EnCase Forensic & Tableau v20.2 Release

OpenText commitment to Digital Forensics

May 2020

Today’s Speakers

SC 2020 awards Winner

Ashley Page
Forensic Account Executive
apage@opentext.com

Stephen Gregory
Sr. Principal Solutions Consultant
sgregory@opentext.com

EnCase v8 Releases – Quick Recap

8.05

- Mobile acquisition *
  25,000 different device types, including mobile phones, drones and smart devices
- Bookmarking a document as an image

8.06

- Lucene® index and search technology *
- Search using standard Lucene syntax
- Enhanced Indexing performance
- Index and search in multiple languages (20)

8.07

- Mac® APFS Support *
- Encryption/decryption updates
- Windows Volume Shadow Copy support *
- Add word delimiters to Search Index

8.08

- Office 365® email and Exchange connectors*
- Encryption/decryption updates
- MS Edge® internet artifacts
- Mac OS X ram and process acquisition
- APFS encryption support (APFS, FileVault2)*

EnCase v8 Releases – Quick Recap

8.09

- Improved –logging and auditing *
- Microsoft® PST 2013, 2016, 365 support *
- Firefox® artifact update
- Linux ram and process acquisition

8.10

- Performance Improvements *
- Lucene Indexing & stability improvements
- Parse OST files
- Analyze Apple Time APFS Snapshot *
- Enhanced Help file options
- Direct access to App Central from UI
- EnCase Mobile Acquisition enhancements *

8.11

- OpenText Media Analyzer module *
- Bug Fixes
- Performance improvements
- OS Support

Global Internet adoption and devices and connection

Nearly two-thirds of the global population will have Internet access by 2023.

5.3 billion total Internet users (66% of global population) by 2023

Increase from 3.9 billion (51%) in 2018.

Internet users

Devices connected to IP networks will be more than three times the global population by 2023.

3.6 networked devices per capita by 2023, up from 2.4 networked devices per capita in 2018.

29.3 billion networked devices by 2023, up from 18.4 billion in 2018.

Devices and connections

Over 70 % of the global population will have mobile connectivity by 2023.

Global mobile subscribers will grow from 5.1 billion (66% of population) in 2018 to 5.7 billion (71%) by 2023.

Mobility growth

* Source Cisco Annual Internet Report (2018-2023)

opentext™

EnCase Media Analyzer

OpenText Media Analyzer

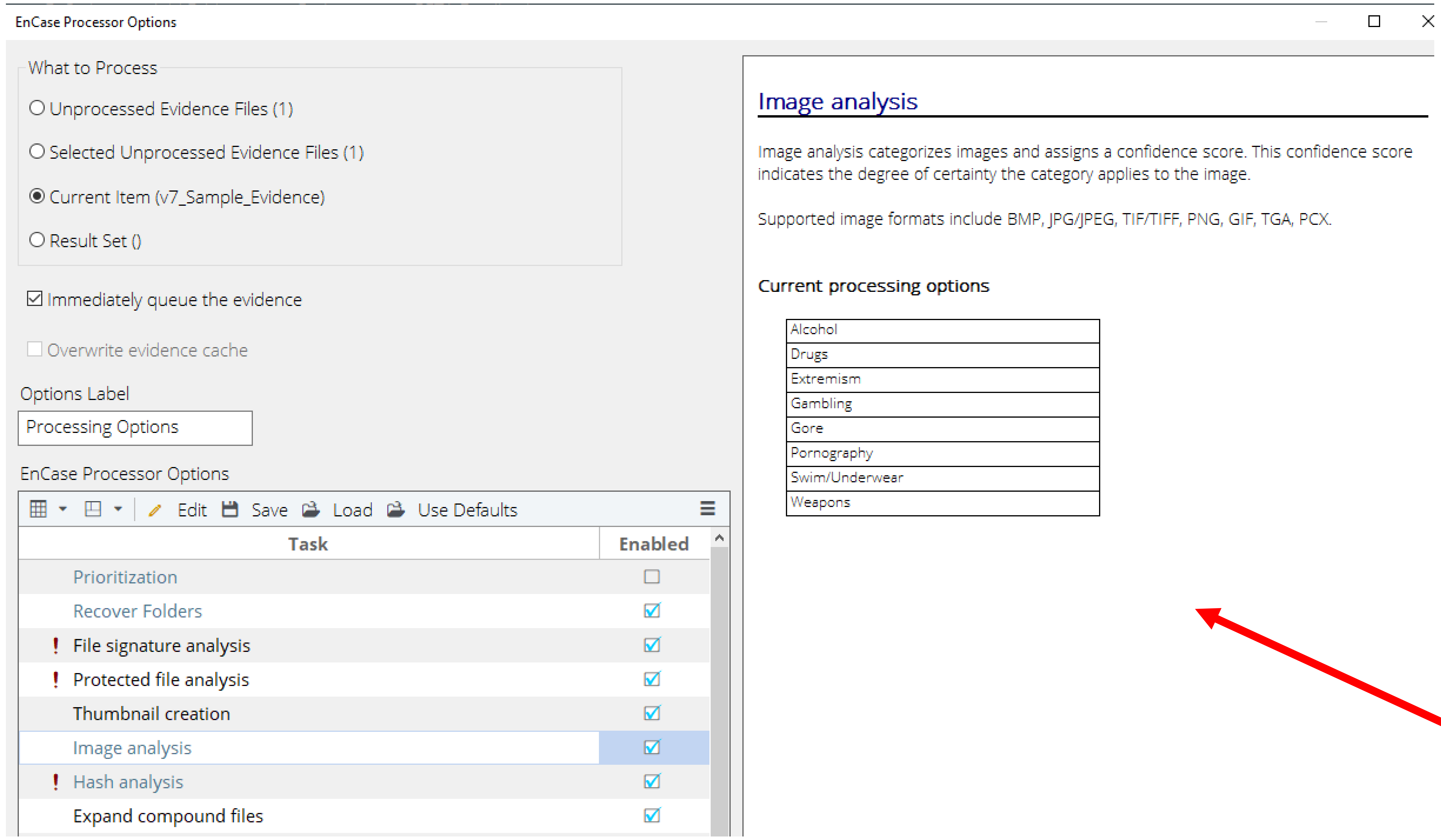
- Available in EnCase Processor and directly for triage in Gallery View
- Classifies and tags the images based on pre-defined risk profiles
- Uses visual markers to identify the images which match, even if they do not have a known fingerprint

AI computer vision technology

Alcohol
Currency
Drug
Gambling
ID / Credit Cards
Swim Underwear
CSAM
Pornography
Extremism
Gore
Documents
Weapons

Risk profiles\categories

OpenText Media Analyzer



EnCase Processor Options

What to Process

○ Unprocessed Evidence Files (1)

○ Selected Unprocessed Evidence Files (1)

● Current Item (v7_Sample_Evidence)

○ Result Set ()

☑ Immediately queue the evidence

☐ Overwrite evidence cache

Options Label

Processing Options

EnCase Processor Options

	Task	Enabled
	Prioritization	☐
	Recover Folders	☑
!	File signature analysis	☑
!	Protected file analysis	☑
	Thumbnail creation	☑
	Image analysis	☑
!	Hash analysis	☑
	Expand compound files	☑

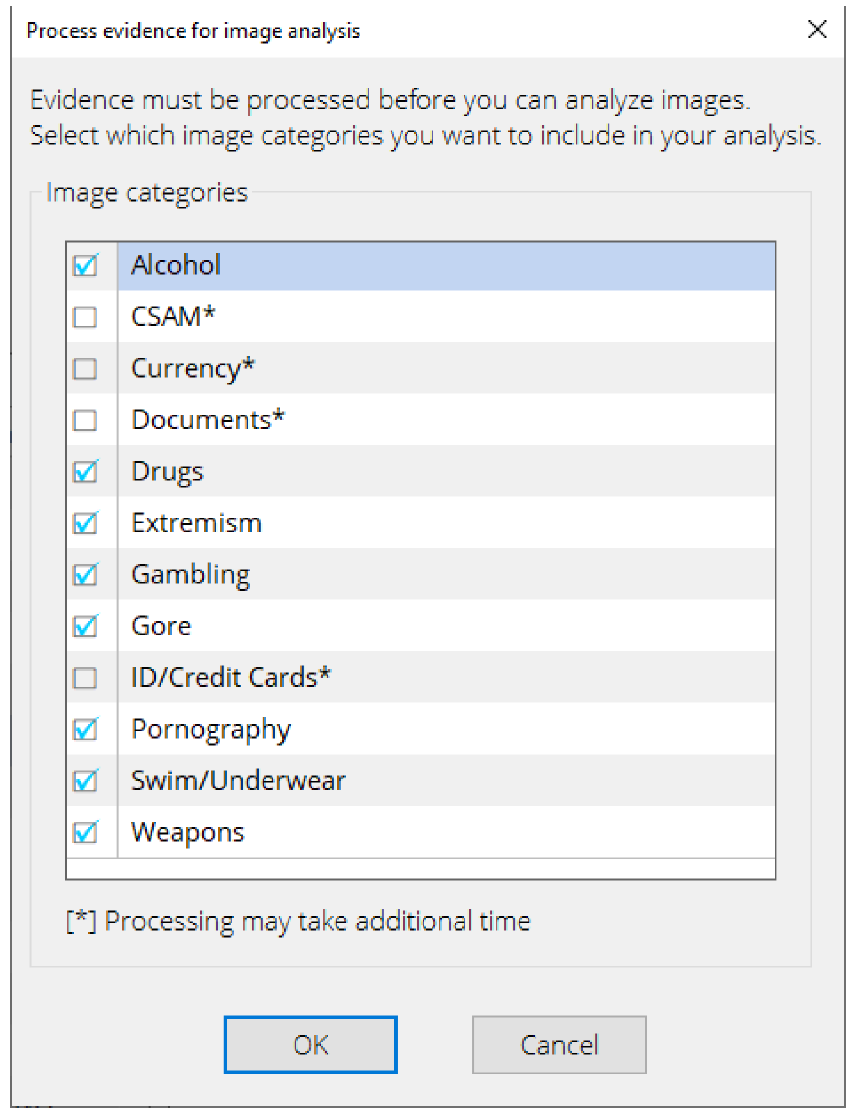
Image analysis

Image analysis categorizes images and assigns a confidence score. This confidence score indicates the degree of certainty the category applies to the image.

Supported image formats include BMP, JPG/JPEG, TIF/TIFF, PNG, GIF, TGA, PCX.

Current processing options

Alcohol
Drugs
Extremism
Gambling
Gore
Pornography
Swim/Underwear
Weapons



Process evidence for image analysis

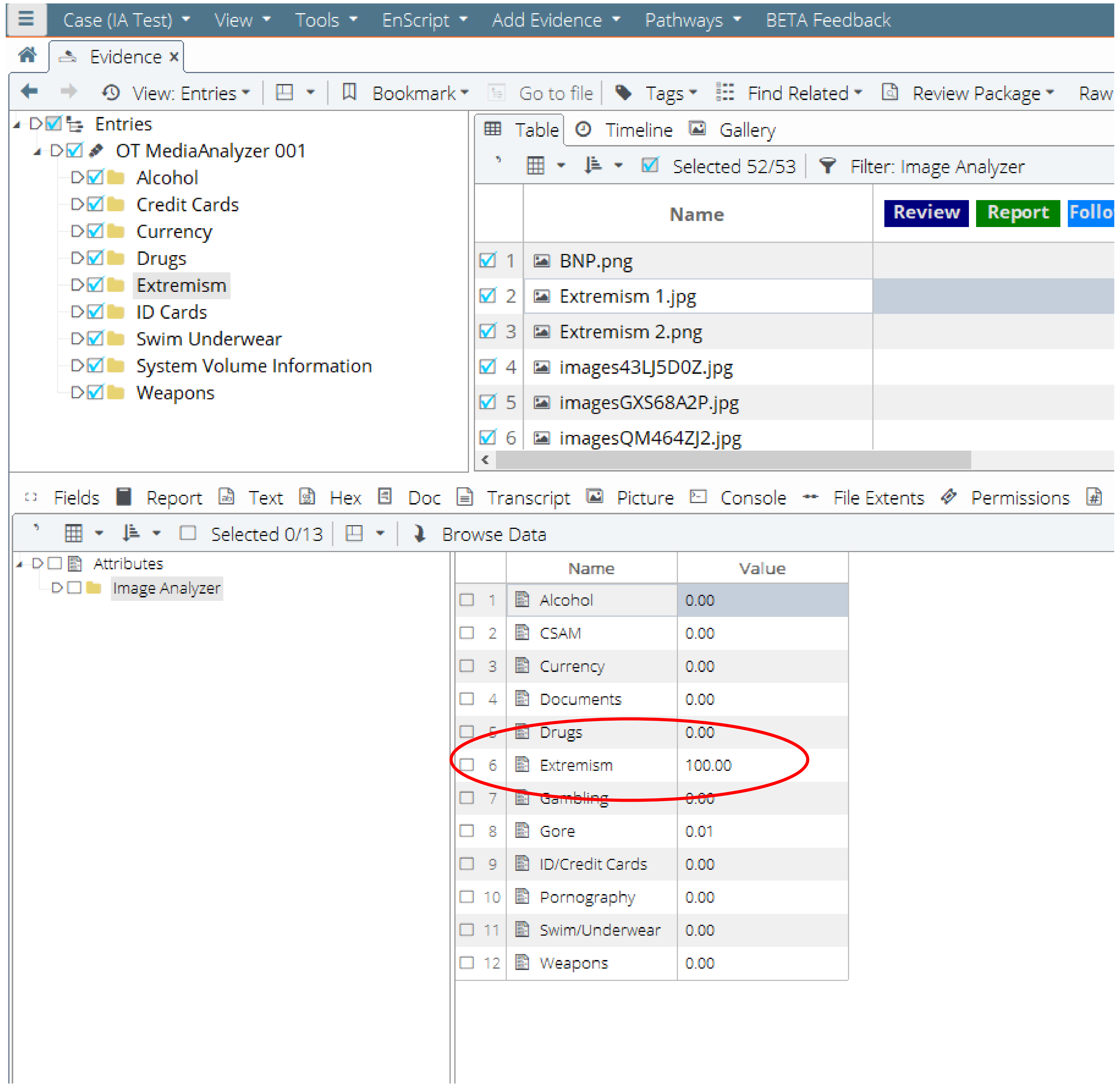
Evidence must be processed before you can analyze images. Select which image categories you want to include in your analysis.

Image categories

☑	Alcohol
☐	CSAM*
☐	Currency*
☐	Documents*
☑	Drugs
☑	Extremism
☑	Gambling
☑	Gore
☐	ID/Credit Cards*
☑	Pornography
☑	Swim/Underwear
☑	Weapons

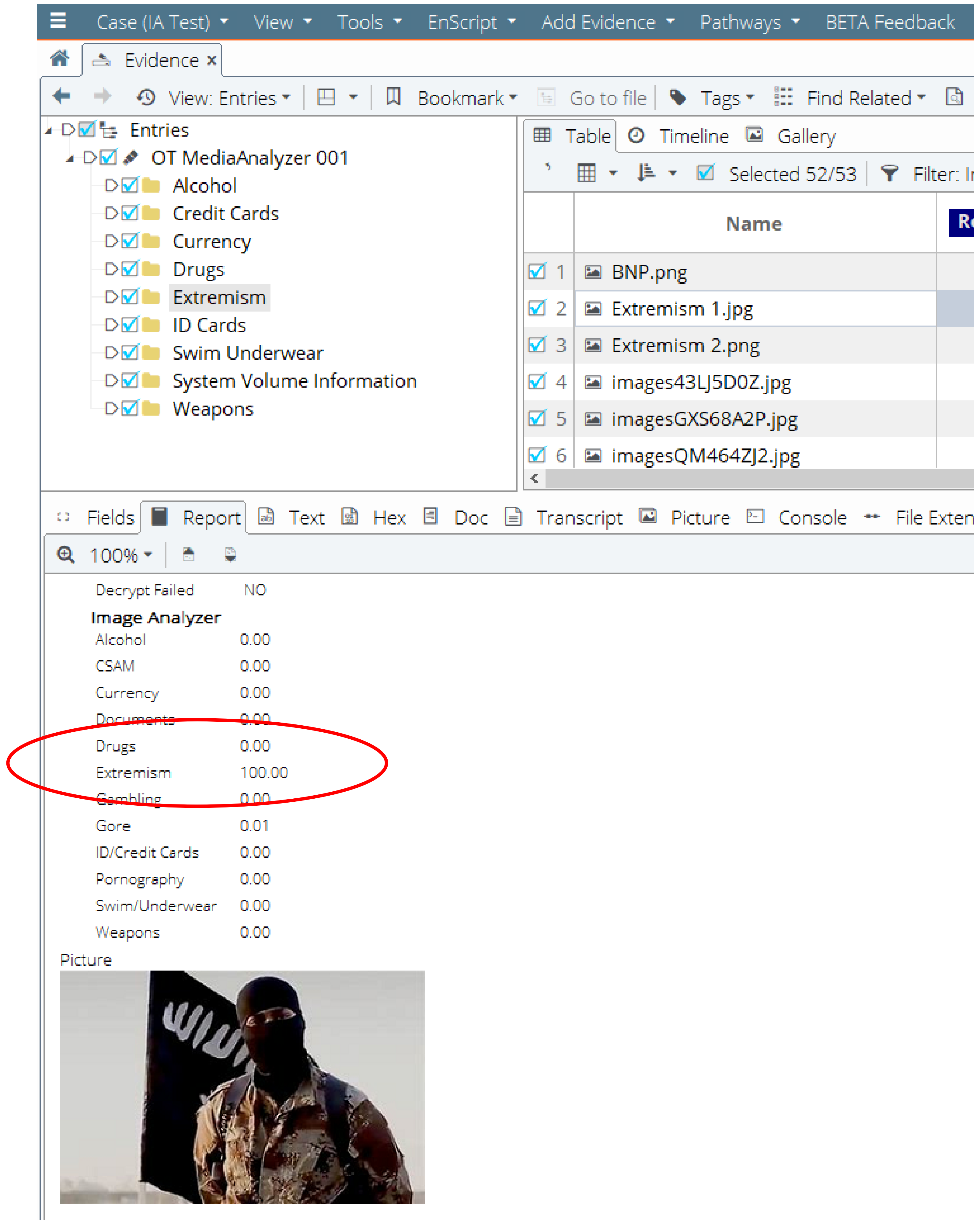
[*] Processing may take additional time

OpenText Media Analyzer



	Name	Review	Report	Follo
☑ 1	BNP.png			
☑ 2	Extremism 1.jpg			
☑ 3	Extremism 2.png			
☑ 4	images43LJ5D0Z.jpg			
☑ 5	imagesGXS68A2P.jpg			
☑ 6	imagesQM464ZJ2.jpg			

	Name	Value
☐ 1	Alcohol	0.00
☐ 2	CSAM	0.00
☐ 3	Currency	0.00
☐ 4	Documents	0.00
☐ 5	Drugs	0.00
☐ 6	Extremism	100.00
☐ 7	Gambling	0.00
☐ 8	Gore	0.01
☐ 9	ID/Credit Cards	0.00
☐ 10	Pornography	0.00
☐ 11	Swim/Underwear	0.00
☐ 12	Weapons	0.00



	Name
☑ 1	BNP.png
☑ 2	Extremism 1.jpg
☑ 3	Extremism 2.png
☑ 4	images43LJ5D0Z.jpg
☑ 5	imagesGXS68A2P.jpg
☑ 6	imagesQM464ZJ2.jpg

Decrypt Failed NO

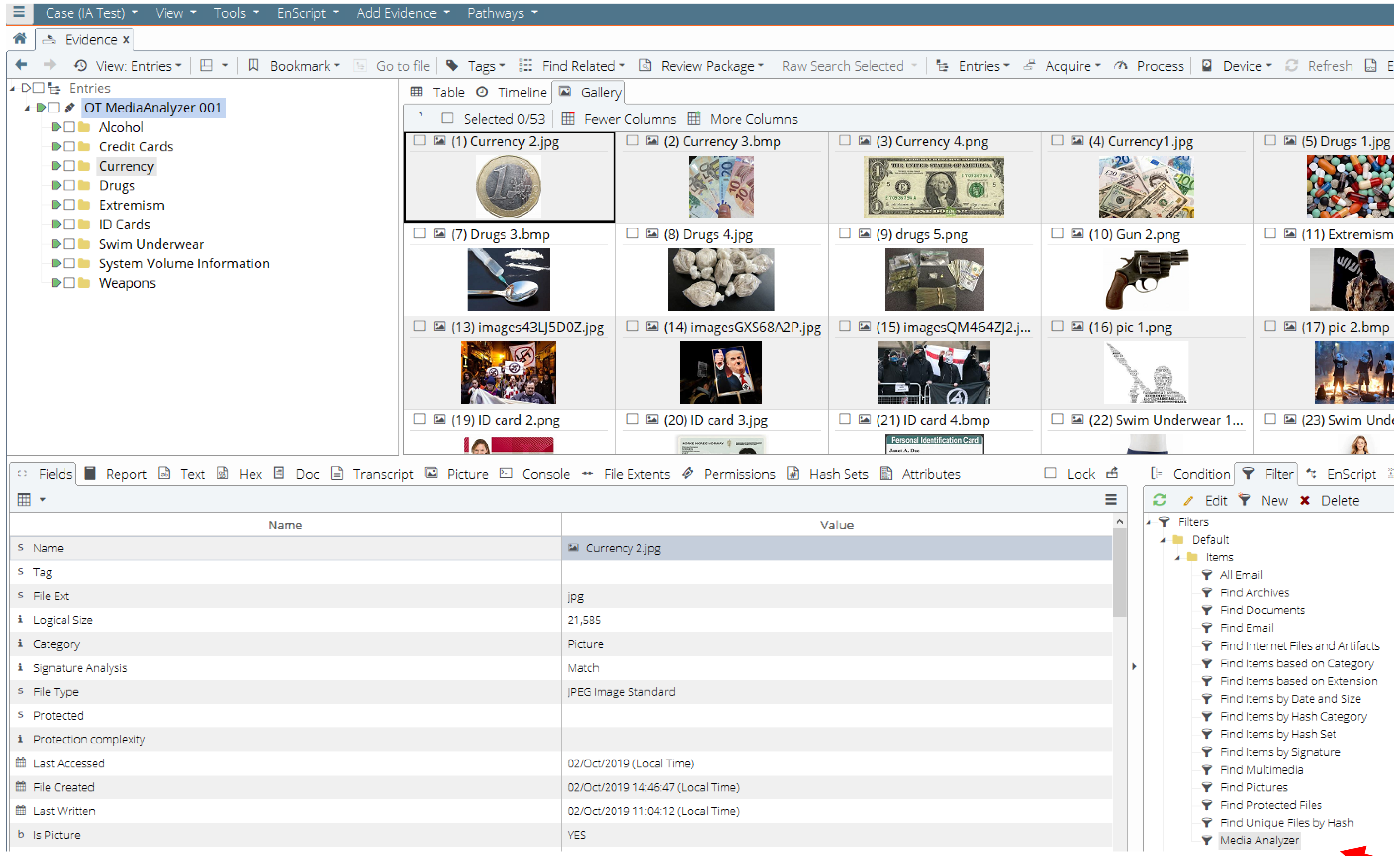
Image Analyzer

Alcohol	0.00
CSAM	0.00
Currency	0.00
Documents	0.00
Drugs	0.00
Extremism	100.00
Gambling	0.00
Gore	0.01
ID/Credit Cards	0.00
Pornography	0.00
Swim/Underwear	0.00
Weapons	0.00

Picture

OpenText Media Analyzer

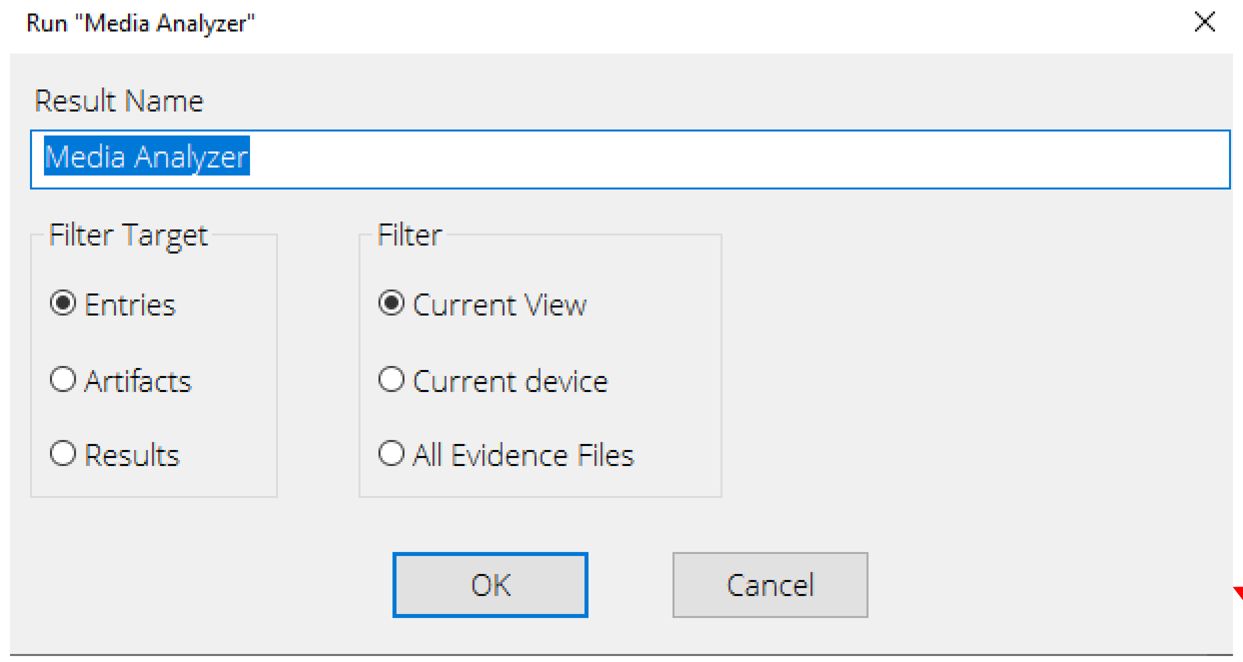
Add filters based on confidence levels



- Entries
  - OT MediaAnalyzer 001
    - Alcohol
    - Credit Cards
    - Currency
    - Drugs
    - Extremism
    - ID Cards
    - Swim Underwear
    - System Volume Information
    - Weapons

Name	Value
Name	Currency 2.jpg
Tag	
File Ext	jpg
Logical Size	21,585
Category	Picture
Signature Analysis	Match
File Type	JPEG Image Standard
Protected	
Protection complexity	
Last Accessed	02/Oct/2019 (Local Time)
File Created	02/Oct/2019 14:46:47 (Local Time)
Last Written	02/Oct/2019 11:04:12 (Local Time)
Is Picture	YES

- Filters
  - Default
    - Items
      - All Email
      - Find Archives
      - Find Documents
      - Find Email
      - Find Internet Files and Artifacts
      - Find Items based on Category
      - Find Items based on Extension
      - Find Items by Date and Size
      - Find Items by Hash Category
      - Find Items by Hash Set
      - Find Items by Signature
      - Find Multimedia
      - Find Pictures
      - Find Protected Files
      - Find Unique Files by Hash
      - Media Analyzer


Run "Media Analyzer"

Result Name: Media Analyzer

Filter Target

● Entries

○ Artifacts

○ Results

Filter

● Current View

○ Current device

○ All Evidence Files

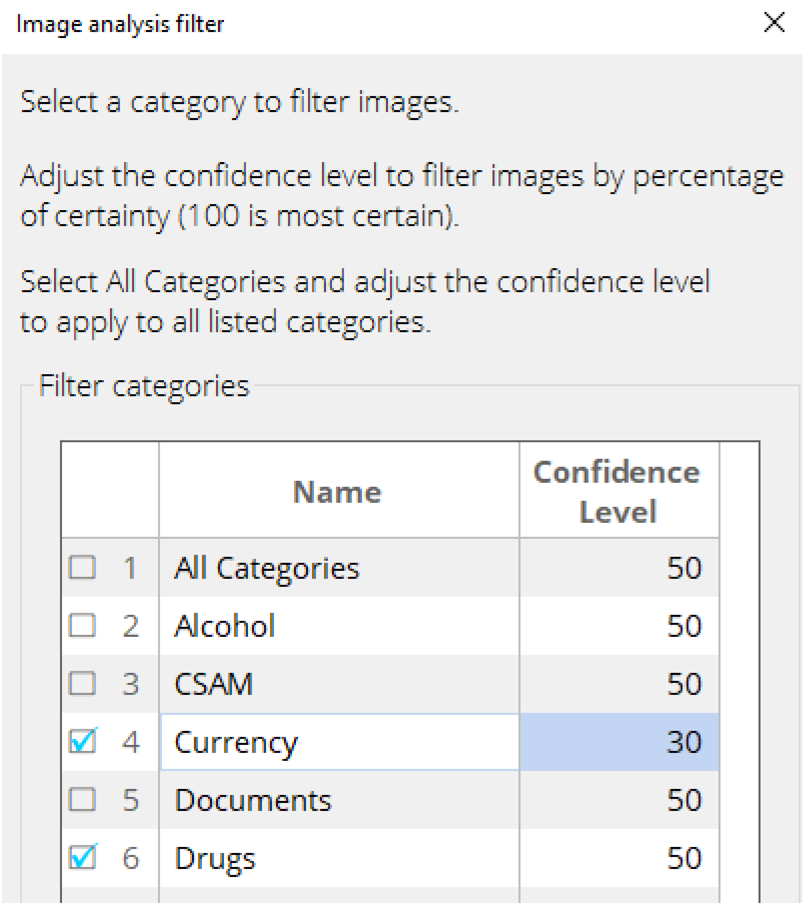


Image analysis filter

Select a category to filter images.

Adjust the confidence level to filter images by percentage of certainty (100 is most certain).

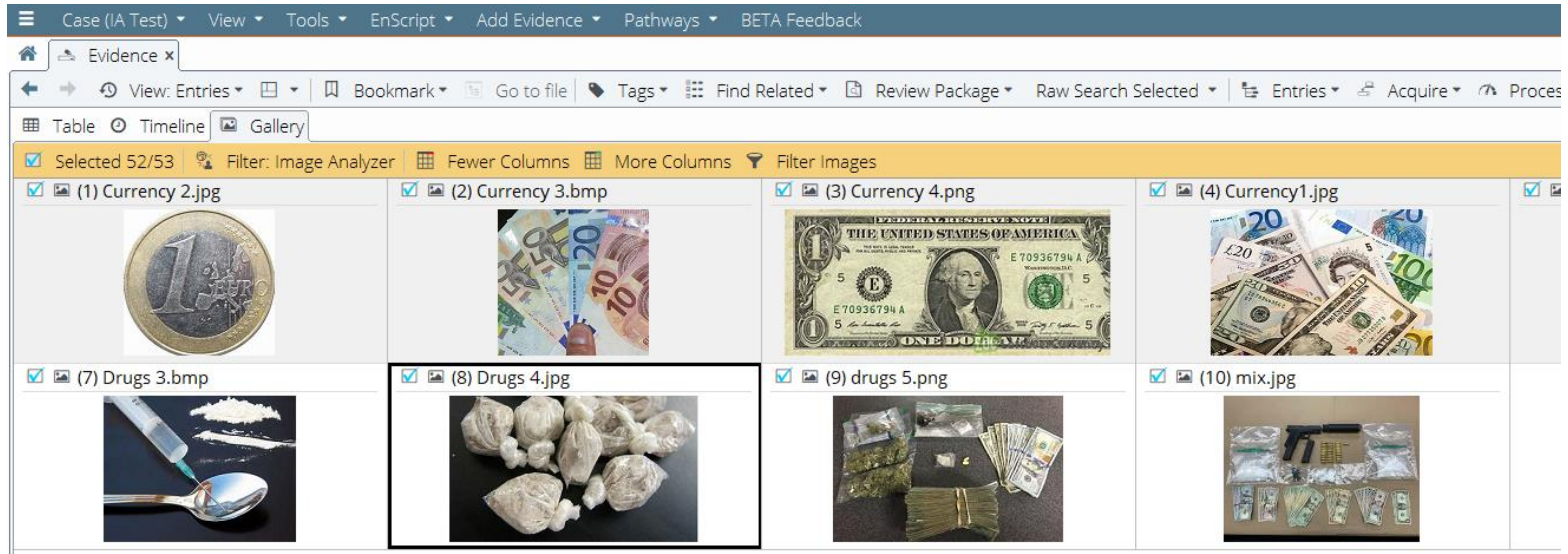
Select All Categories and adjust the confidence level to apply to all listed categories.

