Experiment No .9

9.1 Aim: Live Acquisition: BitLocker, Live Acquisition

Example Scenario:
You are working as a digital forensic analyst and receive a laptop that is currently powered on and suspected to contain important evidence. The drive is protected with **BitLocker encryption**, which means if the system is turned off, the encryption keys will be lost and the data will become unreadable.
To preserve the evidence, you decide to perform **live acquisition** — capturing data from the system while it is still running. You also extract the **BitLocker recovery key** and acquire the encrypted volume for later decryption and analysis.

Tasks:

1. Identify that the target system is **powered on** and **BitLocker is enabled**.
2. Collect **volatile data** such as RAM, network connections, and running processes using tools like **FTK Imager, Belkasoft RAM Capturer, or DumpIt**.
3. Export or record the **BitLocker recovery key** (found in the system settings, command prompt, or via recovery key file).
4. Perform **live acquisition** of the encrypted drive using a forensic imaging tool (e.g., FTK Imager or Magnet Acquire).
5. Save the acquired image file securely to an external storage device.
6. Calculate **hash values (MD5/SHA1)** of the image to verify its integrity.
7. Document each step with screenshots or short notes in your observation record.

9.2 Lab Outcome :

- To learn how to safely collect live data from a running system and acquire a BitLocker-encrypted drive without losing critical information or encryption keys.

9.3 Learning Objectives:

- To understand the concept and importance of **live acquisition** in digital forensics.
- To learn how **BitLocker encryption** affects evidence collection.
- To capture **volatile data** like RAM and running processes.
- To acquire a **BitLocker-protected drive** safely while maintaining data integrity.
- To verify the collected data using **hash values**.

9.4 Requirement:

Hardware:

- Forensic workstation (laptop or desktop)
- Target system (BitLocker-encrypted)
- External storage device for saving image files

Software Tools:

- FTK Imager / Magnet Acquire / Belkasoft RAM Capturer / DumpIt
- Hash calculator (MD5/SHA1)
- Windows 10/11 with BitLocker enabled

9.5 Related Theory :

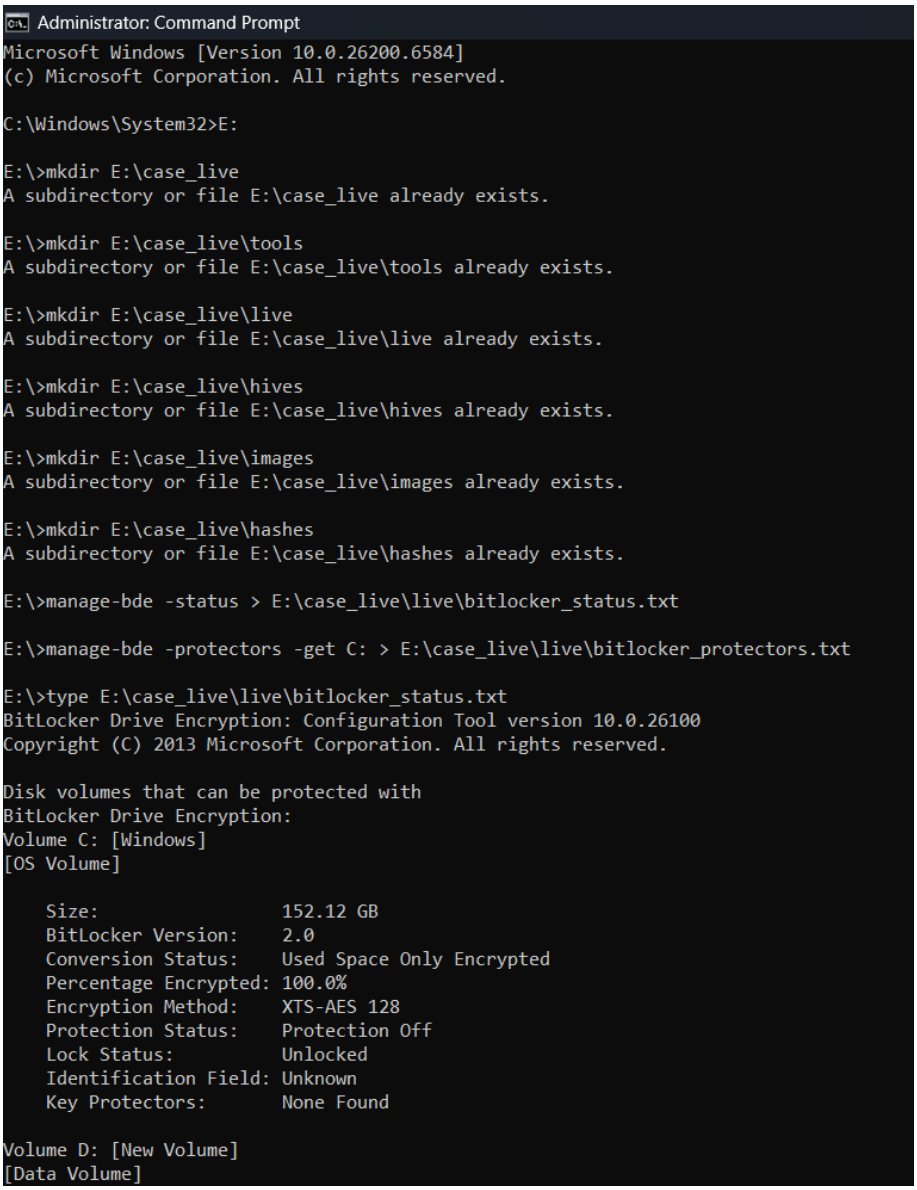
Live Acquisition:
Live acquisition is performed while the computer is still powered on. It allows investigators to capture **volatile data** such as RAM contents, encryption keys, network sessions, and temporary files that will be lost if the system is shut down.

