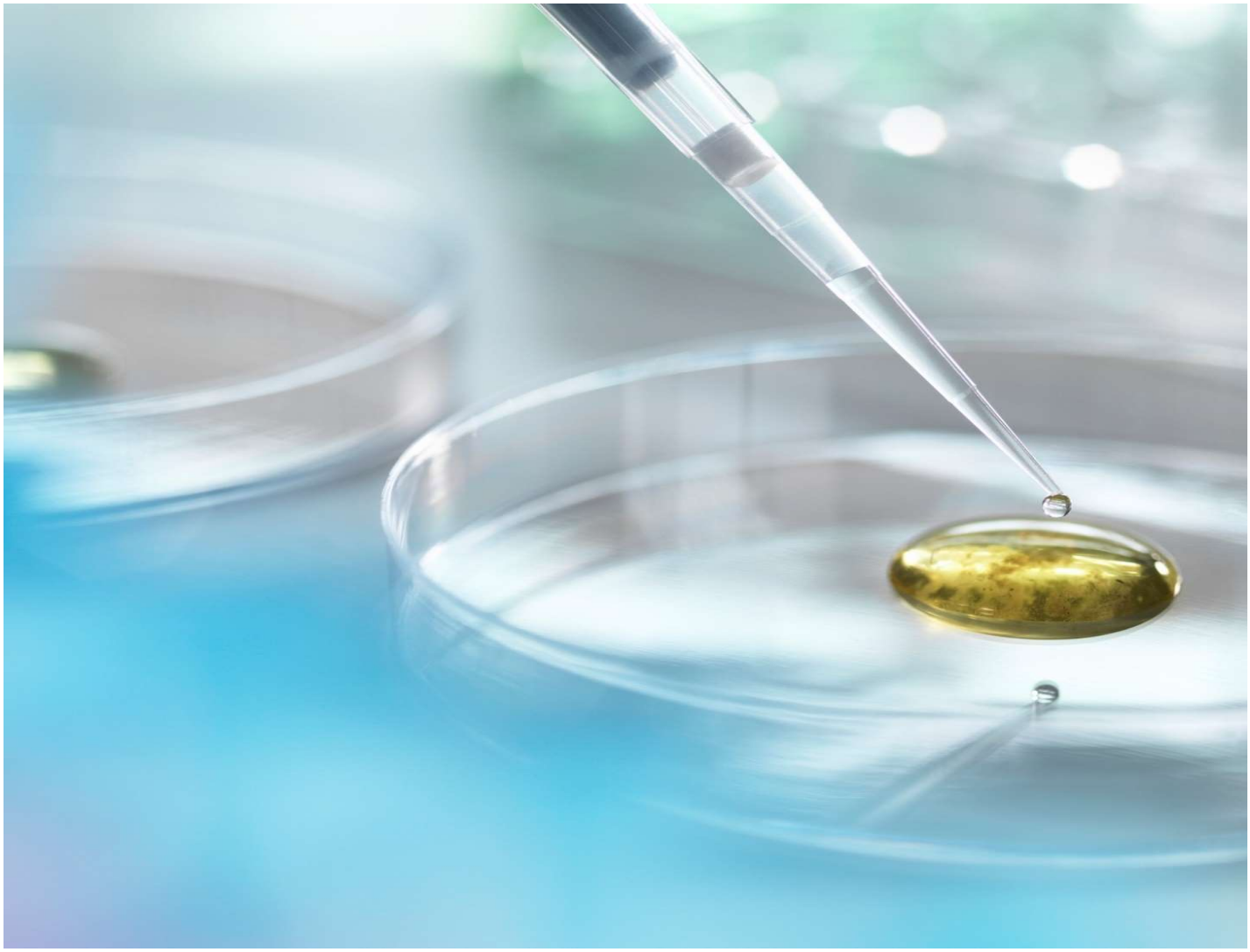
Digital Evidence Collection (Core)