Filter categories

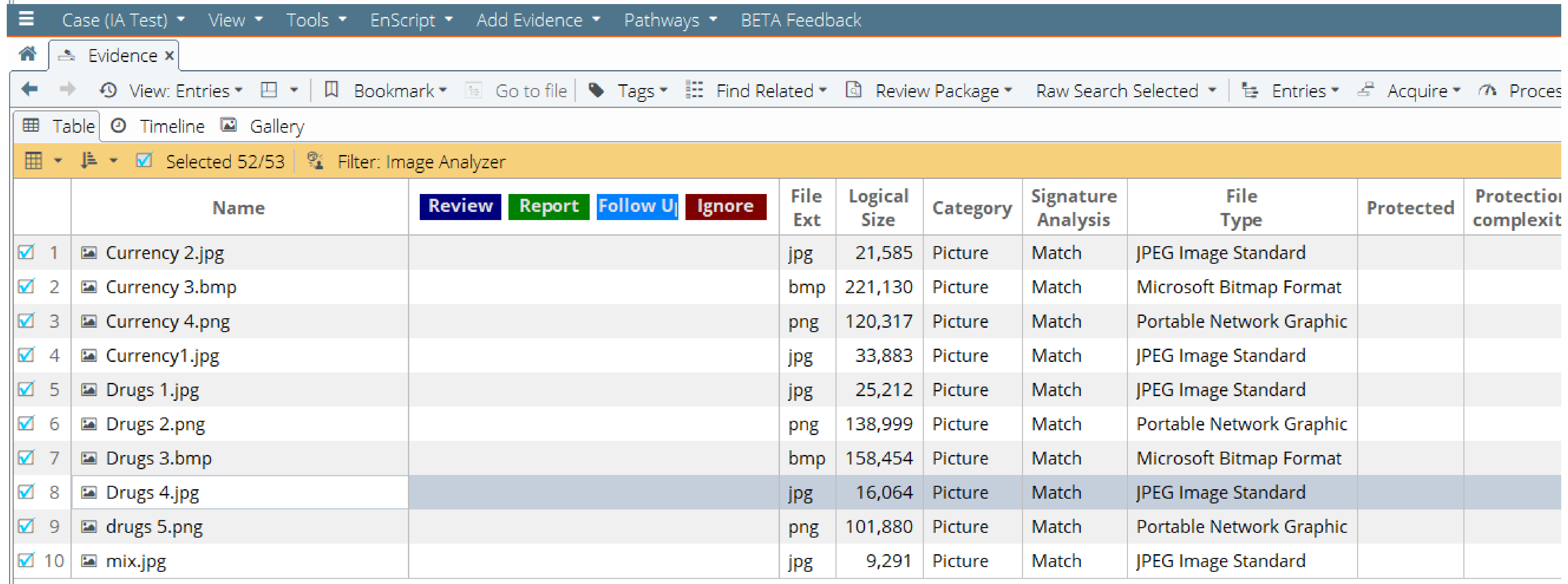
		Name	Confidence Level
☐	1	All Categories	50
☐	2	Alcohol	50
☐	3	CSAM	50
☑	4	Currency	30
☐	5	Documents	50
☑	6	Drugs	50

opentext™

OpenText Media Analyzer



Case (IA Test) View Tools EnScript Add Evidence Pathways BETA Feedback
Evidence ×
View: Entries Bookmark Go to file Tags Find Related Review Package Raw Search Selected Entries Acquire Proces
Table Timeline Gallery
Selected 52/53 Filter: Image Analyzer Fewer Columns More Columns Filter Images
(1) Currency 2.jpg
(2) Currency 3.bmp
(3) Currency 4.png
(4) Currency1.jpg
(7) Drugs 3.bmp
(8) Drugs 4.jpg
(9) drugs 5.png
(10) mix.jpg



Case (IA Test) View Tools EnScript Add Evidence Pathways BETA Feedback
Evidence ×
View: Entries Bookmark Go to file Tags Find Related Review Package Raw Search Selected Entries Acquire Proces
Table Timeline Gallery
Selected 52/53 Filter: Image Analyzer

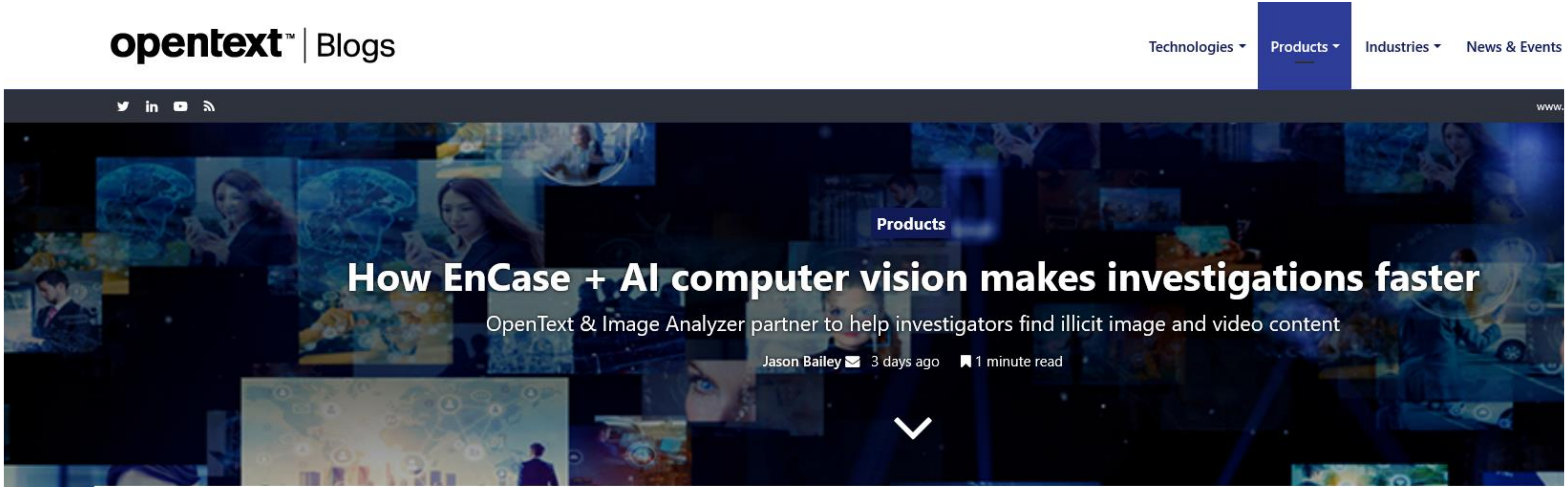
	Name	Review Report Follow U Ignore	File Ext	Logical Size	Category	Signature Analysis	File Type	Protected	Protection complexit
☑ 1	Currency 2.jpg		jpg	21,585	Picture	Match	JPEG Image Standard		
☑ 2	Currency 3.bmp		bmp	221,130	Picture	Match	Microsoft Bitmap Format		
☑ 3	Currency 4.png		png	120,317	Picture	Match	Portable Network Graphic		
☑ 4	Currency1.jpg		jpg	33,883	Picture	Match	JPEG Image Standard		
☑ 5	Drugs 1.jpg		jpg	25,212	Picture	Match	JPEG Image Standard		
☑ 6	Drugs 2.png		png	138,999	Picture	Match	Portable Network Graphic		
☑ 7	Drugs 3.bmp		bmp	158,454	Picture	Match	Microsoft Bitmap Format		
☑ 8	Drugs 4.jpg		jpg	16,064	Picture	Match	JPEG Image Standard		
☑ 9	drugs 5.png		png	101,880	Picture	Match	Portable Network Graphic		
☑ 10	mix.jpg		jpg	9,291	Picture	Match	JPEG Image Standard		

- Law Enforcement Agencies
  - Advanced AI delivers high detection and near zero false positives
  - Speed up CSAM Investigations
  - Reduce case back logs

- Corporates
  - Computer Misuse Investigations
  - Verify Employee Misconduct
  - Perform Internal Audits
  - Embedded SDK available – no content sent to the cloud assuring data and evidence integrity

Where to find more information

- Opentext Blogs



Products

How EnCase + AI computer vision makes investigations faster

OpenText & Image Analyzer partner to help investigators find illicit image and video content

Jason Bailey 3 days ago 1 minute read

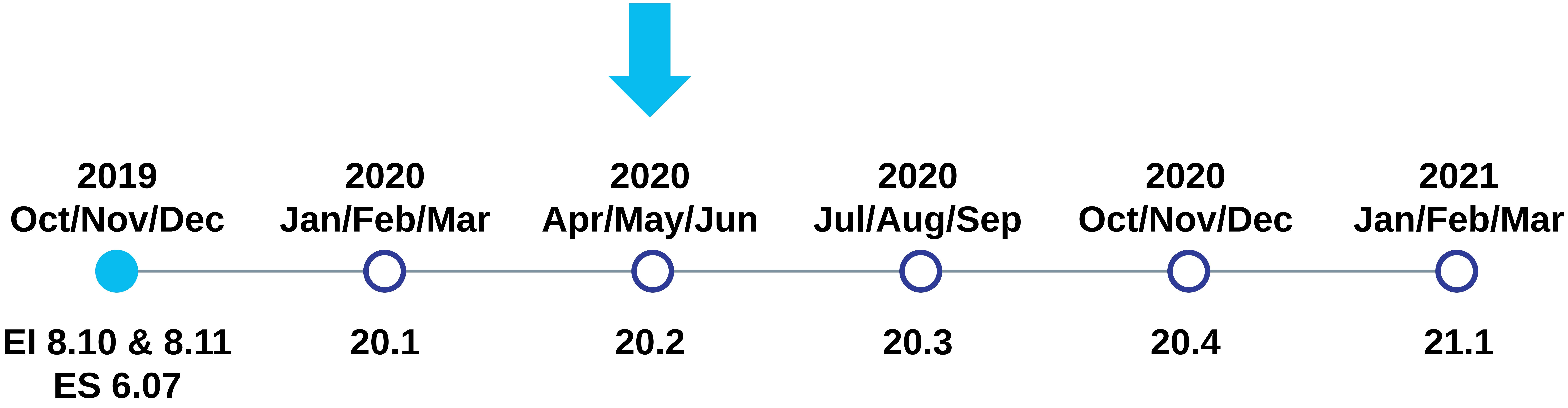
opentext™

What's New in EnCase Forensic 20.2

April, 2020 |

Product Release Timeline

SC 2020 awards
Winner



2019 Oct/Nov/Dec — EI 8.10 & 8.11 ES 6.07

2020 Jan/Feb/Mar — 20.1

2020 Apr/May/Jun — 20.2

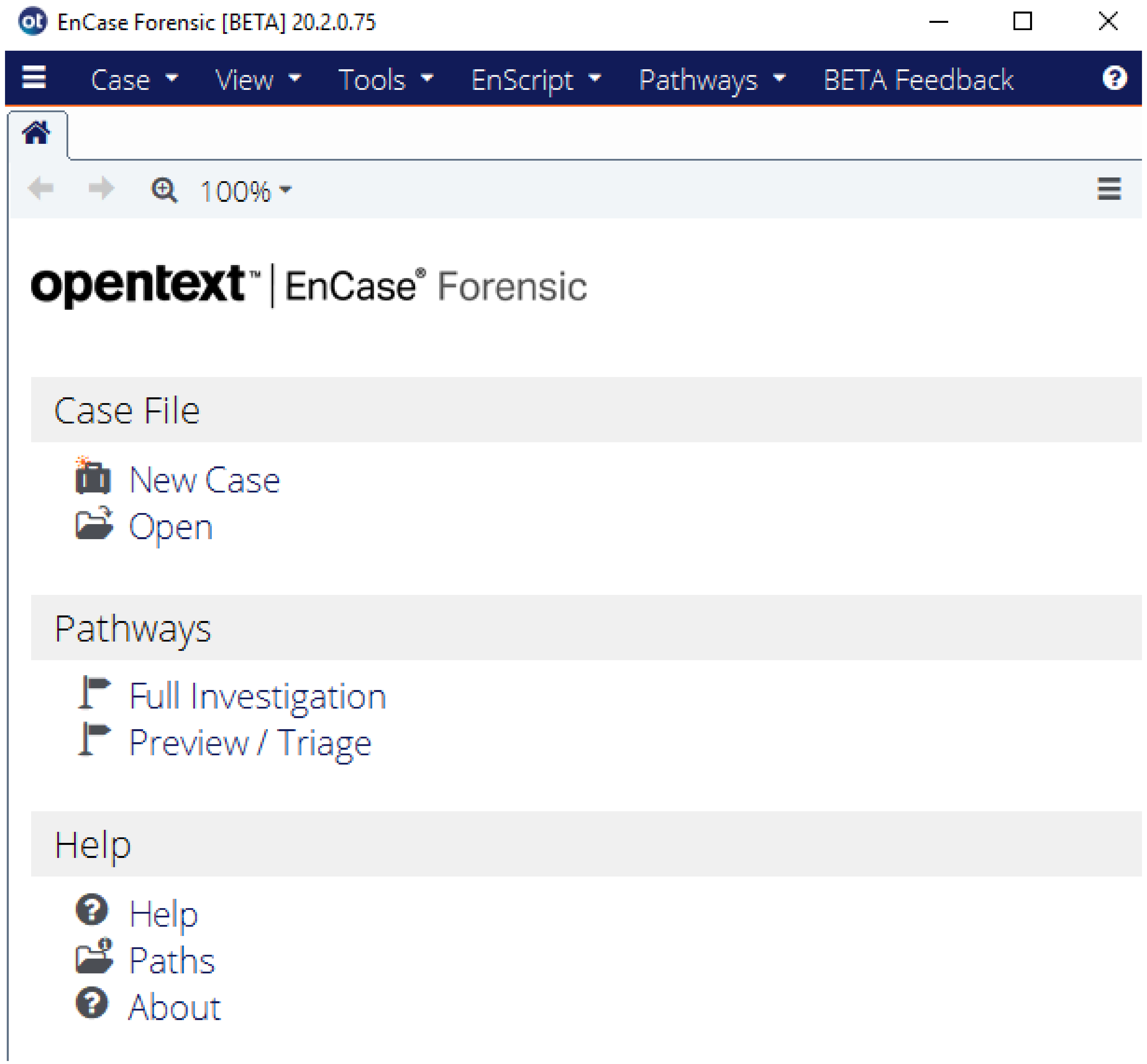
2020 Jul/Aug/Sep — 20.3

2020 Oct/Nov/Dec — 20.4

2021 Jan/Feb/Mar — 21.1

OpenText Rebranding and Versioning

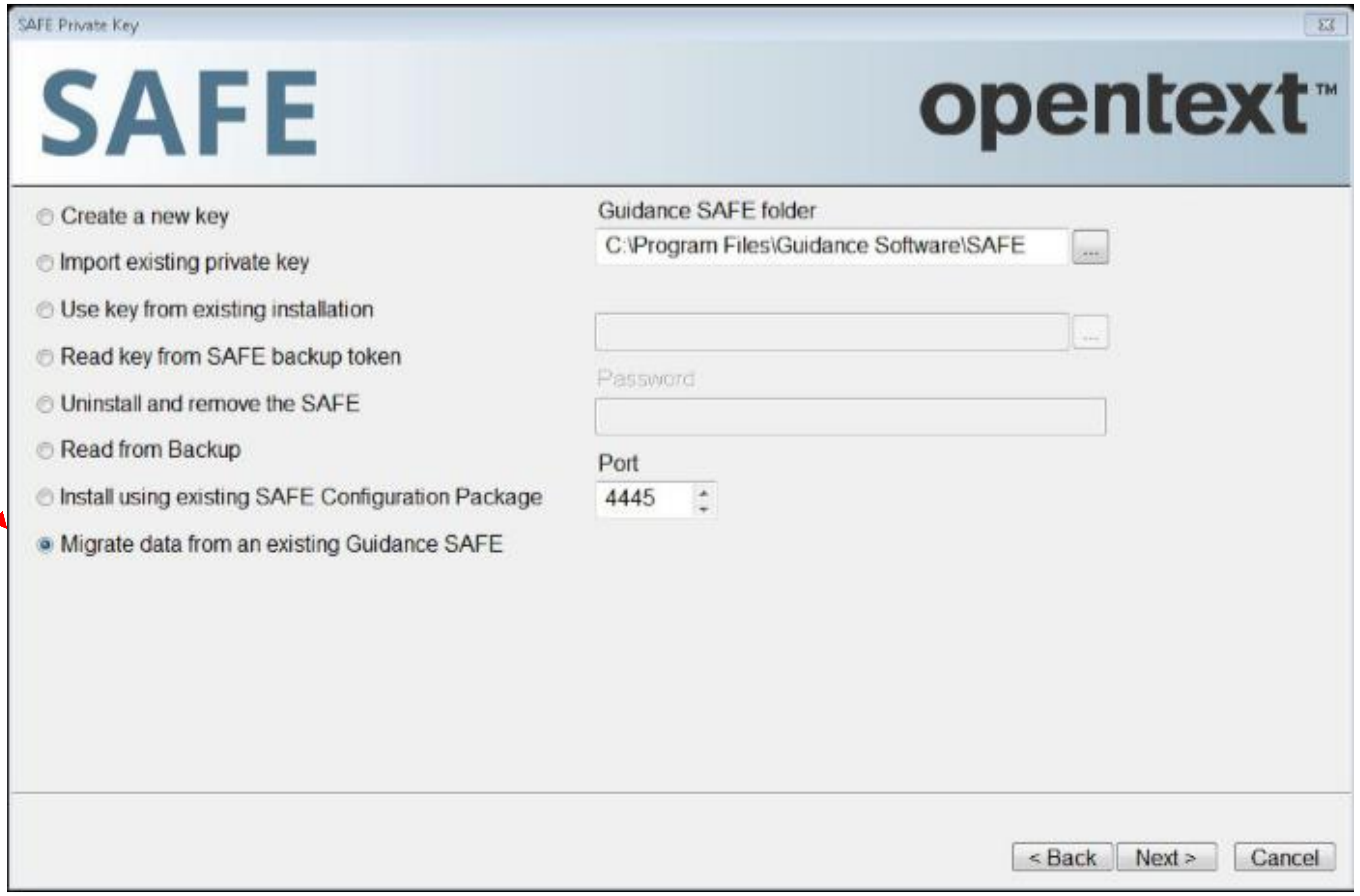
- From version 8.11 to 20.2
  - (Year) . (Quarter)
- Move to quarterly release schedule
- All references to Guidance Software have been removed from the application
- New application icon and colours



OpenText Rebranding and Versioning

- To migrate data to SAFE version 20.2 or later from SAFE versions a.01 through a.11

- The SAFE installer performs the following steps:
- Installs the OpenText SAFE in the folder specified in the first wizard dialog.
- Migrates the Guidance SAFE registry values into 'HKLM\SOFTWARE\OpenText\SAFE’.
- Migrates the Guidance SAFE configuration data into the OpenText SAFE install folder.
- Unregisters the Guidance SAFE service and register the OpenText SAFE service



SAFE Private Key

SAFE opentext™

○ Create a new key
○ Import existing private key
○ Use key from existing installation
○ Read key from SAFE backup token
○ Uninstall and remove the SAFE
○ Read from Backup
○ Install using existing SAFE Configuration Package
● Migrate data from an existing Guidance SAFE

Guidance SAFE folder: C:\Program Files\Guidance Software\SAFE

Password

Port: 4445

OpenText Rebranding and Versioning

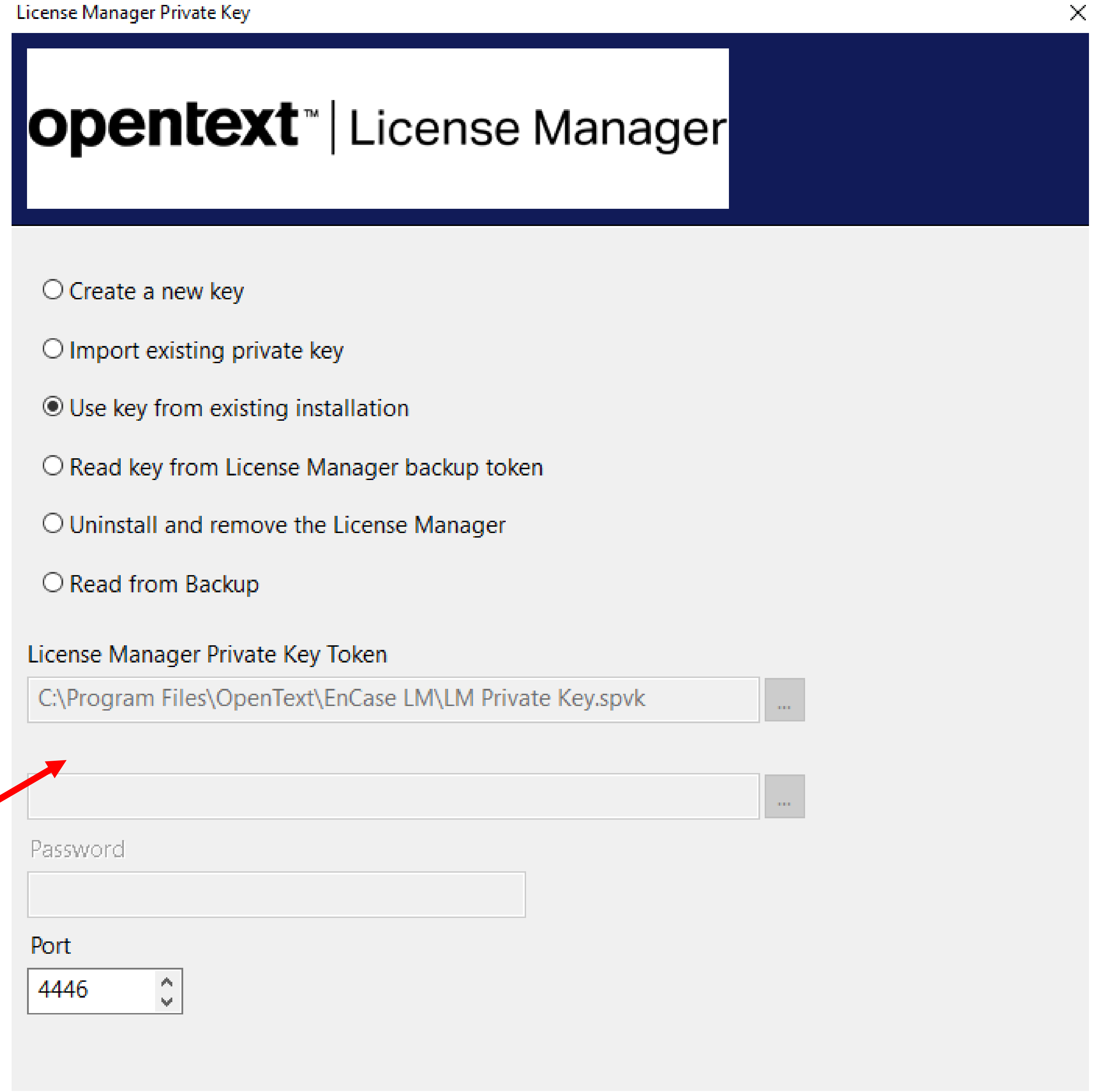
To migrate data to SAFE version 20.2 or later from SAFE versions a.01 through a.11

- We recommend running License Manager on the same machine as your existing SAFE/NAS

- Create a copy of the SAFE folder (c:\Program Files\OpenText\SAFE) (including all its contents) in the same parent folder. Name the copied folder EnCase LM.

- Point the License Manager installer to the EnCase LM folder.

- Using these options, the installer will create a .machine file. Since you have changed no settings, you can point at your existing .setup file to complete the License Manager installation.



License Manager Private Key

○ Create a new key

○ Import existing private key

● Use key from existing installation

○ Read key from License Manager backup token

○ Uninstall and remove the License Manager

○ Read from Backup

License Manager Private Key Token: C:\Program Files\OpenText\EnCase LM\LM Private Key.spvk

Password

Port: 4446

EnCase Forensic 20.2 Features

Forensic – 20.2 Release Themes

Cloud Readiness

1. Microsoft GRAPH API
2. Microsoft SharePoint
3. Microsoft OneDrive
4. Google Drive

Close the Loop

Core Functionality

1. Apple T2 Security Chip
2. Chrome browser for Mac and PC
3. McAfee Drive Encryption 7.1.3
4. Symantec Endpoint Encryption 11.3
5. WinMagic 8.6

Acquire Data

Customer Experience

1. 80% Faster Mac APFS Parsing
2. Keyword Index Searching
3. Persistent Blue Checks
4. SHA 2 Hashing

Do More

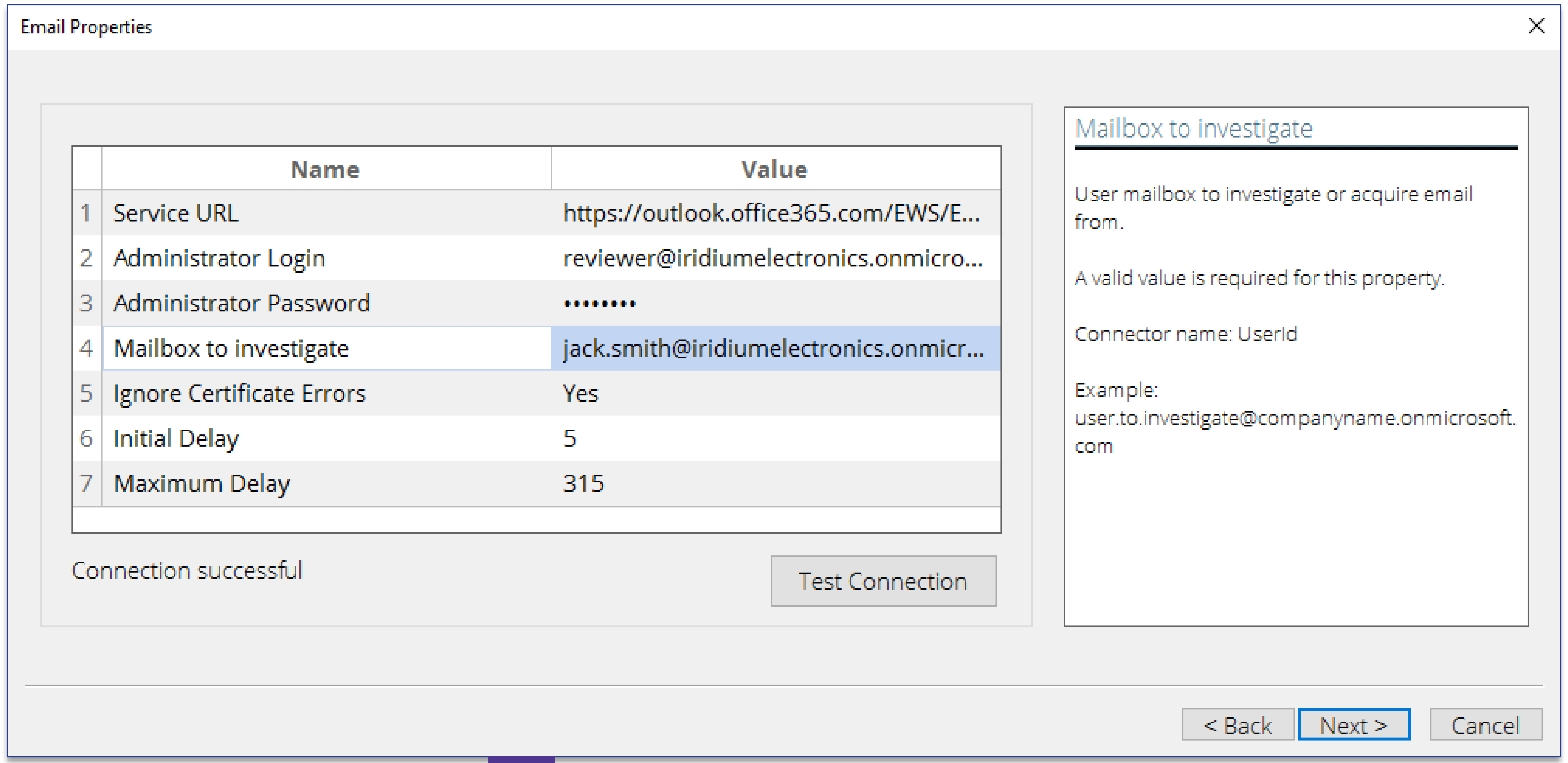
Cloud Connectors

Now Collect from Cloud Repositories

- Support for Microsoft GRAPH API
  - Microsoft Exchange 2013 and up
  - Microsoft O365
- Microsoft SharePoint
- Microsoft OneDrive
- Google Drive

Same Simple Workflow

1. Input Credentials



	Name	Value
1	Service URL	https://outlook.office365.com/EWS/E...
2	Administrator Login	reviewer@iridiumelectronics.onmicro...
3	Administrator Password	••••••••
4	Mailbox to investigate	jack.smith@iridiumelectronics.onmicr...
5	Ignore Certificate Errors	Yes
6	Initial Delay	5
7	Maximum Delay	315

Connection successful

Test Connection

Mailbox to investigate

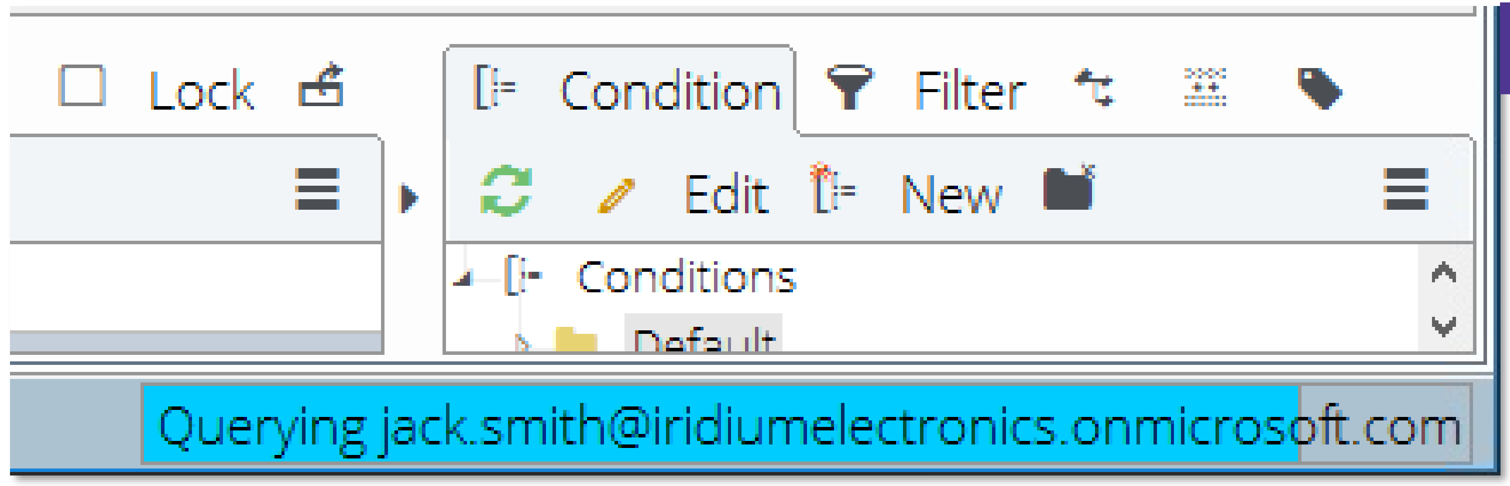
User mailbox to investigate or acquire email from.

A valid value is required for this property.

Connector name: UserId

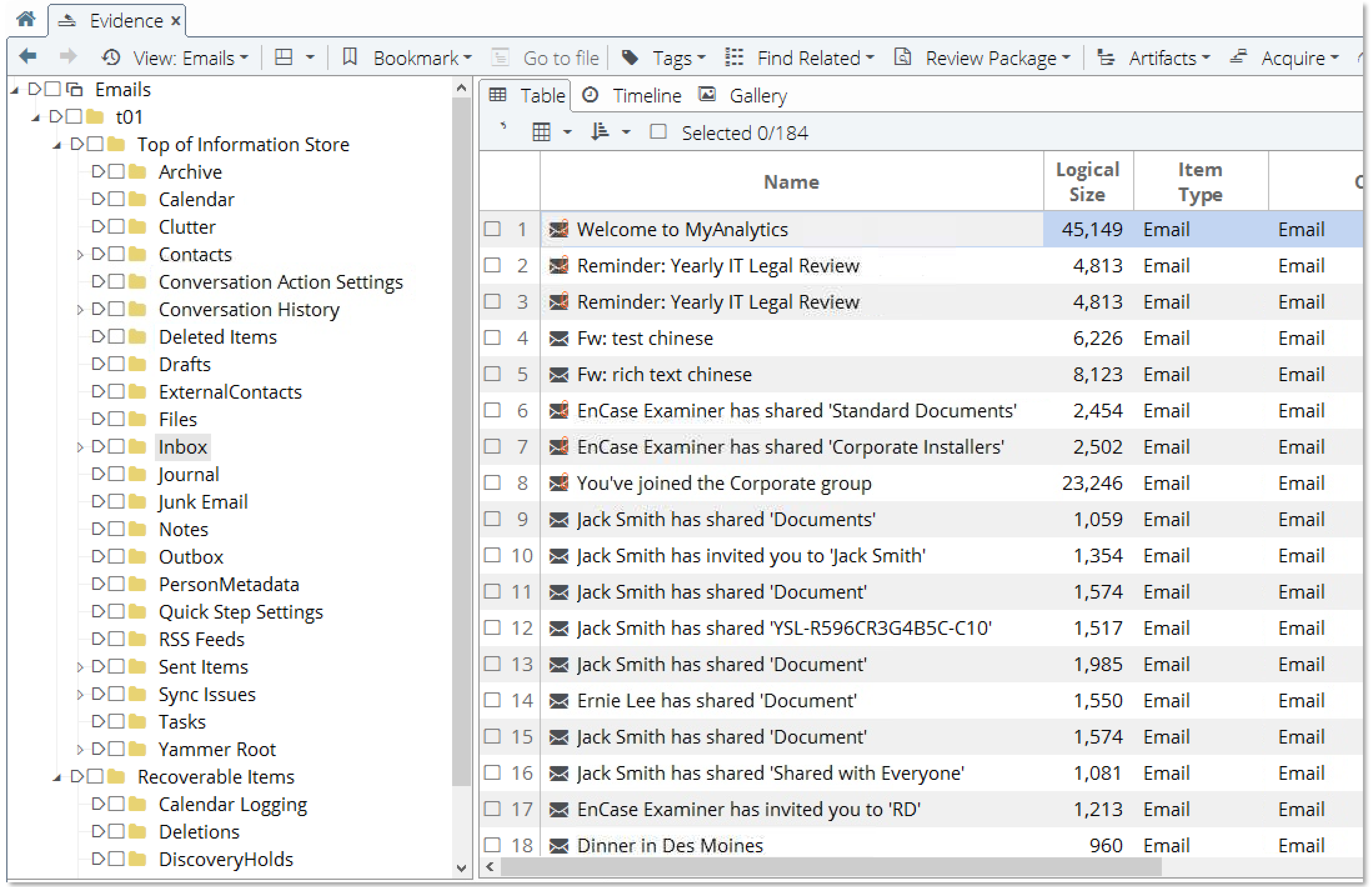
Example: user.to.investigate@companyname.onmicrosoft.com

2. Collect Data



Querying jack.smith@iridiumelectronics.onmicrosoft.com

3. Investigate and Bookmark



Selected 0/184

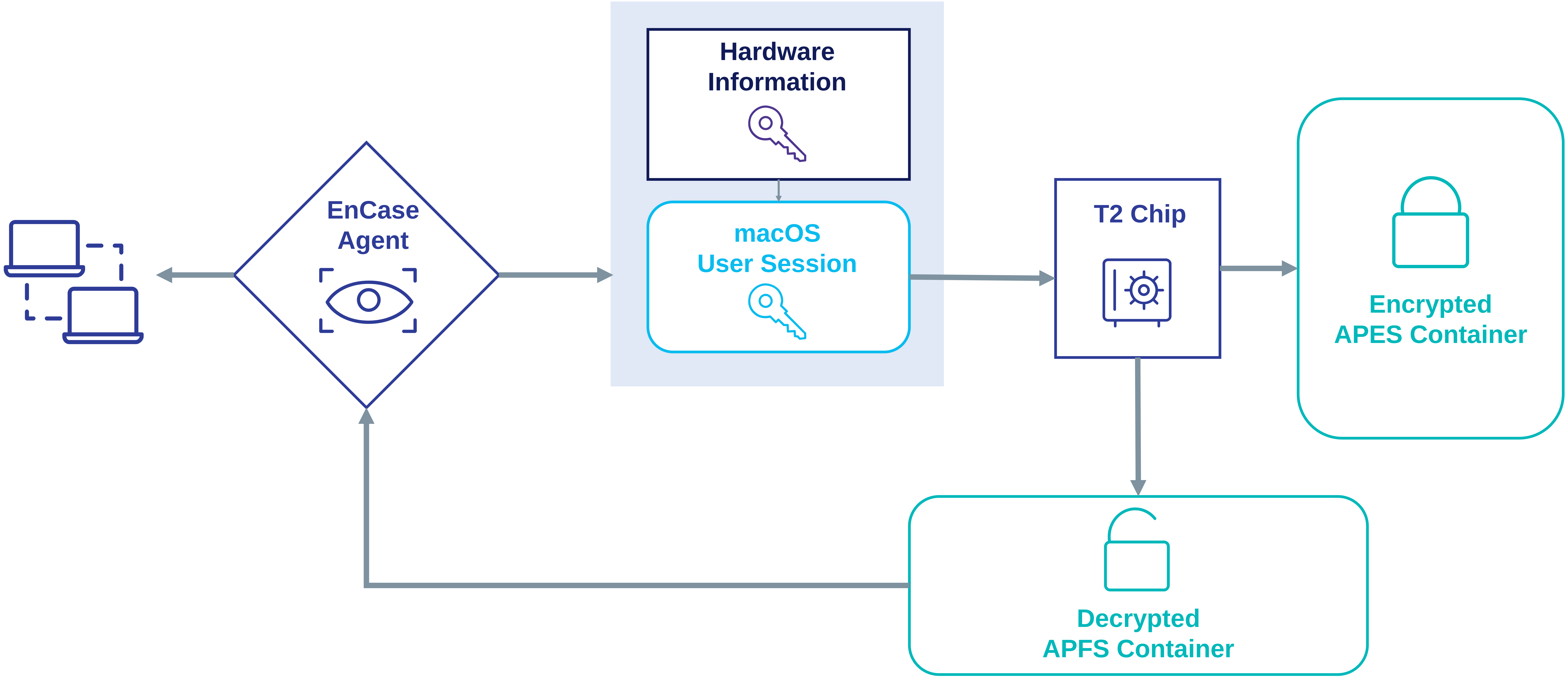
- Emails
  - t01
    - Top of Information Store
      - Archive
      - Calendar
      - Clutter
      - Contacts
      - Conversation Action Settings
      - Conversation History
      - Deleted Items
      - Drafts
      - ExternalContacts
      - Files
      - Inbox
      - Journal
      - Junk Email
      - Notes
      - Outbox
      - PersonMetadata
      - Quick Step Settings
      - RSS Feeds
      - Sent Items
      - Sync Issues
      - Tasks
      - Yammer Root
    - Recoverable Items
      - Calendar Logging
      - Deletions
      - DiscoveryHolds

		Name	Logical Size	Item Type	
☐	1	Welcome to MyAnalytics	45,149	Email	Email
☐	2	Reminder: Yearly IT Legal Review	4,813	Email	Email
☐	3	Reminder: Yearly IT Legal Review	4,813	Email	Email
☐	4	Fw: test chinese	6,226	Email	Email
☐	5	Fw: rich text chinese	8,123	Email	Email
☐	6	EnCase Examiner has shared 'Standard Documents'	2,454	Email	Email
☐	7	EnCase Examiner has shared 'Corporate Installers'	2,502	Email	Email
☐	8	You've joined the Corporate group	23,246	Email	Email
☐	9	Jack Smith has shared 'Documents'	1,059	Email	Email
☐	10	Jack Smith has invited you to 'Jack Smith'	1,354	Email	Email
☐	11	Jack Smith has shared 'Document'	1,574	Email	Email
☐	12	Jack Smith has shared 'YSL-R596CR3G4B5C-C10'	1,517	Email	Email
☐	13	Jack Smith has shared 'Document'	1,985	Email	Email
☐	14	Ernie Lee has shared 'Document'	1,550	Email	Email
☐	15	Jack Smith has shared 'Document'	1,574	Email	Email
☐	16	Jack Smith has shared 'Shared with Everyone'	1,081	Email	Email
☐	17	EnCase Examiner has invited you to 'RD'	1,213	Email	Email
☐	18	Dinner in Des Moines	960	Email	Email

