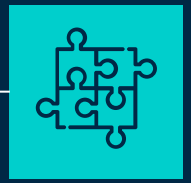
Tool Demonstration – FTK Imager

Digital Forensics and Investigation

Lab Continuous Assessment Activity

PA10. Krishnaraj
TY. CSF Panel A

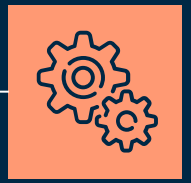
TABLE OF CONTENTS



01

TOOL INFORMATION

Information about the FTK Imager



02

DEMO

Live Demo of the Tool

03

FURTHER INVESTIGATION

How the investigation will continue.

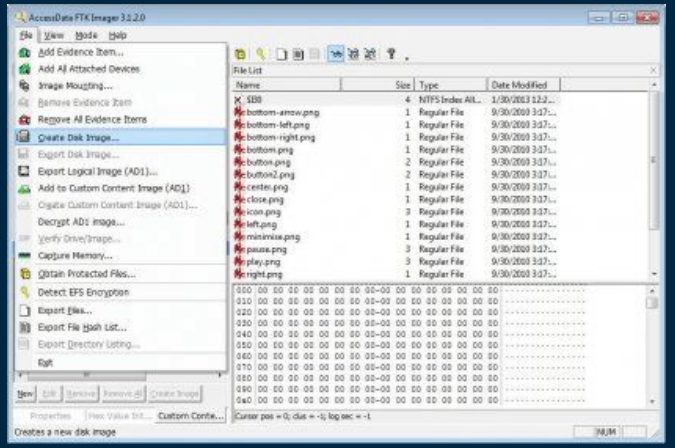
What is FTKImager

Its uses and when it was created.

01

What is it?

FTK Imager is a digital forensic tool.
Developed by AccessData, it's widely used in the field of digital forensics.



Primary Functions

- Disk Imaging: FTK Imager is primarily used for creating forensic disk images.
- Evidence Preservation: It ensures the preservation of digital evidence by creating exact copies of storage media.
- Forensic Analysis: FTK Imager allows investigators to examine disk images for evidence, including files, deleted data, and metadata.

Additional Features

- Memory Analysis: Can analyze RAM of a live system, useful in detecting running processes and potential malware.
- Hashing and Verification: Supports hashing algorithms to verify the integrity of acquired images.
- Export and Reporting: Enables data export and report generation for legal cases and research.

Applications

Its uses and when it was created.

02

Criminal and Corporate Investigations

- Criminal Investigations: FTK Imager aids law enforcement in collecting digital evidence from computers, mobile devices, and storage media for cases involving cybercrimes, fraud, and child exploitation.
- Corporate Investigations: It helps companies investigate employee misconduct, intellectual property theft, and data breaches, uncovering the source of security breaches and inappropriate activities.

Counterterrorism and Cybersecurity

Counterterrorism: FTK Imager is employed in counterterrorism operations to examine digital devices, uncovering communication networks, plans, and digital evidence related to terrorism.

Cybersecurity Incidents: It analyzes systems in cybersecurity incidents like data breaches and ransomware attacks to identify breach extent and access methods.

Child Exploitation and Cold Cases: FTK Imager plays a pivotal role in child exploitation cases and reopening cold cases by recovering, analyzing, and cataloging digital evidence.

License

Its uses and when it was created.

03

Free for Use

FTK Imager is a free tool provided by AccessData for disk imaging and forensic analysis. It can be freely downloaded and used without cost.

AccessData offers a range of forensic software products, including FTK (Forensic Toolkit) which is a comprehensive solution for digital investigations. However, these products are not free and typically require a license that is priced according to the features and scale needed.

Real Life Uses

Its uses and when it was created.

04

exterro®
Legal GRC Software Platform

PRODUCTS MARKETS RESOURCES TRAINING PARTNERS ABOUT LEGAL GRC STORE Get Demo

Case Study: Aurora Police Department Relies on FTK® to Collect Key Digital Evidence in Tragic Colorado Movie Theater Mass Shooting

Download the case study!

In the aftermath of the shooting in the Colorado Century Aurora 16 theater complex on July, 2012, Detective Mike Leiker, lead forensic investigator with the Aurora police department, quickly went to work investigating the devices collected from the suspect. Read his account of the investigation, and how FTK was crucial to help him uncover the evidence needed to bring the killer to justice.

Case Study: Aurora Police Department Relies on FTK® to Collect Key Digital Evidence in Tragic Colorado Movie Theater Mass Shooting

DOWNLOAD

Test Results for Digital Data Acquisition Tool

Tool Tested:	FTK Imager
Version:	2.5.3.14
Run Environments:	Windows XP, Windows Server 2003 & Windows 2000
Supplier:	AccessData
Address:	384 South 400 West Suite 200 Lindon, UT 84042 USA
Tel:	801–377–5410
Fax:	801–765–4370
WWW:	http://www.accessdata.com/

1 Results Summary

Except for two test cases (DA–07 and DA–08), the tested tool acquired all visible and hidden sectors completely and accurately from the test media without any anomalies. In one test case (DA-25) image file corruption was detected, but the location of the corrupt data was not reported. The following four anomalies were observed in test cases DA–07, DA–08, and DA–25:

1. If a logical acquisition is made of an NTFS partition, the last eight sectors of the physical partition are not acquired (DA–07–NTFS).
2. The sectors hidden by a *host protected area* (HPA) are not acquired (DA–08–ATA28 and DA–08–ATA48).
3. The sectors hidden by a *device configuration overlay* (DCO) are not acquired

Live Demo

Its uses and when it was created.

