OpenText™ Tableau™ Forensic TD4 Duplicator

# User Guide

This guide presents a wide range of technical information and procedures for using the OpenText Tableau Forensic TD4 Duplicator.

ISTD240300-UGD-EN-1

**OpenText™ Tableau™ Forensic TD4 Duplicator**
**User Guide**
ISTD240300-UGD-EN-1
Rev.: 2024-Aug-21

**This documentation has been created for OpenText™ Tableau™ Forensic TD4 Duplicator 24.3.**
It is also valid for subsequent software releases unless OpenText has made newer documentation available with the product, on an OpenText website, or by any other means.

**Open Text Corporation**

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Tel: +1-519-888-7111
Toll Free Canada/USA: 1-800-499-6544 International: +800-4996-5440
Fax: +1-519-888-0677
Support: https://support.opentext.com
For more information, visit https://www.opentext.com

Patents may cover this product, see https://www.opentext.com/patents.

**Disclaimer**

No Warranties and Limitation of Liability

Every effort has been made to ensure the accuracy of the features and techniques presented in this publication. However, Open Text Corporation and its affiliates accept no responsibility and offer no warranty whether expressed or implied, for the accuracy of this publication.

# Table of Contents

Chapter 1

# Preface

This guide presents a wide range of technical information and procedures for using the OpenText Tableau Forensic TD4 Duplicator. It is divided into the following chapters:

- **Overview:** Provides general information about TD4, as well as unpacking, starting up, and navigating TD4 menus and reading the LEDs.
- **Configuring OpenText Tableau Forensic TD4 Duplicator:** Provides system overview information about TD4, as well as procedures for configuring and connecting it.
- **Using OpenText Tableau Forensic TD4 Duplicator:** Provides detailed information and procedures for TD4 operation.
- **Adapters:** Describes the adapters that extend the drive acquisition options and destination drive capabilities of TD4.
- **Specifications and troubleshooting:** Provides TD4 specifications and a brief list of potential problems and solutions. For more complete and current troubleshooting information as well as answers to frequently asked questions (FAQ), visit OpenText My Support (https://support.opentext.com).

## 1.1 Drive capacity and transfer rate measurement conventions

The computer industry generally adheres to two different conventions for definitions of the terms megabyte (MB) and gigabyte (GB). For computer RAM, 1 MB is defined as $2^{20}$ = 1,048,576 bytes and 1 GB is defined as $2^{30}$ = 1,073,741,824 bytes. For drive storage, 1 MB is defined as $10^{6}$ = 1,000,000 bytes and 1 GB is defined as $10^{9}$ = 1,000,000,000 bytes. These two conventions are known as powers of two and powers of ten respectively. Microsoft deviates from the hard drive capacity measurement convention and uses the powers of two convention for its operating systems.

OpenText devices report drive capacities and transfer rates according to the industry standard powers of ten convention. In TD4 screens, reports, and documentation, a 4 GB hard drive stores up to 4,000,000,000 bytes; a hard drive with a 150 MB/sec transfer rate transfers 150,000,000 bytes per second.

Chapter 2

# Overview

OpenText Tableau Forensic TD4 Duplicator is a powerful and intuitive forensic device that offers valuable, high-performance imaging capabilities in a small, portable package. The touch screen user interface is easy to use and provides a familiar user experience similar to modern tablets and smartphones. TD4 is custom built for forensics and provides many standard and advanced features that serve the specialized needs of digital forensics practitioners, including:

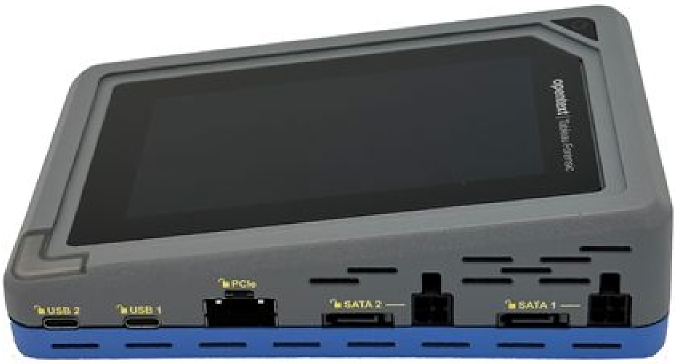
- Acquisition of PCIe, USB, SATA, SAS, FireWire, and IDE drives.

  **Note:** PCIe, IDE, and FireWire adapters (sold separately) are required to image these drive types.

- Output to PCIe, USB, and SATA drives.
- The ability to target file-based evidence with logical imaging functionality and industry standard file outputs (lx01 and metadata csv files).
- The ability to duplicate a source drive to up to five destination drives.
- The ability to prevent damage to disk drives by spinning them down when they are ejected from TD4 prior to physical removal.
- The ability to power down TD4 after the last active job is complete.
- The ability to pause and resume Duplication jobs, including surprise power loss situations. Specific types of failed jobs can also be resumed.
- The ability to lock specific functions and settings with an administrator PIN to enforce standard settings and procedures for your forensic acquisition jobs.
- Superior data transfer rates, even while performing calculations of MD5, SHA-1, and SHA-256 hash values.
- The ability to view extensive drive detail, including partition and filesystem information.
- Browsing drive filesystems.
- Extensive filesystem support - APFS, ExFAT, NTFS, EXT4, FAT(12/16/32), and HFS+.
- Support for source drives with multiple LUNs and multiple NVMe namespaces.
- The ability to detect a source drive with unattached NVMe namespaces and allow their attachment to enable browsing/forensic imaging.
- Whole disk, open standard, destination drive encryption using XTS-AES.
- The ability to detect and inform of the presence of enabled Opal encryption, BitLocker, and APFS encryption.

- The ability to unlock Opal encryption to enable browsing/forensic imaging.
- The ability to mount digital media in Apple devices that support Target Disk Mode.
- Comprehensive destination and accessory drive wiping capabilities, including NIST 800-88 compliant wipes.
- HPA, DCO, and AMA support for the detection and handling of hidden/ protected data areas on source drives. This includes standalone HPA/DCO/AMA disablement, DCO/AMA "shelving," and trim support for the creation of a destination DCO or AMA.
- Localized user interface and virtual keyboard support for the following languages: German, English, Spanish (International), French, Korean, Portuguese (Brazilian), Russian, Turkish, and Chinese (Simplified)
- Detailed forensic logs in HTML format for case documentation.
- The ability to filter the forensic log list to only show logs of interest based on specific case and/or drive information. The filtered logs can also be exported or deleted.
- Always free firmware update support.
- Clearly labeled and color-coded source (write blocked) and destination (read/ write) ports.

The left source (write blocked) side of TD4.

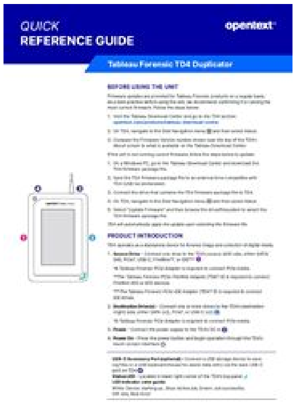


The right destination (read/write) side of TD4.

## 2.1 OpenText Tableau Forensic TD4 Duplicator kit contents

OpenText Tableau Forensic TD4 Duplicator ships in a boxed kit with custom foam that includes the following items:

| Item | Model # | Description |
|---|---|---|
| | OpenText Tableau Forensic TD4 Duplicator | OpenText Tableau Forensic TD4 Duplicator |
| | TP6 | Provides power to TD4. Uses a universal 3-prong style AC line cord and is compatible with 100-240V AC line voltages worldwide. |
| | TC4-8-R4 | Unified SATA/SAS signal and power to 8in. SATA/SAS signal and 8in. power cable (qty 3) |
| | TC-PCIE-8 | 8in. PCIe adapter cable. Must be used with a Tableau PCIe adapter (qty 1) |
| | TCA-USB3-AC | USB Type A female to Type C male adapter cable (qty 2) |

| Item | Model # | Description |
|---|---|---|
| | TPKG-VCT-5 | 5-piece Velcro cable tie kit |
| | TPKG-CLOTH | Microfiber screen cleaning cloth |
| <br>QUICK<br>REFERENCE GUIDE<br>opentext<br>Tableau Forensic TD4 Duplicator<br>BEFORE USING THE UNIT<br>PRODUCT INTRODUCTION | | Quick Reference Guide |

Do not discard the TD4 foam packaging, as it is designed to fit several industry-standard hard sided carrying cases (for example, the Pelican 1500). If you received the TD4 kit in the cardboard box shipped by OpenText, you can reuse the stacking foam inserts in your own hard-sided case.

## 2.2 Navigating TD4

Use the TD4 touchscreen display to navigate the available TD4 functions. Use the onscreen virtual keyboard or a USB keyboard to enter alphanumeric text when prompted. See “USB keyboard and mouse support” on page 17.

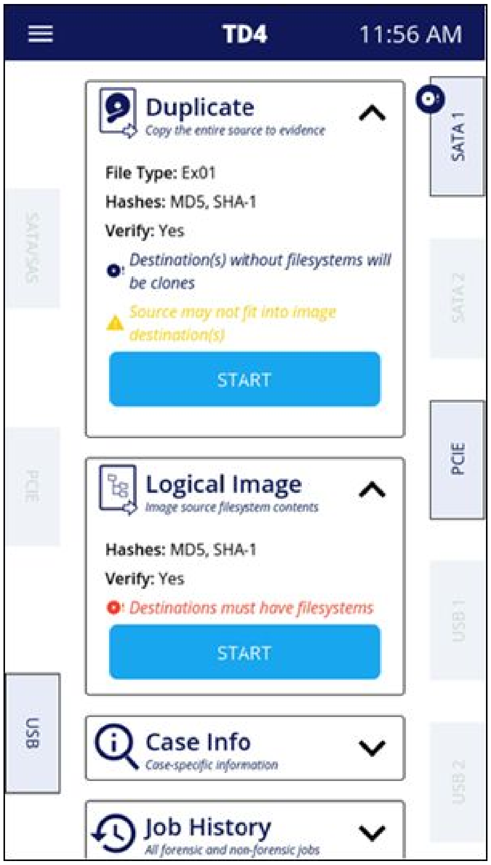
### 2.2.1 Home screen

The home screen of TD4 displays function tiles for initiating the following forensic jobs:

- Duplicate
- Logical Image
- Hash
- Verify
- Restore

It also includes tiles for entering/viewing essential information, as follows:

- Case Info
- Job History



Duplicate
Copy the entire source to evidence

File Type: Ex01
Hashes: MD5, SHA-1
Verify: Yes
Destination(s) without filesystems will be clones
Source may not fit into image destination(s)

Logical Image
Image source filesystem contents

Hashes: MD5, SHA-1
Verify: Yes
Destinations must have filesystems

Case Info
Case-specific information

Job History
All forensic and non-forensic jobs

Each function tile may be opened to show more information, enter data, and, if applicable, start the associated job. Depending on various conditions, the job will either start immediately after hitting the **Start** button or an advanced settings screen will be displayed to allow configuration of specific settings before starting the job. More details for each home screen function can be found later in this user guide.

Across the top navigation bar there are buttons to quickly access the System Navigation Menu ≡ and the home screen and to view the current time. Tapping the TD4 model name in the top navigation bar takes you to the home screen.

**Note:** In the event of abnormal cooling conditions, a thermal event warning icon 🌡 will be shown in the top navigation bar to the right of the System Navigation Menu icon. Such a warning will never be seen under normal operating conditions. Please refer to “Thermal issues” on page 96 for more information.

## 2.2.2 Drive details

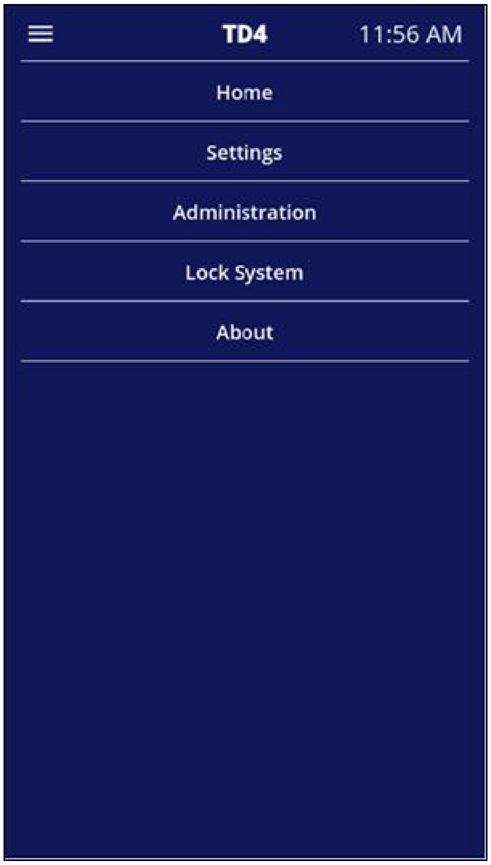
On the left and right sides of the home screen you will find drive tiles that align with the physical drive connection ports. These tiles will be inactive (grayed-out) for any ports that have no drive attached. When a drive is attached to a given port, that tile will become active and can be tapped to access detailed information about that drive and perform drive-specific actions.

**Note:** The drive tile for the rear USB accessory port will only appear when a drive is connected to that port. It will appear beneath the system Navigation Menu icon in the top-left corner of the home screen.

See “Using OpenText Tableau Forensic TD4 Duplicator“ on page 33 for more information on drive details.

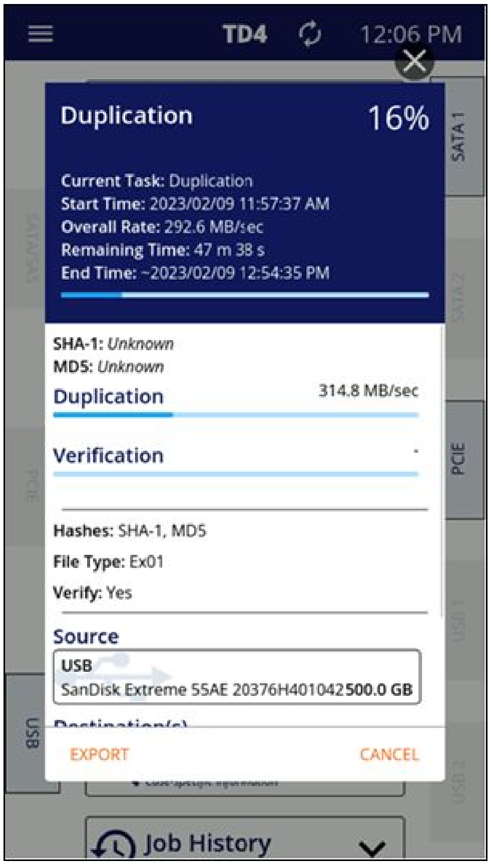
## 2.2.3 System navigation menu

Tapping the System Navigation Menu icon ≡ in the upper-left corner of the top navigation bar displays the TD4 System Navigation Menu, as shown below. For additional information on the items in this menu, see “Configuring TD4” on page 19.



### 2.2.4 Job status

After a job starts, its job status screen is automatically displayed. This status screen shows the details of a given job, including a header showing the job type, its status, its start and end times, the overall data rate, time remaining, and percent complete. The lower area of the job status screen shows additional job details, including hash values (when available) sub-step progress (for example, Duplication separate from Verification in a duplication/verification job), a settings summary, and the drives involved in the job. Tapping a drive tile opens a drive details screen which provides a quick view of all the information available for the drive. The fixed bottom area of the job status screen includes buttons for exporting the forensic log and canceling the job. An example of an active Duplication job status screen is shown below.



Duplication 16%

Current Task: Duplication
Start Time: 2023/02/09 11:57:37 AM
Overall Rate: 292.6 MB/sec
Remaining Time: 47 m 38 s
End Time: ~2023/02/09 12:54:35 PM

SHA-1: *Unknown*
MD5: *Unknown*

Duplication 314.8 MB/sec

Verification -

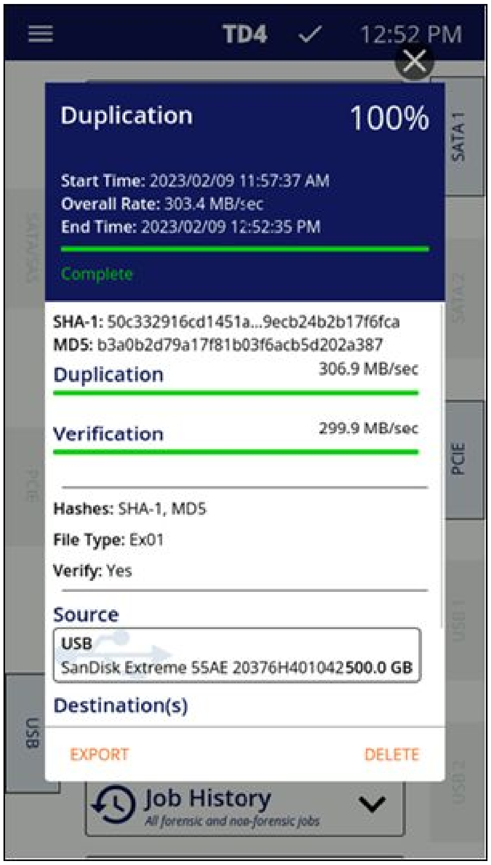
Hashes: SHA-1, MD5
File Type: Ex01
Verify: Yes

Source

USB
SanDisk Extreme 55AE 20376H401042 **500.0 GB**

**Note:** If the detailed job status screen is closed, a brief summary of the job status is still available in the expanded function tile on the home screen. Tapping the lower portion of that function tile will reopen the detailed job status screen. Also, when a job is running a circular spinner is shown in the top navigation bar to the right of the TD4 model name. Tapping the spinner will reopen the detailed job status screen.

Once a job has completed, the job status screen is displayed and shows the final status of that job. An example of a completed Duplication job status screen is shown below.



Duplication 100%

**Start Time:** 2023/02/09 11:57:37 AM
**Overall Rate:** 303.4 MB/sec
**End Time:** 2023/02/09 12:52:35 PM

Complete

**SHA-1:** 50c332916cd1451a...9ecb24b2b17f6fca
**MD5:** b3a0b2d79a17f81b03f6acb5d202a387

Duplication 306.9 MB/sec

Verification 299.9 MB/sec

**Hashes:** SHA-1, MD5

**File Type:** Ex01

**Verify:** Yes

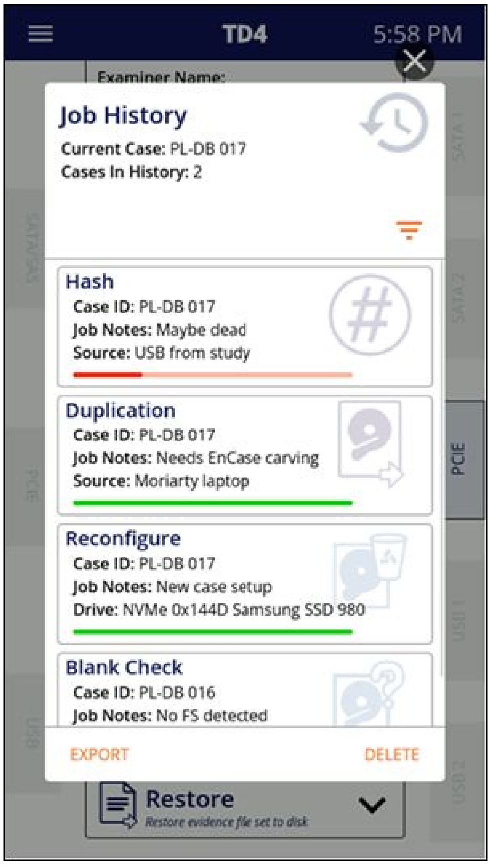
Source

USB
SanDisk Extreme 55AE 20376H401042 **500.0 GB**

Destination(s)

## 2.2.5 Job history

Historical job status screens can be viewed from the Job History list. To access the Job History list, expand the Job History function tile on the home screen. A summary of the total jobs and cases (based on Case ID setting) will be shown in the expanded function tile. Tap the lower portion of the expanded Job History function tile to open the Job History list. The jobs in this list persist across power cycles. Any active jobs will show in the list with an active blue progress bar. Successfully completed jobs will show with a full green progress bar. Canceled jobs will show a partially filled yellow progress bar. And failed jobs will show a partially filled red progress bar. Tapping a specific job tile from the list will open the detailed job status screen for that job. An example of a Job History list is shown below.



Current Case: PL-DB 017
Cases In History: 2

Hash
Case ID: PL-DB 017
Job Notes: Maybe dead
Source: USB from study

Duplication
Case ID: PL-DB 017
Job Notes: Needs EnCase carving
Source: Moriarty laptop

Reconfigure
Case ID: PL-DB 017
Job Notes: New case setup
Drive: NVMe 0x144D Samsung SSD 980

Blank Check
Case ID: PL-DB 016
Job Notes: No FS detected

As can be seen at the top of the Job History screen above, the current case (as identified by the Case ID system setting) is shown along with a count of the number of different cases included in the Job History list.

In some situations, it may be convenient to view and manage (export or delete) only a subset of jobs from the list. To filter the job list, tap on the filter icon ≡ near the top-right side of the Job History screen. Filter criteria can be added to show only the desired jobs. The jobs list can be filtered based on the following criteria:

- Job type
- Examiner name
- Case ID
- Job notes
- Drive vendor
- Drive model
- Drive serial number

Simply tap the desired filter field(s) and enter the filter value(s). A count of how many jobs matched the filter criteria will be shown near the top of the screen next to the filter icon ≡. Note that when multiple criteria are used, all must match for a job to show in the filtered list. The filter criteria section of the screen can be expanded and collapsed by tapping on the filter icon ≡. Tapping the up arrow near the bottom of an open filter criteria section will close it.

**Note:** There is an easy way to filter the Job History list to show only jobs associated with a specific drive. To do so, tap on the desired drive tile from the home screen. Scroll to the Jobs summary section at the bottom of the drive details screen, and then tap on the **View** button. A list of only the jobs associated with that drive will be shown.

To export the logs associated with jobs in the Job History list, tap on the **Export** button at the bottom-left of the Job History screen. Select the desired filesystem and then tap the **Export** button at the bottom-right corner of the browse window.

To delete the jobs (and their associated logs) that are shown in the Job History list, tap the **Delete** button at the bottom-right of the Job History screen and follow the prompt.

**Note:** For both exportation and deletion of jobs/logs, whatever jobs are shown in the Job History list are the ones that will be acted upon. If there are no filters in place, then all jobs/logs will be exported or deleted. If a filter is used to show only a subset of the overall jobs list, then only those filtered jobs/logs will be exported or deleted.

Up to 100 jobs can be stored on TD4. When that limit is hit, the start of any subsequent jobs will require acknowledgement that the oldest job will be automatically deleted. In order to avoid that inefficient job startup step, it is recommended that job logs be exported and jobs be deleted at the end of each case.

## 2.3 Reading the status LEDs

**On/Off indicator LED:** The illuminated power switch is located in the top-left corner of TD4, and it displays a white LED when the unit is on.

**DC In LED:** The TP6 power supply cable has a blue LED ring near the end of the barrel connector that indicates the TD4 power supply is receiving adequate DC input power.

**Activity LED:** The multi-color activity LED is located in the lower-right corner of TD4. It is white when the unit is booting up, blinking white when a power issue is detected, off when the unit is on but idle, blue when an operation is in progress, blinking green when an operation completes successfully, and blinking red when an operation fails.

## 2.4 Interpreting audio feedback

TD4 plays one of two sounds that indicate status at the end of a job. A pleasant chime sound with increasing pitch notes plays for a successful job. For a failed job, the sound has decreasing pitch notes. You can change the volume of the sounds or disable them on the Settings screen.

## 2.5 On-screen warnings

When appropriate, TD4 will provide on-screen warnings within various settings and operations screens. Yellow warnings call the user's attention to a potential risk but do not impede operations. Red warnings mean that a selected setting cannot be accommodated, an operation has failed, or the potential exists for forensic evidence to be missed, such as when a DCO or AMA is detected and not removed. Users are encouraged to pay attention to and read any displayed warnings when they appear and proceed accordingly.

## 2.6 USB keyboard and mouse support

You can plug a standard, English language USB keyboard and/or mouse into any TD4 USB port. (While the Accessory port on the rear of TD4 is intended for this purpose, any USB port will work.) You may find it more convenient to use an external keyboard and/or mouse to navigate the user interface and enter data instead of using the touchscreen and virtual keyboard. Wireless keyboard/mouse adapters are supported as well, including unified adapters.