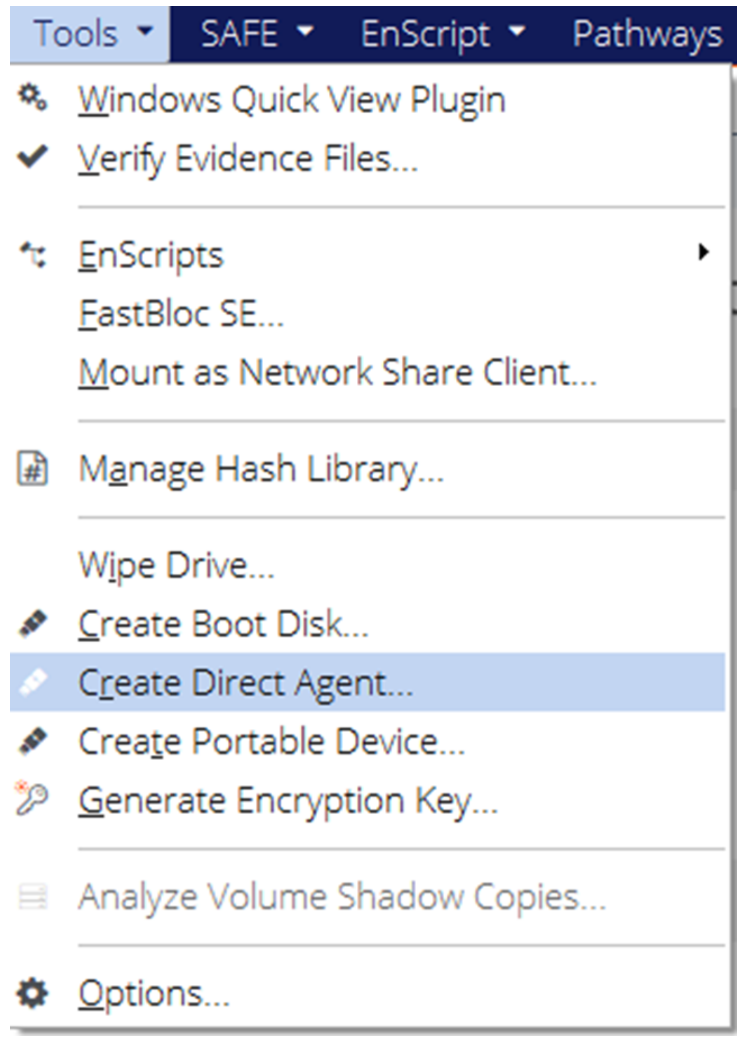
opentext™

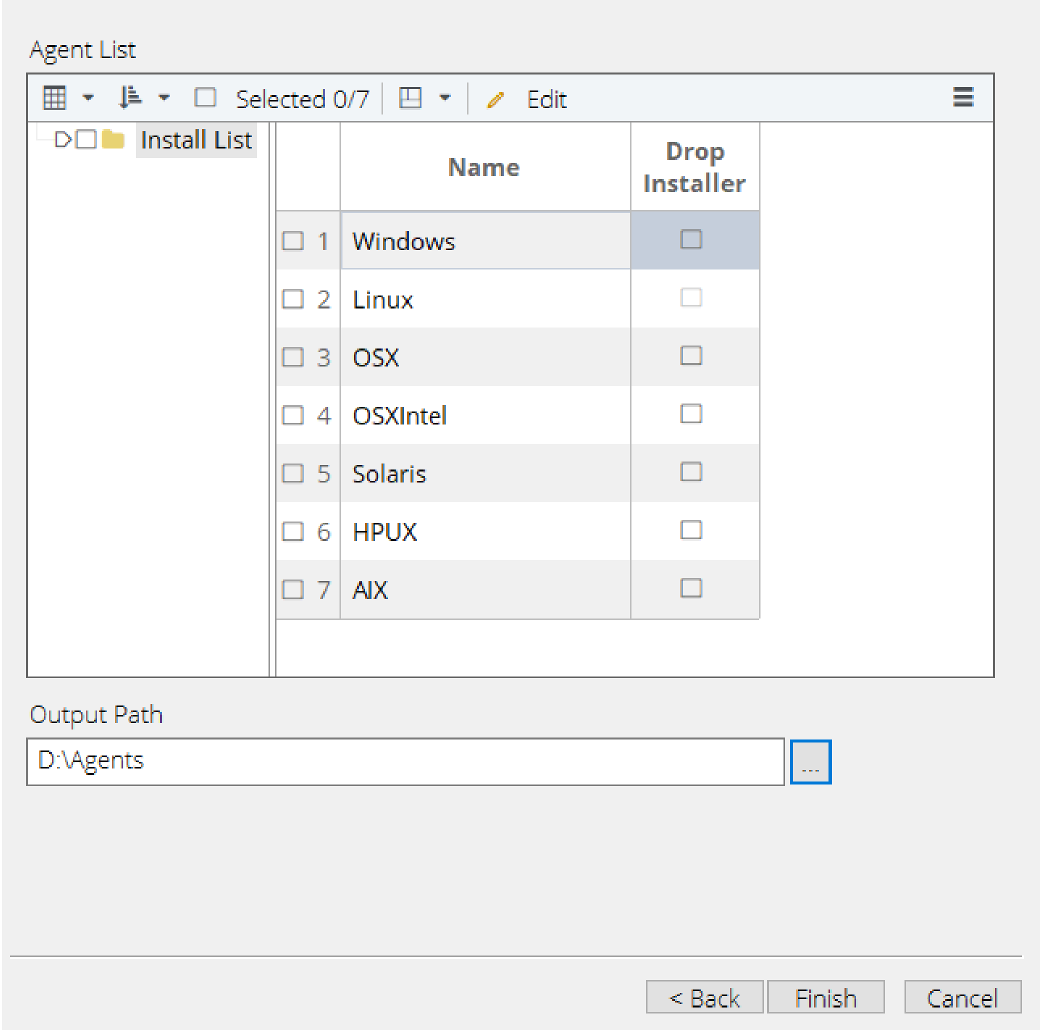
Core Forensic Capability

Apple T2 Security



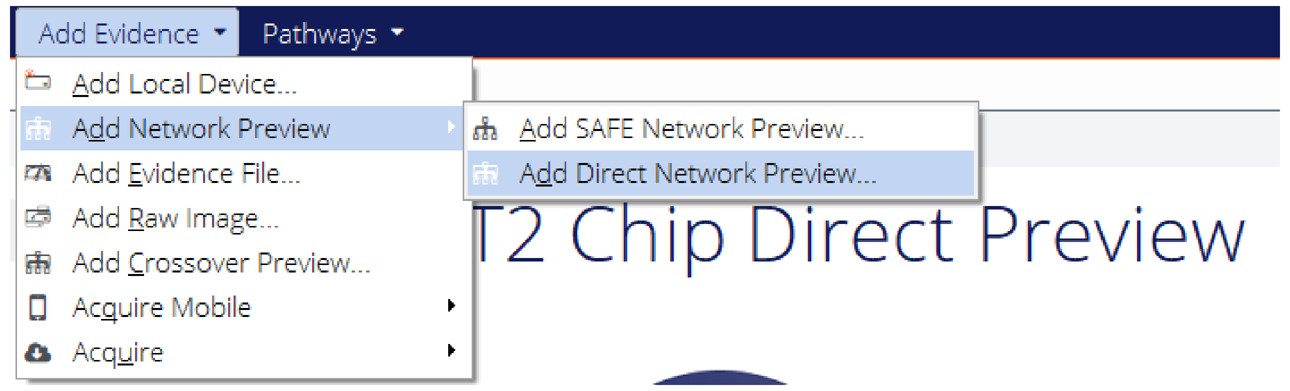
Collect from Macs enabled with Apple T2 Security

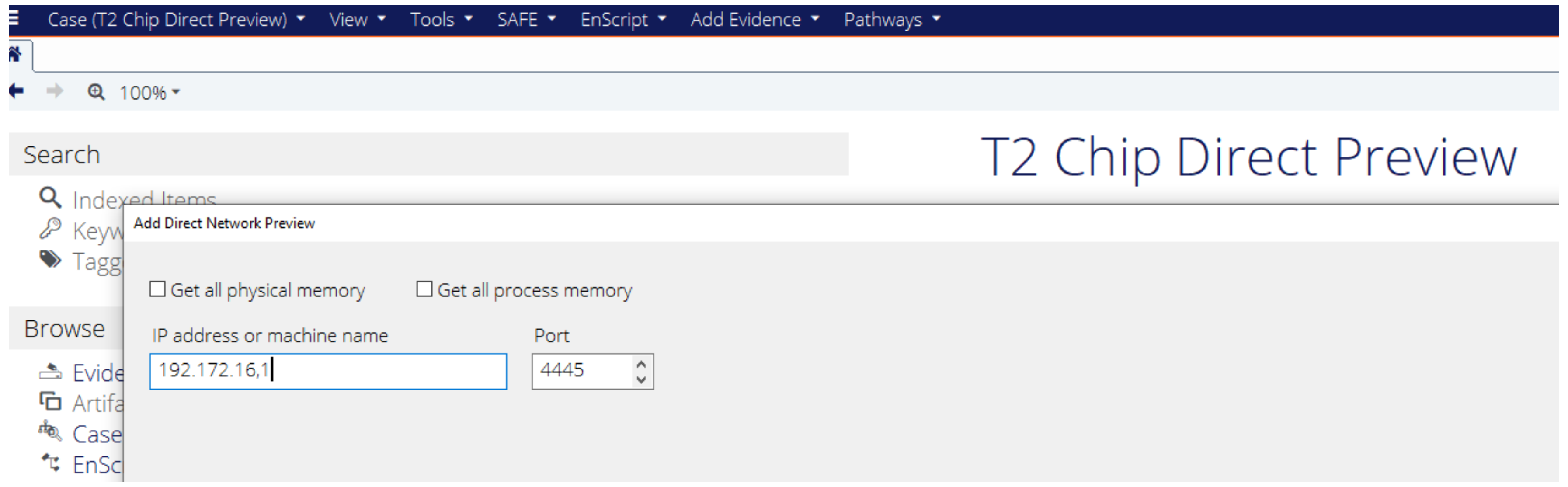




	Name	Drop Installer
□ 1	Windows	□
□ 2	Linux	□
□ 3	OSX	□
□ 4	OSXIntel	□
□ 5	Solaris	□
□ 6	HPUX	□
□ 7	AIX	□

Output Path: D:\Agents

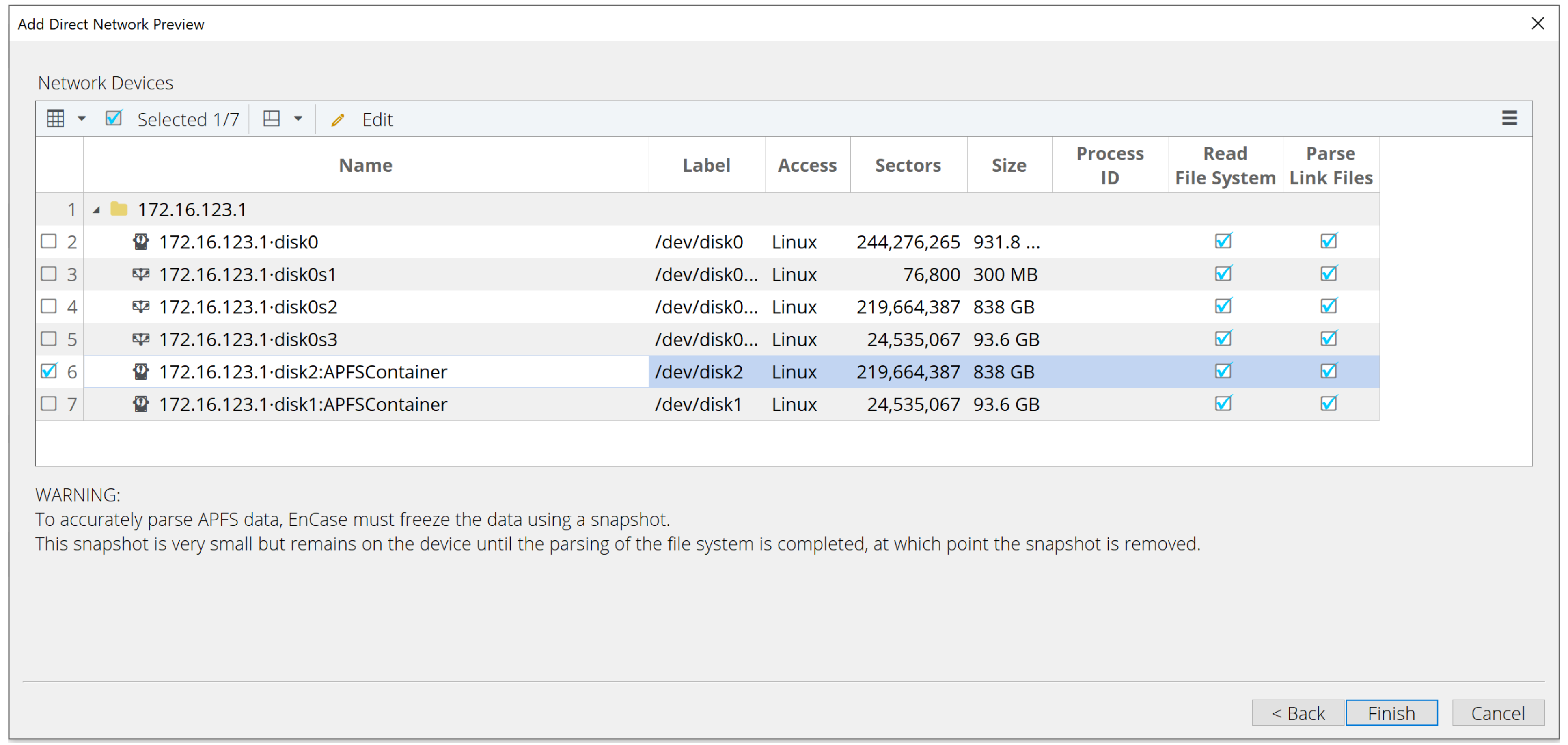




□ Get all physical memory □ Get all process memory

IP address or machine name: 192.172.16.1

Port: 4445



	Name	Label	Access	Sectors	Size	Process ID	Read File System	Parse Link Files
1	172.16.123.1							
□ 2	172.16.123.1·disk0	/dev/disk0	Linux	244,276,265	931.8 ...		☑	☑
□ 3	172.16.123.1·disk0s1	/dev/disk0...	Linux	76,800	300 MB		☑	☑
□ 4	172.16.123.1·disk0s2	/dev/disk0...	Linux	219,664,387	838 GB		☑	☑
□ 5	172.16.123.1·disk0s3	/dev/disk0...	Linux	24,535,067	93.6 GB		☑	☑
☑ 6	172.16.123.1·disk2:APFSContainer	/dev/disk2	Linux	219,664,387	838 GB		☑	☑
□ 7	172.16.123.1·disk1:APFSContainer	/dev/disk1	Linux	24,535,067	93.6 GB		☑	☑

WARNING:
To accurately parse APFS data, EnCase must freeze the data using a snapshot.
This snapshot is very small but remains on the device until the parsing of the file system is completed, at which point the snapshot is removed.

Direct Network Preview - allow for remote preview

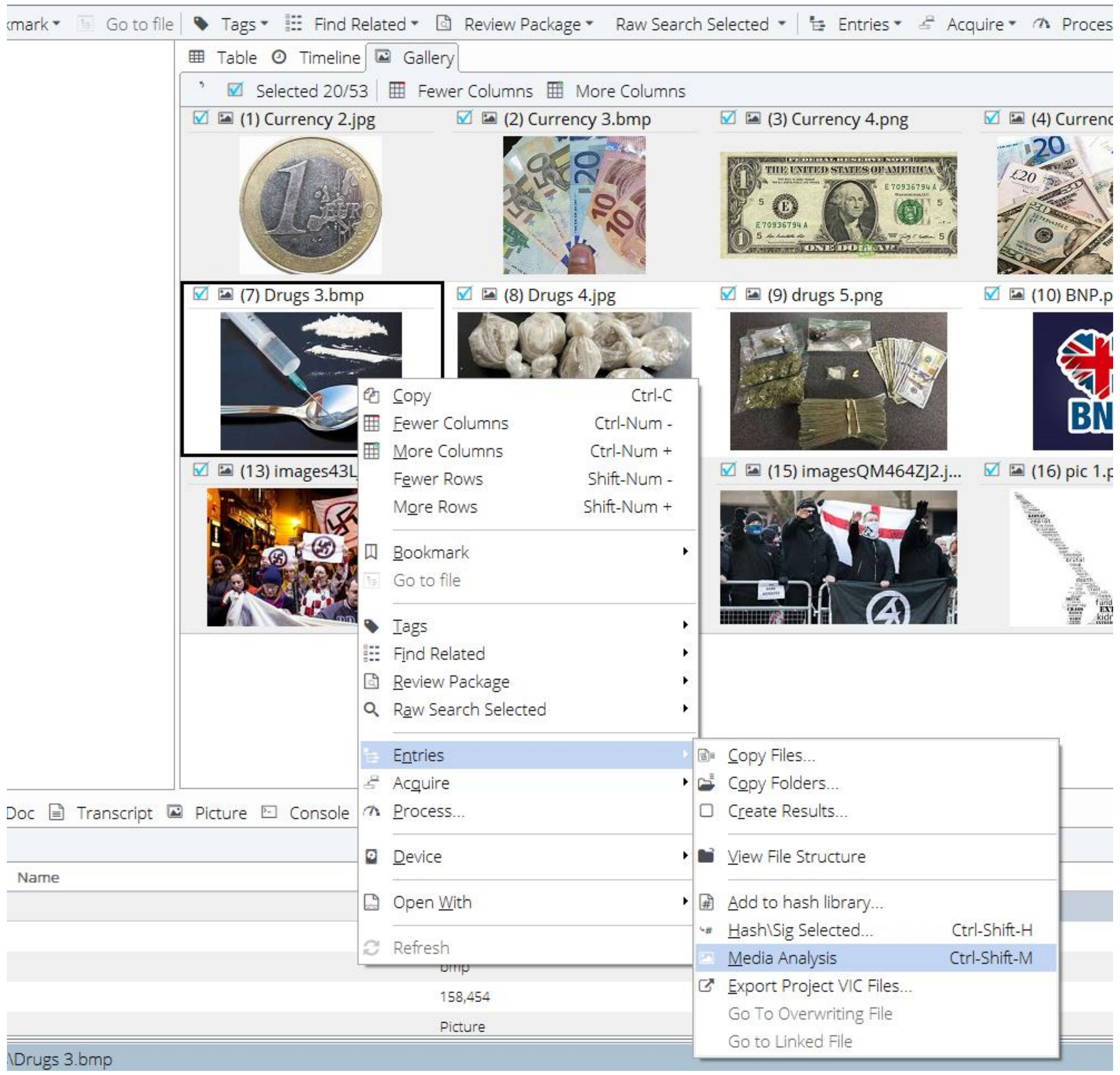
and acquisition using a remote agent called the Direct Agent.

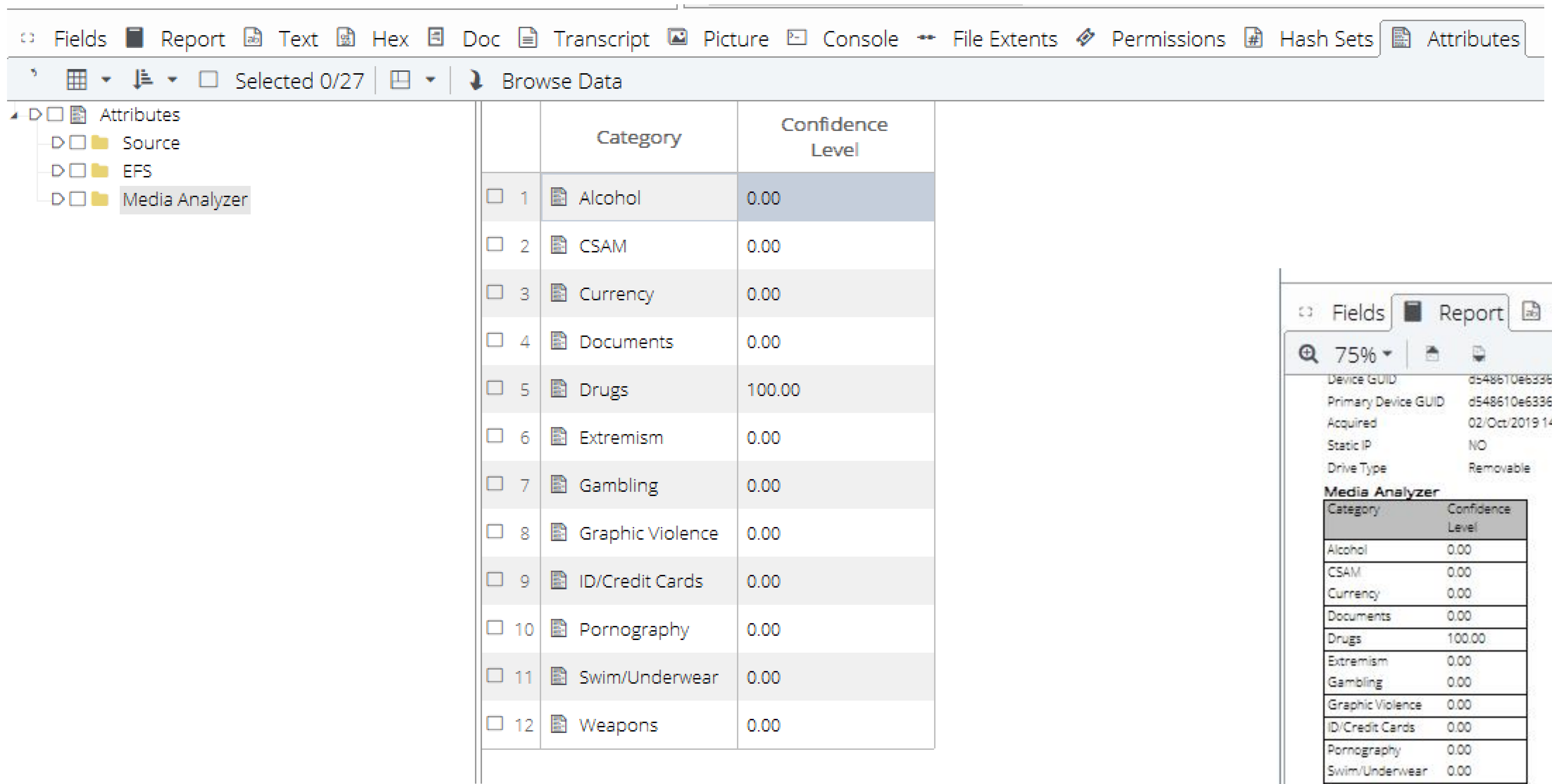
Internet Artifacts Update: Chrome Browser

- Chrome on Mac and PC
  - History
  - Cache
  - Downloads
  - Bookmarks
  - Keyword Search
  - Top Sites
  - New compression supported for parsing future artifacts

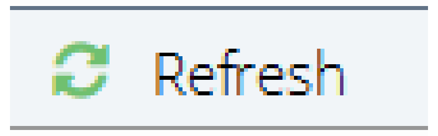
Other Features

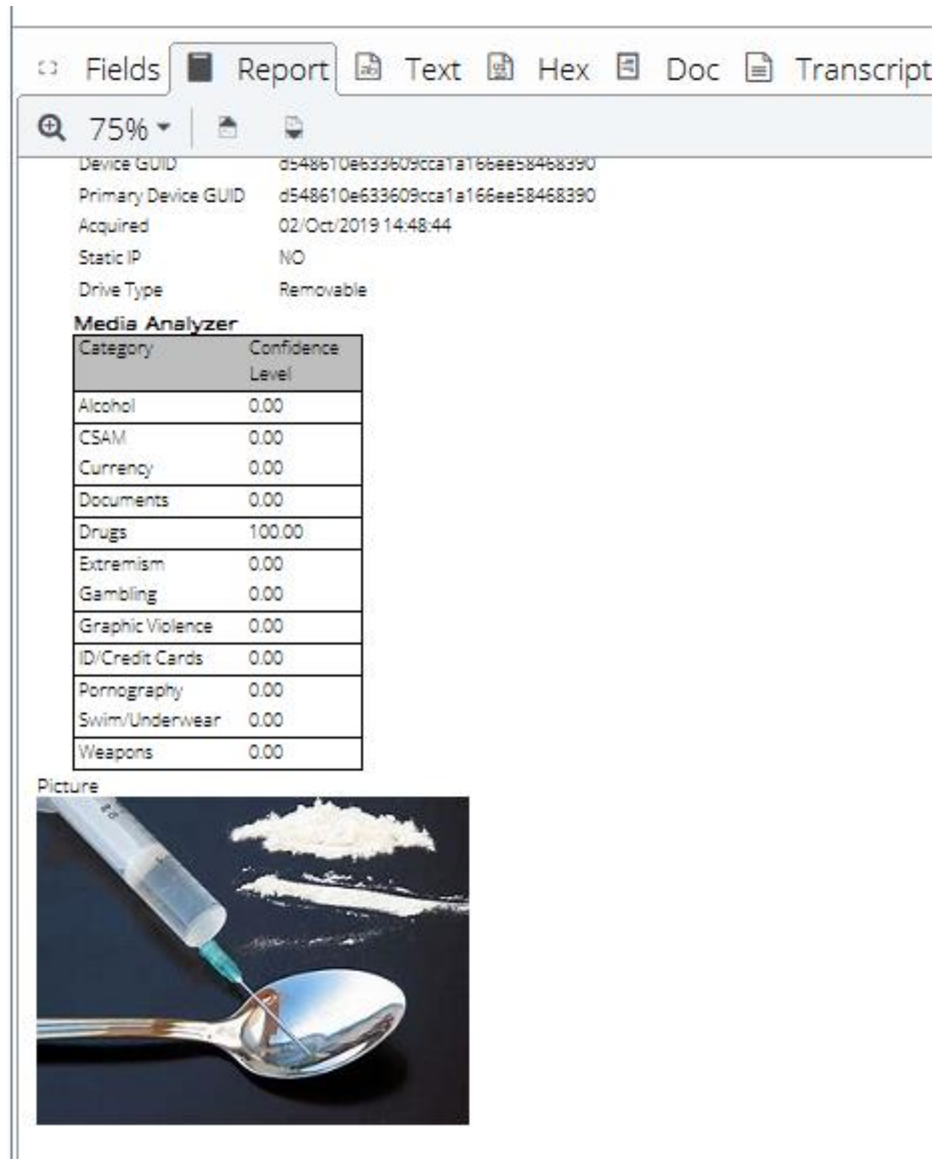
- **Process Media Analyzer attributes from Evidence view**
  You can now triage images quickly using Media Analyzer from the Evidence view





	Category	Confidence Level
1	Alcohol	0.00
2	CSAM	0.00
3	Currency	0.00
4	Documents	0.00
5	Drugs	100.00
6	Extremism	0.00
7	Gambling	0.00
8	Graphic Violence	0.00
9	ID/Credit Cards	0.00
10	Pornography	0.00
11	Swim/Underwear	0.00
12	Weapons	0.00





Device GUID d548610e633609cca1a166ee58468390
Primary Device GUID d548610e633609cca1a166ee58468390
Acquired 02/Oct/2019 14:48:44
Static IP NO
Drive Type Removable

Media Analyzer

Category	Confidence Level
Alcohol	0.00
CSAM	0.00
Currency	0.00
Documents	0.00
Drugs	100.00
Extremism	0.00
Gambling	0.00
Graphic Violence	0.00
ID/Credit Cards	0.00
Pornography	0.00
Swim/Underwear	0.00
Weapons	0.00

Picture

Customer Experience

Performance Enhancements

- Previewing an Apple machine with APFS used to take an upwards of 40 minutes.
- It now takes about 2-5 minutes
- APFS is inherently more complex
- Most competitors are just beginning to parse APFS, let alone optimizing the process

Mac / APFS Preview Speed

- Typing in search terms used to cause a delay in the interface
- Search terms now populate instantly (3-5x faster)

Index Search UI Improvement

Performance Enhancements

- SHA 256 & SHA512 generation support
- Acquisition, verification and item hashes
- Included within conditions, hash sets and reports

Enhanced Hash Algorithm Support

- Support for Android 10
- Support for iOS13 – logical acquisition speeds faster.

Index Search UI Improvement

opentext™

EnCase Forensic / Endpoint Investigator 20.3

EnCase® Endpoint Investigator/Forensic Roadmap

Mar 20, 2020

EnCase Forensic and Endpoint Investigator has been named the *Best Computer Forensic Solution* in the market by SC Magazine for ten consecutive years. No other company offers products with same level of functionality and flexibility, with a track record of court-acceptance as those released under the EnCase brand. Future releases focus on improving performance, stability, ease of use, and core forensic capabilities. All planned releases have been scoped for best effort delivery.

Delivered Recently

Performance and Stability

- Reduce the time it takes to perform key tasks by 50% or more

Forensic Artifacts

- Apple Time Machine backups from Mac APFS volumes
- Microsoft Outlook Data Files (.OST) from Office 365, Outlook 2016 and 2013

Improved Cloud Container Support

Powerful Media Analyzer add on

- Optional evidence processing module that reduces the time and stress examiners endure when manually searching for and viewing images (photos) in digital evidence

Target Operating System Support

- Apple Mac OS 10.15 Catalina
- Windows 10 1909
- Red Hat Enterprise Linux (RHEL) 8.0

Q2CY2020 [20.2]
In progress

Performance and Stability

- 80% Faster Apple Mac APFS parsing
- Instant keyword index query

Forensic Artifacts

- Latest version of Chrome browser for Windows and Mac OS

New Source Connectors

- Microsoft GRAPH API
- Microsoft SharePoint
- Microsoft OneDrive
- Google Drive

Enterprise Drive Encryption

- McAfee Drive Encryption 7.1
- Symantec Endpoint Encryption 11.3
- WinMagic 8.6

Improved Investigation Workflows

- Integration with Endpoint Security

Target Operating System Support

- Apple Mac computers with T2 Security chip

H2CY2020 [20.3]
planned

Performance and Stability

- Newly optimized case-cache architecture
- Instant Gallery View
- OST/Email stability and scalability

Forensic Artifacts

- Internet Artifacts: Safari
- RAR 5.0 support
- Prefetch Dump
- EXIF viewer

Agent Management Platform

- Visibility of enterprise endpoints

Job Scheduling

- Schedule jobs for collection

Target Operating System Support

- RHEL 8.1
- Apple Mac OS 10.16
- Qualcomm chip support
- Windows Server 20H1
- Windows 10 20H1

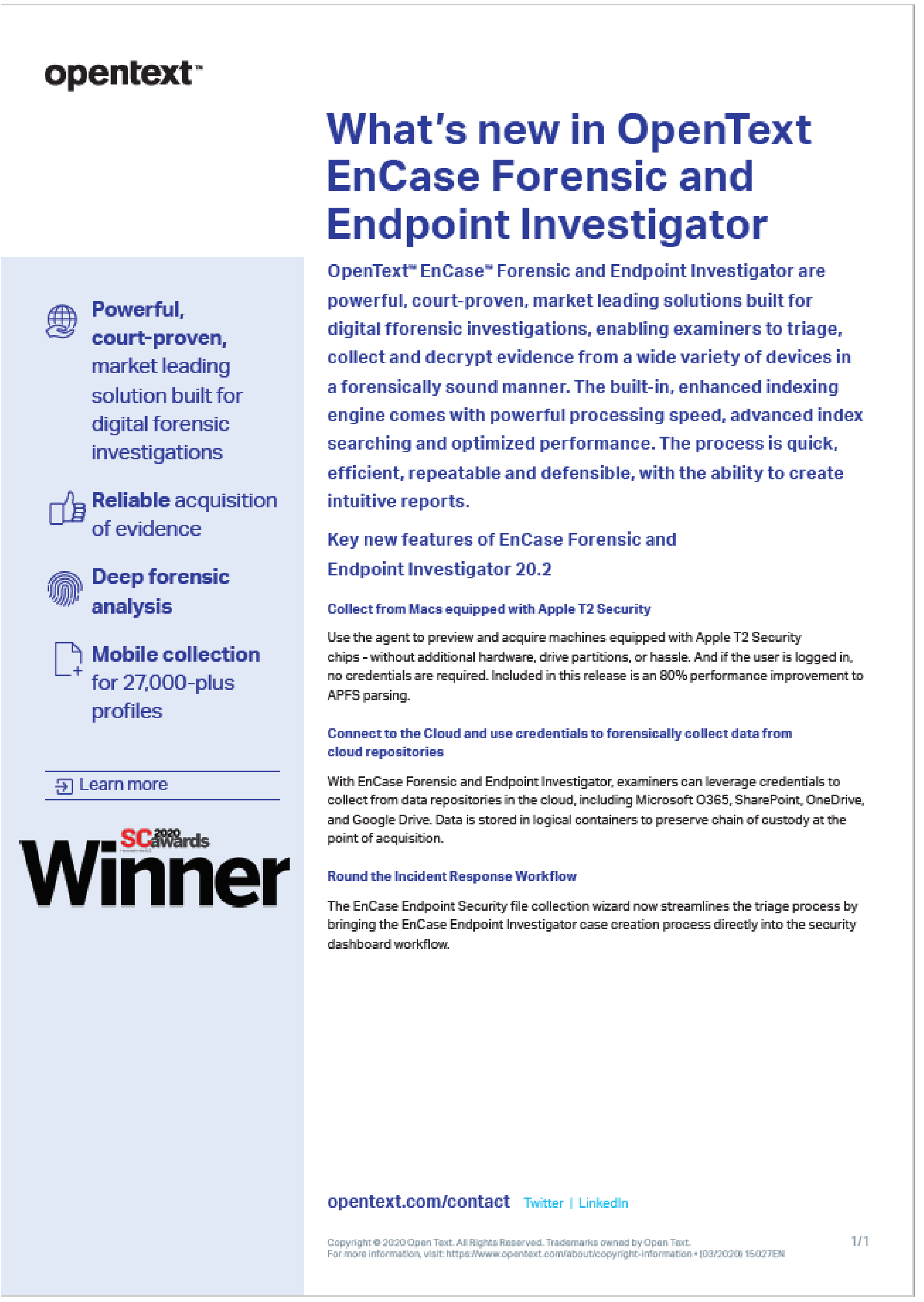
Where to find more information

Product webpage

https://www.opentext.com/products-and-solutions/products/security

EnCase v20.2 blog

https://blogs.opentext.com/whats-new-in-opentext-encase-forensic-and-endpoint-investigator-cloud-edition-ce-20-2/



opentext™

What's new in OpenText EnCase Forensic and Endpoint Investigator

Powerful, court-proven, market leading solution built for digital forensic investigations

Reliable acquisition of evidence

Deep forensic analysis

Mobile collection for 27,000-plus profiles

Learn more

SC 2020 awards Winner

OpenText™ EnCase™ Forensic and Endpoint Investigator are powerful, court-proven, market leading solutions built for digital fforensic investigations, enabling examiners to triage, collect and decrypt evidence from a wide variety of devices in a forensically sound manner. The built-in, enhanced indexing engine comes with powerful processing speed, advanced index searching and optimized performance. The process is quick, efficient, repeatable and defensible, with the ability to create intuitive reports.

Key new features of EnCase Forensic and Endpoint Investigator 20.2

Collect from Macs equipped with Apple T2 Security

Use the agent to preview and acquire machines equipped with Apple T2 Security chips - without additional hardware, drive partitions, or hassle. And if the user is logged in, no credentials are required. Included in this release is an 80% performance improvement to APFS parsing.

Connect to the Cloud and use credentials to forensically collect data from cloud repositories

With EnCase Forensic and Endpoint Investigator, examiners can leverage credentials to collect from data repositories in the cloud, including Microsoft O365, SharePoint, OneDrive, and Google Drive. Data is stored in logical containers to preserve chain of custody at the point of acquisition.

