K &gt;</mark>	
	Container	RW Mapping	

![](_page_14_Figure_2.jpeg)

![](_page_14_Picture_4.jpeg)

# Demo #1

#### **Network Setup & Remote Access**

![](_page_15_Picture_2.jpeg)

### **Bitscout** Disk Management

![](_page_16_Picture_1.jpeg)

![](_page_16_Picture_2.jpeg)

![](_page_16_Picture_3.jpeg)

### **Bitscout** Disk Management

![](_page_17_Picture_1.jpeg)

![](_page_17_Picture_2.jpeg)

![](_page_17_Picture_3.jpeg)

#### /dev/host/evidence0

![](_page_17_Picture_5.jpeg)

# Demo #2

#### **Disk Mapping & Access**

![](_page_18_Picture_2.jpeg)

## Investigation **Classic Disk Tools**

- Mount your filesystems
- Use classic tools
  - Loki
  - BulkExtractor
  - Log2Timeline

![](_page_19_Picture_7.jpeg)

![](_page_19_Picture_8.jpeg)

xavier@ubuntu: ~

File Edit View Search Terminal Help

Copyright by Florian Roth, Released under the GNU General Public License DISCLAIMER - USE AT YOUR OWN RISK Please report false positives via https://github.com/Neo23x0/Loki/issues Starting Loki Scan VERSION: 0.30.4 SYSTEM: bitscout TIME: 20200606T14:56:25Z PLATFORM: PROC: x86 64 ARCH NOTICE] Loaded plugin /opt/loki/plugins/loki-plugin-wmi.py PE-Sieve successfully initialized BINARY: /opt/loki/tools/pe-sieve64.exe SOURCE: https://github.com/hasherez Malicious SHA1 Hashes initialized with 7100 hashes **INFO** Malicious SHA256 Hashes initialized with 22779 hashes **INFO** False Positive Hashes initialized with 30 hashes

INF0] Processing YARA rules folder /opt/loki/signature-base/yara

![](_page_19_Picture_13.jpeg)

![](_page_19_Picture_14.jpeg)

# Demo #3

#### **Classic Disk Analyzis Tools**

![](_page_20_Picture_2.jpeg)

## 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

![](_page_21_Picture_8.jpeg)

# Demo #4

#### Working with Live System

![](_page_22_Picture_2.jpeg)

## 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

![](_page_23_Picture_5.jpeg)

(Memory acquisition as seen by end-users)

![](_page_23_Picture_8.jpeg)

# **Demo #5**

#### **Memory Acquisition**

![](_page_24_Picture_2.jpeg)

## **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!

![](_page_25_Picture_6.jpeg)

![](_page_25_Picture_9.jpeg)

#### **Deployment of Tools Through SMB**

![](_page_26_Picture_2.jpeg)

![](_page_26_Picture_3.jpeg)

## **Other Features Chat between Owner & Expert**

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

-!– **owner** [~owner@bitscout.vpn.rootshell.be] has joined #csirt -!- Topic for **#csirt:** Remote operation channel :10 –!– Topic set by **-Server**– [] [Tue May 19 11:55:53 2020] sers **#csirt**] owner -!- Irssi: #csirt: Total of 1 nicks [0 ops, 0 halfops, 0 voices, 1 normal] -!– Channel #csirt created Tue May 19 11:55:53 2020 Irssi: Join to #csirt was synced in 7 secs owner> Hi! : owner> May I reboot the server? 3:10 -

![](_page_27_Picture_6.jpeg)

## **Other Features** Sensitive Command Approval

xavier@ubuntu: ~

File Edit View Search Terminal Help 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

<ALLOW >

<REJECT>

![](_page_28_Picture_8.jpeg)

## **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

![](_page_29_Picture_7.jpeg)

## 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? <u>https://github.com/vitaly-kamluk/bitscout</u>

## **Thank You!** Q&A

![](_page_31_Picture_1.jpeg)

![](_page_31_Picture_2.jpeg)