opentext™

OpenText™ Forensic TX2 Imager

User Guide

This guide presents a wide range of technical information and procedures for using the OpenText™ Forensic TX2 Imager.

ISTXII260100-UGD-EN-1

OpenText™ Forensic TX2 Imager
User Guide

ISTXII260100-UGD-EN-1
Rev.: 2026-Jan-30

This documentation has been created for OpenText™ Forensic TX2 Imager 26.1.
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

Table of Contents

Chapter 1

Preface

This guide presents a wide range of technical information and procedures for using the OpenText™ Forensic TX2 Imager. It includes the following chapters:

- "Overview": Provides general information about this product, as well as unpacking, starting up, navigating the touchscreen display, and reading the LEDs.
- "Configuring the OpenText Forensic TX2 Imager": Provides system overview information, as well as procedures for configuring and connecting this product.
- "Using the OpenText Forensic TX2 Imager": Provides detailed information and procedures for its operation.
- "Adapters": Describes the adapters that extend the drive acquisition options and destination drive capabilities of the OpenText Forensic TX2 Imager.
- "Specifications and troubleshooting": Provides a brief list of potential problems and solutions. For more complete and current troubleshooting information, as well as answers to frequently asked questions (FAQ), go to 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 defining 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 Forensic Equipment products report drive capacities and transfer rates according to the industry standard *powers of ten* convention. In OpenText TX2 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

The OpenText Forensic TX2 Imager is a powerful, yet intuitive, forensic imager that offers superior local and networked imaging performance with no compromises. The touchscreen user interface is easy to use and provides a familiar user experience, similar to modern tablets and smartphones.

This product is custom built for forensics and provides many standard and advanced features that serve the specialized needs of digital forensics and incident response practitioners, including:

- Acquisition of PCIe (Gen 3 x4), USB (3.2 Gen2), SATA, SAS, FireWire, IDE, and network shares (iSCSI and CIFS).

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

- Output to PCIe (Gen 3 x4), USB (3.2 Gen2), SATA, and network shares (iSCSI and CIFS).
- Support for cableless, toolless, SATA destination drive connections via the optional drive bay (`TX2-S1`), which also provides drive cooling.
- Compatible with the following drive adapters: `TA7–1`, `TA7–2`, `TA7–3`, `TA7–4`, `TA7–5`, `TA7–7`, `TA7–9`, `TDA3–1`, `TDA3–2`, `TDA3–3`, and `TKDA3–LIF`.
- Clearly labeled and color-coded source (write-blocked) and destination (read/write) ports.
- The ability to target file-based evidence with a powerful logical imaging function, including an intelligent, easy to use search engine, with wildcard support and industry standard file outputs (`Lx01` and metadata CSV files).
- The ability to use a file hash database to search for specific files on a source drive. This can be used to eliminate files of non-forensic interest (for example, operating system files) to reduce the evidence set or to find specific files of forensic interest such as known illegal images.
- Two high performance 10-gigabit Ethernet ports (with 1 GbE auto-negotiation), which allow connectivity to two different local-area networks and/or network-attached storage devices. OpenText supports Ethernet port bonding (that is, link aggregation), which combines its two Ethernet links into a single logical interface, to increase bandwidth and/or provide redundancy.
- Browser-based remote user interface to any number of network-connected OpenText TX2 units, with the ability to directly download selected files to the remote system.
- The ability to export locally attached media as an iSCSI share for remote, network-based acquisition.

- The ability to enable and configure 802.1X network authentication, to strengthen network access security.
- The ability to acquire backup files from iOS- and Android-based mobile devices (including tablets).
- The ability to mount USB Still Image Class devices that support PTP (Picture Transfer Protocol) and MTP (Media Transfer Protocol), such as mobile devices and digital cameras, to enable on-screen browsing/triage and logical acquisition of any exposed files.
- The ability to automatically acquire drives connected to the imager's source ports, based on predefined job settings.
- The ability to duplicate a source drive to up to four destination drives (locally connected and/or network shares).
- The ability to simultaneously run multiple jobs of any type (clone, physical image, or logical image) to any available destination media/shares.
- The ability to resume a job that failed due to running out of space on a destination, by adding a new destination drive (known as destination drive spanning).
- Automatic assessment of available system resources, to balance active/queued jobs for maximizing jobs efficiency.
- The ability to manually reorder queued jobs and start them regardless of resource availability.
- The ability to pause and resume imaging jobs, including resumption from power loss and certain types of job failures.
- The ability to prevent damage to disk drives by spinning them down, when they are ejected prior to physical removal.
- The ability to power down the system after the last active job is complete.
- User management – create, delete, and manage user profiles, including support for PIV Smart Card multi-factor authentication via YubiKey devices.
- Superior data transfer rates even while performing calculations of MD5, SHA-1, and SHA-256 hash values on multiple active jobs.
- Industry-leading OpenText Tree Hashing support, which allows for massive parallelization of data block hashing and unmatched imaging performance.
- The ability to readback verify sequentially-hashed acquisition file sets, in a block-based and parallel manner, to maximize the readback verification performance.
- Viewing extensive drive detail, including partition and filesystem information and raw hex data.
- Detection and notification of many popular encryption types (whole disk and volume based), RAID types, proprietary self-encrypting drives, and Apple device Core Storage volumes.
- The ability to detect/acquire multiple namespaces on NVMe SSDs.

- The ability to detect and warn of the presence of detached NVMe namespaces and allow their attachment to enable acquisition of otherwise obscure evidence.
- The ability to unlock Opal-compliant self-encrypting drives (SEDs) and BitLocker encrypted drives/partitions, to enable unencrypted source media acquisition/ browsing and as an alternative to VeraCrypt based encryption for destination/ accessory port media.
- The ability to unlock APFS-encrypted volumes to enable unencrypted source media acquisition (source ports only).
- Browsing drive filesystems, with the ability to view image and text files directly in the touchscreen user interface.
- Gallery View with one-touch scrolling, to allow rapid viewing/triage of image type files on a per folder basis.
- Extensive filesystem support: APFS, ExFAT, NTFS, EXT4, FAT(12/16/32), and HFS+.
- Whole disk, open standard, destination drive encryption using XTS-AES.
- Automatic blank checking of source and destination drives.
- Convenient and configurable destination drive *Reconfigure* utility that allows for removing HPA/DCO/AMA, wiping, encrypting, and/or formatting all in one job.
- Comprehensive destination/accessory drive wiping capabilities, including NIST 800-88 compliant wipes and the ability to specify a custom wipe pattern.
- HPA, DCO, and AMA support for the detection and handling of hidden/ protected data areas on source drives. This includes standalone HPA/DCO/AMA removal, DCO/AMA shelving, and trim support for the creation of a destination DCO or AMA.
- The ability to update the system time via an NTP server.
- Detailed forensic logs for case documentation, in text and HTML formats.
- 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.
- The ability to put the unit into *stealth mode* for situations where bright LCD screens and loud job alerts may be undesirable.
- Regular and free firmware updates, available on OpenText My Support.
- User interface localization support for German, English, Spanish, French, Korean, Portuguese, Russian, Turkish, and Chinese languages, including virtual keyboard support for user inputs.

This product can operate as a standalone device (as shown in the following image), or with a destination imaging bay (TX2-S1).

The following image shows the product's left (source) side (write blocked).

The following image shows the product's right (destination) side (read/write).

2.1 Kit contents

OpenText TX2 ships in a boxed kit (with custom foam) that includes the following items.

Model #	Quantity	Description
TX2	1	OpenText Forensic TX2 Imager
TP8	1	Provides power to TX2, the optional TX2-S1 Drive Bay, and the attached source and destination drives. Uses a universal 3-prong style AC line cord and is compatible with 100-240V AC line voltages worldwide.
TC4-8-R4	4	8" unified SATA data and power adapter cable
TC-PCIE4-8	2	8" PCIe Gen3+ adapter cable. For use with OpenText Forensic PCIe Gen3+ adapters. For more information, see "Adapters" on page 135.
TCA-USB3-AC	2	4" USB 3.2 Type A to Type C adapter cable
TPKG-VCT-5	1	Five-piece Velcro cable tie kit
TPKG-CLOTH	1	Micro fiber screen cleaning cloth
TX2-QRG	1	*Quick Reference Guide*

Do not discard the OpenText TX2 foam packaging, as it is designed to fit several industry-standard hard-sided carrying cases (for example, the *Pelican 1500*). If you received this kit in the cardboard box shipped by OpenText, you can reuse the stacking foam inserts in your own hard-sided case.

2.2 Navigating the touchscreen display

Use the touchscreen display to navigate within the user-friendly interface and choose or modify options. Use the touchscreen keyboard or an external USB keyboard to enter alphanumeric text, when prompted. For more information, see "USB keyboard and mouse support" on page 20.

2.2.1 HOME screen

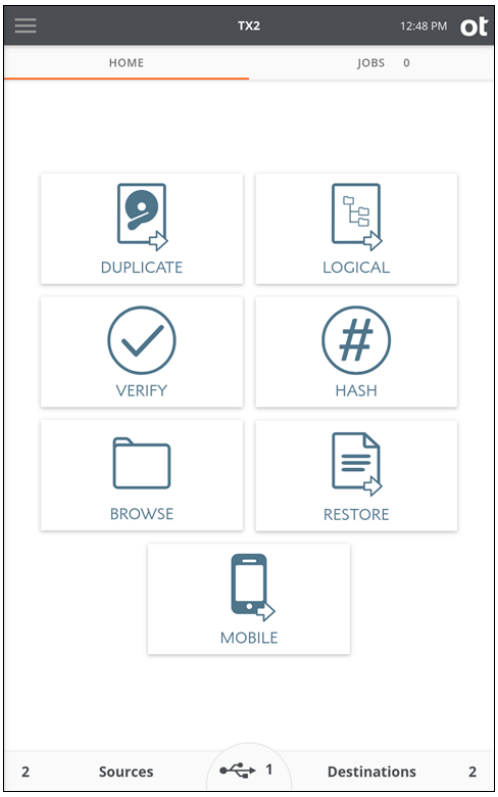
The **HOME** screen includes icons for initiating the following functions:

- Duplicate
- Logical
- Verify
- Hash
- Browse
- Restore
- Mobile

The three buttons at the bottom of the **HOME** screen are for **Sources**, **Accessory drives**, and **Destinations**. The number in each area represents the number of attached and detected drives (including mounted network shares). In addition to providing the drive count, these buttons can be tapped to display a summary list of available drives and allow access to further drive details, screens, and operations.

Note: The middle area of the bottom row of the **HOME** screen (for USB Accessory drives) is only shown when a USB Accessory drive is connected.

The following image shows the **HOME** screen, with two source drives, two destination drives, and one accessory drive attached.



Tap one of the icons on the **HOME** screen to begin a job and enter the Job setup screen. A Job setup screen provides a stepper-based flow from which you can view default settings, enter job notes for your case, change settings, and start the job. Tap the left arrow in the job setup tab to return to the previous screen or to the **HOME** screen.

The top navigation bar provides buttons to quickly access the side navigation menu , the **HOME** screen, and to view the current time. The **TX2** model name in the top navigation bar links to the **HOME** screen.