05

google.com/search?q="mayur+behere"+site:linkedin.com+OR+site:instagram.com+OR+site:indeed.com&sca_esv=580252979&tbm=isch&sxsrf=AM9HkKnhxYxGA_0H0NRHm5ySXw35Ec6neg:16...

Update

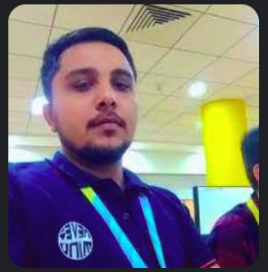
Design | Software... | Linux | Online C... | Downloa... | Typing | Data Scie... | University | Temp | Social | Audio Bo... | My Work | ERP | Mic... | Other bookmark

Google

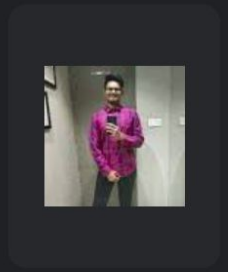
"mayur behere" site:linkedin.com OR site:instagram.com OR site:indeed.co

All | Images | News | Videos | Maps | More | Tools | Saved | SafeSearch

linkedin | certificate | structural consultant | trainee engineer



LinkedIn
Mayur Behere - Softwar...



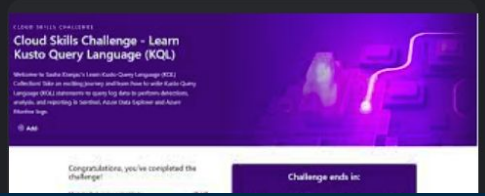
LinkedIn
Mayur Behere - Trai...

LinkedIn
3 "Mayur Behere" profil...

LinkedIn
Mayur Behere - Software Engineer ...

LinkedIn
Mayur Behere - Soft...

LinkedIn
Mayur Behere - Software Engineer ...



- ★ Starred
- Home
- Documents
- Downloads
- Music
- Pictures
- Trash

- krish trans ⏏

- TAA
- DSML
- JavaScript
- Anti-Brutus
- Third Year
- University
- Screenshots
- Imp Docs
- Python
- Decades
- Shows
- Interview Questio...
- Creativity and De...