BitLocker Encryption:
BitLocker is a full-disk encryption feature in Windows that protects data using encryption keys. If a system is turned off, these keys are removed from memory, making the data inaccessible. During live acquisition, the encryption keys are still available in memory, allowing investigators to capture and later decrypt the data.

Volatile Data:
Volatile data includes all information stored temporarily in memory (RAM), such as active processes, chat logs, passwords, and network connections. This data disappears once the system is powered off.

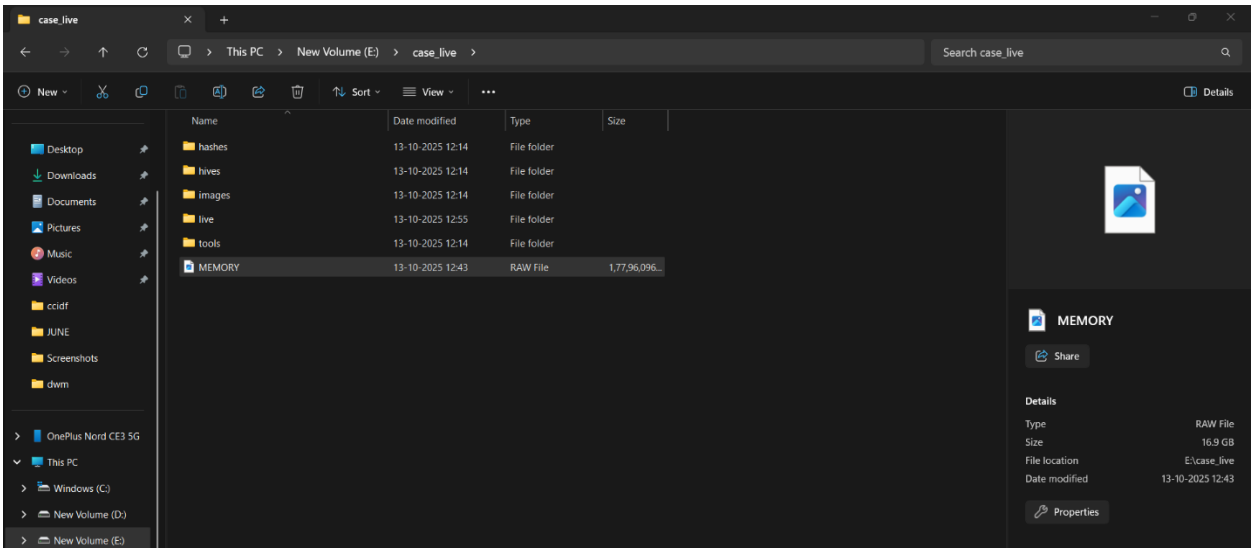
Hash Verification:
Hashing (using algorithms like MD5 or SHA1) ensures that the acquired data matches the original. Identical hash values confirm that no modification occurred during acquisition.