**Notes**

- TD4 supports wireless keyboards and mice. To use a wireless keyboard or mouse, simply plug the USB wireless adapter into TD4’s rear USB accessory port, and it should automatically pair with the keyboard and start working. There are many vendors of wireless keyboards and mice, and some may not be compatible with TD4. If you prefer to use a wireless keyboard or mouse and yours is not working with TD4, contact OpenText Customer Support for keyboard recommendations.

- If you are using a wireless unified keyboard/mouse adapter with only a mouse, the virtual keyboard may not appear on the TD4 screen for data entry situations. TD4 will see the wireless adapter as the keyboard which makes it want to hide the virtual keyboard in data entry situations. To accommodate this use case, a Virtual Keyboard system setting has been added to allow the virtual keyboard to always be shown when entering data. This setting will be off by default, which means that the virtual keyboard will not appear if a USB keyboard is detected.

Chapter 3

# Configuring OpenText Tableau Forensic TD4 Duplicator

This chapter describes the steps to configure TD4 prior to using it on a regular basis.

## 3.1 Startup sequence

When turned on, TD4 displays an initialization screen during the boot sequence. The initial boot cycle (after a factory reset) will show a setup wizard that brings out key system settings to make it easy to configure your TD4 for use. Interacting with that setup wizard screen (by closing it or tapping the **Full Settings** button) will prevent it from appearing in future boot cycles. Once booted past the setup wizard screen, TD4 displays the home screen, and then sequentially powers on and detects connected drives and mounts any supported filesystems.

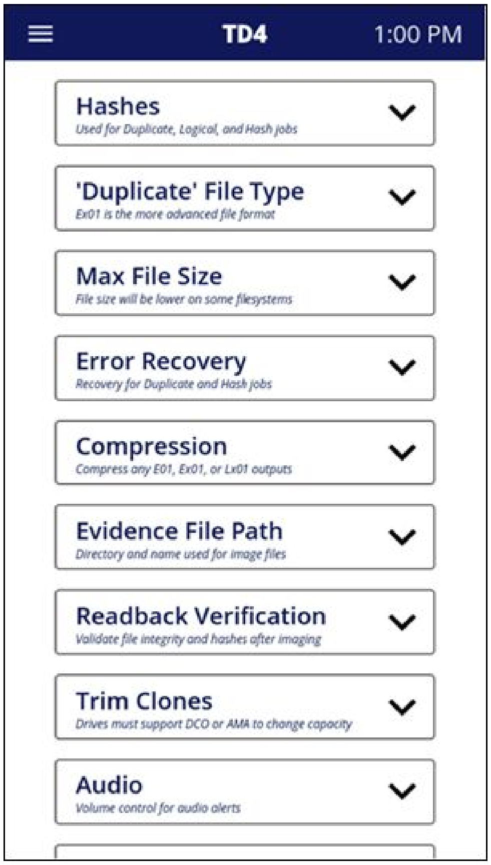
## 3.2 Configuring TD4

TD4 default settings are defined using sensible, best-practice values. There are many options and settings you can configure and customize to your specific needs. Tap the System Navigation Menu icon ≡ in the upper left corner of the user interface to access the System Navigation Menu, which includes following items:

- **Home**: Return to the home screen.
- **Settings**: Access the System Settings screen.
- **Administration**: Access the Administration setup screen.
- **Lock System**: Lock the screen with a PIN to prevent access while unattended.
- **About**: Access the About screen to view additional information such as the unit serial number, firmware version/hash, copyright, and licensing information. Firmware update and factory reset are also initiated from this screen.

### 3.2.1 Settings

Tap **Settings** to display the Settings screen.



Hashes
*Used for Duplicate, Logical, and Hash jobs*

'Duplicate' File Type
*Ex01 is the more advanced file format*

Max File Size
*File size will be lower on some filesystems*

Error Recovery
*Recovery for Duplicate and Hash jobs*

Compression
*Compress any E01, Ex01, or Lx01 outputs*

Evidence File Path
*Directory and name used for image files*

Readback Verification
*Validate file integrity and hashes after imaging*

Trim Clones
*Drives must support DCO or AMA to change capacity*

Audio
*Volume control for audio alerts*

The screenshot above shows the TD4 Settings screen. Each setting and its options and default values are described below.

- **Hashes**: Allows selection of the desired hash calculations for your Duplicate, Logical Imaging, and Hash jobs. The options are MD5, SHA-1, SHA-256, and Prompt. Selecting Prompt will allow the hashes to be chosen at job startup time. The default hash selections are MD5 and SHA-1.
- **'Duplicate' File Type**: Allows selection of the output file type for Duplicate (physical image) jobs. The options are: Ex01, E01, DD, DMG and Prompt. Selecting Prompt will allow the file type to be chosen at job startup time. The default setting is Ex01.
- **Max File Size**: Allows selection of the desired maximum output file segment size. The options are: 2 GB, 4 GB, 8 GB, and Unlimited. The default setting is Unlimited.
- **Error Recovery**: Allows selection of the Recovery Mode and Retry Count for when source drive read errors are encountered during Duplicate and Hash jobs.
  - **Recovery Mode**: This determines the size of reads that will be used to find readable data within regions that have errors. The options are: Standard and Exhaustive. Standard mode means that error recovery attempts will read

  blocks of data that are always 32,768 bytes. In Exhaustive mode, error recovery reads will occur down to the most granular level possible, which is individual sectors. Exhaustive mode will ensure the maximum amount of recoverable data, but it will also add time to the job. The default setting is Standard.

  - **Retry Count**: This tells TD4 how many times to attempt to re-read a given block of data when an error is encountered. The options are: 0, 1, 10, and 100. The default setting is 1.

> **Caution**
>
> A retry count setting of 100 is not recommended. If a read continually errors over 10 attempts, it is likely it will never succeed, and continuing to attempt many failed reads could potentially damage an already failing drive and waste valuable investigation time.

- **Compression**: Allows selection of data compression for E01, Ex01, and LX01 outputs. Selecting the box will ensure that data compression is used whenever possible. The default setting is to compress when possible.

- **Evidence File Path**: Allows definition of the specific filename and directory for output files. Note that wildcards can be used to automatically enter key information into the filenames and/or output directory, as follows:

| Wildcard | Directory/filename data |
|---|---|
| %d | Date (current system date at time of acquisition) |
| %t | Time (current system time at time of acquisition) |
| %e | Evidence ID for the source drive in use |
| %s | Serial number of the source drive in use |
| %m | Model number of the source drive in use |
| %c | Case ID at time of acquisition |

  The default filename is `image`. The default directory name is `td4 images/%d_%t/`.

- **Readback Verification**: Allows selection of readback verification to be done at the end of the duplication/logical image portion of jobs, to ensure the stored data matches what was acquired. Selecting the Verify box will enable readback verification for all jobs. Selecting Prompt will allow readback verification to be enabled at job startup time. The default setting is Verify.

- **Trim Clones**: Allows selection of the desired destination “trimming” configuration for all jobs. Trimming a destination drive means that a DCO or AMA will be applied to the destination drive (if it supports them) so that the destination drive size will appear to match that of the original clone source drive. The options are: Never, When possible, and Prompt. Selecting Prompt will allow the Trim Clones setting to be selected at job startup time. The default setting is Never.

**Note:** For clone trimming to work, the chosen destination drive must support DCO or AMA.

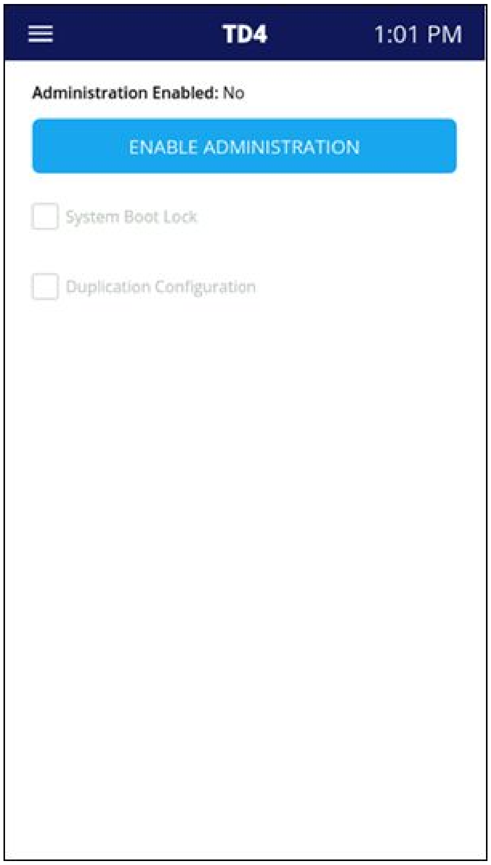
- **Audio**: Allows selection of the system volume level to be used for all audible alerts. Selecting the Idle Chirp box will cause the job completion sound to be repeatedly played every one minute until the job status screen has been closed. Note that, even if Idle Chirp is disabled, the job completion sound will be played one time at the end of the job and the indicator LED will flash completion status until the job status screen has been closed. The default setting is to enable Idle Chirp.
- **Time Display**: Allows selection of the displayed system time zone and time display mode (12-hour or 24-hour). Time Display setting changes must be explicitly saved to take effect. Note that changing time-related settings is not allowed while a job is running. The default display mode setting is 12-hour mode.
- **System Time**: Allows entry of the system time. System Time setting changes must be explicitly saved to take effect. Note that changing time-related settings is not allowed while a job is running.
- **System Date**: Allows entry of the system date. System Date setting changes must be explicitly saved to take effect. Note that changing time-related settings is not allowed while a job is running.
- **Brightness**: Allows selection of the brightness of the LCD screen.
- **Virtual Keyboard**: Provides the option to always show the on-screen, virtual keyboard, even when an external keyboard is detected. This is useful for a specific scenario, where a unified (dual-purpose) wireless keyboard/mouse is plugged into TD4, but only the mouse part is being used. Select the 'Always show' option to ensure that the virtual keyboard appears in this situation. By default the virtual keyboard is hidden when a USB keyboard is detected.
- **Language**: Allows selection of the system language. The options are: German, English, Spanish, French, Korean, Portuguese, Russian, Turkish, and Chinese. The default language is English.

**Note:** When the system language is changed, the virtual keyboard will automatically be switched to that language. If desired, the virtual keyboard can be manually changed to a language that is different than the system language setting. To manually select the virtual keyboard language, tap an input field and then tap the localization button 🌐 on the keyboard to select the desired language.

### 3.2.2 Administration

In some forensic work environments, it may be desirable to prohibit unauthorized users from accessing the unit or changing specific settings. TD4 allows an administrative level user to lock specific areas of the user interface to allow such control.

Tap the **Administration** button in the System Navigation Menu to initiate this setup. The initial Administration setup screen is shown below.



**Administration Enabled:** No

□ System Boot Lock

□ Duplication Configuration

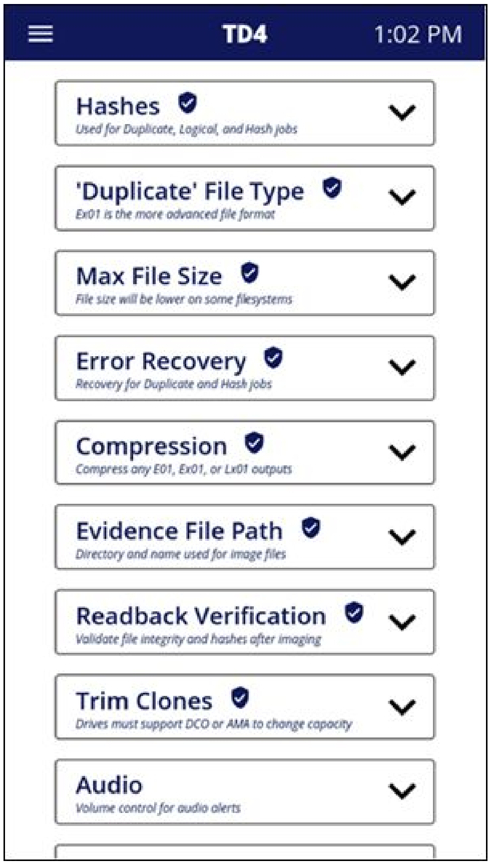
Tap **Enable Administration** to get started. The first step is to set a six-digit Administration PIN. The PIN must be entered twice to ensure accuracy.

Once Administration is enabled, the following areas can be selected to block access to anyone without the PIN:

- **System Boot Lock**: If selected, the unit will boot directly to the PIN pad, and the Administrator PIN will need to be entered to use the unit.
- **Duplication Configuration**: If enabled, the following Duplication settings will require the Administrator PIN to make any changes:
  - Hashes

- 'Duplicate' File Type
- Max File Size
- Error Recovery
- Compression
- Evidence File Path
- Readback Verification
- Trim Clones

The screenshot below shows the Settings menu after Administration control has been enabled for Duplication Configuration. Note the shield with checkmark icon next to the setting items enumerated above. This indicates which settings will require the Administrator PIN to make changes. All users will be able to view the current settings, but any attempts to change any of the locked settings will prompt the user for the Administrator PIN.

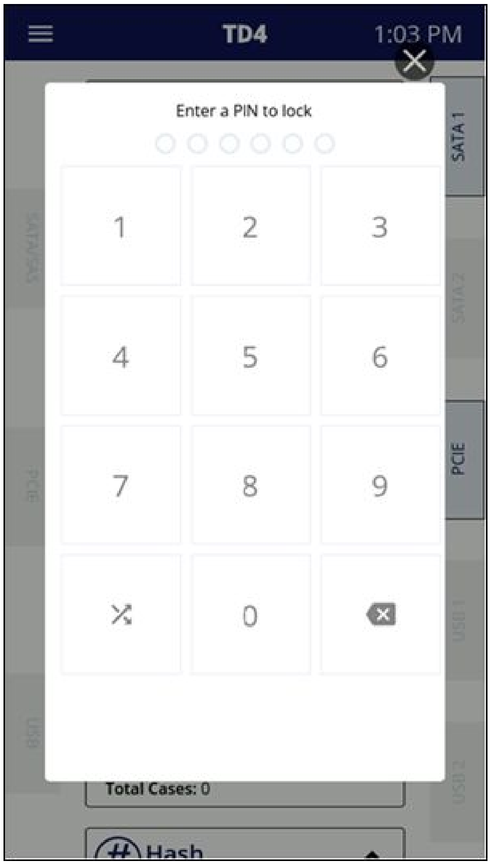

TD4
1:02 PM
Hashes
Used for Duplicate, Logical, and Hash jobs
'Duplicate' File Type
Ex01 is the more advanced file format
Max File Size
File size will be lower on some filesystems
Error Recovery
Recovery for Duplicate and Hash jobs
Compression
Compress any E01, Ex01, or Lx01 outputs
Evidence File Path
Directory and name used for image files
Readback Verification
Validate file integrity and hashes after imaging
Trim Clones
Drives must support DCO or AMA to change capacity
Audio
Volume control for audio alerts

To disable TD4 Administration, tap **Administration** from the System Navigation Menu and then tap **Disable Administration**. The Administration PIN will need to be entered to complete disablement.

**Note:** When Administration has been enabled, even if none of the individual control options has been selected, the Administrator PIN will be required to update the firmware on the unit. This prevents circumvention of the Administration settings by downgrading firmware.

### 3.2.3 Locking the system

It may be desirable to lock your TD4 system while unattended to ensure no settings are changed or that your active jobs are not altered in any way. To lock your system, simply tap on the **Lock System** item in the System Navigation Menu. A screen will appear that allows for entry of a six-digit personal identification number (PIN), as shown below.



You will need to enter the six-digit code a second time to verify the PIN. Once the PIN has been verified, the unit will be locked, showing only the PIN pad on the screen.

To unlock the system, simply enter the PIN.

**Note:** The button at the bottom-left of the keypad allows for randomizing the layout of the digits on the keypad. This can be used to ensure that commonly used PINs do not create a distinct pattern on the screen.

This PIN locking mechanism is temporary in the sense that each unlock event will keep the unit unlocked until it is re-locked. Note that power cycling TD4 will clear the screen PIN lock.

### 3.2.4 Updating TD4 firmware

TD4 firmware is stored on a non-volatile, non-removable memory device inside the unit. When a TD4 firmware update becomes available on the OpenText My Support portal, you can download the firmware package file and use it to update the unit.

**Note:** A firmware update cannot be started while a job is running.

To update your TD4 firmware, go to the OpenText My Support Portal Knowledge Base (https://support.opentext.com/csm?id=csm_knowledge_home), then follow these steps.

**Note:** Filtered results appear on the right. You can skip any of steps 1–5 when you see the link you want.

1. In the **Product** section on the left, expand **Tableau Forensic**.
2. In the **Duplicator/Imager** section, select **TD4**.
3. Expand the **Version** section, then select the version of the firmware you want.
4. Expand the **Content Type** section, then select **Software Download**.
5. Click **Software**.
6. Click the link for the firmware package. A page containing the download link is displayed. (The TD4 firmware package file extension is `.td4_pkg`.)
7. Click **Download**. The firmware package is downloaded to your machine.

   **Note:** If this is your first time downloading TD4 firmware from OpenText My Support, you will need to perform steps 8-10, after which the package will be downloaded to your machine.

8. The **OpenText End User License Agreement** page is displayed.
9. Click the box accepting the terms of the license agreement. The **Accept** button becomes enabled.
10. Click the **Accept** button.
11. Copy the downloaded firmware package file to a USB stick and then eject and remove that drive from your computer.
12. Insert the USB stick into any TD4 USB port.
13. Go to the System Navigation Menu by tapping on the ≡ icon at the left side of the top navigation bar. Then tap the **About** menu item.
14. In the About screen, tap the **Update Firmware** button.
15. Select the appropriate drive/filesystem by tapping on the filesystem tile.

16. Browse to the location of the desired `.td4_pkg` file and tap on that file.
17. Once you are sure you want to initiate the update with the selected file, tap the **Select** button at the bottom-right of the screen.

TD4 will begin the firmware update process using the selected firmware file.

**Caution**

Once the firmware update process begins, do not remove or add any drives, turn off the unit, or remove power from the unit. Doing so could cause issues with the firmware update process possibly resulting in a non-functional TD4. If something should occur during the firmware update process that results in a failure to update, it is possible that the firmware recovery procedure may be required. See "Troubleshooting common problems" on page 94 for information on the firmware recovery process.

TD4 will automatically reboot into the new firmware once the update process is complete.

Note that the SHA-256 hash value of the currently loaded firmware package is calculated and displayed in the top portion of the About screen along with the full firmware version. This allows for verification that the proper firmware version is running and that it has not been altered. For hash verification purposes, the hash value for a given firmware version is available in the release notes document for each TD4 update, which is available on the OpenText My Support Portal Knowledge Base (https://support.opentext.com/csm?id=csm_knowledge_home).

## 3.3 Connecting drives

The following sections provide information that will allow for the safe and reliable connection of drives to TD4.

**Note:** For drives that require adapter cables to connect to TD4, OpenText highly recommends leaving the adapter cables plugged into TD4 and attaching/removing the drives from the other end of the cables. While the drive connectors on TD4 are robust and designed for many mating cycles, attaching/removing drives from the other end of the cables will help maximize the life of your TD4.

## 3.3.1 USB versions and connector types

USB specifications have changed over time, and, along with them, the naming convention for various USB interface ports/speeds has also changed. For example, when USB 3.0 (SuperSpeed USB) first came out, interface speeds jumped to 5 Gbps over the previous USB 2.0 speed of 480 Mbps. With the advent of USB 3.1, the concept of generations was introduced to cover the various interface speeds. For example, USB 3.0 SuperSpeed is equivalent to USB 3.1 Gen 1 at 5 Gbps, and USB 3.1 Gen 2 doubled that speed to 10 Gbps. More recently, the USB 3.2 standard has been released. However, the generational reference for speeds remains the same as USB 3.1, with USB 3.2 Gen 1 being 5 Gbps and USB 3.2 Gen 2 being 10 Gbps. Using the most recent USB specification language, TD4's source USB port is USB 3.2 Gen 1 running at 5 Gbps. Its destination USB ports are USB 3.2 Gen 2 running at 10 Gbps. For simplicity, these ports are labeled as "USB" on the TD4 itself, and they will commonly be referred to as USB ports in this user guide.

TD4 USB ports all use USB Type C connectors. Type C drives and drive cables can be inserted into TD4 without regard for orientation. To connect a USB Type A drive to TD4, a Tableau TCA-USB3-AC Type A-to-Type C adapter cable (or equivalent commercially available adapter) is required.

## 3.3.2 Drive adapters

For some of the TD4 ports, external adapters are required to connect certain types of drives. Chapter 5 of this user guide contains a comprehensive list of available Tableau drive adapters. Here is a summary of commonly used adapters:

| Drive Type | Tableau Adapter Part Number |
|---|---|
| PCIe add-in card SSD | TDA7-1 |
| m.2 PCIe SSD | TDA7-2 |
| Apple PCIe SSD 2013+ | TDA7-3 |
| u.2 SSD (PCIe) | TDA7-4 |
| IDE | TDA7-5 |
| Apple PCIe SSD 2016+ | TDA7-7 |
| FireWire | TDA7-9 |
| mSATA/m.2 SATA SSD | TDA3-3 |

### 3.3.3 Drive tiles

On the left and right sides of the home screen you will find drive tiles that align with the physical drive connection ports. These tiles will be grayed-out for any ports that have no drive attached. When a drive is attached to a given port, that tile will become active and can be tapped to access detailed information about that drive and perform drive-specific actions.

**Note:** The drive tile for the rear USB accessory port will only appear when a drive is connected to that port. It will appear beneath the System Navigation Menu icon ≡ in the top-left corner of the home screen.

### 3.3.4 Source drives

TD4 runs one forensic job at a time, and, as a result, it was designed to only allow connecting one source drive at a time. Multiple source drives can physically be connected to TD4, and doing so will not cause any damage to the device. However, when more than one source drive is connected, the source drive tiles will turn red and all operations that require a source drive (Duplication, Logical Image, Hash, and Restore) will be prohibited. Verify is the one operation that can still be done with multiple source drives attached, as it uses only destination drives.

Connect a drive (or a drive adapter with drive in place) to one of the TD4 source (left) side interfaces: SATA/SAS, PCIe, USB. The associated user interface drive tile will become active and can be tapped to view detailed information about the drive and perform drive specific actions. For source drives, the available drive actions are as follows:

- Browse filesystems
- Blank check
- Remove HPA/DCO/AMA
- Encryption unlock (Tableau and Opal encrypted drives)

A job summary specific to that drive can also be viewed on the drive details screen, with a link to view the filtered job history list for that drive. The **Eject** button for each drive is located at the bottom-right side of the drive details screen.

**Note:** Some USB drives can contain multiple SCSI LUNs (Logical Unit Numbers), and some PCIe/NVMe drives can contain multiple NVMe namespaces. These are contained within a single physical drive and thus warrant special consideration in terms of informing of their presence and allowing selection of a specific LUN/namespace from a TD4 source drive. See "Viewing sources and destinations" on page 39 for more information.

### 3.3.5 Destination drives

Connect one or more drives to the TD4 destination (right) side: SATA (x2), PCIe, and/or USB (x2). The associated user interface drive tile(s) will become active and can be tapped to view detailed information about the drive and perform drive specific actions. For destination drives, the available drive actions are as follows:

- Browse filesystems
- Blank check
- Reconfigure (see "Reconfigure" on page 44 section for detailed information about the destination drive Reconfigure function)
- Encryption unlock (Tableau and Opal encrypted drives)

A job summary specific to the drive can also be viewed on this screen, with a link to view the filtered Job History list for that drive. The **Eject** button for each drive is located at the bottom-right side of the drive details screen.

See "Duplicating" on page 60 and "Performing a logical image" on page 72 for details on running Duplicate and Logical Image jobs.

### 3.3.6 Accessory drives

An Accessory USB port is available on the rear of TD4. This port can be used to attach a USB drive to allow for exporting job logs or updating TD4 firmware. It can also be used to attach a keyboard and/or mouse (wired or wireless).

