

DRAFT

Blumberg No. 5114

DEFENDANT'S
EXHIBIT

961



FEDERAL BUREAU OF INVESTIGATION
COMPUTER ANALYSIS RESPONSE TEAM
NEW YORK DIVISION

EXAMINATION NOTES

Examiner:	SA/FET Virginia Donnelly (VD) ITS/SFE Brian Booth (BB)	UCFN:	50A-NY-2233091
Case Agent:	SA Michael Lever, (Squad: C-2)	Submission ID:	196817
Phone:	(212) 384-3245	Title/Sub:	NXIVM; KEITH RANIERE (Subjects); ...
Date Assigned:	05/21/2018	Legal Authority:	Search and Seizure Warrant

Item #	Date	Init	Notes
	08/08/18	VD	Legal Authority Reviewed: Search and Seizure Warrant and Request Form reviewed.
			BEGIN EXAM
NYC023721 _1B16 NYC023722 _1B19 NYC023723 _1B23 NYC023724 _1B26	08/08/18	VD	Receipt of Evidence: Evidence received directly from Case Agent. E6261242 - 1B16 Western Digital external hard drive, dark gray, 500GB, model: WD5000P032, serial number (s/n): WCAS81365334, affixed barcode and designated as NYC023721_1B16 . Evidence received in brown paper bag sealed with evidence tape.
NYC023725 _1B27 NYC023725 _1B27-1 NYC023725 _1B27-2			E6261245 - 1B19 Amazon Kindle, white, model: D00611,s/n: B00418219322086, affixed barcode and designated as NYC023722_1B19 . Evidence received in brown paper bag sealed with evidence tape. Item contained in black cover.
NYC023726 _1B28 NYC023727 _1B31 NYC023728 _1B32 NYC023729 _1B33 NYC023730 _1B41 NYC023731 _1B43 NYC023732 _1B50			E6261247 - 1B23 Toshiba USB drive, silver, 4GB, model: U3 Smart, unique identifier: 6491J90506BM8K1, affixed barcode and designated as NYC023723_1B23 . Evidence received in brown paper bag sealed with evidence tape. Key attached to USB drive.
			E6261250 - 1B26 Western Digital external hard drive, white, 1TB, model: WD10000H1NC-00, s/n: WCAU47036371, affixed barcode and designated as NYC023724_1B26 . Evidence received in brown paper bag sealed with evidence tape.
			E6261251 - 1B27 Lenovo ThinkCentre M77 tower, black, model: A5U, s/n: MJREEDN, affixed barcode and designated as NYC023725_1B27 . Containing: One (1) Western Digital hard drive, 500GB, model: WD5000AAKX, s/n: WMAYUX846984, designated as NYC023725_1B27-1 . Containing: One (1) Seagate hard drive, 2TB, model: ST2000DM001, s/n: S1E0GFDN, designated as NYC023725_1B27-2 . Tower was sealed with evidence tape.

THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION.
DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.

Affix Label Here

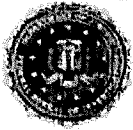
DRAFT



FEDERAL BUREAU OF INVESTIGATION
COMPUTER ANALYSIS RESPONSE TEAM
NEW YORK DIVISION

EXAMINATION NOTES

			Power cord was taped to tower. E6261252 - 1B28 Lacie external hard drive, silver, 500GB, model: 300964U, s/n: 164400534, affixed barcode and designated as NYC023726_1B28. Evidence received in a red accordion folder sealed with evidence tape. E6261239 - 1B31 ULTRA USB 2.0 Storage High Speed drive enclosure, black, no unique identifiers, affixed barcode and designated as NYC023727_1B31. Containing: Seagate hard drive, 120GB, model: ST9120821AS, s/n: 5PLOWPQC. Evidence received in a clear plastic bag sealed with evidence tape. Mini USB 2.0 cord provided. Item missing two (2) screws on each side, thus a total of four (4) screws. E6261238 - 1B32 Western Digital external hard drive, black, 1TB, product number (p/n): WDBAAH0010HCH-00, s/n: WCAV54873732, affixed barcode and designated as NYC023728_1B32. Evidence received in brown paper bag sealed with evidence tape. Digital screen reads "PICTURES 09." E6261237 - 1B33 Echo, black, 8GB, no unique identifiers, affixed barcode and designated as NYC023729_1B33. Evidence received in brown paper bag sealed with evidence tape. Item was in a black case with a micro USB 2.0 cord along with other accessories. E6280005 - 1B41 Lacie external hard drive, silver, 1TB, unique ID: 300798U, s/n: 154107441, affixed barcode and designated as NYC023730_1B41. Evidence received in a red accordion folder sealed with evidence tape. Item has a brown substance on the bottom. E6280007 - 1B43 Lexar Compact Flash Card, 256MB, p/n: 2250, Unique ID: 3884256AC2806A20A, affixed barcode and designated as NYC023731_1B43. Evidence received in a clear plastic bag sealed with evidence tape. E6280003 - 1B50 Apple iPod, black/silver, back has decorative skin, 100 GB, no visible unique identifiers, model: MA450LL, s/n: 8K7278QGV9R, affixed barcode and designated as NYC023732_1B50. Evidence received in brown paper bag sealed with evidence tape. Item was in a black case with accessories. Back of item has sticker
--	--	--	--



FEDERAL BUREAU OF INVESTIGATION
COMPUTER ANALYSIS RESPONSE TEAM
NEW YORK DIVISION

EXAMINATION NOTES

			Forensic Exam Station F2552510 (s/n: H09381A020H) is a MAC Pro/2.26 Model A1289 running Windows 10 Enterprise 64-bit Operating System with 32GB RAM and 2 Intel Xeon E5520 processors.
	09/13/18	VD	Performance Verification: Forensic Exam Station F2630035 posted correctly. Forensic Exam Station F2673128 posted correctly.
Staging Drive 1	09/12/18	VD	Staging Drive: One forensically wiped Western Digital hard drive, 2TB, model: WD20EARX, s/n: WCAZAE561750, was formatted with New Technology File System (NTFS). This drive will be utilized for staging images.
Staging Drive 2	09/12/18	VD	Staging Drive: One forensically wiped Western Digital hard drive, 2TB, model: WD20EARX, s/n: WCAZAJ020571, was formatted with New Technology File System (NTFS). This drive will be utilized for staging images.
NYC023725 _1B27-1 Staging Drive 1 NYC023725 _1B27-1.E01	09/12/18	VD	Preserve Evidence: Image NYC023725_1B27-1 was imaged using a Tableau TD3 Forensic Imager, model: TD3-B, s/n: 01D3B0A6, to Staging Drive 1. -----Source Disk----- Interface: SATA Model: WDC WD5000AAKX-083CA1 Firmware revision: 19.01H19 Serial number: WD-WMAYUX846984 Capacity in bytes: 500,107,862,016 (500.1 GB) Block Size: 512 bytes Block Count: 976,773,168 Power-ON Block Count: 976,773,168 HPA Block Count: 976,773,168 DCO Block Count: 976,773,168 -----Destination Disk----- Interface: SATA Model: WDC WD20EARX-00PASB0 Firmware revision: 51.0AB51 Serial number: WD-WCAZAE561750 Capacity in bytes: 2,000,398,934,016 (2.0 TB) Block Size: 512 bytes Block Count: 3,907,029,168 Power-ON Block Count: 3,907,029,168 HPA Block Count: 3,907,029,168 DCO Block Count: 3,907,029,168 -----Disk Imaging Results----- Output file format: E01 - EnCase format

THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION.
DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.

Affix Label Here



FEDERAL BUREAU OF INVESTIGATION
COMPUTER ANALYSIS RESPONSE TEAM
NEW YORK DIVISION

EXAMINATION NOTES

			covering entire back. These additional items were included but will not be examined by CART at this time: E6261253 - 1B29 Apple AirPort Extreme Base Station, white, model: A1354, s/n: 6F1169XWACC. Evidence received in brown paper bag sealed with evidence tape. Power cord provided. E6261236 - 1B34 Ubee Cable Modem/Router, white/blue, model: DDW3611, s/n: B831U27000562. Evidence received in brown paper bag sealed with evidence tape. Power cord provided. E6261235 - 1B35 Netgear N600 Wireless Dual Band Router, black/silver, model: WNDR3400, s/n: 2BK3117S22DD3. Evidence received in brown paper bag sealed with evidence tape.
	08/08/18	VD	Administrative note: Met Case Agent SA Michael Lever and SA Delise Jeffrey to discuss case while they dropped off the evidence. Agents asked CART to image items first and process later in order to provide copies of the images to AUSA. Agents then requested CART complete a standard exam process for the evidence provided. No specific additional analysis was requested.
	09/10/18	VD	Administrative Note: Met with CA to discuss evidence items. CA was informed that routers would contain IP addresses and that Computer Scientists usually handle this type of item. CA stated to not image or process the routers.
	09/13/18	VD	Case Volume Creation: A new case volume was created on NYCART-FS (\\NYCART-FS\\cases02\\NY-2233091_196817) using the Case Administration Tool v1.15.0.11, and mounted to Forensic exam station, hereinafter referred to as CASE VOLUME.
	09/13/18	VD	Equipment: Forensic Exam Station F2630035 (s/n: H01290MGEUH) is a MAC Pro/2.4 Model A1289 running Windows 10 Enterprise 64-bit Operating System with 28GB RAM and 2 Intel Xeon E5620 processors. Forensic Exam Station F2673128 (s/n: CMVJ11M7F4MH) is a MAC Pro/2.4 Model A1289 running Windows 10 Enterprise 64-bit Operating System with 24GB RAM and 2 Intel Xeon E5645 processors.