+ Other Locations

EHEv1 Module 00 Student Introduction.pdf
2.8 MB
Document
Document

EHEv1 Module 01 Information Security Fundamentals.pdf
4.8 MB
Document
Document

calci.exe
73.8 kB
Program
Program

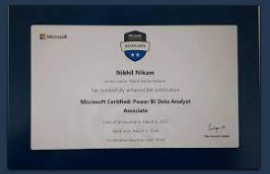
download.jpeg
8.2 kB
Image
Image

download ①.jpeg
7.7 kB
Image
Image

download ②.jpeg
1.7 kB
Image
Image

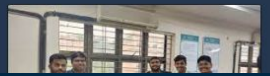
download ③.jpeg
8.2 kB
Image
Image

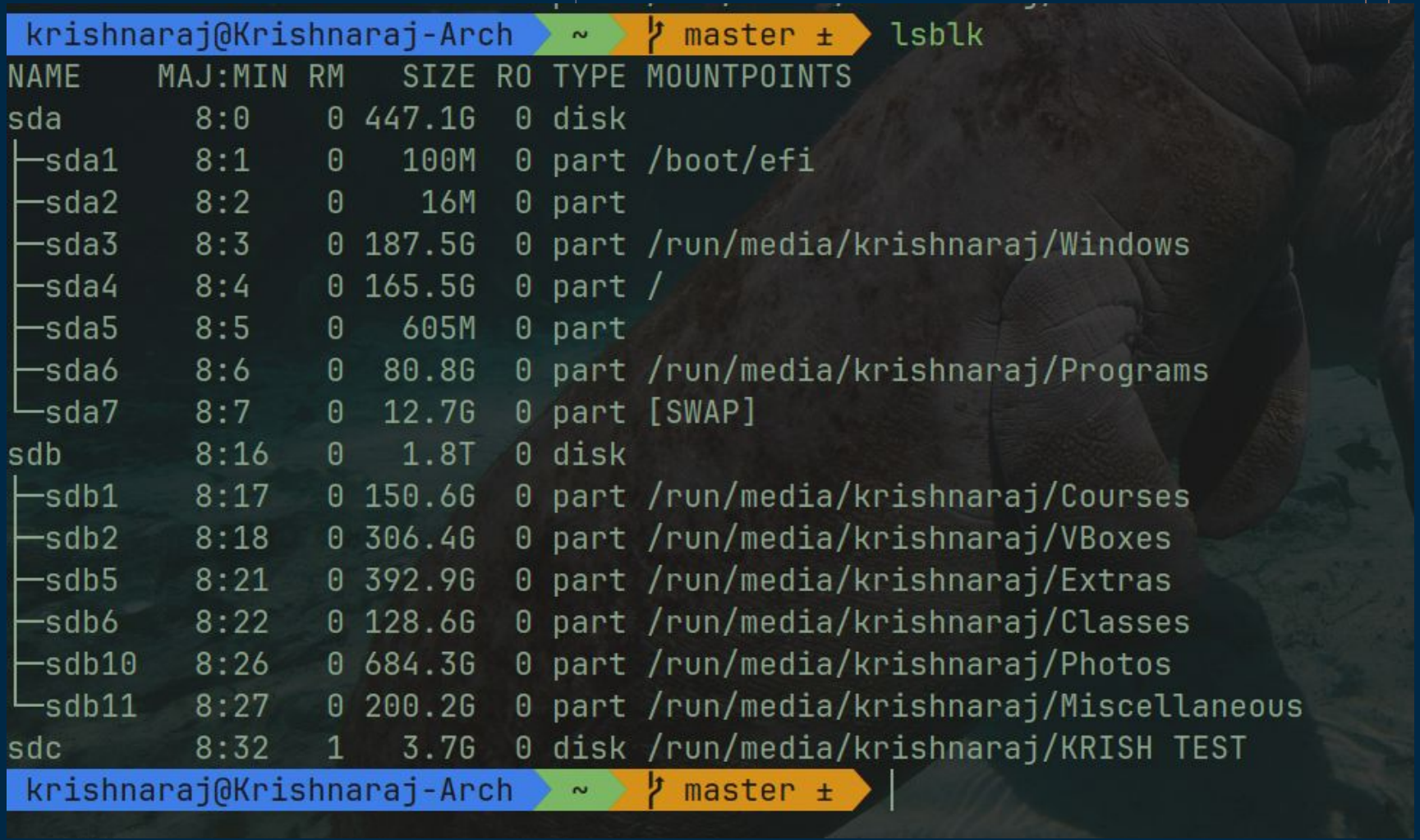
download ④.jpeg
6.5 kB
Image
Image

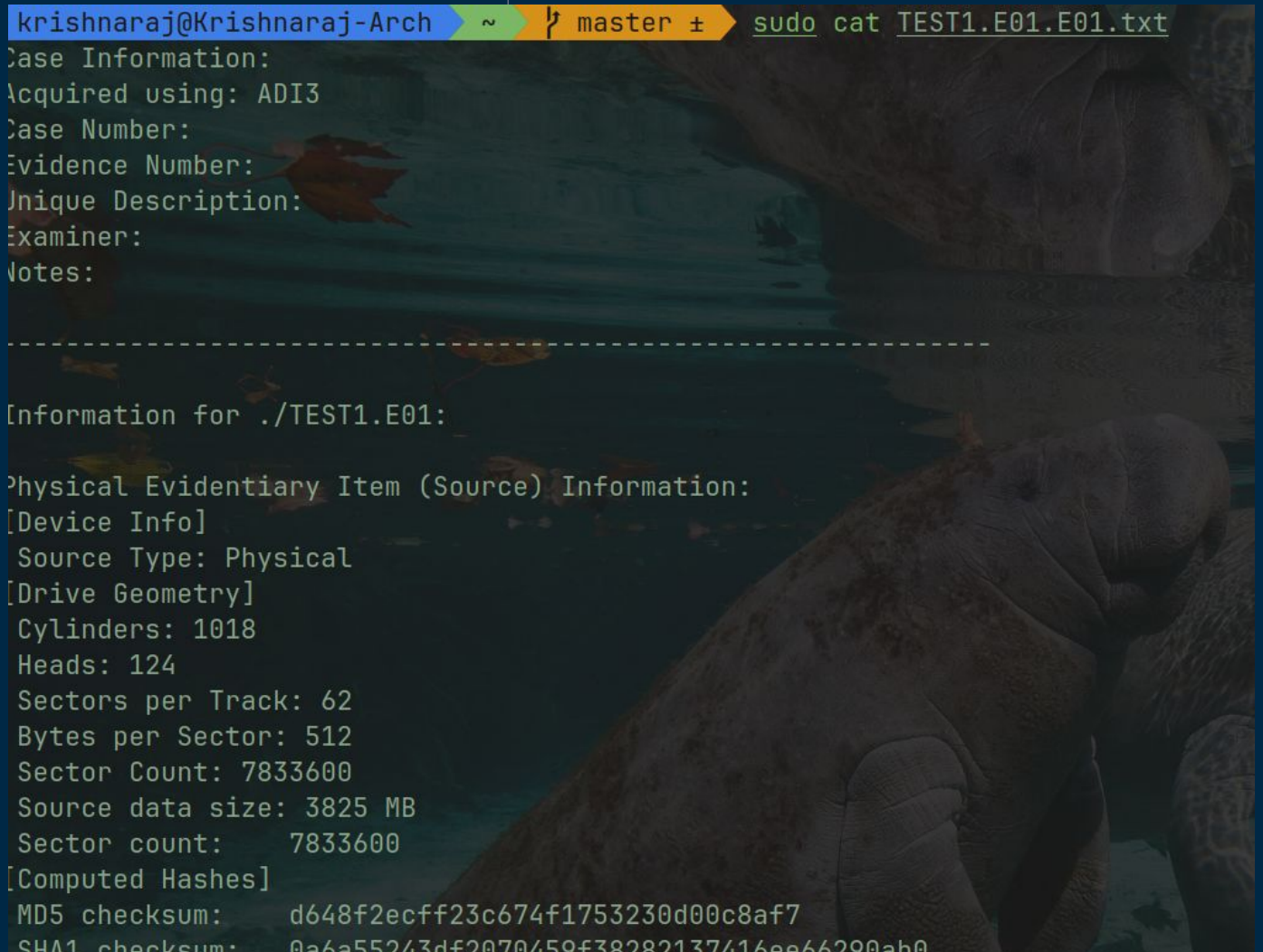


download ⑤.jpeg
4.9 kB
Image
Image

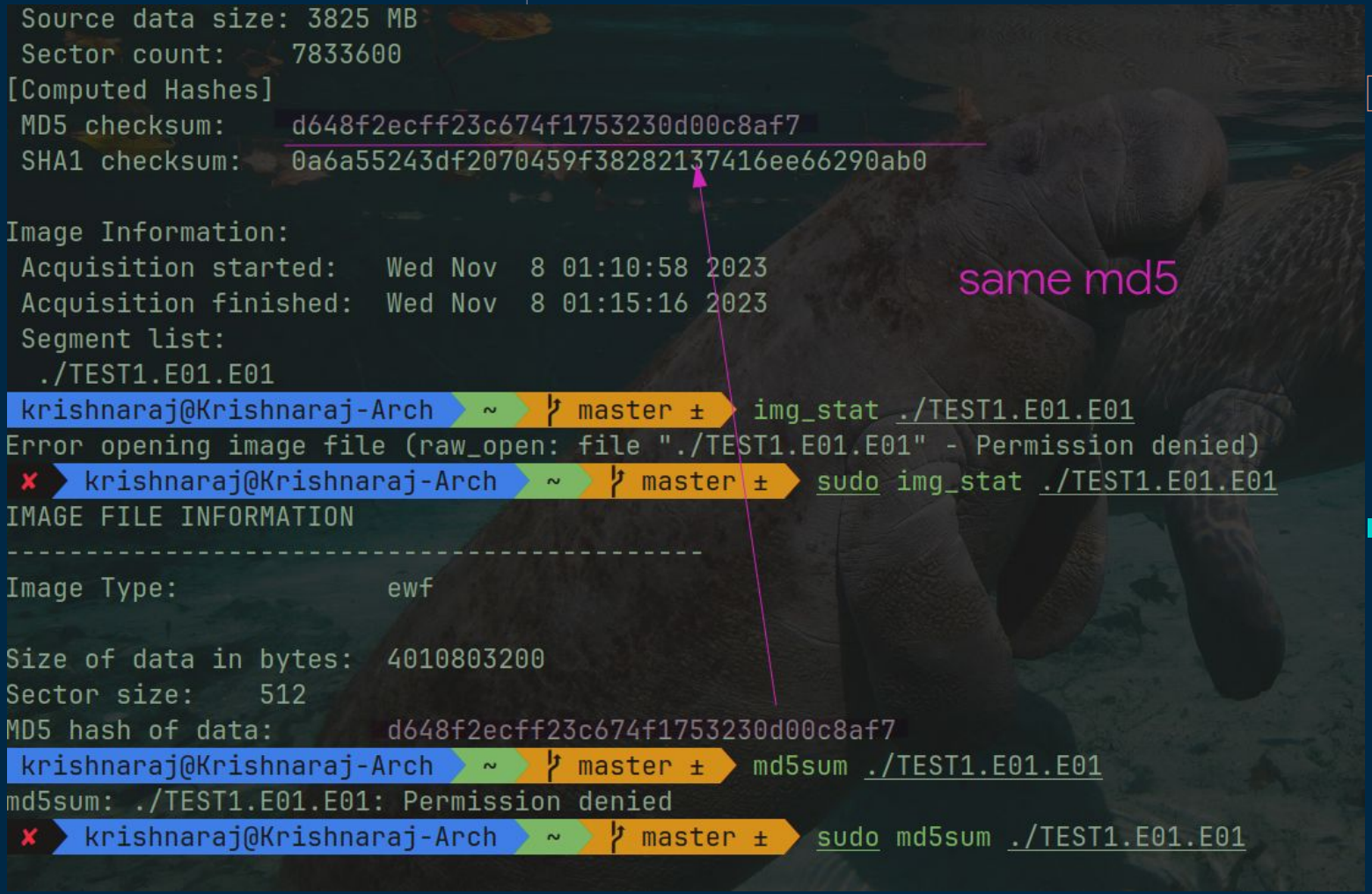
download ⑥.jpeg
9.2 kB
Image
Image

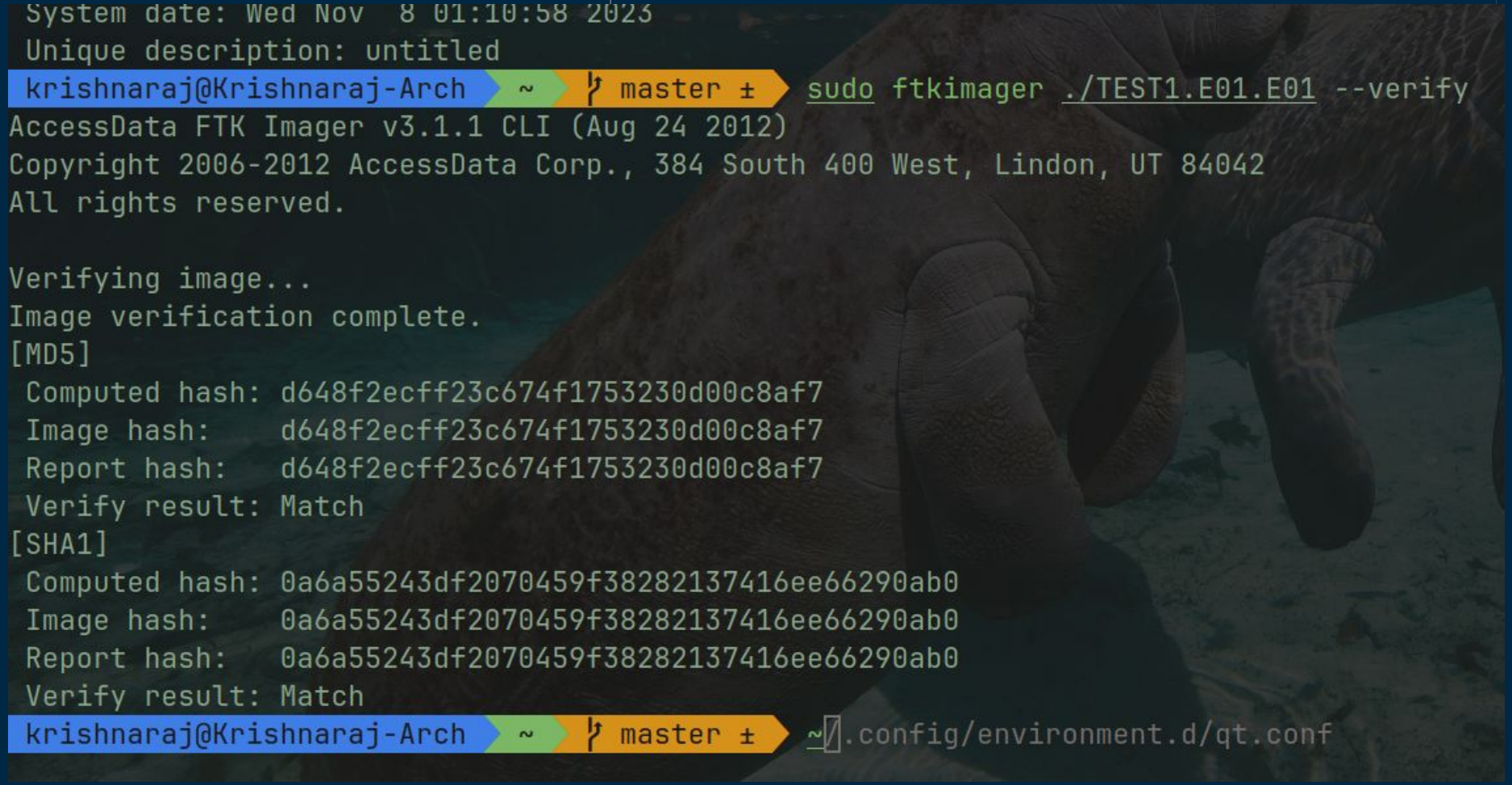


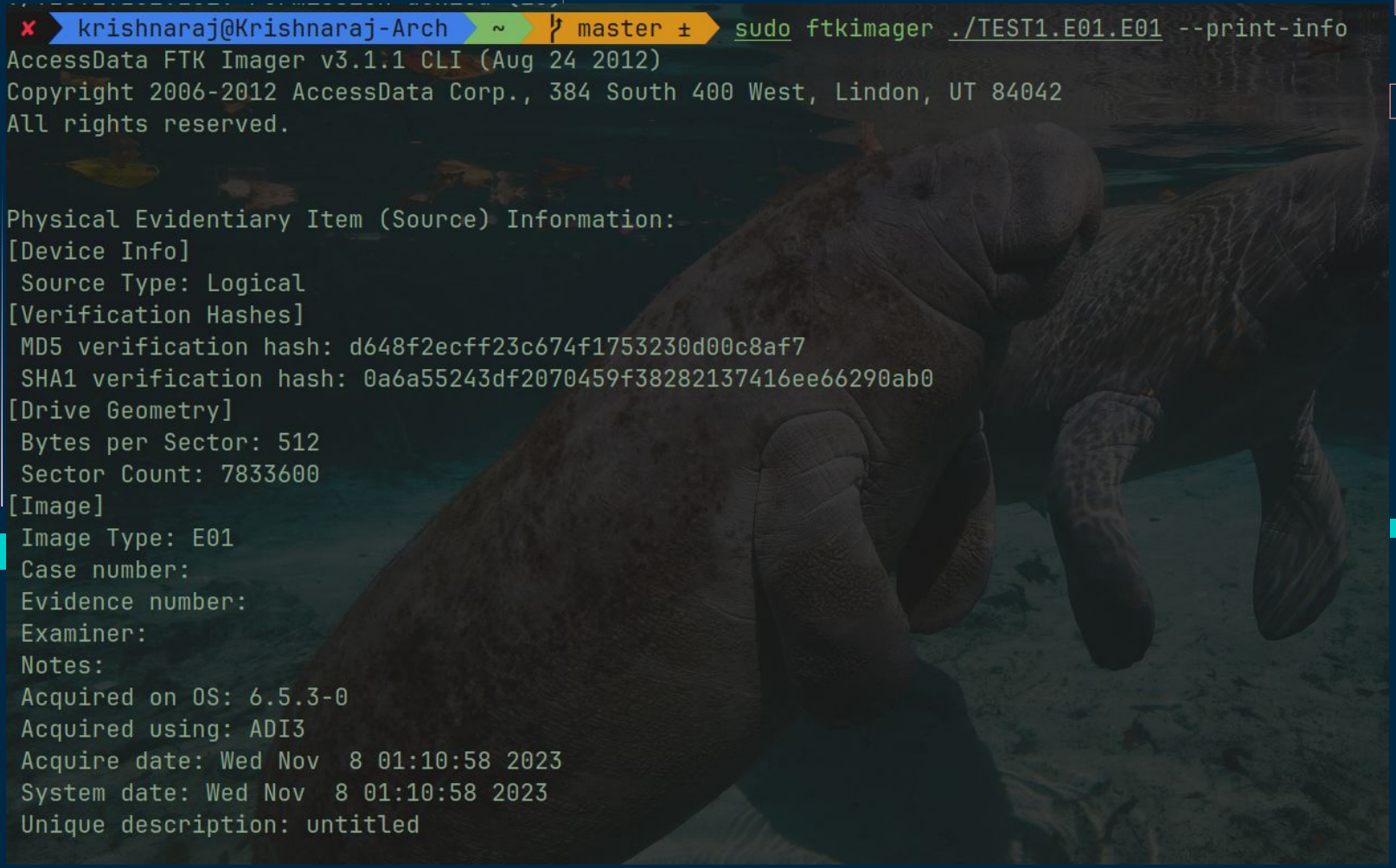