⚠ **Caution**

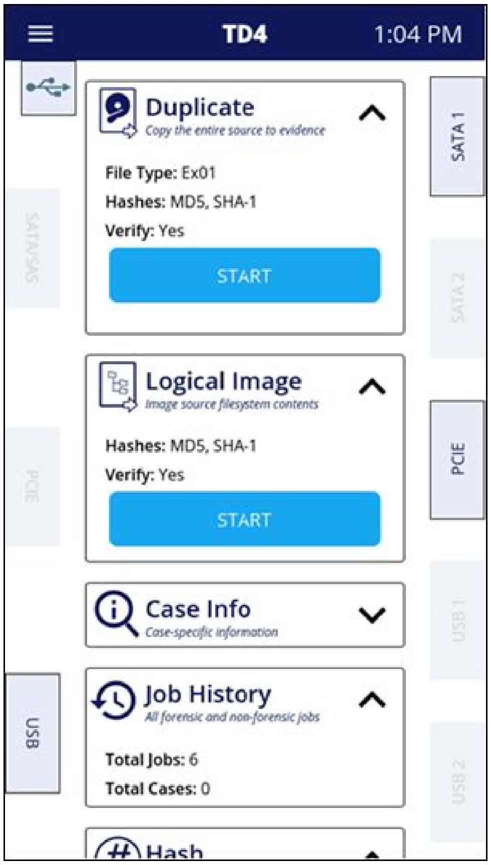
The USB Accessory port on the rear of TD4 is not write-protected! Evidence media should never be connected to this port.

When an Accessory USB drive is attached to TD4 and detected, a small drive tile will appear just below the System Navigation Menu icon ≡ in the top left of the user interface.

### 3.3.7 Drive detection

After booting, TD4 begins detecting connected drives sequentially. Inactive drive tiles shown on the left and right sides of the screen will become fully visible and active when a drive is detected. Tap any drive tile to view detailed information about the connected drive and to perform drive-specific actions. See "Source drives" on page 29 and "Destination drives" on page 30 earlier in this chapter for more information on available actions.

The image below shows the TD4 home screen with the following drives connected: USB source, USB accessory, SATA destination, PCIe destination.


TD4
1:04 PM
SATA/SAS
PCIE
USB
SATA 1
SATA 2
PCIE
USB 1
USB 2
Duplicate
Copy the entire source to evidence
START
Logical Image
Image source filesystem contents
START
Case Info
Case-specific information
Job History
All forensic and non-forensic jobs
Hash

**File Type:** Ex01
**Hashes:** MD5, SHA-1
**Verify:** Yes

**Hashes:** MD5, SHA-1
**Verify:** Yes

**Total Jobs:** 6
**Total Cases:** 0

TD4 can detect USB drives that expose a CDFS volume. This is a common configuration for proprietary self-encrypting drives. The small CDFS volume typically contains an application that can be run on a host computer system which allows for entering credentials that will unlock the drive. TD4 cannot run these proprietary applications, as they are typically made for x86-based Windows systems, and thus TD4 cannot unlock these types of self-encrypting drives. That also means it cannot access the data volume of the drive (even in encrypted form) and thus cannot create an image of the drive. However, TD4 will detect these drives and report their type.

## 3.4 Turning TD4 off

To turn off your TD4, simply push the power button in the top left corner of the unit. Confirm the request by tapping the **Shutdown** button or tap the **Cancel** button to keep the unit powered up.

In some cases, it may be desirable to have TD4 power itself off after the current job is completed. In the case of running a job overnight or over a weekend with the unit unattended, this can help reduce power consumption and unnecessary runtime on any attached drives. To turn off TD4 when the current job is complete, simply push the power button in the top left corner of the unit as you normally would, and then tap the **Shutdown** button. The current job will complete and then the unit will power itself off. This will work for any job type.

**Note:** If the power button shutdown method described above is used, there is no need to eject any attached drives before shutting down TD4. Using this proper shutdown method allows the software time to quiesce any active tasks and eject drives prior to turning the unit off. Forcing TD4 to power off by pulling the power cord or holding down the power button is not recommended as it may corrupt any existing partition/filesystem information.

Chapter 4

# Using OpenText Tableau Forensic TD4 Duplicator

This chapter covers detailed procedures and information for using TD4.

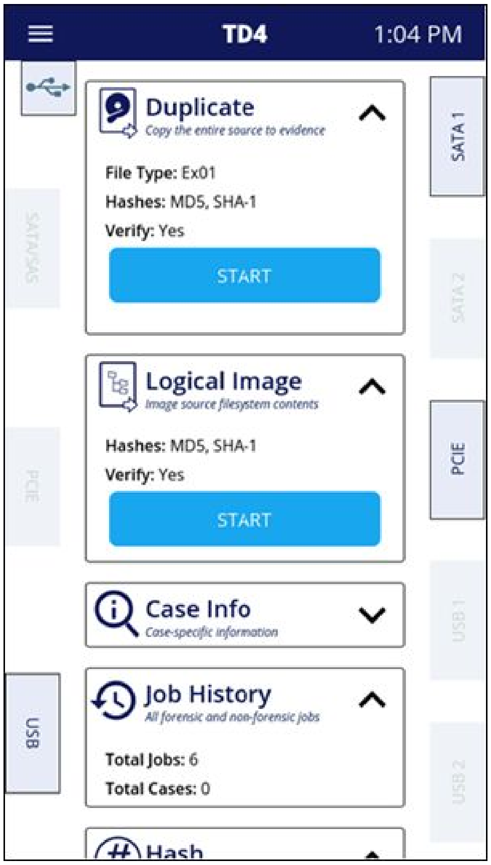
## 4.1 Home screen

The home screen of TD4 displays function tiles for initiating the following forensic jobs:

- Duplicate
- Logical Image
- Hash
- Verify
- Restore

It also includes tiles for entering/viewing essential information, as follows:

- Case Info
- Job History


TD4
1:04 PM
SATA 1
SATA/SAS
SATA 2
PCIE
PCIE
USB 1
USB
USB 2
Duplicate
Copy the entire source to evidence
START
Logical Image
Image source filesystem contents
START
Case Info
Case-specific information
Job History
All forensic and non-forensic jobs
Hash

File Type: Ex01
Hashes: MD5, SHA-1
Verify: Yes

Hashes: MD5, SHA-1
Verify: Yes

Total Jobs: 6
Total Cases: 0

Each function tile may be opened to show more information, enter data, and, if applicable, start the associated job. Depending on various conditions, the job will either start immediately after hitting the **Start** button or an advanced settings screen will be displayed to allow configuration of specific settings before starting the job. More details for each home screen function can be found later in this chapter.

Across the top navigation bar there are buttons to quickly access the System Navigation Menu ≡ and the home screen and to view the current time. Tapping the TD4 model name in the top navigation bar takes you to the home screen.

**Note:** In the event of abnormal cooling conditions, a thermal warning icon 🌡 will be shown in the top navigation bar to the right of the System Navigation Menu icon. Such a warning will never be seen under normal operating conditions. See “Thermal issues” on page 96 for more information.

## 4.2 Drive details

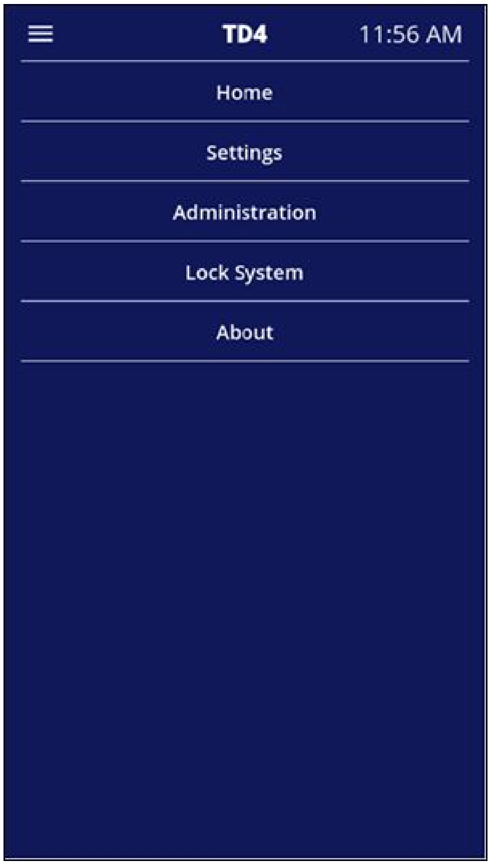
On the left and right sides of the home screen you will find drive tiles that align with the physical drive connection ports. These tiles will be inactive for any ports that have no drive attached. When a drive is attached to a given port, that tile will become active and can be tapped to access detailed information about the drive and perform drive-specific actions.

**Note:** The drive tile for the rear USB accessory port will only appear when a drive is connected to that port. It will appear beneath the System Navigation Menu icon ≡ in the top-left corner of the home screen.

See "Viewing sources and destinations" on page 39 for more information on the drive details screen and associated functionality.

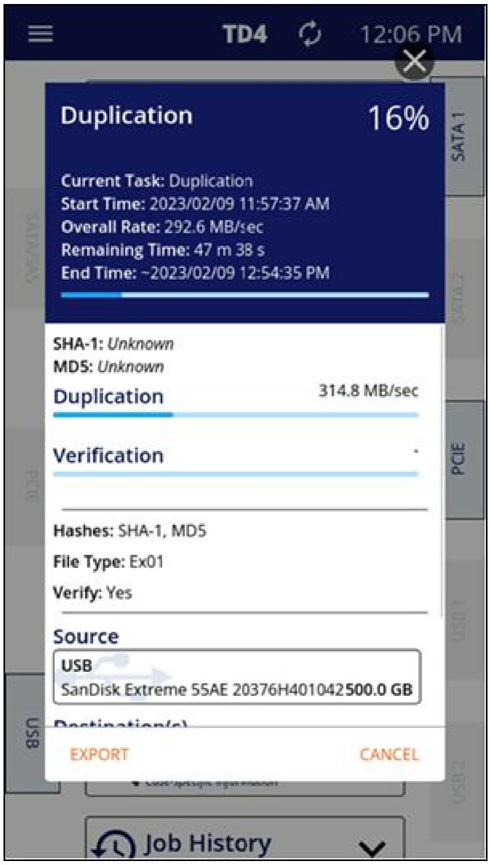
## 4.3 System navigation menu

Tapping the System Navigation Menu icon ≡ in the upper-left corner of the top navigation bar displays the TD4 System Navigation Menu, as shown below. For additional information on the items in this menu, see "Configuring TD4" on page 19.



## 4.4 Job status

After a job starts, its job status screen is automatically displayed. This status screen shows the details of a given job, including a header showing the job type, its status, its start and end times, the overall data rate, remaining time, and percent complete. The lower area of the job status screen shows additional job details, including hash values (when available) sub-step progress (for example, Duplication separate from Verification in a duplication/verification job), a settings summary, and a listing of the drives involved in the job. Tapping a drive tile opens its drive details screen which provides a view of all the information available for the drive. The fixed bottom area of the job status screen includes buttons for exporting the forensic log for that job and canceling the job. An example of an active Duplication job status screen is shown below.



Duplication 16%

**Current Task:** Duplication
**Start Time:** 2023/02/09 11:57:37 AM
**Overall Rate:** 292.6 MB/sec
**Remaining Time:** 47 m 38 s
**End Time:** ~2023/02/09 12:54:35 PM

**SHA-1:** *Unknown*
**MD5:** *Unknown*

Duplication 314.8 MB/sec

Verification -

**Hashes:** SHA-1, MD5
**File Type:** Ex01
**Verify:** Yes

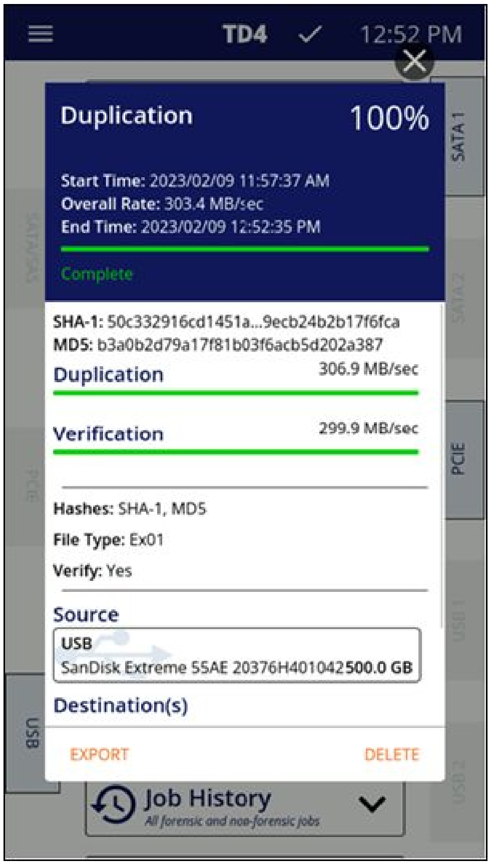
Source

USB
SanDisk Extreme 55AE 20376H401042 **500.0 GB**

Destination(s)

**Note:** If the job status screen is closed, a brief summary of the job status is still available in the expanded function tile on the home screen. Tapping the lower portion of that function tile will reopen the job status screen. Also, when a job is running, a circular spinner is shown in the top navigation bar to the right of the TD4 model name. Tapping the spinner reopens the job status screen.

Once a job has completed, the job status screen is displayed and shows the final status of that job.



TD4 ✓ 12:52 PM

Duplication 100%

Start Time: 2023/02/09 11:57:37 AM
Overall Rate: 303.4 MB/sec
End Time: 2023/02/09 12:52:35 PM

Complete

SHA-1: 50c332916cd1451a...9ecb24b2b17f6fca
MD5: b3a0b2d79a17f81b03f6acb5d202a387

Duplication 306.9 MB/sec

Verification 299.9 MB/sec

Hashes: SHA-1, MD5

File Type: Ex01

Verify: Yes

Source

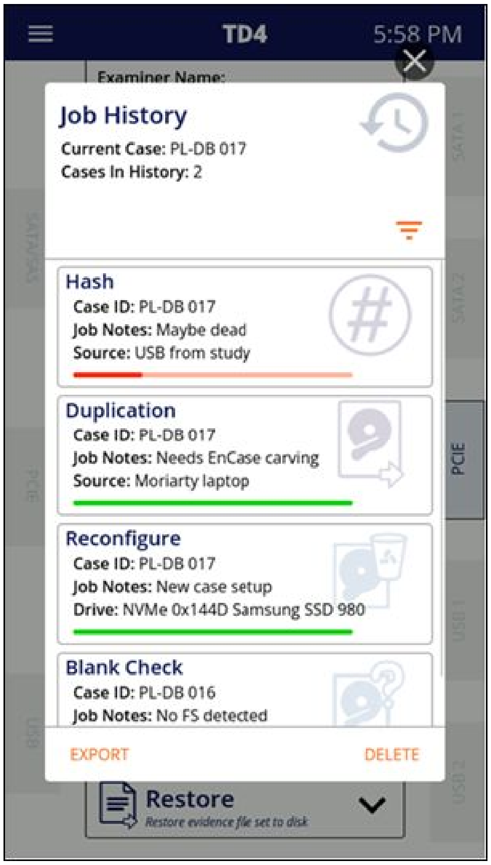
USB
SanDisk Extreme 55AE 20376H401042500.0 GB

Destination(s)

If the job status screen is left open after completion of the job, completion status indicators will continue until the job status screen is closed. Those completion status indicators include a flashing status LED and, if Idle Chirp is enabled in system settings, audible notification (once every minute). If Idle Chirp is disabled, the job completion audible notification will only be provided one time.

## 4.5 Job history

Job status screens can be viewed from the jobs list which is accessible from the Job History tile on the home screen. Tapping the lower portion of the expanded Job History tile opens the jobs list for that unit. The jobs in this list are stored on the unit and persist across power cycles. Any active jobs will show in the list with an active blue progress bar. Successfully completed jobs will show with a full green progress bar. Canceled jobs will show a partially filled yellow progress bar. And failed jobs will show with a partially filled red progress bar. Tapping a specific job tile from the list will open the job status screen for that job. An example of a Job History list is shown below.



Job History

Current Case: PL-DB 017
Cases In History: 2

Hash
Case ID: PL-DB 017
Job Notes: Maybe dead
Source: USB from study

Duplication
Case ID: PL-DB 017
Job Notes: Needs EnCase carving
Source: Moriarty laptop

Reconfigure
Case ID: PL-DB 017
Job Notes: New case setup
Drive: NVMe 0x144D Samsung SSD 980

Blank Check
Case ID: PL-DB 016
Job Notes: No FS detected

As can be seen at the top of the Job History screen above, the current case (as identified by the Case ID setting) is shown along with a count of the number of different cases included in the Job History list.

In some situations, it may be convenient to view and manage (export or delete) only a subset of jobs from the list. To filter the job list, tap on the filter icon ≡ near the top-right side of the Job History screen. Filter criteria can be added to show only the desired jobs. Note that when multiple criteria are used, all must match for a job to show in the filtered list. The jobs list can be filtered based on the following criteria:

- Examiner name
- Case ID
- Job notes
- Drive vendor
- Drive model
- Drive serial number

**Note:** There is an easy way to filter the Job History list to show only jobs associated with a specific drive. To do so, tap on the desired drive tile from the home screen. Scroll to the Jobs summary section at the bottom of the drive details screen and then tap the **View** button. A list of only the jobs associated with that drive will be shown. You can expand the filter in that view to see the specific criteria that was used to filter the list.

To export the logs associated with jobs in the Job History list, tap on the **Export** button at the bottom-left of the Job History screen. Select the desired filesystem and folder and then tap the **Export** button at the bottom-right corner of the browse window.

To delete the jobs that are shown in the Job History list, tap the **Delete** button at the bottom-right of the Job History screen and follow the prompt.

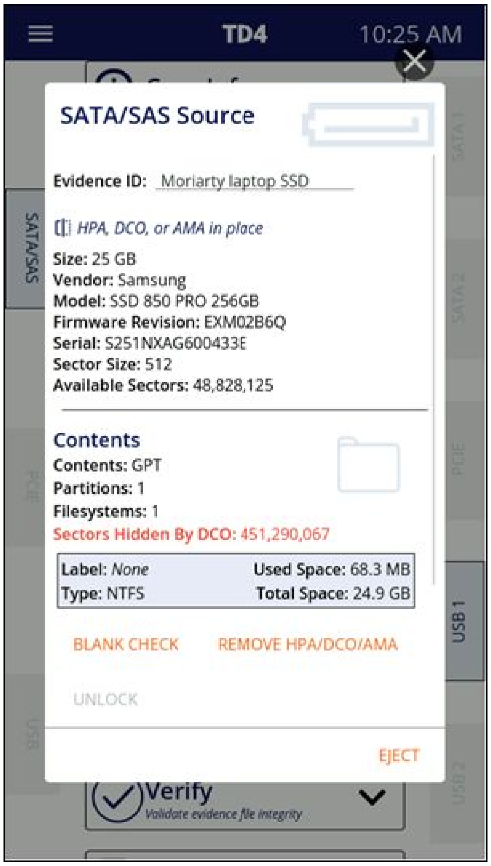
**Note:** For both log exportation and job deletion, whatever jobs are shown in the Job History list are the ones that will be acted upon. If there are no filters in place, then all logs/jobs will be exported or deleted. If a filter is used to show only a subset of the overall jobs list, then only those logs/jobs will be exported or deleted.

Up to 100 jobs can be stored on TD4. When that limit is hit, the start of any subsequent jobs will require acknowledgement that the oldest job will be automatically deleted. To avoid that inefficient job startup step, it is recommended that logs be exported and then jobs deleted at the end of each case.

See “Forensic logs” on page 82 for more information regarding TD4 forensic logs.

## 4.6 Viewing sources and destinations

To access the drive details screen for a source or destination, tap the desired drive tile on the TD4 home screen. Drive tiles are shown on the left (source) and right (destination) sides of the TD4 user interface. The drive details screen for a source SATA drive is shown below.



SATA/SAS Source

Evidence ID: Moriarty laptop SSD

*HPA, DCO, or AMA in place*

**Size:** 25 GB
**Vendor:** Samsung
**Model:** SSD 850 PRO 256GB
**Firmware Revision:** EXM02B6Q
**Serial:** S251NXAG600433E
**Sector Size:** 512
**Available Sectors:** 48,828,125

Contents

**Contents:** GPT
**Partitions:** 1
**Filesystems:** 1
**Sectors Hidden By DCO:** 451,290,067

| | |
|---|---|
| **Label:** *None* | **Used Space:** 68.3 MB |
| **Type:** NTFS | **Total Space:** 24.9 GB |

The Evidence ID field at the top of the drive details screen allows a brief description of the drive to be entered. This Evidence ID value is an informal way to identify drives which allows them to be more easily recognized throughout the TD4 user interface. This Evidence ID will appear in the drive details screens and drive cards, which are seen in various places such as in the Source and Destination(s) sections of the job status screen. Evidence ID will also appear in the forensic logs. If no Evidence ID is entered for a given drive, the drive will be identified by the vendor name, model, and serial number.

After the Evidence ID field, the top section of the drive details screen shows key information about the selected drive, such as size, vendor, model, firmware revision, serial number(s), sector size, and available (reported) sectors. USB drives will have additional information shown, including a USB specific serial number.

The Contents section of the drive details screen provides information about what is on the drive, and it also allows for drive specific actions such as Blank Check, Reconfigure (destinations only), Remove HPA/DCO/AMA (sources only), and Encryption Unlock (Tableau and Opal encrypted drives). For drives with detectable filesystems, the top portion of the Contents section indicates the partition table type, number of partitions, and number of filesystems. Each detectable filesystem will have a filesystem card that shows more information about the filesystem. To browse a filesystem, tap the filesystem card. If a drive has any sector limitations in place

(HPA/DCO/AMA), a warning message will be provided in the top portion of the Contents section. Such sector limitations are also identified with the icon attached to the drive tiles on the home screen.

The Jobs section of the Drive Details screen provides information about jobs that have been performed with that drive. The Jobs count indicates the number of all forensic jobs done using that drive, and it includes the following operations: Duplications, Logical Images, Hashes, Verifications, Reconfigures, Blank Checks, Restores, and Remove Sector Limitations. The Completed Acquisitions count indicates the number of fully completed, successful acquisition type jobs, namely Duplications and Logical Images. If all the jobs for a given drive have the same Case ID, that Case ID is shown in this section as well. If there are multiple Case IDs associated with a given drive, “Multiple” will be shown in the Case ID field. The **View** button in the bottom right of the Jobs section will display a filtered Job History list showing only the jobs associated with that specific drive.

At the bottom right of any Drive Details screen is the **Eject** button. Simply tap the **Eject** button and respond to the prompt to eject a drive from the system. Ejecting a drive removes it from the system software in a safe manner and is recommended before unplugging any attached media from a powered TD4 and before powering down TD4 with drives attached. For destination and accessory drives in particular (since they are read/write), failure to eject a drive prior to removal from the system could corrupt the drive filesystem, which could result in loss of previously captured evidence/data. Note that ejection of media being used in a job will not be allowed until the job is complete.

In addition to quiescing the drive for system removal, pressing the **Eject** button will issue an ATA spin down command to drives that may support it. Spinning down rotating hard disk drives is recommended to minimize the chance of platter damage upon physical removal of the drive from the system. Note that not all drives support this command, and some may take longer to eject from the system due to lack of spin down command support. But this is considered a minor inconvenience compared to the benefit of minimizing the chance of drive damage.

### Caution

It is highly recommended to eject all drives from the system prior to physically removing them from TD4. This puts the drives in a quiescent state, which will ensure system stability and the integrity of the data on the drives.

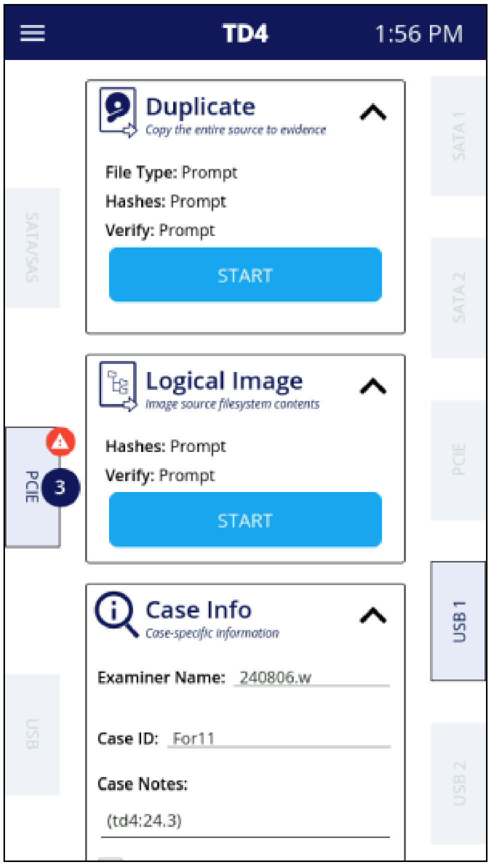
For media attached to TD4 PCIe ports, ejection prior to removal is required. Hot-swapping PCIe drives without ejecting them may cause system instability and unpredictable TD4 behavior/performance.