FEDERAL BUREAU OF INVESTIGATION
COMPUTER ANALYSIS RESPONSE TEAM
NEW YORK DIVISION

EXAMINATION NOTES

			Chunk size in bytes: 2,147,483,648 (2.1 GB) Chunks written: 54 Filename of first chunk: 2018-09-12_11-04-14/NYC023725_1B27-1.E01 Total errors: 0 Acquisition MD5: 5c4aead15ef34a54ddcd558dc2f7f947 -----Readback Verification Results----- Verification MD5: 5c4aead15ef34a54ddcd558dc2f7f947 Status: Verified
Staging Drive 1 NYC023725_1B27-1.E01	09/18/18	VD	Using Forensic Exam Station F2630035 and Tableau eSATA Forensic Bridge write blocker, model: T35es-R2, s/n: 3135D086, copy images of NYC023725_1B27-1 from Staging Drive 1 to CASE VOLUME.
NYC023725_1B27-1.E01	09/19/18	VD	Copy was verified using FTK® Imager 4.2.0.13 . Examiner created NYC023725_1B27-1.E01.txt to CASE VOLUME to retain logs. Image Verification Results: Verification started: Wed Sep 19 08:15:52 2018 Verification finished: Wed Sep 19 09:53:23 2018 MD5 checksum: 5c4aead15ef34a54ddcd558dc2f7f947 : verified
NYC023725_1B27-2 Staging Drive 1	09/12/18	VD	Preserve Evidence: Image Attempted to image NYC023725_1B27-2 using a Tableau TD3 Forensic Imager, model: TD3-B, s/n: 01D3B0A6, to Staging Drive 1. Drive inoperable.
NYC023725_1B27-2	09/21/18	VD	Connected NYC023725_1B27-2 to Tableau TX1 Forensic Imager, version: 1.2.0, s/n: 000ecc5801109b. Drive inoperable. Cooled drive to a lower temperature. Connected NYC023725_1B27-2 to Tableau TD3 Forensic Imager, model: TD3-B, s/n: 01D3B0A6. Drive inoperable.
NYC023725_1B27-2	09/21/18	VD	Administrative Note: Notified CA that drive was inoperable. CA not interested in sending drive to HQ at this time. No further processing to be conducted at this time.
NYC023727_1B31	09/11/18	VD	Preserve Evidence: Image NYC023727_1B31 was imaged using a Tableau TX1 Forensic Imager,

THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION.
DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.

Affix Label Here



FEDERAL BUREAU OF INVESTIGATION
COMPUTER ANALYSIS RESPONSE TEAM
NEW YORK DIVISION

EXAMINATION NOTES

Staging Drive 2 Image.E01			version: 1.2.0, s/n: 000ecc5801109b, to Staging Drive 2. Errors encountered but image successful. First attempt to image with TD3 was unsuccessful. -----Source Disk----- Interface: SATA Model: ATA ST9120821AS Firmware revision: 7.01 Serial number: 5PL0WPQC Capacity in bytes: 120,034,123,776 (120.0 GB) Block Size: 512 bytes Block Count: 234,441,648 Power-ON Block Count: 234,441,648 HPA Block Count: 234,441,648 DCO Block Count: 234,441,648 Encrypted: No Error granularity: 32,768 bytes -----Imaging----- Output file format: E01 Chunk size in bytes: 2,000,000,000 (2.0 GB) -----Image Destination----- Interface: SATA Model: WDC WD20EARX-00PASB0 Firmware revision: 51.0AB51 Serial number: WD-WCAZAJ020571 Capacity in bytes: 2,000,398,934,016 (2.0 TB) Block Size: 512 bytes Block Count: 3,907,029,168 Power-ON Block Count: 3,907,029,168 HPA Block Count: 3,907,029,168 DCO Block Count: 3,907,029,168 Encrypted: No Folder: /tx1_images/ File name base: image Verification Status: Finished OK Verification Md5: bdcc 8a77 2491 4693 2587 181e 0e1a 2c0d -----Duplication Results----- LBA Range Duplicated: Entire Source Disk Total errors: 200 Acquisition Md5: bdcc 8a77 2491 4693 2587 181e 0e1a 2c0d
Staging Drive 2 Image.E01	09/20/18	VD	Using Forensic Exam Station F2630035 and Tableau eSATA Forensic Bridge write blocker, model: T35es-R2, s/n: 3135D086, copy images of NYC023727_1B31 (image.E01) from Staging Drive 2 to CASE VOLUME. Copy was verified using FTK® Imager 4.2.0.13. Examiner created image.E01.txt to CASE VOLUME to retain logs.



FEDERAL BUREAU OF INVESTIGATION
COMPUTER ANALYSIS RESPONSE TEAM
NEW YORK DIVISION

EXAMINATION NOTES

			Image Verification Results: Verification started: Thu Sep 20 08:53:11 2018 Verification finished: Thu Sep 20 09:44:37 2018 MD5 checksum: bdcc8a77249146932587181e0e1a2c0d : verified
NYC023723_1B23 Staging Drive 1 NYC023723_1B23.E01	09/13/18	VD	Preserve Evidence: Image NYC023723_1B23 was imaged using a Tableau TD3 Forensic Imager, model: TD3-B, s/n: 01D350ED, to Staging Drive 1. -----Source Disk----- Interface: USB Model: TOSHIBA TransMemory Firmware revision: 6.51 Serial number: u USB Serial number: 0B901C6022B368A4 Capacity in bytes: 3,993,304,576 (3.9 GB) Block Size: 512 bytes Block Count: 7,799,423 -----Destination Disk----- Interface: SATA Model: WDC WD20EARX-00PASB0 Firmware revision: 51.0AB51 Serial number: WD-WCAZAE561750 Capacity in bytes: 2,000,398,934,016 (2.0 TB) Block Size: 512 bytes Block Count: 3,907,029,168 Power-ON Block Count: 3,907,029,168 HPA Block Count: 3,907,029,168 DCO Block Count: 3,907,029,168 -----Disk Imaging Results----- Output file format: E01 - EnCase format Chunk size in bytes: 2,147,483,648 (2.1 GB) Chunks written: 2 Filename of first chunk: 2018-09-13_08-44-54/NYC023723_1B23.E01 Total errors: 0 Acquisition MD5: dd5fcb5d670976ca749c35d14bba7f8e -----Readback Verification Results----- Verification MD5: dd5fcb5d670976ca749c35d14bba7f8e Status: Verified
Staging Drive 1 NYC023723_1B23.E01	09/19/18	VD	Using Forensic Exam Station F2630035 and Tableau eSATA Forensic Bridge write blocker, model: T35es-R2, s/n: 3135D086, copy images of NYC023723_1B23 from Staging Drive 1 to CASE VOLUME. Copy was verified using FTK® Imager 4.2.0.13 .



FEDERAL BUREAU OF INVESTIGATION
COMPUTER ANALYSIS RESPONSE TEAM
NEW YORK DIVISION

EXAMINATION NOTES

			Examiner created NYC023723_1B23.E01.txt to CASE VOLUME to retain logs. Image Verification Results: Verification started: Wed Sep 19 14:00:29 2018 Verification finished: Wed Sep 19 14:02:18 2018 MD5 checksum: dd5fcb5d670976ca749c35d14bba7f8e ; verified
NYC023730_1B41	09/13/18	VD	Preserve Evidence: Image NYC023730_1B41 was imaged with Forensic Exam Station F2630035 using a Tableau Forensic USB Bridge, model: T8-R2, s/n: 0208710F and a AccessData® FTK® Imager 4.2.0.13, to the CASE VOLUME.