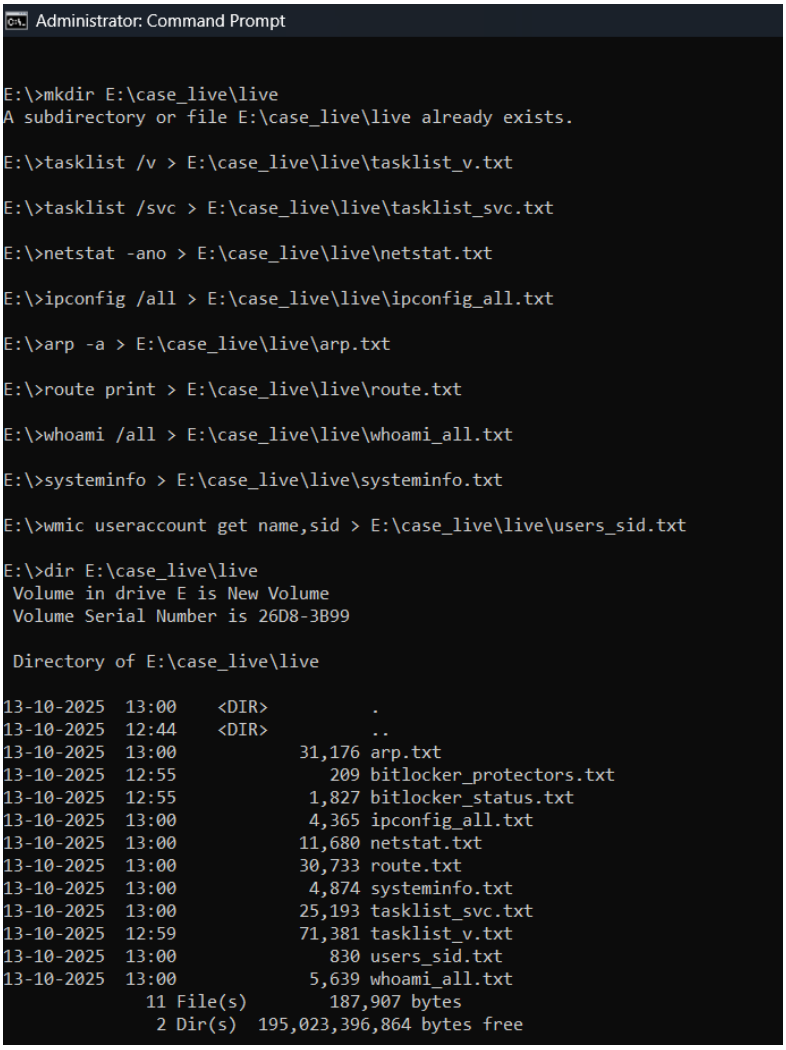
9.6 Output:

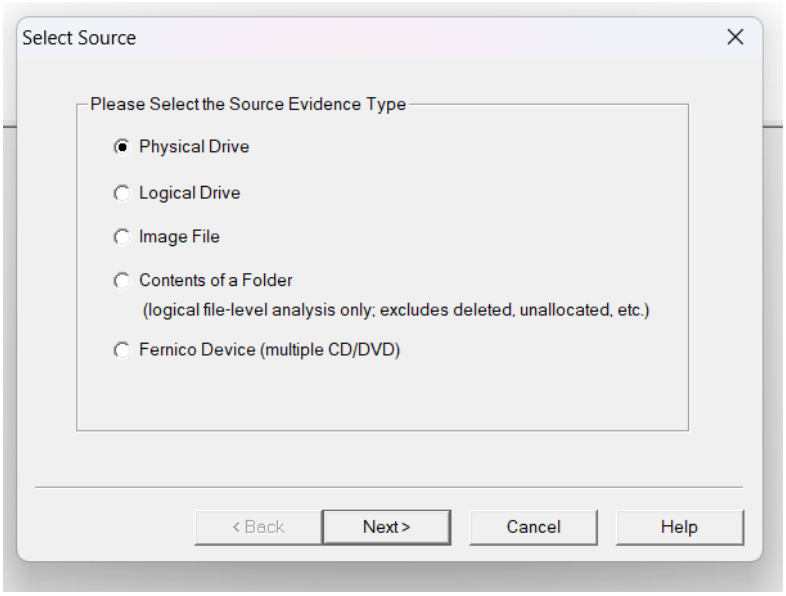


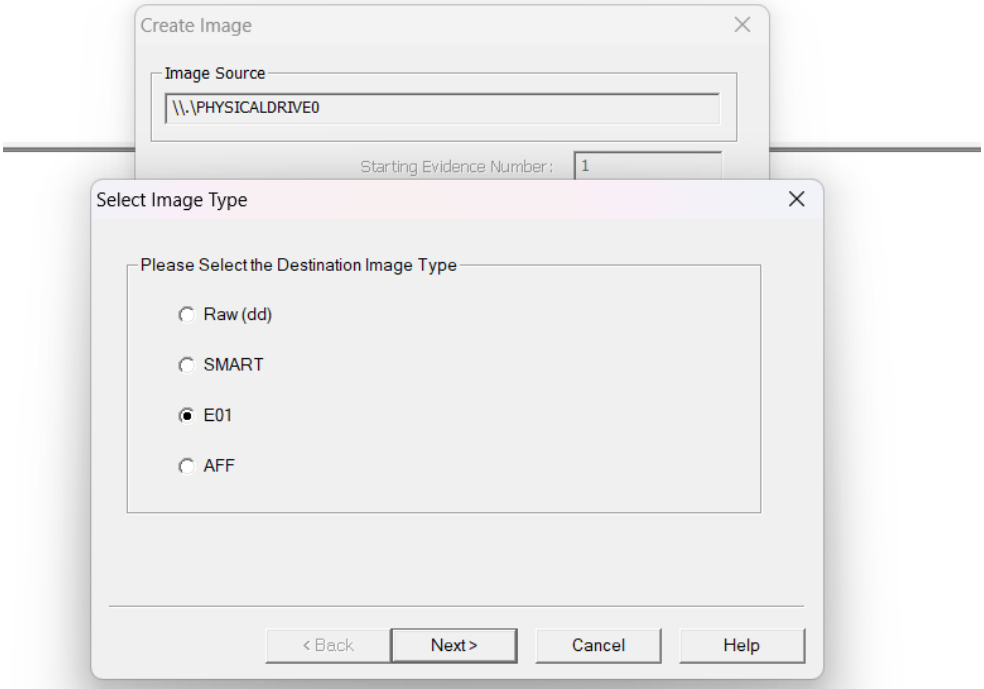
Administrator: Command Prompt

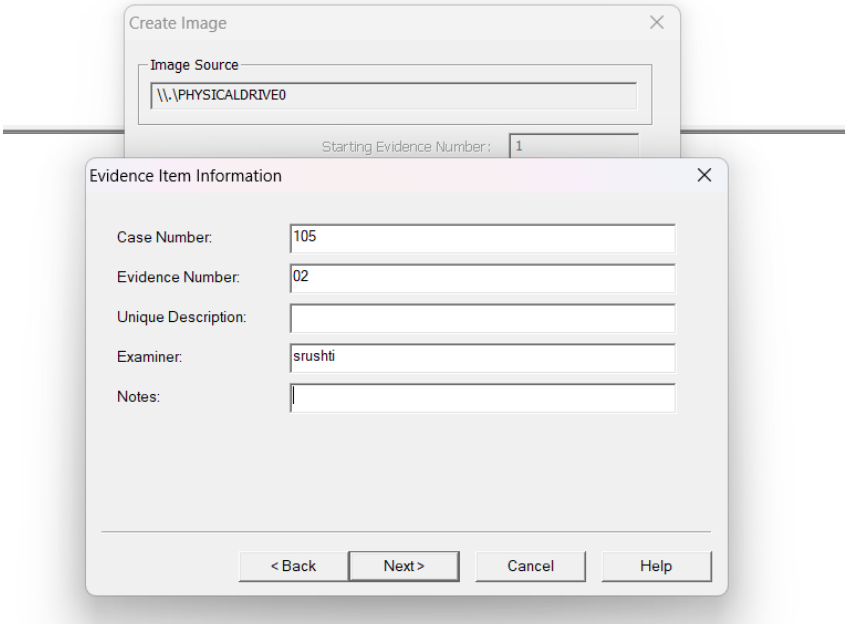
```
Volume D: [New Volume]
[Data Volume]

    Size:                 400.00 GB
    BitLocker Version:    2.0
    Conversion Status:    Used Space Only Encrypted
    Percentage Encrypted: 100.0%
    Encryption Method:    XTS-AES 128
    Protection Status:    Protection Off
    Lock Status:          Unlocked
    Identification Field: Unknown
    Automatic Unlock:     Disabled
    Key Protectors:       None Found

Volume E: [New Volume]
[Data Volume]

    Size:                 400.00 GB
    BitLocker Version:    2.0
    Conversion Status:    Used Space Only Encrypted
    Percentage Encrypted: 100.0%
    Encryption Method:    XTS-AES 128
    Protection Status:    Protection Off
    Lock Status:          Unlocked
    Identification Field: Unknown
    Automatic Unlock:     Disabled
    Key Protectors:       None Found

Volume F: []
[Data Volume]

    Size:                 232.91 GB
    BitLocker Version:    None
    Conversion Status:    Fully Decrypted
    Percentage Encrypted: 0.0%
    Encryption Method:    None
    Protection Status:    Protection Off
    Lock Status:          Unlocked
    Identification Field: None
    Automatic Unlock:     Disabled
    Key Protectors:       None Found


E:\>
```