Note: In the event of unusual cooling conditions, a warning triangle will be shown in the top navigation bar, near the time indicator. This warning is not displayed during standard operating conditions. For more information, see "Troubleshooting common problems" on page 143.

The main screen includes the following tabs:

- **HOME** tab: shows the Home screen or one of the many other screens.
- **JOBS** tab: Always shows the Jobs summary screen and the current number of total active and queued jobs.

2.2.2 Side navigation menu

Click the menu icon in the top navigation bar to display the side navigation panel, which provides a menu of additional options and information. For more information about this menu, see "Configuration settings" on page 22.

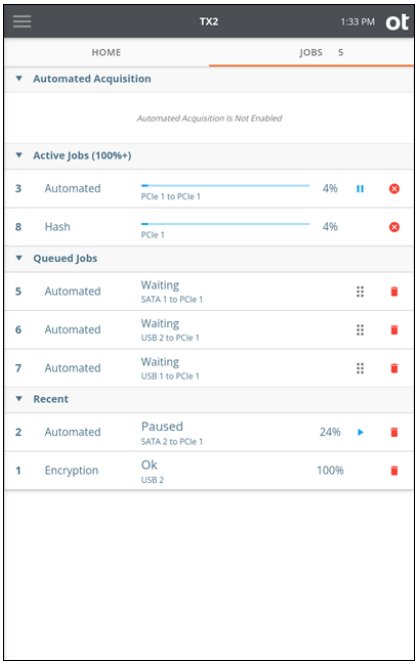
2.2.3 JOBS tab

The **JOBS** tab provides a convenient way to keep track of your active jobs, queued jobs, and recent work done. It includes a counter in the top tab area. When OpenText TX2 is first powered on, the jobs counter is at `0`. Once jobs are underway, each active or queued job will increment the counter.

The **JOBS** tab has the following areas.

Automated Acquisition	This area indicates if the **Automated Acquisition** mode is turned on. When it is turned on, the count of any duplication jobs run during that automated session will be displayed. For more information about this valuable, time-saving feature, see "Using the Automated Acquisition mode" on page 67.
Active Jobs	This area displays any active jobs. The imager will automatically decide when to start jobs or enqueue them, based on available system resources. Queued jobs start as soon as system resources become available, or when the source or destination resource for which the job is waiting becomes available. The automated resource assessment system can be overridden by manually dragging a job from the queue into the **Active Jobs** area. As jobs are completed, they are moved to the **Recent** jobs area. The detailed **Job Status** screen for any given job can be viewed by tapping on the job tile shown in the **JOBS** tab.
Queued Jobs	This area displays any queued jobs. Jobs are queued in the order in which they were entered. You can reorder queued jobs by dragging individual jobs, to place them in the order you prefer. On the touchscreen, press and hold the drag icon of the job you want to move, then drag the job to the desired position in the queue and release. Queued jobs may also be dragged into the **Active Jobs** area, to force them to start, regardless of available system resources.
Recent	This area displays any recently completed jobs. **Note:** This area is cleared out upon power-cycling the imager. A complete and non-volatile list of all jobs can always be found in the side navigation bar, by tapping the **Logs** button.
Media Utilities	This area displays media utility operations and appears only when such an operation is active. Media utility operations will move to the **Recent** area when they are complete. Media utility jobs cannot be queued like forensic jobs.

The following image shows an example of the acquisition jobs.



In this example, there are two active jobs – a hash and an automated duplication job. There are three automated duplication jobs queued and waiting for resources to be able to start. Note the textured grab areas in the queued job tiles, which can be used for drag-and-drop job reordering or for manually starting a queued job. In the **Recent** area there are two jobs, one that completed successfully and one that was paused. Since the pending job count includes both active and queued jobs, the **JOBS** tab counter reads *5*.

In this example, *Job 2* has moved from the **Active Jobs** area down to **Recent** (due to being paused), which allowed *Job 8* to start as shown in the **Active Jobs** area. For more information regarding that feature, see "Pausing and resuming a duplication job" on page 75.

There are several actions that can be taken on jobs from the **JOBS** tab, depending on both the state and type of the job:

- Queued jobs and jobs shown in the **Recent** area can be deleted by tapping the **Delete** button on the job row.
- Jobs in the **Active Jobs** area can be canceled by tapping the **Cancel** button.
- Imaging jobs in the **Active** area that are capable of being paused and resumed (of type `E01`, `ExO1`, `DD`, and `DMG`) can be paused by tapping on the **Pause** button, at which point the job will be moved to the **Recent** area with a status of *Paused*.

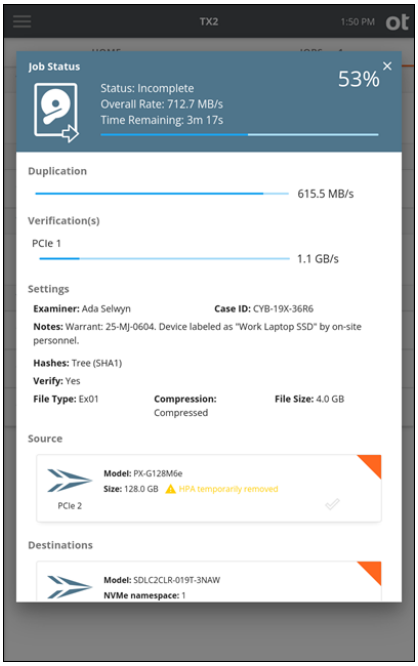
Tapping the **Play** button (or tapping the **Resume Job** button in the header of the **Job Status** screen) will display a **Resume Duplication** screen.

For more information about pause and resume, see "Pausing and resuming a duplication job" on page 75.

2.2.4 Job status

After a job starts, its **Job Status** screen is automatically displayed. This screen shows the details of a given job, including a header with its status, overall data rate, time remaining, and percent complete. The lower area of the **Job Status** screen shows additional job details, including 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 a drive details screen, which provides a quick view of all the information available for the drive.

The following image shows an example of an active **Job Status** screen.



Note: A solid orange triangle in the corner of a drive tiles indicates that the drive is currently being used by an active job. This is shown regardless of the location of the drive tile and makes it easy to spot drives that are in use. Similarly, drives that are part of a queued job will show as an orange border triangle with white in the middle.

Once a job has completed, the **Job Status** screen is displayed and shows the final status of that job. Completed jobs have a link to the log file for that job, on the header area at the top of the status screen.

Clicking the **View Log** link displays the detailed log for that job. You can click back to the **Job Status** screen or close the log and return to the **HOME** screen. The link back to the **Job Status** screen works regardless of the method used to get into the log details screen. For example, if you navigated to the log details for a given job through the side navigation menu **Logs** view, there will be a link at the bottom of the log to view the **Job Status** screen (**View Job**).

Note: The **Job Status** screen can also be viewed for completed jobs that are shown in the **Recent** area of the **Jobs** tab. Tapping the job row from the **Recent** jobs area will display the final **Job Status** screen for that completed job, including a link to the job log.

2.2.5 Quick Reference Guide

This product ships with a *Quick Reference Guide*, which illustrates the firmware update procedure, drive connections, status LEDs, power button, cable/adapter recommendations, and tips for getting started. Keep this card handy as you familiarize yourself with this product.

2.3 Reading the status LEDs

Power supply LED

The TP8 power supply DC cable has a blue LED ring near the end of the barrel connector, which indicates that the power supply is connected to an AC power source and functioning properly.

On/Off indicator LED

The illuminated power switch is located in the top-left corner of your device and it displays a white LED when the unit is on.

Activity LED

The multi-color activity LED is located in the lower-right corner of your device. The following table provides details for interpreting the status of this LED.

Status	Activity LED
The unit is booting up.	White
A power issue is detected.	Blinking white
The unit is idle.	Off
An operation is in progress.	Blue
An operation completes successfully.	Blinking green
An operation fails.	Blinking red

Network interface LED

The dual Ethernet connector is located on the back of your device and it has two LEDs for each port. The following table provides details for interpreting the status of these network interface LEDs.

Status	Link Status/Activity LED (Left side of the unit, looking at the connectors from the rear of your device; yellow in color)	Link Speed LED (Right side of the unit, looking at the connectors from the rear of your device)
No Link	Off	Off
1 Gbps Link	On/Blink	Green
10 Gbps Link	On/Blink	Orange

2.4 Interpreting audio feedback

This product plays one of two sounds that indicate status at the end of a job. A chime sound plays for a successful job, and a buzzer sound plays for a failed job. You can change the sound volume in the side navigation menu, from **System Settings**.

2.5 On-screen warnings

When necessary, this product provides on-screen warnings within various settings and operations screens of the user interface:

- Yellow warnings call the user's attention to a potential risk, but do not impede operations.
- Red warnings mean either that a selected setting cannot be accommodated, an operation has failed, or a 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 USB keyboard and/or mouse into either of the USB accessory ports on the front of your device. Some users find it more convenient to use an external keyboard/mouse to enter data, instead of using the touchscreen and on-screen virtual keyboard. Language-localized keyboard support is limited to the virtual keyboard only.

Note: If you prefer to use a wireless keyboard/mouse, plug the USB wireless adapter into either of the front USB accessory ports, and it should automatically pair with the keyboard/mouse and start working. There are many vendors of wireless keyboards/mice, and some may not be compatible with OpenText TX2. Contact OpenText Customer Support for wireless keyboard/mouse recommendations.

Chapter 3

Configuring the OpenText Forensic TX2 Imager

This chapter describes how to configure the OpenText Forensic TX2 Imager.

3.1 Startup sequence

1. When you turn on the unit, the activity LED (in the lower-right corner of the device) will immediately turn on (and display white color), which indicates that the unit is starting the boot sequence.
2. After a short time, the fan will turn on and then an OpenText branded splash screen will appear during the rest of the boot sequence.
3. Once booted, the unit displays the **HOME** screen (or the user login screen, if the auto-login is turned off), and then it sequentially powers on the drive ports.

   Once all of that is complete, your OpenText TX2 is ready for use.

For situations or locations where drawing attention to your presence is undesirable, OpenText TX2 can be put into *stealth mode*. This mode will deactivate all audio alerts, deactivate the status LED, and set the LCD brightness to a minimum setting.

To turn on the stealth mode:

1. Open the SSD access door on the bottom of the unit and change the first DIP switch (labeled 1 on the DIP switch block) to the OFF position.
2. Replace the SSD access door.

   The unit will power up in stealth mode until the switch is returned to its default (ON) position.

Note: Do not change the state of any of the other DIP switches when turning on the stealth mode. While switch 1 is the only assigned switch at initial release of this product, other switches may be activated in future firmware updates. Leaving all other switches in their default (ON) state will prevent undesirable unit behavior after future firmware updates.

3.2 Configuration settings

The 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 side navigation menu icon, to access the following options:

- **Home**: Return to the **Home** screen.
- **Logs**: Access the forensic **Logs** screen.
- **System settings**: Access the **System Settings** screen.
- **Network settings**: Access the **Network Settings** screen.
- **Defaults**: Access the operational **Defaults** settings screen.
- **Users**: Access the administrator level **User Management** 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 serial number, network MAC address, firmware build ID and version, firmware SHA-256 value, and copyright and licensing information. This area also includes the firmware update utility.
- **User**: Access the **User Management** screen for the current user.