FEDERAL BUREAU OF INVESTIGATION
COMPUTER ANALYSIS RESPONSE TEAM
NEW YORK DIVISION

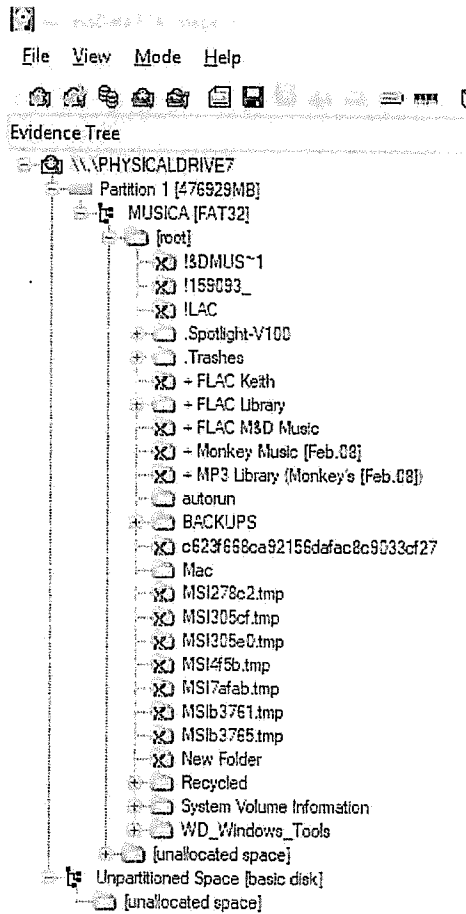
EXAMINATION NOTES

			Properties ☐ Evidence Source Path ☐ Evidence Type ☒ Disk ☒ Drive Geometry Cylinders Tracks per Cylinder Sectors per Track Bytes per Sector Sector Count ☒ Physical Drive Information Drive Model Drive Serial Number Drive Interface Type Removable drive Program shutdown before completion.
NYC023730 _1B41 NYC023730 _1B41.E01	09/14/18	VD	Restart image process. NYC023730_1B41 was imaged with Forensic Exam Station F2630035 using a Tableau Forensic USB Bridge, model: T8-R2, s/n: 0208710F and a AccessData® FTK® Imager 4.2.0.13, to the CASE VOLUME. Physical Evidentiary Item (Source) Information: [Device Info] Source Type: Physical [Drive Geometry] Cylinders: 121,605 Tracks per Cylinder: 255 Sectors per Track: 63 Bytes per Sector: 512 Sector Count: 1,953,588,224 [Physical Drive Information] Drive Model: LaCie BiggerDisk USB Device Drive Serial Number: A7E511243137 Drive Interface Type: USB Removable drive: False Source data size: 953900 MB Sector count: 1953588224 [Computed Hashes] MD5 checksum: 07df4939e1107220aa5dd1a39fb04767 Image Verification Results: Verification started: Fri Sep 14 22:38:22 2018 Verification finished: Sat Sep 15 03:19:25 2018 MD5 checksum: 07df4939e1107220aa5dd1a39fb04767 : verified A Directory/File Listing was generated when evidence was imaged using



FEDERAL BUREAU OF INVESTIGATION
COMPUTER ANALYSIS RESPONSE TEAM
NEW YORK DIVISION

EXAMINATION NOTES

			FTK® Imager 4.2.0.13. Listing file is co-located along with the respective image files. Listing contains filename, full path, modified date/time stamp, created (change) date/time stamp, and accessed date/time stamp. Directory listing created and saved as NYC023730_1B41.E01.csv within CASE VOLUME.
NYC023721_1B16 NYC023721_1B16.E01	09/13/18	VD	Preserve Evidence: Image NYC023721_1B16 was imaged with Forensic Exam Station F2673128 using a Tableau Forensic USB Bridge, model: T8-R2, s/n: 020870B7, and AccessData® FTK® Imager 4.2.0.13 , to the CASE VOLUME.  The screenshot shows the FTK Imager interface with the 'Evidence Tree' pane expanded. The tree structure is as follows: \\PHYSICALDRIVE7 - Partition 1 [476929MB] - MUSICA [FAT32] [root] !3DMUS~1 !159C93_ - ILAC .Spotlight-V100 .Trashes + FLAC Keith + FLAC Library + FLAC M&D Music + Monkey Music [Feb.08] + MP3 Library (Monkey's [Feb.08]) - autorun - BACKUPS - c623f668ca92156dafac8c9033cf27 - Mac - MSI278c2.tmp - MSI305cf.tmp - MSI305e0.tmp - MSI4f5b.tmp - MSI7afab.tmp - MSIb3761.tmp - MSIb3765.tmp - New Folder - Recycled - System Volume Information - WD_Windows_Tools [unallocated space] - Unpartitioned Space [basic disk] [unallocated space]



FEDERAL BUREAU OF INVESTIGATION
COMPUTER ANALYSIS RESPONSE TEAM
NEW YORK DIVISION

EXAMINATION NOTES

			Properties ☐ Evidence Source Path ☐ Evidence Type ☐ Disk ☐ Drive Geometry Cylinders Tracks per Cylinder Sectors per Track Bytes per Sector Sector Count ☐ Physical Drive Information Drive Model Drive Serial Number Drive Interface Type Removable drive 1st attempt never went past preparing for imaging.
NYC023721 _1B16	09/14/18	VD	Restart image process. Not reading the drive.
	09/19/18	VD	Open source search revealed Western Digital renamed the model number of NYC023721_1B16 from WD5000P032 to WDG1C5000N. Item name is "My Book Premium Edition."
NYC023721 _1B16 NYC023721 _1B16.E01	09/19/18	VD	NYC023721_1B16 was imaged with Forensic Exam Station F2673128 using a Tableau Forensic USB Bridge, model: T8-R2, s/n: 020870B7, and AccessData® FTK® Imager 4.2.0.13, to the CASE VOLUME. Physical Evidentiary Item (Source) Information: [Device Info] Source Type: Physical [Drive Geometry] Cylinders: 60,801 Tracks per Cylinder: 255 Sectors per Track: 63 Bytes per Sector: 512 Sector Count: 976,773,168 [Physical Drive Information] Drive Model: WD 5000A A External USB Device Drive Serial Number: 57442D57434153383133 Drive Interface Type: USB Removable drive: False



FEDERAL BUREAU OF INVESTIGATION
COMPUTER ANALYSIS RESPONSE TEAM
NEW YORK DIVISION

EXAMINATION NOTES

			Source data size: 476940 MB Sector count: 976773168 [Computed Hashes] MD5 checksum: 7aa8f3297f288252ed69ffd983725b5e Image Verification Results: Verification started: Wed Sep 19 15:37:01 2018 Verification finished: Wed Sep 19 20:09:15 2018 MD5 checksum: 7aa8f3297f288252ed69ffd983725b5e : verified A Directory/File Listing was generated when evidence was imaged using FTK® Imager 4.2.0.13. Listing file is co-located along with the respective image files. Listing contains filename, full path, modified date/time stamp, created (change) date/time stamp, and accessed date/time stamp. Directory listing created and saved as NYC023721_1B16.E01.csv within CASE VOLUME.
NYC023731_1B43 NYC023731_1B43.E01	09/14/18	VD	Preserve Evidence: Image NYC023731_1B41 was imaged with Forensic Exam Station F2552510 using a Digital Intelligence USB 3.0 Forensic Card Reader, SKU# W2525, and AccessData® FTK® Imager 4.2.0.13, to the CASE VOLUME.



FEDERAL BUREAU OF INVESTIGATION
COMPUTER ANALYSIS RESPONSE TEAM
NEW YORK DIVISION

EXAMINATION NOTES

		Properties 21 - Evidence Source Path - Evidence Type - Disk - Drive Geometry - Cylinders - Tracks per Cylinder - Sectors per Track - Bytes per Sector - Sector Count - Physical Drive Information - Drive Model - Drive Serial Number - Drive Interface Type - Removable drive Physical Evidentiary Item (Source) Information: [Device Info] Source Type: Physical [Drive Geometry] Cylinders: 31 Tracks per Cylinder: 255 Sectors per Track: 63 Bytes per Sector: 512 Sector Count: 503,808 [Physical Drive Information] Drive Model: Generic- USB3.0 CRW-CF/MD USB Device Drive Serial Number: 2012062914345300 Drive Interface Type: USB Removable drive: True Source data size: 246 MB Sector count: 503808 [Computed Hashes] MD5 checksum: a489bb0b99f598ba60e1ae3a1e591b38 Image Verification Results: Verification started: Fri Sep 14 10:08:57 2018 Verification finished: Fri Sep 14 10:09:05 2018 MD5 checksum: a489bb0b99f598ba60e1ae3a1e591b38 : verified A Directory/File Listing was generated when evidence was imaged using FTK® Imager 4.2.0.13. Listing file is co-located along with the respective image files within the CASE VOLUME. Listing contains filename, full path, modified date/time stamp, created (change) date/time stamp, and accessed date/time stamp.
--	--	---



FEDERAL BUREAU OF INVESTIGATION
COMPUTER ANALYSIS RESPONSE TEAM
NEW YORK DIVISION

EXAMINATION NOTES

NYC023728 _1B32 NYC023728 _1B32.E01	09/14/18	VD	Preserve Evidence: Image NYC023728_1B32 was imaged with Forensic Exam Station Forensic Exam Station F2673128 using a Tableau Forensic USB Bridge, model: T8-R2, s/n: 020870B7, and AccessData® FTK® Imager 4.2.0.13, to the CASE VOLUME. AccessData FTK Imager 4.2.0.13 File View Mode Help Evidence Tree - W:\PHYSICALDRIVE7 - Partition 1 [953198MB] - My Book [HFSX] (unallocated space) 000168585 034784603 - My Book - HFS+ Private Data .fsvented .HFS+ Private Directory Data .Spotlight-V100 .Trashes - Backups.backupdb - Unpartitioned Space [basic disk] (unallocated space) Properties A↓ ☒ Evidence Source Path Evidence Type ☒ Disk ☒ Drive Geometry - Cylinders - Tracks per Cylinder - Sectors per Track - Bytes per Sector - Sector Count ☒ Physical Drive Information - Drive Model - Drive Serial Number - Drive Interface Type - Removable drive Physical Evidentiary Item (Source) Information:
--	----------	----	---

THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION.
DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.