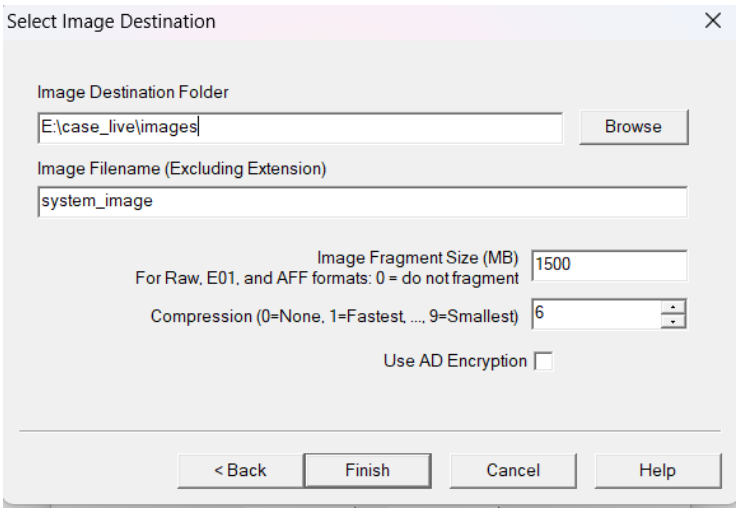


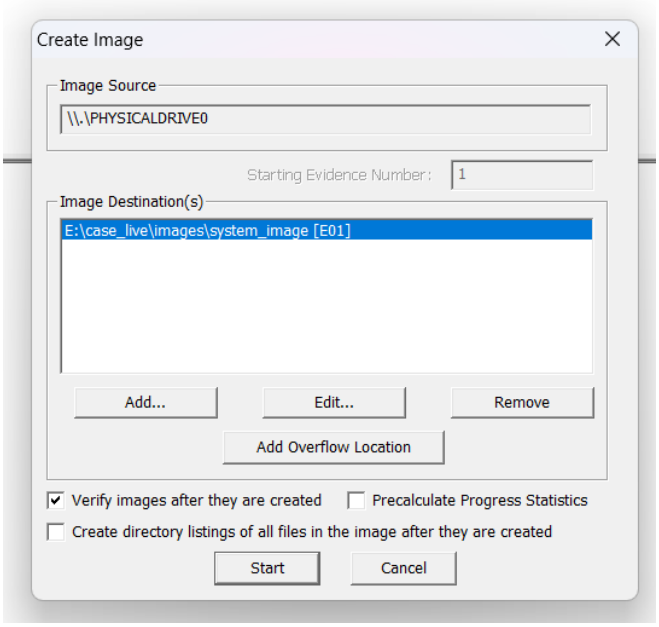

Administrator: Command Prompt
E:\>mkdir E:\case_live\live
A subdirectory or file E:\case_live\live already exists.
E:\>tasklist /v > E:\case_live\live\tasklist_v.txt
E:\>tasklist /svc > E:\case_live\live\tasklist_svc.txt
E:\>netstat -ano > E:\case_live\live\netstat.txt
E:\>ipconfig /all > E:\case_live\live\ipconfig_all.txt
E:\>arp -a > E:\case_live\live\arp.txt
E:\>route print > E:\case_live\live\route.txt
E:\>whoami /all > E:\case_live\live\whoami_all.txt
E:\>systeminfo > E:\case_live\live\systeminfo.txt
E:\>wmic useraccount get name,sid > E:\case_live\live\users_sid.txt
E:\>dir E:\case_live\live
Volume in drive E is New Volume
Volume Serial Number is 26D8-3B99
Directory of E:\case_live\live
13-10-2025 13:00 <DIR> .
13-10-2025 12:44 <DIR> ..
13-10-2025 13:00 31,176 arp.txt
13-10-2025 12:55 209 bitlocker_protectors.txt
13-10-2025 12:55 1,827 bitlocker_status.txt
13-10-2025 13:00 4,365 ipconfig_all.txt
13-10-2025 13:00 11,680 netstat.txt
13-10-2025 13:00 30,733 route.txt
13-10-2025 13:00 4,874 systeminfo.txt
13-10-2025 13:00 25,193 tasklist_svc.txt
13-10-2025 12:59 71,381 tasklist_v.txt
13-10-2025 13:00 830 users_sid.txt
13-10-2025 13:00 5,639 whoami_all.txt
11 File(s) 187,907 bytes
2 Dir(s) 195,023,396,864 bytes free

