2026

USB Analysis

PREPARED FOR FORENSICS PROGRAM

ON JANUARY 30TH 2026

Logan Wendel
Jr. Forensic Investigator
logan.wendel@mymail.champlain.edu
Connor Schuler
Jr. Forensic Investigator
connor.schuler@mymail.champlain.edu

Table of Contents

USB Analysis Report

Background

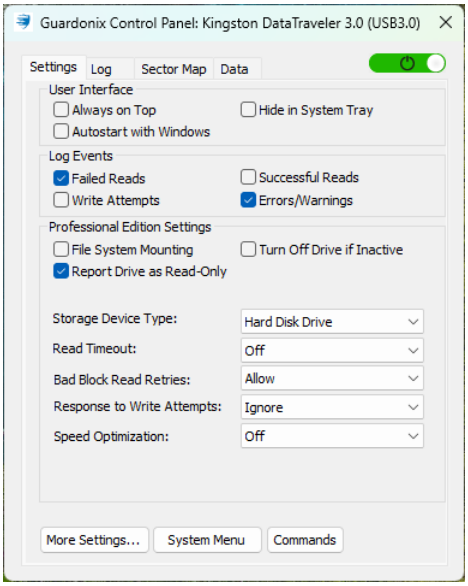
Logan Wendel, Digital Investigator with Champlain College, as well as Connor Schuler, Digital Investigator with Champlain College, have been appointed to Analyze a suspicious USB that was found by a Champlain College Faculty Member. We have been tasked to take an image of the USB drive to find any possible harmful files that could be contained within the drive.

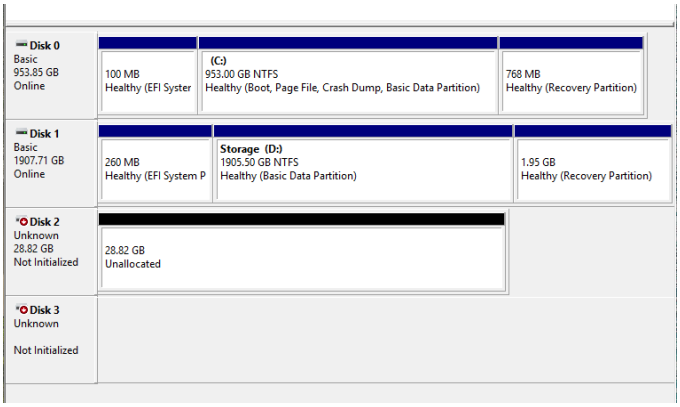
This report contains a detailed description of the same.

Evidence and Processing

1 USB hard drive was provided by the client on 30 January 2026. Forensic images of the disk were obtained, and they had the following hash values:

- Drive 1: Kingston 32GB USB drive (Labeled as G3) -
    - MD5 Hash: bd4a3b736e7eb71ea344e09bda6fa7cf
    - SHA1 Hash: 43040f7dfd8e7bc9cf4d8b05a264e743113a37ed





Images #1, 2, and 3 - In this screenshot, Investigator Schuler has the USB disk attached and the correct settings are enabled from the Guardonix application. This shows that the Guardonix Application is downloaded and that write-blocking is enabled.