Affix Label Here



FEDERAL BUREAU OF INVESTIGATION
COMPUTER ANALYSIS RESPONSE TEAM
NEW YORK DIVISION

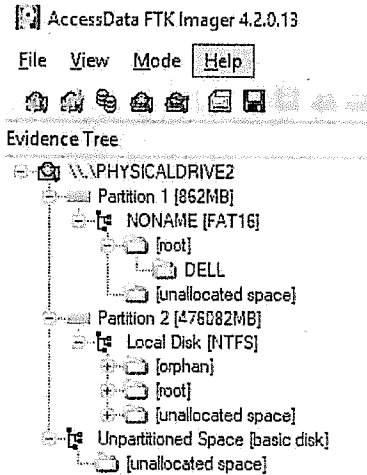
EXAMINATION NOTES

			[Device Info] Source Type: Physical [Drive Geometry] Cylinders: 121,515 Tracks per Cylinder: 255 Sectors per Track: 63 Bytes per Sector: 512 Sector Count: 1,952,151,552 [Physical Drive Information] Drive Model: WD My Bo ok 1111 USB Device Drive Serial Number: 57434156353438373337 Drive Interface Type: USB Removable drive: False Source data size: 953199 MB Sector count: 1952151552 [Computed Hashes] MD5 checksum: 6ce5db0fcdc512ac9dc635dd17068a12 Image Verification Results: Verification started: Sat Sep 15 00:31:12 2018 Verification finished: Sat Sep 15 03:17:38 2018 MD5 checksum: 6ce5db0fcdc512ac9dc635dd17068a12 : verified A Directory/File Listing was generated when evidence was imaged using FTK® Imager 4.2.0.13. Listing file is co-located along with the respective image files. Listing contains filename, full path, modified date/time stamp, created (change) date/time stamp, and accessed date/time stamp. Directory listing created and saved as NYC023728_1B32.E01.csv within CASE VOLUME.
NYC023732_1B50	09/14/18	VD JC	Preserve Evidence: Extraction Powered on device 09/14/2018 at approximately 12:00noon. No pin associated with device. Settings identifies the device as "Keith's iPod." Changed Backlight Timer from 10 seconds to Always On. Using Forensic Exam Station F2552510: UFED 4PC 7.8.0.942 Did not recognize device. UFED Physical Analyzer 7.1.0.106 Did not recognize device. Under the guidance of ITS/SFE John Chan, attempted iPEX 2.1.8 and iPhAT 1.13.0. Did not recognize device.



FEDERAL BUREAU OF INVESTIGATION
COMPUTER ANALYSIS RESPONSE TEAM
NEW YORK DIVISION

EXAMINATION NOTES

NYC023732 _1B50	09/21/18	BB	Preserve Evidence: Extraction Using Forensic Exam Station F5405659 XRY 7.8 Physical- Successful Called CA to notify that XRY was working on device.
NYC023726 _1B28 NYC023726 _1B28.E01	09/17/18	VD	Preserve Evidence: Image NYC023726_1B28 was imaged with Forensic Exam Station F2630035 using a Tableau Forensic USB Bridge, model: T8-R2, s/n: 0208710F, and AccessData® FTK® Imager 4.2.0.13 , to the CASE VOLUME.  The screenshot shows the AccessData FTK Imager 4.2.0.13 interface. The 'Evidence Tree' is expanded, showing the following structure: \\PHYSICALDRIVE2 - Partition 1 [862MB] - NONAME [FAT16] [root] - DELL [unallocated space] - Partition 2 [476082MB] - Local Disk [NTFS] [orphan] [root] [unallocated space] - Unpartitioned Space [basic disk] [unallocated space]



FEDERAL BUREAU OF INVESTIGATION
COMPUTER ANALYSIS RESPONSE TEAM
NEW YORK DIVISION

EXAMINATION NOTES

Properties



Evidence Source Path

Evidence Type



Disk



Drive Geometry

Cylinders

Tracks per Cylinder

Sectors per Track

Bytes per Sector

Sector Count



Physical Drive Information

Drive Model

Drive Serial Number

Drive Interface Type

Removable drive

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 60,802

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 976,794,336

[Physical Drive Information]

Drive Model: LaCie Bi gDisk USB Device

Drive Serial Number: AAC3CC45261F

Drive Interface Type: USB

Removable drive: False

Source data size: 476950 MB

Sector count: 976794336

[Computed Hashes]

MD5 checksum: c3831223db43f2042a69f970bacb0b0a

Image Verification Results:

Verification started: Mon Sep 17 18:40:58 2018

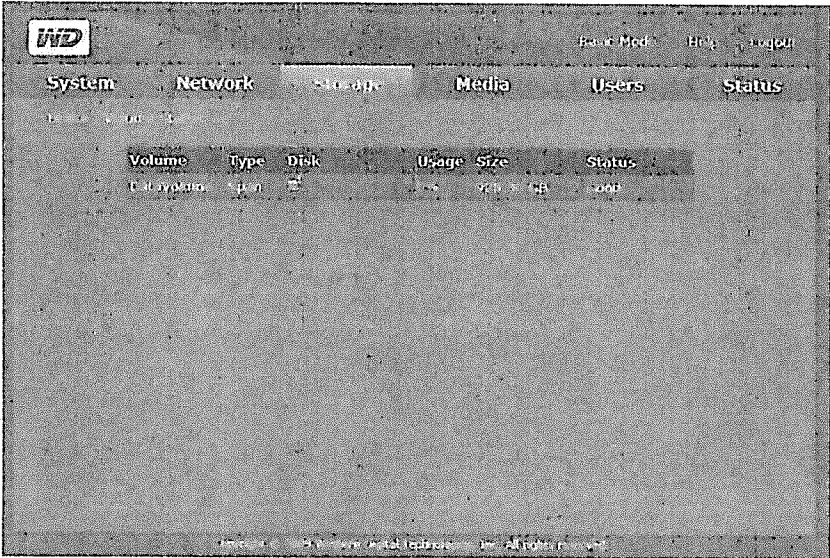
Verification finished: Mon Sep 17 19:29:44 2018

MD5 checksum: c3831223db43f2042a69f970bacb0b0a : verified

A Directory/File Listing was generated when evidence was imaged using **FTK® Imager 4.2.0.13**. Listing file is co-located along with the respective image files. Listing contains filename, full path, modified date/time stamp, created (change) date/time stamp, and accessed date/time stamp.

Directory listing created and saved as NYC023726_1B28.E01.csv within

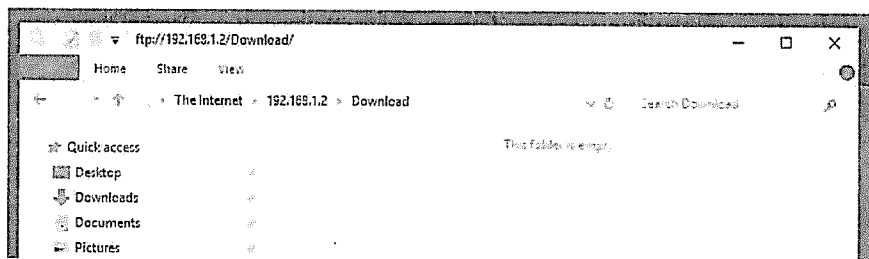
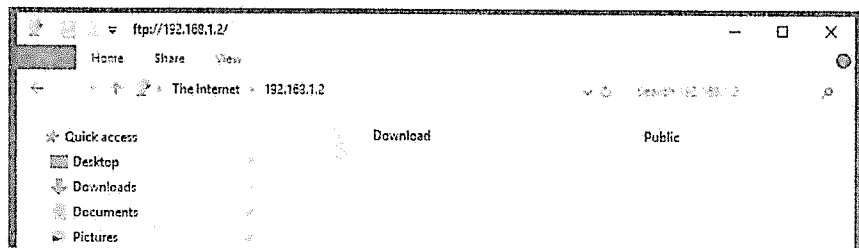
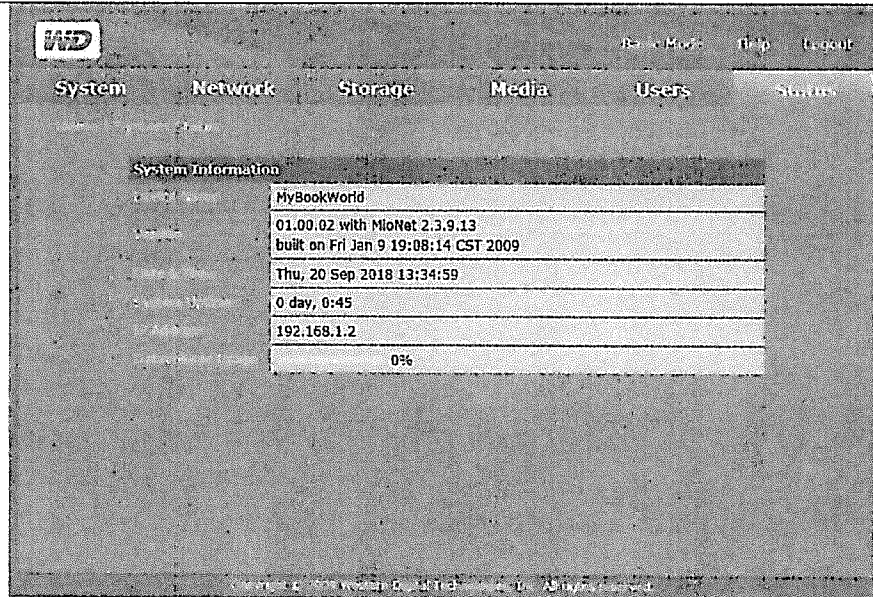