3.2.1 System settings

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

The **System Settings** screen allows you to configure system options including **Date & time**, **24-hour clock**, **Set time via NTP server**, **Timezone**, **Language**, **LCD brightness**, **Audio notification volume**, and **LED notifications**. You can also perform a factory reset.

Note: A factory reset restores all system settings to their factory defaults and deletes all user-generated data. This includes job logs, 802.1x certificates, PIV Smart Card (YubiKey) certificates, SSL certificate, saved logical image searches, user configuration, and bookmarked CIFS/iSCSI logins. It is recommended that you make notes regarding any of that information and export all logs to an external device, before initiating a factory reset.

Tap the toggle buttons to activate or deactivate a setting, such as the **24-hour clock**. To define a slider setting value, such as the **LCD brightness**, tap and hold the slider selector, then slide to the desired value. For the **Timezone** setting, a multi-value selection box will be displayed to allow selection from a predefined list of settings.

Tap the setting row to reveal additional settings such as **Date & Time**. Once the area expands, tap a setting value to reveal and select from a drop-down list.

To set the OpenText TX2 system time via an NTP server, a valid network connection and at least one NTP server source is required. The default NTP server is a public

internet option (http://pool.ntp.org). This can be changed to one of the other public internet options or a local network NTP server. Tapping on **Set time via NTP server** displays a list of options for NTP server connectivity. Note that the **UPDATE TIME VIA NTP** button is inactive if there is no network connectivity or no working NTP server available. Contact your local network administrator for assistance in setting up your NTP server.

Note: Due to the forensic implications of changing the OpenText TX2 system time during an active job, the ability to use an NTP server to set the time has intentionally been limited to a manual call to the NTP server that is only available when no jobs are in progress. Also, should the NTP server update routine fail for any reason, a warning message to that effect will be shown instructing you to manually set the time and date.

The user interface display language can be set to German, English, Spanish, French, Korean, Portuguese, Russian, Turkish, or Chinese. Changing the language automatically configures the virtual keyboard to match the new language selection.

3.2.2 Network settings

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

This screen includes the following areas:

- **Port Selection** allows you to select an Ethernet port from the list of available options. If port bonding is desired, tap **Add Bond** in this area to initiate this action.

  Note: All of the settings on this screen are done on a per Ethernet port basis or per the single bonded network (if port bonding is utilized). Before configuring any network settings, make sure to select the appropriate Ethernet port or Bonded Network in the **Port Selection** area.

- **Current status** displays network-related information and the current connection status.
- **Configuration** allows you to set the **Bond Mode** and **Bond Transmit Policy** (if applicable), **IP address**, **MTU** (maximum transmission unit) value, and **Custom hostname**.

  The following **Bond Mode** options are available.

Bond Mode	Best for	Description	Customer value	Use case	Bond Transmit Policy	Switch Port Aggregation
Active Backup	Field work, unattended imaging.	Primary port only is actively used for traffic. If the active port fails, another port becomes active. Does not require switch configuration.	Ensures uninterrupted imaging. No network configuration required. Simple and reliable.	**Overnight or unattended imaging.** If a network cable or switch port fails during a long acquisition, imaging continues automatically without interruption.	N/A	N/A
Balance XOR	Managed switch environments.	Traffic is distributed across ports using a hash-based algorithm.	Load balancing + fault tolerance. Predictable traffic distribution.	**Structured network environments.** Labs with managed switches configured for port aggregation that want both performance and redundancy.	Yes	Yes/ Ethernet Channel
802.3ad	Enterprise labs, NAS storage.	Uses IEEE 802.3ad (LACP) to combine multiple Ethernet ports into one logical high bandwidth link.	Redundancy + performance. Enterprise-grade networking.	**High-speed forensic lab or data center.** OpenText TX2 connects to a managed switch and NAS/SAN storage where large evidence files must be transferred quickly and reliably.	Yes	Yes, with Link Aggregation Control Protocol (LACP)
Balance TLB	Standard labs, no switch changes.	Adaptive Transmit Load Balancing (TLB) distributes outgoing traffic across multiple ports based on load. Incoming traffic uses a single active port.	Improved performance. No special switch configuration needed. Ideal for standard lab networks.	**Busy forensic lab.** Multiple imaging jobs are writing data at the same time. OpenText TX2 balances outgoing traffic across ports to reduce bottlenecks.	N/A	N/A

Bond Mode	Best for	Description	Customer value	Use case	Bond Transmit Policy	Switch Port Aggregation
Balance ALB	Multi connection environments.	Adaptive Load Balancing (ATL) balances both outgoing and incoming traffic across multiple Ethernet ports.	Higher overall throughput. No switch-side configuration required. Efficient use of available network links.	**Multi connection workflows.** Handling multiple acquisitions or simultaneous transfers where balanced send and receive traffic improves responsiveness.	N/A	N/A

The following **Bond Transmit Policy** options are available.

Bond Transmit Policy	Description
Layer 2	It is recommended to use this option when OpenText TX2 and the target servers are on the same network segment (also referred to as broadcast domain).
Layer 2 and 3	It is recommended to use this option when OpenText TX2 and the target servers are on different network segments (or broadcast domain).

For static IP address assignments, the DNS address and Domain fields can be entered to make mounting CIFS shares easier.

The default MTU value is `1,500`. If your device is attached to a network that supports jumbo frames, change the MTU value to `9,000`, which may allow for much faster network transfer speeds.

Note: The maximum allowed MTU settings on this device is `9,000`. Attempting to manually set the **MTU** to a value higher than `9,000` will result in no change to the setting. This prevents slow network performance due to mismatched MTU settings.

Each network device in the end-to-end communication path should use the same MTU value to achieve optimal and reliable performance. Contact your network administrator to verify the network configuration.

- **802.1X** allows you to configure the 802.1X network authentication.
- **HTTPS certificate** allows you to setup the HTTPS certificate.

3.2.2.1 Configuring 802.1X network authentication

OpenText TX2 can be configured to connect to a network using IEEE 802.1X port-based authentication. This standard is designed to provide greater control over which physical devices are allowed on a given network, which greatly improves overall network security. A typical 802.1X network consists of an authentication server (RADIUS), an authenticator (LAN switch), and supplicants (network client devices).

To configure your device for use on a network with 802.1X authentication:

1. Tap **Edit** in the bottom right of the **802.1X** settings area, to choose one of the three EAP types (**TLS**, **TTLS**, or **PEAP**).
2. Tap **Identity** to enter your 802.1X identity (required).
3. One or more certificates (depending on the EAP type and other settings) may need to be loaded onto your device before attempting to authenticate on the network. The certificate loading process is straightforward:
   a. Store the required certificates on a USB memory device, and then insert that device into an OpenText TX2 USB Accessory port.
   b. In the **CA** and/or **Client certificate** areas in the **Network Settings** screen, tap the appropriate certificate installation button (**Install CA Cert** or **Install Client Cert**).

      A browse screen will appear, allowing navigation to the appropriate memory device and certificate file.
   c. Select the desired certificate file from the browser and tap the **Install** button.
4. Each EAP type has additional requirements and configuration settings depending on the type selected, as follows:

   - **TLS**: The OpenText TX2 and the authentication server authenticate each other by mutually verifying their certificates. A CA (Certificate Authority) certificate and a client certificate, issued by the certification authority, must be installed before authenticating using this method.

     Tap **SAVE** to show the selected EAP type and status in the settings summary.
   - **TTLS**: Select a **Phase two** internal protocol (**EAP-MSCHAPv2**, **MSCHAPv2**, **MSCHAP**, **CHAP**, or **PAP**). A CA certificate must be installed on OpenText TX2, to turn on the server authentication. This method uses an identity and password for client authentication. A client certificate is not required.

     Tap **SAVE** to show the selected EAP type and status in the settings summary.
   - **PEAP**: Select a supported **Phase two** internal protocol (**EAP-MSCHAPv2** or **MSCHAPv2**). A CA certificate must be installed on OpenText TX2, to turn on the server authentication. This method uses an identity and password for client authentication. A client certificate is not required.

Tap **SAVE** to show the selected EAP type and status in the settings summary.

After saving the selected EAP type and **Phase two** internal protocol settings, a yellow icon appears on the top navigation bar, and an **Add Password** button becomes active in the settings summary area.

5. Tap the navigation bar icon or **Add Password** to enter an 802.1X passphrase/password.

   Note: 802.1X passphrases are required to decrypt encrypted private keys. These passphrases can be between 4 and 1,023 characters in length.

6. Tap **SUBMIT** to begin the authentication procedure.

   Upon successful authentication, the network lock icon will disappear and the settings summary will report status as *Authenticated*.

3.2.2.2 HTTPS certificate setup

OpenText TX2 generates an SSL certificate on startup. You can use this certificate, manually generate a new certificate, or install your own certificate.

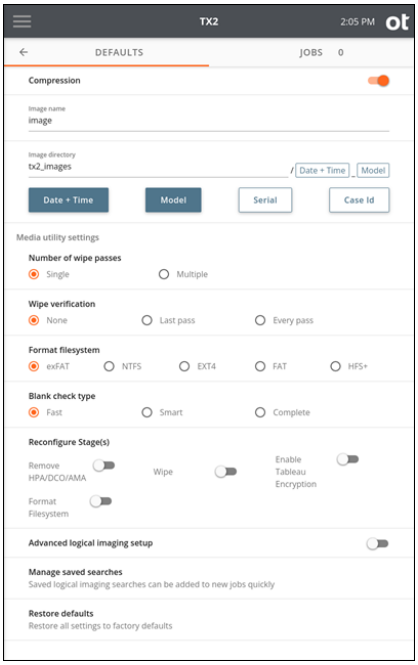
The bottom area of the **Network Settings** screen shows the current SSL certificate information and provides options for manually generating a new OpenText TX2 certificate or installing a custom certificate. For more information about SSL certificate options, see "Remote web interface" on page 130.

3.2.3 Default settings

Tap **Defaults** to display the **Operations Defaults** screen.

Several different entry methods are used for the settings on this screen, including direct data entry, sliders, option buttons, and an **Image Directory** name builder area. As shown in the following image, the **Date + Time** and **Model** directory path element boxes have been selected (in that order), so therefore the image directory path is `tx2_images/<Date+Time>`.

Note: The source drive Serial number and Case ID are not used in this example.



Tapping a selected directory path variable box deselects it. Changing the order of selection changes the order in which each element is incorporated into the image directory path.

Note: Certain combinations of image directory and image name settings can result in filename duplication on the destination filesystem for a given job. OpenText TX2 checks for this situation at job startup, and, if it detects a file name conflict, it automatically appends sequential numbers to the subsequent filenames. Though this feature exists, it is recommended that the image directory and image name values be set such that no conflicts occur.

