

# Digital Evidence Collection (core)

Otis Smith / Cybersecurity Professional / 8.29.23

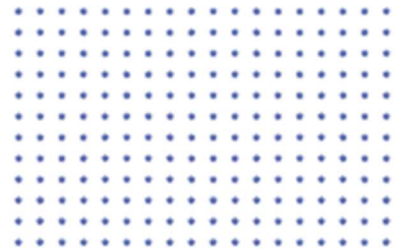




# TABLE OF CONTENTS

Summary .....	
Discovery.....	
Vulnerability.....	
Exploitation.....	
References.....	
Mitigation.....	

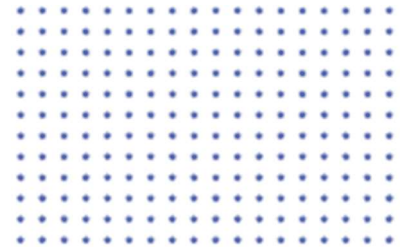
# SUMMARY



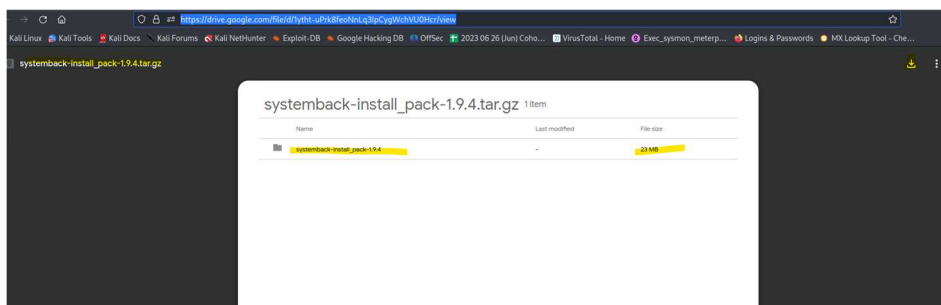
This report outlines the process of Digital Evidence Collection, focusing on creating an image of an OS using SystemBack and verifying data integrity with Autopsy. The objective is to ensure the validity of evidence in a digital forensics investigation. The report covers the steps from downloading SystemBack to comparing MD5 hashes in Autopsy, demonstrating a thorough and successful evidence collection process.



# DISCOVERY



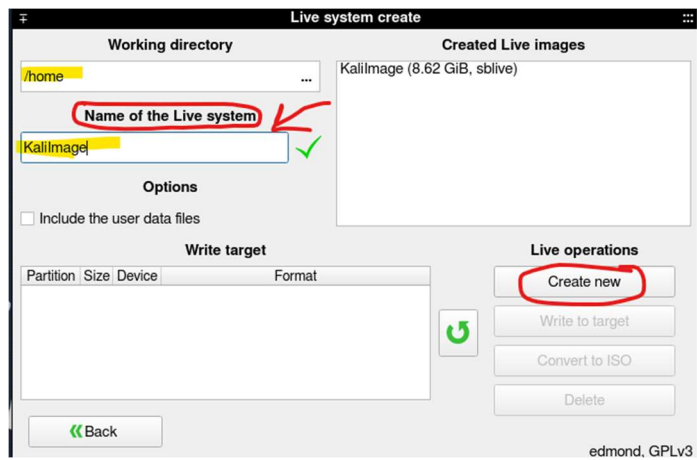
The discovery phase involved downloading the SystemBack file from a provided link, navigating through the terminal to unzip and install SystemBack, and configuring its settings for live system creation. Key steps included selecting the appropriate operating system (Ubuntu 20.04), creating a new live system named "Kalilimage," and patiently waiting for the image creation to complete.



```
(kali@kali)-[~]
└─$ cd Downloads
(kali@kali)-[~/Downloads]
└─$ ls
2020-04-24-traffic-analysis-exercise.pcap.zip
4624_LT3_AnonymousLogon_Localhost_-_JuicyPotato.evtx-20230829T232702Z-001.zip
credentials-a9839a-2023-Sep-05--16_31_53.csv
Default_Gateway_Scan_zxxovn.pdf
DE_RDP_Tunnel_5156.evtx
DE_RDP_Tunnel_5156.evtx-20230829T232715Z-001.zip
Exec_sysmon_meterpreter_reversetcp_msipackage.evtx
Exec_sysmon_meterpreter_reversetcp_msipackage.evtx-20230830T195948Z-001.zip
header.docx
header.txt
House
Nessus-10.5.2-debian10_amd64.deb
New_W2D1_AwkPractice_file.txt
New_W2D1_AwkPractice.txt
Raw_Wireshark_Chrome
Raw_Wireshark_findings
Security_Appliance_Analyzing_log
systemback-install_pack-1.9.4
systemback-install_pack-1.9.4.tar.gz
valid_directories.txt
W2D1_AwkPractice.txt
```