			CASE VOLUME.
NYC023724 _1B26	09/20/18	VD	Preserve Evidence: Image NYC023724_1B26 is a My Book World Edition network-attached storage system. Connected NYC023724_1B26 to internal network. - Installed and launched WD Link software. - Used default password to connect to the unit. - Connected to unit via web browser and continued through configuration settings to assign permanent password for administrative access (admin). - Noticed item was configured via DHCP (Dynamic Host Configuration Protocol). - Assigned static IP address of 192.168.1.2. - Enabled FTP (File Transfer Protocol) connection through anonymous authentication. - Removed device from internal network and connected the unit to a standalone network switch. The following images capture the findings: 



FEDERAL BUREAU OF INVESTIGATION
COMPUTER ANALYSIS RESPONSE TEAM
NEW YORK DIVISION

EXAMINATION NOTES



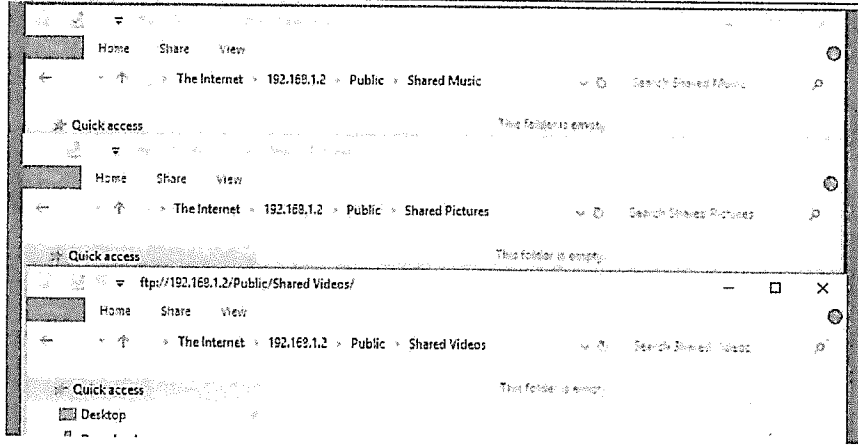
THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION.
DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.

Affix Label Here



FEDERAL BUREAU OF INVESTIGATION
COMPUTER ANALYSIS RESPONSE TEAM
NEW YORK DIVISION

EXAMINATION NOTES

			 System Log was screen grabbed and saved as WorldBook System Log.txt. See attached addendum for further information.
NYC023724 _1B26	09/20/18	VD	Administrative Note: Notified CA that examination of NYC023724_1B26 to date showed no data stored on the device; no further processing conducted at this time.
NYC023729 _1B26	09/20/18	VD	Preserve Evidence: Image NYC023729_1B26 was connected to Forensic Exam Station F2673128 using a Tableau Forensic USB Bridge, model: T8-R2, s/n: 020870B7. Device would not turn on. Did not recognize device. Set aside device to charge.
NYC023729 _1B26	09/21/18	VD	Device would not turn on. NYC023729_1B26 was connected to Forensic Exam Station F2673128 using a Tableau Forensic USB Bridge, model: T8-R2, s/n: 020870B7. Did not recognize device. Connected device directly to Forensic Exam Station F2673128. Did not recognize device.
	09/21/18	VD	Administrative Note: Notified CA that the device was not recognized by forensic machines. No further processing at this time.
NYC023725 _1B27- 1.E01 Staging Drive 1	09/14/18	VD	Preserve Evidence: Discovery Produce verified copies of images for discovery saved to Seagate Expansion Portable Drive, 1TB, model: SRD0NF1, p/n: 1TEAP5-500, s/n: NA8ZLFSQ, which was provided to CART by SA Lever. Using Forensic Exam Station F2552510 and Tableau eSATA Forensic Bridge



FEDERAL BUREAU OF INVESTIGATION
COMPUTER ANALYSIS RESPONSE TEAM
NEW YORK DIVISION

EXAMINATION NOTES

Seagate HD			write blocker, model: T35es-R2, s/n: 3135D086, copy images of NYC023725_1B27-1 from Staging Drive 1 to provided Seagate HD. Copy was verified using FTK® Imager 4.2.0.13. Drive/Image Verify Results Name NYC023725_1B27-1 Sector count 1000000 MD5 Hash Computed hash 21b1c1e1e1e1e1e1e1e1e1e1e1e1e1e1 Stored verification hash 21b1c1e1e1e1e1e1e1e1e1e1e1e1e1e1 Verify result Match SHA1 Hash Computed hash 21b1c1e1e1e1e1e1e1e1e1e1e1e1e1e1 Bad Blocks List Bad block(s) in image
NYC023723_1B23.E01 NYC023727_1B31.E01 NYC023731_1B43.E01 Staging Drive 1 Staging Drive 2 Seagate HD	09/17/18	VD	Preserve Evidence: Discovery Using Forensic Exam Station F2552510 and Tableau eSATA Forensic Bridge write blocker, model: T35es-R2, s/n: 3135D086, copy images of NYC023723_1B23 from Staging Drive 1 to provided Seagate HD. Drive/Image Verify Results Name NYC023723_1B23 Sector count 1000000 MD5 Hash Computed hash 21b1c1e1e1e1e1e1e1e1e1e1e1e1e1e1 Stored verification hash 21b1c1e1e1e1e1e1e1e1e1e1e1e1e1e1 Verify result Match SHA1 Hash Computed hash 21b1c1e1e1e1e1e1e1e1e1e1e1e1e1e1 Bad Blocks List Bad block(s) in image Using Forensic Exam Station F2552510 and Tableau eSATA Forensic Bridge write blocker, model: T35es-R2, s/n: 3135D086, copy images of NYC23727_1B31 from Staging Drive 2 to provided Seagate HD. Copy was verified using FTK® Imager 4.2.0.13.



FEDERAL BUREAU OF INVESTIGATION
COMPUTER ANALYSIS RESPONSE TEAM
NEW YORK DIVISION

EXAMINATION NOTES

			Drive/Image Verify Results Name Sector count MD5 Hash Computed hash Stored verification hash Verify result SHA1 Hash Computed hash Stored verification hash Verify result Bad Blocks List Bad block(s) in image Using Forensic Exam Station F2552510, copy images of NYC023731_1B43 from the CASE VOLUME to provided Seagate HD. Copy was verified using FTK® Imager 4.2.0.13. Drive/Image Verify Results Name Sector count MD5 Hash Computed hash Stored verification hash Report Hash Verify result SHA1 Hash Computed hash Stored verification hash Report Hash Verify result Bad Blocks List Bad block(s) in image
Seagate HD	09/17/18	VD	Administrative Note: Seagate HD provided to SA Lever. FD-597 completed and signed by SA Lever to accept.