The **Advanced Logical Imaging Setup** switch sets the mode of operation for the **Logical Imaging** setup screens. The default value is off, which provides a basic and easy-to-use search method for targeting forensically valuable information on a given source drive. For more information about basic and advanced setup modes, see "Logical imaging" on page 82.

The **Manage Saved Searches** item allows for management of logical imaging searches that have been previously saved and the addition of new searches via direct entry or importation. Using saved searches makes `Lx01` job setup more straightforward and efficient. In this area, saved searches can also be exported to any mounted destination (including network-based filesystems) which allows for easy sharing of desirable/standard searches across all your OpenText TX2 units. For more information about search setup and utilization, see "Logical imaging" on page 82.

Default settings can be restored to their factory set values. Select the **Defaults** item from the side navigation menu and then scroll to the bottom of the screen. Select the

Restore defaults item and all settings will be immediately returned to their factory set values.

3.2.4 User management

In some forensic work environments, it may be desirable to set up distinct users with unique credentials to limit access to the available devices. Also, with the addition of remote access capability, the ability to set user credentials has become a security requirement. OpenText TX2 ships with a default user named *User1*, which has administrator rights but no authentication and no remote access. *User1* also has **Auto Login** turned on (which is only possible for users with no set password). These defaults make this device easy to use in environments that do not require user management or remote access.

If your work environment would benefit from setting up individual users with credentials, or to add remote access capability to any user (even default User1), tap the **Users** item from the side navigation menu. A list of defined users is displayed on the left tab (default *User1* is the base user). From this initial user list screen, a user with administrator rights can delete or modify any existing user and create new users.

Note: Only users with administrator rights (including default *User1*) can access this **User Management** area. If a user with no administrator rights is logged in, the **Users** button on the side navigation menu will be dimmed and unusable.

Tapping on any user in the list will show a **User Management** screen which contains the available options for each user.

On this screen, an administrator can change any user's authentication configuration (username, password, multi-factor authentication), set administrator rights, allow remote access, allow tree hashing enablement, and enable auto login.

Note: Remote access is allowed only for users that have authentication setup. Auto login is allowed only for users that do not have authentication setup. Turning off administrator rights for a currently logged-in administrator is not allowed.

While using the **User Management** screen to set up new and edit existing users, you will be prompted to re-enter your password for each change to the credentials for a given user. This ensures no unauthorized changes can be made. For other User Management configuration changes (not related to authentication) there is a 30-second timeout that allows additional changes to be made without password re-entry.

At the bottom of each **User Management** screen, either one or two buttons are displayed. All **User Management** screens will show the **Logout All** option. This will logout all instances of that particular user (local and/or remote logins). When the administrator is logged in and viewing their own **User Management** screen, a **Logout** button is also visible. This button logs out only that instance (local or remote) of that user.

To create a new user, tap the **Create New User** button at the bottom-right of the **Users** list screen and enter the desired username. If authentication is not required for the new user, tap **Submit** and the **User Management** screen for that user will appear, allowing you to complete that user's configuration. If authentication is required, it can be set up on this initial user creation screen. OpenText TX2 supports two authentication methods, as follows:

- Password based authentication: An initial alphanumeric, case-sensitive password may be entered to allow user access.
- PIV Smart Card via YubiKey authentication: After configuring the YubiKey device for the new user (for more information, see https://www.yubico.com/), insert it into any USB port on your OpenText TX2. Within the new user creation screen, enter the PIN for the Smart Card.

  Note: OpenText TX2 requires validation of the PIV Smart Card certificate chain up to the root certificate. Depending on your Smart Card configuration, that root certificate may reside on the user's YubiKey device (known as a self-signed configuration) or it may need to be separately installed onto your OpenText TX2. If you enter the Smart Card PIN during user configuration and a PIV Smart Card certificate chain (up to a root certificate) cannot be found, a failure message will appear, and the credentials will not be entered/changed for that user. To install a PIV Smart Card certificate chain (`.pem` file type), insert a USB drive into any OpenText TX2 port that contains the certificate file(s) (up to and including the root certificate), and then tap the **Manage Smart Card Validation Certificates** button on the main **Users list** screen. At the bottom of the Certificates screen, tap the **Install From File** button. A browse window will appear that will allow you to navigate to the certificate file(s) on the attached drive. Once located, tap on the desired certificate file(s) and then tap the **Install** button at the bottom right of that screen. Once this step is successfully completed, then the Smart Card PIN may be entered for the associated individual user(s) on their User Management screen.

Regardless of the chosen authentication method, once the appropriate credentials are configured, tap the **Submit** button at the bottom-right of the **Create New User** screen and the **User Management** screen for that user will appear, allowing you to complete that user's configuration.

Note: The currently logged-in local user is always shown at the bottom of the side navigation bar. Also, the username associated with the logged-in user is shown in the forensic log. For systems that do not have multiple users set up, the default *User1* will be shown in the side navigation bar and in the forensic log.

For more information about setting up users, contact OpenText Customer Support.

3.2.4.1 Resetting a forgotten administrator user password

This section provides instructions for resetting a forgotten administrator user password.

Note: If a non-administrator user has forgotten their password, the administrator can log in and change the non-administrator user's password. The only time a factory reset is required to recover a unit is if the designated administrator has forgotten their password.

To reset a user password:

1. Enter an incorrect password five times, consecutively.
2. Perform a factory reset, as prompted by the system.

   Important
   A factory reset will delete all user-sourced data. This includes all job logs, settings (system, network, and defaults), user management configuration, and network share bookmarks. For more information about the factory reset, see "System settings" on page 22.

   After completing the factory reset, all system settings are restored to their factory defaults. No password is required in this state as the default user (*User1*) will be configured for auto-login with no password.

3.2.5 Locking the system

OpenText recommends locking your device while unattended, to ensure that no settings are changed and your active/queued jobs are not altered in any way.

To lock your system:

1. Tap **Lock System** on the side navigation menu.
2. In the screen that appears, enter the desired six-digit personal identification number (PIN), then tap **Submit** to begin the locking process.

   Note: The  button on 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.

   The system will prompt you for a second entry of the same PIN to confirm the desired digits have been entered.
3. Enter the same PIN again.

   After verifying that both PINs match, the system will be locked. A message will appear at the top of the lock screen, stating the time at which the system was locked.

This PIN locking mechanism is temporary in the sense that a power cycle of your device will remove the lock.

To unlock the system:

- Enter the current PIN and then tap **Submit** in the lower right corner of the screen.

3.2.6 Updating the firmware

The OpenText TX2 firmware is stored on an `m.2 NVMe SSD` located on the bottom of the unit, behind a removable access door.

Note: A firmware update cannot be started while a job is running. This is true when initiating an update from the local user interface (after selecting the firmware package file) or after a remote user has uploaded a firmware package file using the web interface. It is recommended that all active users on a given device (local and remote) collaborate to ensure no jobs are running or will be started before a firmware update is initiated.

To update your device firmware, go to OpenText My Support https://support.opentext.com and log in (or register) to access firmware package files for your OpenText Forensic TX2 Imager. Locate and download the most recent firmware package file (`.tx2_pkg`) and then select one of the following methods.

To update the firmware using the local package file:

1. Copy the desired OpenText TX2 firmware package file to a USB drive or to a network share that will be accessible to your device.
2. Tap **Firmware version** (or **About**) on the side navigation menu, and then tap **BROWSE FOR FIRMWARE**.
3. In the file browse window, tap the desired drive or network file share and then use the **Browse** window to navigate to the folder that contains the firmware package file.
4. Select the desired firmware package file (`.tx2_pkg`) and then tap **SELECT** in the bottom-right corner.

   The browse window will automatically close, showing the name of the package file that was selected on the **About** screen.
5. Optional Tap **HASH FIRMWARE** to generate a hash of the selected firmware package file. This hash value can then be compared to the hash value from the source download page (from https://support.opentext.com) providing confidence that you will be updating your unit with the exact desired firmware package file.
6. Once you are confident you want to proceed with the update, tap **UPDATE**.

   The firmware update process starts.

Note: Depending on the state of the sub-system firmware packages on the unit, your device may perform multiple reboots/power-cycles. Do not interact with the unit or power it down during this time. Once the login screen or Home screen appears (depending on user configuration), your updated device is ready to use.

To update the firmware using the remote user interface:

1. Establish a remote user interface connection to the OpenText TX2 to be updated.
2. On the remote user interface, open the side navigation menu and select **About**.
3. Tap the **SELECT FILE** button in the **Upload device firmware** area.

   This launches a file browser window on your host system, allowing you to navigate to and select the desired firmware package file.
4. Check the name of the selected package file in the **Upload device firmware** area, then tap **UPLOAD DEVICE FIRMWARE** to initiate the firmware file upload.

   A progress bar appears, indicating that the file upload is in progress.

Caution

Navigating away from this page when a firmware file upload is in progress will stop the firmware update process.

Once the file has been fully uploaded, OpenText TX2 will automatically update its local firmware and reboot the unit.

Note: Depending on the state of the sub-system firmware packages on the unit, your device may perform multiple reboots/power-cycles. Do not interact with the unit or power it down during this time. Once the login screen or Home screen appears (depending on user configuration), your updated device is ready to use.

Updating the firmware with either of these methods will leave all previously stored user data (settings, logs, saved searches, HTTPS/802.1x certificates, etc.) intact. To wipe all user data from the system drive, perform a Factory Reset which is available at the bottom of the **System Settings** screen.

Regardless of the firmware update method used, the hash of the currently loaded firmware package is calculated and displayed in the top portion of the **About** screen. This allows for verification that the proper firmware version is running and that it has not been altered.

3.3 Media utilities (traditional media)

Accessible from the Sources, USB Accessories, or Destinations buttons at the bottom of the **Home** screen (and all locations that provide drive lists), OpenText TX2 provides the following media utilities for all traditional media types (mobile devices excluded):

- Eject
- Content Breakdown
- Reconfigure (destination/accessory only) – Includes HPA/DCO/AMA removal, Wipe, Enable Tableau Encryption, Format Filesystem
- Encryption Unlock (source or destination; Tableau, Opal, BitLocker, APFS)
- HPA/DCO/AMA Disable (ATA source drives only)
- Blank Check
- Browse Filesystem
- SMART (ATA drives only)
- Export (iSCSI target)

Note: Mobile devices connected to OpenText TX2 have host system interactions and capabilities that are very different from traditional media devices (HDDs, SSDs). The media utilities listed in this section are specific to traditional media devices. See "Mobile backup acquisition" on page 104 for information specific to that type of job.

3.3.1 Eject

This media utility is provided to allow for safe ejection of attached drives. Ejecting a drive removes it from the system software in a safe manner and is recommended before unplugging any attached media from a powered OpenText TX2. 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. Ejection of media being used in an active job will not be allowed until the job is complete.

Note: OpenText TX2 supports PCIe drive hot-swap. Ejection of PCIe drives is required prior to removal from a powered-on system. Failure to do so can result in unpredictable system behaviors.