Forced power removal (by pulling the power cord or holding down the power button) can cause issues with attached drives, including corruption of formatting information. If possible, it is highly recommended to power down through the user interface (via a quick power button press), which will automatically eject all attached drives prior to shutting down the unit.

TD4 was designed to detect/mount one source drive at time to run a single job. If multiple source drives are attached to TD4, their home screen drive tiles will show in red, and no jobs can be started until only one drive remains.

There are two specific types of drive configurations that warrant special consideration on TD4. Some USB drives can be configured to have multiple SCSI LUNs (logical unit numbers) and some PCIe/NVME drives can be configured to have multiple NVMe namespaces. Each SCSI LUN and NVMe namespace presents itself to the TD4 as if it were a standalone drive, even though there can be multiple of them on a single physical drive. When such a drive is plugged into a TD4 source port, the home screen drive tile will show a red warning triangle to indicate that there is something unusual about the attached drive. It will also display a circle with the number of sub-devices the system detected on the drive, as shown in the screenshot below. This is a clear indication that the attached drive has multiple LUNs or namespaces. Tapping on the drive tile will show a drive selection screen from which you can select the specific LUN or namespace you want to use.

**Note:** TD4 supports multiple LUNs and NVMe namespaces only on drives attached to its source ports. If such a drive is attached to a TD4 destination port, only one of the available LUNs or NVMe namespaces will be detected/usable.

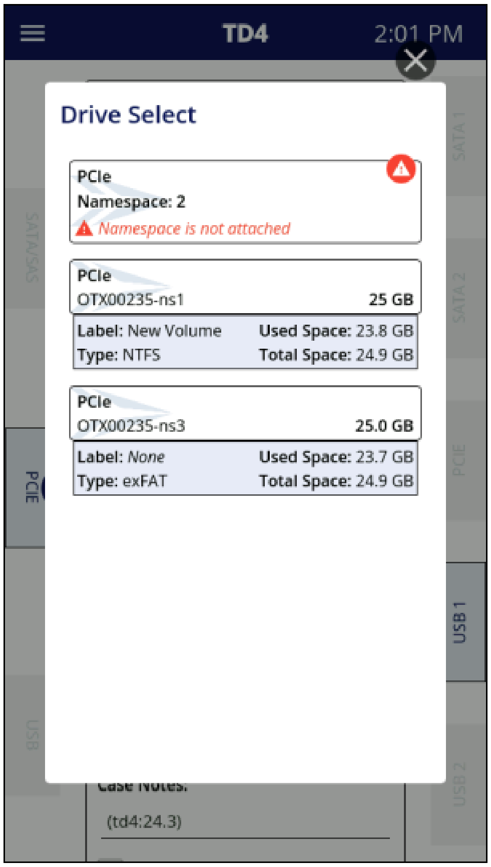


File Type: Prompt
Hashes: Prompt
Verify: Prompt

Hashes: Prompt
Verify: Prompt

Examiner Name: 240806.w
Case ID: For11
Case Notes:
(td4:24.3)

Drives that support NVMe namespace management allow for each namespace to be either attached or detached from each NVMe controller. The primary use case for such NVMe drive configurations is in a multi-tenant server setup where namespace access can be independently configured per NVMe controller. While that is not a standard setup for an individual PCIe/NVMe drive (which typically has only one NVMe controller), it is still possible for an individual NVMe drive to contain namespaces that are detached from the controller. Any such namespaces would not be detected and shown in most commercial computer systems. It is of significant forensic importance to be able to see any unattached namespaces on a target NVMe drive and attach them before acquiring the evidence. TD4 has this covered well. After tapping on the home screen drive tile of a drive with multiple NVMe namespaces, the drive select screen will show all defined namespaces, even if they are detached from the controller, as shown in the screenshot below.



Drive Select

PCIe
Namespace: 2
⚠ *Namespace is not attached*

PCIe
OTX00235-ns1 25 GB
Label: New Volume Used Space: 23.8 GB
Type: NTFS Total Space: 24.9 GB

PCIe
OTX00235-ns3 25.0 GB
Label: *None* Used Space: 23.7 GB
Type: exFAT Total Space: 24.9 GB

Case Notes:
(td4:24.3)

TD4 will allow such detached namespaces to be attached by simply tapping on the detached namespace tile. This will allow all namespaces on a source drive to be individually acquired, whether that be a clone, physical image, or logical image.

**Notes**

- When selecting an individual detached NVMe namespace to attach, TD4 will automatically attach all the unattached namespaces on a given drive.

- Attaching previously unattached NVMe namespaces is a permanent (non-volatile) change to a drive's configuration.

### 4.6.1 Blank check

The Blank Check utility checks a drive for the presence of meaningful data. To access the Blank Check Setup screen, tap Blank Check in the Contents section of any drive details screen.

The following table provides Blank Check option details:

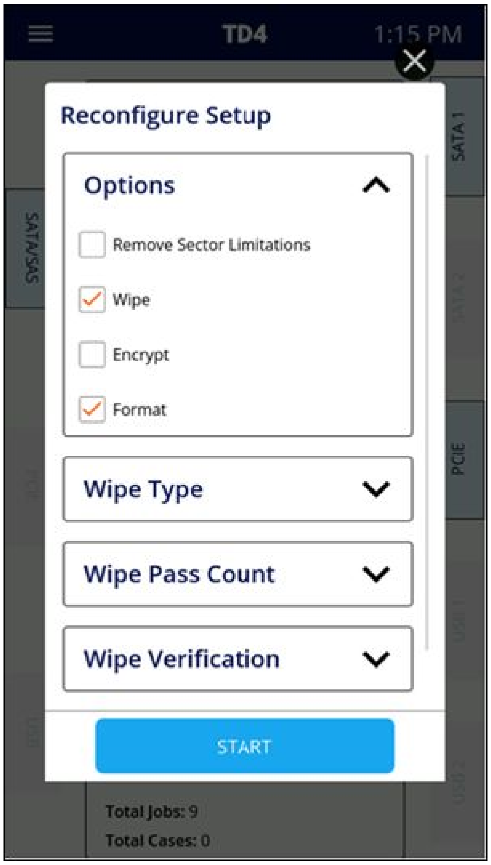
| Option | Description |
|---|---|
| Fast | Quickly checks to determine if the drive appears to be blank by reading in and checking the sectors in the Master Boot Record, the Primary GPT, and the Secondary GPT. |
| Random | Performs the Fast check, then reads in up to 75% of the available sectors randomly to determine if they are blank. The blank check will stop as soon as a non-blank data pattern is detected. |
| Linear | Linearly reads in up to 100% of the available sectors to check if the drive is blank. The blank check will stop as soon as a non-blank data pattern is detected. |

A sector is considered blank if it contains only the same repeated 2-byte pattern. Any non-repeating pattern is considered to be non-blank. However, each individual sector may contain different repeating patterns. If any sector is found to not be blank, the drive is not considered blank, and the blank check will stop.

**Note:** The Fast and Random blank check options do not perform exhaustive checks of the entire drive. It is possible for a drive to appear to be blank according to a Fast or Random check while still storing forensically relevant information.

### 4.6.2 Reconfigure

The Reconfigure utility allows for execution of drive specific actions, mostly related to preparing a destination drive to be used for future Duplication and Logical Imaging jobs. Due to the drive-altering nature of the actions available in this utility, Reconfigure is only available for destination drives. To access the Reconfigure utility setup screen (shown below), tap **Reconfigure** from the Contents section of the drive details screen.



Reconfigure Setup

Options

☐ Remove Sector Limitations

☑ Wipe

☐ Encrypt

☑ Format

Reconfigure allows sequential completion of the requested tasks without need for user intervention. This makes it easy to execute common destination media preparation steps in automated fashion, without having to do each one as a separate step. For example, a destination drive could be wiped and then formatted in one job by selecting Wipe and Format, setting the options for each sub-step, and then tapping **Start**. Note that the listed order of the optional sub-functions of Reconfigure is intentional and matches the order in which they will be applied to the drive. Details on each Reconfigure sub-function are provided in the sub-sections below.

#### 4.6.2.1 Remove sector limitations

In the past, the most common method of intentionally limiting the reported capacity of a drive was by using the ATA HPA (host protected area) and/or DCO (device configuration overlay) feature sets. Starting with the ACS-3 (ATA/ATAPI Command Set 3) specification update, the concept of Addressable Maximum Address (AMA) was introduced. Newer drives may support this method of limiting the reported drive capacity. TD4 supports all these methods with automated detection, identification, and notification that will make dealing with them seamless and easy. From a forensic point of view, it is valuable to know if HPA, DCO, or AMA are in use. With that knowledge, the forensic practitioner can make an informed decision about whether to acquire data in the hidden regions of the drive.

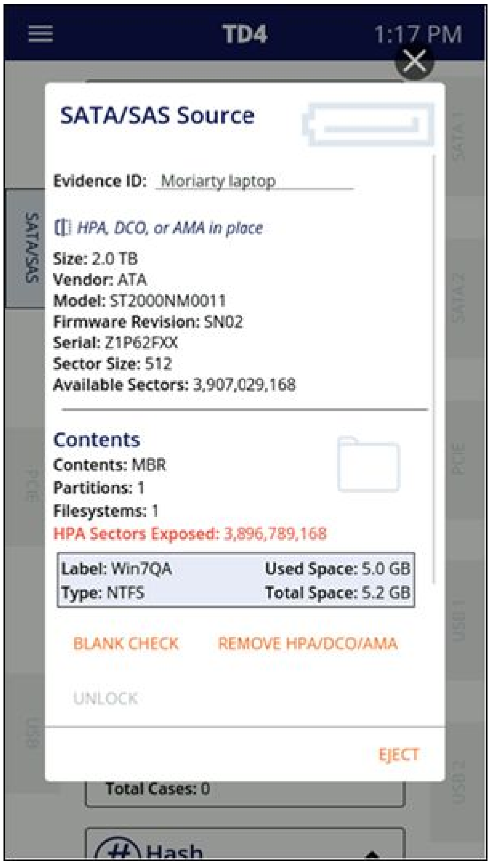
Note that these methods (HPA/DCO and AMA) are mutually exclusive. A drive that supports HPA/DCO will not support AMA, and a drive that supports AMA will not support HPA/DCO. Also, while HPA and DCO are related features for a given drive, HPA has a unique attribute (volatile, or temporary, removal) that distinguishes it from DCO and AMA. For that reason, this section will cover volatile HPA removal as a separate topic before addressing non-volatile (permanent) removal of HPA/DCO or AMA.

TD4 also provides the ability to “shelve” a DCO or AMA, which means disabling a source drive DCO or AMA for the purposes of evidence duplication and then putting the same DCO/AMA back after the job is complete. See “Duplicating” on page 60 for more details on shelving a DCO.

### Volatile HPA removal

HPA can be disabled without making a permanent modification to the drive. This is known as volatile, or temporary, removal of the HPA configuration. When a drive that has had its HPA removed in this manner is removed from TD4 (or is otherwise powered down) and then reconnected, it will always come back in its original state (with the original HPA configured and enabled). Since this is a temporary drive configuration change only (not a change to the data stored on the drive), TD4 automatically disables HPA on any drive connected to one of its source ports. Since DCO and AMA settings can only be disabled on a permanent basis, TD4 does not automatically disable them on connected source drives.

In the case of an automatic, volatile HPA removal from a connected source drive, the TD4 user interface makes it obvious what has occurred by stating how many HPA sectors have been exposed, as shown in the following screenshot.



SATA/SAS Source

Evidence ID: Moriarty laptop

HPA, DCO, or AMA in place

Size: 2.0 TB
Vendor: ATA
Model: ST2000NM0011
Firmware Revision: SN02
Serial: Z1P62FXX
Sector Size: 512
Available Sectors: 3,907,029,168

Contents

Contents: MBR
Partitions: 1
Filesystems: 1
HPA Sectors Exposed: 3,896,789,168

| Label: Win7QA | Used Space: 5.0 GB |
|---|---|
| Type: NTFS | Total Space: 5.2 GB |

Total Cases: 0

Referring to the drive details screenshot above, the fact that the HPA has been removed is reflected in two ways. One, the drive's Size field reflects the full capacity of the drive (with HPA removed). And two, the Contents section shows how many HPA sectors were exposed in red text. Note that this HPA related information is also captured in the forensic logs.

TD4 never makes automatic changes to any drive capacity limiting configurations on destination drives. TD4 was designed to give the forensic practitioner complete control over the destination drive. If you choose to restrict the destination drive capacity using HPA, DCO, or AMA, TD4 will not override that decision.

### Non-volatile HPA/DCO/AMA removal

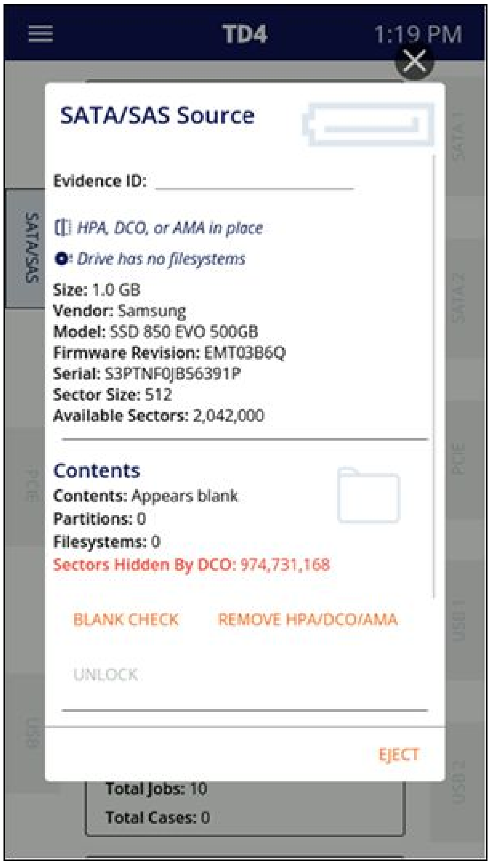
The Remove Sector Limitations utility permanently disables the HPA, DCO, or AMA configurations on the selected drive. These changes are permanent, cannot be undone, and will persist over drive power cycles.

For destination drives, the Remove Sector Limitations utility is included in the Reconfigure function, which is available in the Contents section of the drive details screen. Tap the desired destination drive tile from the home screen, and then tap the Reconfigure button on the drive details screen. In the Reconfigure Setup screen, select Remove Sector Limitations, and then press the **Start** button. Any identified sector limitations (HPA/DCO or AMA) will be removed from the destination drive.

For source drives, the Remove Sector Limitations utility is available directly in the Contents section of the drive details screen. This is because there is no Reconfigure utility for source drives, since most of the Reconfigure options are specifically intended for destination drives.

Note that for HPA/DCO, you cannot remove a DCO-protected region on a drive without also removing any HPA-protected region, as defined by the ATA specification.

If a drive has an HPA/DCO or AMA configured, a red warning message is displayed in the Contents section of the drive details screen indicating the number of sectors that are hidden by the HPA/DCO/AMA. The [⁞ icon is also shown on the edge of the drive tile on the home screen and near the top of the drive details screen to provide at-a-glance identification of the presence of a sector limiting configuration. The screenshot below shows the drive details screen for a drive with a DCO-protected region.



SATA/SAS Source

Evidence ID: ____________

[⁞ *HPA, DCO, or AMA in place*

●: *Drive has no filesystems*

**Size:** 1.0 GB
**Vendor:** Samsung
**Model:** SSD 850 EVO 500GB
**Firmware Revision:** EMT03B6Q
**Serial:** S3PTNF0JB56391P
**Sector Size:** 512
**Available Sectors:** 2,042,000

Contents

**Contents:** Appears blank
**Partitions:** 0
**Filesystems:** 0
**Sectors Hidden By DCO:** 974,731,168

**Total Jobs:** 10
**Total Cases:** 0

IDE drives with a DCO require special considerations with TD4. DCO setting changes require power-cycling the drive which, for directly connected SATA drives, is done automatically by TD4. However, since IDE drive power can be provided in several ways, TD4 cannot deterministically cycle an IDE drive's power.

To disable a DCO on an IDE drive, ensure that the IDE drive (via TDA7-5) is the only connected source drive and then complete the following steps:

1. Tap **Remove Sector Limitations** from the source drive details screen and confirm that DCO removal is desired to start the task.
2. Tap **Eject** at the bottom-right of the drive details screen.
3. Remove power from the IDE drive.
4. Remove TDA7-5 from TD4.
5. Re-connect TDA7-5 (with IDE drive connected) to TD4.
6. Re-connect power to the IDE drive.

**Note:** Specifically for IDE drives connected via TDA7-5, the forensic log for a DCO/AMA removal job will report successful completion of the DCO removal operation immediately after the command has been issued to the drive. TD4 has no way of knowing if the command actually completed at the drive level. The DCO state should be manually verified after the reboot is complete and before subsequent jobs are started.

### 4.6.2.2 Wiping destination or accessory drives

The Wipe media utility provides six wipe types for destination and accessory drives. The table below provides detailed information on each type of supported wipe.

**Note:** If an HPA/DCO/AMA configuration is present on a drive that you intend to wipe and you want to wipe the entire drive (not just the exposed portion), select the Remove Sector Limitations function in the Reconfigure setup screen along with the Wipe function prior to starting the Reconfigure job.

**Caution**

Wiping drives results in sustained writing of the media, which can create abnormally high thermal operating conditions inside the drive. OpenText highly recommends using a fan or an external drive cooler when wiping media on TD4 to help prevent thermal damage to drives.

| Option | Description |
|---|---|
| Overwrite | Single Pass: TD4 will write a constant pattern (all zeros) to the drive in a single pass. Verification is optional.<br>Multiple Pass: TD4 performs three full write passes to the destination or accessory drive. The first pass writes zeros (0x0000) and the second pass writes ones (0xFFFF), and the third pass writes a randomly selected constant value between 0x0001 and 0xFFFE. Verification is optional. If enabled, it can be configured to verify after each wipe pass or after only the last pass. |
| Secure Erase<br>(SSD only) | The ATA Secure Erase command instructs the drive to reset all available blocks to the erase state. How the erase state is implemented on the drive is not mandated by the ATA specification, which means the final data state on drives is manufacturer dependent (and not necessarily all zeros). For drives that do not support Secure Erase, TD4 will indicate this limitation during wipe type selection.<br>Due to the indeterminate nature of the post-wipe data state, TD4 does not offer verification for Secure Erase wipes.<br>Due to known issues with inconsistent and unreliable Secure Erase support on rotating drives (HDDs), TD4 only supports this feature on SSDs.<br>Note that Secure Erase will erase all accessible drive space, but it will not necessarily erase over-provisioned space or other space reserved by the drive's internal controller.<br>TD4 will force removal of any detected HPA/DCO/AMA configurations prior to starting a Secure Erase wipe. |
| Sanitize - Block Erase<br>(SSD only) | The ATA and SCSI Sanitize – Block Erase commands instruct the drive to erase all flash memory blocks. This is typically done electrically, not through writing of data to the drive. While the state of post-wipe data is not mandated by the ATA/SCSI specifications, Sanitize – Block Erase typically leaves a drive in a cleared (all zeros) state, which allows for post-wipe verification. For drives that do not support Sanitize – Block Erase, TD4 will indicate this limitation during wipe type selection.<br>Note that Sanitize – Block Erase will erase all user accessible drive space as well as over-provisioned space and any other space reserved by the drive's internal controller.<br>TD4 will force removal of any detected HPA/DCO/AMA configurations prior to starting a Sanitize – Block Erase wipe. |

| Option | Description |
|---|---|
| Sanitize – Overwrite | The ATA and SCSI Sanitize – Overwrite command instructs the drive to overwrite all drive data in both storage and on-drive cache with zeros. This feature is typically implemented on HDDs but is available on some SSDs. For drives that do not support Sanitize – Overwrite, TD4 will indicate this limitation during wipe type selection.<br>Note that, for SSDs that support Sanitize – Overwrite, in addition to all user-accessible drive space, over-provisioned space and other space reserved by the drive's internal controller will also be erased.<br>TD4 will force removal of any detected HPA/DCO/AMA configurations prior to starting a Sanitize – Overwrite wipe. |
| NIST 800-88 R1 Clear | A NIST Clear wipe will perform an overwrite wipe with post-wipe verification. For USB drives it will perform three passes, and for all other drives it will perform one pass.<br>TD4 will force removal of any detected HPA/DCO/AMA configurations prior to starting a NIST 800-88 R1 Clear wipe.<br>For more details regarding NIST 800-88 R1 Clear, refer to *SP 800-88 r1: Guidelines for Media Sanitization* which is available on NIST's web site. |
| NIST 800-88 R1 Purge | A NIST Purge wipe is only possible if the drive supports certain wipe commands. For SSDs that support Sanitize - Block Erase, that method will be used with post-wipe verification. Otherwise, if a drive supports Sanitize – Overwrite (HDD or SSD), then that method will be used with post-wipe verification. Drives that do not support either of these commands cannot be NIST 800-88 R1 Purged, and TD4 will indicate this limitation during wipe type selection.<br>TD4 will force removal of any detected HPA/DCO/AMA configurations prior to starting a NIST 800-88 R1 Purge wipe.<br>For more details regarding NIST 800-88 R1 Purge, refer to *SP 800-88 r1: Guidelines for Media Sanitization* which is available on NIST's web site. |

**Note:** Secure Erase and Sanitize wipes have notable nuances, as follows:

- The exact differences between Secure Erase and Sanitize can be subtle, depending on the drive manufacturer's implementation. But, in general terms, Secure Erase is adequate for environments that are not concerned with removing any evidence of previous data in the physical memory chips. Secure Erase will guarantee that a typical host system read will return only wiped data, but someone with advanced capabilities to do chip-off memory structure analysis could theoretically discern previous data bit states. Sanitize is meant to cover situations that demand more secure data removal where advanced data retrieval techniques are of concern, with the downside of it taking much longer to complete.

- Secure Erase and Sanitize command requirements do not guarantee the final state of the data on wiped drives, which can result in wipe job failures that are out of TD4's control. From OpenText empirical testing over a large sample size of drives from different manufacturers, Secure Erase will reliably wipe drives in a very short period of time, but with a higher likelihood of a non-deterministic data state when complete, which makes reliable verification impossible. Sanitize has proven to be more reliable in clearing all data to zeros, which allows for post-wipe verification. If you experience Sanitize wipe verification failures, contact OpenText My Support at https://support.opentext.com to report the specific make and model of the drive, and the Tableau team will investigate.

#### 4.6.2.3 Encrypting destination and accessory drives

TD4 can encrypt destination and accessory drives using password-based XTS-AES whole disk encryption. This Tableau-based encryption is compatible with the OpenText Tableau Forensic TD2u Duplicator, OpenText Tableau Forensic TX1 Imager, and the open source VeraCrypt utility. Encryption can only be setup on destination and accessory drives as it requires a write modification to the drive.

**Caution**

The encryption process overwrites the destination/accessory drive, so remember to encrypt the destination drive before using it in a TD4 acquisition job.

To encrypt a drive attached to a TD4 destination or accessory port, select Encrypt from the Reconfigure option list. Enter the desired encryption password and then tap the **Start** button.

**Note:** TD4 supports auto-capitalization for text entry fields. This means that the first character in an entry will be capitalized, and subsequent character entries will be automatically switched to lower case. The exception is password entry fields. Auto-capitalization is disabled for password entry fields to avoid confusion and prevent incorrect password entries. It is recommended to double-check password entries by viewing them in plain text (using the eye icon at the end of the entry field) before submission.

A Tableau-encrypted destination or accessory drive can be unlocked with the password to allow browsing or imaging/restoring to the encrypted container.

A Tableau-encrypted source drive can be unlocked with the password to allow browsing or imaging/restoring of the drive’s unencrypted contents to a destination drive.

**Note:** OpenText is not able to recover lost passwords for TD4 encrypted media, so take appropriate steps to ensure you never lose your password.

To remove encryption from a drive, connect the drive to a TD4 destination or accessory port and then, without unlocking the encryption, wipe the drive.