FEDERAL BUREAU OF INVESTIGATION
COMPUTER ANALYSIS RESPONSE TEAM
NEW YORK DIVISION

EXAMINATION NOTES

NYC023730 _1B41.E01 Addonics HD	09/17/18	VD	Preserve Evidence: Discovery Produce verified copies of images for discovery saved to Addonics Diamond Cipher II ExDrive, 3TB, model: DCED6GEU3, s/n: 9797100411, which was provided to CART by SA Lever. Using Forensic Exam Station F2673128, copy images of NYC023730_1B41 from the CASE VOLUME to provided Addonics HD. Copy was verified using FTK® Imager 4.2.0.13. Original Computed Hashes: MD5 checksum: 07df4939e1107220aa5dd1a39fb04767 Image Verification Results: Verification started: Mon Sep 17 16:39:58 2018 Verification finished: Mon Sep 17 18:43:47 2018 MD5 checksum: 07df4939e1107220aa5dd1a39fb04767 : verified
NYC023728 _1B32.E01 NYC023726 _1B28.E01 Addonics HD	09/18/18	VD	Preserve Evidence: Discovery Produce verified copies of images for discovery saved to Addonics Diamond Cipher II ExDrive, 3TB, model: DCED6GEU3, s/n: 9797100411, which was provided to CART by SA Lever. Using Forensic Exam Station F2673128, copy images of NYC023728_1B32 from the CASE VOLUME to provided Addonics HD. Copy was verified using FTK® Imager 4.2.0.13. Original Computed Hashes MD5 checksum: 6ce5db0fcdc512ac9dc635dd17068a12 Image Verification Results: Verification started: Tue Sep 18 10:07:13 2018 Verification finished: Tue Sep 18 11:55:47 2018 MD5 checksum: 6ce5db0fcdc512ac9dc635dd17068a12 : verified Using Forensic Exam Station F2673128, copy images of NYC023726_1B28 from the CASE VOLUME to provided Addonics HD. Copy was verified using FTK® Imager 4.2.0.13. Original Computed Hashes: MD5 checksum: c3831223db43f2042a69f970bacb0b0a Image Verification Results: Verification started: Tue Sep 18 12:47:22 2018 Verification finished: Tue Sep 18 13:33:48 2018 MD5 checksum: c3831223db43f2042a69f970bacb0b0a : verified
Addonics HD	09/19/18	VD	Administrative Note: Addonics HD provided to SA Michael Lever. FD-597 completed and signed by SA Lever to accept. SA Lever and AUSA stated that the kindle, NYC023722_1B19, did not need



FEDERAL BUREAU OF INVESTIGATION
COMPUTER ANALYSIS RESPONSE TEAM
NEW YORK DIVISION

EXAMINATION NOTES

			to be processed since the device powered on to the "thank you for purchasing" screen and seemed to only have the dictionary loaded.
NYC023732_1B50 Addonics HD 2	09/26/18	VD	Preserve Evidence: Discovery Produce verified copies of images for discovery saved to Addonics Diamond Cipher II ExDrive, 3TB, model: DCED6GEU3, s/n: 9797100412, which was provided to CART by SA Lever. Using Forensic Exam Station F2630035, copy images and reports of NYC023732_1B50 from the CASE VOLUME to provided Addonics HD using VeriCopy v.3.18 .
NYC023721_1B16.E01 Addonics HD 2	09/27/18	VD	Using Forensic Exam Station F2630035, copy images of NYC023721_1B16 from the CASE VOLUME to provided Addonics HD. Copy was verified using FTK® Imager 4.2.0.13 . Original Computed Hashes: MD5 checksum: 7aa8f3297f288252ed69ffd983725b5e Image Verification Results: Verification started: Thu Sep 27 11:12:28 2018 Verification finished: Thu Sep 27 12:58:24 2018 MD5 checksum: 7aa8f3297f288252ed69ffd983725b5e : verified
Addonics HD 2	09/28/18	VD	Administrative Note: Addonics HD provided to SA Michael Lever. FD-597 completed and signed by SA Lever to accept.
NYC023721_1B16.E01 NYC023723_1B23.E01 NYC023725_1B27-1.E01 NYC023726_1B28.E01 NYC023727_1B31.E01 NYC023728_1B32.E01 NYC023730_1B41.E01 NYC023731_1B43.E01	09/24/18	VD	Processing: Images of NYC023721_1B16, NYC023723_1B23, NYC023725_1B27-1, NYC023726_1B28, NYC023727_1B31, NYC023728_1B32, NYC023730_1B41, and NYC023731_1B43 were added to AD Lab v6.3.1.26 utilizing the Field Mode Processing Profile, default settings, on Forensic Exam Station F2673128. AD Lab will be used for examination in this case unless otherwise noted. Time zone setting: Eastern Time with Daylight Saving (US – New York) Additional Analysis: First: - Expand Compound Files (include deleted files) - Flag Bad Extensions - File Signature Analysis
	09/25/18	VD	AD Lab Additional Analysis: Second:



FEDERAL BUREAU OF INVESTIGATION
COMPUTER ANALYSIS RESPONSE TEAM
NEW YORK DIVISION

EXAMINATION NOTES

			▪ Data Carve (all types selected) ▪ Meta Carve Errors encountered, failed.
	09/26/18	VD	AD Lab Additional Analysis: Third: ▪ Data Carve (all types selected)
	09/27/18	VD	AD Lab Additional Analysis: Fourth: ▪ Meta Carve Fifth: ▪ Create Thumbnails for Graphics
	10/01/18	VD	Administrative Note: Spoke to SA Delise Jeffrey in person. Do not need thumbnails for videos.
	10/01/18	VD	AD Lab Additional Analysis: Sixth: ▪ MD5 Hash ▪ Flag Duplicate Files Seventh: ▪ Search Text Index (TR1) ▪ Entropy Test (do not index compressed or encrypted items) ▪ Include extended information ▪ Merge case index when finished
	10/03/18	VD	Administrative Note: E-mailed SA Lever and SA Jeffrey that the images and reports were available in CAIR.
	09/26/18	VD	Evidence Disposition: All evidence items were returned to SA Lever.
NYF00739 NYF01088	10/09/18 10/10/18	VD	Preserve Evidence: Master Copy Images were archived from the CASE VOLUME to two (2) TDK Tapes, both Model: Ultrium LTO 5, 1.5TB, previously affixed barcode and designated as NYF00739 and NYF01088, using Back This Up 3.1.17.5/Arcserve Backup. Logs retained.
NYF00739 NYF01088	10/12/18	VD	Evidence Disposition: CART created Master Copy was relinquished to Evidence Control. NYF00739 and NYF01088 were assigned 1B135 in captioned case file.
	11/16/18	VD	Administrative Note: SA Lever requested, via e-mail, a copy of the Directory File Listing for each individual device processed.



FEDERAL BUREAU OF INVESTIGATION
COMPUTER ANALYSIS RESPONSE TEAM
NEW YORK DIVISION

EXAMINATION NOTES

NYC023723 _1B23.csv	12/17/18	VD	Processing: Using Forensic Exam Station F2673128: FTK Imager, build 4.2.0.13 Process Directory File Listings for the following imaged evidence items: NYC023723_1B23 and NYC023725_1B27-1.csv
image.E01.csv	12/18/18	VD	Process Directory File Listings for the following imaged evidence items: NYC023727_1B31 (image.E01.csv)
	12/28/18	VD	Administrative Note: E-mailed SA Lever indicating that directory file listings were available for all evidence items with the exception of 1B50 and to inform the examiner if the directory file listing was necessary for 1B50.
	01/22/19	VD	Administrative Note: Met and spoke to SA lever. He no longer needed a copy of the Directory File Listings from the examiner.
	02/22/19	VD	Administrative Note: SA Lever e-mailed examiner to do an internet evidence review of AOL e-mail found on 1B28.
	02/25/19	VD	Administrative Note: SA Lever requested access via e-mail for SA Leslie Adamczyk to review evidence item 1B16. In a separate e-mail, SA Lever provided a copy of a new Search and Seizure Warrant pertaining to the search of evidence item 1B16 for evidence of child pornography.
NYC023726 _1B28	02/26/19	VD	Processing: Using Internet Evidence Finder (IEF) v6.14.0.10770 , processed 1B28 for internet remnants SA Lever requested.
NYC023721 _1B16	02/26/19	VD	Administrative Note: SA Leslie Adamczyk granted access to entire case. E-mailed case agents of the same and indicated the scope of the new warrant only allows the search for child pornography on 1B16.
NYC023726 _1B28 NYC023744	03/05/19	VD	Processing: Created DVD-R of IEF report generated for item 1B28, affixed barcode and designated as NYC023744. Notified SA Jeffrey, in person, that the report was completed and ready for pick up.
	03/06/19	BB	Administrative Note:

THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION.
DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.