Otis Smith / Cybersecurity Professional / 8.29.23



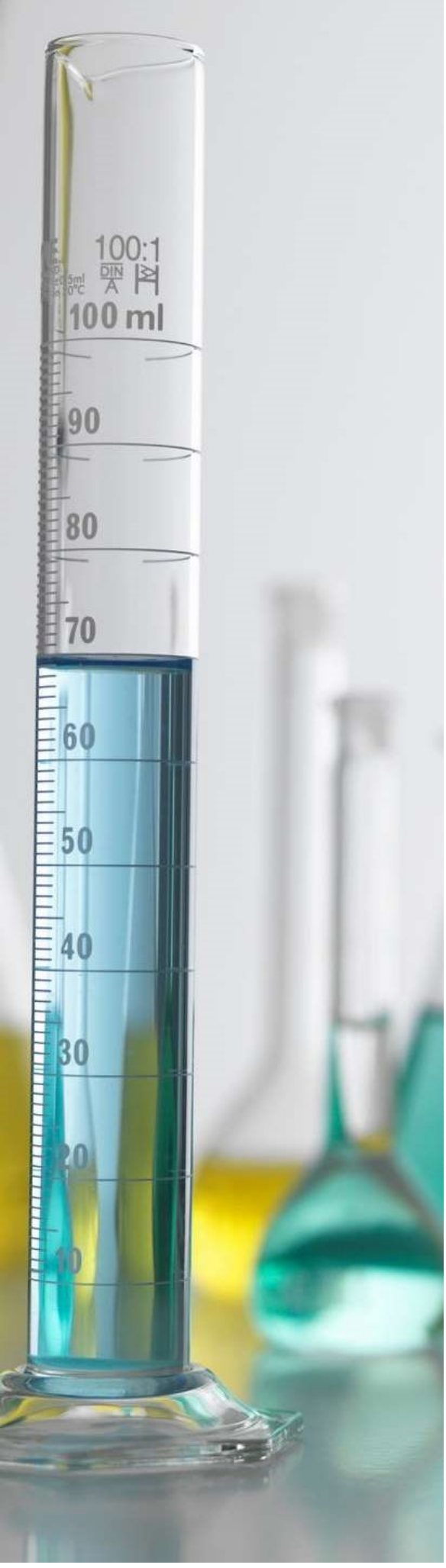


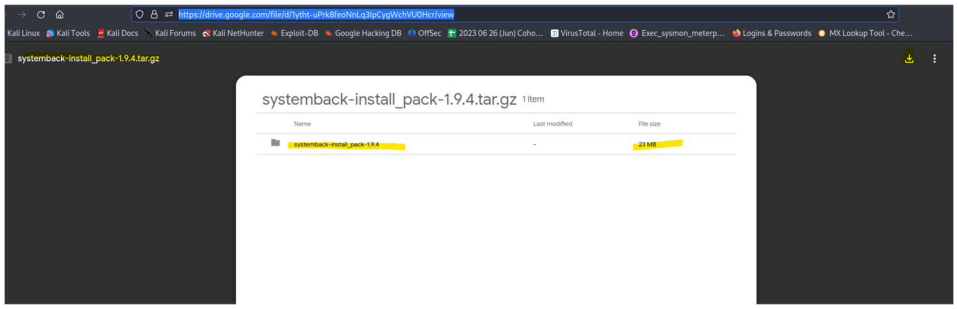
TABLE OF CONTENTS

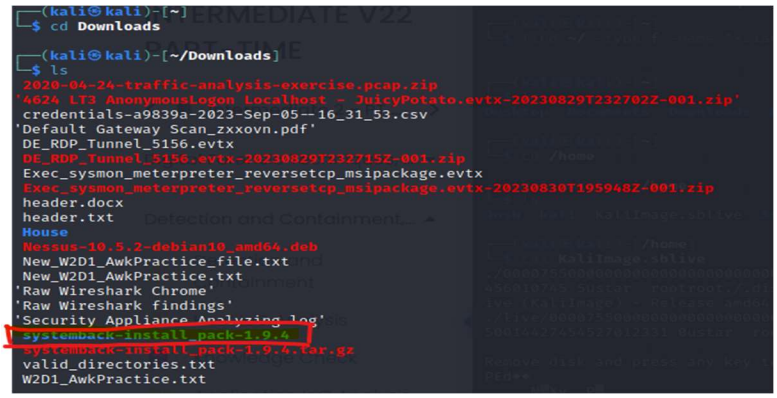
SUMMARY

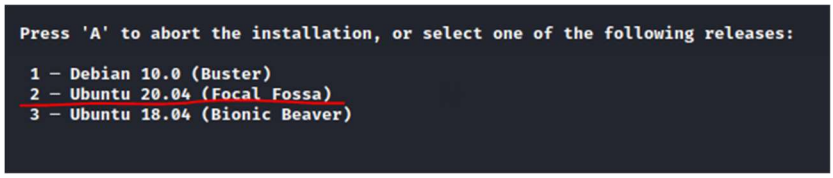
This report outlines the process of Digital Evidence Collection, focusing on creating an image of an OS using SystemBack and verifying data integrity with Autopsy. The objective is to ensure the validity of evidence in a digital forensics investigation. The report covers the steps from downloading SystemBack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

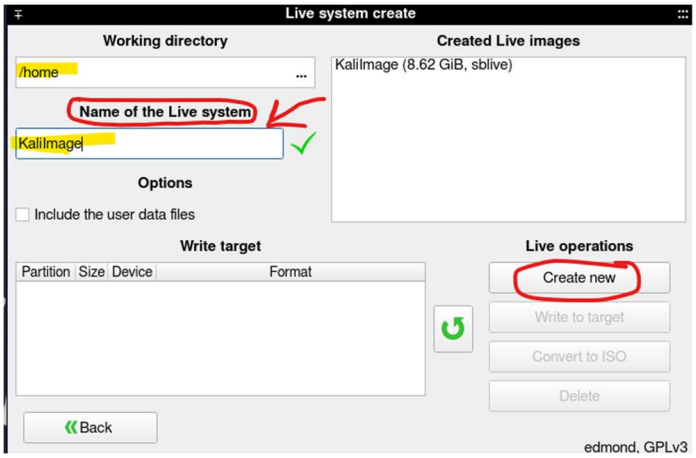
DISCOVERY