krishnaraj@Krishnaraj-Arch ~ master ± lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
sda 8:0 0 447.1G 0 disk
├─sda1 8:1 0 100M 0 part /boot/efi
├─sda2 8:2 0 16M 0 part
├─sda3 8:3 0 187.5G 0 part /run/media/krishnaraj/Windows
├─sda4 8:4 0 165.5G 0 part /
├─sda5 8:5 0 605M 0 part
├─sda6 8:6 0 80.8G 0 part /run/media/krishnaraj/Programs
└─sda7 8:7 0 12.7G 0 part [SWAP]
sdb 8:16 0 1.8T 0 disk
├─sdb1 8:17 0 150.6G 0 part /run/media/krishnaraj/Courses
├─sdb2 8:18 0 306.4G 0 part /run/media/krishnaraj/VBoxes
├─sdb5 8:21 0 392.9G 0 part /run/media/krishnaraj/Extras
├─sdb6 8:22 0 128.6G 0 part /run/media/krishnaraj/Classes
├─sdb10 8:26 0 684.3G 0 part /run/media/krishnaraj/Photos
└─sdb11 8:27 0 200.2G 0 part /run/media/krishnaraj/Miscellaneous
sdc 8:32 1 3.7G 0 disk /run/media/krishnaraj/KRISH TEST
krishnaraj@Krishnaraj-Arch ~ master ±

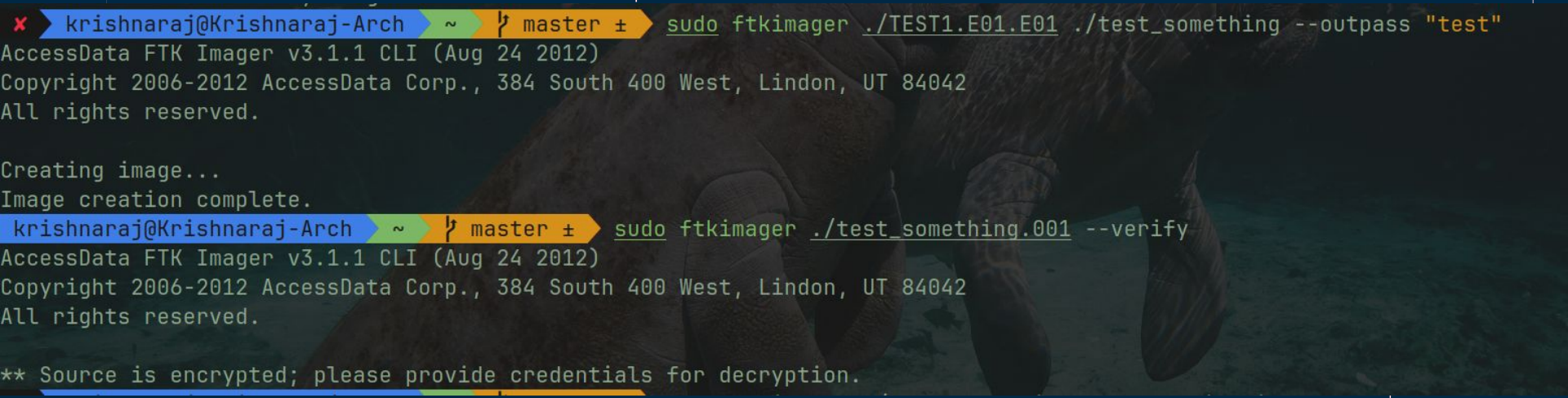

krishnaraj@Krishnaraj-Arch ~ master ± sudo cat TEST1.E01.E01.txt
Case Information:
Acquired using: ADI3
Case Number:
Evidence Number:
Unique Description:
Examiner:
Notes:

Information for ./TEST1.E01:
Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Physical
[Drive Geometry]
Cylinders: 1018
Heads: 124
Sectors per Track: 62
Bytes per Sector: 512
Sector Count: 7833600
Source data size: 3825 MB
Sector count: 7833600
[Computed Hashes]
MD5 checksum: d648f2ecff23c674f1753230d00c8af7


Source data size: 3825 MB
Sector count: 7833600
[Computed Hashes]
MD5 checksum: d648f2ecff23c674f1753230d00c8af7
SHA1 checksum: 0a6a55243df2070459f38282137416ee66290ab0
Image Information:
Acquisition started: Wed Nov 8 01:10:58 2023
Acquisition finished: Wed Nov 8 01:15:16 2023
Segment list:
./TEST1.E01.E01
krishnaraj@Krishnaraj-Arch ~ master ± img_stat ./TEST1.E01.E01
Error opening image file (raw_open: file "./TEST1.E01.E01" - Permission denied)
krishnaraj@Krishnaraj-Arch ~ master ± sudo img_stat ./TEST1.E01.E01
IMAGE FILE INFORMATION
Image Type: ewf
Size of data in bytes: 4010803200
Sector size: 512
MD5 hash of data: d648f2ecff23c674f1753230d00c8af7
krishnaraj@Krishnaraj-Arch ~ master ± md5sum ./TEST1.E01.E01
md5sum: ./TEST1.E01.E01: Permission denied
krishnaraj@Krishnaraj-Arch ~ master ± sudo md5sum ./TEST1.E01.E01
same md5