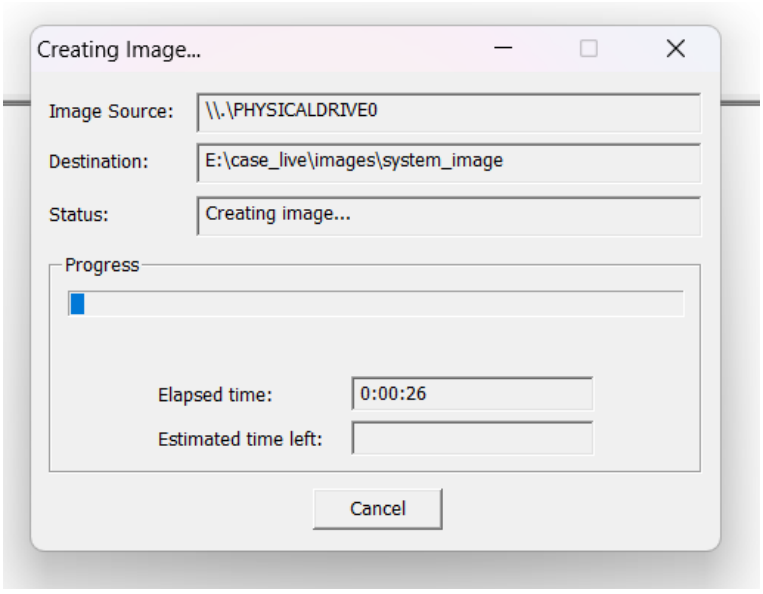

Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
Fernico Device (multiple CD/DVD)
< Back
Next >
Cancel
Help

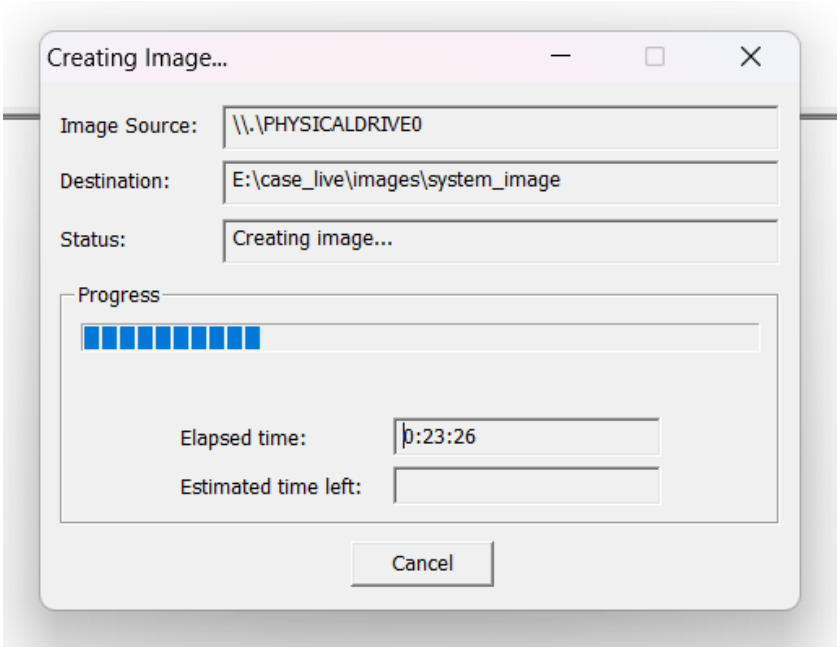

Create Image
Image Source
\\.\PHYSICALDRIVE0
Starting Evidence Number:
1
Select Image Type
Please Select the Destination Image Type
Raw (dd)
SMART
E01
AFF
< Back
Next >
Cancel
Help