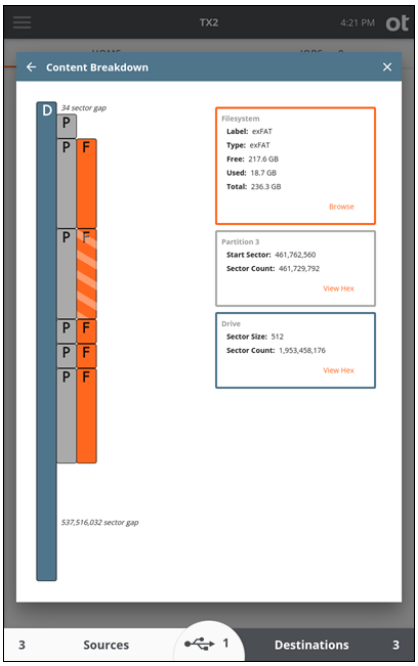
In addition to quiescing the drive for system removal, ejecting will issue an ATA spin down command to drives that may support it. Spinning down rotating hard disk drives is recommended to minimize the chance of platter damage upon physical removal of the drive from the system. Some drives do not support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

3.3.2 Content Breakdown

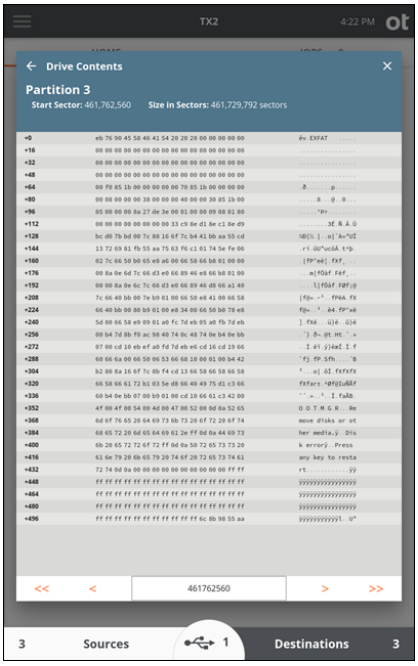
The **Content Breakdown** utility is available for all mounted drives and offers a unique perspective on drive geometry that is quite intuitive and powerful. This screen provides a physical map style overview of the selected drive and all its partitions and filesystems. Tapping on each element (rectangular box) of the drive map provides basic information about that element and allows further exploration. The selected element from the map is always shown at the top of the screen (in the right area), but the parent element information is also shown under the selected element.

Drive and **Partition** elements include sector-related information (sector size, sector count, and, for partitions, the starting sector) as well as a **View Hex** button, which opens a window that shows the selected drive or partition hex data on a sector-by-sector basis.

The following image shows the drive **Content Breakdown** screen for a drive that has multiple partitions, with one of its filesystems selected.

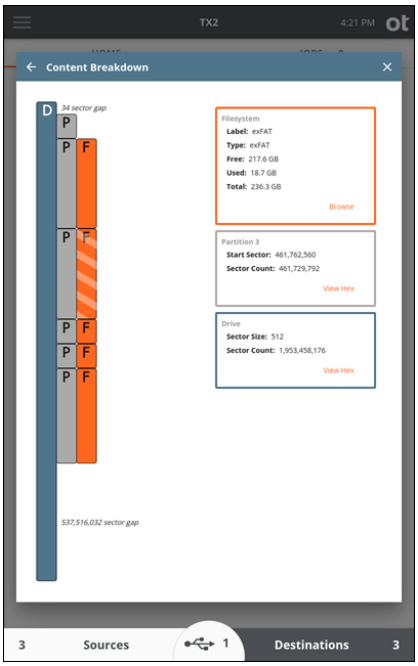


To view the raw hex data for a given drive/partition, tap the **View Hex** button within the information box. The following image shows a sample hex view window.



Each row shows 16 bytes of hex data, followed by each byte's ASCII equivalent. The number with the plus sign (located at the beginning of each row) represents the byte value offset from the start of the shown sector. The initial sector number (shown in the top blue header) is always the starting sector for the selected drive or partition. This starting sector number is also shown as the initial value in the rectangular box near the bottom of the screen (between the orange arrows). It is easy to navigate through the sectors within a given drive/partition and even into adjacent sectors by tapping the orange arrows. The single arrows will take you either one sector forward (right single arrow) or one sector backward (left single arrow). The double arrows will jump you to the next (or previous) boundary. That is to say, if you are in the middle of a given partition, the double-right arrow will jump to the end of that partition. Tapping the double-right arrow again in that scenario will take you to the beginning of the next partition or gap area (whichever happens to be there). These double-arrows make it easy to peruse an entire drive and see the very beginning and end of each drive element (partition or gap area), without having to go back to the map view to select a different element. A specific sector number can also be entered in the box at the bottom of the screen. Tap the box, enter the desired sector number, and tap outside the entry field to go directly to that sector.

Filesystem elements show basic filesystem information (label, type, and free/used/total space) and a **Browse** button that opens the OpenText TX2 standard browse modal, as shown in the following image.



3.3.3 Reconfigure

The **Reconfigure** utility provides an easy way to perform the following actions on a destination or accessory drive all in a single job:

- HPA/DCO/AMA removal
- Wipe
- Enable Tableau Encryption
- Format Filesystem

3.3.3.1 Remove HPA/DCO/AMA

If a destination or accessory drive has an HPA, DCO, or AMA drive capacity limitation set, it will be removed when this **Reconfigure** option is selected. For detailed information regarding these types of drive configurations, see "Removing drive capacity limiting configurations" on page 46.

Note: This specific function (within the **Reconfigure** utility on destination and accessory drives) is a non-volatile (or permanent) HPA/DCO/AMA removal.

3.3.3.2 Wipe

The **Wipe** portion of **Reconfigure** provides three wipe types for destination and accessory drives.

Note: Wiping drives results in sustained writing of the media, which can create abnormally high thermal operating conditions inside the drive. OpenText highly recommends using the `TX2-S1` drive bay (which has active cooling) or an external drive cooler or fan when wiping media on your device, to help prevent thermal damage to drives.

Overwrite	This method writes known pattern data to every accessible region of a drive. This can be done with one pass or multiple passes. Verification is optional.
Secure Erase	This method is only available for ATA-based SSDs that support the command. OpenText TX2 only issues the **Secure Erase** command to the drive, and the rest is done by the controller on the drive. Verification is not supported with this method, because the state of the post-wipe data on the drive is drive manufacturer-specific.
Sanitize	This method is available for ATA and SCSI-based media (both rotating and SSD) that support the command. Two wipe options are available for drives that support Sanitize – **Overwrite** and **Block Erase**. The OpenText TX2 only issues the **Sanitize** command to the drive, and the rest is done by the controller on the drive. Verification is optional. **Note:** An active **Sanitize** wipe may make a drive unresponsive for an extended period of time.

The exact differences between **Secure Erase** and **Sanitize** can be subtle, depending on the drive manufacturer's implementation. In general, 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.

Note: **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 the OpenText TX2'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 the support of post-wipe verification. If you experience **Sanitize** wipe verification failures, contact OpenText Customer Support to report the specific make and model of the drive.

The following table provides **Wipe** option details.

Option	Description
Overwrite - One Pass	OpenText TX2 writes a constant pattern to the destination or accessory drive in a single pass. If a custom wipe pattern is set, it will be written to the drive. Otherwise, zeros will be written. Verification is optional. **Note:** When an HPA/DCO/AMA configuration is present on a drive, a toggle may be set when configuring the wipe job, to remove such configuration prior to starting the wipe, which will ensure the entire accessible drive space is overwritten.
Overwrite - Multiple Pass	OpenText TX2 performs three full write passes to the destination or accessory drive. The first pass writes zeros (`0x0000`) and the second pass writes ones (`0xFFFF`). When a custom data pattern is specified, it will be written only on the third pass. Otherwise, the third pass writes a randomly selected constant value between `0x0001` and `0xFFFE`. Verification is optional. If turned on, it can be configured to verify after each wipe pass or after only the last pass. **Note:** When an HPA/DCO/AMA configuration is present on a drive, a toggle may be set to remove such configuration prior to starting the wipe, which will ensure the entire accessible drive space is overwritten.
Secure Erase (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). Due to the indeterminate nature of the post-wipe data state, OpenText TX2 does not offer verification for Secure Erase wipes. Due to known issues with inconsistent and unreliable Secure Erase support on rotating drives (HDDs), OpenText TX2 only supports this feature on SSDs. **Note:** 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. OpenText TX2 will force the removal of any detected HPA/DCO/AMA configurations prior to starting a Secure Erase wipe, except for USB connected media. It cannot remove HPA/DCO/AMA configurations for USB-connected media, which means Secure Erase is not supported in that situation.

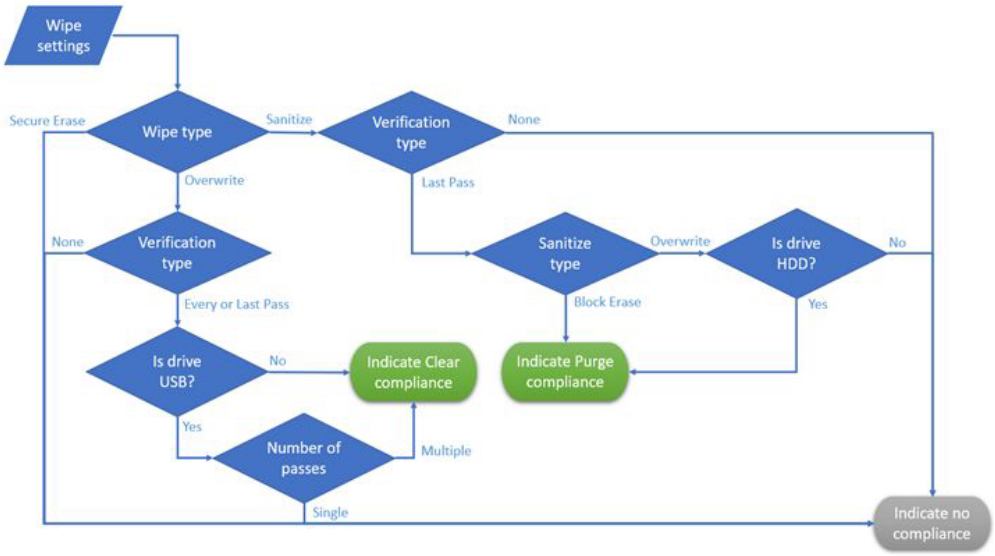
Option	Description
Sanitize – Overwrite	The ATA and SCSI Sanitize – Overwrite command instructs the drive to overwrite all drive data (in both storage and on-drive cache) with zeros. This feature is typically implemented on HDDs, but is available on some SSDs. **Note:** For SSDs that support Sanitize – 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. OpenText TX2 will force the removal of any detected HPA/DCO/AMA configurations prior to starting a Sanitize – Overwrite wipe, except for USB connected media. It cannot remove HPA/DCO/AMA configurations for USB-connected media, which means Sanitize - Overwrite is not supported in that situation.
Sanitize - Block Erase (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. **Note:** 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. OpenText TX2 will force the removal of any detected HPA/DCO/AMA configurations prior to starting a Secure Erase wipe, except for USB-connected media. It cannot remove HPA/DCO/AMA configurations for USB-connected media, which means Secure Erase is not supported in that situation.