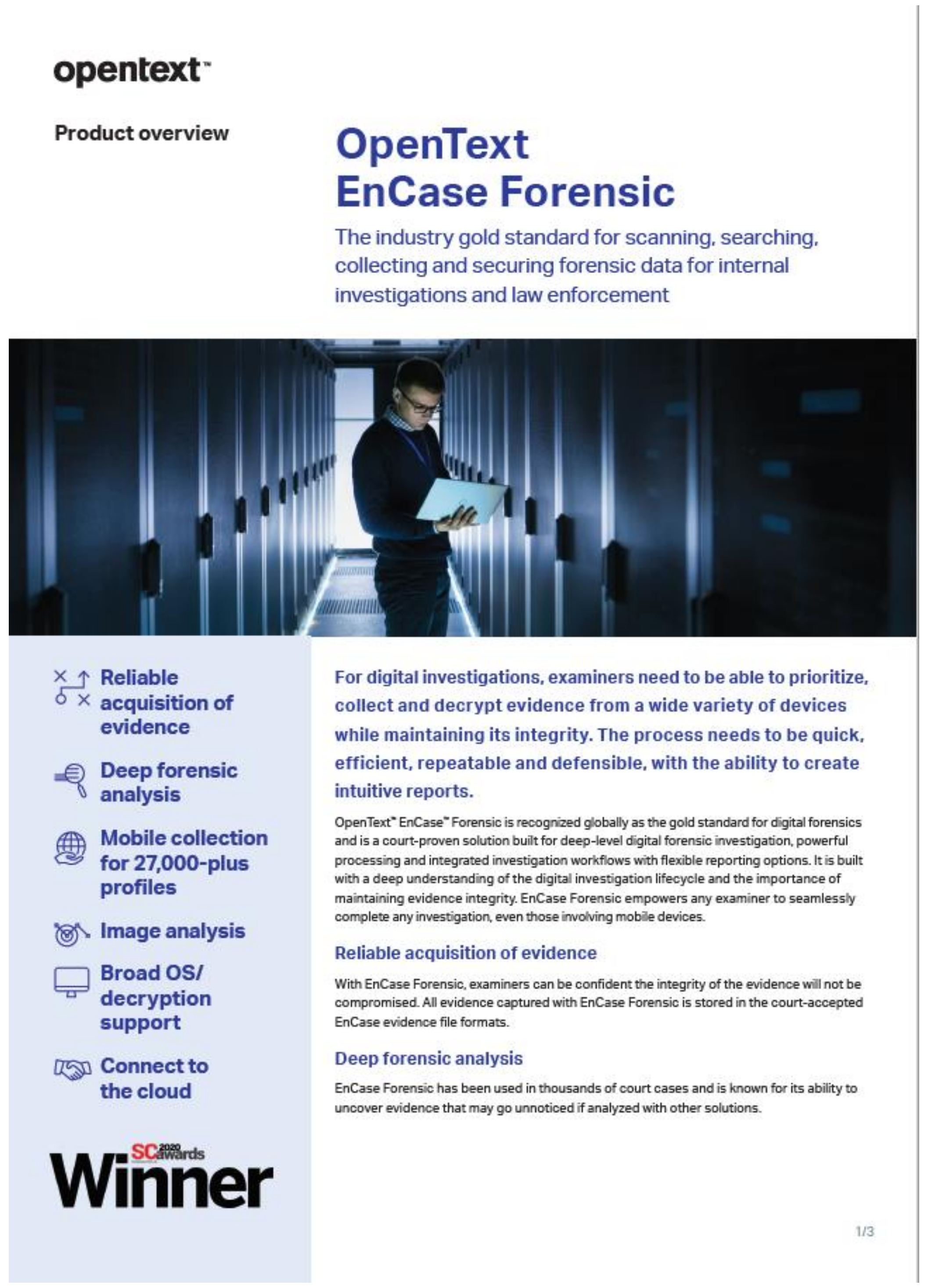
Round the Incident Response Workflow

The EnCase Endpoint Security file collection wizard now streamlines the triage process by bringing the EnCase Endpoint Investigator case creation process directly into the security dashboard workflow.

opentext.com/contact Twitter | LinkedIn

Copyright © 2020 Open Text. All Rights Reserved. Trademarks owned by Open Text.
For more information, visit: https://www.opentext.com/about/copyright-information • (03/2020) 15027EN

1/1



opentext™

Product overview

OpenText EnCase Forensic

The industry gold standard for scanning, searching, collecting and securing forensic data for internal investigations and law enforcement

Reliable acquisition of evidence

Deep forensic analysis

Mobile collection for 27,000-plus profiles

Image analysis

Broad OS/ decryption support

Connect to the cloud

SC 2020 awards Winner

For digital investigations, examiners need to be able to prioritize, collect and decrypt evidence from a wide variety of devices while maintaining its integrity. The process needs to be quick, efficient, repeatable and defensible, with the ability to create intuitive reports.

OpenText™ EnCase™ Forensic is recognized globally as the gold standard for digital forensics and is a court-proven solution built for deep-level digital forensic investigation, powerful processing and integrated investigation workflows with flexible reporting options. It is built with a deep understanding of the digital investigation lifecycle and the importance of maintaining evidence integrity. EnCase Forensic empowers any examiner to seamlessly complete any investigation, even those involving mobile devices.

Reliable acquisition of evidence

With EnCase Forensic, examiners can be confident the integrity of the evidence will not be compromised. All evidence captured with EnCase Forensic is stored in the court-accepted EnCase evidence file formats.

Deep forensic analysis

EnCase Forensic has been used in thousands of court cases and is known for its ability to uncover evidence that may go unnoticed if analyzed with other solutions.

1/3

EnCase Forensic Evaluation

30 Day evaluation licence of EnCase v20.2 and Media Analyzer Module

Please contact DataExpert for further information

opentext™

Tableau Forensic Hardware

Most Comprehensive Forensic Hardware Product Line

Forensic Bridges

Reliable, hardware-based write-blocked access to digital media in portable and integrated form factors.

Forensic Imagers

Standalone, high-performant forensic imaging and triage of physical media and network shares.

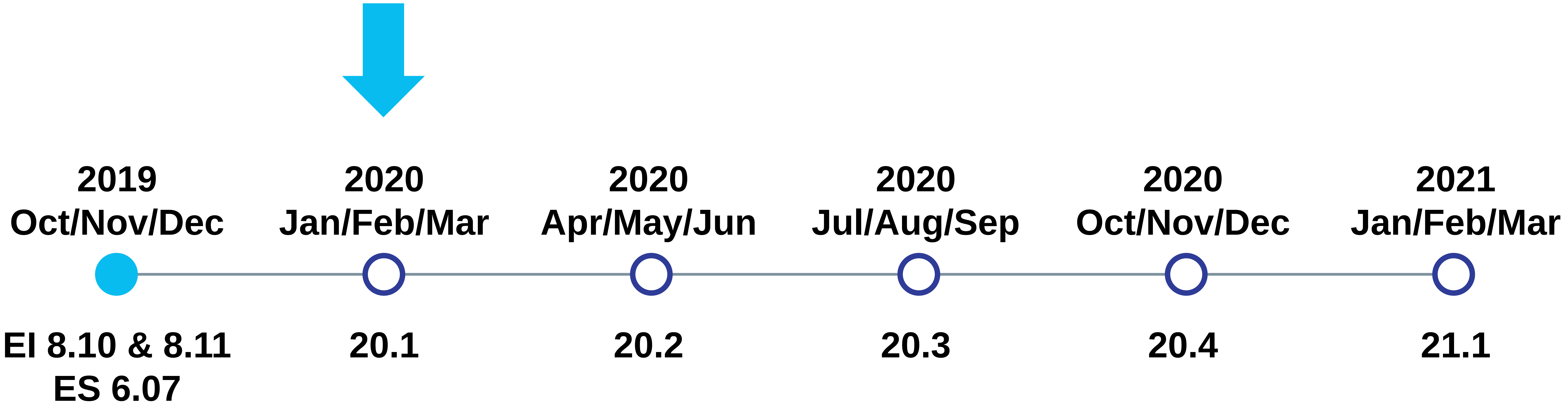
Accessories

Custom-designed adapters and cables enable acquisition of numerous media types.

Software Utilities

Extends the hardware value through complementary software applications.

Product Release Timeline



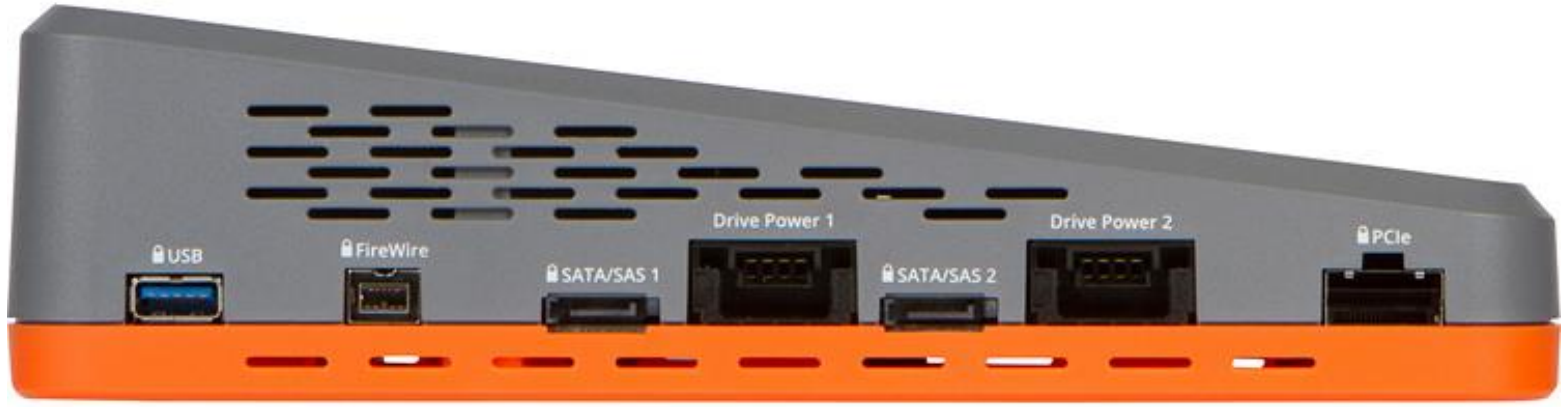
2019 Oct/Nov/Dec	2020 Jan/Feb/Mar	2020 Apr/May/Jun	2020 Jul/Aug/Sep	2020 Oct/Nov/Dec	2021 Jan/Feb/Mar
EI 8.10 & 8.11 ES 6.07	20.1	20.2	20.3	20.4	21.1

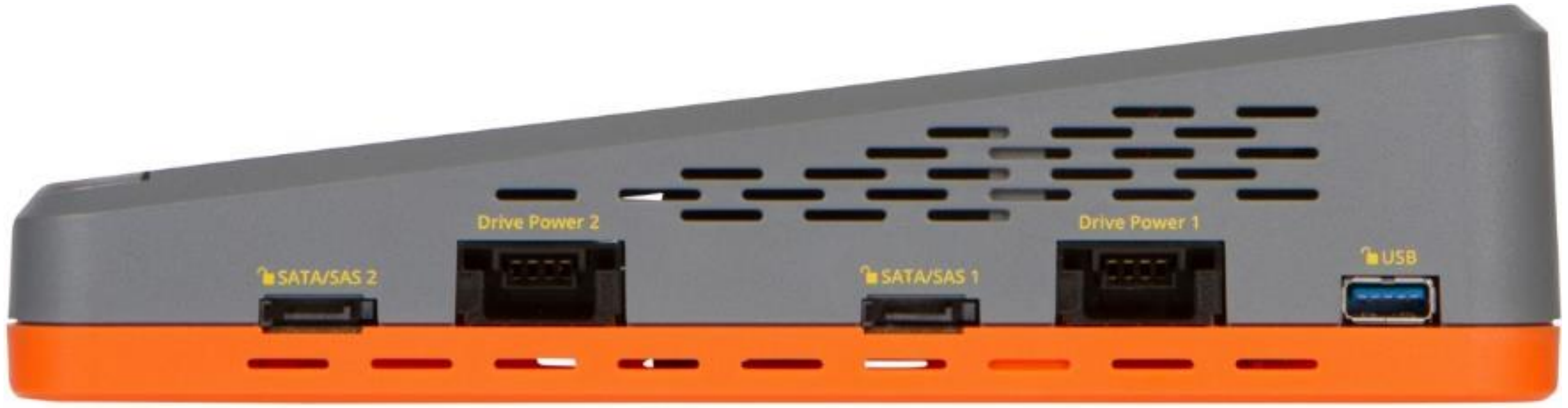
Tableau Forensic Imager (TX1) 20.1

- Built with one purpose: for Digital Forensics
- Design and layout of all circuit boards built from scratch
- Built on a custom Linux kernel,
  making it lean, powerful & easy to use!
- UI localization in eight languages (English, German, Spanish, French, Portuguese, Russian, Turkish and Chinese (simplified))

TX1: Intuitive hardware design

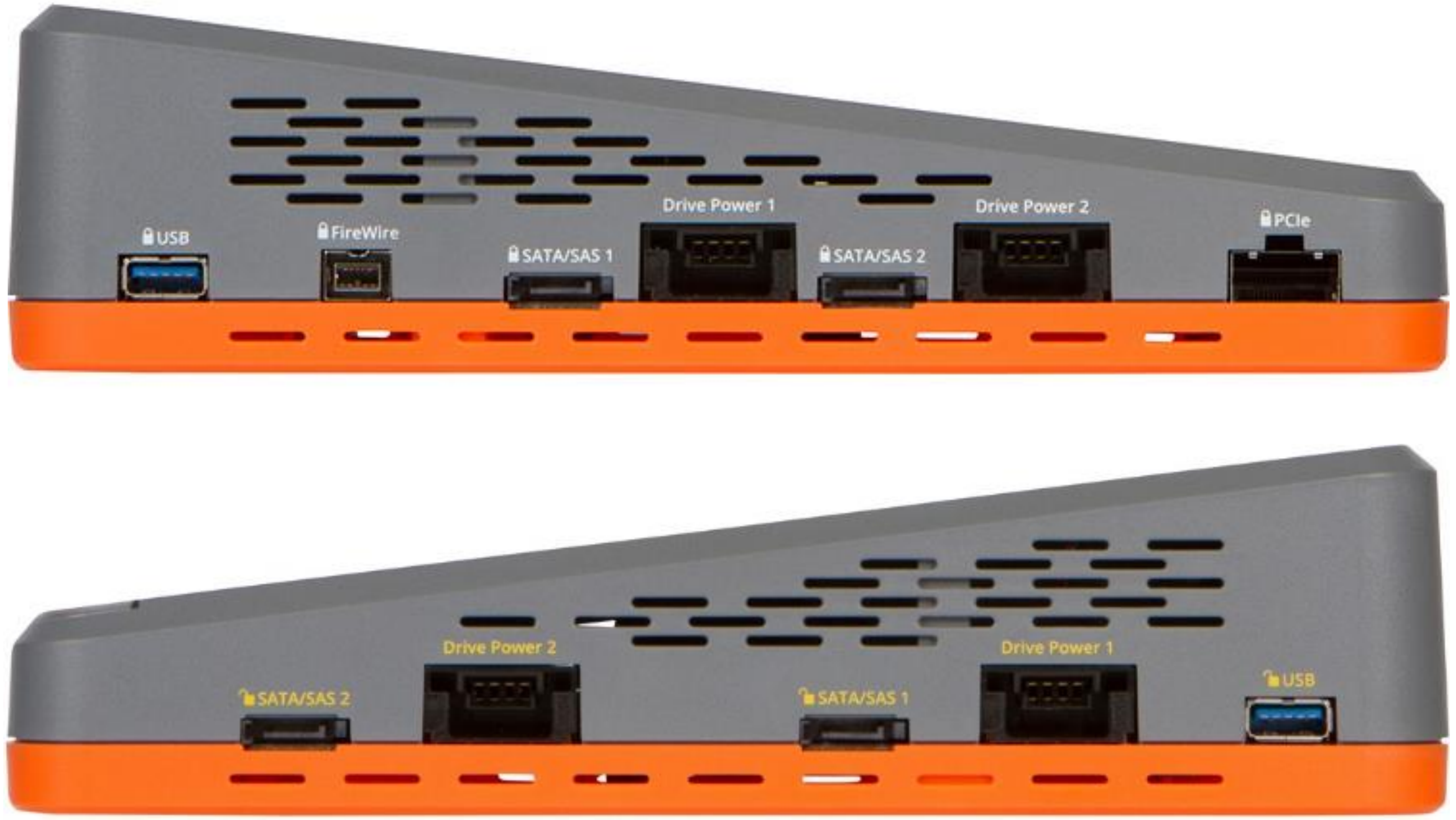
- Sources on the left (input)
  - Port labels colored white with lock icon to indicate read-only
- Destinations on the right (output)
  - Port labels colored yellow with unlock icon to indicate read-write
- Ethernet in the back (input/output)
  - Port label colored yellow to indicate read-write
- Accessories in the front
  - Port labels colored yellow to indicate read-write





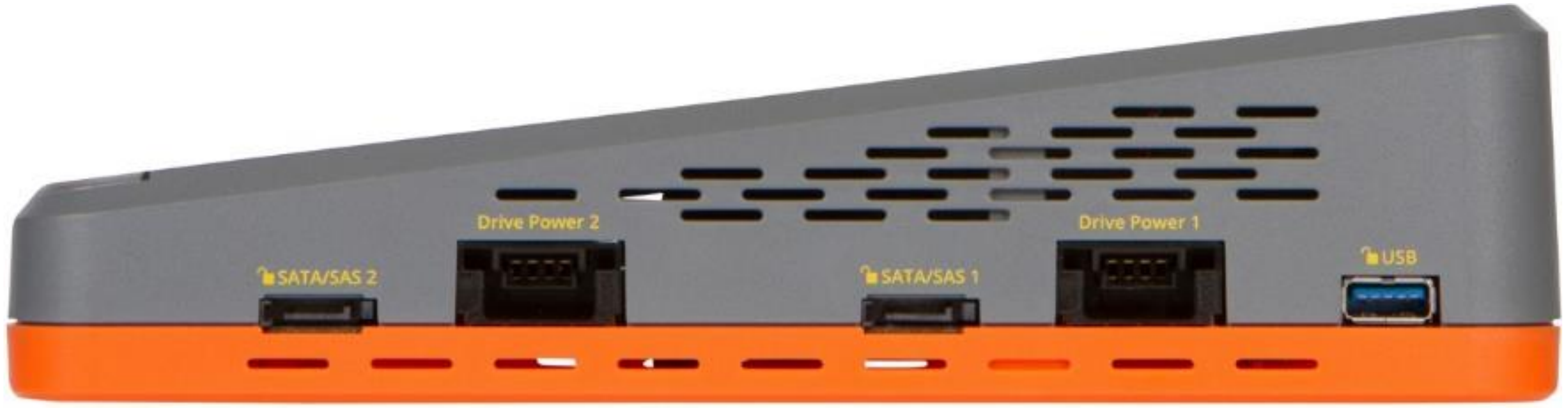
TX1: Broad media support

- 10GbE (10 Gigabit Ethernet)
- Acquire PCIe, USB 3, SATA, SAS, FireWire 800, IDE, and network shares
- Output to USB 3, SATA, SAS, and network shares
- Extensive file system support (source and destination)
  - ExFAT, NTFS, EXT4, FAT32, HFS+
- Use Accessory ports for USB keyboard, downloading logs



TX1: Flexible output options

- Connect output SATA/SAS drives with cables or use included TX1-S1 imaging bay, which offers cable-less connection and drive cooling
- Output to mix of local and network shares
- Output to up to four destinations per source
- Output using image, clone, or both



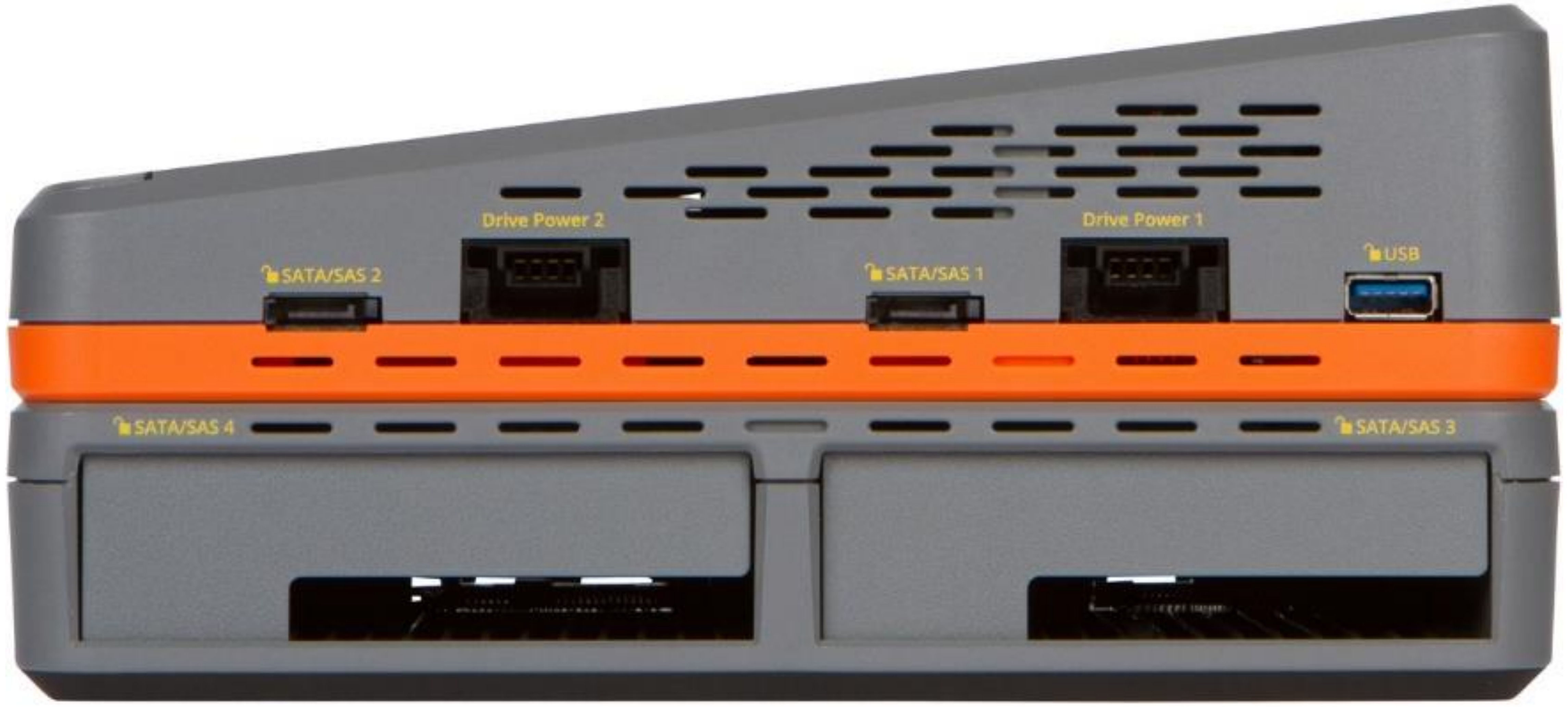


Tableau 20.1 Enhancements – Themes

Improved Efficiency

1. Remote access (remote web interface)
2. Pause and resume
3. Export and import logical image searches

Productivity

Thorough Media Detail

1. View images and plain text files
2. Display file size in Browse screens
3. Disk > Partition > File System display
4. Enhanced media characterization (presence of encryption and/or RAID)

More Information

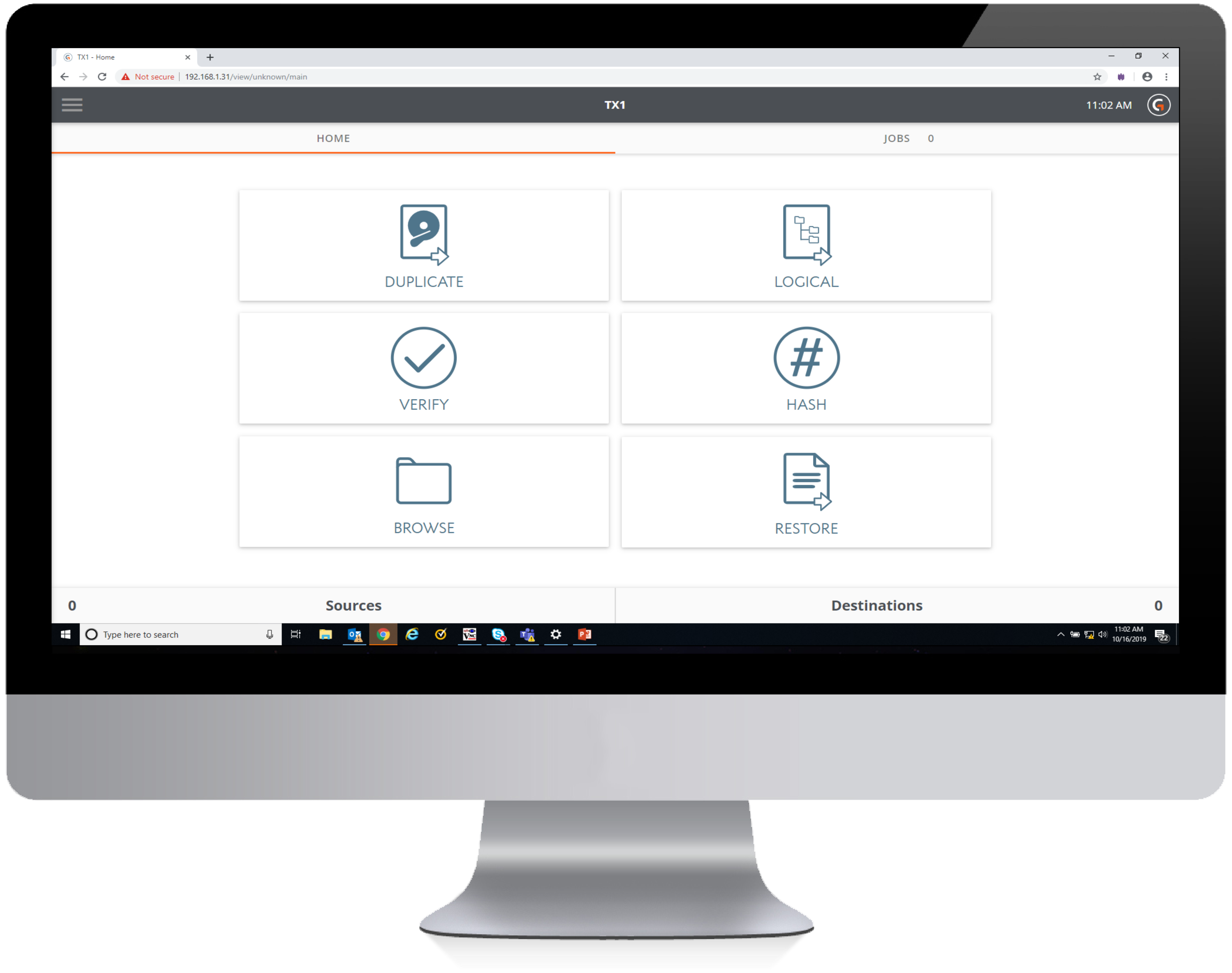
Enhanced User Experience

1. Multi-user access
2. Update TX1 firmware via USB or any mounted file system
3. Improved forensic lab operations
4. Localization updates from TX1 2.2

Customer Focus

Remote Access

opentext™ | Tableau Hardware



Remote Access (remote web interface)

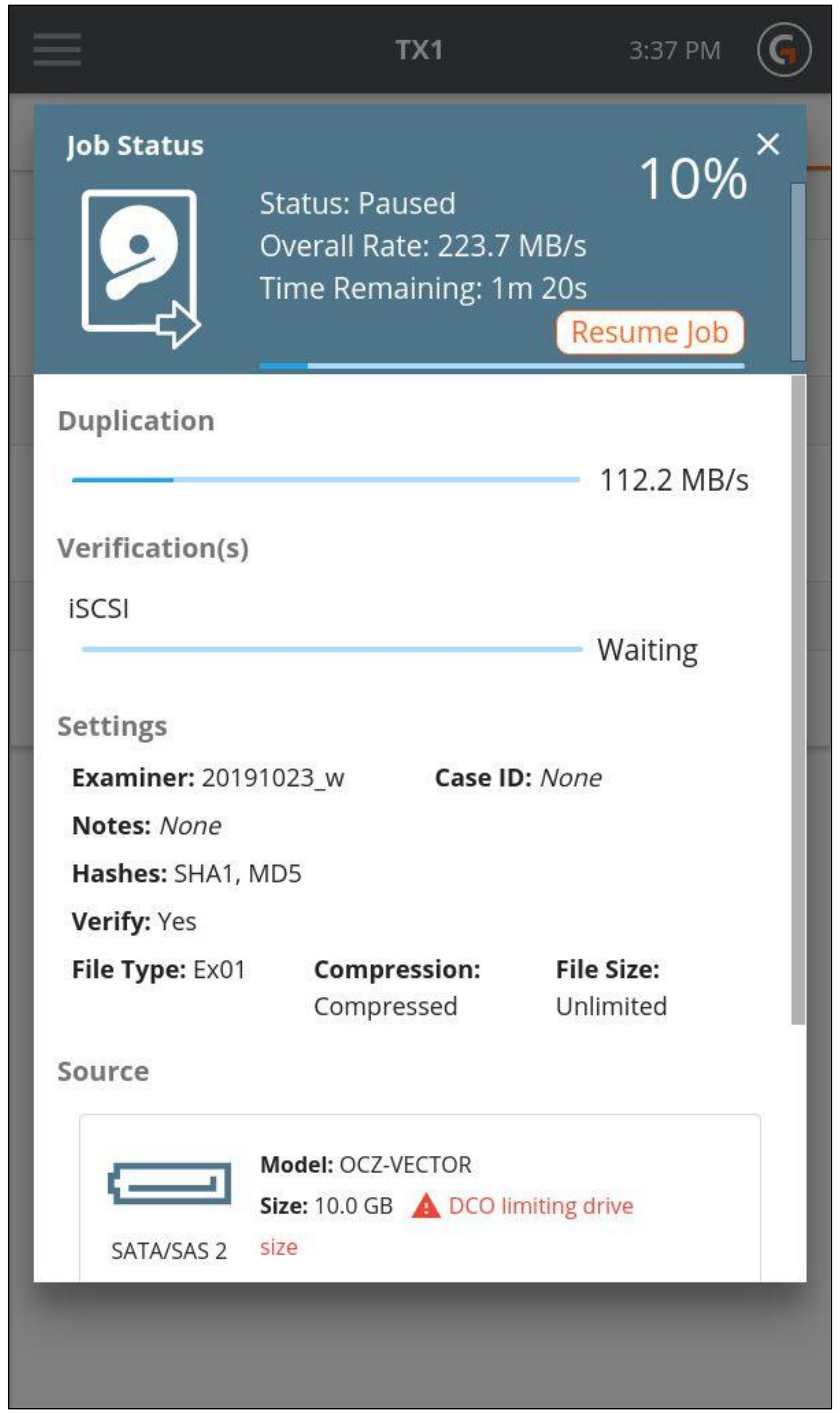
- Save time by quickly accessing the TX1's UI through the web UI on a computer, smartphone or tablet when connected to the same network.
- Users can now easily setup and monitor TX1 operations **without** the need to be physically at the device.
- Provides an efficient division of labor as an expert examiner can remotely manage operations for multiple TX1's to support their investigation while a junior examiner is connecting media.
- Ability to download images through the remote web UI.

Remote API

- Provides customers the ability to extend, automate and integrate the TX1 with their forensic workflow.

Pause & Resume

opentext™ | Tableau Hardware



TX1 3:37 PM

Job Status

10%

Status: Paused
Overall Rate: 223.7 MB/s
Time Remaining: 1m 20s

Resume Job

Duplication

112.2 MB/s

Verification(s)

iSCSI

Waiting

Settings

Examiner: 20191023_w **Case ID:** *None*

Notes: *None*

Hashes: SHA1, MD5

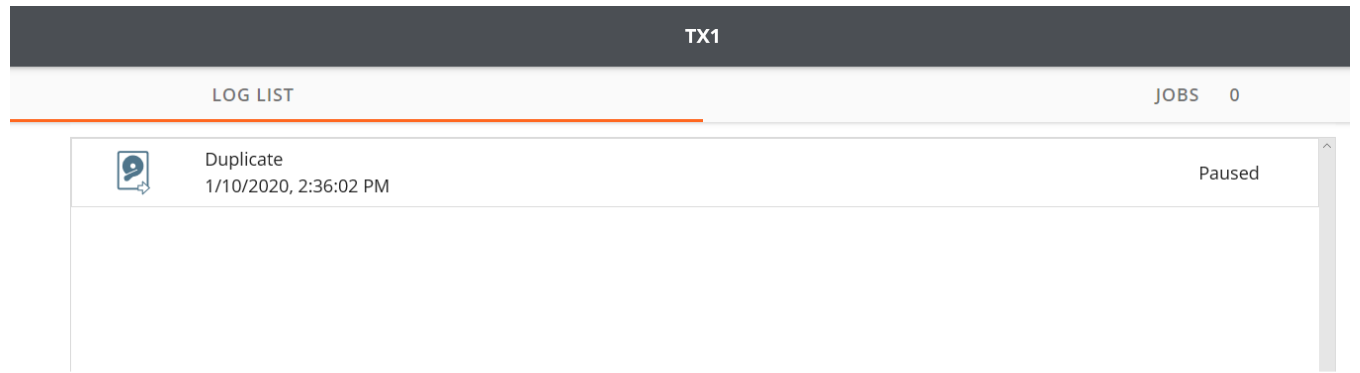
Verify: Yes

File Type: Ex01 **Compression:** Compressed **File Size:** Unlimited

Source

SATA/SAS 2

Model: OCZ-VECTOR
Size: 10.0 GB ⚠ DCO limiting drive size



TX1

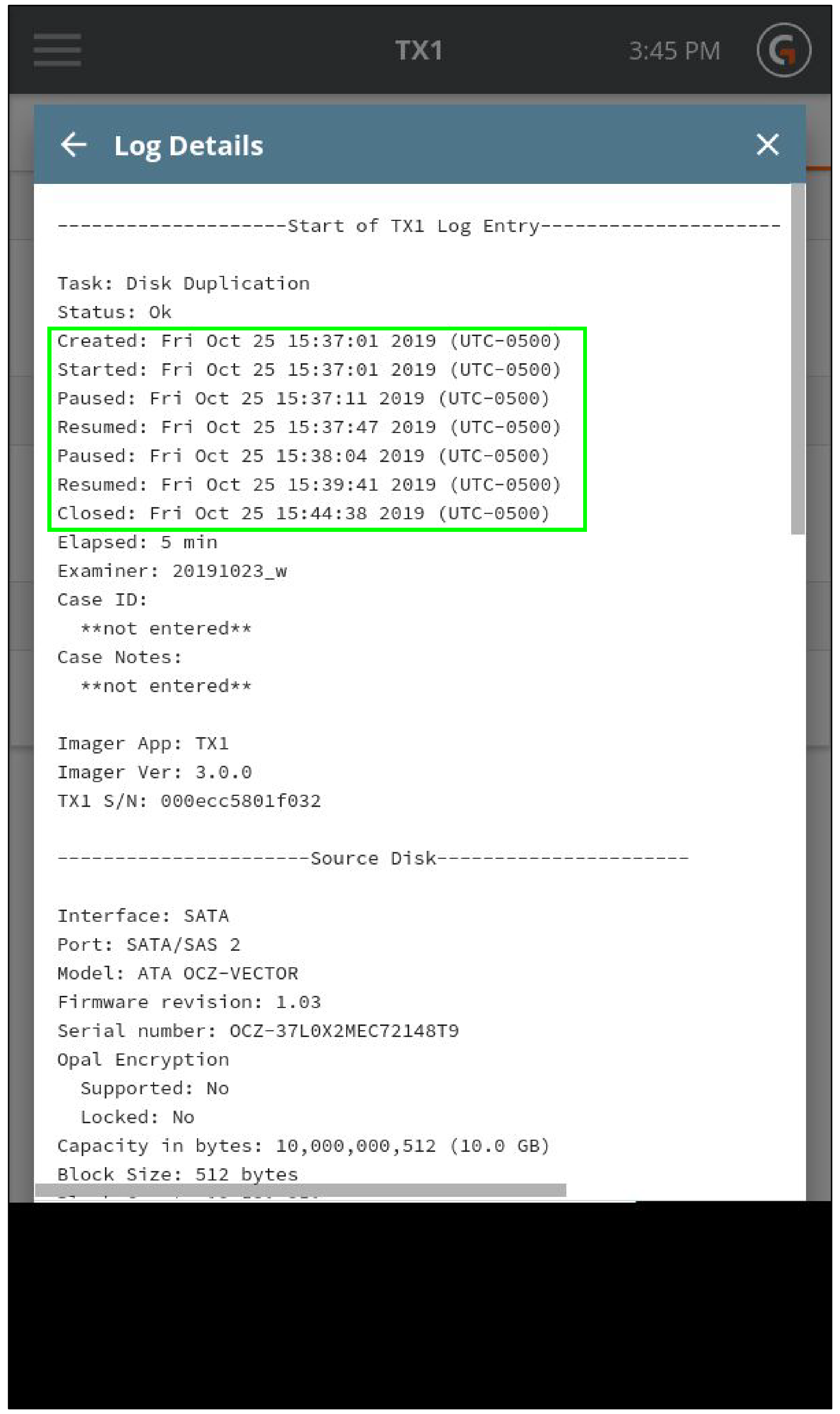
LOG LIST JOBS 0

Duplicate
1/10/2020, 2:36:02 PM
Paused

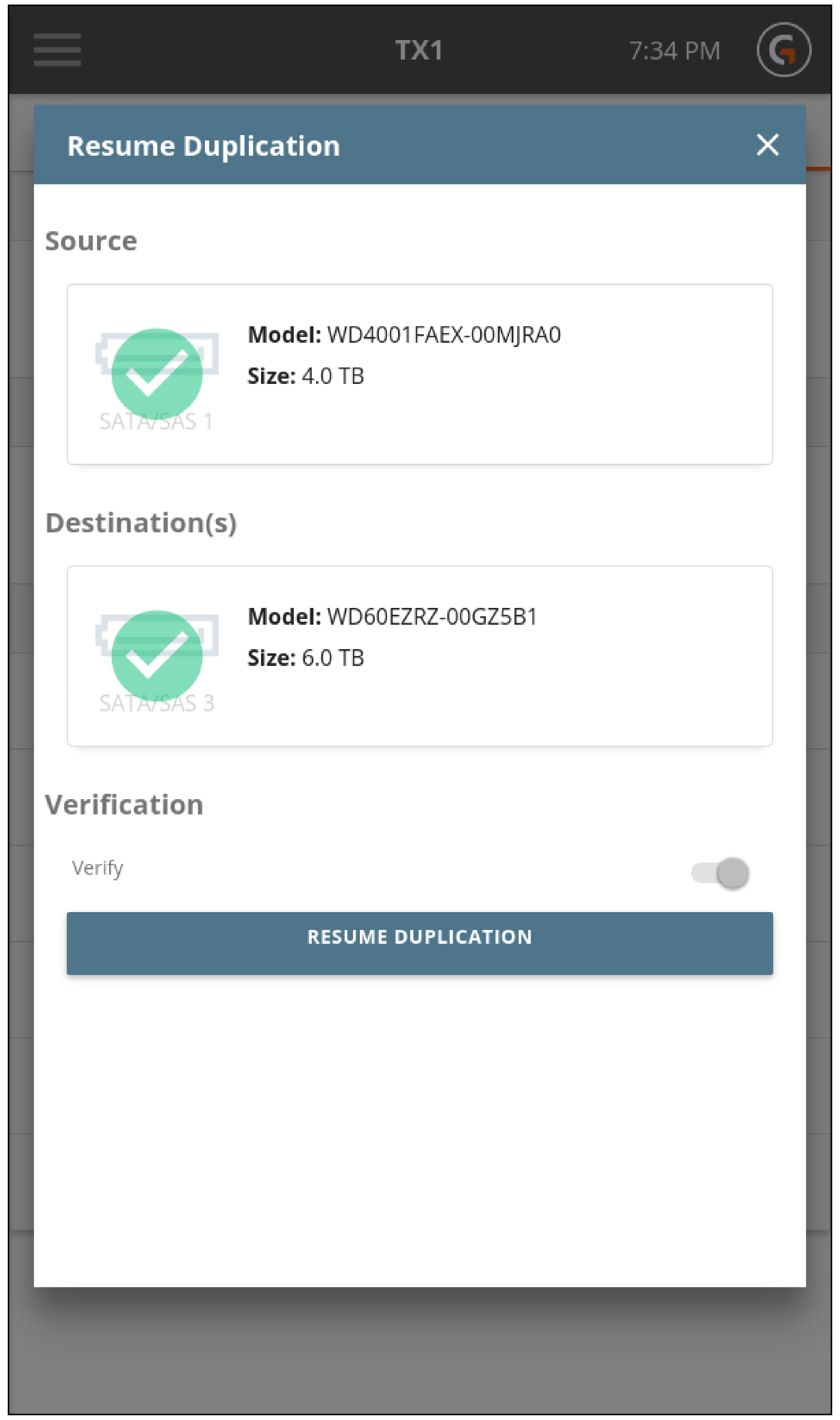
Pause and Resume

- Users can now pause any running imaging job (E01, Ex01, DD, DMG) and then resume it later, even across power-cycles.
- Pause and resume saves time in a variety of scenarios that previously required the job to be restarted:
    - Unexpected loss of power or drive connection
    - Acquisition priorities change
    - Unsafe scene or time on scene has expired
    - A critical TX1 hardware failure occurs (this scenario involves a second TX1 and moving the original TX1’s SD card)