Create Image
Image Source
\\.\PHYSICALDRIVE0
Starting Evidence Number:
1
Evidence Item Information
Case Number:
105
Evidence Number:
02
Unique Description:
Examiner:
srushti
Notes:
< Back
Next >
Cancel
Help

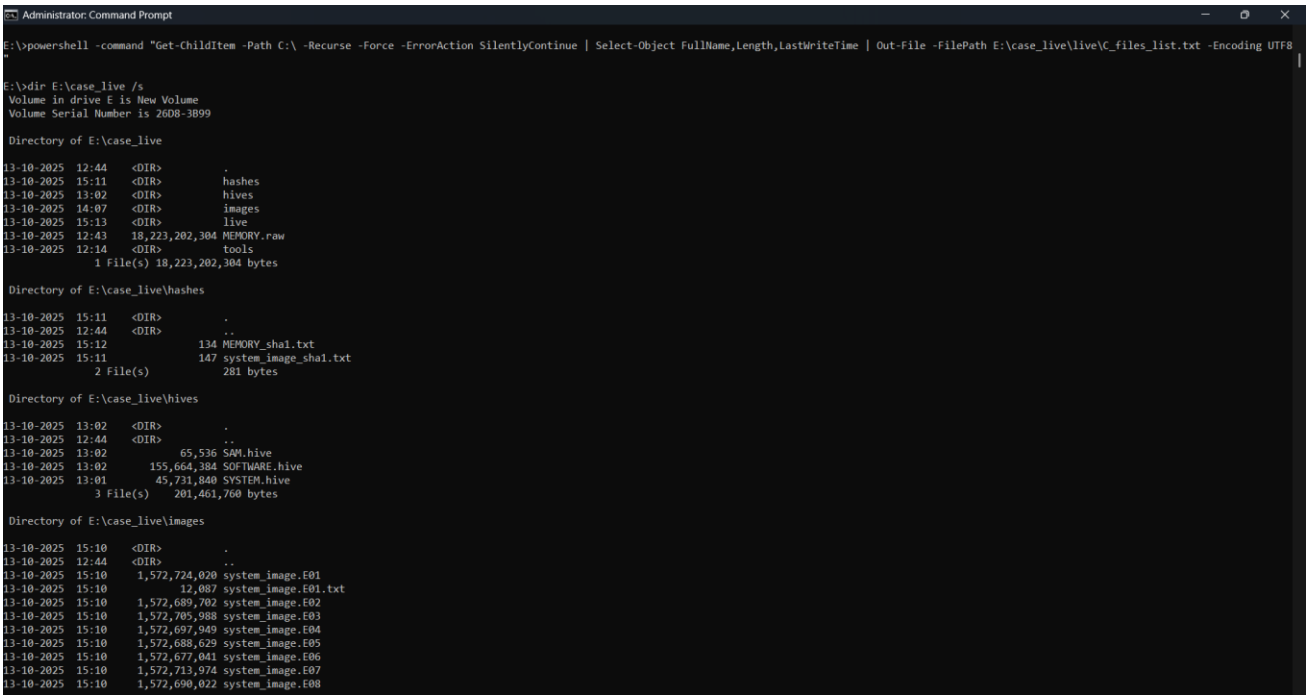

Select Image Destination
Image Destination Folder
E:\case_live\images
Browse
Image Filename (Excluding Extension)
system_image
Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment
1500
Compression (0=None, 1=Fastest, ..., 9=Smallest)
6
Use AD Encryption
< Back
Finish
Cancel
Help

