CERIAS

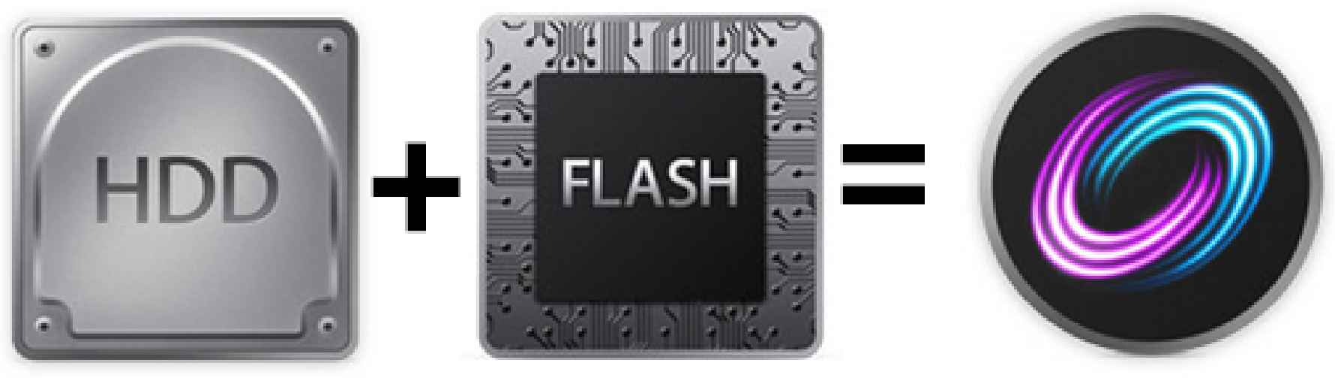
The Center for Education and Research in Information Assurance and Security

ESTABLISHING FORENSIC ACQUISITION PROCEDURES FOR THE APPLE FUSION DRIVE

Adolfo Montironi, Prof. Marcus Thompson
Department of Computer and Information Technology
Purdue University

What is a Fusion Drive?

It is a logical hybrid volume which merges a flash SSD with a magnetic HDD. Its purpose is to combine the high performance of the flash SSD with the available capacity of the magnetic HDD.

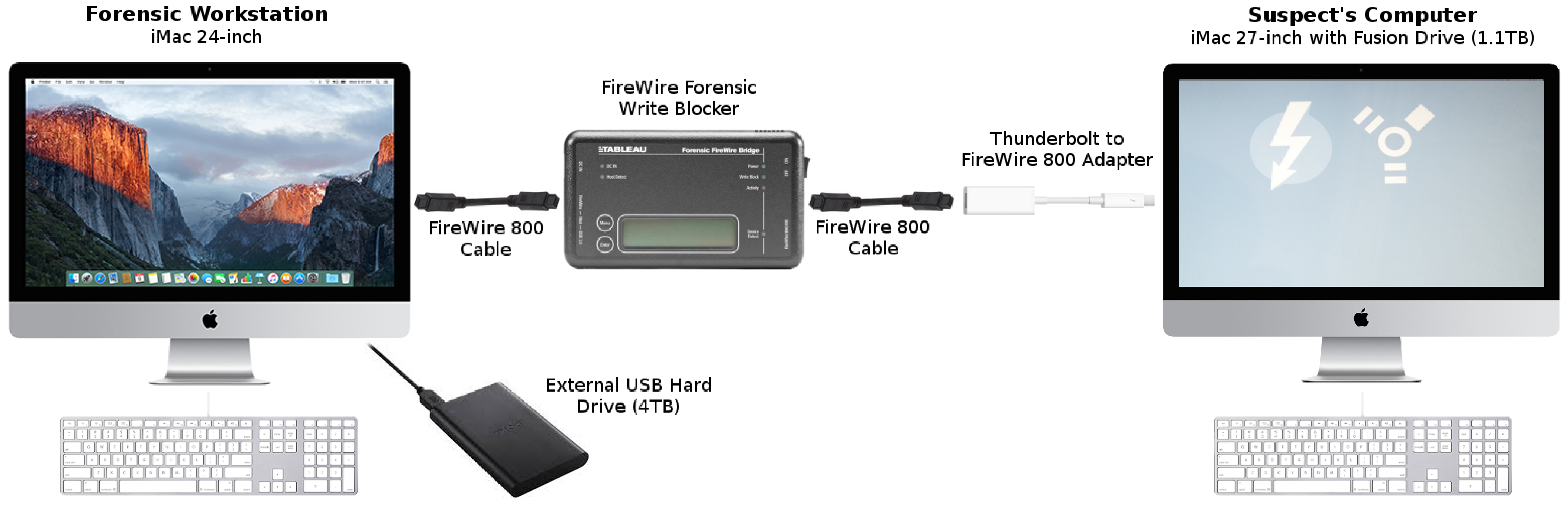


Problem Statement

- Is it possible to perform a forensic acquisition of Fusion Drives without using commercial tools such as Macquisition?
- Is it reliable to create a bit stream copy from an SSD as a forensic image?

Research Scenario

- The Fusion Drive of the suspect's computer was imaged using core utilities of the OS from the forensic workstation.
- The images were verified and stored in an external USB hard drive.
- A forensic write blocker was used throughout the research process.


Forensic Workstation
iMac 24-inch
FireWire 800 Cable
FireWire Forensic Write Blocker
FireWire 800 Cable
Thunderbolt to FireWire 800 Adapter
Suspect's Computer
iMac 27-inch with Fusion Drive (1.1TB)
External USB Hard Drive (4TB)

Research Process

- 🍎 Create a forensic image from the SSD using Mac OS (command dd)
- 🐧 Create two forensic images from the SSD using Ubuntu (dd and dc3dd)
- 🐧 Develop and execute a Bash script to create 10 forensic images, at different intervals of time, from the SSD
- 🍎🐧 Compare MD5 and SHA1 values from all the images created
- 🐧 Create and verify a forensic image from the HDD
- 🍎 Reassemble the original Fusion Drive from the images of the SSD and HDD
- 🍎 Create and verify a new image from the reassembled Fusion Drive
- 🪟 Perform a basic examination with FTK on the Fusion Drive forensic image

Results

1. All the images created from the SSD had the same MD5 and SHA1 values. Thus, under stable conditions (regarding TRIM, garbage collection, and wear leveling processes) it was valid to create bit stream images from the SSD.
2. Using core utilities of Mac OS, the Fusion Drive was reassembled from the forensic images of the SSD and the HDD.
3. A forensic image from the reassembled Fusion Drive was created. Then, it was examined with FTK and all the files from the suspect's computer were accessed.

Conclusion

A practical procedure is now defined using core utilities of the operating system, to create, verify, and validate a forensic image from a Fusion Drive.

CERIAS®

PURDUE
UNIVERSITY