Pause & Resume



```
--------------------Start of TX1 Log Entry--------------------

Task: Disk Duplication
Status: Ok
Created: Fri Oct 25 15:37:01 2019 (UTC-0500)
Started: Fri Oct 25 15:37:01 2019 (UTC-0500)
Paused: Fri Oct 25 15:37:11 2019 (UTC-0500)
Resumed: Fri Oct 25 15:37:47 2019 (UTC-0500)
Paused: Fri Oct 25 15:38:04 2019 (UTC-0500)
Resumed: Fri Oct 25 15:39:41 2019 (UTC-0500)
Closed: Fri Oct 25 15:44:38 2019 (UTC-0500)
Elapsed: 5 min
Examiner: 20191023_w
Case ID:
  **not entered**
Case Notes:
  **not entered**

Imager App: TX1
Imager Ver: 3.0.0
TX1 S/N: 000ecc5801f032

----------------------Source Disk----------------------

Interface: SATA
Port: SATA/SAS 2
Model: ATA OCZ-VECTOR
Firmware revision: 1.03
Serial number: OCZ-37L0X2MEC72148T9
Opal Encryption
  Supported: No
  Locked: No
Capacity in bytes: 10,000,000,512 (10.0 GB)
Block Size: 512 bytes
```



Source

SATA/SAS 1
Model: WD4001FAEX-00MJRA0
Size: 4.0 TB

Destination(s)

SATA/SAS 3
Model: WD60EZRZ-00GZ5B1
Size: 6.0 TB

Verification

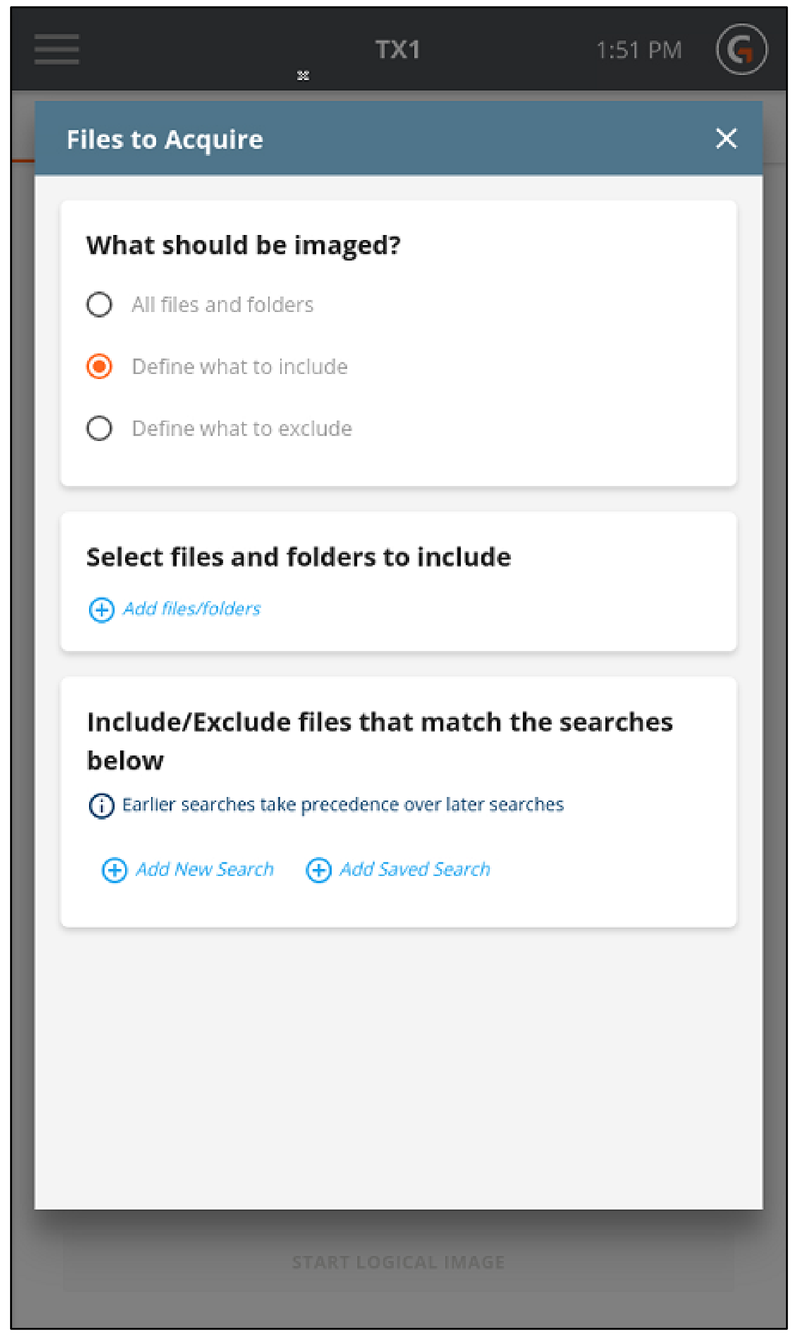
Verify

Pause and Resume

- TX1 checks source/destination media is correct before allowing the job to resume
- The Log Details document when a job has been paused and resumed

Logical Image Search Enhancements

opentext™ | Tableau Hardware



TX1 1:51 PM

Files to Acquire

What should be imaged?

○ All files and folders
● Define what to include
○ Define what to exclude

Select files and folders to include

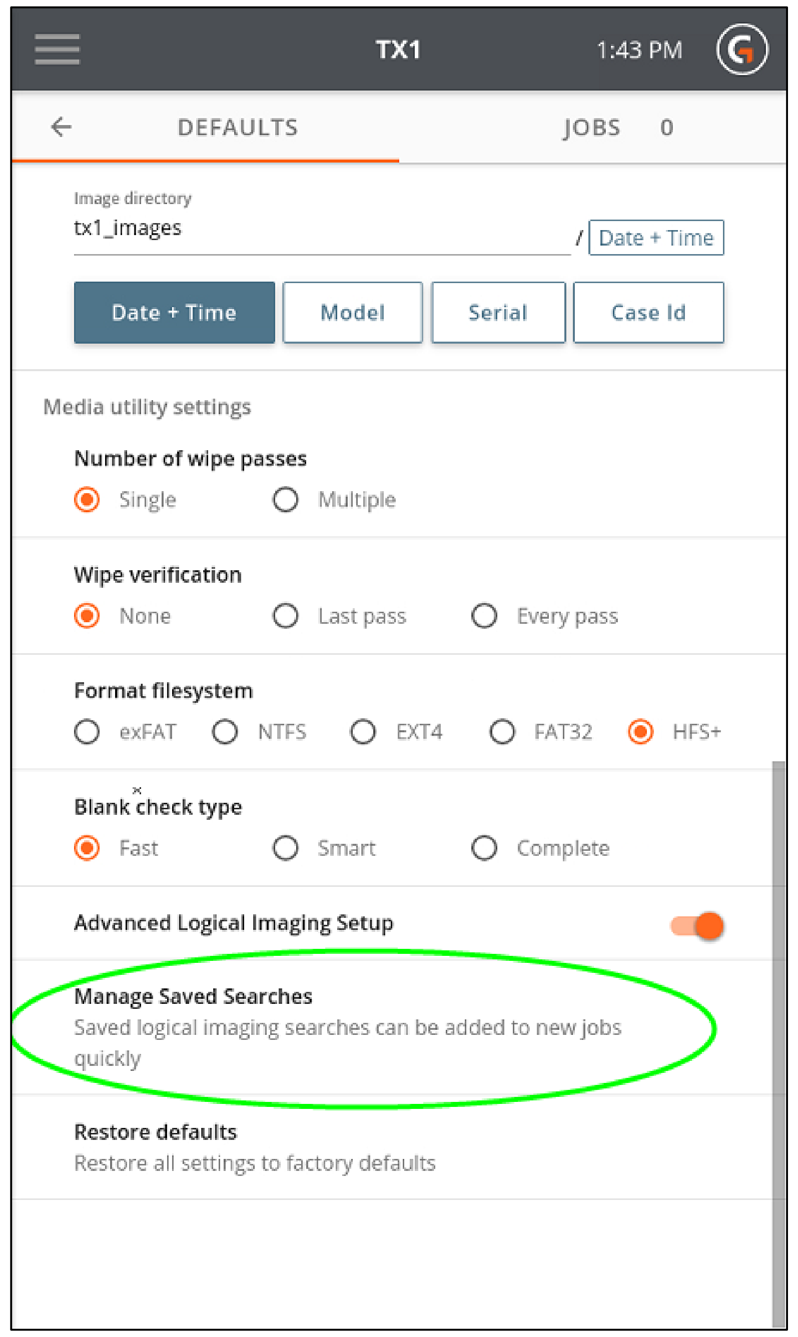
Add files/folders

Include/Exclude files that match the searches below

Earlier searches take precedence over later searches

Add New Search   Add Saved Search

START LOGICAL IMAGE



TX1 1:43 PM

DEFAULTS   JOBS 0

Image directory
tx1_images / Date + Time

Date + Time | Model | Serial | Case Id

Media utility settings

Number of wipe passes
● Single ○ Multiple

Wipe verification
● None ○ Last pass ○ Every pass

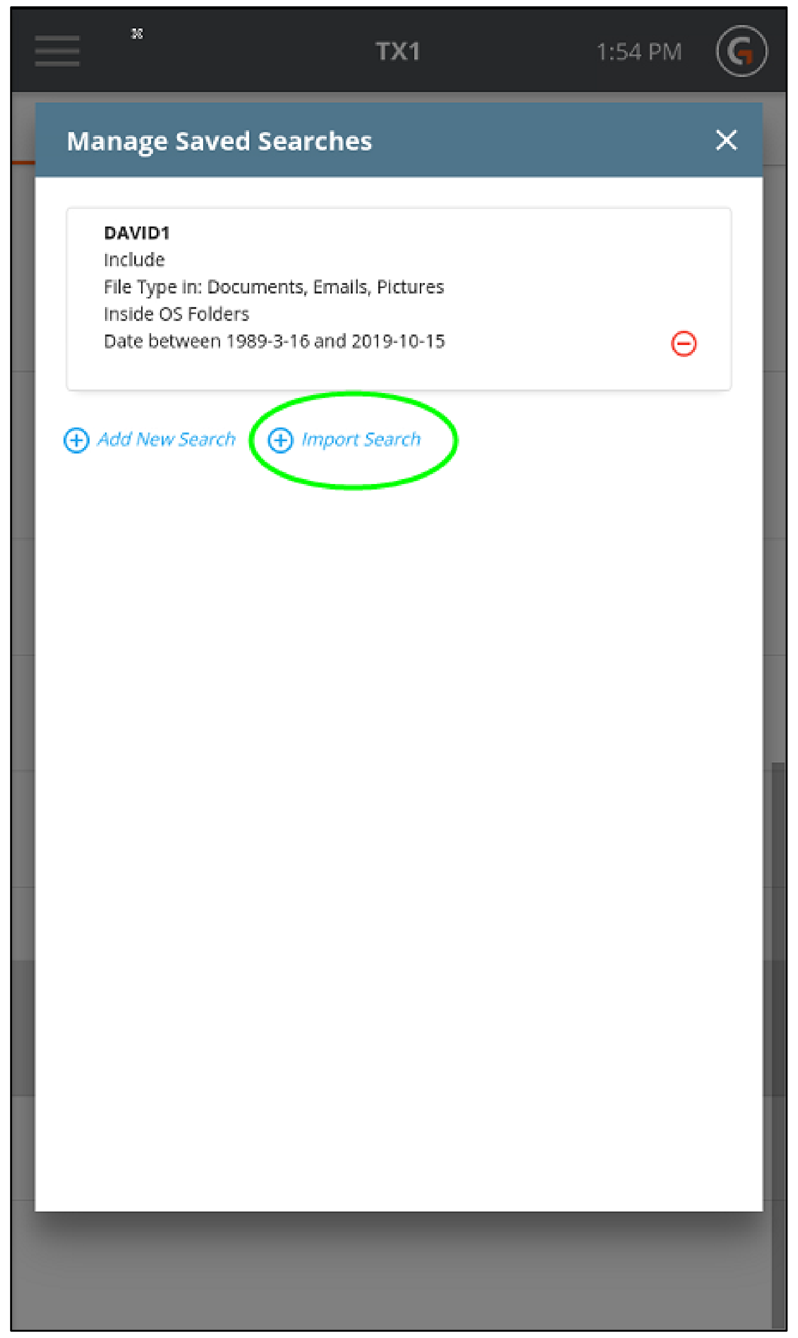
Format filesystem
○ exFAT ○ NTFS ○ EXT4 ○ FAT32 ● HFS+

Blank check type
● Fast ○ Smart ○ Complete

Advanced Logical Imaging Setup

Manage Saved Searches
Saved logical imaging searches can be added to new jobs quickly

Restore defaults
Restore all settings to factory defaults

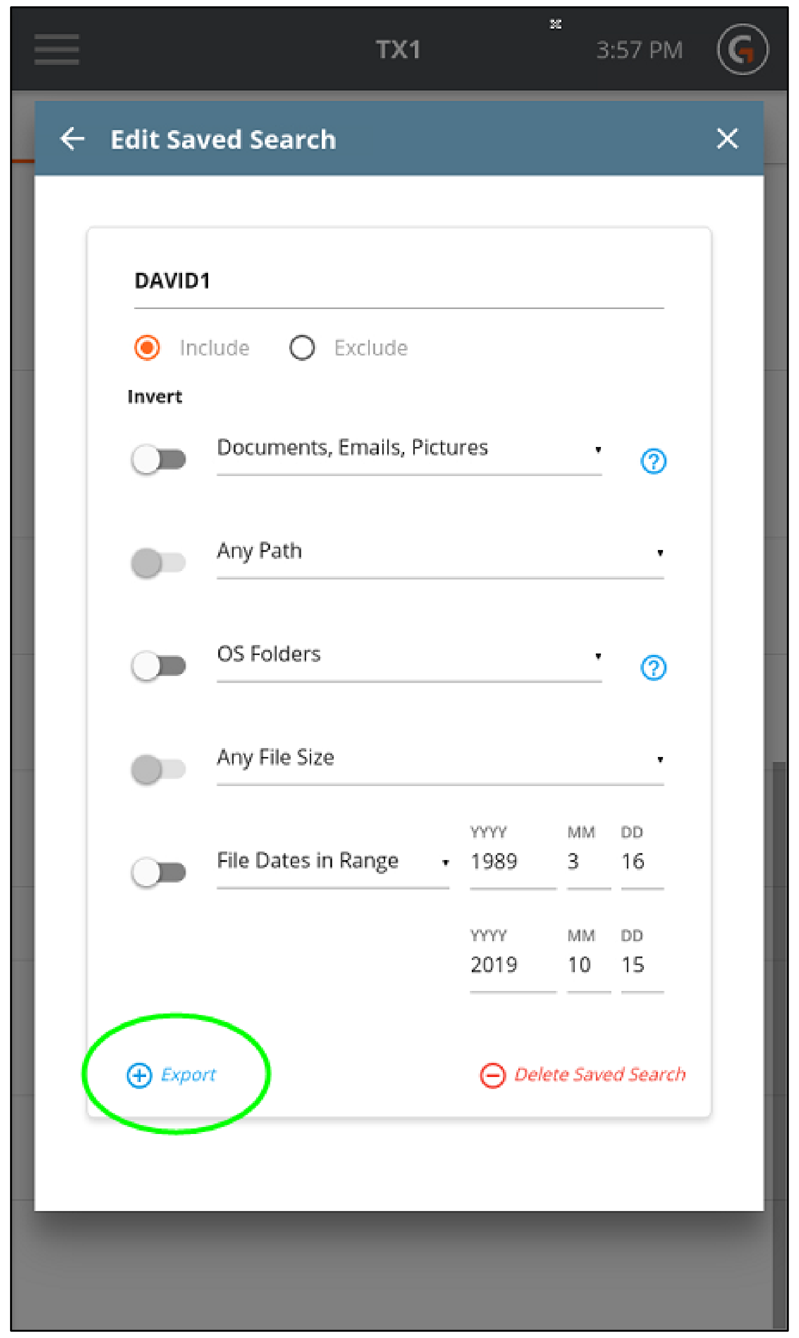


TX1 1:54 PM

Manage Saved Searches

DAVID1
Include
File Type in: Documents, Emails, Pictures
Inside OS Folders
Date between 1989-3-16 and 2019-10-15

Add New Search   Import Search



TX1 3:57 PM

Edit Saved Search

DAVID1

● Include ○ Exclude

Invert

Documents, Emails, Pictures
Any Path
OS Folders
Any File Size
File Dates in Range   YYYY 1989   MM 3   DD 16
YYYY 2019   MM 10   DD 15

Export   Delete Saved Search

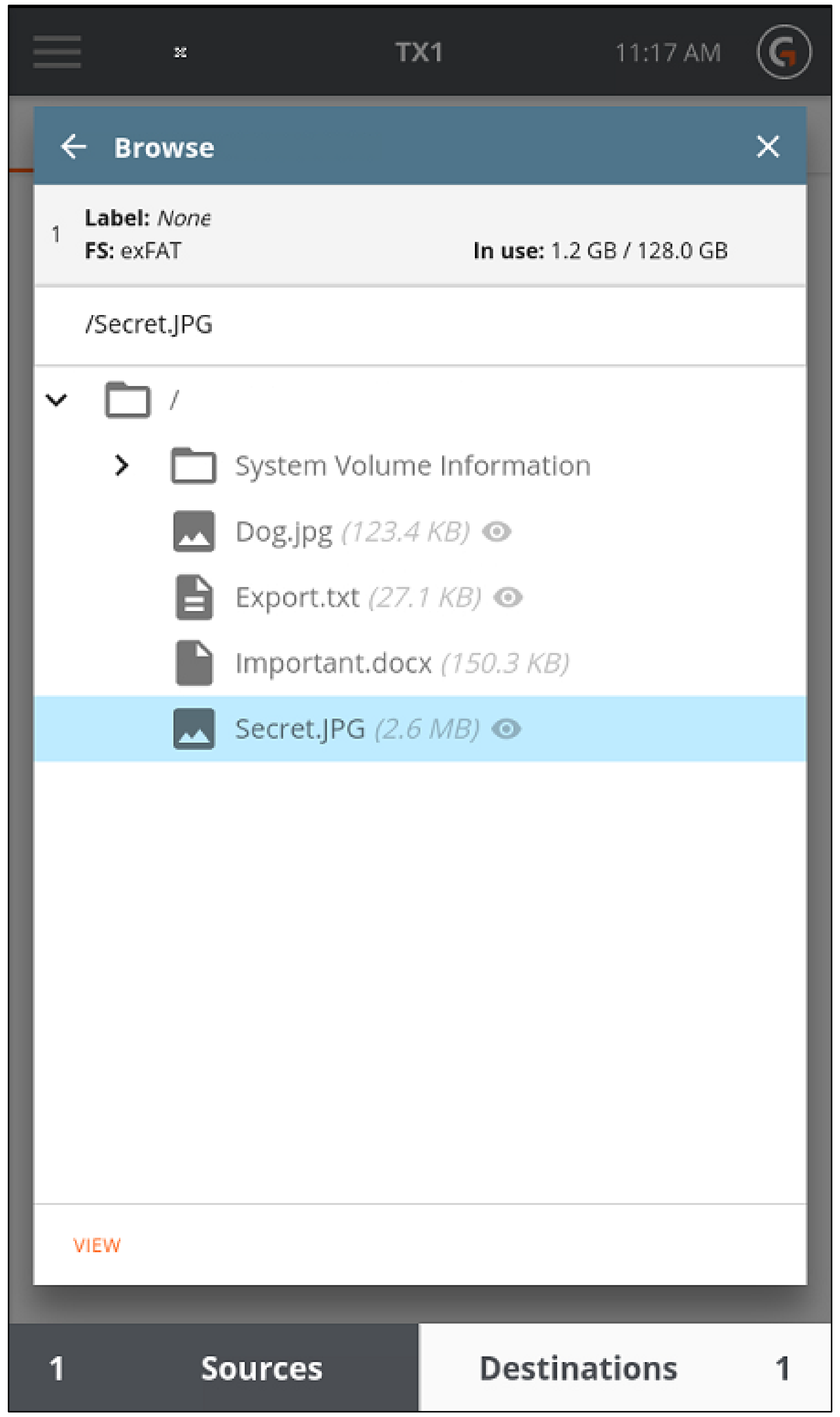
Export and Import Logical Image Searches

- Exporting and importing saved logical image searches enables users to quickly share best practices and standardize search criteria across their team, department or agency.
- Allow senior investigators to enable junior investigators without intensive training.

Wildcard Characters Now Supported for Logical Image Search Criteria

View Images and Plain Text Files

opentext™ | Tableau Hardware



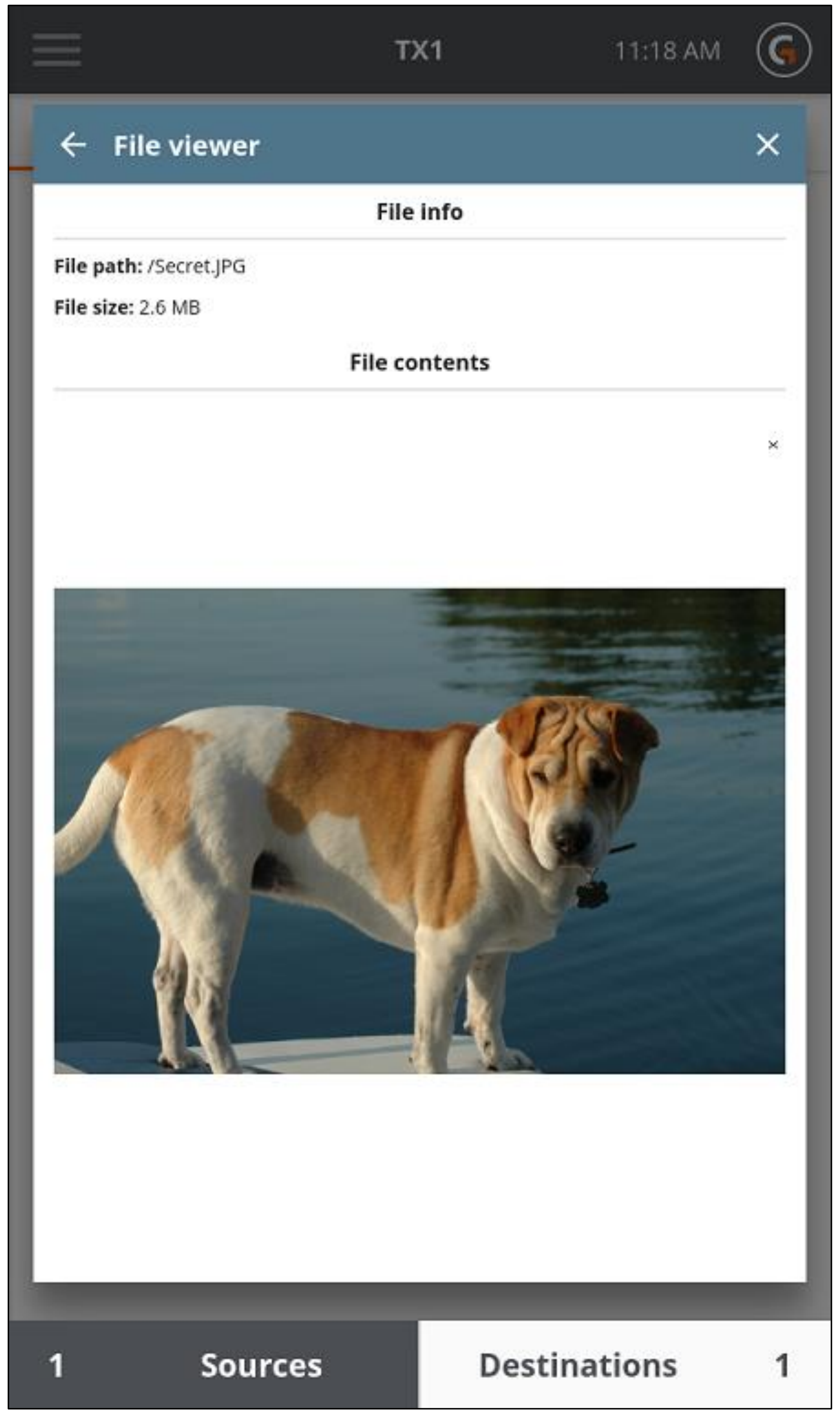
TX1 11:17 AM

Browse

1 **Label:** *None*
FS: exFAT **In use:** 1.2 GB / 128.0 GB

/Secret.JPG

- /
  - System Volume Information
  - Dog.jpg *(123.4 KB)*
  - Export.txt *(27.1 KB)*
  - Important.docx *(150.3 KB)*
  - Secret.JPG *(2.6 MB)*



TX1 11:18 AM

File viewer

File info

File path: /Secret.JPG

File size: 2.6 MB

File contents

View Images and Plain Text Files

- Viewing images and text files of suspect media directly on the TX1 LCD enables users to quickly triage and determine the priority or relevance of that suspect media to the investigation.
- Files can also be downloaded through the remote web interface.

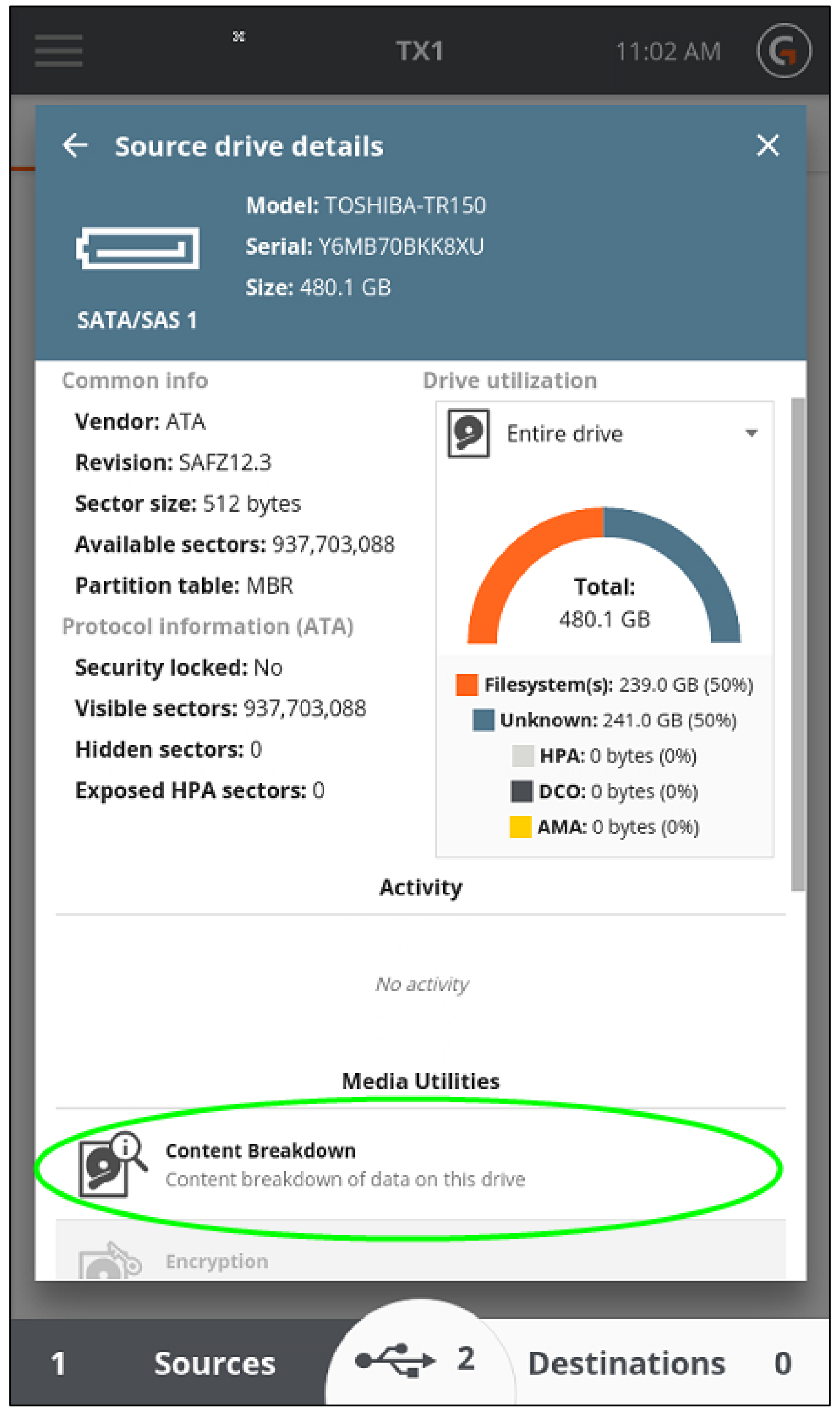
File size also now displayed within the Browse screen

The following file extensions are viewable on TX1:

Text type: .bat, .c, .conf, .csv, .h, .htm, .html, .ini, .js, .json, .log, .nfo, .py, .readme, .sh,
.text, .tsv, .txt, .xml

Image type: .apng, .bmp, .gif, .ico, .cur, .jpg, .jpeg, .jfif, .pjpeg, .pjp, .png, .svg, .webp

Disk > Partition > File System Display



Source drive details

SATA/SAS 1

Model: TOSHIBA-TR150
Serial: Y6MB70BKK8XU
Size: 480.1 GB

Common info

Vendor: ATA
Revision: SAFZ12.3
Sector size: 512 bytes
Available sectors: 937,703,088
Partition table: MBR

Protocol information (ATA)

Security locked: No
Visible sectors: 937,703,088
Hidden sectors: 0
Exposed HPA sectors: 0

Drive utilization

Entire drive

Total: 480.1 GB

🟧 **Filesystem(s):** 239.0 GB (50%)
🟦 **Unknown:** 241.0 GB (50%)
□ **HPA:** 0 bytes (0%)
■ **DCO:** 0 bytes (0%)
🟨 **AMA:** 0 bytes (0%)