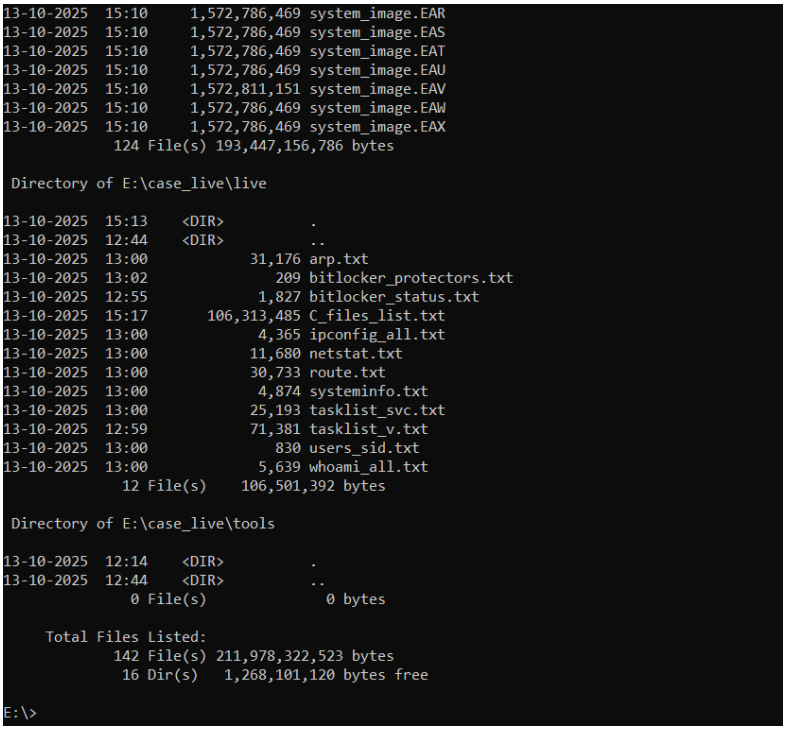

Create Image
Image Source
\\.\PHYSICALDRIVE0
Starting Evidence Number:
1
Image Destination(s)
E:\case_live\images\system_image [E01]
Add...
Edit...
Remove
Add Overflow Location
Verify images after they are created
Precalculate Progress Statistics
Create directory listings of all files in the image after they are created
Start
Cancel


Creating Image...
Image Source:
\\.\PHYSICALDRIVE0
Destination:
E:\case_live\images\system_image
Status:
Creating image...
Progress
Elapsed time:
0:00:26
Estimated time left:
Cancel




```
Administrator: Command Prompt

E:\>mkdir E:\case_live\hives
A subdirectory or file E:\case_live\hives already exists.

E:\>reg save HKLM\SYSTEM E:\case_live\hives\SYSTEM.hive
The operation completed successfully.

E:\>reg save HKLM\SOFTWARE E:\case_live\hives\SOFTWARE.hive
The operation completed successfully.

E:\>reg save HKLM\SAM E:\case_live\hives\SAM.hive
The operation completed successfully.

E:\>dir E:\case_live\hives
 Volume in drive E is New Volume
 Volume Serial Number is 26D8-3B99

 Directory of E:\case_live\hives

13-10-2025  13:02    <DIR>          .
13-10-2025  12:44    <DIR>          ..
13-10-2025  13:02            65,536 SAM.hive
13-10-2025  13:02       155,664,384 SOFTWARE.hive
13-10-2025  13:01        45,731,840 SYSTEM.hive
               3 File(s)    201,461,760 bytes
               2 Dir(s)  194,821,935,104 bytes free

E:\>manage-bde -protectors -get C: > E:\case_live\live\bitlocker_protectors.txt

E:\>certutil -hashfile E:\case_live\images\system_image.E01 SHA1
SHA1 hash of E:\case_live\images\system_image.E01:
741d9c4f14f38857d8cbedd9c7f79a8109f4b78d
CertUtil: -hashfile command completed successfully.

E:\>certutil -hashfile E:\case_live\images\system_image.E01 SHA1 > E:\case_live\hashes\system_image_sha1.txt

E:\>certutil -hashfile E:\case_live\MEMORY.raw SHA1 > E:\case_live\hashes\MEMORY_sha1.txt

E:\>type E:\case_live\hashes\system_image_sha1.txt
SHA1 hash of E:\case_live\images\system_image.E01:
456697a40b1a5143834875ec70143ab554a21150
CertUtil: -hashfile command completed successfully.

E:\>type E:\case_live\hashes\MEMORY_sha1.txt
SHA1 hash of E:\case_live\MEMORY.raw:
f2aa505b79d5d3b6b4ef40431c8e96ddc7fef40d
CertUtil: -hashfile command completed successfully.
```





9.7 Conclusion:

In this experiment, a live data acquisition was performed on a BitLocker-enabled Windows system. Volatile information such as running processes, network connections, and registry hives was collected while the system was active. A memory image was successfully captured using Belkasoft RAM Capturer, and a live disk image of the running system was created using FTK Imager. The acquired image files were hashed and verified to ensure data integrity. This experiment demonstrated the complete procedure for performing live forensic acquisition and preserving evidence from an encrypted system without shutting it down.