**Note:** If a Tableau encrypted drive is unlocked prior to wiping, the encryption will remain intact and only the contents of the unlocked encryption container will be wiped. If clearing the encrypted state is desired, the drive's encryption must remain locked prior to initiating a wipe.

#### 4.6.2.4 Formatting destination and accessory drives

To perform an image duplication to or save logs to a drive, you must format the destination or accessory drive with a filesystem that is recognizable by TD4. TD4 supports formatting destination and accessory drives in the following filesystem formats: exFAT, NTSF, FAT, HFS+, EXT4, or No Filesystem.

**Note:** TD4 cannot format a drive with an APFS nor write to a drive with a pre-existing APFS. It will mount APFS formatted volumes as read-only on all TD4 ports (source, destination, and accessory). Such filesystems are not usable for any activities that require writing, even on destination and accessory ports.

exFAT is recommended for best compatibility when accessing drives with all modern operating systems. EXT4 is recommended for use with Linux forensic tools. HFS+ is recommended for use with MacOS forensic tools.

**Note:** When FAT is selected as the filesystem type for a destination drive format, TD4 will format the drive as FAT32. However, job logs (including the format log) and all user interface elements will simply show this as FAT. That is because TD4 supports reading from all FAT formats (12, 16, and 32) and simply identifying them all as FAT is considered acceptable and accurate for filesystem identification purposes.

The option to format a destination/accessory drive with No Filesystem is a special type of format. It provides an easy way to remove prior formatting on a drive with the specific purpose of making it easy to turn an image type Duplication job destination into a clone type. Because TD4 will automatically select the Duplication output type based on the existence of a mountable filesystem, this is the easiest way to get a clone destination onto a drive that has previously been formatted.

**Caution**

Formatting a drive with No Filesystem will make any prior formatting/data permanently unusable. While this is not equivalent to a full drive wipe, it will effectively wipe the drive in terms of being able to easily access its previous contents. Make sure to back up any important data on such a drive before formatting it with the No Filesystem option.

To format a destination or accessory drive, attach the drive to the desired TD4 port and then tap on the associated drive tile on the TD4 home screen. Tap the **Reconfigure** button in the Contents section of the drive details screen and then select the **Format** option. Select the desired filesystem type and then tap the **Start** button.

**Note:** OpenText strongly recommends not using FAT as a destination or accessory drive filesystem. On TD4, FAT filesystems are limited to a maximum output file size of 2GB and reading from or writing to them is known to be slower than other filesystem types. Also, FAT does not support drives over 2TB.

## 4.6.3 Encryption unlock

When a Tableau or Opal encrypted drive is attached to any TD4 port, the Unlock button in the Contents section of its drive details screen will be active. To unlock the encrypted drive, simply tap the Unlock button, enter the password, and tap Start. If the unlock operation was successful, the unencrypted drive contents will be available for use on TD4.

**Notes**

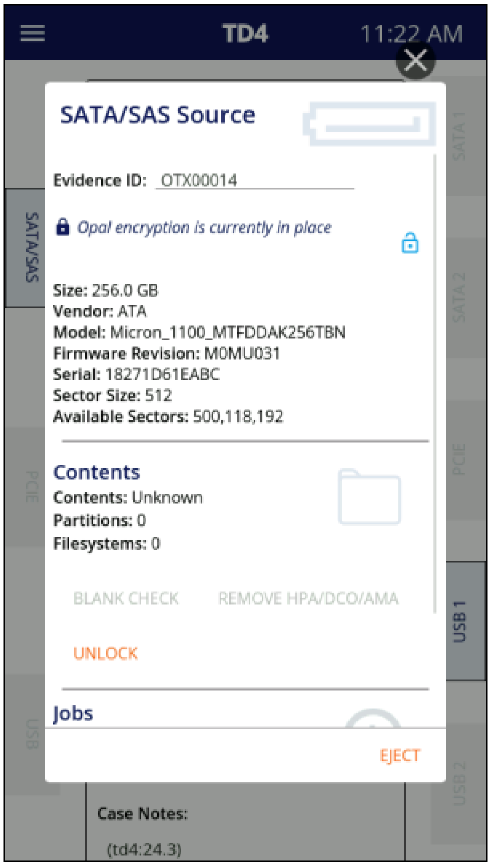
- An informative message will appear near the top of the drive details screen for any locked Tableau or Opal encrypted drives. A shortcut to the unlock media utility (blue padlock icon) is available to the right of that message, allowing easy access to the unlock function. This is in addition to the Unlock button in the Contents section of the drive details screen.
- Opal drives with an enabled Shadow MBR will be treated as locked, encrypted drives. That includes the ability to unlock the drive, which will do a volatile removal of the Shadow MBR and unlock the underlying Opal encryption. See “Opal encryption” on page 54 for more information on Opal encryption and Opal Shadow MBR.

## 4.6.4 Opal encryption

Opal encryption is a hardware-based encryption method that is managed by the controller on the drive with only minimal host system interaction. Opal is an industry standard created by the Trusted Computing Group (TCG) consortium that defines, among other things, the interface protocol to these types of hardware encrypted drives. These are commonly referred to as self-encrypting drives (SEDs) as the host system does little more than provide a front-end interface to manage the encryption. The control system on the drive is responsible for encrypting/ unencrypting all stored data on the drive and controlling access to it.

TD4 can detect Opal SEDs that have had their encryption enabled and will warn of the presence of Opal encryption in various places in the user interface and forensic logs. A detected locked Opal drive will have a red lock icon (with the lock closed) on the edge of its home screen drive tile. Such a drive will also include a warning message near the top of the drive details screen indicating that Opal encryption is currently in place, as shown in the screenshot below.

See “Encryption unlock” on page 54 for information regarding the unlocking of an Opal encrypted drive.



SATA/SAS Source

Evidence ID: OTX00014

*Opal encryption is currently in place*

Size: 256.0 GB
Vendor: ATA
Model: Micron_1100_MTFDDAK256TBN
Firmware Revision: M0MU031
Serial: 18271D61EABC
Sector Size: 512
Available Sectors: 500,118,192

Contents
Contents: Unknown
Partitions: 0
Filesystems: 0

Jobs

Case Notes:
(td4:24.3)

Note that Opal drives that have not had their encryption enabled will behave as regular, non-encrypted drives.

An additional consideration for Opal drives is a unique configuration that exposes a shadow MBR. This shadow MBR can be enabled by drive/system developers to expose a small portion of the drive as a non-encrypted container, which overrides the main drive information presented to the host. A typical use case for this configuration is to enable computer manufacturers to request credentials from a user before revealing the main portion of the drive. Regardless of the use case, it is important to be able to identify situations where only the shadow MBR is revealed, to make it clear that the entire drive contents are not being seen. TD4 will detect when an Opal shadow MBR is enabled and clearly inform of its presence. The lock icon will show in the affected drive tile on the home screen, and the presence of an Opal MBR will be explicitly called out in the drive details screen. TD4 can perform a volatile (temporary) removal of an Opal shadow MBR, which will expose the main portion of the drive to TD4 and allow for browsing and acquisition of its contents. This is done in the same manner as unlocking a locked Opal drive. See “Encryption unlock” on page 54 for more information.

**Caution**

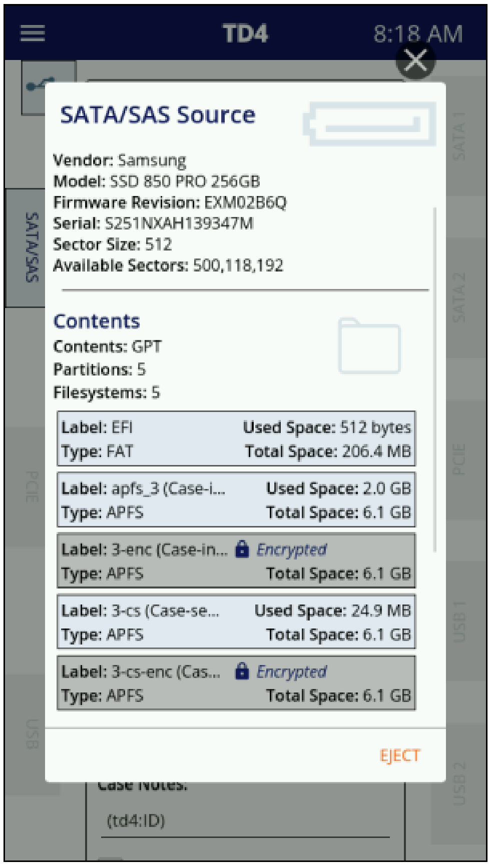
Docking station type devices that have Opal drives in them must support ATA command pass-through for TD4 to properly detect the presence of Opal encryption. Docking stations that do not support ATA command pass-through may present locked Opal media as all zeros with no indication of Opal encryption being present in the TD4 user interface. Use caution when acquiring any media via a docking station. If you suspect a drive in a docking station is Opal encrypted but is not being presented that way in the TD4 user interface, removing the drive from the enclosure and connecting it directly to TD4 may yield the desired outcome.

### 4.6.5 APFS and BitLocker encryption

TD4 can detect the presence of filesystems encrypted with Apple's APFS and Microsoft's BitLocker encryption. These encryption methods only apply to filesystems, which is distinct from full (or whole) disk encryption methods that are applied at the drive level, regardless of formatting. As a result, indicating the presence of APFS and BitLocker encryption on TD4 is done differently than the other detectable full disk encryption types (Tableau and Opal).

TD4 will show the presence of APFS and BitLocker encryption in the filesystem tiles shown on the drive details screen, as shown in the screenshots below.

**Note:** Unlike the other full disk encryption methods (Tableau and Opal), drives with APFS and BitLocker encrypted filesystems can be physically acquired (Duplication job) in their locked state, and then unlocked during subsequent investigative workflow steps using tools such as TD4.



SATA/SAS Source

**Vendor:** Samsung
**Model:** SSD 850 PRO 256GB
**Firmware Revision:** EXM02B6Q
**Serial:** S251NXAH139347M
**Sector Size:** 512
**Available Sectors:** 500,118,192

Contents

**Contents:** GPT
**Partitions:** 5
**Filesystems:** 5

**Label:** EFI **Used Space:** 512 bytes
**Type:** FAT **Total Space:** 206.4 MB

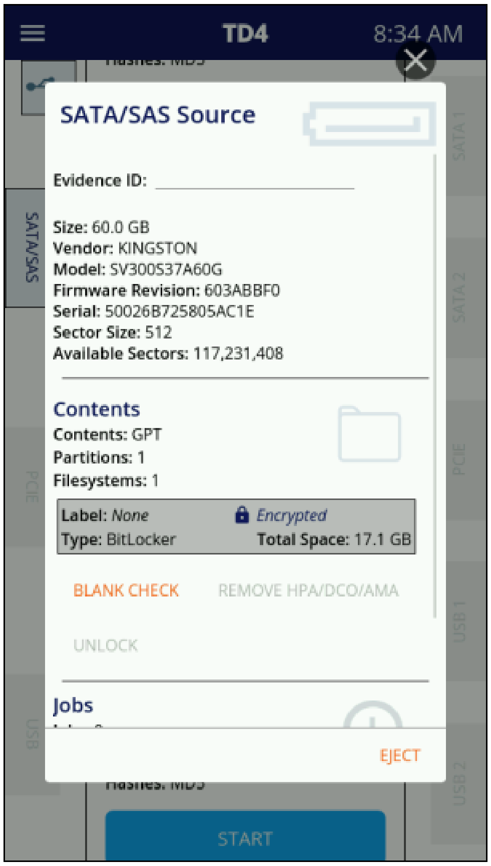
**Label:** apfs_3 (Case-i... **Used Space:** 2.0 GB
**Type:** APFS **Total Space:** 6.1 GB

**Label:** 3-enc (Case-in... 🔒 *Encrypted*
**Type:** APFS **Total Space:** 6.1 GB

**Label:** 3-cs (Case-se... **Used Space:** 24.9 MB
**Type:** APFS **Total Space:** 6.1 GB

**Label:** 3-cs-enc (Cas... 🔒 *Encrypted*
**Type:** APFS **Total Space:** 6.1 GB

Case Notes:
(td4:ID)



SATA/SAS Source

Evidence ID:

Size: 60.0 GB
Vendor: KINGSTON
Model: SV300S37A60G
Firmware Revision: 603ABBF0
Serial: 50026B725805AC1E
Sector Size: 512
Available Sectors: 117,231,408

Contents
Contents: GPT
Partitions: 1
Filesystems: 1

Label: *None* | *Encrypted*
Type: BitLocker | Total Space: 17.1 GB

BLANK CHECK REMOVE HPA/DCO/AMA

UNLOCK

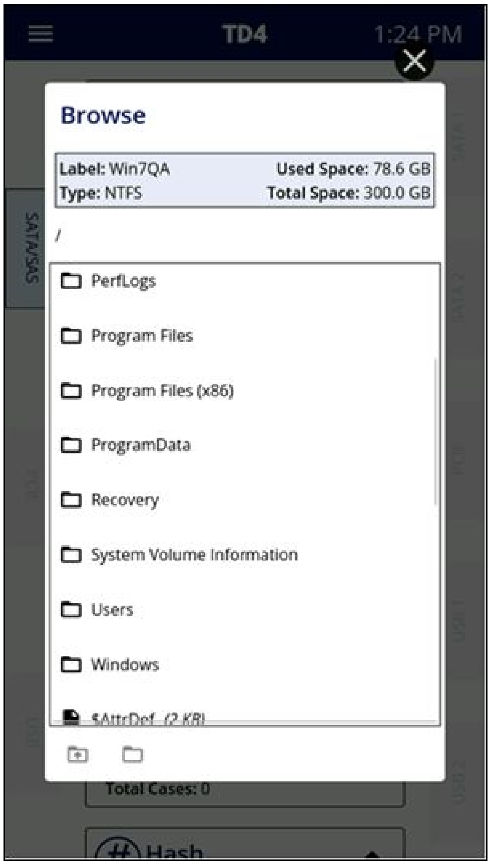
Jobs

EJECT

**Note:** Unlike the other full disk encryption methods (Tableau and Opal), drives with APFS and BitLocker encrypted filesystems can be physically acquired (Duplication job) in their locked state and then unlocked during subsequent investigative workflow steps using tools such as OpenText's OpenText Forensic.

## 4.7 Browsing

The browse function provides an easy way to view the contents of a mounted filesystem. To browse a filesystem, tap the desired drive tile from the home screen. The drive details screen for the selected drive will be displayed. For drives with at least one mounted filesystem, the Contents section of the drive details screen will show general information about the partition(s)/filesystem(s), and a filesystem card will be displayed showing key information for each filesystem. To browse a given filesystem, simply tap the filesystem card from the Contents section of the drive details screen, which will display a browse modal. A sample browse modal is shown below.



Label: Win7QA Used Space: 78.6 GB
Type: NTFS Total Space: 300.0 GB

/

- PerfLogs
- Program Files
- Program Files (x86)
- ProgramData
- Recovery
- System Volume Information
- Users
- Windows
- $AttrDef (2 KB)

Total Cases: 0

The top part of the browse window will show the filesystem information, followed by the current file path. The starting path location is always the root of the filesystem, as indicated by the forward slash (/) just above the filesystem contents section. That path information will be updated as folders are navigated to always indicate the current path.

In the browser portion of the screen, you can scroll up and down to view the list of directories and files. Scrolling right/left is also enabled if filenames are long and go off the screen. The size of each file is shown in parentheses at the end of the filename.

To open individual directories, double-tap the directory name or single-tap the directory to select, and then tap the open directory icon 🗀. Tap the up directory icon 🗀 to back out of a directory.

For destination and accessory drives, new directories can be created and directories/files can be deleted. To create a new directory, simply tap the create directory icon 🗀 and enter the new directory name. To delete a directory or file, single-tap the directory or file to select, and then tap the delete icon 🗑.

## 4.8 Case information

Case information is a key part of any digital investigation. When entered on TD4, case information will be displayed in key places throughout the user interface during job execution and captured in forensic logs. This allows easy correlation of key acquisition artifacts with specific cases throughout an investigation.

To enter case information, expand the Case Info function tile from the home screen. Tap each of the fields to enter the desired text. Note that text entry fields on TD4 are live. That means what you type will automatically be saved when you navigate away from the text entry field, with no need to explicitly save the new entry.

The following case information can be entered on TD4: Examiner Name, Case ID, and Case Notes.

At the bottom of the Case Info function tile is a selection box that will drive a prompt to enter Job Notes at the start of each job. When this box is checked, an advanced settings screen will appear before the start of each job that allows Job Notes to be entered. This allows for specific information about a particular piece of digital evidence to be entered and captured in the forensic log for each job.

## 4.9 Duplicating

TD4 will duplicate one source drive to up to five destination drives. Only one source may be connected at a time and thus only one forensic job can be run at a time. For a given job, the destinations can be a mix of cloned and imaged copies.

**Note:** This section is focused on whole-disk duplication operations, also known as physical imaging. See “Logical imaging” on page 71 for details on that alternative acquisition method.

Before starting any forensic job, TD4 automatically checks for preconditions. These preconditions are related to specific job setup parameters that could impact the ability of TD4 to execute the desired job. Some preconditions produce warnings that appear in the expanded function tile on the home screen. Some of those warnings require changes before being able to start the job, while others are informational and do not prevent the job from starting. For any precondition checks that may require changes, an advanced settings screen will appear after pressing the **Start** button to allow the appropriate settings to be adjusted before starting the job.

### 4.9.1 Cloning

A clone, also known as a disk-to-disk duplication, makes an exact copy of the source drive to the destination drive(s).

TD4 will automatically select clone for any destinations that have no detectable filesystems. If any such destinations are connected, an informational message will appear in the expanded Duplicate function tile on the home screen to indicate that those drives will be clones.

**Notes**

- The ⊙! icon indicates no detectable filesystems and will be shown next to the clone informational message in the expanded Duplicate function tile and on the left side of any applicable destination drive tiles. Those types of destination drives will always become a clone of the source drive.
- A destination drive that has a mountable filesystem will automatically be configured to receive an image file type output (E01, Ex01, dd, or dmg, depending on system settings) during a Duplication job. If you would instead like to create a clone on such a drive, you may either wipe the drive or format it with the No Filesystem format option prior to the start of the Duplication job. See “Formatting destination and accessory drives” on page 53 for more information on formatting a drive with No Filesystem.

It is best practice to wipe destination media before duplicating to it as a clone, as this can help to identify potentially defective media and bad sectors, and it can reduce the risk of cross-contaminating a clone duplication with stale data.

Note that, at the beginning of clone and restore jobs, TD4 prepares the destination drive by wiping sectors 0, 1, and end-of-drive minus 1. This ensures there is no stale partition table data on the drive, which reduces the possibility of drive detection issues at the end of the job.

**Note:** Because partition table information is relative to the sector size of the source drive, cloning to a destination drive with a different sector size is not allowed. TD4 will detect this sector size mismatch issue and warn the user. This condition will need to be rectified before the clone job can be started.

## 4.9.2 Imaging

An image, also known as disk-to-file duplication, copies the source drive to a series of files (sometimes called segments) on the destination drive. TD4 supports EnCase file formats Ex01 and E01 and raw file formats `dd` and `dmg`. For Ex01 and E01 output types, compression is supported and enabled by default.

**Note:** TD4 will automatically select image file as the output type for any destination drives that have a mountable filesystem. If you would instead like to create a clone on such a drive, you may either wipe the drive or format it with the No Filesystem format option prior to the start of the Duplication job. See "Formatting destination and accessory drives" on page 53 for more information on formatting a drive with No Filesystem.

For image file outputs, the maximum segment size can be set in system settings to any of the following: 2 GB, 4 GB, 8 GB, or Unlimited. Smaller segments create more segment files and Unlimited creates one large file segment.

**Note:** Not all image file size options are available in all situations. Due to filesystem addressing limitations, FAT32 formatted destinations have a maximum file size of 2 GB.

If the destination drive is smaller than the source, a `dd` or `dmg` image will not fit on the destination drive. However, if using Ex01 or E01, the source drive may fit on a smaller drive because these formats can compress the data before writing to the destination drive. There is no guarantee that the data will be compressed enough to fit on a smaller destination drive, especially in cases where the data is mostly incompressible such as encrypted data.

**Note:** Be careful when attempting to image a source drive to a same size or smaller destination drive, even if compression is enabled. Image file formatting adds overhead and, when coupled with incompressible data (such as encrypted data), a larger destination drive may be needed.

If the available filesystem space on a destination drive is the same size as or smaller than the source drive for an imaging job (Ex01 or E01 format), and compression is disabled, TD4 will prevent the job from being started. Enable compression and/or use a destination with more available filesystem space to be able to start such a job.

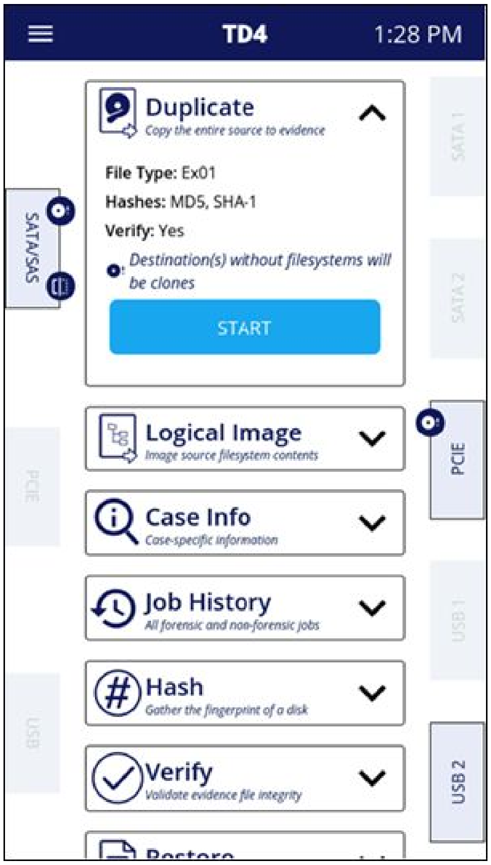
### 4.9.3 Performing a duplication

To perform a duplication:

1. Follow the steps listed in “Connecting drives” on page 27 to connect the source drive and destination drive(s).
2. Ensure that all destination drives are formatted according to the type of duplication job output desired for each drive. Destinations that have filesystems will automatically receive an image file type output according to the ‘Duplicate’ File Type system setting (Ex01, E01, DD, or DMG). Destinations that have no detectable filesystems will automatically receive a clone of the source drive.

   **Notes**

   - The ⊙! icon indicates no detectable filesystems and will be shown next to the clone informational message in the expanded Duplicate function tile and on the left side of any applicable destination drive tiles. Those types of destination drives will always become a clone of the source drive.
   - A destination drive that has a mountable filesystem will automatically be configured to receive an image file type output (E01, Ex01, dd, or dmg, depending on system settings). If you would instead like to create a clone on such a drive, you may either wipe the drive or format it with the No Filesystem format option prior to the start of the Duplication job. See the “Formatting destination and accessory drives” on page 53 for more information on formatting a drive with No Filesystem.
3. Expand the Duplicate function tile on the home screen. A summary of the main job settings will be shown along with any pertinent warning messages, as can be seen in the screenshot below. Verify the settings, resolve any blocking warnings, and then tap the **Start** button. If none of the settings are set to prompt and there are no other job configuration issues that need to be resolved, the job will start, and the job status screen will be displayed.