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 "KaliImage," and patiently waiting for the image creation to complete.

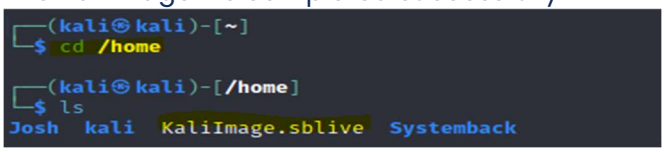








The KaliImage file completed successfully



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.

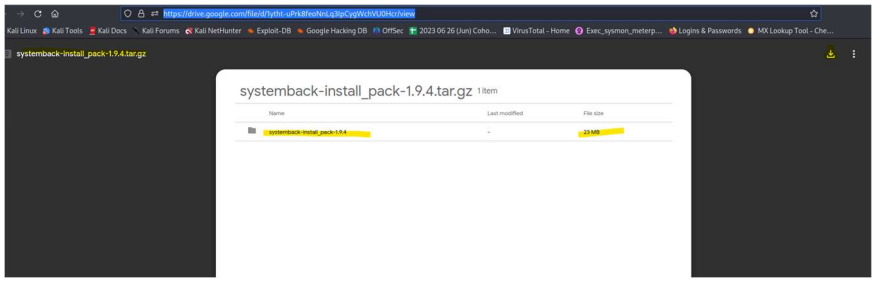
EXPLOITATION

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

REFERENCES

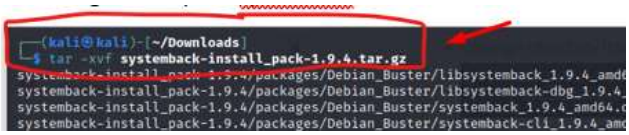
1. Downloading SystemBack:

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

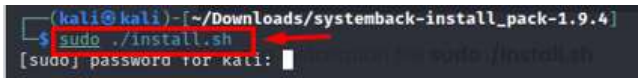


2. Commands:

    - 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
^CEnd 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.