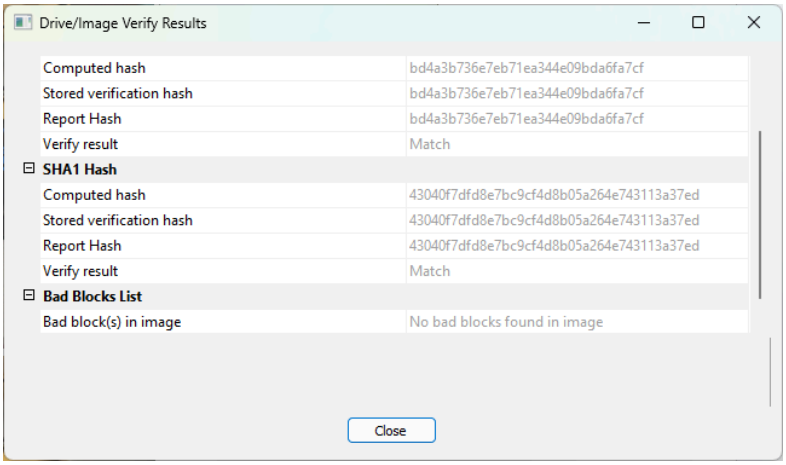
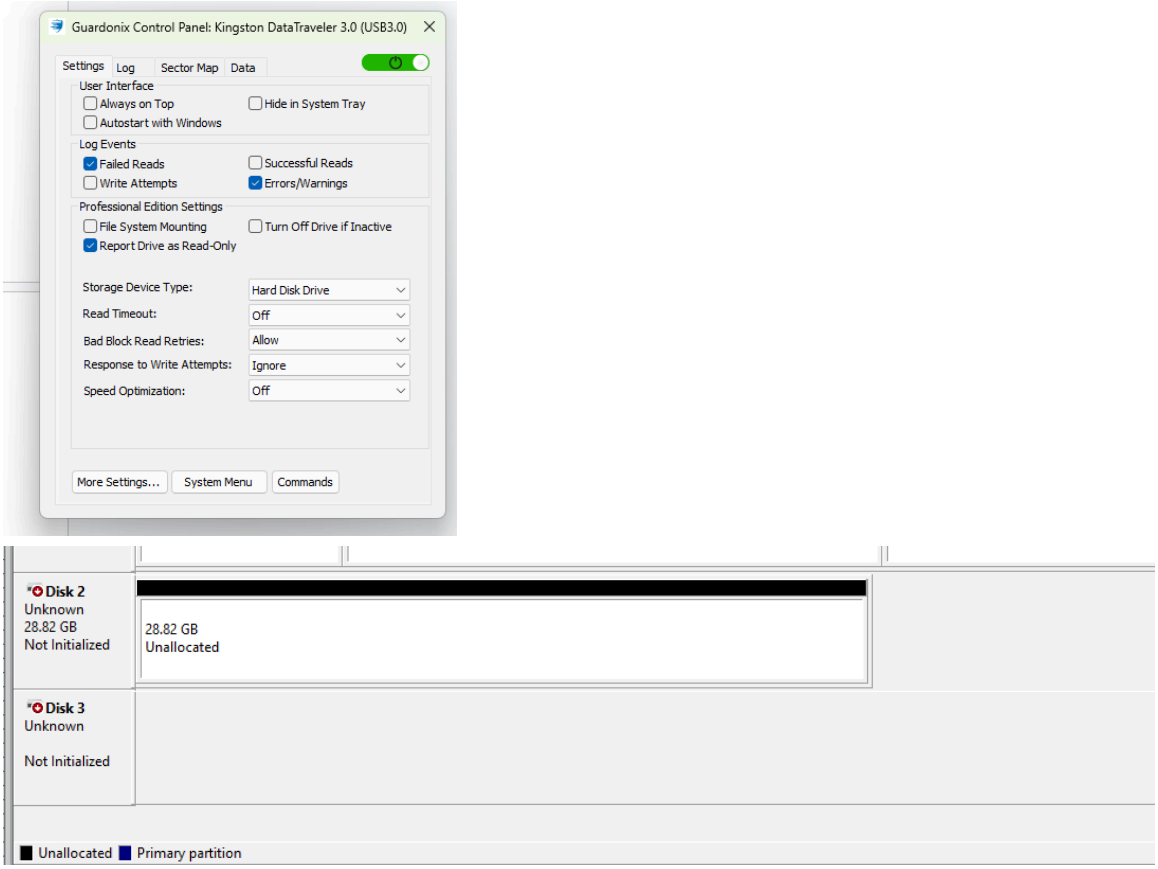


Image #4 - In this screenshot, Investigator Schuler has the verification image for the E01 image disk with the MD5 and SHA1 hashes as well as the bad blocks list.



Images #5 and 6 - In this screenshot, Investigator Wendel has the USB disk attached and the correct settings are enabled from the Guardonix application. This shows that the Guardonix Application is downloaded and that write-blocking is enabled.