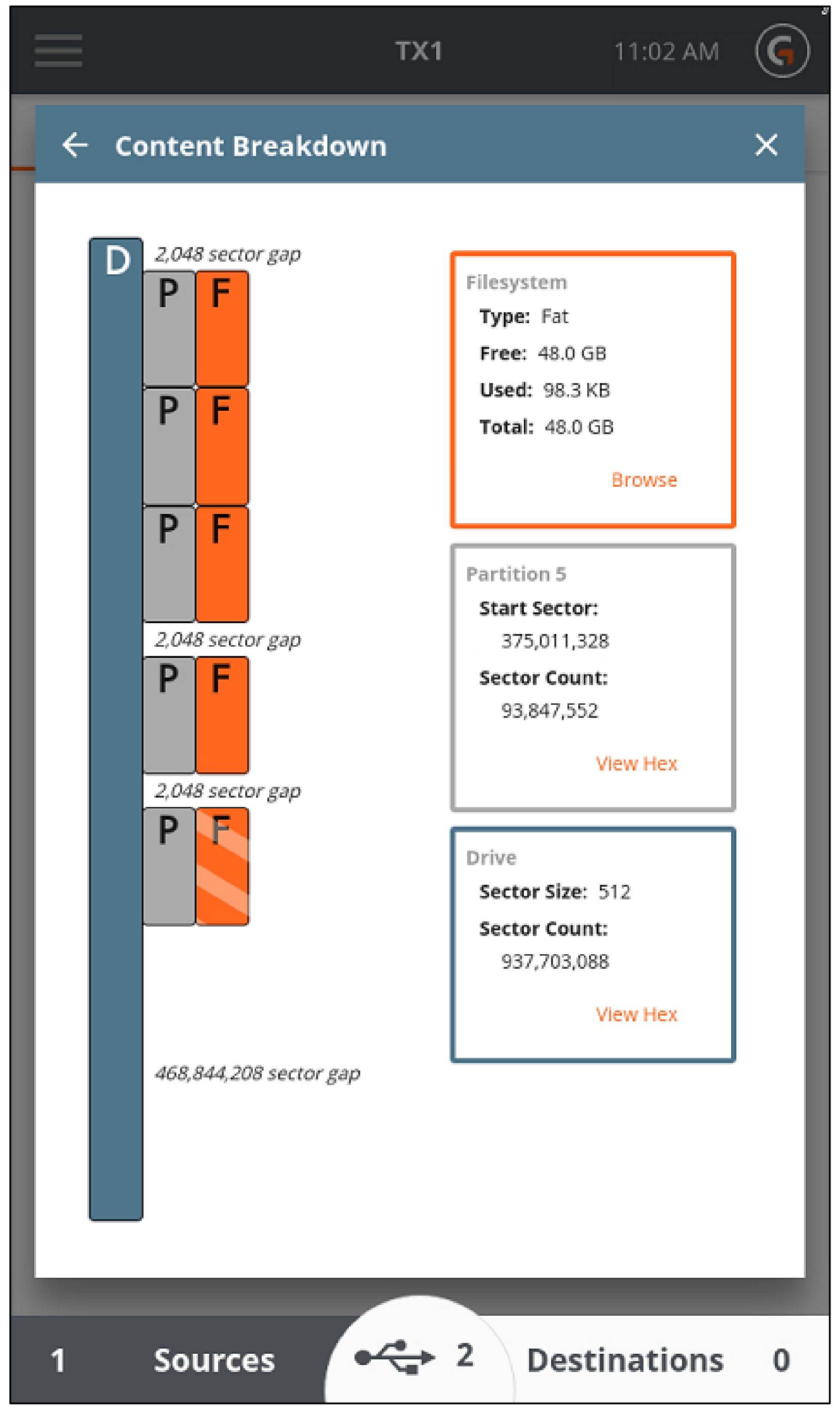
Activity

No activity

Media Utilities

Content Breakdown
Content breakdown of data on this drive

Encryption

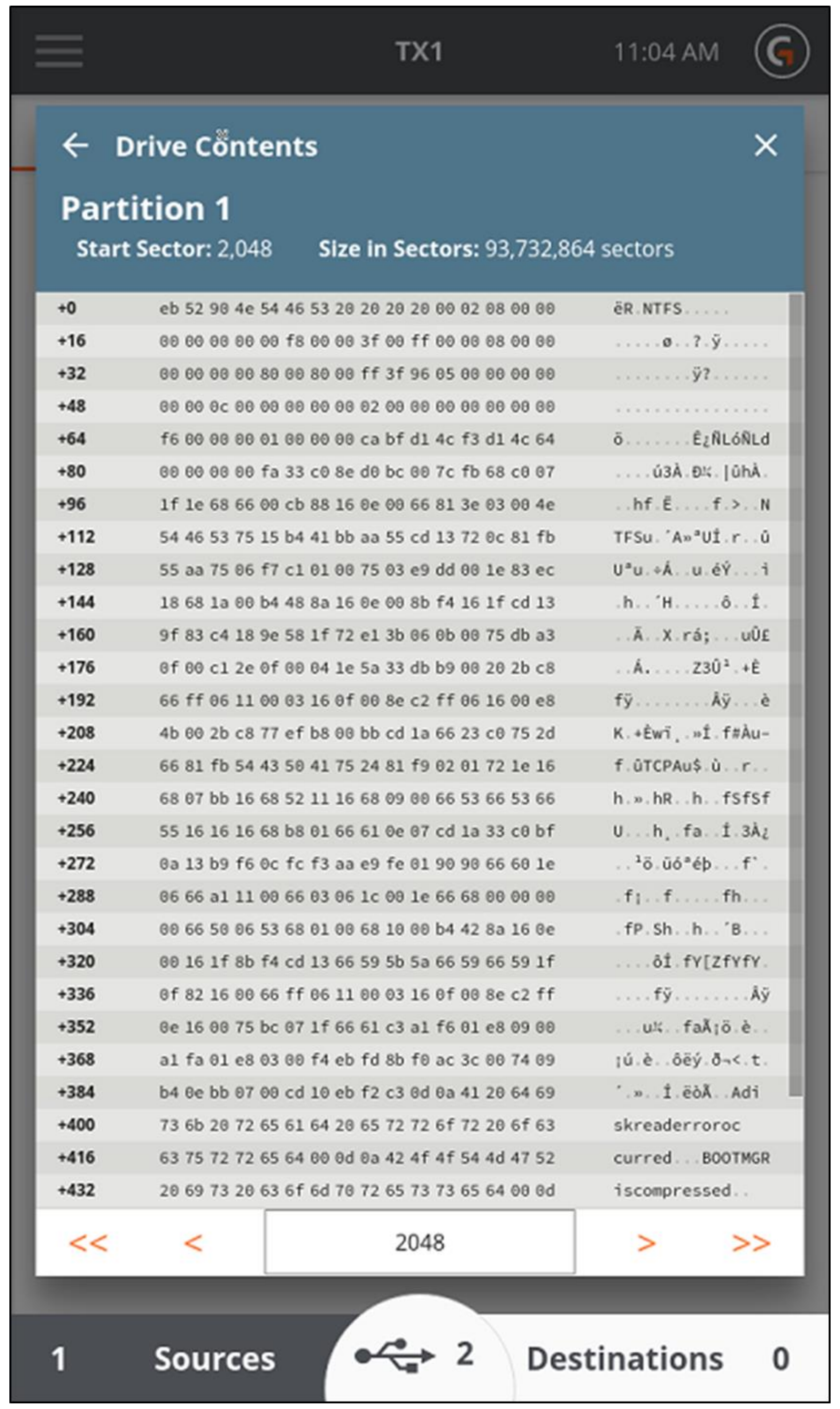


Content Breakdown

Filesystem
Type: Fat
Free: 48.0 GB
Used: 98.3 KB
Total: 48.0 GB
Browse

Partition 5
Start Sector:
375,011,328
Sector Count:
93,847,552
View Hex

Drive
Sector Size: 512
Sector Count:
937,703,088
View Hex



Drive Contents

Partition 1
Start Sector: 2,048 **Size in Sectors:** 93,732,864 sectors

```
+0      eb 52 90 4e 54 46 53 20 20 20 20 00 02 08 00 00   ëR.NTFS.....
+16     00 00 00 00 00 f8 00 00 3f 00 ff 00 00 08 00 00   .....ø..?.ÿ.....
+32     00 00 00 00 80 00 80 00 ff 3f 96 05 00 00 00 00   ........ÿ?......
+48     00 00 0c 00 00 00 00 00 02 00 00 00 00 00 00 00   ................
+64     f6 00 00 00 01 00 00 00 ca bf d1 4c f3 d1 4c 64   ö.......Ê¿ÑLóÑLd
+80     00 00 00 00 fa 33 c0 8e d0 bc 00 7c fb 68 c0 07   ....ú3À.Ð¼.|ûhÀ.
+96     1f 1e 68 66 00 cb 88 16 0e 00 66 81 3e 03 00 4e   ..hf.Ë....f.>..N
+112    54 46 53 75 15 b4 41 bb aa 55 cd 13 72 0c 81 fb   TFSu.´A»ªUÍ.r..û
+128    55 aa 75 06 f7 c1 01 00 75 03 e9 dd 00 1e 83 ec   Uªu.÷Á..u.éÝ...ì
+144    18 68 1a 00 b4 48 8a 16 0e 00 8b f4 16 1f cd 13   .h..´H.....ô..Í.
+160    9f 83 c4 18 9e 58 1f 72 e1 3b 06 0b 00 75 db a3   ..Ä..X.rá;...uÛ£
+176    0f 00 c1 2e 0f 00 04 1e 5a 33 db b9 00 20 2b c8   ..Á.....Z3Û¹. +È
+192    66 ff 06 11 00 03 16 0f 00 8e c2 ff 06 16 00 e8   fÿ........Âÿ...è
+208    4b 00 2b c8 77 ef b8 00 bb cd 1a 66 23 c0 75 2d   K.+Èwï¸.»Í.f#Àu-
+224    66 81 fb 54 43 50 41 75 24 81 f9 02 01 72 1e 16   f.ûTCPAu$.ù..r..
+240    68 07 bb 16 68 52 11 16 68 09 00 66 53 66 53 66   h.».hR..h..fSfSf
+256    55 16 16 16 68 b8 01 66 61 0e 07 cd 1a 33 c0 bf   U...h¸.fa..Í.3À¿
+272    0a 13 b9 f6 0c fc f3 aa e9 fe 01 90 90 66 60 1e   ..¹ö.üóªéþ...f`.
+288    06 66 a1 11 00 66 03 06 1c 00 1e 66 68 00 00 00   .f¡..f.....fh...
+304    00 66 50 06 53 68 01 00 68 10 00 b4 42 8a 16 0e   .fP.Sh..h..´B...
+320    00 16 1f 8b f4 cd 13 66 59 5b 5a 66 59 66 59 1f   ....ôÍ.fY[ZfYfY.
+336    0f 82 16 00 66 ff 06 11 00 03 16 0f 00 8e c2 ff   ....fÿ........Âÿ
+352    0e 16 00 75 bc 07 1f 66 61 c3 a1 f6 01 e8 09 00   ...u¼..faÃ¡ö.è..
+368    a1 fa 01 e8 03 00 f4 eb fd 8b f0 ac 3c 00 74 09   ¡ú.è..ôëý.ð¬<.t.
+384    b4 0e bb 07 00 cd 10 eb f2 c3 0d 0a 41 20 64 69   ´.»..Í.ëòÃ..A di
+400    73 6b 20 72 65 61 64 20 65 72 72 6f 72 20 6f 63   sk read error oc
+416    63 75 72 72 65 64 00 0d 0a 42 4f 4f 54 4d 47 52   curred...BOOTMGR
+432    20 69 73 20 63 6f 6d 70 72 65 73 73 65 64 00 0d    is compressed..
```

2048

Disk > Partition > File System Display

- TX1 now enables investigators to view a drive's layout of partitions, file systems, and raw hex and ASCII data.
- Investigators have a more complete view of suspect media and what evidence might be hidden on it earlier in an investigation.
- For technical investigators, sometimes partition data details are not enough and they want to see individual file details.
- Best practice for drive detail is to look at the hexadecimal (hex) data on the physical suspect media.

Encryption and RAID Detection

opentext™ | Tableau Hardware

Encryption Detection in 3.0

- Check Point Full Disk Encrption
- McAfee Drive Encryption (SafeBoot)
- Sophos Safeguard (Enterprise and Easy/Ultimaco)
- WinMagic SecureDoc Full Disk Encryption
- GuardianEdge Encryption (Plus, Anywhere, Hard Disk Encryption)
- Symantec Endpoint Encryption
- Opal SEDs
- Apple FileVault 2

Already Supported

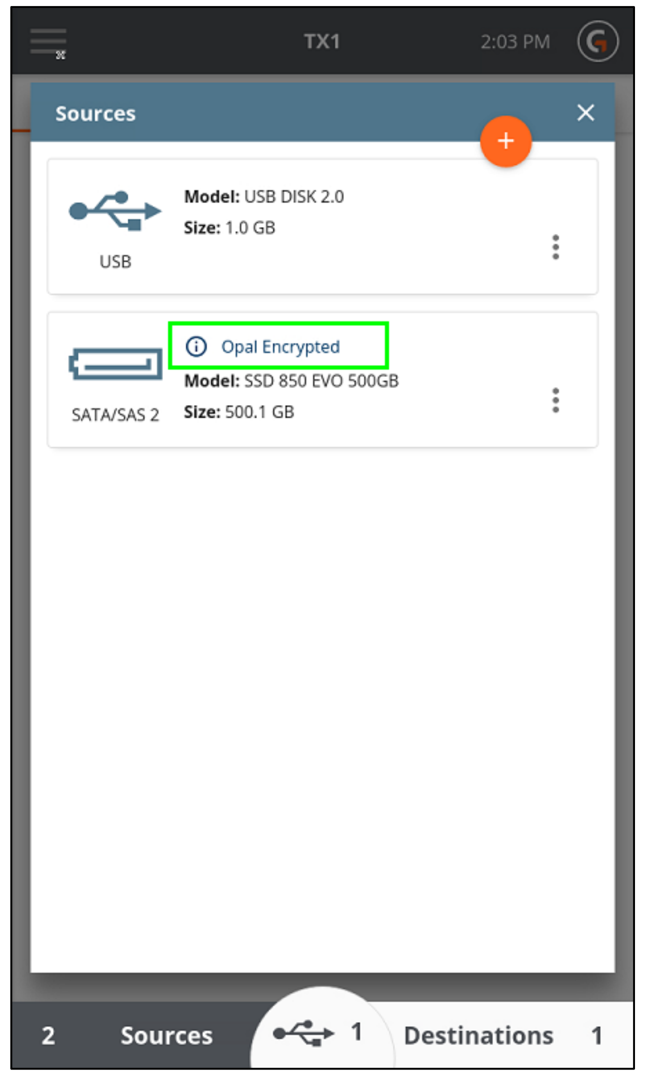
- BitLocker
- BitLocker To Go
- Symantec PGP Disk
- LUKS
- BestCrypt

RAID Detection in 3.0

- Intel RST (BIOS)
- SNIA DDF
- Linux MD
- Adaptec HostRAID ASR
- Highpoint (HPT37X HPT45X)
- Intel Software RAID
- Jmicron JMB36x
- LSI Logic MegaRAID
- Promise FastTrack
- Silicon Image Medley
- VIA Software RAID

Encryption and RAID Detection

- Industry leader in detection of encrypted drive types and drives that are part of a RAID.
- TX1 detecting if a drive is encrypted or part of a RAID provides more information about suspect media earlier in the investigation.



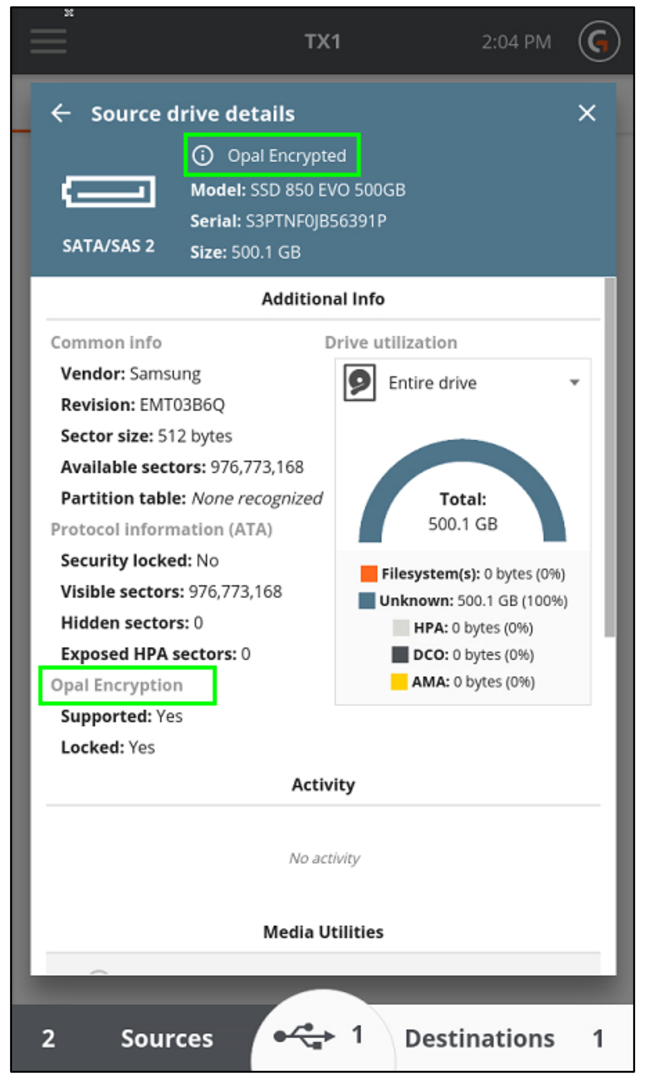
TX1 2:03 PM

Sources

USB
Model: USB DISK 2.0
Size: 1.0 GB

Opal Encrypted
SATA/SAS 2
Model: SSD 850 EVO 500GB
Size: 500.1 GB

2 Sources 1 Destinations 1



TX1 2:04 PM

Source drive details

Opal Encrypted
SATA/SAS 2
Model: SSD 850 EVO 500GB
Serial: S3PTNF0JB56391P
Size: 500.1 GB

Additional Info

Common info
Vendor: Samsung
Revision: EMT03B6Q
Sector size: 512 bytes
Available sectors: 976,773,168
Partition table: *None recognized*

Protocol information (ATA)
Security locked: No
Visible sectors: 976,773,168
Hidden sectors: 0
Exposed HPA sectors: 0

Opal Encryption
Supported: Yes
Locked: Yes

Drive utilization
Entire drive
Total: 500.1 GB
Filesystem(s): 0 bytes (0%)
Unknown: 500.1 GB (100%)
HPA: 0 bytes (0%)
DCO: 0 bytes (0%)
AMA: 0 bytes (0%)

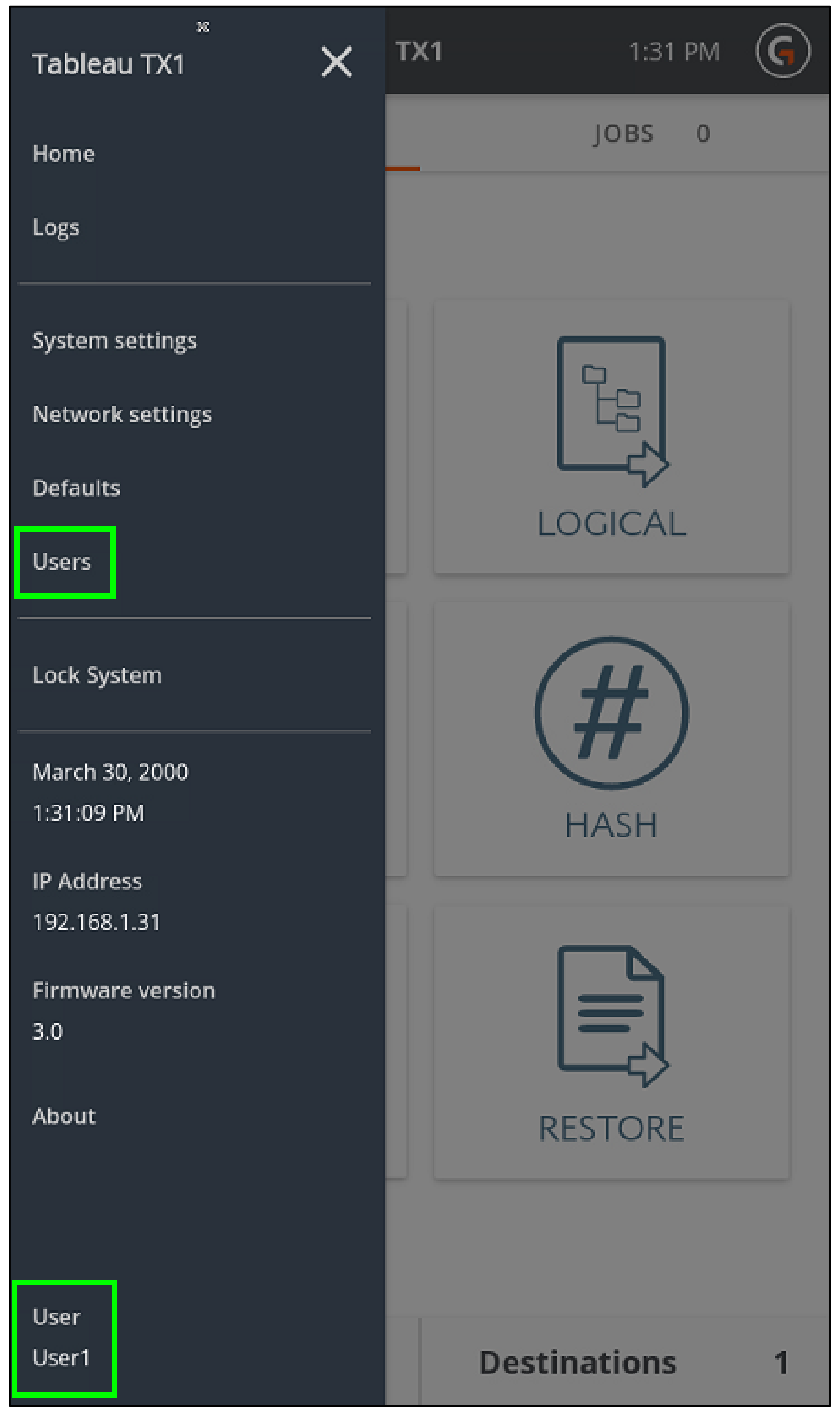
Activity

No activity

Media Utilities

2 Sources 1 Destinations 1

TX1 Multi-user Access

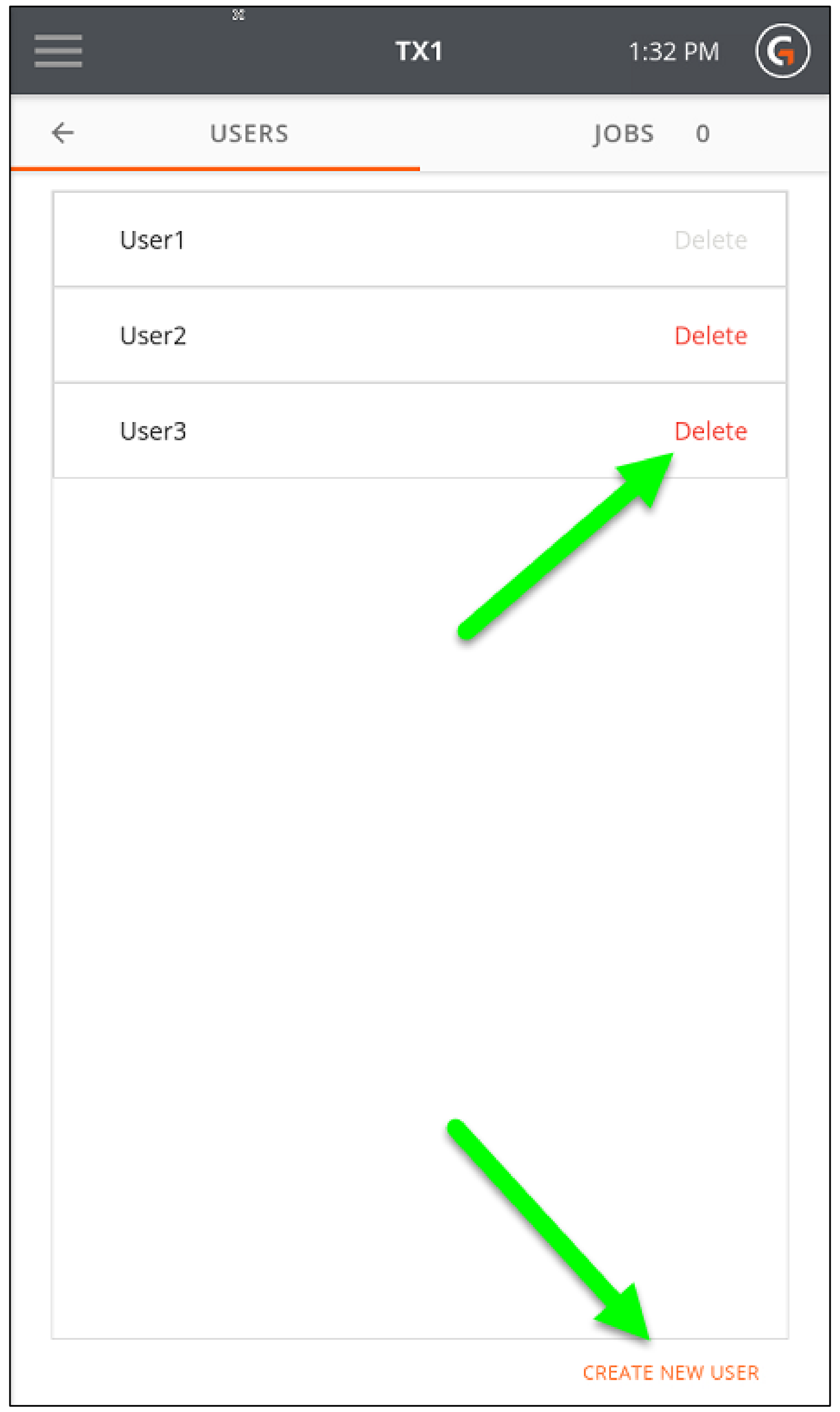


March 30, 2000
1:31:09 PM

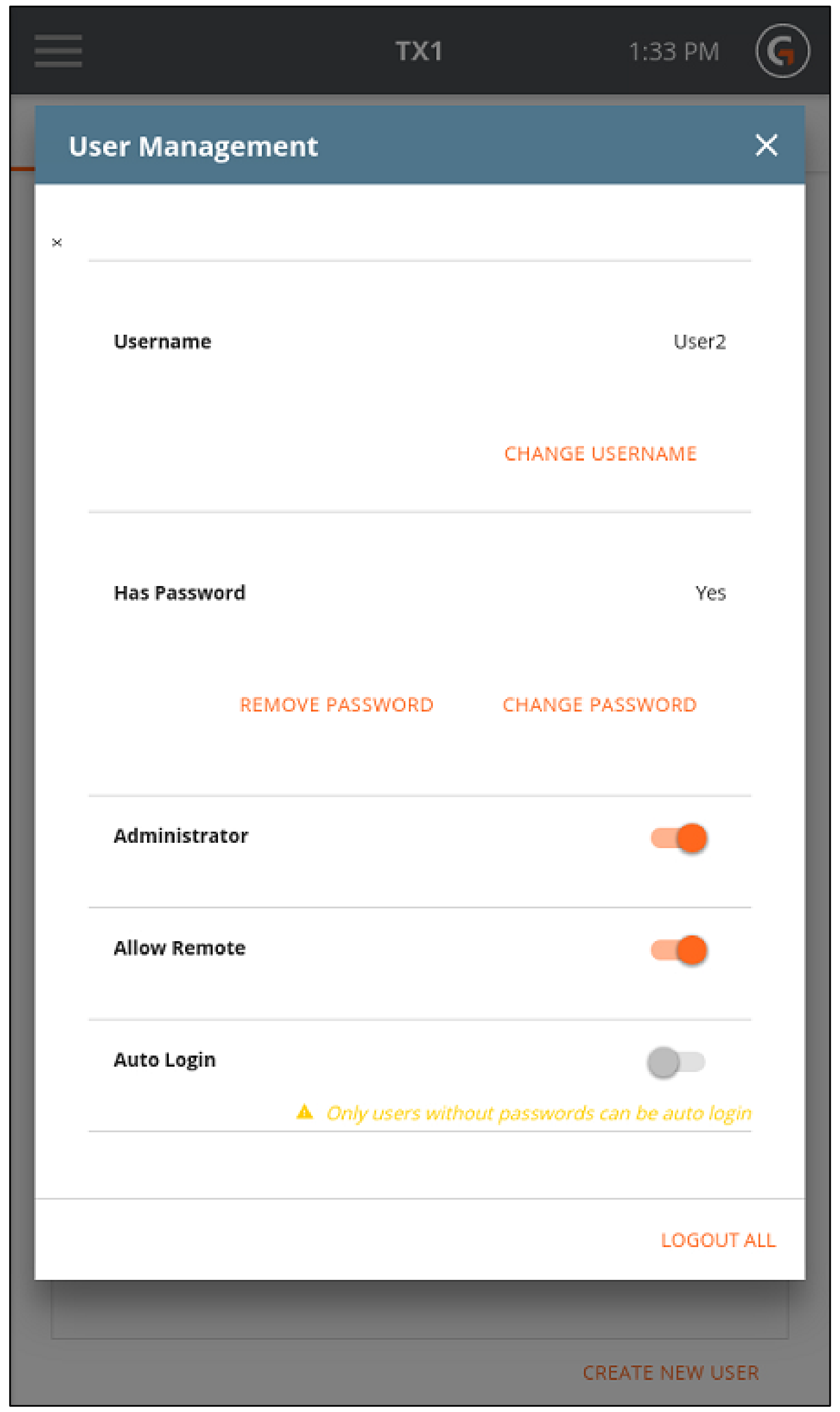
IP Address
192.168.1.31

Firmware version
3.0

User
User1



User1	Delete
User2	Delete
User3	Delete



Username User2

Has Password Yes

Administrator ●

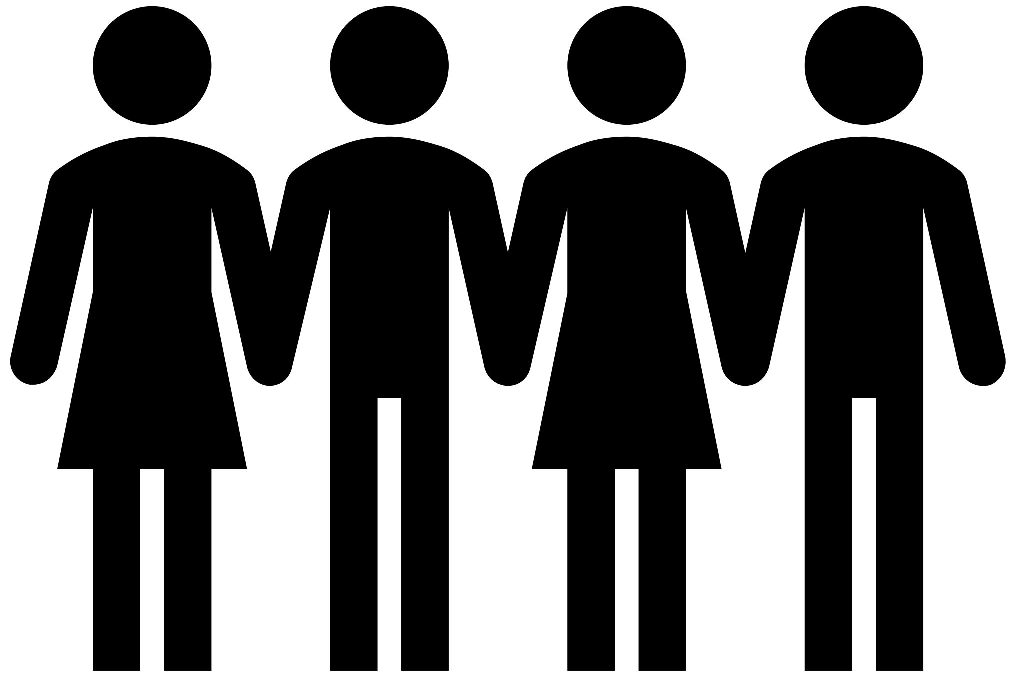
Allow Remote ●

Auto Login ○

⚠ *Only users without passwords can be auto login*

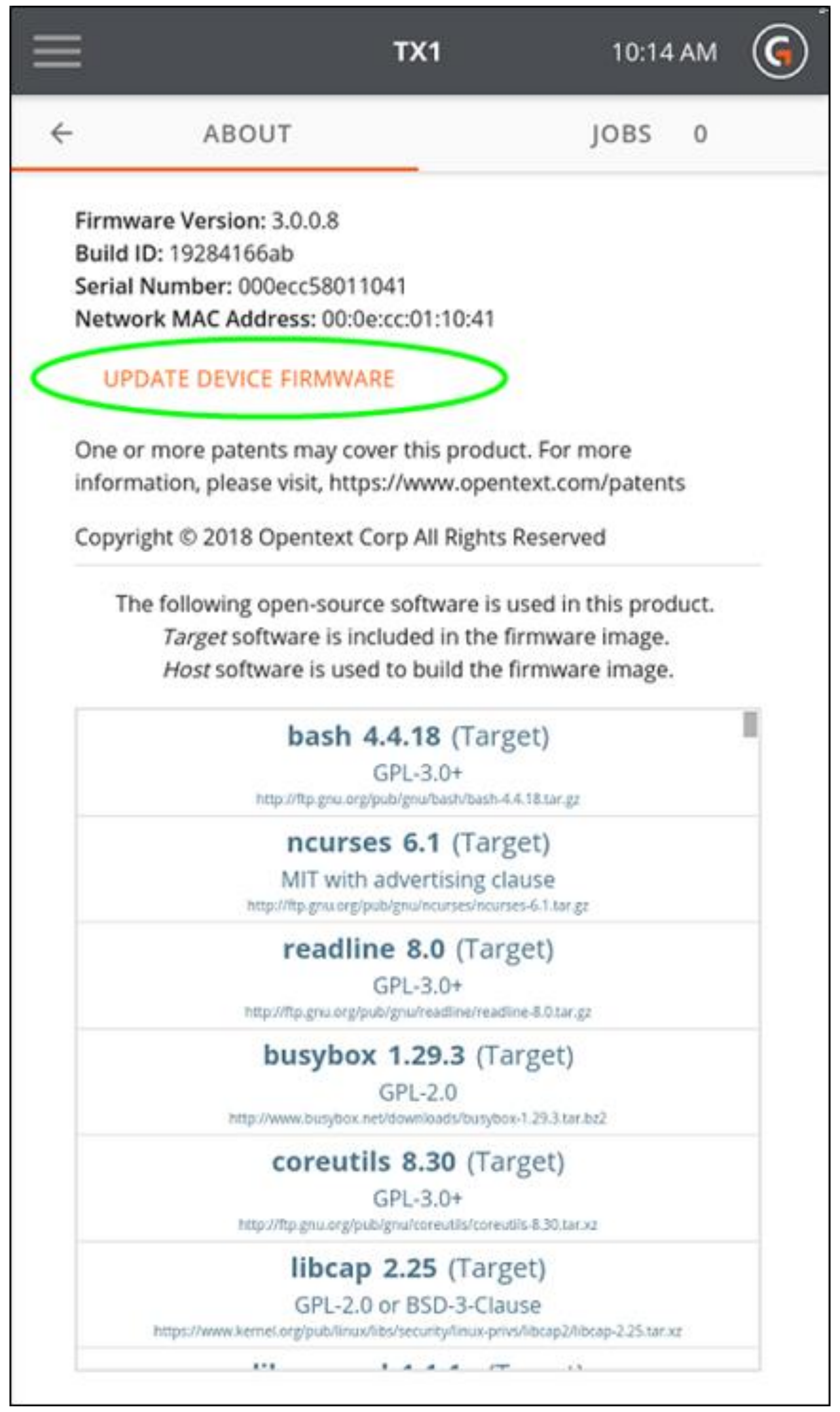
User Profiles

- TX1 now provides the option to create user profiles and administrator rights can be granted to certain users
- Multiple case types can now be pre-configured by an administrator according to an agencies policies and best practices.
- User Profiles can also be used to limit access to available TX1 units by creating unique passwords.
- Multiple users can access a TX1 simultaneously.