Affix Label Here



FEDERAL BUREAU OF INVESTIGATION
COMPUTER ANALYSIS RESPONSE TEAM
NEW YORK DIVISION

EXAMINATION NOTES

			ITS/SFE Booth provided hand written notes on research of EXIF data pertaining to the CP images identified on 1B16.
1B16	03/13/19	BSB	Administrative Note: Provided access for separate review of 1B16 to defense council. Computer installed and 1B16 ran in AD Lab for full processing. SA Lever advised via Bureau cell phone that data was available for review in CART Review room on the 22 nd floor of 26 Federal Plaza.
NYC023744	03/15/19	VD	Administrative Note: Provided NYC023744 to SA Lever. Completed FD-597.
	03/15/19	VD	Administrative Note: SA Lever and AUSA, in person, requested a copy of evidence item 1B16 without CP for discovery.
1B16 My Passport	03/18/19	VD	Processing: SA Lever provided a My Passport Western Digital hard drive, 2TB, model: WDBS4B0020BBK-WESN, s/n: WXP1A38H88CX, for the copy of 1B16 sans possible CP. Logical export of 1B16 without files identified by case agent as contraband saved to the My Passport drive.
My Passport	03/20/19	VD	Administrative Note: Provided My Passport drive to SA Jeffrey. Completed FD-597. Agents were advised to review the drive for contraband prior to distribution.
	04/04/19	VD	Administrative Note: SA Lever and SA Jeffrey indicated other possible CP was identified on 1B16. Agents are retrieving the previously distributed drive for discovery and requested a new copy be made without CP once they review the newly identified images. Agents provided handwritten list of files they identified as contraband.
My Passport 2	04/04/19	VD	Processing: SA Lever and SA Jeffrey provided a My Passport Western Digital hard drive, 2TB, model: WDBS4B0020BBK-WESN, s/n: WX81A38D01U0, for the copy of 1B16 without possible CP. Logical export of 1B16 without files identified by case agents as contraband saved to the My Passport drive.
My Passport 2	04/05/19	VD	Administrative Note: Provided My Passport drive to SA Lever. Completed FD-597. Agents were advised to review the drive for contraband prior to any distribution.
	04/10/19	BSB	Processing: AD Lab not reporting EXIF data for item 1B16 as separate reportable html

THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION.
DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.

Affix Label Here



FEDERAL BUREAU OF INVESTIGATION
COMPUTER ANALYSIS RESPONSE TEAM
NEW YORK DIVISION

EXAMINATION NOTES

			files. Re-ran "Expand Compound Files" in AD Lab on item 1B16 for only EXIF data expansion.
NYC023288 NYC023289	04/11/19	BSB	Processing: Created AD Lab Report containing bookmarks of the "Studies Folders" identified from item 1B16 as indicated by SA Lever. Report burned to Adams Evidence Grade DVD-R and affixed label and noted herein as NYC023288. Created AD Lab Report containing bookmarks of the "Suspected CP Images" identified from item 1B16 as indicated by SA Lever. Report burned to Adams Evidence Grade DVD-R and affixed label and noted herein as NYC023289. Items signed over and entered into NY Evidence Control Unit (ECU). Generated AD1 image of two reports with FTK Imager 4.2.0.3 as 041119_Reports.ad1 directly to the CASE VOLUME / DE NYCART. Staging drive was forensically wiped. Case agent requested a copy of bookmarked CP images to be redacted for facial identification. A list of requested image names were provided in an e-mail by SA Delise Jeffery. Using Microsoft Photos, a crop of each image was done to show only facial features. These images were then saved to the CASE FOLDER in addition to one CD-R that was burned and marked as a "Working Copy". Disc was provided to SA Lever at 2:30PM.
NYC023290	04/23/19	BSB	Processing: Spoke to Agent Lever about received email from AUSA with a request from defense attorney for a copy of 1B16 image files in a redacted format. Request verbally denied to agent Lever as against DEPG and CART policy. Advised Agent Lever that images have been made available for full review by the defense team in the CART Review room located on the 22nd floor of 26 Federal Plaza. CART NY has made the review available to the defense team since it had been placed for review on As per agent Lever request, created AD Lab Report containing bookmarks of the "Suspected CP" identified from item 1B16 sans the graphic images. Report burned to Adams Evidence Grade CD-R and affixed label and noted herein as NYC023290. Agent working copy generated on separate white label CD-R. Items signed over and entered into NY Evidence Control Unit (ECU).
	04/30/19	VD	Administrative Note: SA Lever requested printed copies of 22 images which he identified as possible CP for judge and jury purposes. Examiner printed the images and



FEDERAL BUREAU OF INVESTIGATION
COMPUTER ANALYSIS RESPONSE TEAM
NEW YORK DIVISION

EXAMINATION NOTES

			completed a Chain of Custody. SA Lever put the printed photos into evidence, 1Bxxxx.
	06/07/19	BSB	Administrative Note: Request was made by SA Lever of item 1B15 to be processed in lieu of ITS/SFE Steven Flatleys availability as he would be overseas during trial. This exam would be utilized in trial. SSA Trenton Schmatz concurred and authorized to process the item.
1B15	06/10/19	BSB	Receipt of Evidence: Evidence received directly from Case Agent. E6261241 1B15 One (1) Cannon Ultrasonic Digital Camera, model:DS126061, s/n: 1420908348. In black Cannon camera bag stored in brown cardboard evidence box. Containing: One (1) Lexar Professional 2GB WA compact flash card, model:2389, s/n:39132GBCI39052D97, in separate cellophane baggie affixed barcode NYC024299 . Initialed by ITS/SFE Stephen Flatley on 02/22/2019
NYC024299	06/11/19	BSB	Administrative Note: Forensic Exam Station F5405659 (S/N: 3YSZDB2), identified as BBOOTH-01 , successfully completed the Power On Self Test (POST) process and is being used to process evidence images. F5405659 is a Dell T7910 running Windows 10 Enterprise Edition 64-bit Operating System with sixty-four (64) GB RAM and two (2) Intel Xeon X2650 processors at 2.30GHz. F5405659 is running AccessData Lab 6.3.1.26 configured in a multi-node DPE cluster. AccessData Lab Lab 6.3.1.26 will be utilized in processing for this examination of NYC024299, unless otherwise noted.
NYC024299	06/11/19	BSB	Preserve Evidence: NYC242299 NYC024299 was imaged using a Tableau Forensic Card Reader (s/n: CR000004832) and a AccessData® FTK® Imager 4.2.0.13 , to the CASE VOLUME. Drive Geometry as reported by FTK Imager: [Drive Geometry] Cylinders: 249 Tracks per Cylinder: 255 Sectors per Track: 63 Bytes per Sector: 512 Sector Count: 4,008,816

[illegible]



FEDERAL BUREAU OF INVESTIGATION
COMPUTER ANALYSIS RESPONSE TEAM
NEW YORK DIVISION

EXAMINATION NOTES

Examiner:

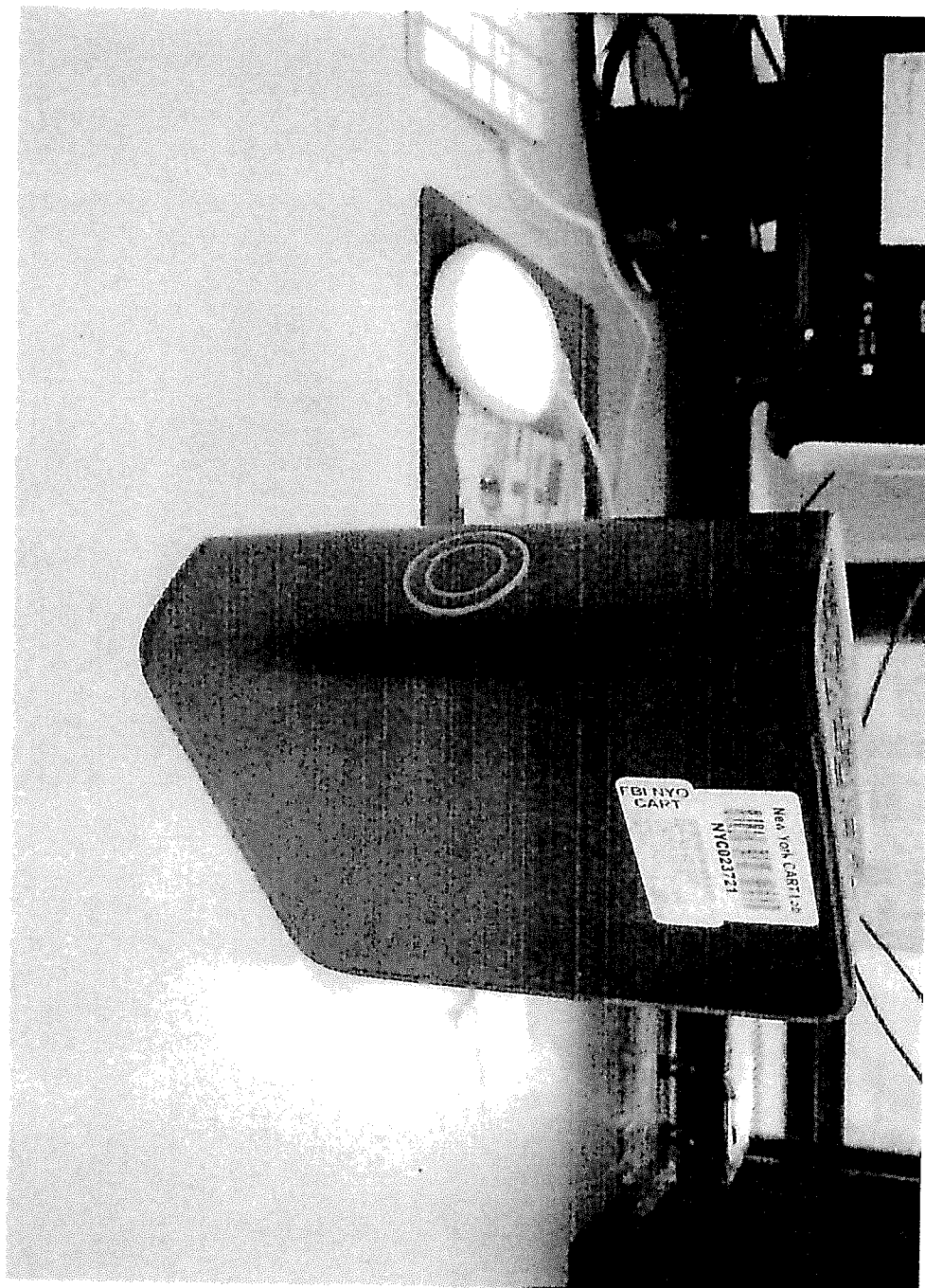
SA/FET Virginia Donnelly
ITS/SFE Brian Booth