System date: Wed Nov 8 01:10:58 2023
Unique description: untitled
krishnaraj@Krishnaraj-Arch ~ master ± sudo ftkimager ./TEST1.E01.E01 --verify
AccessData FTK Imager v3.1.1 CLI (Aug 24 2012)
Copyright 2006-2012 AccessData Corp., 384 South 400 West, Lindon, UT 84042
All rights reserved.
Verifying image...
Image verification complete.
[MD5]
Computed hash: d648f2ecff23c674f1753230d00c8af7
Image hash: d648f2ecff23c674f1753230d00c8af7
Report hash: d648f2ecff23c674f1753230d00c8af7
Verify result: Match
[SHA1]
Computed hash: 0a6a55243df2070459f38282137416ee66290ab0
Image hash: 0a6a55243df2070459f38282137416ee66290ab0
Report hash: 0a6a55243df2070459f38282137416ee66290ab0
Verify result: Match
krishnaraj@Krishnaraj-Arch ~ master ± ~/.config/environment.d/qt.conf

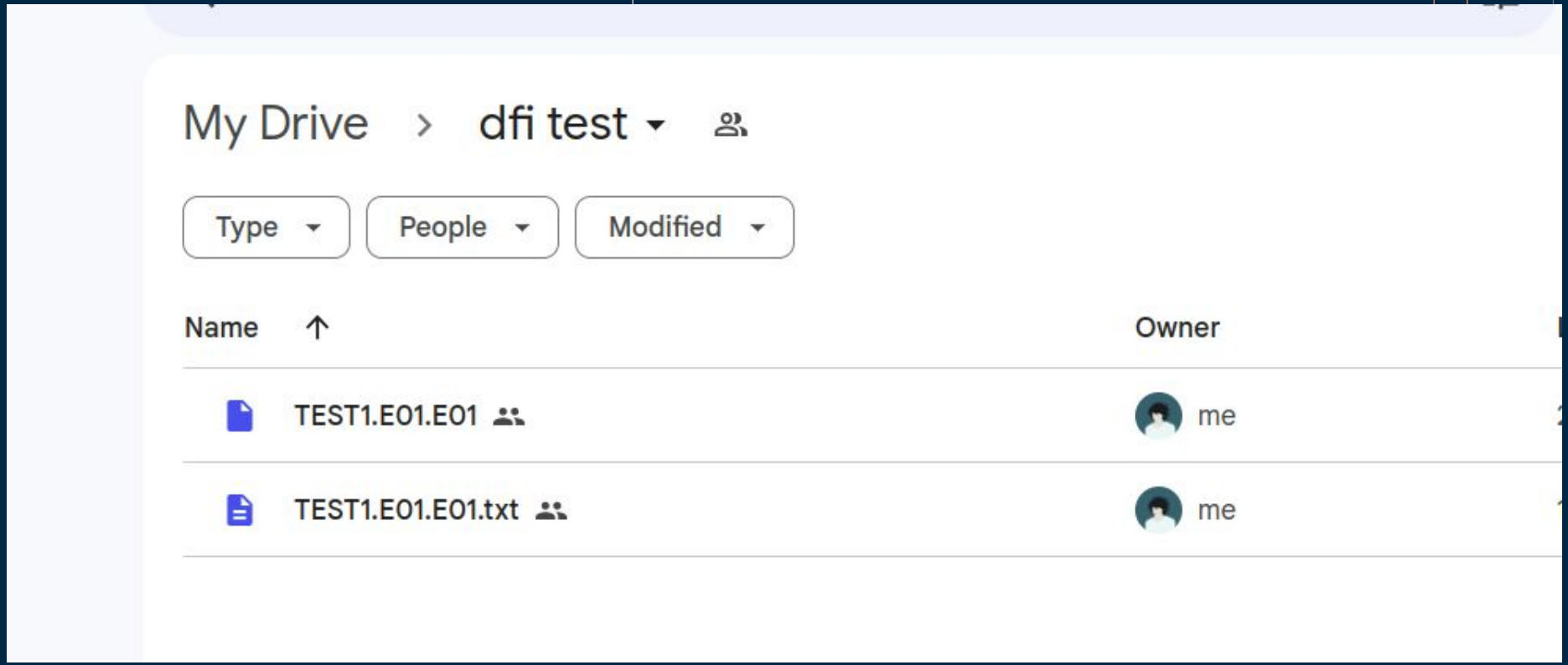

krishnaraj@Krishnaraj-Arch ~ master ± sudo ftkimager ./TEST1.E01.E01 --print-info
AccessData FTK Imager v3.1.1 CLI (Aug 24 2012)
Copyright 2006-2012 AccessData Corp., 384 South 400 West, Lindon, UT 84042
All rights reserved.
Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Logical
[Verification Hashes]
MD5 verification hash: d648f2ecff23c674f1753230d00c8af7
SHA1 verification hash: 0a6a55243df2070459f38282137416ee66290ab0
[Drive Geometry]
Bytes per Sector: 512
Sector Count: 7833600
[Image]
Image Type: E01
Case number:
Evidence number:
Examiner:
Notes:
Acquired on OS: 6.5.3-0
Acquired using: ADI3
Acquire date: Wed Nov 8 01:10:58 2023
System date: Wed Nov 8 01:10:58 2023
Unique description: untitled