Update TX1 Firmware Faster

opentext™ | Tableau Hardware



Firmware Version: 3.0.0.8
Build ID: 19284166ab
Serial Number: 000ecc58011041
Network MAC Address: 00:0e:cc:01:10:41

One or more patents may cover this product. For more information, please visit, https://www.opentext.com/patents

Copyright © 2018 Opentext Corp All Rights Reserved

The following open-source software is used in this product.
Target software is included in the firmware image.
Host software is used to build the firmware image.

bash 4.4.18 (Target)
GPL-3.0+
http://ftp.gnu.org/pub/gnu/bash/bash-4.4.18.tar.gz

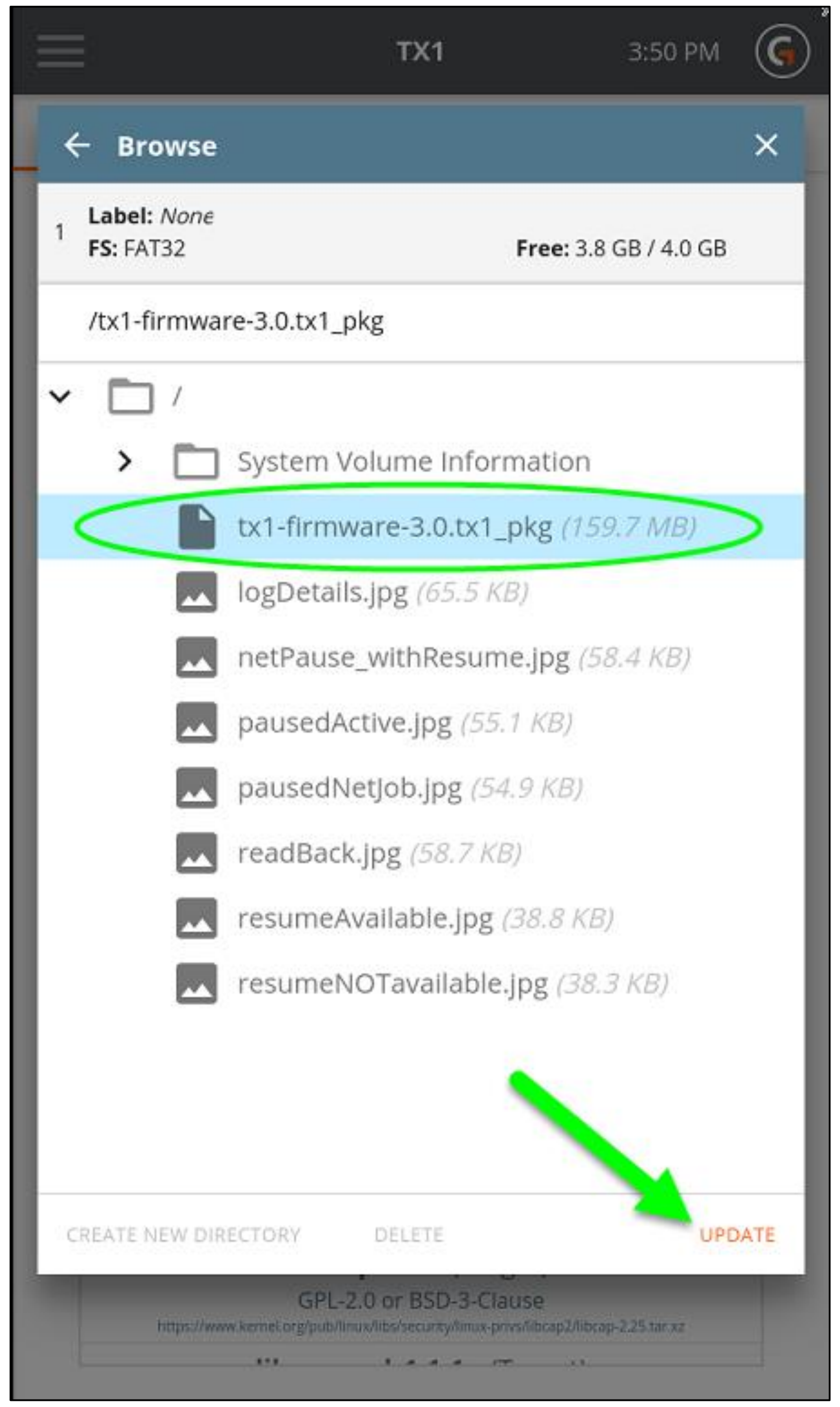
ncurses 6.1 (Target)
MIT with advertising clause
http://ftp.gnu.org/pub/gnu/ncurses/ncurses-6.1.tar.gz

readline 8.0 (Target)
GPL-3.0+
http://ftp.gnu.org/pub/gnu/readline/readline-8.0.tar.gz

busybox 1.29.3 (Target)
GPL-2.0
http://www.busybox.net/downloads/busybox-1.29.3.tar.bz2

coreutils 8.30 (Target)
GPL-3.0+
http://ftp.gnu.org/pub/gnu/coreutils/coreutils-8.30.tar.xz

libcap 2.25 (Target)
GPL-2.0 or BSD-3-Clause
https://www.kernel.org/pub/linux/libs/security/linux-privs/libcap2/libcap-2.25.tar.xz



1 **Label:** *None*
FS: FAT32 **Free:** 3.8 GB / 4.0 GB

/tx1-firmware-3.0.tx1_pkg

/
System Volume Information
tx1-firmware-3.0.tx1_pkg *(159.7 MB)*
logDetails.jpg *(65.5 KB)*
netPause_withResume.jpg *(58.4 KB)*
pausedActive.jpg *(55.1 KB)*
pausedNetJob.jpg *(54.9 KB)*
readBack.jpg *(58.7 KB)*
resumeAvailable.jpg *(38.8 KB)*
resumeNOTavailable.jpg *(38.3 KB)*

GPL-2.0 or BSD-3-Clause
https://www.kernel.org/pub/linux/libs/security/linux-privs/libcap2/libcap-2.25.tar.xz

Update Firmware via USB or Any Mounted File System

- No need to remove SD card.
- Can push Firmware file over mounted network share, then update via the remote web UI rather than updating from the physical unit.
- Firmware update 7.32 onwards

opentext™

opentext™

Tableau v20.2

Tableau TX1 20.2 Enhancements – Themes

Efficiency

1. Pause & Resume Improvements
2. More Media Detection

Faster Acquisitions

Security

1. 802.1X Authentication

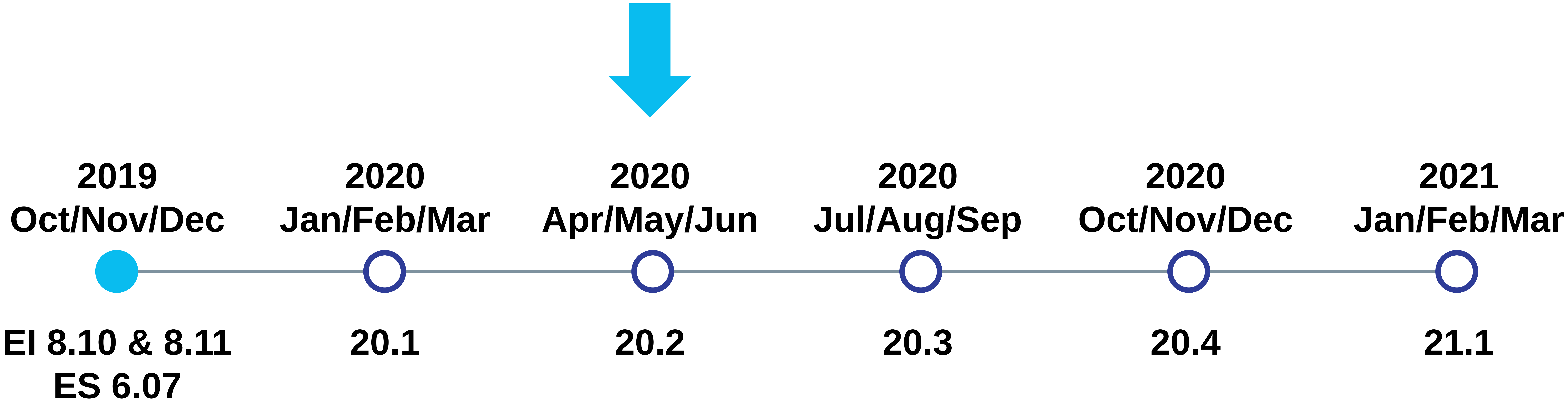
Secure Remote Access

User Experience

1. Multiple UI improvements
2. Multiple log improvements
3. Localization updates
4. Bug fixes

Customer Focus

Product Release Timeline



2019 Oct/Nov/Dec
EI 8.10 & 8.11
ES 6.07

2020 Jan/Feb/Mar
20.1

2020 Apr/May/Jun
20.2

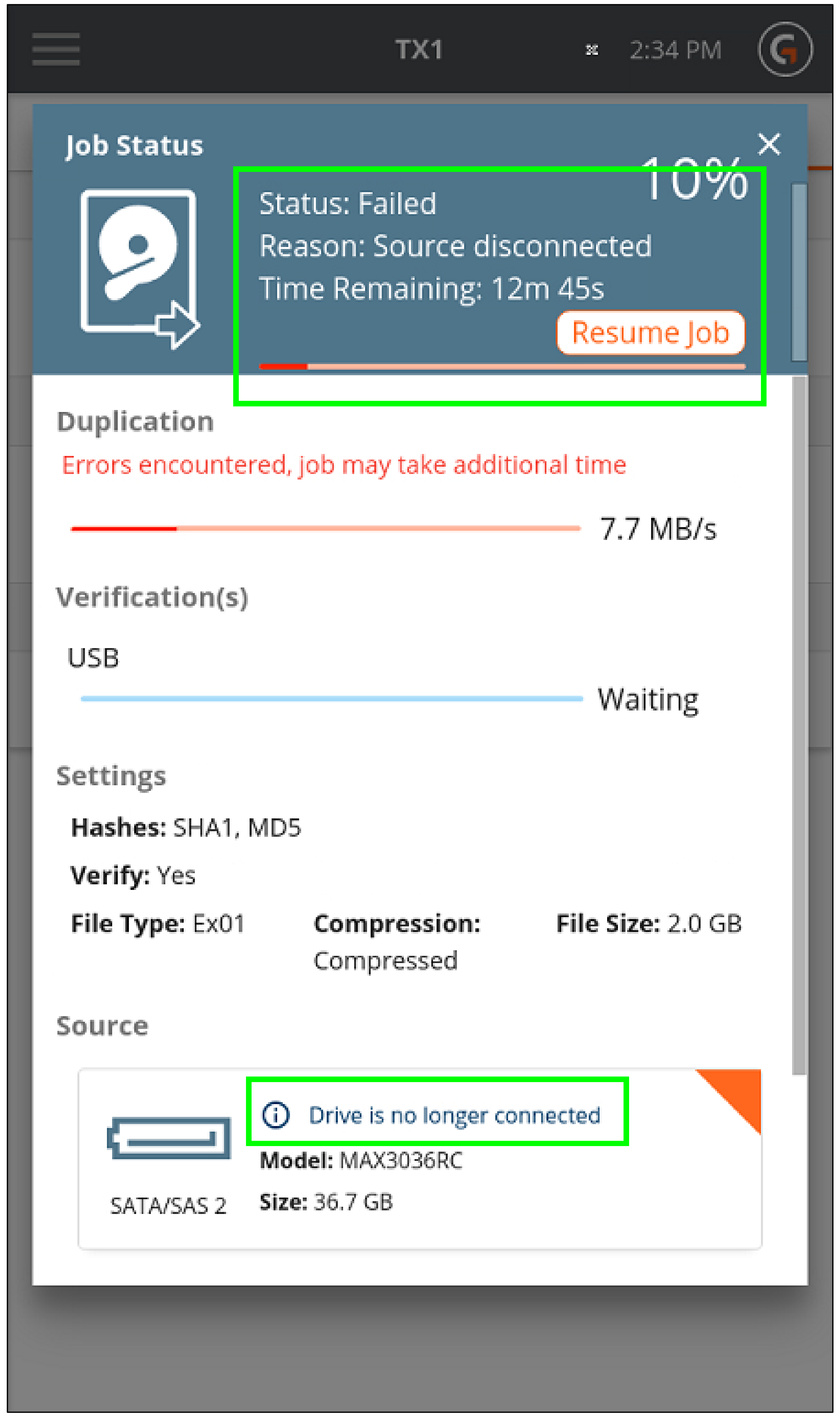
2020 Jul/Aug/Sep
20.3

2020 Oct/Nov/Dec
20.4

2021 Jan/Feb/Mar
21.1

Improved efficiency: Pause and resume imaging jobs

- Users can now resume a job that failed due to the following scenarios:
  - Source drive disconnected
  - Destination drive disconnected
  - Destination drive full



Status: Failed
Reason: Source disconnected
Time Remaining: 12m 45s

Duplication
Errors encountered, job may take additional time
7.7 MB/s

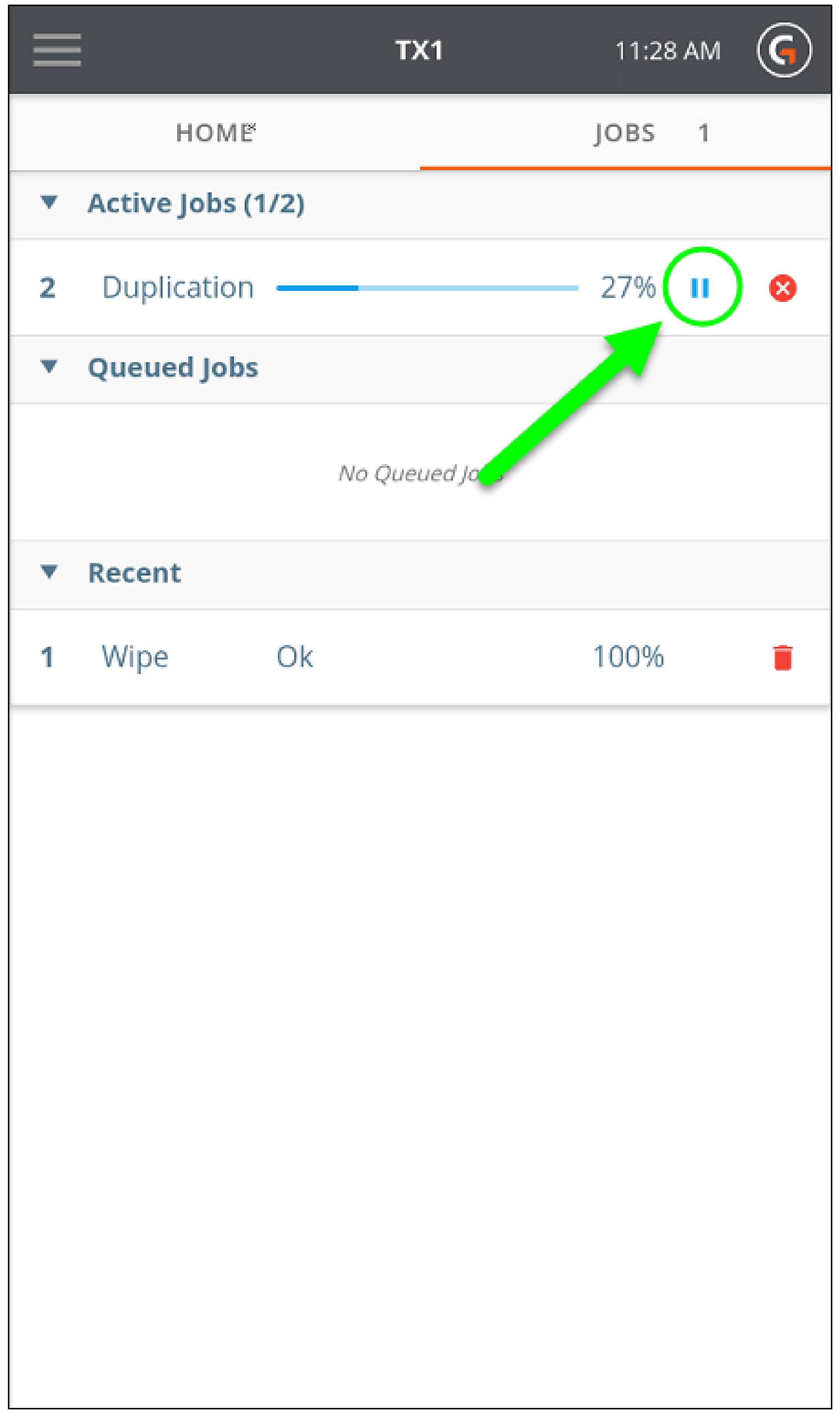
Verification(s)
USB
Waiting

Settings
Hashes: SHA1, MD5
Verify: Yes
File Type: Ex01
Compression: Compressed
File Size: 2.0 GB

Source
Drive is no longer connected
SATA/SAS 2
Model: MAX3036RC
Size: 36.7 GB

Pause & Resume

- Pause and resume any imaging job (E01, Ex01, DD, DMG), even across power-cycles



TX1 11:28 AM

HOME JOBS 1

▼ Active Jobs (1/2)

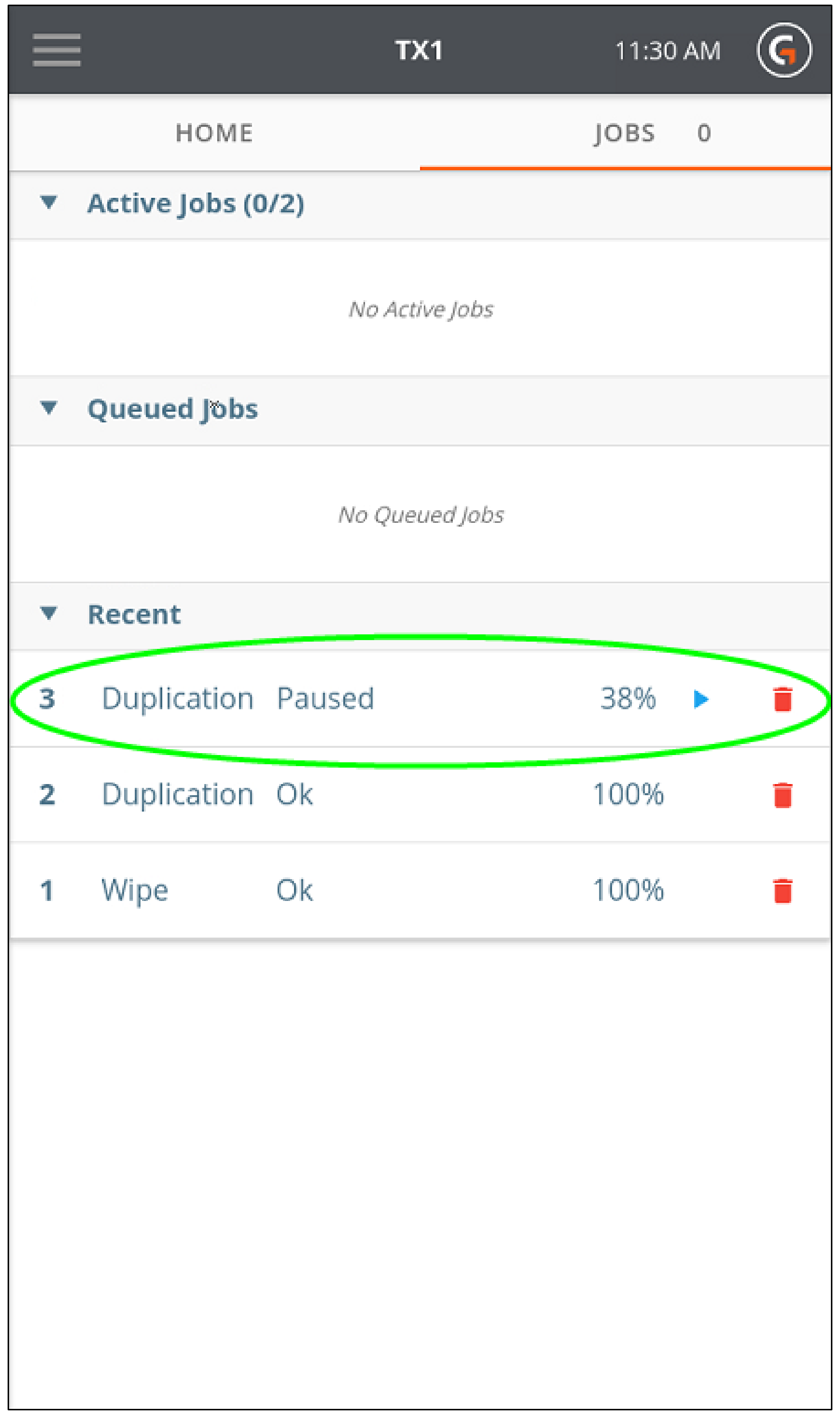
2 Duplication 27%

▼ Queued Jobs

No Queued Jobs

▼ Recent

1 Wipe Ok 100%



TX1 11:30 AM

HOME JOBS 0

▼ Active Jobs (0/2)

No Active Jobs

▼ Queued Jobs

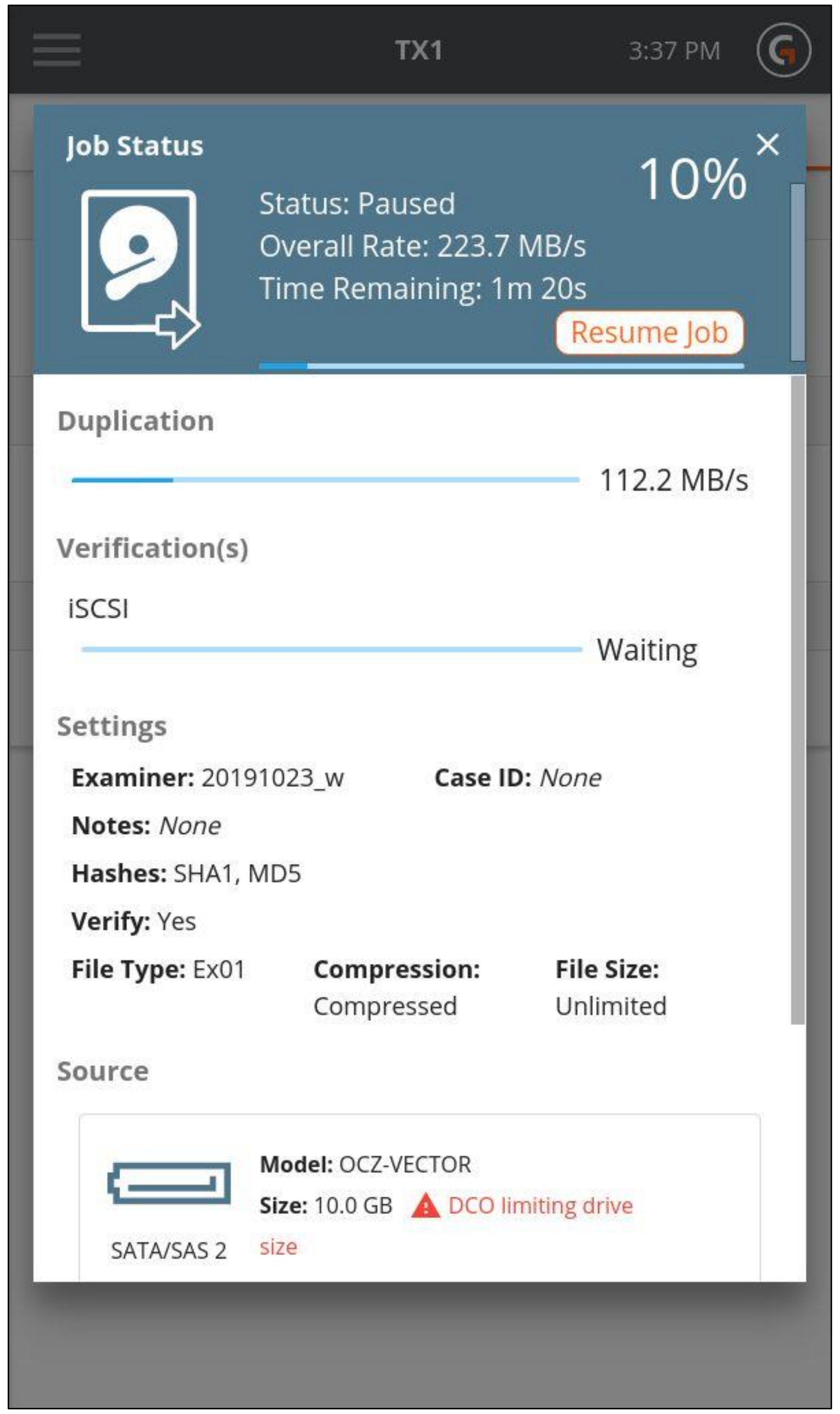
No Queued Jobs

▼ Recent

3 Duplication Paused 38% ▶

2 Duplication Ok 100%

1 Wipe Ok 100%



TX1 3:37 PM

Job Status 10%

Status: Paused
Overall Rate: 223.7 MB/s
Time Remaining: 1m 20s

Resume Job

Duplication

112.2 MB/s

Verification(s)

iSCSI

Waiting

Settings

Examiner: 20191023_w **Case ID:** *None*

Notes: *None*

Hashes: SHA1, MD5

Verify: Yes

File Type: Ex01 **Compression:** Compressed **File Size:** Unlimited

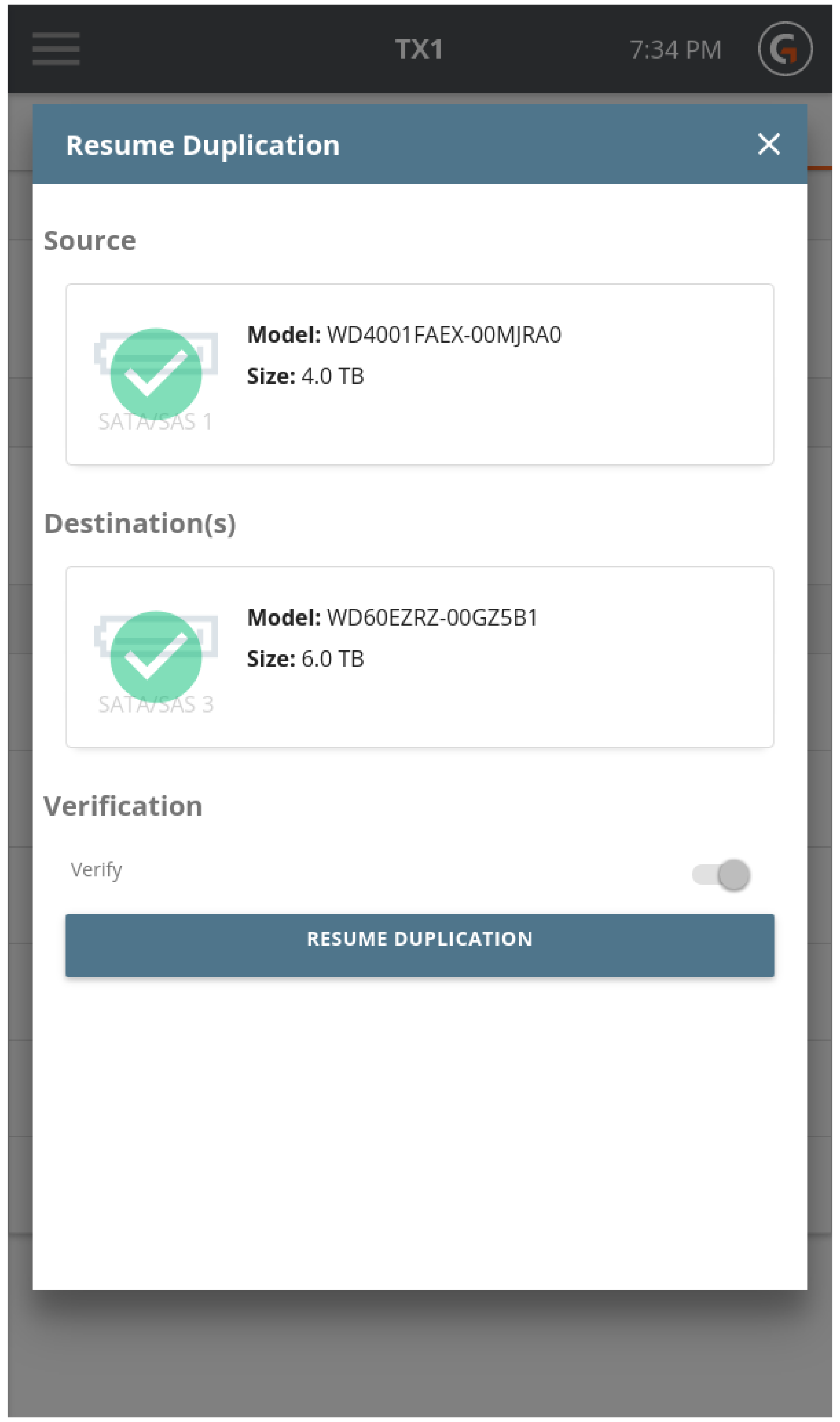
Source

SATA/SAS 2

Model: OCZ-VECTOR
Size: 10.0 GB ⚠ DCO limiting drive size

Pause & Resume – User action

- TX1 checks source/destination media is correct before allowing the job to resume
- The Log Details document when a job has been paused and resumed



Source

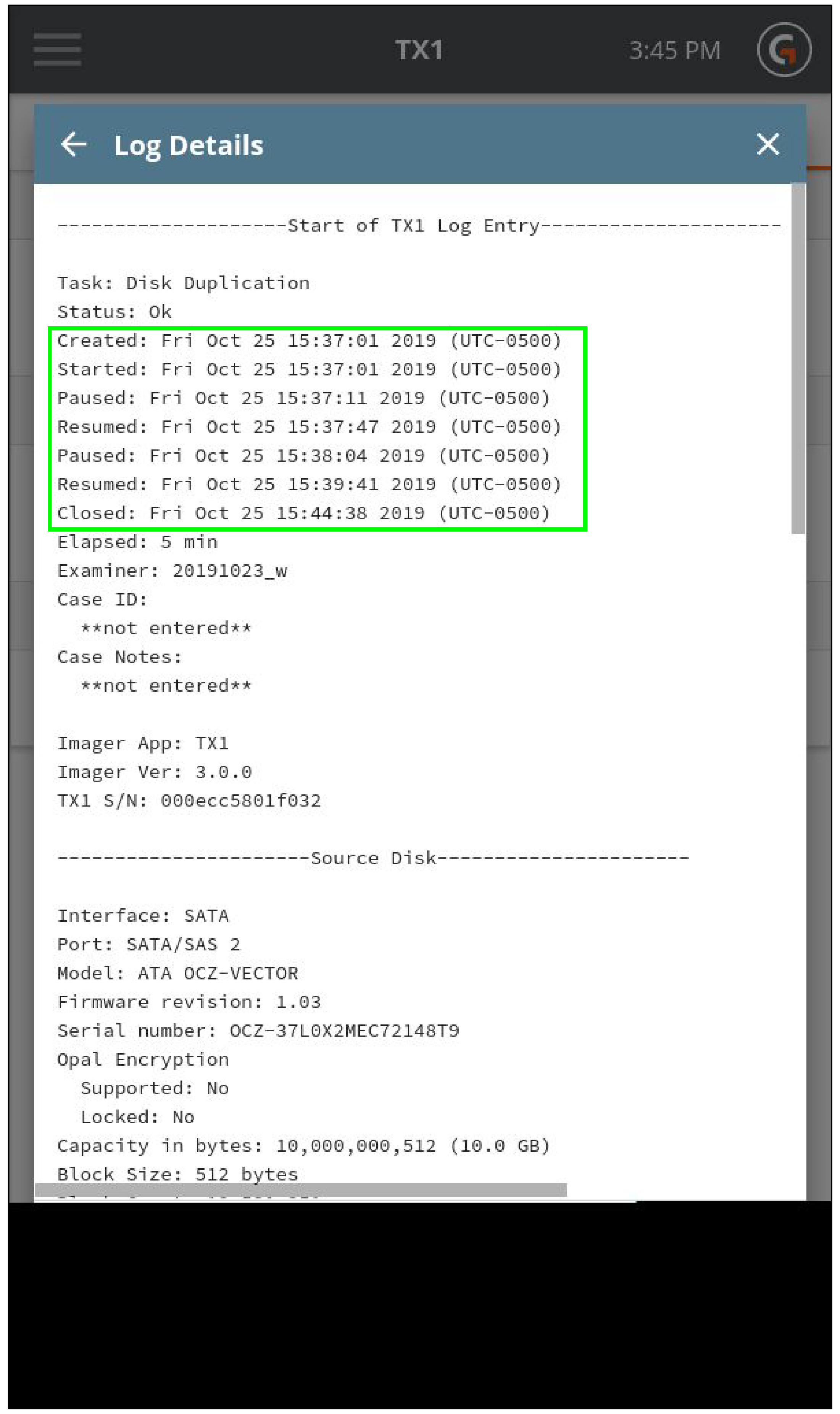
Model: WD4001FAEX-00MJRA0
Size: 4.0 TB

Destination(s)

Model: WD60EZRZ-00GZ5B1
Size: 6.0 TB

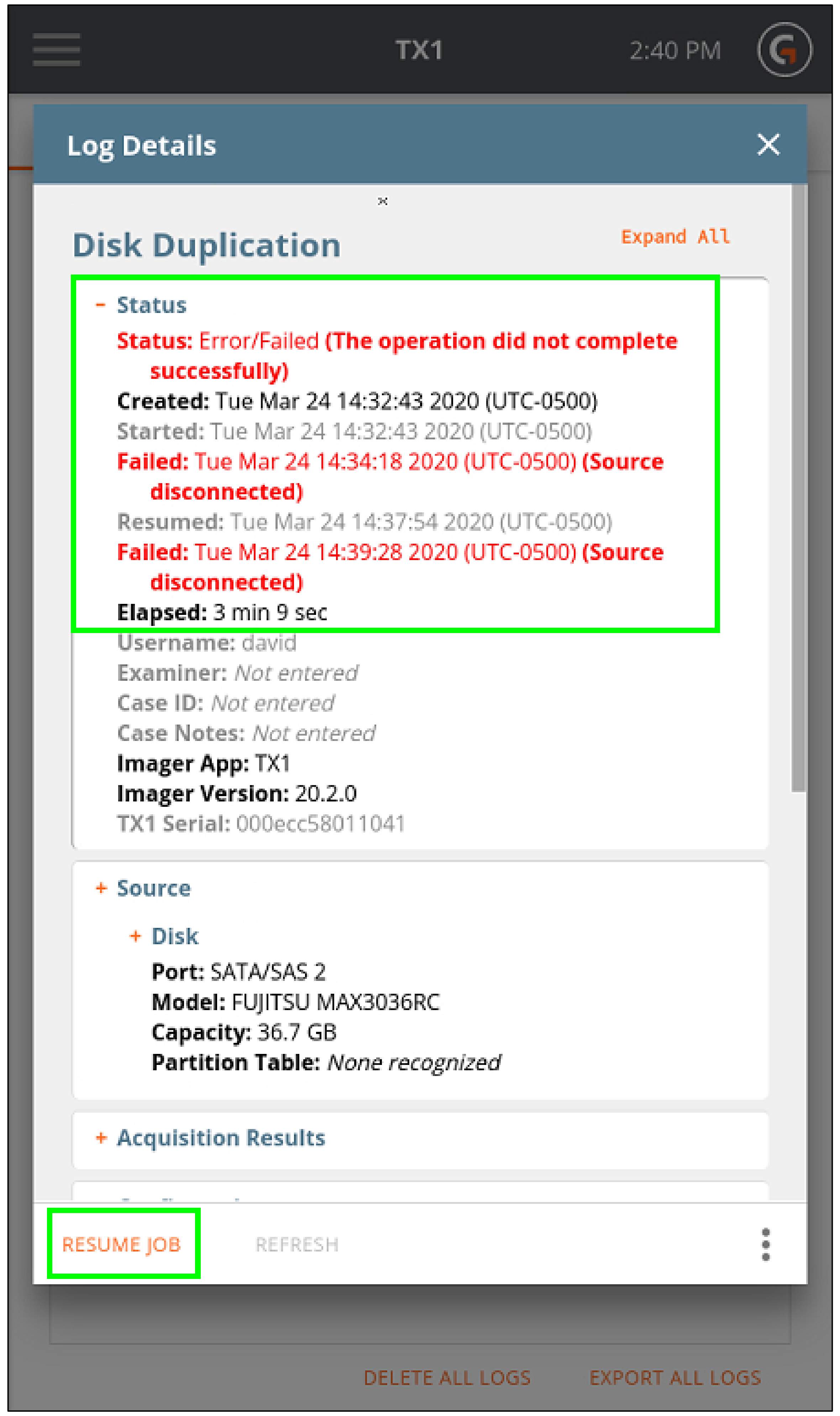
Verification

Verify



```
--------------------Start of TX1 Log Entry---------------------

Task: Disk Duplication
Status: Ok
Created: Fri Oct 25 15:37:01 2019 (UTC-0500)
Started: Fri Oct 25 15:37:01 2019 (UTC-0500)
Paused: Fri Oct 25 15:37:11 2019 (UTC-0500)
Resumed: Fri Oct 25 15:37:47 2019 (UTC-0500)
Paused: Fri Oct 25 15:38:04 2019 (UTC-0500)
Resumed: Fri Oct 25 15:39:41 2019 (UTC-0500)
Closed: Fri Oct 25 15:44:38 2019 (UTC-0500)
Elapsed: 5 min
Examiner: 20191023_w
Case ID:
  **not entered**
Case Notes:
  **not entered**

Imager App: TX1
Imager Ver: 3.0.0
TX1 S/N: 000ecc5801f032

---------------------Source Disk---------------------

Interface: SATA
Port: SATA/SAS 2
Model: ATA OCZ-VECTOR
Firmware revision: 1.03
Serial number: OCZ-37L0X2MEC72148T9
Opal Encryption
  Supported: No
  Locked: No
Capacity in bytes: 10,000,000,512 (10.0 GB)
Block Size: 512 bytes
```

Pause & Resume with Drive Interruption / Failure



Disk Duplication

- Status

Status: Error/Failed **(The operation did not complete successfully)**
Created: Tue Mar 24 14:32:43 2020 (UTC-0500)
Started: Tue Mar 24 14:32:43 2020 (UTC-0500)
Failed: Tue Mar 24 14:34:18 2020 (UTC-0500) **(Source disconnected)**
Resumed: Tue Mar 24 14:37:54 2020 (UTC-0500)
Failed: Tue Mar 24 14:39:28 2020 (UTC-0500) **(Source disconnected)**
Elapsed: 3 min 9 sec
Username: david
Examiner: *Not entered*
Case ID: *Not entered*
Case Notes: *Not entered*
Imager App: TX1
Imager Version: 20.2.0
TX1 Serial: 000ecc58011041

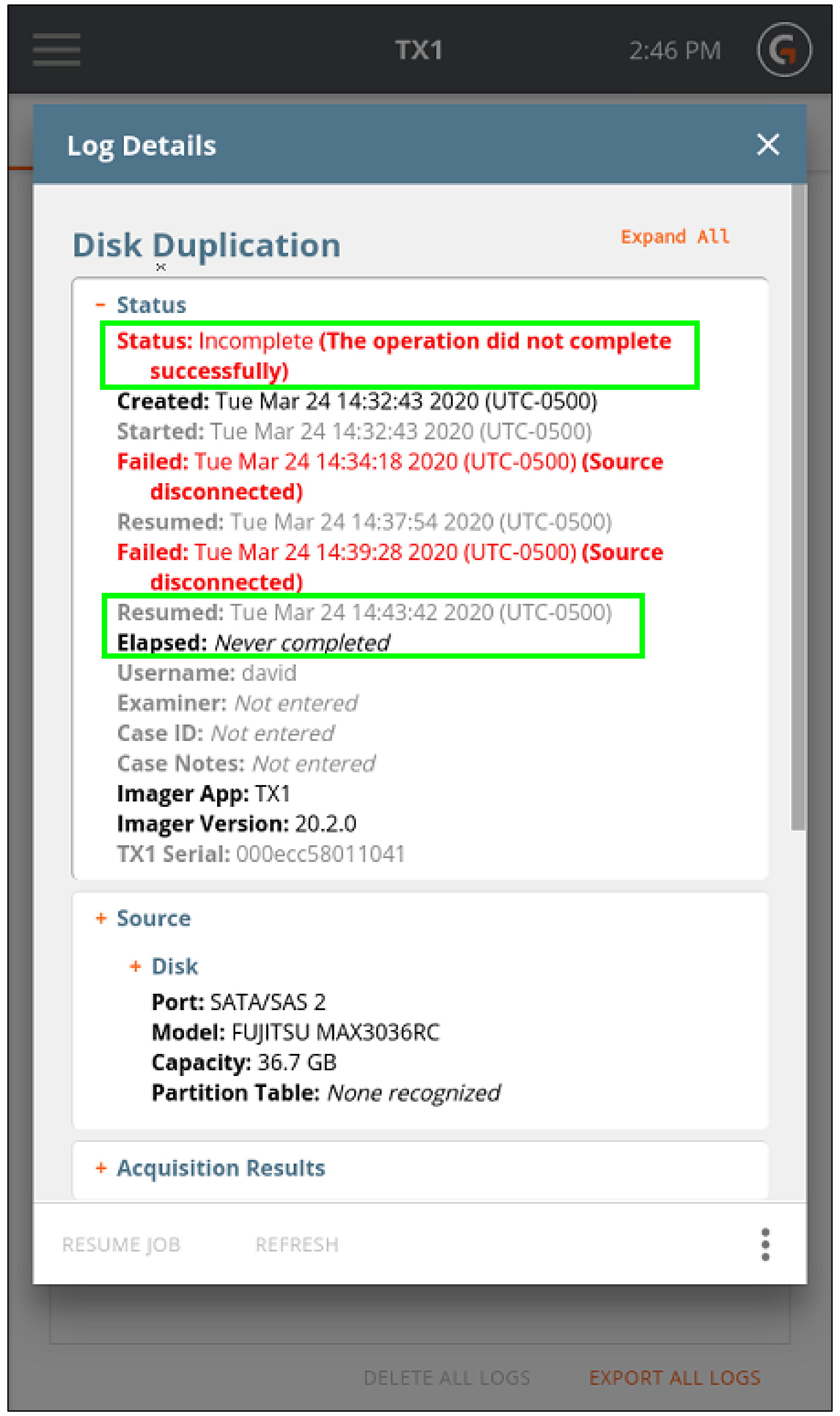
+ Source

+ Disk

Port: SATA/SAS 2
Model: FUJITSU MAX3036RC
Capacity: 36.7 GB
Partition Table: *None recognized*