NIST 800-88r1 Compliance

In the document *SP 800-88 r1: Guidelines for Media Sanitization*, the National Institute of Standards and Technology (NIST) describes two data sanitization methods – **Clear** and **Purge**. OpenText TX2 indicates compliance with these data sanitization methods when the appropriate wipe settings are selected – as indicated by the appropriate box turning green with a checkmark (at the top of the **NIST 800-88 r1 Compliance** area of the screen). Conversely, tapping either the **Clear** or **Purge** button (when this functionality is turned on) will automatically select compliant wipe settings.

OpenText TX2 can purge drives that support conformant Sanitize commands. The Purge **option** is deactivated if the **Sanitize** command is not supported by the drive.

The following flowchart depicts how OpenText TX2 determines wipe setting conformity to NIST 800-88 r1. This flowchart reflects handling of drives with no HPA/DCO/AMA settings.



3.3.3.3 Enable Tableau Encryption

OpenText TX2 can encrypt destination and accessory drives using a password-based XTS-AES whole disk encryption. This Tableau-based encryption is compatible with the OpenText Tableau Forensic TD2u Duplicator, OpenText Forensic TD4 Duplicator, OpenText Forensic TX1 Imager, and the open source *VeraCrypt* utility. This section only covers the encryption formatting option. For information regarding unlocking a drive with pre-existing Tableau encryption, see "Encryption Unlock" on page 42.

Note: The encryption formatting process overwrites the destination/accessory drive, so remember to copy any pre-existing drive data that is of value prior to encrypting the drive.

Caution

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

To remove encryption from a drive, connect the drive to the OpenText TX2 as a destination or accessory and wipe the drive.

Note: The **Reconfigure** media utility is not available for use on unlocked Tableau-encrypted drives. If you wish to perform any other Reconfigure functions on a drive that you intend to encrypt, those should all be done in one Reconfigure job.

3.3.3.4 Format Filesystem

To perform a duplication to or save logs to a drive, you must format the destination or accessory drive with a recognizable file system. OpenText TX2 supports formatting destination/accessory drives with the following file system formats: **exFAT**, **NTFS**, **EXT4**, **FAT**, or **HFS+**.

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.

Notes

- When FAT is selected as the filesystem type for a destination drive format, OpenText TX2 will format the drive as FAT32. However, job logs (including the format log) and all user interface elements will show this as FAT. That is because OpenText TX2 supports reading from all FAT formats (12, 16, and 32), and identifying them all as FAT is considered acceptable and accurate for filesystem identification purposes.
- OpenText TX2 cannot format a destination drive with an APFS filesystem, though it can mount a previously formatted APFS volume on any connected drive (source, destination, or accessory port).

3.3.4 Encryption Unlock

OpenText TX2 can unlock drives/volumes that have been encrypted with Tableau encryption, APFS, BitLocker, and Opal. APFS encryption support is limited to source drives, but Tableau, BitLocker, and Opal encrypted media can be unlocked regardless of which port they are connected to.

Whether dealing with Tableau, APFS, BitLocker, or Opal encryption on a given drive/volume, the same **Encryption Unlock** media utility is used to unlock it. A pull-down field at the top of the **Encryption Unlock** screen lists all the detected encrypted types on a given drive, whether they be at the whole disk or volume level.

To unlock an encrypted drive/volume:

1. Select the encrypted entity you want to unlock, enter the password (or BitLocker recovery key), and then tap **UNLOCK**.

   If successful, the progress bar turns green and a confirming message box appears.

2. Tap **OK** to close the message box and then close the **Encryption Unlock** screen to access the other functions with the now unlocked drive/volume.

   Once unlocked, each drive/volume can be used with any supported operations, including browsing, imaging (physical, logical, or mobile), and any applicable media utilities.

While unlocking Tableau, APFS, BitLocker, and Opal encryption is simple and done using the same **Encryption Unlock** media utility, there are some notable differences

in how OpenText TX2 handles these types of encryptions, that warrant special consideration, as covered in the following sections.

3.3.4.1 Opal encryption

OpenText TX2 can unlock Opal Self Encrypting Drives (SEDs) that have had their encryption enabled in a Linux environment, as described in "Encryption Unlock" on page 42. The presence of Opal encryption is noted in any area of the user interface that shows information about the attached drive, including drive tiles (which show in numerous locations), the **Drive Details** screen, and the **Content Breakdown** screen.

A locked Opal drive exposes no useful forensic information to OpenText TX2. The only options available for such media are ejection and unlocking. An unlocked Opal drive will appear as an unencrypted drive to the system and be usable for all supported forensic functions.

Note: The Opal standard does not specify an algorithm for generating a lock key from a plain text password. OpenText TX2 uses the Linux `SEDUTIL` function to report information about Opal drives and unlock them. This function uses an Opal-specific key generation algorithm, as defined by the Trusted Computing Group. Other systems exist for enabling encryption on Opal drives (for example, BitLocker), which may employ a key derivation algorithm other than what the `SEDUTIL` function uses. Attempting to use a known password for such drives using OpenText TX2 will result in failed unlock attempts. If you encounter such a situation, contact OpenText Customer Support.

An additional consideration for Opal drives is a unique configuration that exposes a Shadow MBR. This Shadow MBR can be enabled by drive/system manufacturers to initially identify the drive as a small, non-encrypted volume, which overrides the actual MBR information.

A typical use case for this configuration is to enable system manufacturers to request credentials from a user before revealing the actual MBR information on 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. OpenText TX2 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 in the **Sources** list, and the presence of an Opal MBR will be explicitly called out in the **Drive Details** screen. Note that the Shadow MBR configuration is essentially a unique form of a locked Opal drive, therefore unlocking the Opal encryption on OpenText TX2 will disable the Shadow MBR (regardless of the underlying encryption state) and make the full, unencrypted drive contents available for triage/acquisition. Also, Opal encryption unlock (including Shadow MBR disablement) is a volatile change, meaning that the drive will revert to its original configuration after it is power-cycled.

Caution

Docking station devices that contain Opal drives must support ATA command pass-through for the OpenText TX2 to properly detect the

presence of Opal encryption and allow it to be unlocked. 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 OpenText TX2 user interface. Use caution when acquiring any docking station-based media. If you suspect a drive in a docking station is Opal-encrypted, but is not being presented that way in your device display, removing the drive from the enclosure and connecting it directly to OpenText TX2 may yield the desired outcome.

3.3.4.2 BitLocker encryption

OpenText TX2 can unlock drives and partitions that are encrypted with Microsoft BitLocker, as described in "Encryption Unlock" on page 42. The presence of BitLocker encryption is noted in any area of the user interface that shows information about the attached drive and/or partitions on the drive. This includes drive tiles (shown in the **Source** and **Destination** drive lists, among other locations), partition tiles (which show whenever a filesystem is being selected for an operation), the **Drive Details** screen, and the **Content Breakdown** screen.

Note: It is possible for BitLocker drives to have been originally encrypted and secured in a manner that your device will not be able to unlock/unencrypt. In particular, Smart Card and Trusted Platform Module (TPM) methods secure a BitLocker encrypted drive with hardware-based interactions that are not supported by your device.

Unlike an Opal SED, a BitLocker drive can be physically imaged (`E01`, `Ex01`, `DD`, and `DMG`) or cloned in its encrypted state. Such evidence can then be used with forensic investigation tools, such as OpenText Forensic, to unencrypt and analyze the evidence.

Once unlocked, the drive/partition can be used for any supported operations, including browsing, logical imaging, and any applicable media utilities. While OpenText TX2 cannot format media as BitLocker, any previously formatted BitLocker drives/partitions can be unlocked and used as a destination for file-based operations, such as writing image files and exporting logs.

Note: BitLocker encryption can be disabled, which is also known as **Clear Key** mode. While the data at rest remains encrypted in this mode, a password or recovery key is not required to unlock the encryption. The OpenText TX2 method to unlock a disabled BitLocker drive/partition is similar to the method described in this section, except that the **Password/Recovery Key** field will be disabled. Instead, OpenText TX2 will retrieve the **Clear Key** from the BitLocker metadata and use it to unlock the encrypted drive/partition.

When a drive/partition is BitLocker-encrypted, it is assigned a Recovery ID number. OpenText TX2 will display the assigned BitLocker **Recovery ID** on the **Encryption Unlock** screen, which can help to identify specific drives that require a specific password/recovery key.

3.3.4.3 APFS encryption

OpenText TX2 can unlock drive volumes that are encrypted with APFS, as described in "Encryption Unlock" on page 42. The presence of an encrypted APFS volume is noted in any area of the user interface that shows information about the attached drive, including drive tiles (which show in numerous locations), the **Drive Details** screen, and the **Content Breakdown** screen.

Once unlocked, the APFS volume can be used for any supported operations including browsing, imaging (physical or logical), and any applicable media utilities.

It is important to note that there are distinct and critical differences in how OpenText TX2 handles the various encryption methods that it can unlock – APFS, BitLocker, Opal, and Tableau encryption. The following table summarizes how each of these encryption types will appear or be used in various operations, in both their locked and unlocked states.

		Operation				
		Logical Image (Source)	**Physical Image/ Clone (Source)**	**Wipe (Dest)**	**Format (Dest)**	**Blank check (Source/ Dest)**
APFS	**Locked**	n/a (no filesystems to image from)	Full drive will be imaged/ cloned; encrypted state	Clears drive starting at sector/ block 0	n/a (no APFS support on destination)	Checks full drive starting at sector/ block 0
	Unlocked	Selected files/ folders will be imaged	Full drive will be imaged/ cloned; encrypted state	Clears drive starting at sector/ block 0	n/a (no APFS support on destination)	Checks full drive starting at sector/ block 0
BitLocker	**Locked**	n/a (no filesystems to image from)	Full drive will be imaged/ cloned; encrypted state	Clears drive starting at sector/ block 0	Will overwrite existing formatting, including BitLocker	Checks full drive starting at sector/ block 0
	Unlocked	Selected files/ folders will be imaged	Full drive will be imaged/ cloned; encrypted state	Clears drive starting at sector/ block 0	Will overwrite existing formatting, including BitLocker	Checks full drive starting at sector/ block 0
Opal	**Locked**	n/a (no reads possible)	n/a (no reads possible)	n/a (no writes possible)	n/a (no writes possible)	n/a (no reads possible)

		Operation				
		Logical Image (Source)	**Physical Image/ Clone (Source)**	**Wipe (Dest)**	**Format (Dest)**	**Blank check (Source/ Dest)**
	Unlocked	Selected files/ folders will be imaged	Full drive will be imaged/ cloned; unencrypted state	Clears drive starting at sector/ block 0	Formats drive starting at sector/ block 0	Checks full drive starting at sector/ block 0
Tableau	**Locked**	n/a (no filesystems to image from)	Full drive will be imaged/ cloned; encrypted state	Clears drive starting at sector/ block 0	Not allowed	Not allowed
	Unlocked	Selected files/ folders will be imaged	Only the unlocked encryption container contents will be imaged/ cloned; unencrypted state	Clears only the unlocked encryption container leaving encryption intact	Formats unlocked encryption container only leaving encryption intact	Checks contents of unlocked encryption container only

3.3.5 Removing drive capacity limiting configurations

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) or DCO (device configuration overlay) feature sets. The ACS-3 (ATA/ATAPI Command Set 3) specification update introduced the concept of Addressable Maximum Address (AMA). Newer drives may support this method of limiting the reported drive capacity.