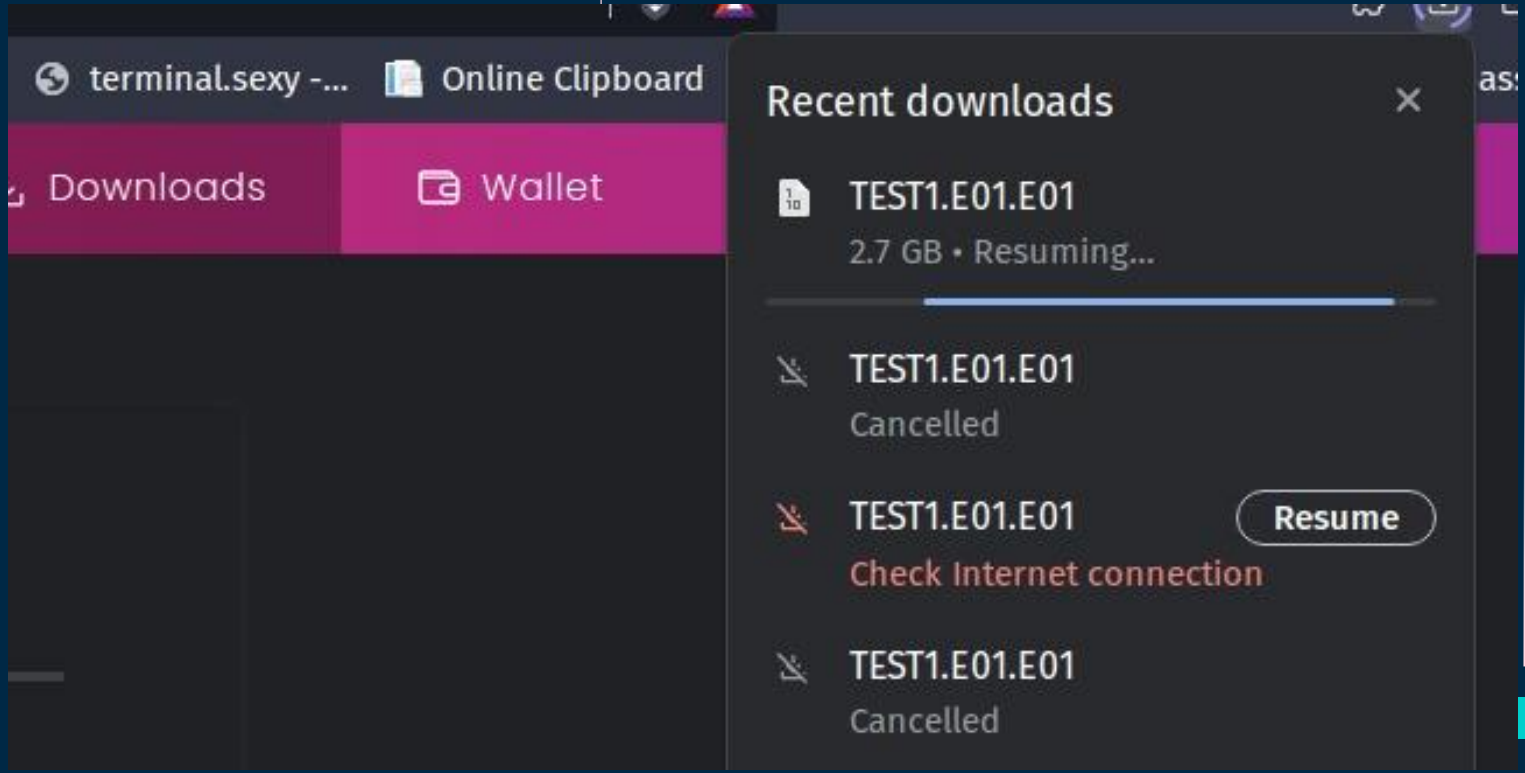

krishnaraj@Krishnaraj-Arch ~ master ± sudo ftkimager ./TEST1.E01.E01 ./test_something --outpass "test"
AccessData FTK Imager v3.1.1 CLI (Aug 24 2012)
Copyright 2006-2012 AccessData Corp., 384 South 400 West, Lindon, UT 84042
All rights reserved.
Creating image...
Image creation complete.
krishnaraj@Krishnaraj-Arch ~ master ± sudo ftkimager ./test_something.001 --verify
AccessData FTK Imager v3.1.1 CLI (Aug 24 2012)
Copyright 2006-2012 AccessData Corp., 384 South 400 West, Lindon, UT 84042
All rights reserved.
** Source is encrypted; please provide credentials for decryption.

Further Investigation

05

Image file, and its data sent to Parth Zarekar for analysis.


My Drive
dfi test
Type
People
Modified
Name
Owner
TEST1.E01.E01
me
TEST1.E01.E01.txt
me


terminal.sexy -...
Online Clipboard
Downloads
Wallet
Recent downloads
TEST1.E01.E01
2.7 GB • Resuming...
TEST1.E01.E01
Cancelled
TEST1.E01.E01
Resume
Check Internet connection
TEST1.E01.E01
Cancelled

File | /mnt/sda1/DFIR/003-Krish/Autopsy/0003-Krish/Reports/0003-Krish%20H

Dashboard - E... Watch Cartoon... MODCOMBO -... Temp Mail - Di... (17) Wh

Autopsy Forensic Report

HTML Report Generated on 2023/11/08 03:11:39

Case:	0003-Krish
Case Number:	003
Number of data sources in case:	1
Examiner:	Parth Zarekar

Image Information:

References

- Case Study: Aurora Police Department Relies on FTK® to Collect Key Digital Evidence in Tragic Colorado Movie Theater Mass Shooting
- Test Results for Digital Data Acquisition Tool: FTK Imager 2.5.3.14

Thank You