

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

Background	2
Evidence and Processing	2
Tools Used	5
Findings	5
Summary/Conclusion	5
Signed by	6

USB Analysis Report

Background

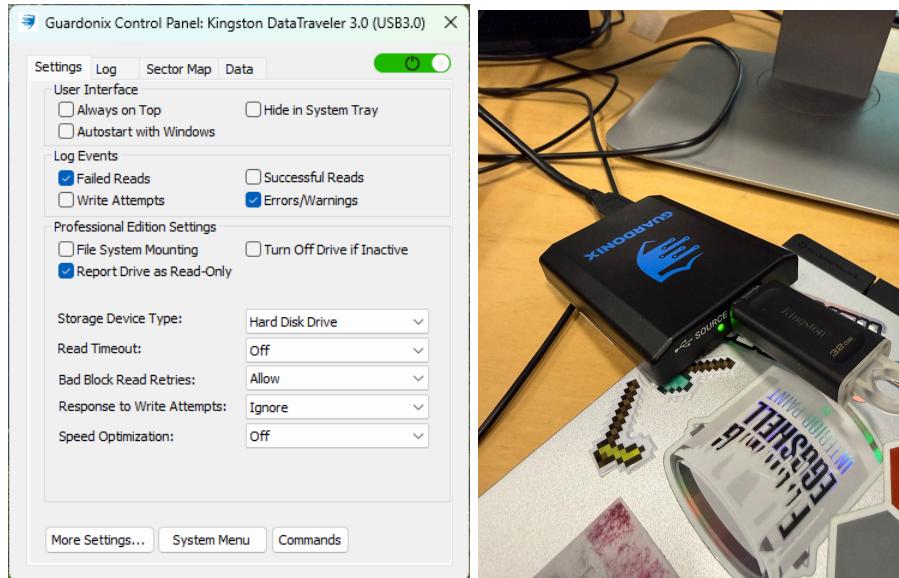
Logan Wendel, Digital Investigator with Champlain College, as well as Connor Schuler, Digital Investigator with Champlain College, have been appointed to Analyze a suspicious USB that was found by a Champlain College Faculty Member. We have been tasked to take an image of the USB drive to find any possible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

This report contains a detailed description of the same.

Evidence and Processing

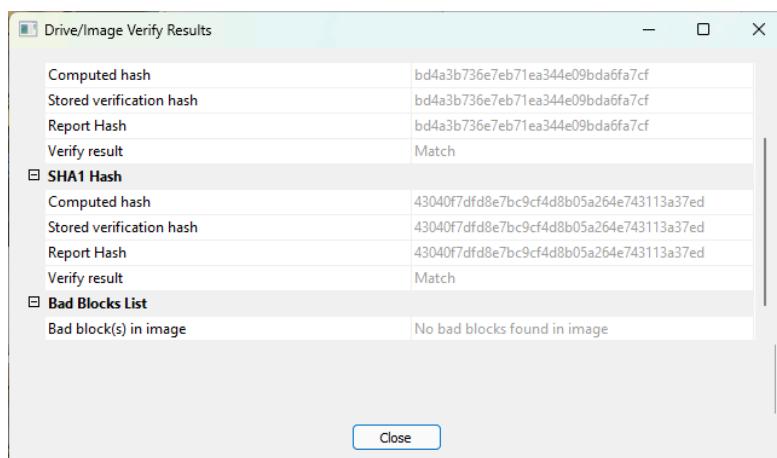
1 USB hard drive was provided by the client on 30 January 2026. Forensic images of the disk were obtained, and they had the following hash values:

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



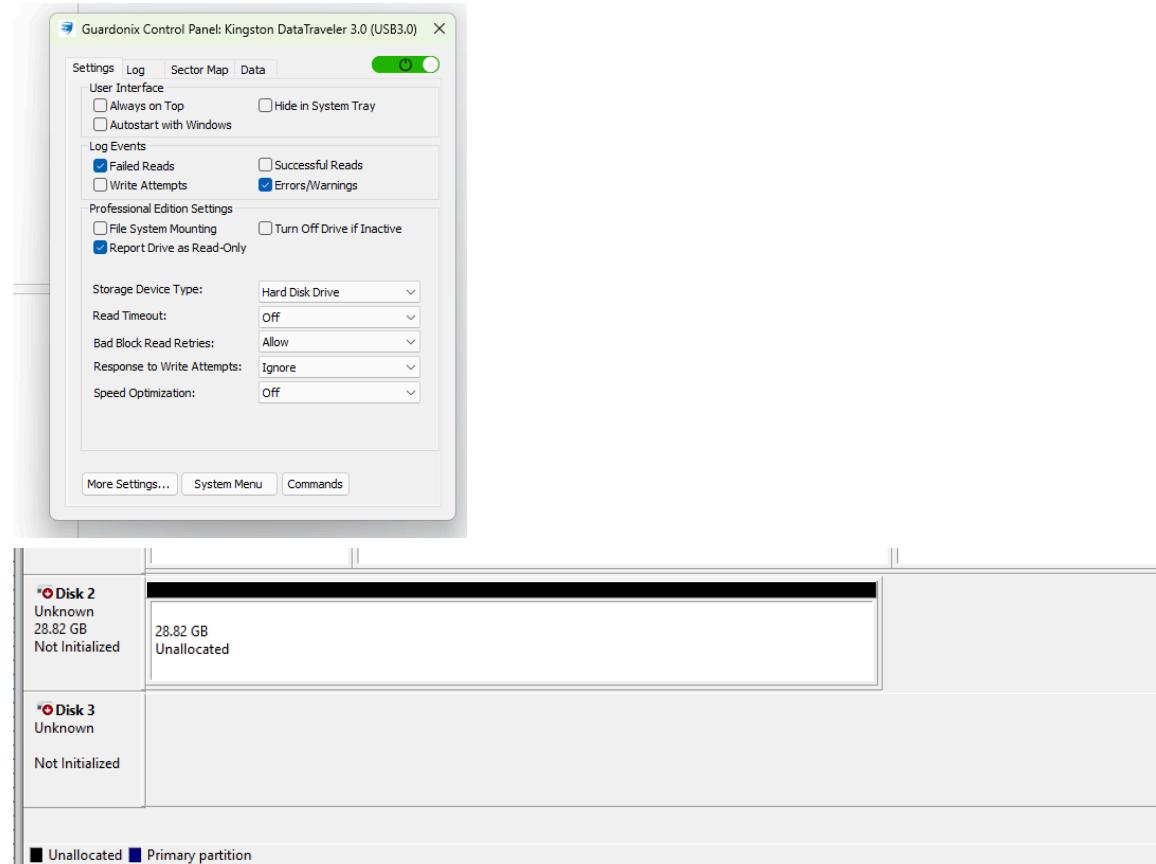
Disk 0	
Basic 953.85 GB Online	100 MB (C) Healthy (EFI System) 100 MB (C) Healthy (Boot, Page File, Crash Dump, Basic Data Partition)
Basic 1907.71 GB Online	260 MB (D) Storage (D) 1905.50 GB NTFS Healthy (Basic Data Partition)
Disk 1 Unknown 28.82 GB Not Initialized	1.95 GB Healthy (Recovery Partition)
Disk 2 Unknown 28.82 GB Not Initialized	28.82 GB Unallocated
Disk 3 Unknown Not Initialized	

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.



SHA1 Hash	Computed hash	Stored verification hash	Report Hash	Verify result
Computed hash	bd4a3b736e7eb71ea344e09bda6fa7cf	bd4a3b736e7eb71ea344e09bda6fa7cf	bd4a3b736e7eb71ea344e09bda6fa7cf	Match
Computed hash	43040f7df8e7bc9cf4d8b05a264e743113a37ed	43040f7df8e7bc9cf4d8b05a264e743113a37ed	43040f7df8e7bc9cf4d8b05a264e743113a37ed	Match
Bad Blocks List	Bad block(s) in image	No bad blocks found in image		

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.

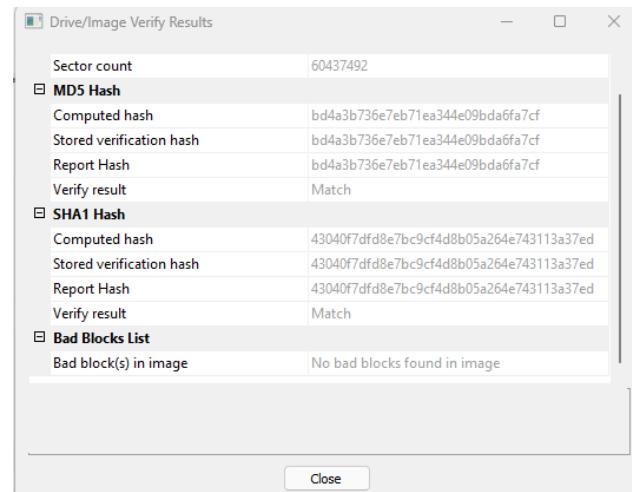


Image #7 - In this screenshot, Investigator Wendel has the verification image for the E01 image disk with the MD5 and SHA1 hashes as well as the bad blocks list.

Tools Used

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

Findings

The image contains two side-by-side screenshots of the FTK Imager 'Drive/Image Verify Results' window. Both windows show identical verification results for two different images.

Screenshot 1 (Top):

Drive/Image Verify Results	
Sector count	60437492
MD5 Hash	
Computed hash	bd4a3b736e7eb71ea344e09bda6fa7cf
Stored verification hash	bd4a3b736e7eb71ea344e09bda6fa7cf
Report Hash	bd4a3b736e7eb71ea344e09bda6fa7cf
Verify result	Match
SHA1 Hash	
Computed hash	43040f7dfd8e7bc9cf4d8b05a264e743113a37ed
Stored verification hash	43040f7dfd8e7bc9cf4d8b05a264e743113a37ed
Report Hash	43040f7dfd8e7bc9cf4d8b05a264e743113a37ed
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Screenshot 2 (Bottom):

Drive/Image Verify Results	
Computed hash	bd4a3b736e7eb71ea344e09bda6fa7cf
Stored verification hash	bd4a3b736e7eb71ea344e09bda6fa7cf
Report Hash	bd4a3b736e7eb71ea344e09bda6fa7cf
Verify result	Match
SHA1 Hash	
Computed hash	43040f7dfd8e7bc9cf4d8b05a264e743113a37ed
Stored verification hash	43040f7dfd8e7bc9cf4d8b05a264e743113a37ed
Report Hash	43040f7dfd8e7bc9cf4d8b05a264e743113a37ed
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

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