OpenText TX2 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 or not to acquire data in the hidden regions of the drive.

Note: Removing drive capacity limiting configurations applies to both source and destination drives. For source drives it is a stand-alone media utility, but for destination drives it is part of the **Reconfigure** utility. For details regarding HPA/DCO/AMA removal for destination drives, see "Reconfigure" on page 37.

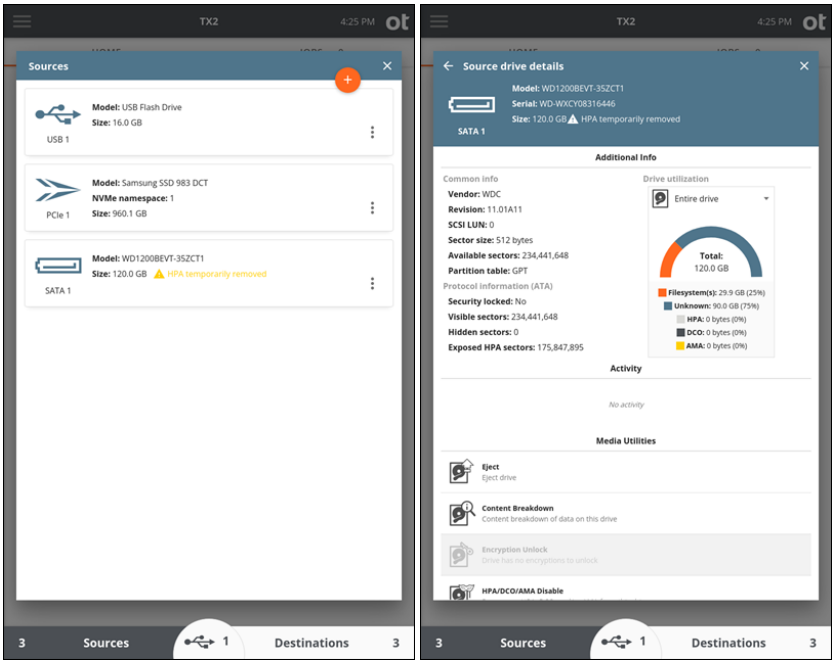
These methods (HPA/DCO and AMA) are mutually exclusive. A drive that supports HPA/DCO does not support AMA, and a drive that supports AMA does not support HPA/DCO. Also, while HPA and DCO are related features for a given drive, HPA has a unique attribute (volatile, or temporary, removal) that distinguishes it from DCO and AMA. For that reason, this section covers the volatile HPA removal as a

separate topic before addressing the non-volatile (permanent) removal of HPA/DCO or AMA.

3.3.5.1 Volatile HPA removal

An HPA can be removed 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 OpenText TX2 (or is otherwise powered down) and then re-powered, 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), your device automatically removes HPA on any drive connected to one of its source ports. Since DCO and AMA settings can only be removed on a permanent basis, your device does not automatically remove them on connected source drives.

In the case of an automatic, volatile HPA removal from a connected source drive, a message stating “HPA temporarily removed” will be shown in any affected drive tiles (**Sources** drive list) and in the header section of the associated drive details screen, as shown in the following images.



Referring to the drive details image, the fact that the HPA has been removed is reflected in the following areas on this screen:

- The **Size** field in the header reflects the full capacity of the drive (with HPA removed), along with a warning to draw attention to the HPA removal event.
- The **Drive utilization** data accurately reflects the existence of 0 bytes of HPA (since the HPA was removed).

- The **Protocol Information** area shows the fact that no sectors are currently hidden, as well as how many were exposed when the HPA was removed.

OpenText TX2 never makes automatic changes to any drive capacity-limiting configurations on destination drives. It 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, your device will not override that decision. For details regarding HPA/DCO/AMA removal for destination drives, see "Reconfigure" on page 37.

3.3.5.2 Non-volatile HPA/DCO/AMA removal

The **HPA/DCO/AMA Disable** media utility permanently removes the HPA, DCO, or AMA configurations on the source drive. 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 DCO or AMA configured, a red warning message is displayed on the drive tile indicating DCO or AMA is limiting the drive size. Permanently removing a DCO (and any HPA on that drive) or AMA is done using the **HPA/DCO/AMA Disable** utility found in the Media Utilities section of the source drive details screen. Drive details can be viewed through the **Sources** and **Destinations** areas of the main **Home** screen or from the **Select a Source** or **Select a Destination** areas during duplication job setup.

Note: Removing drive capacity limiting configurations applies to both source and destination drives. For source drives, it is a stand-alone media utility (**HPA/DCO/AMA Disable**), but for destination drives it is part of the **Reconfigure** utility. For details regarding HPA/DCO/AMA removal for destination drives, see "Reconfigure" on page 37.

OpenText TX2 also provides the ability to "shelve" a DCO or AMA, which will remove a source drive DCO or AMA for the purposes of evidence acquisition and then put the same DCO or AMA back after the job is complete. See "Duplicating" on page 58 for more details on shelving a DCO.

3.3.6 Blank checking

The **Blank Check** utility checks a drive for the presence of meaningful data.

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*.
Smart	Performs the **Fast** check, then reads in up to 75% of the available sectors randomly, to determine whether they are blank. The blank check will stop as soon as a non-blank data pattern is detected.

Option	Description
Complete	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.

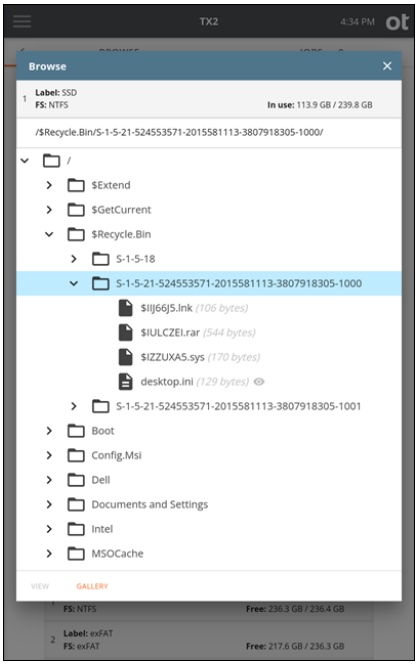
A sector is considered blank if it contains only the same repeated 2-byte pattern. Any non-repeating pattern is considered to be non-blank. However, each individual sector may contain different repeating patterns. If any sector is found to not be blank, the drive is not considered blank, and the blank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

Note: The **Fast** and **Smart** 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 the **Fast** or **Smart** check, while still storing forensically relevant information.

3.3.7 Browse Filesystem

The **Browse** function provides an easy way to view the contents of a recognized filesystem on any attached drive, whether it is connected locally or via the network interface (iSCSI or CIFS). Tap the **Browse** button on the Home screen and select the desired drive/filesystem. The **Browse** operation is also accessible from the **Media Utilities** list in the drive details screen and from the filesystem details box within the **Content Breakdown** media utility.

The following image shows a sample **Browse** screen.



The first row of the **Browse** window provides basic information about the selected filesystem (label, type, and used space). When multiple filesystems are present on a

drive, tapping the top information row will allow for selection of a different filesystem on the same drive, without needing to back out of the **Browse** window to select the other filesystem.

The second row of the **Browse** window shows the complete path name for the currently selected folder/file.

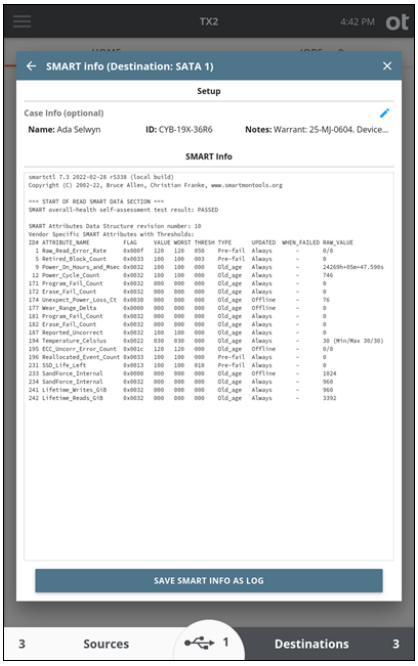
The main browse window (under the path name), shows the complete filesystem tree, including all folders/files contained on the drive or share.

In the browser portion of the window, you can scroll up and down the list of folders/files and tap individual folders to drill down to the desired level, to expose the names of individual files located on the drive. The size of each file is shown at the end of the filename. Many users will find this utility helpful when attempting to triage a large evidence set and determine the priority by which each drive should be imaged, or when checking the contents of a destination drive, to free up space by deleting unneeded directories and files.

Note: Certain text and image files can now be viewed directly on OpenText TX2. For more information about this feature, see "Viewing text and image files" on page 102.

3.3.8 SMART data

This media utility is available for ATA drives that support **SMART** data reporting. Selecting this feature will display available SMART data as reported by the drive, as shown in the following image.



This information can be annotated with case information, and saved as a log.

3.3.9 Export

This media utility allows the user to export any source, accessory, or destination drive as an iSCSI target in read-only mode. This makes the drive available to be read by a remote user on any IP-based network via the Ethernet connection on the rear of your device, which can be useful for evidence file transfer purposes.

During the export process, your device will assign a unique IQN (iSCSI Qualified Name) to each exported drive. This IQN is used by the remote initiator to gain access to the exported media. The following is an example of an IQN produced by OpenText TX2, by exporting a locally-connected SATA drive: `iqn.2015-10.com.guid:sn-000ecc5801000c.sata.1`.

The breakdown of this number is as follows.

Number Portion	Description
`iqn.2015-10.com.guid:`	Base identification number/domain for all OpenText Forensic Equipment products (as provided by the iSCSI naming authority).
`sn-000ecc5801000c.`	The serial number of the specific OpenText TX2 in use, which serves as a unique identifier within the domain.
`sata.1`	OpenText TX2 specific suffix. The default is the protocol of the drive being exported with an incrementing number at the end. However, the user can edit this portion of the IQN via the optional **Suffix** entry field on the **iSCSI Export** setup screen.

If successful, the final exported IQN is provided along with a listing of any initiator limits (IP address and/or IQN values). The IQN of the exported drive should then be available for selection via the **Discovery** function of an initiator on that same network.

Any exported drives can be un-exported by navigating to the **iSCSI Export** media utility for the drive and tapping the **Remove Export** button in the **iSCSI Export** screen.

3.4 Connecting drives

This section provides instructions for safely connecting drives to an OpenText TX2.

`TX2` operates as a standalone device or with the `TX2-S1` drive bay.

To connect the drive bay to TX2:

1. Ensure `TX2` is powered off.
2. Align `TX2` into place on top of the drive bay, and slide it back to lock it into place.