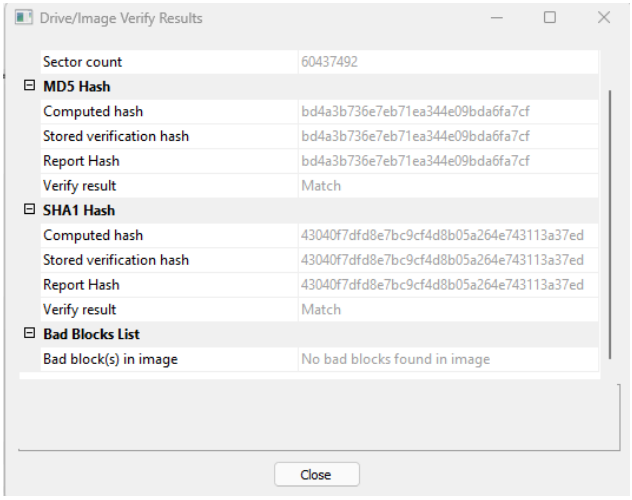
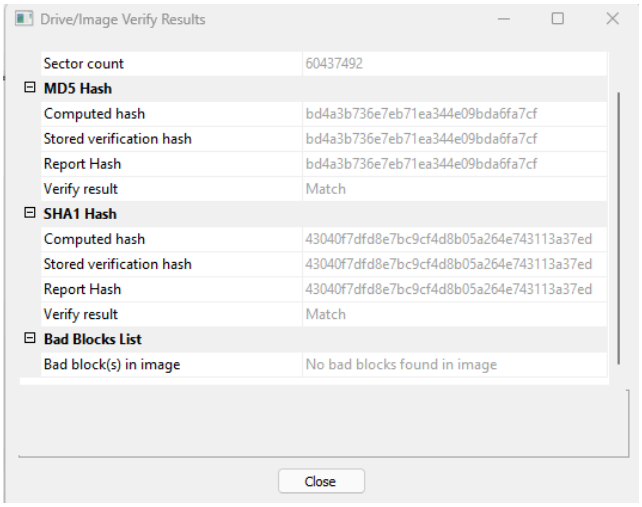


Image #7 - In this screenshot, Investigator Wendel has the verification image for the E01 image disk with the MD5 and SHA1 hashes as well as the bad blocks list.

Tools Used

FTK Imager - 4.7.3.81
Guardonix GRDNX-100, Serial Number DSU00462
Guardonix Application
Windows Disk Management

Findings



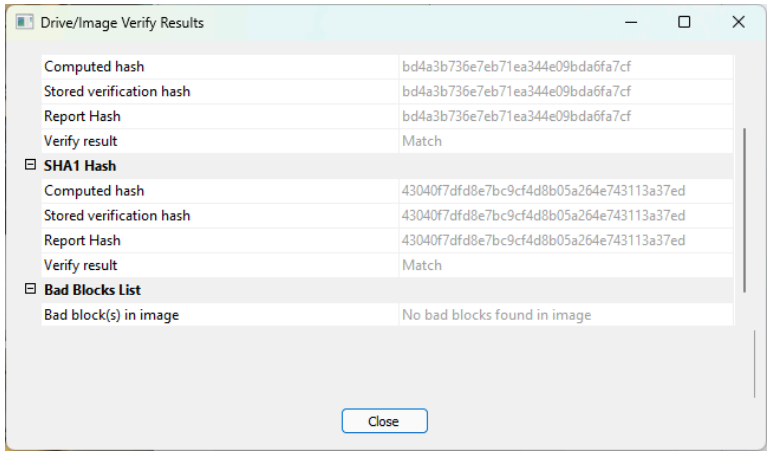


Image #8 and 9 - In this screenshot, Investigator Schuler has verified the hashes of the E01 images using FTK Imager.

Summary/Conclusion

Investigators Logan Wendel and Connor Schuler each took an E01 physical images of a Kingston 32GB drive using a Guardonix Write Blocker and the Guardonix Application. These images were cross validated in FTK imager and had the same

hash values. This validates the images taken by the investigators.

Signed by

L.Wendel
Logan Wendel

C. Schuler
Connor Schuler