Press 'A' to abort the installation, or select one of the following releases:

- 1 - Debian 10.0 (Buster)
- 2 - Ubuntu 20.04 (Focal Fossa)
- 3 - Ubuntu 18.04 (Bionic Beaver)

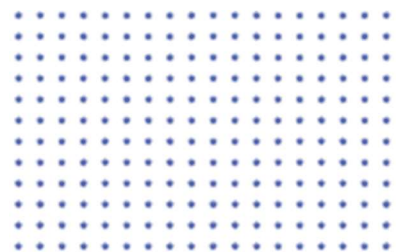


The KaliImage file completed successfully

```
(kali㉿kali)-[~]
$ cd /home

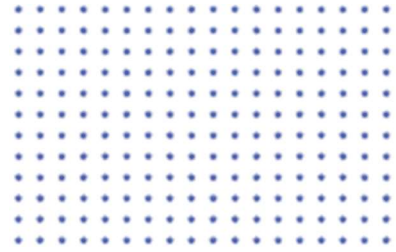
(kali㉿kali)-[/home]
$ ls
Josh  kali  KaliImage.sblive  Systemback
```

# VULNERABILITY



One potential vulnerability mentioned is the limitation on filesystem size. If the filesystem becomes too large, it may hinder the creation of a correct image. Users are advised to manage file sizes or consider a fresh installation of the Kali instance.

# EXPLOITATION



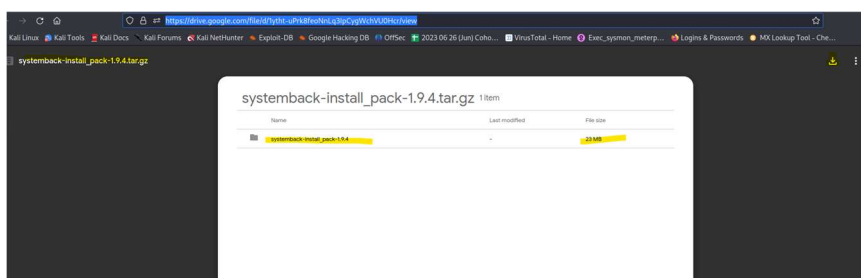
No exploitation activities were conducted in this process. The focus was on creating a valid image of the operating system for forensic analysis.



# REFERENCES

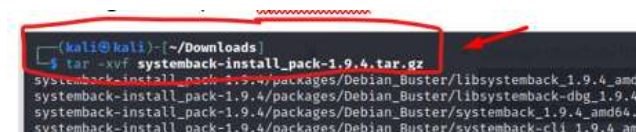
## 1. Downloading SystemBack:

- Link: <https://drive.google.com/file/d/1ytht-uPrk8feoNnLq3IpCygWchVU0Hcr/view>

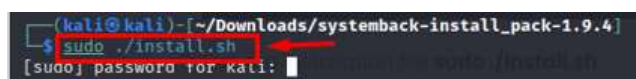


## 2. Commands:

- Unzipping SystemBack: `tar -xvf systemback-install_pack-1.9.4.tar.gz`



- Installation: `sudo ./install.sh`



- Checking hash: `md5sum filename`



## 3. Autopsy:

- Autopsy command: `sudo autopsy`



```
(kali@kali)~[/home]
$ sudo autopsy
[sudo] password for kali:

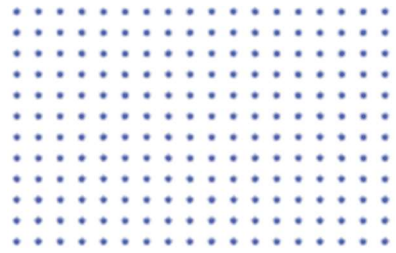
Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24

Evidence Locker: /var/lib/autopsy
Start Time: Tue Sep 12 10:24:53 2023
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:
http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
*End Time: Tue Sep 12 10:25:22 2023

(kali@kali)~[/home]
$
```



## MITIGATION:

To mitigate the risk of filesystem size limitations:

- Regularly manage files/backups to keep the filesystem size within limits.
- Consider a fresh installation of the Kali instance if filesystem size becomes a persistent issue.

In conclusion, the comprehensive execution of the outlined steps, including downloading, installing, and configuring SystemBack, followed by the successful comparison of MD5 hashes in Autopsy, ensures the integrity of the digital evidence. The report demonstrates a meticulous approach to digital evidence collection in a forensics investigation, enhancing the reliability of the obtained data.

This process provides a valuable resource for professionals engaged in digital forensics, emphasizing the importance of systematic procedures in maintaining the integrity of evidence throughout the investigation lifecycle.