TD4
1:28 PM
Duplicate
Copy the entire source to evidence
SATA/SAS
SATA 1
SATA 2
PCIE
USB 1
USB 2
PCIE
USB
START
Logical Image
Image source filesystem contents
Case Info
Case-specific information
Job History
All forensic and non-forensic jobs
Hash
Gather the fingerprint of a disk
Verify
Validate evidence file integrity
Restore

**File Type:** Ex01

**Hashes:** MD5, SHA-1

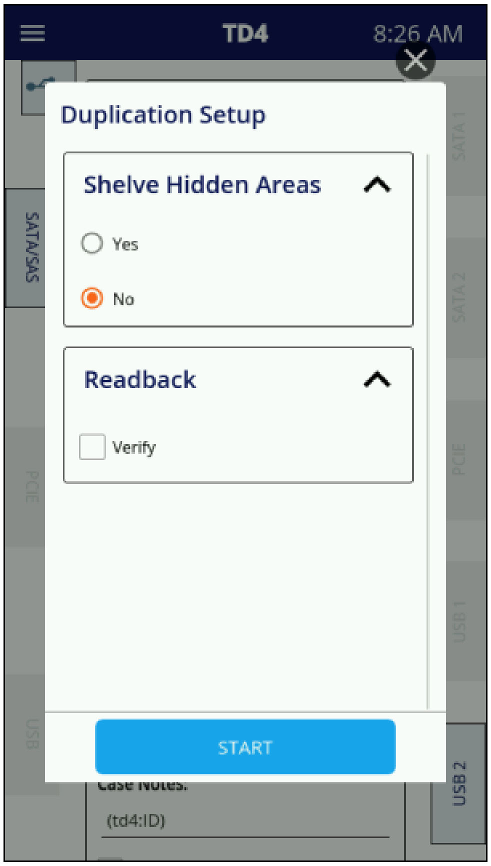
**Verify:** Yes

*Destination(s) without filesystems will be clones*

If any of the job settings are set to Prompt, the advanced settings screen will appear which will allow selection of the specific settings desired for the impending job. The Prompt option is available for the following system settings: Hashes, 'Duplicate' File Type, Readback Verification, and Trim Clones.

If there are any issues with the job setup/configuration that TD4 considers to be blocking or of forensic significance, the advanced settings screen will appear and provide information about the issue and the ability to rectify it, if possible. An example of a blocking configuration issue is if a SHA-256 hash is selected with E01 file type output. E01 does not support SHA-256 hashes.

The screenshot below is an example of the advanced settings screen for a Duplicate job with a Prompt setting (Readback Verification) and an issue of forensic significance (DCO present on source).



Duplication Setup

Shelve Hidden Areas

○ Yes

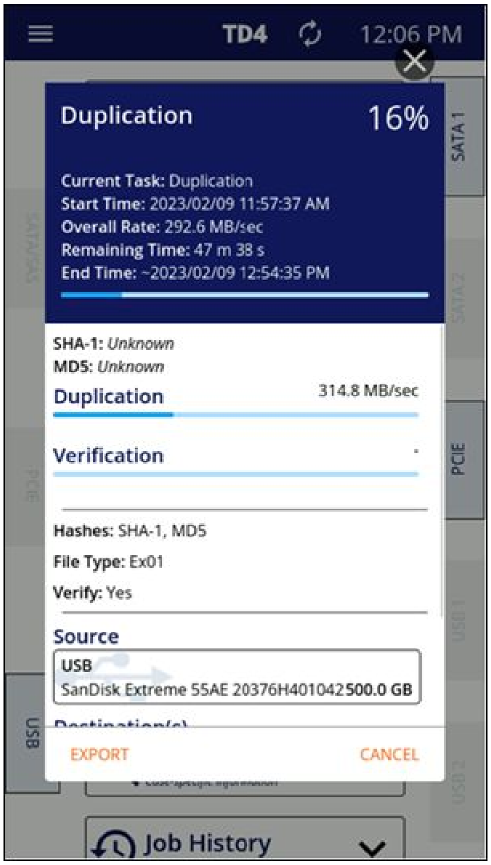
● No

Readback

□ Verify

Once all the advanced setup screen settings have been resolved/verified, tap the **Start** button to begin the Duplication job.

4. After a Duplication job is started, a job status screen will appear, as shown below.



Duplication 16%

Current Task: Duplication
Start Time: 2023/02/09 11:57:37 AM
Overall Rate: 292.6 MB/sec
Remaining Time: 47 m 38 s
End Time: ~2023/02/09 12:54:35 PM

SHA-1: *Unknown*
MD5: *Unknown*

Duplication 314.8 MB/sec

Verification

Hashes: SHA-1, MD5
File Type: Ex01
Verify: Yes

Source
USB
SanDisk Extreme 55AE 20376H401042 **500.0 GB**

You may cancel an active job by tapping **Cancel** in the bottom-right corner of the job status screen. You may also export the job log from this screen (even for in-progress jobs, if desired) by tapping the **Export** button in the bottom-left corner and then selecting the desired destination or accessory drive/filesystem.

The source and destination drives used in a job are shown near the bottom of the job status screen. These drive cards provide basic drive information, such as the connected port name, the overall size of the drive, and either the Evidence ID (if entered) or the drive's make/model/serial number.

**Note:** The drive cards in the job status screen can be tapped to show detailed drive information. However, when drive details are viewed from this area, the information is considered historical as of the start of the job, as indicated by date and time information in the top-right corner of the drive details screen. This means that changes to drive information during the job (such as reduced free space on the destination drive) will not be reflected and browsing of any mounted filesystems is disabled. To see a live version of the drive details and to be able to browse mounted filesystems (even during an active job), use the drive tiles on the home screen to access the drive details screens.

Icons will appear on the job status screen drive cards to provide at-a-glance indication of things like no detectable filesystem present ⊙, HPA/DCO/AMA in place ⦙, or the presence of certain types of encryption (locked or unlocked) 🔒.

**Note:** An easy way to tell which destination drives are getting which type of Duplication job output (clone or image) is to look for the ‘no filesystem’ icon ⊙ in the top-right area of the destination drive cards on the job status screen. Seeing that icon means that drive will be made a clone of the source drive.

### 4.9.4 Files created during disk-to-file duplication

When performing an image-based duplication job, TD4 creates files (sometimes called segments) on the destination drive that contain the data copied from the drive.

Segments are written to the destination drive according to the following convention (Ex01 output shown as an example):

```
[directory_name]/

[filename].Ex01

[filename].Ex02

.

.

.

[filename].Ex99

[filename].log.html

[filename].td4_packed_log
```

`[directory_name]` is defined in the Evidence File Path Directory setting. The default value is `/td4_images/%d_%t/`, where `%d` is the current date and `%t` is the current time at the start of the Duplication job.

`[filename]` is defined in the Evidence File Path Filename setting. The default value is `image`.

`[filename].Ex01` (or `.E01` or, for dd/dmg outputs, `.001`) is the first segment or portion of the data copied from the source drive. All other segments have sequential standard segment names (for example, [filename].Ex02, [filename].Ex03, and so on). Note that, for cancelled or failed jobs, there may also be a `[filename].Ex01.partial` file in the output directory.

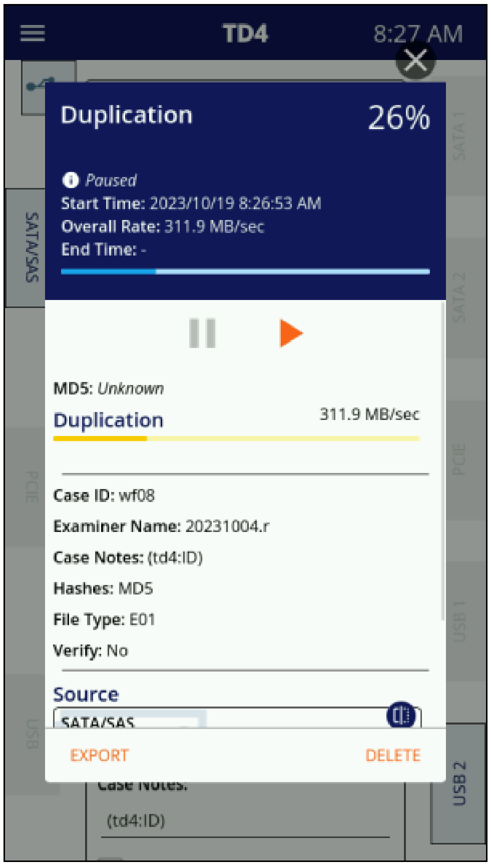
**Note:** The Max File Size system setting will determine the size of the output segment files. The options are 2GB, 4GB, 8GB, and Unlimited. The information above regarding segment file naming conventions applies to all but the Unlimited setting. For Unlimited, TD4 will capture all source drive data in one large segment file on each destination with an extension of .EX01, .E01, or, for dd/dmg, .001. Also, due to a FAT32 filesystem limitation, if any one of the destination drives is formatted as FAT32, all destinations will get 2GB segment files.

TD4 generates a `[filename].log.html` file for each image job. This is the forensic log for each job. It also creates a `[filename].TD4_packed_log` file, which can be used to do a standalone verification of the original image or to restore an image file to the original drive format.

### 4.9.5 Pausing and resuming a duplication job

In certain situations, significant amounts of imaging time can be saved by being able to pause and later resume a duplication job. And losing hours of imaging time due to an unexpected power loss can be frustrating and inefficient. TD4 has you covered, providing the means to pause and resume imaging jobs with the following output file formats: e01, ex01, dd, and dmg.

To pause a running duplication imaging job, simply tap the **Pause** button ⏸ near the top of the active job status screen and confirm your desire to pause the job. The job will be paused, as shown in the screenshot below.



Duplication 26%

*Paused*
Start Time: 2023/10/19 8:26:53 AM
Overall Rate: 311.9 MB/sec
End Time: -

MD5: *Unknown*
Duplication 311.9 MB/sec

Case ID: wf08
Examiner Name: 20231004.r
Case Notes: (td4:ID)
Hashes: MD5
File Type: E01
Verify: No

Source
SATA/SAS

To resume a paused job, tap the **Play** button ▶ near the top of the job status screen. If the job status screen of a paused job is not currently displayed, it can be re-displayed by tapping on the paused job in the Job History list.

**Note:** If an imaging job has been paused and a new Duplicate job is started, that new job will start from the beginning. To resume a previously paused job, you must locate the paused job in the Job History list and tap on it to display its job status screen before tapping the **Play** button.

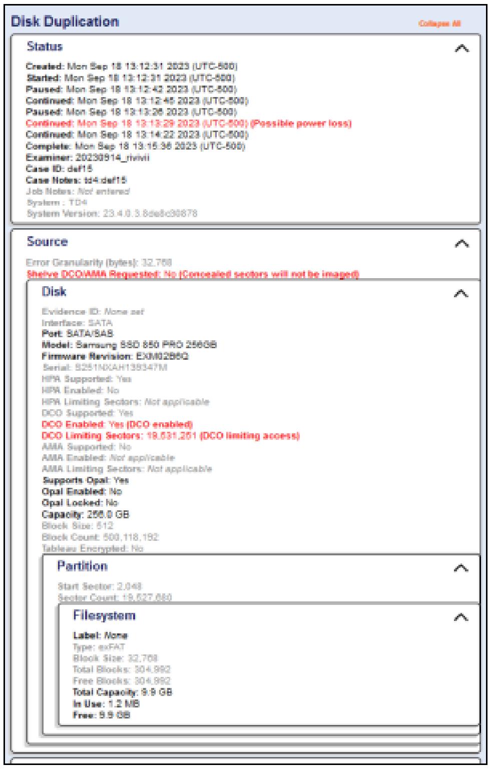
If the **Play** button is grayed out on the job status screen of a previously paused job, it likely means that the job conditions are not the same as before the pause. This can include obvious conditions like the original source and destination drives not being present. Another possible reason for an inactive **Play** button is if the destination is full-disk encrypted and the unit was power cycled after the initial pause, and the encryption was not unlocked after the subsequent power up. In general, check to make sure that the job conditions are exactly the same prior to attempting to resume a previously paused job.

TD4 also supports resuming a job after a power loss. For the supported job types (E01, Ex01,dd, dmg), if power is unexpectedly lost during an imaging job (including manual shut down from power button long press), it can be resumed after power is restored. To resume a job after a power loss event, make sure the original drives are connected to TD4 before turning it back on. Then locate the paused job in the Job History screen. Note that paused jobs will show with a partially completed blue status bar and the pause icon. Tap on the paused job to view its job status screen, and then tap on the **Play** button to resume the job.

For specific types of Duplication job failures, it is possible to resume the job after the failure condition has been resolved. The job failures that may allow for job resumption are as follows:

- **Source or destination drive disconnected –** This can happen if the drive interface cable is inadvertently disconnected or if the cable is going bad and showing intermittent failures. Once the drive is reconnected or the intermittent cable is replaced, the job can be resumed.
- **Destination drive full –** If during a Duplication imaging job the destination drive becomes full, the job will fail. If there are files on that drive unrelated to the current/failed job that could be saved off and then deleted, then that drive can be used to resume the failed job.

The forensic logs for paused and resumed jobs will provide some specific and unique information. The information differs slightly depending on the source of the pause event (manually/failure initiated or power loss). In the case of a manual or failure initiated pause event, a line will be added to the log to indicate the date and time of the event. Each subsequent pause (if manually/failure initiated) and resume event is logged, providing an accurate capture of how many pause/resume cycles occurred during the job. When unexpected power loss is the cause of the pause, there is no time for the system to log the pause time before shutting down, so that information is unavailable and thus not included in the log. In that case, a message is added to the log after the job is resumed to indicate that the missing pause information is likely due to a power loss event, and the job's elapsed time is not calculated, since it cannot be accurately determined. The following log sample shows a completed power loss paused/resumed job. Note that, had this been a manually paused/resumed job, the line with the possible power loss warning would be replaced by a **Paused** field, with the date and time of the pause event.



Status

Created: Mon Sep 18 13:12:31 2023 (UTC-500)
Started: Mon Sep 18 13:12:31 2023 (UTC-500)
Paused: Mon Sep 18 13:12:42 2023 (UTC-500)
Continued: Mon Sep 18 13:12:45 2023 (UTC-500)
Paused: Mon Sep 18 13:13:26 2023 (UTC-500)
Continued: Mon Sep 18 13:13:29 2023 (UTC-500) (Possible power loss)
Continued: Mon Sep 18 13:14:22 2023 (UTC-500)
Complete: Mon Sep 18 13:15:36 2023 (UTC-500)
Examiner: 20230914_rivivii
Case ID: def15
Case Notes: td4:def15
Job Notes: *Not entered*
System : TD4
System Version: 23.4.0.3.8de8c30878

Source

Error Granularity (bytes): 32,768
Shelve DCO/AMA Requested: No (Concealed sectors will not be imaged)

Disk

Evidence ID: *None set*
Interface: SATA
Port: SATA/SAS
Model: Samsung SSD 850 PRO 256GB
Firmware Revision: EXM02B6Q
Serial: S251NXAH138347M
HPA Supported: Yes
HPA Enabled: No
HPA Limiting Sectors: *Not applicable*
DCO Supported: Yes
DCO Enabled: Yes (DCO enabled)
DCO Limiting Sectors: 18,631,251 (DCO limiting access)
AMA Supported: No
AMA Enabled: *Not applicable*
AMA Limiting Sectors: *Not applicable*
Supports Opal: Yes
Opal Enabled: No
Opal Locked: No
Capacity: 256.0 GB
Block Size: 512
Block Count: 500,118,192
Tableau Encrypted: No

Partition

Start Sector: 2,048
Sector Count: 19,527,680

Filesystem

Label: None
Type: exFAT
Block Size: 32,768
Total Blocks: 304,992
Free Blocks: 304,992
Total Capacity: 9.9 GB
In Use: 1.2 MB
Free: 9.9 GB

## 4.10 Logical imaging

TD4 provides the ability to logically image source drive folders and files from detectable filesystems. When used in conjunction with physical disk imaging, logical imaging enables rapid acquisition of source file data, providing TD4 users the ability to balance thoroughness with acquisition time and effort for the demands of a given case.

TD4 logical imaging jobs will create industry standard Lx01 logical evidence files, which are compatible with EnCase Forensic and other common digital forensics investigation tools. Each logical imaging job will also create a forensic log file, with a file extension of `.log.html`. For details on all logical imaging output files, see “Files created during a logical image job” on page 76.

TD4 logical imaging acquires all files/folders on the source filesystem with no opportunity to down select or target specific files/folders as is possible on TX1. TD4 logical imaging is still considered a valuable option for time-sensitive situations where acquiring a full physical image of the drive is not possible or to get a jump on file analysis/triage while a secondary physical image is being acquired.

Due to the fact that source file data compressibility is not determined prior to starting a logical imaging job, it is not possible to determine with certainty if the data from a source filesystem will fit on a destination filesystem. As a result, TD4 only warns the user that a destination may be too small when the used space of the source filesystem is larger than the available space on the destination, and the job can still be started. However, if the source data is highly incompressible (or if compression is disabled), it is possible for the destination filesystem to become full, thus causing the job to fail.

**Note:** Use caution when attempting to logically image from a source filesystem to a smaller destination filesystem. If the source data is not compressible, the job may fail due to lack of space on the destination.

Unlike a physical duplication job, the option of shelving a source drive DCO/AMA (removing it and then re-applying it at the end of the job) does not exist in logical imaging. The existence of a DCO or AMA will be obvious (per warnings in multiple locations), but the DCO/AMA will need to be permanently removed using the Remove HPA/DCO/AMA utility before gaining access to all portions of the source media.

Filesystem read errors encountered during logical imaging jobs may result in unpredictable acquisition behavior. When they occur, such errors are indicated by a red warning message at the top of the Logical Image progress section of the job status screen. TD4 will skip any file that results in a read error and will attempt to read any remaining files. The CSV output will show an error status for any files that were not acquired. If you encounter filesystem read errors during a logical imaging job, we recommend that you clone or physically image the drive (e01, ex01, dd, dmg) instead of trying to do a logical image.

### 4.10.1 Performing a logical image

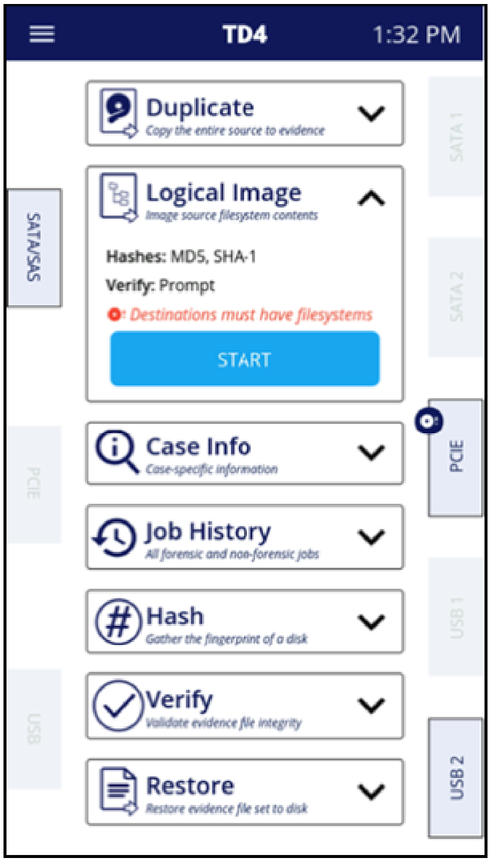
To perform a logical image:

1. Follow the steps listed in "Connecting drives" on page 27 to connect the source and destination drives.
2. Ensure that all destination drives have at least one mountable filesystem. Destinations that have mounted filesystems will receive an Lx01 image file output. Destinations that have no detectable filesystems will not receive any outputs from a Logical Image job.

   **Note:** Each destination drive used in a Logical Image job must have a filesystem to store the resulting acquisition output files. If any of the attached destination drives do not have a detectable filesystem, a warning message will appear above the **Start** button indicating that destinations must have filesystems. If there is at least one destination drive with a filesystem, the Logical Image job may still be started, but only the destinations that have mounted filesystems will receive the output evidence files.

3. Expand the Logical Image function tile on the home screen. A summary of the main job settings will be shown along with any pertinent warning messages as can be seen in the screenshot below. Verify the settings, resolve any blocking warnings, and then tap the Start button. If none of the settings are set to prompt

and there are no other job configuration issues that need to be resolved, the job will start, and the job status screen will be displayed.


TD4
1:32 PM
Duplicate
Copy the entire source to evidence
Logical Image
Image source filesystem contents

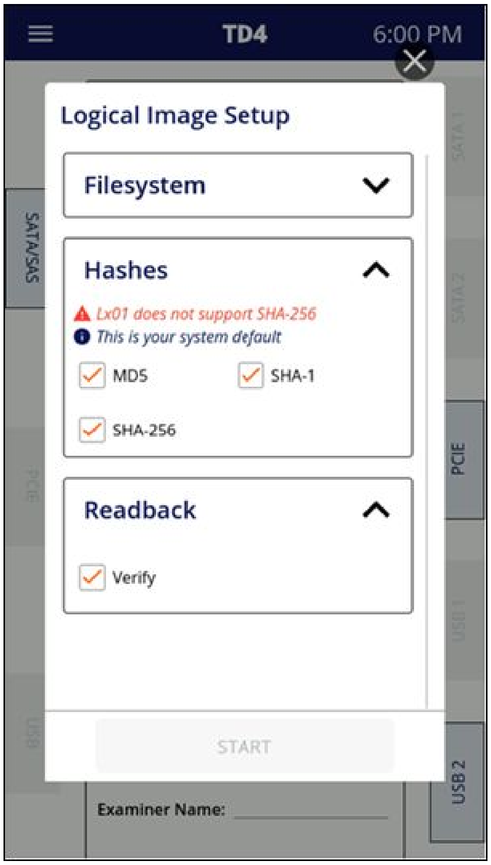
Hashes: MD5, SHA-1
Verify: Prompt
Destinations must have filesystems

START
Case Info
Case-specific information
Job History
All forensic and non-forensic jobs
Hash
Gather the fingerprint of a disk
Verify
Validate evidence file integrity
Restore
Restore evidence file set to disk
SATA/SAS
PCIE
USB
SATA 1
SATA 2
PCIE
USB 1
USB 2

If any of the job settings are set to Prompt, an advanced settings screen will appear which will allow selection of the specific settings desired for the impending job. The Prompt option is available for the following system settings related to Logical Imaging: Hashes and Readback Verification.

If there are any issues with the Logical Image job setup/configuration that TD4 considers to be blocking or of forensic significance, an advanced settings screen will appear and provide information about the issue and the ability to rectify it, if possible. An example of a blocking configuration issue is if SHA-256 is selected in system settings. LX01 does not support SHA-256 hashing.

The screenshot below is an example of the advanced settings screen for a Logical Image job with a Prompt setting (Readback Verification) and an issue of forensic significance (SHA-256 selected). Note that the items that directly caused the advanced settings screen to be displayed are shown as expanded but that other, potentially related setting items will also appear in that screen unexpanded.



Logical Image Setup

Filesystem

Hashes

*Lx01 does not support SHA-256*

*This is your system default*

☑ MD5 ☑ SHA-1

☑ SHA-256

Readback

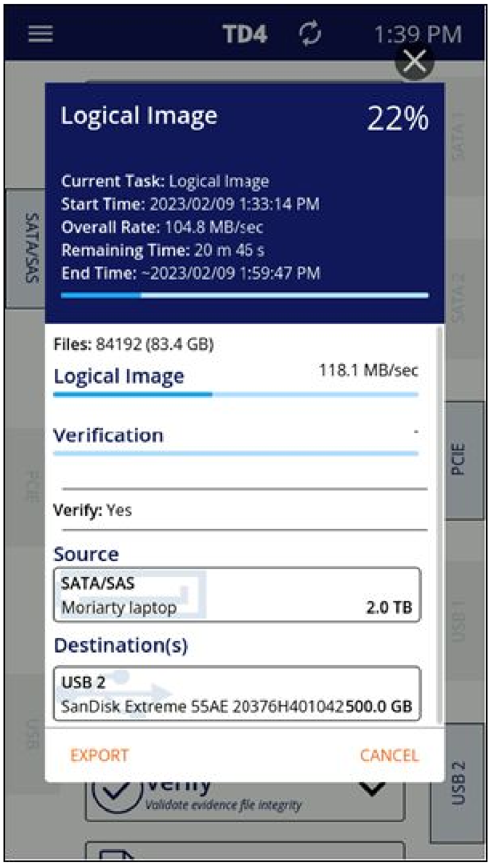
☑ Verify

Examiner Name:

Once all the advanced settings screen settings have been resolved/verified, tap the **Start** button to begin the Logical Image job.

**Note:** As indicated by the informative message in the screenshot above (“This is your system default”), whenever a setting is changed in an advanced settings screen as part of the setup for a specific job, that is equivalent to changing that setting in the main Settings menu.

4. After a Logical Image job is started, its job status screen will appear, as shown below.



Logical Image 22%

**Current Task:** Logical Image
**Start Time:** 2023/02/09 1:33:14 PM
**Overall Rate:** 104.8 MB/sec
**Remaining Time:** 20 m 46 s
**End Time:** ~2023/02/09 1:59:47 PM

**Files:** 84192 (83.4 GB)

Logical Image 118.1 MB/sec

Verification -

**Verify:** Yes

Source

SATA/SAS
Moriarty laptop 2.0 TB

Destination(s)

USB 2
SanDisk Extreme 55AE 20376H401042 500.0 GB

EXPORT CANCEL

The number of files found on the source filesystem along with the total size of those files is shown just under the header section of the job status screen, above the Logical Image progress bar. Note that TD4 logical imaging acquires all files/folders on the source filesystem with no opportunity to down select or target specific files/folders as is possible on TD4.