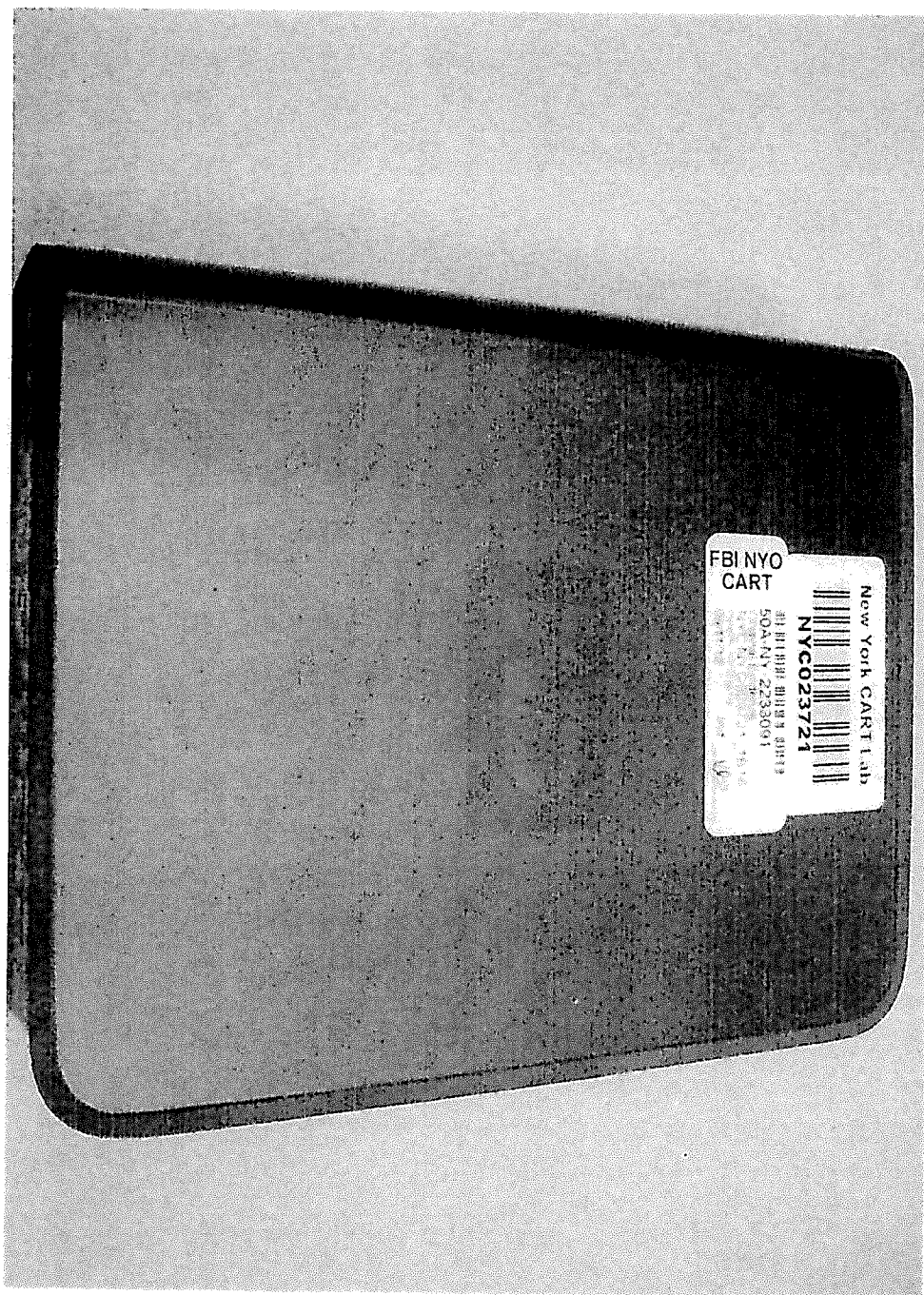
Date of Report:

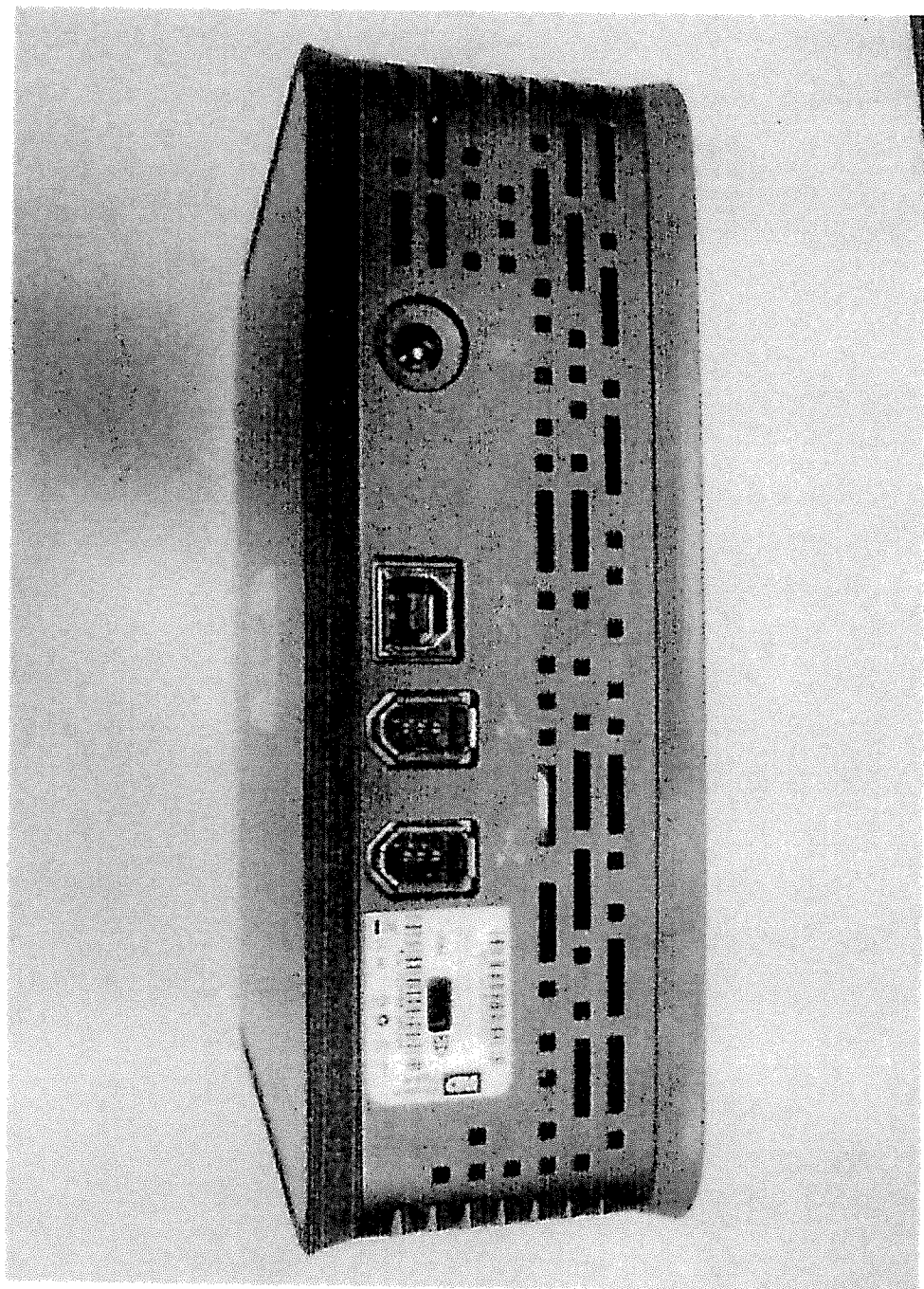
Month XX, 20XX

THIS DOCUMENT AND ITS CONTENTS ARE THE PROPERTY OF THE FEDERAL BUREAU OF INVESTIGATION.
DISTRIBUTION OF THIS DOCUMENT OR ITS CONTENTS IS STRICTLY PROHIBITED.

Affix Label Here







Western Digital
WD
1508A
MDL WD5000P032
S/N WCAS81365334
CE FC
X
1508A
WD
Digital
Western