3.4.1 Source drives

Users can connect one or more drives to the OpenText TX2 source (left), write-blocked side interfaces: USB 3.2 Gen 2 Type C (x2), PCIe Gen 3x4 (x2), SATA Gen 3 (x2).

Note: While all OpenText TX2 device ports support hot swapping, it is highly recommended that all drives be ejected from the system before removing them. This is especially true of PCIe drives, which have a rather nuanced relationship with system level software.

An OpenText Forensic PCIe adapter (sold separately) is required to acquire PCIe drives. The OpenText Forensic IDE-PCIe adapter (TA7-5, sold separately) is required to acquire IDE drives. The OpenText Forensic FireWire-PCIe adapter (TA7-9, sold separately) is required to acquire FireWire media. For more information about adapters available for OpenText TX2, see “Adapters“ on page 135.

To acquire SAS drives, an OpenText T6u Forensic SAS bridge (sold separately) may be used on any source USB port. Alternatively, there are many high quality and reliable commercially available SAS-USB adapters that can be used.

OpenText TX2 can acquire certain Apple computers that support Target Disk Mode via the USB 3.0 or FireWire source side connections. This can be done via three different types of Apple computer interfaces: USB Type C, FireWire, and Thunderbolt. Commercially available adapters are required to convert these interfaces to USB for connecting to OpenText TX2. For more information about the required adapters, see “Adapters“ on page 135 or contact OpenText Customer Support.

OpenText TX2 can acquire backup files from Apple and Android mobile devices. This done by directly connecting the mobile device to one of the OpenText TX2 USB Type C ports. For more information, see “Mobile backup acquisition” on page 104.

OpenText TX2 also provides two 1/10 Gbps RJ-45 Ethernet connections, which allow the use of network-based acquisition of iSCSI physical media (clones and physical or logical images) and mounted CIFS shares (logical images). For more information, see “Duplication over a network” on page 73.

Source drives are listed in the user interface in the order of the OpenText TX2 physical port layout: iSCSI/CIFS, USB 1, USB 2, PCIe 1, PCIe 2, SATA 1, SATA 2.

3.4.2 Destination drives

Users can connect one or more drives to the OpenText TX2 destination (right) side interfaces: USB 3.2 Gen 2 Type C (x2), PCIe Gen 3x4 (x2), SATA Gen 3 (x2).

Two additional SATA Gen 3 destination ports are available through use of the OpenText Forensic `TX2-S1` Drive Bay (sold separately). This is a drive docking bay that attaches to the bottom of the imager, allowing for cable-free attachment of up to two 2.5" or 3.5" SATA destination drives. `TX2-S1` also includes built-in fans to help keep drives cool during acquisition jobs.

OpenText TX2 also provides two 1/10 Gbps RJ-45 Ethernet connections, which allow the use of network-based iSCSI physical media and CIFS shares as destinations, to store clone or image file data. For more information, see "Duplication over a network" on page 73.

Destination drives are listed in the user interface in the order of the OpenText TX2 physical port layout: iSCSI/CIFS, USB 1, USB 2, PCIe 1, PCIe 2, SATA 1, SATA 2.

3.4.3 Accessory drives

Users can connect up to two USB drives to the Accessory USB 3.2 Gen 1 Type C ports on the front of OpenText TX2. These drive interfaces are mostly used for saving stored log files, loading HTTPS/802.1x certificates, or updating the firmware. They may also be used for other purposes, including attachment of a physical (wired or wireless) keyboard and/or mouse.

Caution

The USB accessory ports on your device are NOT write-protected! Evidence media should never be connected to these ports.

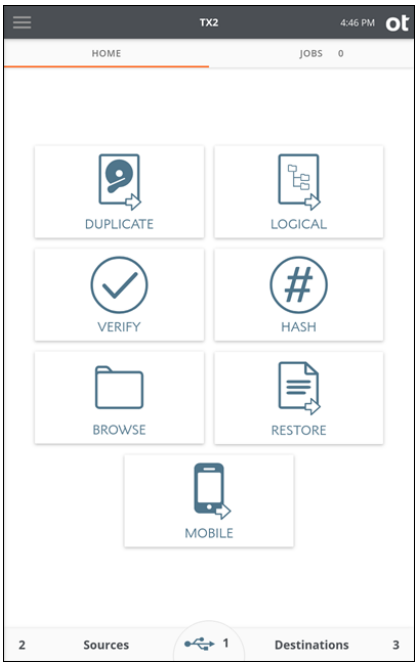
Accessory drives are listed in the user interface in the order of the OpenText TX2 physical port layout, with the leftmost USB drive always on top, and the rightmost USB drive on the bottom.

3.4.4 Drive detection

After booting, OpenText TX2 begins powering on and detecting connected drives, sequentially. Source and destination drive counts are displayed in the **Sources** and **Destinations** buttons at the bottom of the **HOME** screen, indicating the number of detected source and destination drives. If any accessory USB drives are connected and detected, the center USB accessory portion of that bottom row will appear with the detected accessory drive count.

Tap the **Sources**, **USB Accessory**, or **Destinations** button to view more details about the connected drives and to access media utilities.

The following screenshot shows the **HOME** screen and highlights the source, USB accessory, and destination drive counts.



OpenText TX2 can detect PCIe NVMe drives that have multiple namespaces defined. NVMe namespaces are similar to SCSI Logical Units (LUNS) in that there can be multiple of them configured on a single physical drive and each appears as a distinct drive in the imager's user interface. Each namespace will have a distinct drive tile (as shown in the **Sources** and **Destinations** drive lists) and will be treated as an individual drive by the imager. It is important to note that namespaces can be "detached" from the controller on some NVMe drives. A detached namespace would normally not be exposed to a user when its parent drive is connected to a typical host computer, but OpenText TX2 will detect the presence of any such detached namespaces and inform the user of their presence, by way of a dedicated drive tile in the **Sources** and **Destinations** drive lists. When you see a drive tile with the *Unattached NVMe namespace* warning message, tap the tile and a media utility modal will appear, allowing you to attach the namespace. Enter case information (optional) and tap the **ATTACH NAMESPACE(S)** button to begin the attachment process. If successful, the namespace will show as a regular drive tile and that namespace will be usable for any forensic activity (browsing, logical imaging, physical imaging, etc.).

Your device 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. Your device cannot run these proprietary applications, as they are typically made for x86-based Windows systems, therefore OpenText TX2 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, OpenText TX2 will detect these drives and report their type.

Note: Mobile devices connected to OpenText TX2 have unique detection interactions compared to traditional media devices (HDDs, SSDs). Once connected and detected, they will be displayed in the **Sources** list, but the similarities with traditional media end there. For information specific to that type of job, see "Mobile backup acquisition" on page 104.

3.5 Turning off your unit

To turn off your unit:

1. Push the power button in the top left corner of the unit.

   The shutdown options will be different for an idle unit versus one that has active/queued jobs.

2. For an idle unit, confirm the request by tapping the **SHUTDOWN** button, or keep the unit powered up by tapping the **CANCEL** button.

3. For a unit with active/queued jobs, the choices are expanded to include an option to wait for jobs to complete before the unit is turned off. This feature is convenient for running a job overnight or over a weekend with the unit unattended, as it will help reduce power consumption and unnecessary runtime on any attached drives.

   To turn off your unit when the current job(s) is (are) complete, push the power button in the top left corner of the unit, and then tap the **WAIT FOR JOBS** button.

   After all active/queued jobs complete, the unit will power itself off. This will work for any job type.

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

Chapter 4

Using the OpenText Forensic TX2 Imager

This chapter provides detailed procedures and information for using OpenText TX2.

4.1 Navigating OpenText TX2 features and options

The OpenText TX2 user interface includes the following elements:

- **Home** screen: Provides access to the following functions:
  - Duplicate
  - Logical
  - Verify
  - Hash
  - Browse
  - Restore
  - Mobile
  - Sources, Accessory Drives, and Destinations
    - View connected drive detail
    - Access media utilities
- **JOBS** screen: Provides the Job summary list and job details/status.
- **Side navigation menu**: Provides access to the following functions:
  - Home shortcut
  - Logs
  - Settings (system, network, and operation defaults)
  - User Management
  - Lock system
  - About
  - User

4.2 Preconditions checking

Before starting duplications and other jobs, OpenText TX2 automatically checks for preconditions. Some preconditions produce warnings, and you can choose to continue or cancel after viewing each one. Some preconditions are gating; they require mitigation or that the duplication process be stopped.

4.3 Duplicating

For each active job, OpenText TX2 duplicates one source drive to up to four destination drives simultaneously. The destinations can be any combination of clone and/or image jobs, and a mix of network shares and/or locally attached drives may be used.

There is no predefined limit on the number of jobs that can be active at the same time. However, the system automatically monitors available processor resources as job requests are added and determines whether to start them or queue them. This helps to ensure maximum efficiency for all the requested jobs, by minimizing job context switching while simultaneously ensuring that processor resources are being fully utilized.

While it is recommended to let OpenText TX2 determine when to start jobs, this system may be manually overridden. To start a job that the system has decided to enqueue, tap and hold the **drag** icon near the queued job tile and drag it into the **Active Jobs** section. If reordering jobs is the goal, it is recommended to pause the lower priority active job(s) before manually activating a higher priority job.

Note: This section focuses on whole disk duplication operations. See "Logical imaging" on page 82 for details on that alternative acquisition method. See "Mobile backup acquisition" on page 104 for information specific to that type of job.

4.3.1 Cloning

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

If a destination drive is not blank, a yellow warning is displayed, to indicate that a clone will overwrite the contents of the destination drive. This reduces the risk of overwriting valuable data.

There is no need to format the destination media, as the clone will apply the file system of the source media (if one exists) to the destination media automatically. It is, however, a best practice to wipe destination media before duplicating to it, as this can help to identify potentially defective media and bad sectors, and it can reduce the risk of cross contaminating a duplication with stale data.

At the beginning of a clone job, your device 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. The device issues a warning when a sector size mismatch is detected. This condition will need to be rectified before the clone job can be started.

4.3.2 Physical imaging

A physical image, also known as disk-to-file duplication, copies the entire source drive to a series of files (sometimes called segments) on the destination drive(s). OpenText TX2 supports *EnCase* file formats `Ex01` and `E01` and raw file formats `DD` and `DMG`. Compression is supported and turned on by default with `Ex01` and `E01` file formats. File sizes from 4 GB per segment to Unlimited are supported. Smaller segments create more directory entries and Unlimited creates one large file segment.

Note: Due to filesystem addressing limitations, FAT32 formatted destinations have a maximum file size of 2 GB. If such a destination is detected by the imager, the output file size is automatically set to 2 GB with no option to change it.

When imaging, the destination media must first be formatted with a recognized filesystem. Format destination drives by selecting the **Reconfigure** media utility in the drive details screen. For more details, see "Reconfigure" on page 37. The drive details screen can be accessed through the **Destinations** button on the **Home** screen or through the **Select Destinations** screen during the setup of a duplication job.

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: Use caution when attempting to copy a source drive to a same size or smaller destination drive. Image file formatting adds overhead and, when coupled with incompressible data (such as encrypted data), a larger destination drive may be needed.