You may cancel an active Logical Image job by tapping **Cancel** in the bottom-right corner of the job status screen. You may also Export the job log from this screen (even for an in-progress job, if desired) by tapping the **Export** button in the bottom-left corner and then selecting the desired destination or accessory drive/filesystem.

The source and destination drives used in a Logical Image job are shown near the bottom of the job status screen. These drive cards provide basic drive information, such as the connected port name, the overall size of the drive, and either the Evidence ID (if entered) or the drive's make/model/serial number. Icons will appear on these drive cards to provide at-a-glance indication of things like no detectable filesystem present ⊙!, HPA/DCO/AMA in place [|, or the presence of certain types of encryption (locked or unlocked) 🔒.

**Note:** The drive cards in the job status screen can be tapped to show detailed drive information. However, when drive details are viewed from this area, the information is considered historical as of the start of the job, as indicated by date and time information in the top-right corner of the drive details screen. This means that changes to drive information during the job (such as reduced free space on the destination drive) will not be reflected and browsing of any mounted filesystems is disabled. To see a live version of the drive details and to be able to browse mounted filesystems (even during an active job), use the drive tiles on the home screen to access the drive details screens.

### 4.10.2 Files created during a logical image job

When performing a logical image on TD4, multiple different files may be output to each destination depending on the job configuration, as follows:

- `{image_name}.Lx01`, `{image_name}.Lx02`, etc. are the forensic evidence files for the operation. They contain all the data and metadata for each file and folder acquired.
- `{image_name}.csv` is a comma-separated values file that contains certain metadata for every file and folder acquired. This type of file can easily be imported into many common data processing applications such as Microsoft Excel. CSV file data contents and format information can be found in “Source file metadata” on page 76.
- `{image_name}.log.html` contains the forensic log of the logical imaging job.
- `{image_name}.TD4_packed_log` contains a TD4 readable copy of the forensic log that can later be used for standalone verification of the Lx01 file set.

### 4.10.3 Logical image verification

Verification of Lx01 files differs from verification of physical imaging operations because, in an Lx01 file, there is no overall hash. Each file's data stored in the Lx01 has an associated hash that was calculated during the original acquisition. The logical imaging verification function reads back the file data from the Lx01 on the destination, calculates a new hash value for each file, and compares that hash value to the originally stored acquisition hash value. A failure of any one file to match the original acquisition hash value will result in a verification failure.

### 4.10.4 Source file metadata

Logical imaging with TD4 includes source file metadata in the CSV output file, as shown in the table below.

| Column | Content |
|---|---|
| Path | Contains the full, filesystem-relative path for this entry. Example: /users/charles/pictures. |
| Type | Either contains “Directory,”“Symlink,” or “File,” depending on what kind of entry this row represents. |

| Column | Content |
|---|---|
| Filesize | The file size, in bytes, of the entry. This field is empty for directories. |
| Creation Date | The IS0 8601 UTC date/time string for the creation date of this entry. This field is empty if the creation date is unavailable. |
| Accessed Date | The IS0 8601 UTC date/time string for the accessed date of this entry. This field is empty if the accessed date is unavailable. |
| Modified Date | The IS0 8601 UTC date/time string for the modified date of this entry. This field is empty if the modified date is unavailable. |
| Written Date | The IS0 8601 UTC date/time string for the written date of this entry. This field is empty if the written date is unavailable. |
| MD5 Hash | The MD5 Hash of the entry. This field is empty for directories. It is also empty if no MD5 hash was calculated, no MD5 hash was configured, or the entry did not match the rules for acquisition. |
| SHA1 Hash | The SHA1 Hash of the entry. This field is empty for directories. It is also empty if no SHA1 hash was calculated, no SHA1 hash was configured, or the entry did not match the rules for acquisition. |
| File Status | OK if there were no problems reading file data/metadata.<br>ERRORS if there were errors reading file data and/or metadata.<br>This field is empty for directories. |
| Matched Rules | "Y"if the file matched the acquisition's rules for inclusion. For TD4, this will always show a match as file/folder down selection/filtering is not supported. |

## 4.11 Hashing

Forensic practitioners may need to calculate the hash values, or fingerprints, for a source drive without making a copy of the drive. The Hash function can generate MD5, SHA-1, and SHA-256 hash values for a source drive, as determined by the Hashes system setting.

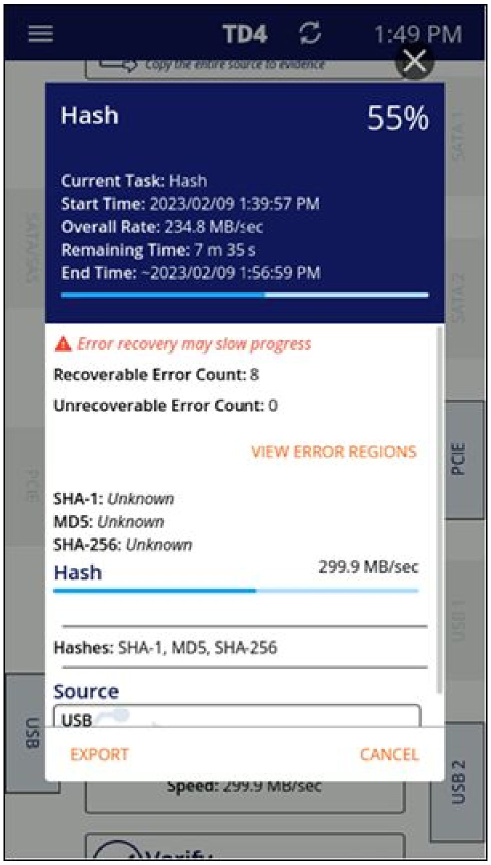
1. Follow the steps listed in "Connecting drives" on page 27 to connect the desired source drive.

   **Note:** Since TD4 only allows one source drive to be used for any job, connect only the desired hash source drive and ensure no other source drives are attached. If any other source drives are attached, a warning will be provided in the Hash function tile and the **Start** button will be inactive (grayed out).

2. Expand the Hash function tile on the home screen. A summary of the pertinent job settings will be shown along with any applicable warning messages. Verify the settings, resolve any blocking warnings, and then tap the **Start** button. If none of the settings are set to Prompt and there are no other job configuration issues that need to be resolved, the job will start, and the job status screen will be displayed.

If the Hash system setting is set to Prompt, an advanced settings screen will appear which will allow selection of the hash types for the job. Select the desired hash types and then tap the Start button to begin the Hash job.

3. After the Hash job is started, the job status screen will appear, as shown below.



Hash 55%

Current Task: Hash
Start Time: 2023/02/09 1:39:57 PM
Overall Rate: 234.8 MB/sec
Remaining Time: 7 m 35 s
End Time: ~2023/02/09 1:56:59 PM

⚠ *Error recovery may slow progress*
Recoverable Error Count: 8
Unrecoverable Error Count: 0

SHA-1: *Unknown*
MD5: *Unknown*
SHA-256: *Unknown*
Hash 299.9 MB/sec

Hashes: SHA-1, MD5, SHA-256

Source
USB

You may cancel an active Hash job by tapping **Cancel** in the bottom-right corner of the job status screen. You may also export the job log from this screen (even for an in-progress job, if desired) by tapping the **Export** button in the bottom-left corner and then selecting the desired destination or accessory drive/filesystem.

The source drive used in the Hash job will be shown near the bottom of the job status screen. This drive card provides basic drive information, such as the connected port name, the overall size of the drive, and either the Evidence ID (if entered) or the drive’s make/model/serial number. Icons will appear on these drive cards to provide at-a-glance indication of things like no detectable filesystem present ⊙!, HPA/DCO/AMA in place [⁞, or the presence of certain types of encryption (locked or unlocked) 🔒.

**Note:** The drive cards in the job status screen can be tapped to show detailed drive information. However, when drive details are viewed from this area, the information is considered historical as of the start of the job, as indicated by date/time information in the top-right corner of the drive details screen. To see a live version of the drive details and to be able to browse mounted filesystems, use the drive tiles on the home screen to access the drive details screen.

## 4.12 Verifying

The standalone Verify function verifies the integrity of an existing image file by reading back the data from the image file, calculating a hash value of that data, and then comparing that calculated hash value with the value of the original acquisition hash.

Note that, while the same Verify function can be used for standalone verification of physical and logical images, the underlying mechanism is different. This is because physical images contain whole disk acquisition hash values and logical images contain file-based acquisition hash values. No difference will be noticed during the verification job itself, but the source image type will make a difference in how the results are reported. For a physical image verification job, the drive-level readback hash values will be reported in the forensic log. For a logical image verification job, a simple pass/fail indication will be reported in the forensic log. A pass indicates that all the file-based verification hashes match the original acquisition file hashes. If any individual file in a logical image file fails to verify, the entire verification job will show as failed.

1. Follow the steps listed in "Connecting drives" on page 27 to connect the desired destination drive.

   **Note:** Verification jobs use only destination or accessory drives as the source of the verification inputs.

2. Expand the Verify function tile on the home screen, and then tap the **Start** button.
3. In the advanced settings screen, tap the **Select a log file** button to launch a browse modal. Browse to the appropriate destination/accessory drive and filesystem, locate the desired `.td4_packed_log` file, and select that file by tapping it once. Then tap the **Select** button.

   **Note:** When browsing for packed log files, only files with an extension of `.td4_packed_log` will be shown in the browse window.

4. Review the selected filesystem and file path information, and, if accurate, tap the **Start** button to begin the verification job. The Verify job status screen will appear.

   You may cancel an active Verify job by tapping **Cancel** in the bottom-right corner of the job status screen. You may also Export the job log from this screen (even for an in-progress job, if desired) by tapping the **Export** button in the bottom-left corner and then selecting the desired destination or accessory drive/ filesystem.

The drive used in the Verification job will be shown near the bottom of the job status screen. This drive card provides basic drive information, such as the connected port name, the overall size of the drive, and either the Evidence ID (if entered) or the drive's make/model/serial number. Icons will appear on these drive cards to provide at-a-glance indication of things like no detectable filesystem present ⊙!, HPA/DCO/AMA in place [⁞, or the presence of certain types of encryption (locked or unlocked) 🔒.

**Note:** The drive cards in the job status screen can be tapped to show detailed drive information. However, when drive details are viewed from this area, the information is considered historical as of the start of the job, as indicated by the date and time information in the top-right corner of the drive details screen. To see a live version of the drive details and to be able to browse mounted filesystems, use the drive tiles on the home screen to access the drive details screen.

## 4.13 Restoring

The Restore function allows for recreation of the original drive format from a previously created TD4 forensic image file. The uses for this feature are varied but include the ability to use a restored drive as a system boot disk and to simply create an archival copy of the evidence in its original format for future case reference.

The Restore function works with all physical duplication image file types (E01, Ex01, dd, dmg). It does not support restoration from a logical image file set (Lx01).

It is best practice to wipe destination media before restoring to it as this can help to identify potentially defective media and bad sectors, and it can reduce the risk of cross-contaminating a restored drive with stale data.

Note that, at the beginning of a Restore job, TD4 prepares the destination drive by wiping sectors 0, 1, and end-of-drive minus 1. This ensures there is no stale partition table data on the drive which reduces the possibility of drive detection issues at the end of the job.

**Note:** Because partition table information is relative to the sector size of the source drive, restoring to a destination drive with a different sector size is not allowed. TD4 will detect this sector size mismatch issue and warn the user. This condition will need to be rectified before the Restore job can be started.

To restore a drive from an image file:

1. Follow the steps listed in "Connecting drives" on page 27 to connect the desired source and destination drives.

   **Note:** Restore jobs use source drives as the source of the input files (packed log file and image segment files). Also, a Restore job will effectively wipe any destination drives that are attached/detected at the time the job is started. Make sure none of your destinations have critical files on them before starting a Restore job.

2. Expand the Restore function tile on the home screen, and then tap the **Start** button. The Restore Setup screen will appear.

3. In the Restore Setup screen, tap the **Select a log file** button to launch a browse modal. Browse to the appropriate source drive/filesystem, locate the desired *.td4_packed_log* file (the one from which you want to restore), and select that file by tapping it once. Then tap the **Select** button.

   **Note:** When browsing for packed log files, only files with an extension of `.td4_packed_log` will be shown in the browse window.

4. Review the selected filesystem and file path information, verify any other settings in the Restore Setup screen, and, if everything is set properly, tap the **Start** button to begin the Restore job. The Restore job status screen will appear.

   **Notes**

   - During the Restore job, hashes are calculated as data is extracted from the source evidence file set and written out to the destination. These hashes are considered source hashes and are thus captured in the source section of the Restore job's forensic log. Even if Readback Verification is not enabled for the Restore job, these source hashes are compared to the original physical image acquisition hashes and, if a mismatch is detected, the Restore job will fail.

   - If Readback Verification is enabled for a Restore job, the portion of the destination drive that was written out during the Restore (which matches the size of the original source drive) will be read back, and readback hash values will be calculated and compared to the source hashes. If a mismatch is detected, the verification portion of the Restore job will fail. These readback hashes are captured in the destination section of the Restore job's forensic log. Note that if the readback hash values matched the source hash values, they will be considered lower priority pieces of data in the HTML forensic logs and thus hidden by default. These hashes can be viewed by expanding the destination drive section(s) of the forensic log.

## 4.14 Forensic logs

TD4 generates a detailed log for all forensic jobs and most media utility operations. The information captured during each job is used to create both the job status screens seen in the user interface (available from the Job History list) and the forensic job logs that can be exported to an external drive. This section is specific to the exported forensic logs. For information on the Job History list and job status screens, see “Job history” on page 37 and “Job status” on page 36.

The detailed information captured in the forensic logs will depend on the job type. A summary of the information captured for an image-based duplication job is shown below. See the sample logs at the end of this section for some specific job log examples.

- **Status**: Overall job status (Incomplete, Ok, Error/Failed, Canceled), date/time stamps, identification of TD4 as the acquisition system, and the firmware version in use at the time of the acquisition. The following pieces of optional information will also be included in this section: Examiner name, Case ID, Case Notes, and Job Notes.
- **Source**: Source drive details, including overall drive information (Evidence ID (if set), interface type, TD4 port, make/model number, firmware version, serial number(s), protocol specific details (e.g., SCSI/USB info), HPA/DCO/AMA related information, RAID and encryption information, size/layout information, and the partition table type), partition details, and, if present and supported by TD4, filesystem specific information.
- **Acquisition Results**: Details about the acquisition aspects of the job, including block start and count numbers, acquisition hash values, and read error information.
- **Configuration**: Job configuration information, such as the output file format type, segment file size, and whether or not compression was enabled.
- **Image Destination**: Destination drive details, including readback verification hash values (if enabled for the job), overall drive information (interface type, TD4 port, make/model number, firmware version, serial number(s), protocol specific details (e.g., SCSI/USB info), HPA/DCO/AMA related information, RAID and encryption information, size/layout information, and the partition table type), partition details, and filesystem specific information.
- **Failure Summary**: If a failure occurred during the job, this section will be shown and will include a failure reason and code. Note that the failure code is not intended to be meaningful to the end user. In cases where customer support is required to resolve a job failure situation, the failure code should be noted and included in the incident report. This information will help in determining the root cause of the failure.

To access the job logs stored on your TD4, expand the Job History function tile on the home screen and then tap in the lower portion of the function tile. A list of all the jobs stored on the unit will be displayed. Tapping on a job will display its job status screen. Note that you cannot open and view forensic logs files directly on TD4. job status screens show the key information about the job, but the job log will need to be exported to a destination or accessory drive to be able to view the forensic log file on a separate computer.

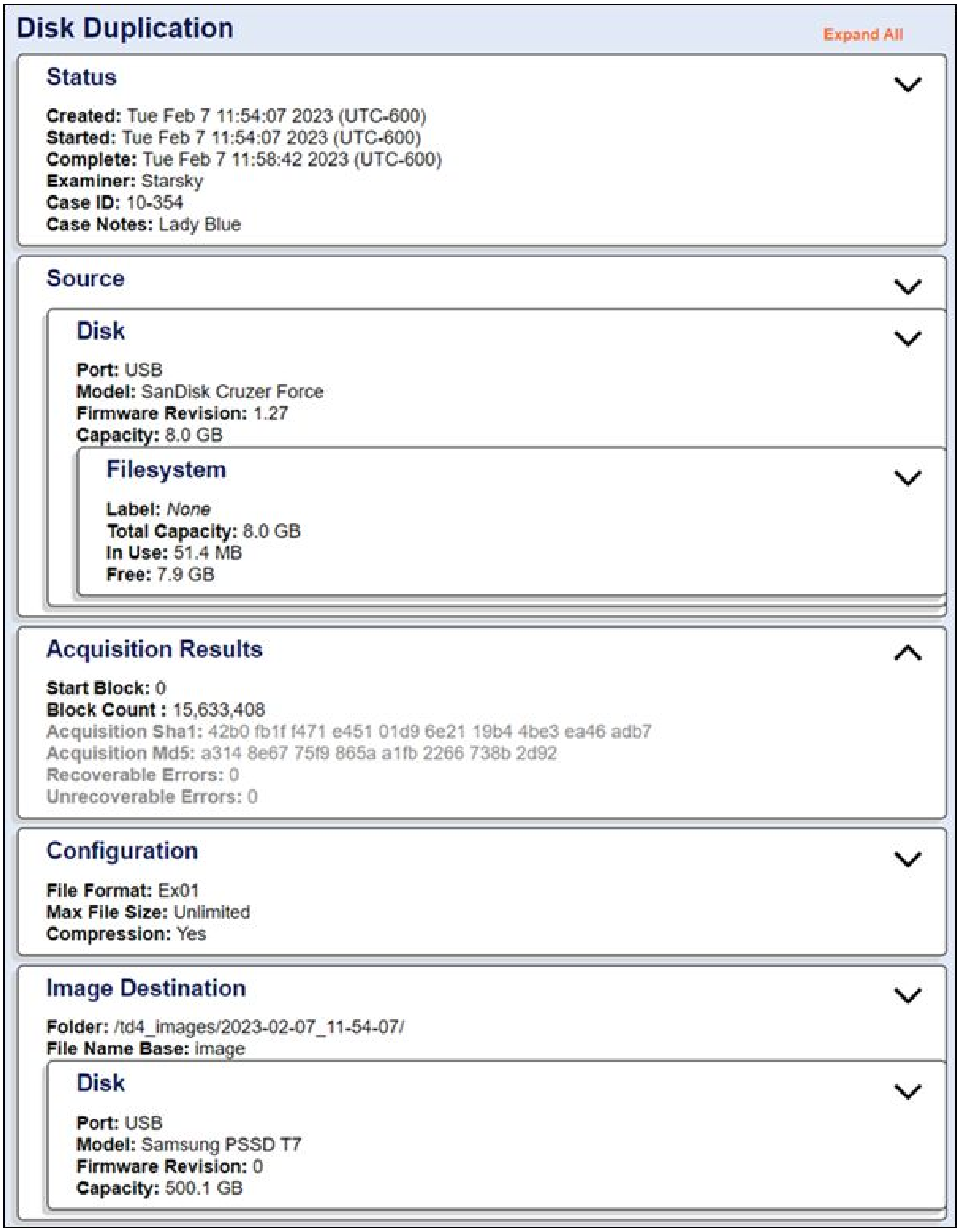
### 4.14.1 Sample logs

Two sample logs are shown below - one from a successful duplication and one from a failed standalone verification. As shown in the HTML log samples, there are up/ down arrows on the right side of each section header. A down arrow indicates the section is collapsed; An up arrow indicates it has been expanded. The sample HTML logs below are shown with all fields collapsed for simplicity. Each piece of log information was categorized as critical or supplementary, and only the critical information is shown when a section is collapsed. When an exported log is viewed on a separate computer, each section can be expanded to show the detailed, supplementary information. In that expanded view, the critical information is highlighted with bold field descriptions, while the supplementary information is shown in light gray. Note that specific pieces of log information may be considered supplementary in one situation but critical in another. For example, the encryption information for a given source drive will be considered supplementary if the drive has no encryption but will become critical if encryption is detected.

The initial state for any HTML log will be to show all fields collapsed with only the critical information displayed. While individual sections can be toggled between showing all the information or just a summary, there is a button at the top right side of the HTML log screen that will allow all sections to be expanded or collapsed.

Error messaging in the HTML logs has some unique functionality as well. Any error conditions will show in red text as critical information in the summarized view. Expanding the section with an error condition will show more detailed information on the error status, including the cause of the error.

**Sample Log 1 – Successful EX01 Duplication**



Disk Duplication

Status

**Created:** Tue Feb 7 11:54:07 2023 (UTC-600)
**Started:** Tue Feb 7 11:54:07 2023 (UTC-600)
**Complete:** Tue Feb 7 11:58:42 2023 (UTC-600)
**Examiner:** Starsky
**Case ID:** 10-354
**Case Notes:** Lady Blue

Source

Disk

**Port:** USB
**Model:** SanDisk Cruzer Force
**Firmware Revision:** 1.27
**Capacity:** 8.0 GB

Filesystem

**Label:** *None*
**Total Capacity:** 8.0 GB
**In Use:** 51.4 MB
**Free:** 7.9 GB

Acquisition Results

**Start Block:** 0
**Block Count :** 15,633,408
Acquisition Sha1: 42b0 fb1f f471 e451 01d9 6e21 19b4 4be3 ea46 adb7
Acquisition Md5: a314 8e67 75f9 865a a1fb 2266 738b 2d92
Recoverable Errors: 0
Unrecoverable Errors: 0

Configuration

**File Format:** Ex01
**Max File Size:** Unlimited
**Compression:** Yes

Image Destination

**Folder:** /td4_images/2023-02-07_11-54-07/
**File Name Base:** image

Disk

**Port:** USB
**Model:** Samsung PSSD T7
**Firmware Revision:** 0
**Capacity:** 500.1 GB

**Note:** All log sections are collapsed except for Acquisition Results.

**Sample Log 2 – Failed Standalone Verification (source unreadable)**

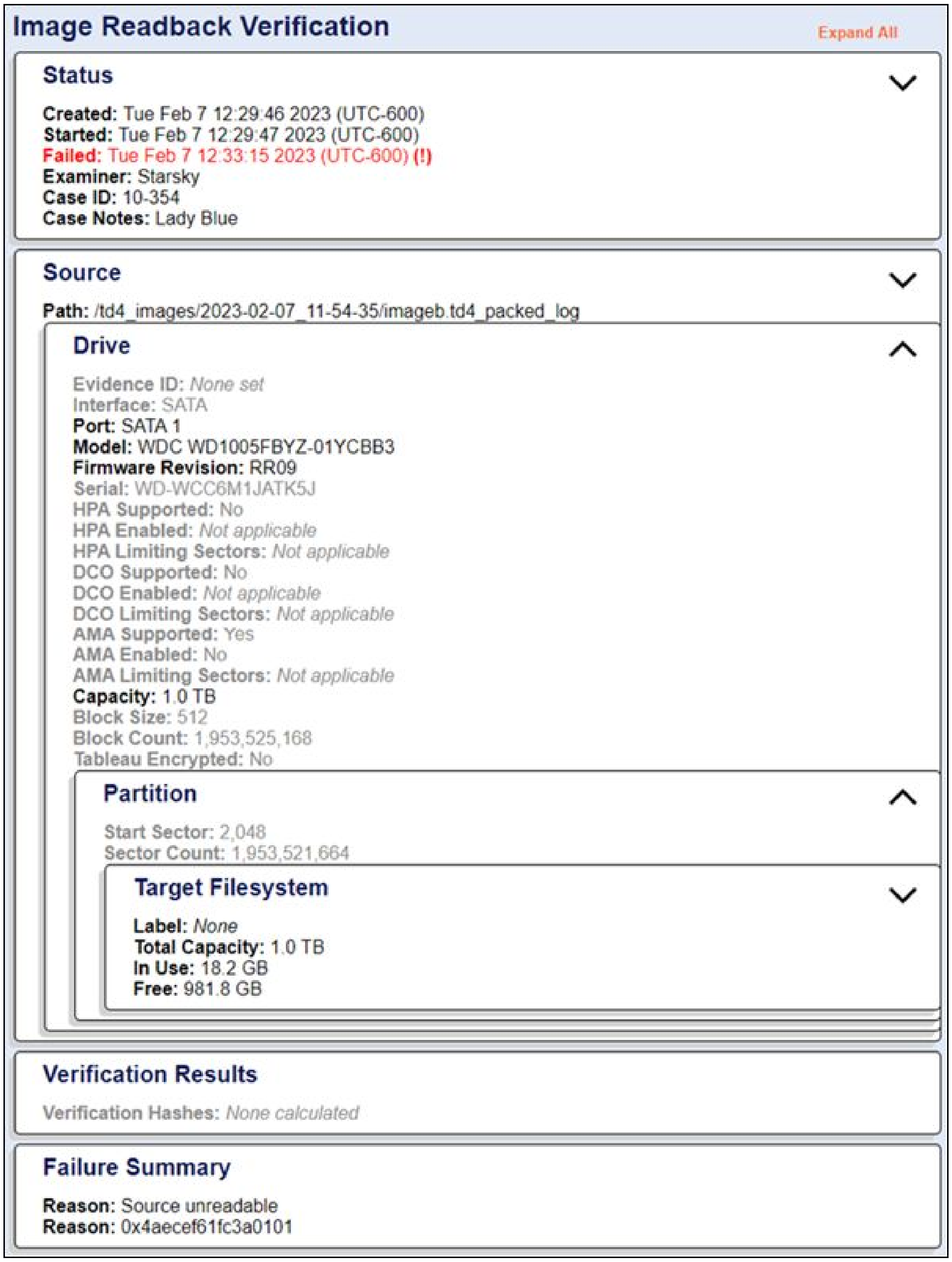


Image Readback Verification

Status

**Created:** Tue Feb 7 12:29:46 2023 (UTC-600)
**Started:** Tue Feb 7 12:29:47 2023 (UTC-600)
**Failed:** Tue Feb 7 12:33:15 2023 (UTC-600) **(!)**
**Examiner:** Starsky
**Case ID:** 10-354
**Case Notes:** Lady Blue

Source

**Path:** /td4_images/2023-02-07_11-54-35/imageb.td4_packed_log

Drive

**Evidence ID:** *None set*
**Interface:** SATA
**Port:** SATA 1
**Model:** WDC WD1005FBYZ-01YCBB3
**Firmware Revision:** RR09
**Serial:** WD-WCC6M1JATK5J
**HPA Supported:** No
**HPA Enabled:** *Not applicable*
**HPA Limiting Sectors:** *Not applicable*
**DCO Supported:** No
**DCO Enabled:** *Not applicable*
**DCO Limiting Sectors:** *Not applicable*
**AMA Supported:** Yes
**AMA Enabled:** No
**AMA Limiting Sectors:** *Not applicable*
**Capacity:** 1.0 TB
**Block Size:** 512
**Block Count:** 1,953,525,168
**Tableau Encrypted:** No

Partition

**Start Sector:** 2,048
**Sector Count:** 1,953,521,664

Target Filesystem

**Label:** *None*
**Total Capacity:** 1.0 TB
**In Use:** 18.2 GB
**Free:** 981.8 GB

Verification Results

**Verification Hashes:** *None calculated*

Failure Summary

**Reason:** Source unreadable
**Reason:** 0x4aecef61fc3a0101

**Note:** All log sections are collapsed except for the Drive and Partition sections.

If TD4 detects any bad sectors on the source drive, it adds a section at the end of the job log. This additional section lists the sector address and the number of sectors of each unreadable region of the source drive. As an example, the following forensic log read error entry means that an error was encountered in at least one of the 64 sectors starting at sector offset 234,567: `Error # 1: Read error (source), address= 234567, length=64`

**Note:** The default error granularity setting is Standard, which will result in a minimum chunk of 32KB of source data (64 sectors for a 512B sector drive) that will get skipped and filled with zeros upon completion of the attempted reads (assuming no reads were successful). If this condition is encountered, consider changing the error granularity setting to be Exhaustive, which will result in repeated read attempts of the error region with decreasing sector sizes. This will maximize the amount of recoverable data and minimize the sectors that get skipped and filled with zeros.

If error retries are enabled and TD4 is able to successfully read sector data after an initial read error is encountered, the Recoverable Errors count shown in the Acquisition Results section (as shown in the sample log 1, above) will reflect the number of original read errors encountered. The Unrecoverable Errors count will reflect read errors for which no retry attempts were successful.

Chapter 5

# Adapters

This chapter describes the drive adapters available for TD4, which extend imaging capabilities in an easy to connect and use manner.

## 5.1 PCIe SSD adapters

Tableau PCIe SSD adapters enable the acquisition of PCIe based SSDs of various types via the TD4 PCIE source port. The following adapters are available individually or as part of an adapter kit:

- PCIe card SSD adapter – TDA7-1
- PCIe m.2 SSD adapter – TDA7-2
- PCIe adapter for Apple SSDs 2013+ (through 2016) – TDA7-3
- PCIe u.2 SSD adapter cable – TDA7-4
- PCIe adapter for Apple SSDs 2016+ – TDA7-7

Visit https://www.opentext.com/assets/documents/en-US/pdf/opentext-ds-tableau-forensic-adapters-and-accessories-data-sheet-en.pdf to learn more about available Tableau PCIe SSD adapters.

**Note:** If you need to redetect PCIe SSD after ejecting it, the cable must be removed from TD4 and then reinserted. Removing only the downstream evidence drive from the adapter and reattaching it will result in no power to the drive.

## 5.2 PCIe IDE adapter (TDA7–5)

The PCIe IDE Adapter (TDA7-5) enables the acquisition of IDE drives via TD4's PCIe source port. The IDE adapter kit (sold as an add-on to the TD4 kit) includes the IDE power and signal cables used to connect the IDE drive to the adapter. The PCIe cable used to connect the adapter to TD4 is included with the TD4 kit.

To use TDA7-5 with TD4, follow these steps:

1. With TD4 powered off, attach the TDA7-5 to TD4 by connecting it to the source (left side) PCIe port using a Tableau PCIe cable (TC-PCIE-4 or TC-PCIE-8).
2. Connect an IDE drive using the TC6-2 ribbon cable (blue connector goes to the TDA7-5) and TC2-8-R2 power cable.
3. Power on TD4.
4. The PCIe drive tile on the home screen will become active which indicates it is available for use.

**Note:** If you need to redetect an IDE drive attached to TDA7–5 after ejecting it, the cable must be removed from TD4 and then reinserted. Removing only the downstream evidence drive from the adapter and reattaching it will result in no power to the drive.

## 5.3 PCIe FireWire adapter (TDA7–9)

The PCIe FireWire adapter (TDA7-9) enables the acquisition of FireWire drives via the TD4's PCIe source port. The PCIe FireWire adapter kit (sold as an add-on to the TD4 kit) includes 9-pin and 6-pin FireWire adapter cables which are used to connect the FireWire media to the adapter. The PCIe cable used to connect the adapter to TD4 is included with the TD4 kit.

**Note:** There is a 9-pin 1394b port and a 6-pin 1394a port on TDA7-9. Since TD4 works on only one source drive at a time, ensure that only one type of FireWire drive is connected to TDA7-9 prior to plugging it into TD4.

To use TDA7-9 with TD4, follow these steps:

1. With TD4 powered off, attach the TDA7-9 to TD4 by connecting it to the source (left side) PCIe port using a Tableau PCIe cable (TC-PCIE-4 or TC-PCIE-8).
2. Connect a FireWire drive to the adapter using either the TC7-6-6 cable (for 1394a devices) or the TC7-9-9 cable (for 1394b devices).

**Note:** Some FireWire devices may not be powered through the main FireWire interface cable. Such devices will require an external power source.

3. Power on TD4.

4. The PCIe drive tile on the home screen will become active which indicates it is available for use.

**Note:** If you need to redetect a FireWire drive attached to TDA7–9 after ejecting it, the cable must be removed from TD4 and then reinserted. Removing only the downstream evidence drive from the adapter and reattaching it will result in no power to the drive.

## 5.4 SATA/IDE adapters

Tableau SATA/IDE adapters enable the acquisition of such drives. The following SATA/IDE adapters are available for use with TD4:

- 3.5″ SATA-microSATA Hard Disk Adapter (TDA3-1)
- SATA – Blade-Type SSD Adapter (TDA3-2)
- mSATA / m.2 SATA SSD Adapter (TDA3-3)
- SATA LIF Hard Disk Adapter (TDA3-LIF)
- 3.5″ – 1.8″ IDE Hard Disk Adapter (TDA5-18)
- 3.5″ – 2.5″ IDE Hard Disk Adapter (TDA5-25)
- 3.5″ – ZIF IDE Hard Disk Adapter (TDA5-ZIF)

Visit www.opentext.com/assets/documents/en-US/pdf/opentext-ds-tableau-forensic-adapters-and-accessories-data-sheet-en.pdf to learn more about available Tableau adapters.

Chapter 6

# Specifications and troubleshooting

## 6.1 Specifications

| **Connectors: Source Side** | |
|---|---|
| SATA/SAS | One SATA/SAS (6 GBPS) signal connectors |
| Drive Power | One 4-pin Molex Mini-Fit power connector for SATA/SAS drive power |
| PCIe | One PCIe (10 GBPS) adapter connector |
| USB | One USB 3.2 Gen 1 (5 GBPS) Type-C connector<br>(USB 3.0 SuperSpeed equivalent) |
| **Connectors: Destination Side** | |
| SATA | Two SATA (6 GBPS) signal connectors |
| Drive Power | Two 4-pin Molex Mini-Fit power connectors for SATA drive power |
| PCIe | One PCIe (10 Gbps) adapter connector |
| USB | Two USB 3.2 Gen 2 (10 Gbps) Type-C connectors |
| **Connectors: Miscellaneous** | |
| USB<br>(Rear Accessory Port) | One USB 3.2 Gen 1 (5 Gbps) Type-C connector<br>(USB 3.0 SuperSpeed equivalent) |
| DC Input | One barrel connector for use with Tableau TP6 Power Supply |
| **User Interface** | |
| LCD | 4.95 in. graphic LCD (480 x 854 resolution) with capacitive touchscreen |
| Power Button | One on/off power button |
| **Indicators** | |
| Power Indicator<br>(top left) | White LED (in power button) indicates TD4 is powered on |
| Status Indicator<br>(bottom right) | Multi-color LED indicates TD4 job status |
| Speaker | Plays audio tones to indicate job completion/error status |
| **Physical / Environment** | |

| | |
|---|---|
| Power | 18 Watts typical (TD4 alone, no drives connected)<br>50 Watts typical (TD4 during a 1:2 imaging job)<br>120 Watts max (including external drive power) |
| DC Input (see "Powering TD4 with a portable battery unit" on page 92 for battery power considerations) | 24 VDC (nominal), as provided by TP6 power adapter); 14 VDC min.; 34 VDC max. |
| DC Output (per drive) | +5/12V @2A (Spin-up max)<br>+5/12V @1A (Continuous max) |
| Dimensions | 6.75 in. (L) x 4.6 in. (W)<br>(17.12 cm (L) x 11.68 cm (W))<br>Rear height: 1.8 in. (4.6 cm)<br>Front height: 1 in. (2.54 cm) |
| Weight | 16 oz (454 g) |
| Storage Temperature Range | -20 to 70$^o$ Celsius |
| Operating Temperature Range | 0 to 40$^o$ Celsius ambient |
| Relative Humidity | Up to 90% (Non-condensing) |
| **Warranty** | |
| TD4 Unit | Three Years Parts and Workmanship from Date of Purchase |
| TD4 Kit Accessories | One Year Parts and Workmanship from Date of Purchase |

### 6.1.1 Powering TD4 with a portable battery unit

It is possible to power TD4 with an external, portable battery solution. OpenText recommends using a portable battery unit with an AC outlet which allows use of the standard OpenText TP6 power adapter, eliminating the need for any custom DC adapter cables. An AC output on a portable battery unit also eliminates issues with low voltage conditions, as the AC output voltage is typically guaranteed to be at the nominal level until it shuts down when the battery power gets low.

As long as your chosen battery meets the following key parameters, it should work well with TD4 when used in a typical manner:

- Required battery unit output voltage:
  - DC output: 14 VDC min to 34 VDC max.
  - AC output: 100 VAC min to 240 VAC max (for use with OpenText's TP6 power adapter)

- Recommended battery unit power and capacity (AC or DC output):
  - 100 W minimum; 250 W peak
  - 600 W-hrs

OpenText engineering has done empirical testing with TD4 using several different commercially available portable battery solutions. Taking all the requirements above into consideration as well as cost and availability, OpenText recommends the Rallye 600 from Runhood. With that unit powering a TD4, a 1:2 duplication (physical image) job of a 1 TB Seagate Barracuda 7200.11 HDD to two high-power Western Digital HDD destination drives was completed with 40% charge left on the battery unit. The duration of that job was 5 hours and 42 minutes.

There are two noteworthy portable battery unit features worth mentioning that will improve the user experience with TD4, as follows:

- Backup battery hot swap - Running out of power during a long acquisition job can result in many hours of wasted imaging time. Fortunately, all Tableau Forensic imager/duplicator products, including TD4, support pause and resume of physical imaging jobs (output types E01, Ex01, DD, DMG). This includes automatic pausing for unexpected power loss situations. That feature allows any job to be restarted from the most recent checkpoint after a power loss event, which will typically result in minimal (if any) lost imaging time. In addition to Tableau Forensic's pause and resume functionality, another insurance policy against unexpected power loss when using portable battery power during evidence acquisition is to use a battery unit that allows for hot swap of its battery modules. Such units allow for separate charging of backup battery modules that can then be inserted into the portable battery unit before the active battery module drains down below the required minimum output voltage level.
- Pass-through charging – This feature allows a portable battery unit to power a load device while it is connected to an external power source to charge its internal batteries. In this mode, it is important that there is no output power glitch when the charging source is removed.

Note that, if you choose to use a portable battery unit with only a DC output, you will need to find a way to safely connect it to your TD4. Also, when direct DC battery power is used, it will be possible for TD4's input voltage level to drop below the level required for normal operation. TD4 senses its input voltage, and it will warn of an initial low voltage condition at approximately 19 VDC (yellow battery icon at the top of the home screen). At about 16 VDC, that warning icon will turn red. TD4 will still run as the input voltage drops further, but it will automatically shut down when the voltage drops to approximately 13.5 VDC. To help prevent issues caused by low input voltage, it is highly recommended that a battery unit be used that is capable of seamless hot-swap of the underlying battery modules.

**Note:** Because the power demand from TD4 will stay relatively constant during an acquisition job, the battery will need to supply more current as the input voltage drops. The maximum current level will increase as much as 85% compared to the nominal 24 VDC input level as the voltage approaches the

TD4 shutdown point (~13.5 VDC). This must be considered when selecting an external battery supply for TD4 that has only DC output voltage.

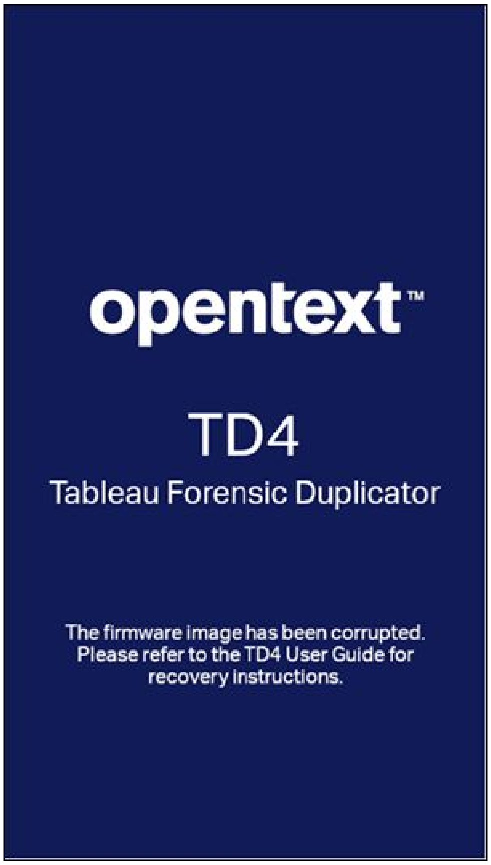
## 6.2 Troubleshooting common problems

This section covers the following troubleshooting issues and solutions:

- Firmware recovery
- Power supply issues
- Thermal issues
- Problems with drive detection
- Time/date data retention issues

### 6.2.1 Firmware recovery

If your TD4 is not booting properly, it could be due to a corrupt main firmware image. When this occurs, the boot time splash screen shown below will be seen on the unit, and it will not boot into the normal TD4 application.



opentext™

TD4

Tableau Forensic Duplicator

The firmware image has been corrupted.
Please refer to the TD4 User Guide for
recovery instructions.

To recover from this condition, follow these steps:

1. On any computer, format a USB stick with a FAT32 filesystem.
2. Download the latest TD4 firmware package file from the OpenText My Support Portal Knowledge Base (https://support.opentext.com/csm?id=csm_knowledge_home) and store it at the root directory on that FAT32 filesystem.

   See “Updating TD4 firmware” on page 26 for details.
3. After the firmware package file has been written to the USB stick, eject the USB stick from your computer and then plug it into the rear accessory port on your unpowered TD4.
4. Turn TD4 on.

The unit should detect the presence of the firmware package file on the USB stick and automatically launch into the firmware recovery process. The unit will reboot at the end of the process, and, if the problem has been resolved, your unit should boot into the normal TD4 application and be ready to use.

### 6.2.2 Power supply issues

The TP6 power supply provided with TD4 is capable of powering TD4 and nearly all combinations of drives. If your TD4 will not turn on, check the status of the DC power LED on the plug at the end of the TP6 power supply output cord. If the blue ring is not lit up, then check to make sure the AC power cord is plugged into the TP6 and that the other end is plugged into a live AC outlet. If all that checks out, it is likely your TP6 power supply has failed. If you suspect your TP6 has failed, contact OpenText My Support at https://support.opentext.com to initiate repair/replacement actions.

Regarding external drive power, TD4 employs staggered power sequencing for the source and destination drives. With staggered sequencing, power is first provided to one drive, then, after a brief delay, to the second drive, and so on. This feature prevents large current demand spikes at initial power-up when many drives are connected, which helps to ensure reliable operation even with a heavily loaded system. Due to staggered power sequencing, it is normal to hear the source and destination drives spin up separately.

TD4 is constantly monitoring its internal voltages. If any of them are out of specification, the unit will be shut down and the power button LED will flash. If this occurs, remove all drives from the unit, remove the power cord from the back, reconnect it, and then attempt to turn your TD4 on again. If the problem persists, contact OpenText My Support at https://support.opentext.com to initiate repair/replacement actions.

### 6.2.3 Thermal issues

TD4 is constantly monitoring the operating temperature of key components inside the unit. While it was designed to have plenty of operating temperature margin, conditions that affect the airflow or the effectiveness of the cooling system inside the unit can occur. Depending on the severity of the issue, overheating can possibly cause performance issues, functionality issues, or physical damage to the unit.

Should any of the key TD4 components become overheated for any reason, a warning will be provided in the top navigation bar (dark blue bar across the top of the home screen). The first level warning will be a yellow thermometer icon which indicates temperatures are on the rise and above a set threshold. A yellow thermal warning indicates that the unit is running abnormally hot but is still within its normal operating temperature range. If you see this yellow thermal warning, check to make sure the fan inside the unit is running and that none of the vents (inlet or outlet) are blocked. If everything looks okay and the yellow thermal warning persists for more than one hour, turn the unit off and let it cool for a few minutes before attempting to use it again. If after powering the unit up again, the yellow thermal warning returns and persists for more than one hour, contact OpenText My Support at https://support.opentext.com for further guidance.

The second level thermal warning will show a red thermometer in the top navigation bar. A red thermal warning indicates the unit has hit an extreme temperature threshold at which functionality can no longer be guaranteed and above which the unit could possibly be damaged. Check to make sure the fan inside the unit is running, and that there are no obstructions to the inlet or outlet air vents; let the unit cool down for a few minutes before attempting to use it again. If the red thermal warning condition returns, please immediately shut down the unit and contact OpenText My Support at https://support.opentext.com for further guidance.

Note that to cover situations in which TD4 is overheating while unattended, there is an automatic shutdown mechanism. If the internal temperature ever exceeds the extreme temperature threshold by five degrees C, software will immediately attempt to shut down the unit without warning

**Caution**

If your TD4 shows a red thermal warning in the top navigation bar on the home screen, it is highly recommended that you immediately power off your TD4. If the power button is unresponsive, remove the power from the rear of the unit. Check to make sure the fan inside the unit is running and that there are no obstructions to the inlet or outlet air vents; let the unit cool down for a few minutes before attempting to use it again. If the red thermal warning condition returns, please immediately shut down the unit and contact OpenText My Support at https://support.opentext.com.

## 6.2.4 Problems with drive detection

When using a product like TD4, the most common problem you may encounter is a failure to achieve drive detection. Most drive detection problems are the result of improper cabling. The following table lists the most common drive detection problems and possible corrective actions.

| Problem | Possible Corrective Action |
|---|---|
| General drive detection | Check the power and signal cable connections between TD4 and the drive to ensure that all connectors are properly seated. If TD4 still does not detect the drive, cycle the power to attempt to detect the drive during a fresh start-up sequence. |
| PCIe SSD is not detected | While TD4 supports hot insertion of PCIe drives, it is possible that doing so may cause drive detection issues that would otherwise not occur. If you hot insert a PCIe drive (via an appropriate Tableau PCIe adapter) and it does not detect, power off the unit, connect the PCIe drive/adapter to TD4, and then power on the unit.<br>Note that the m.2 drive stick form factor is not exclusive to PCIe drives. SATA SSDs exist in that same form factor, and they can physically be plugged into the Tableau TDA7-2 PCIe adapter. Such a setup will result in no drive detection. If you experience no detection on an m.2 SSD, verify that it is a PCIe (AHCI or NVMe) drive. If it is a SATA m.2 drive, try connecting the drive to your TD4 with a Tableau TDA3-3 mSATA / m.2 SATA SSD Adapter. |
| IDE drive is not detected (using TDA7-5 on a TD4 PCIe port) | Ensure that the blue end of the IDE signal cable faces the IDE adapter, and that the IDE drive is configured for Master or Single Drive mode. Also, if the IDE PCIe adapter was hot plugged into TD4, power off the unit, connect the PCIe drive/ adapter to TD4, and then power on the unit. |
| SATA or SAS drive is not detected | Use only the unified SATA/SAS cables provided by Tableau (TC4-8-R4). With some SATA drives, the SATA connector may be loose. Ensure the cable is seated properly in the SATA connector of the drive. Note that SATA/SAS interface cables can develop connectivity issues over time through normal use. It is recommended to periodically replace your SATA/SAS cables or to keep some spares on hand in case of a suspected bad cable. |

| Problem | Possible Corrective Action |
|---|---|
| USB drive is not detected | While there are a variety of reasons a USB drive may not detect on TD4, one possible explanation is that it is a self-encrypting drive with a proprietary detection/unlocking interface. Kingston's IronKey is an example of such a drive series. These types of drives expose a small CDFS volume to the host system instead of the main data volume. This CDFS volume typically includes product literature and, more importantly, an application that allows for password entry on a x86/Windows based host system. While TD4 cannot run these unlocking applications (as they are designed for x86 based systems), as of the 24.3 firmware version, it will at least detect such a drive and report its type to the user in the drive tile and drive details screen. |

OpenText has tested TD4 with an extensive in-house library of different drives spanning many years of drive development, but there may still be compatibility issues with some drives. OpenText issues firmware updates to address most compatibility issues. If your drive is not recognized by TD4, check the OpenText My Support Portal Knowledge Base (https://support.opentext.com/csm?id=csm_knowledge_home) to see if any firmware updates are available for TD4.

If there are no firmware updates available to resolve your detection issue, contact your Tableau reseller or OpenText My Support at https://support.opentext.com to report your issue.

### 6.2.5 Real-time clock data retention issue

Under normal operating conditions, the real-time clock on your TD4 should retain the time and date settings for the life of the product. If the time and/or date setting is not being retained after power cycles, there could be an issue with the battery inside the unit. We do not recommend opening your TD4 for any reason, including battery replacement. If you notice an issue with the time and/or date setting not being retained, contact OpenText My Support at https://support.opentext.com to report your issue and ask for further assistance.