+ Acquisition Results

Log when job fails



Disk Duplication

- Status

Status: Incomplete **(The operation did not complete successfully)**
Created: Tue Mar 24 14:32:43 2020 (UTC-0500)
Started: Tue Mar 24 14:32:43 2020 (UTC-0500)
Failed: Tue Mar 24 14:34:18 2020 (UTC-0500) **(Source disconnected)**
Resumed: Tue Mar 24 14:37:54 2020 (UTC-0500)
Failed: Tue Mar 24 14:39:28 2020 (UTC-0500) **(Source disconnected)**
Resumed: Tue Mar 24 14:43:42 2020 (UTC-0500)
Elapsed: *Never completed*
Username: david
Examiner: *Not entered*
Case ID: *Not entered*
Case Notes: *Not entered*
Imager App: TX1
Imager Version: 20.2.0
TX1 Serial: 000ecc58011041

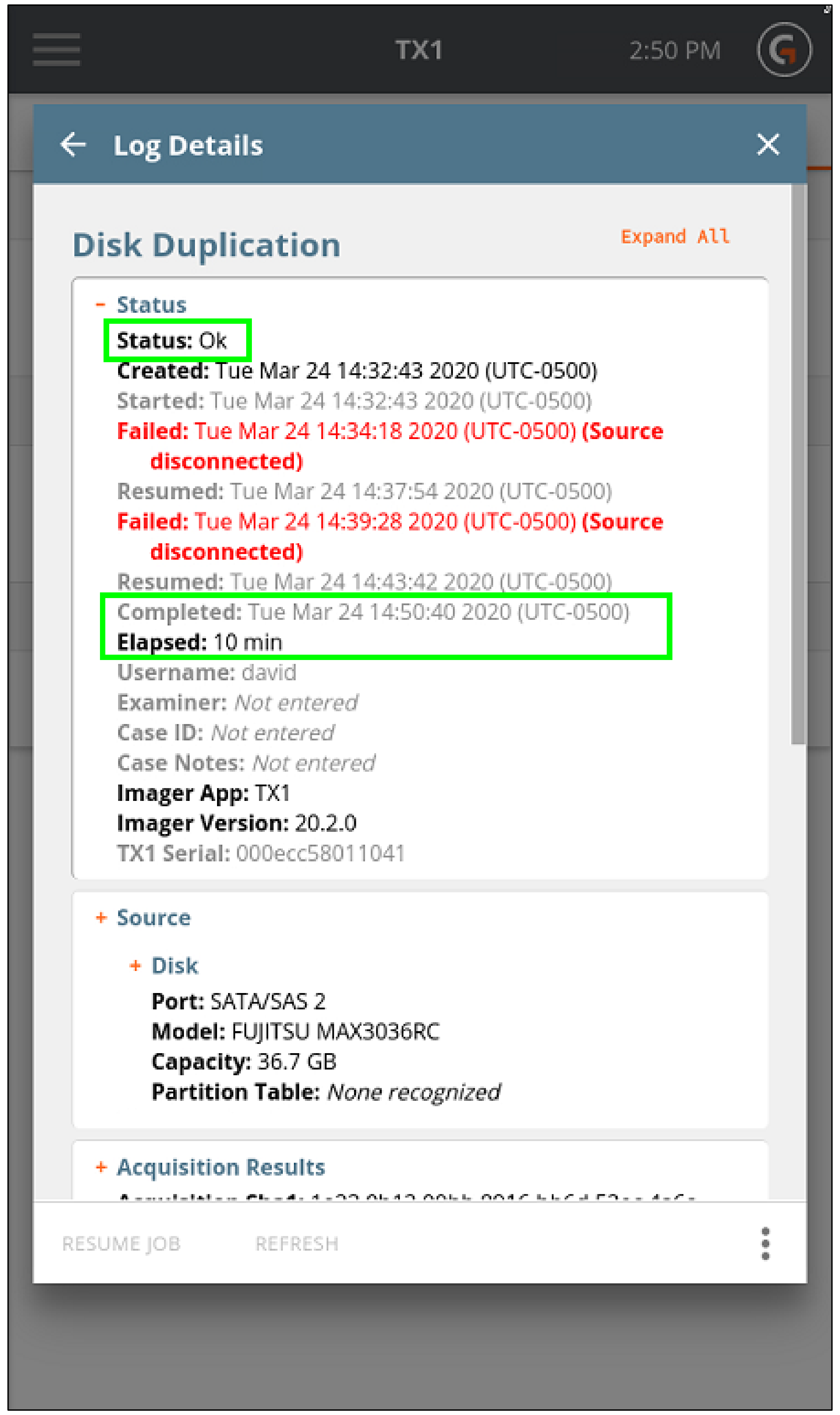
+ Source

+ Disk

Port: SATA/SAS 2
Model: FUJITSU MAX3036RC
Capacity: 36.7 GB
Partition Table: *None recognized*

+ Acquisition Results

Log when failed job is resumed but still in progress



Disk Duplication

- Status

Status: Ok
Created: Tue Mar 24 14:32:43 2020 (UTC-0500)
Started: Tue Mar 24 14:32:43 2020 (UTC-0500)
Failed: Tue Mar 24 14:34:18 2020 (UTC-0500) **(Source disconnected)**
Resumed: Tue Mar 24 14:37:54 2020 (UTC-0500)
Failed: Tue Mar 24 14:39:28 2020 (UTC-0500) **(Source disconnected)**
Resumed: Tue Mar 24 14:43:42 2020 (UTC-0500)
Completed: Tue Mar 24 14:50:40 2020 (UTC-0500)
Elapsed: 10 min
Username: david
Examiner: *Not entered*
Case ID: *Not entered*
Case Notes: *Not entered*
Imager App: TX1
Imager Version: 20.2.0
TX1 Serial: 000ecc58011041

+ Source

+ Disk

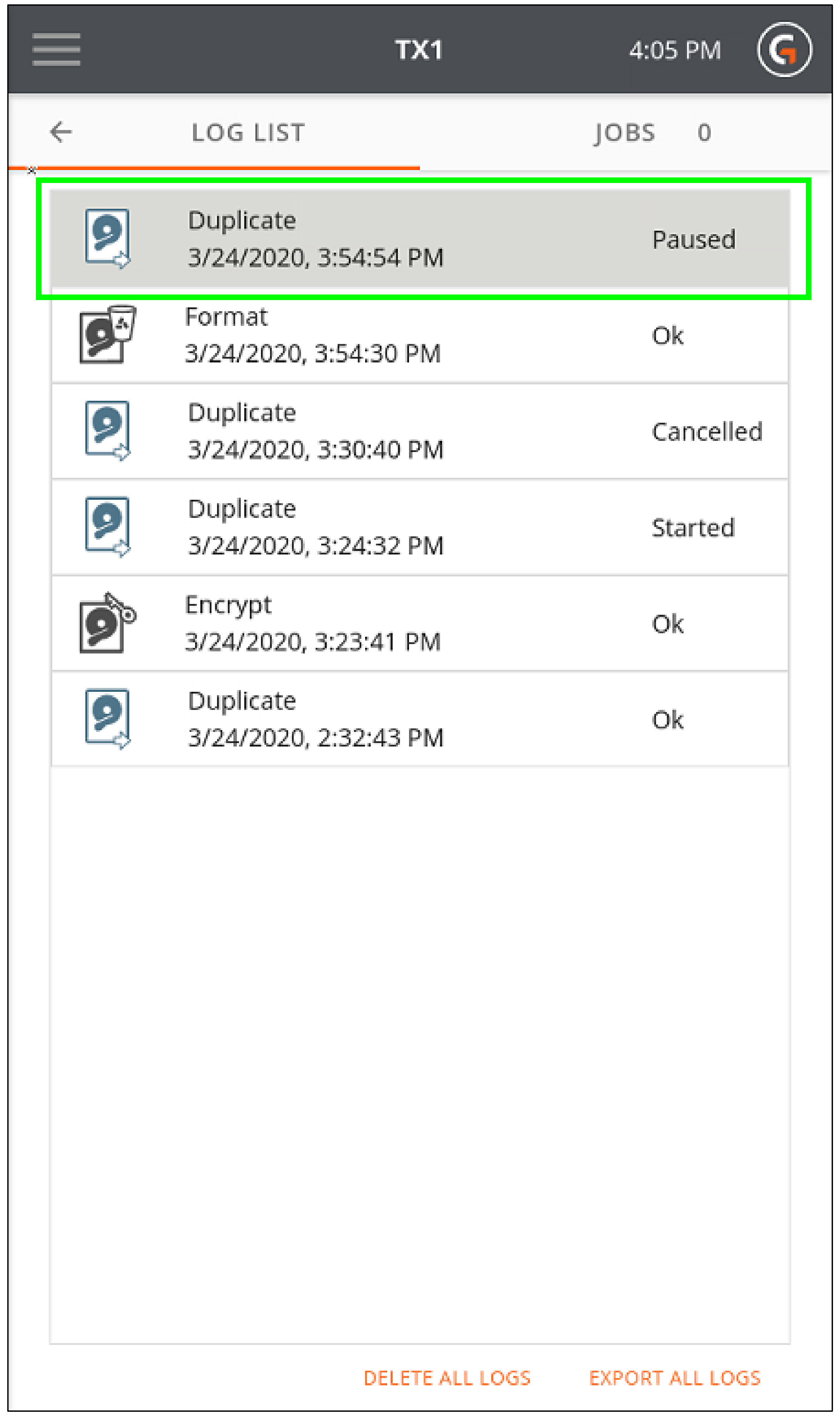
Port: SATA/SAS 2
Model: FUJITSU MAX3036RC
Capacity: 36.7 GB
Partition Table: *None recognized*

+ Acquisition Results

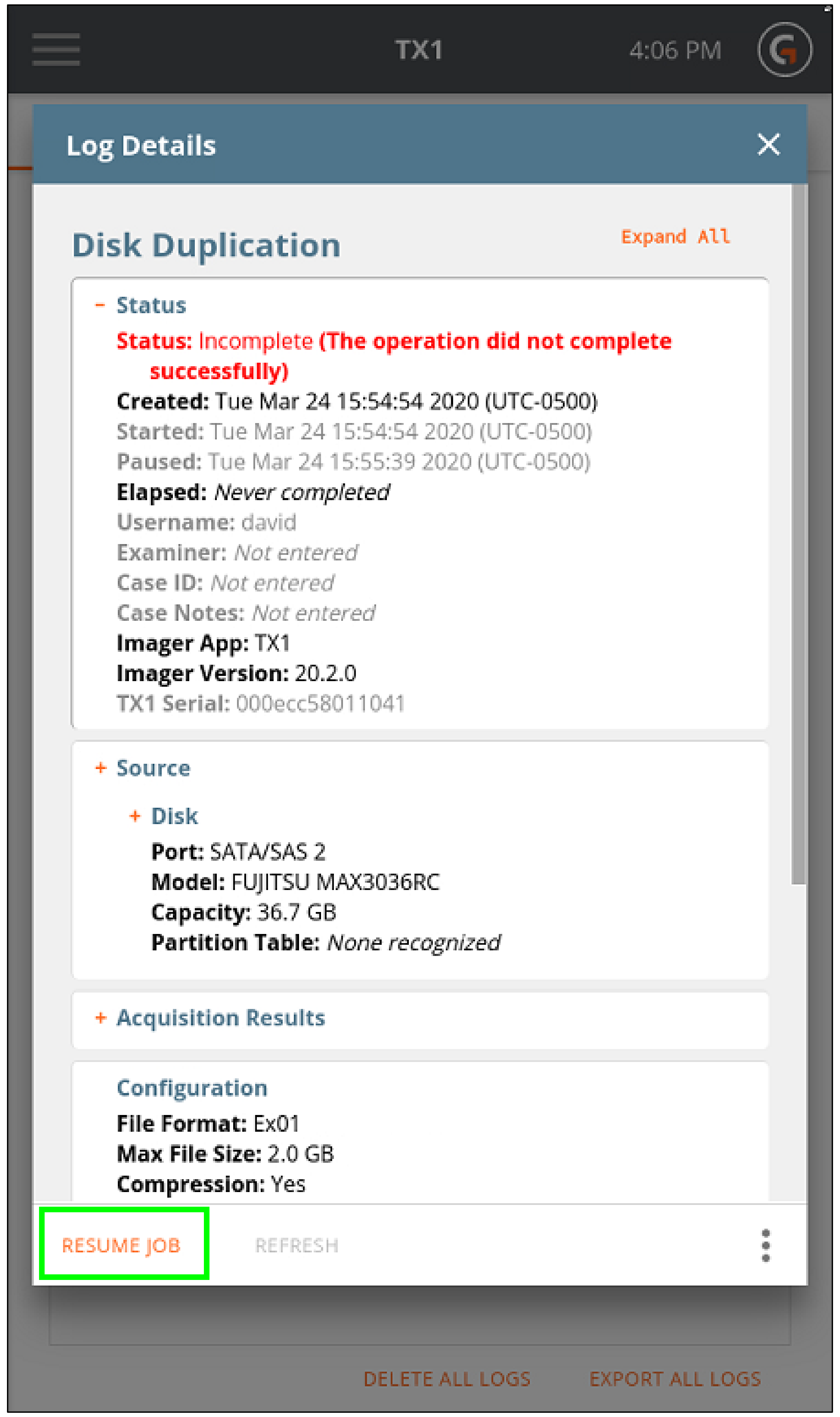
Log when failed job is resumed and completed successfully

opentext™

Inform About Locked Tableau Encryption in Resume Duplication Modal



Duplicate 3/24/2020, 3:54:54 PM	Paused
Format 3/24/2020, 3:54:30 PM	Ok
Duplicate 3/24/2020, 3:30:40 PM	Cancelled
Duplicate 3/24/2020, 3:24:32 PM	Started
Encrypt 3/24/2020, 3:23:41 PM	Ok
Duplicate 3/24/2020, 2:32:43 PM	Ok



Disk Duplication

- Status

Status: Incomplete **(The operation did not complete successfully)**
Created: Tue Mar 24 15:54:54 2020 (UTC-0500)
Started: Tue Mar 24 15:54:54 2020 (UTC-0500)
Paused: Tue Mar 24 15:55:39 2020 (UTC-0500)
Elapsed: *Never completed*
Username: david
Examiner: *Not entered*
Case ID: *Not entered*
Case Notes: *Not entered*
Imager App: TX1
Imager Version: 20.2.0
TX1 Serial: 000ecc58011041

+ Source

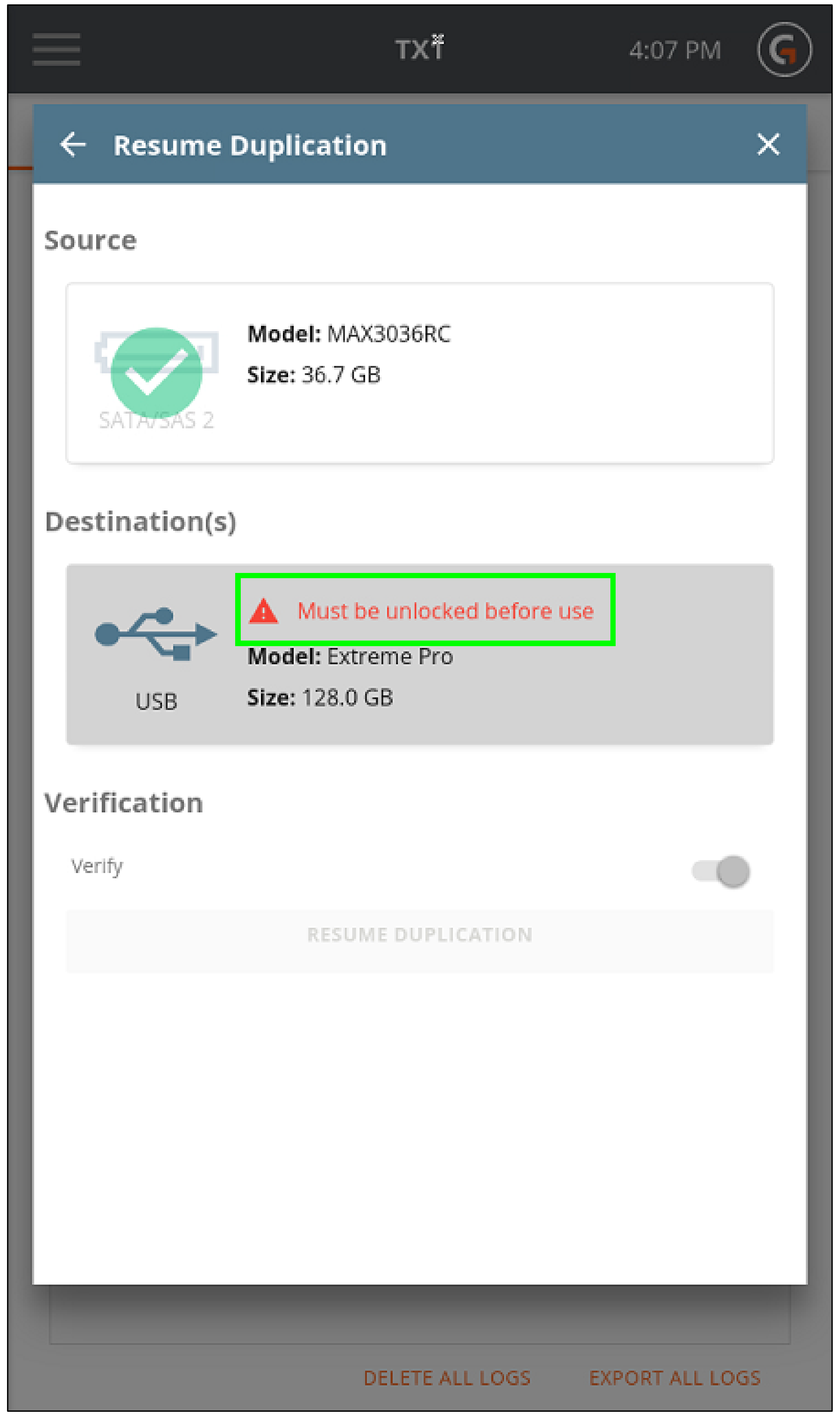
+ Disk

Port: SATA/SAS 2
Model: FUJITSU MAX3036RC
Capacity: 36.7 GB
Partition Table: *None recognized*

+ Acquisition Results

Configuration

File Format: Ex01
Max File Size: 2.0 GB
Compression: Yes



Source

SATA/SAS 2
Model: MAX3036RC
Size: 36.7 GB

Destination(s)

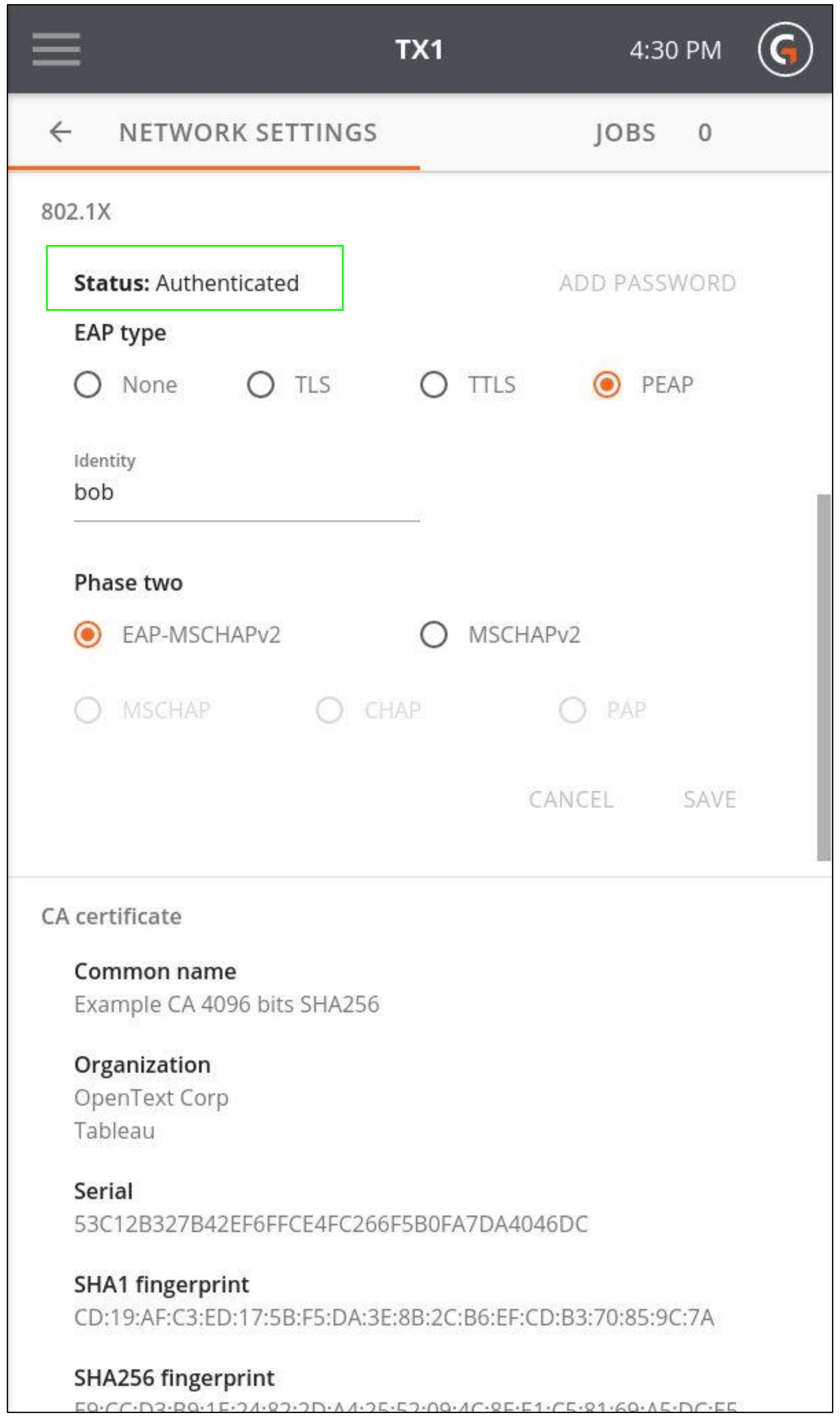
USB
⚠ Must be unlocked before use
Model: Extreme Pro
Size: 128.0 GB

Verification

Verify

Remote Access: 802.1X Authentication

- TX1 can now be connected to networks locked down with 802.1X Network Access Control policies
  - 802.1X provides port-based Network Access Control options
  - 802.1X networks typically consist of an authentication server (RADIUS), an authenticator (LAN switch) and supplicants (network client devices)
  - Required by some forensic labs, government agencies and corporations



802.1X

Status: Authenticated

EAP type

○ None ○ TLS ○ TTLS ● PEAP

Identity
bob

Phase two

● EAP-MSCHAPv2 ○ MSCHAPv2

○ MSCHAP ○ CHAP ○ PAP

CA certificate

Common name
Example CA 4096 bits SHA256

Organization
OpenText Corp
Tableau

Serial
53C12B327B42EF6FFCE4FC266F5B0FA7DA4046DC

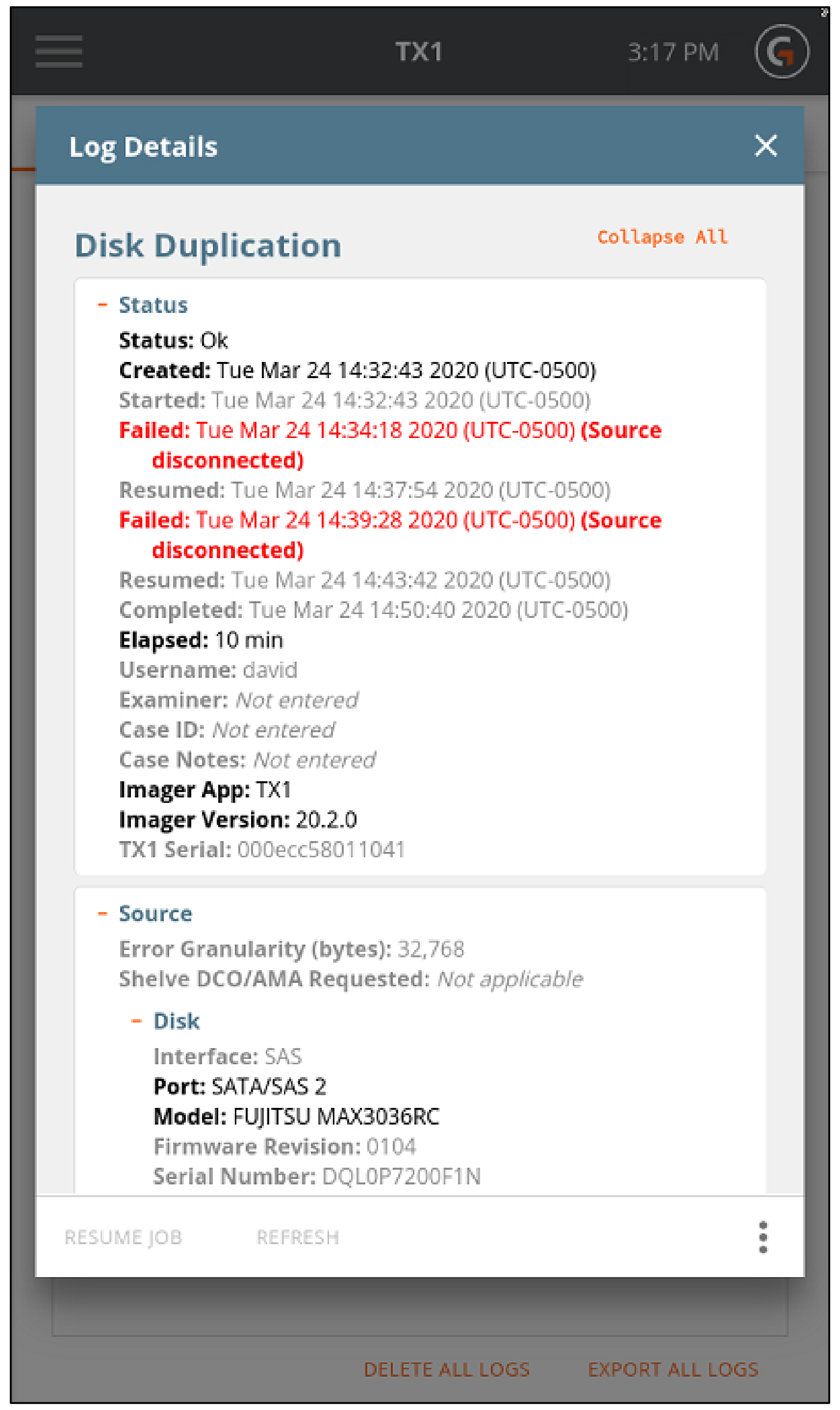
SHA1 fingerprint
CD:19:AF:C3:ED:17:5B:F5:DA:3E:8B:2C:B6:EF:CD:B3:70:85:9C:7A

SHA256 fingerprint
F9:CC:D3:B9:1F:24:82:2D:A4:25:52:09:4C:8F:F1:C5:81:69:A5:DC:F5

Improved UI

HTML Logs

- Logs can now be created in either HTML or text format

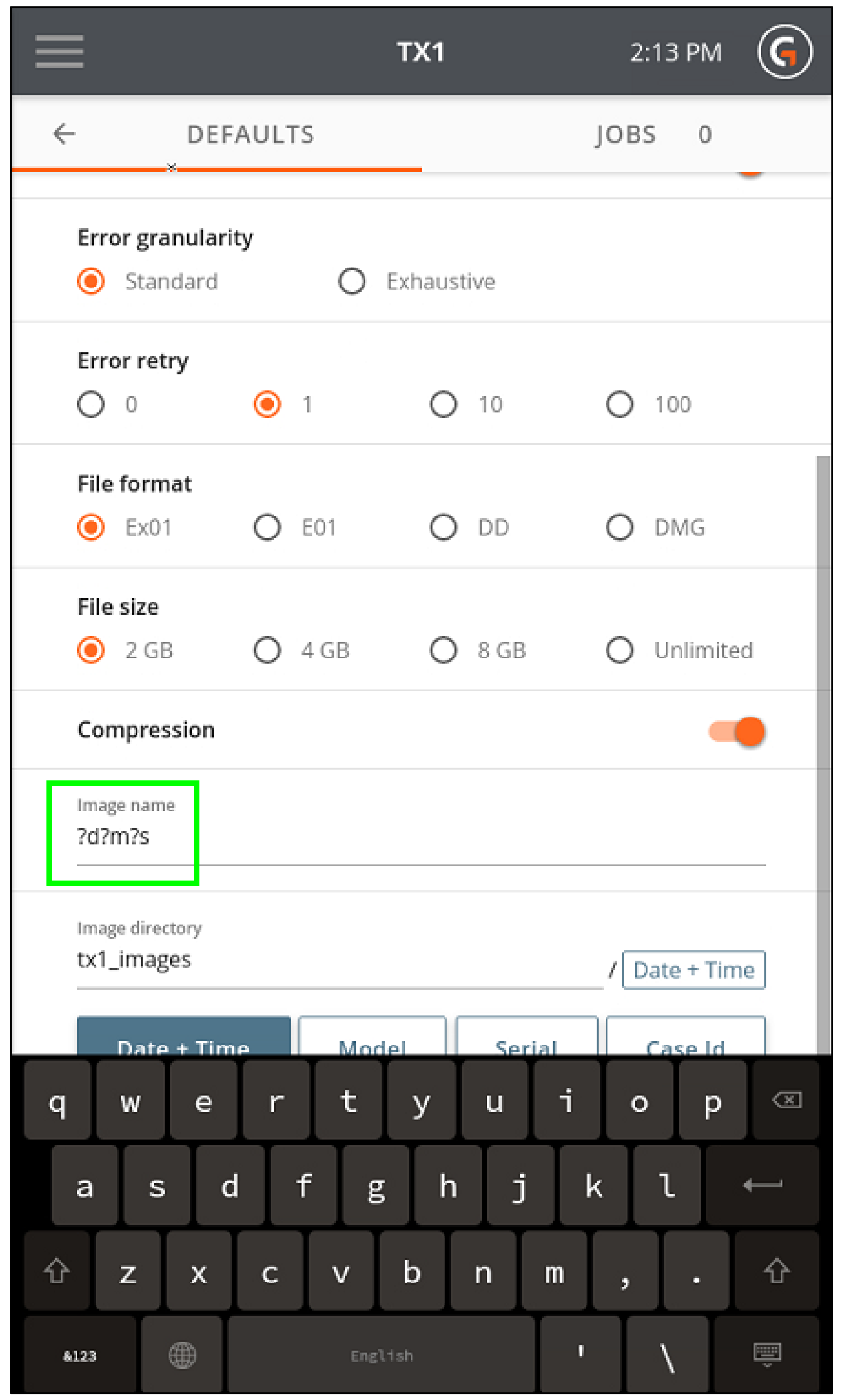


Disk Duplication

```
- Status
Status: Ok
Created: Tue Mar 24 14:32:43 2020 (UTC-0500)
Started: Tue Mar 24 14:32:43 2020 (UTC-0500)
Failed: Tue Mar 24 14:34:18 2020 (UTC-0500) (Source
    disconnected)
Resumed: Tue Mar 24 14:37:54 2020 (UTC-0500)
Failed: Tue Mar 24 14:39:28 2020 (UTC-0500) (Source
    disconnected)
Resumed: Tue Mar 24 14:43:42 2020 (UTC-0500)
Completed: Tue Mar 24 14:50:40 2020 (UTC-0500)
Elapsed: 10 min
Username: david
Examiner: Not entered
Case ID: Not entered
Case Notes: Not entered
Imager App: TX1
Imager Version: 20.2.0
TX1 Serial: 000ecc58011041

- Source
Error Granularity (bytes): 32,768
Shelve DCO/AMA Requested: Not applicable
  - Disk
  Interface: SAS
  Port: SATA/SAS 2
  Model: FUJITSU MAX3036RC
  Firmware Revision: 0104
  Serial Number: DQL0P7200F1N
```

Wildcard character input

- Allow wildcard input for the Image Name Field in TX1 Default Settings



Error granularity
● Standard ○ Exhaustive

Error retry
○ 0 ● 1 ○ 10 ○ 100

File format
● Ex01 ○ E01 ○ DD ○ DMG

File size
● 2 GB ○ 4 GB ○ 8 GB ○ Unlimited

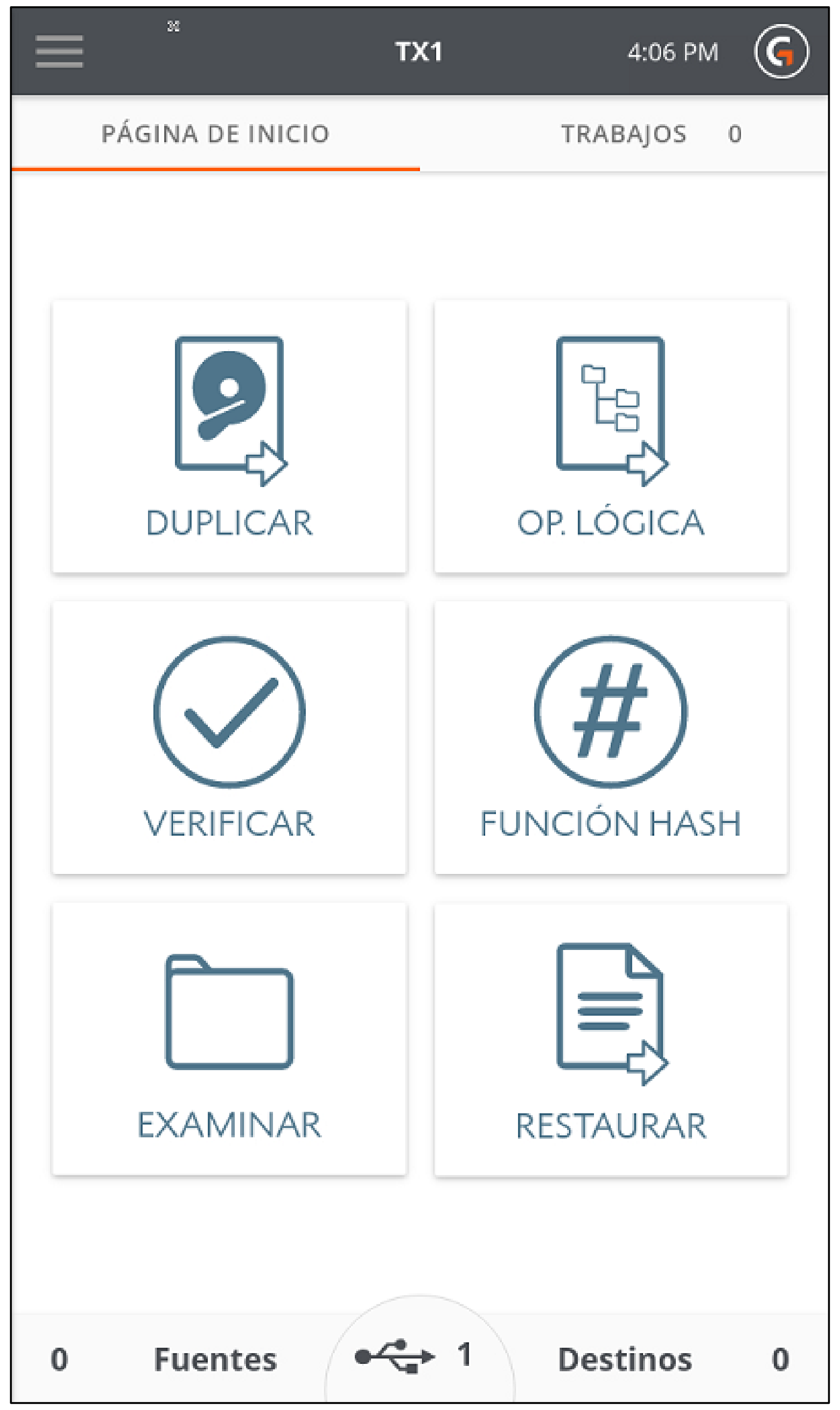
Compression

Image name
?d?m?s

Image directory
tx1_images / Date + Time

Localization updates

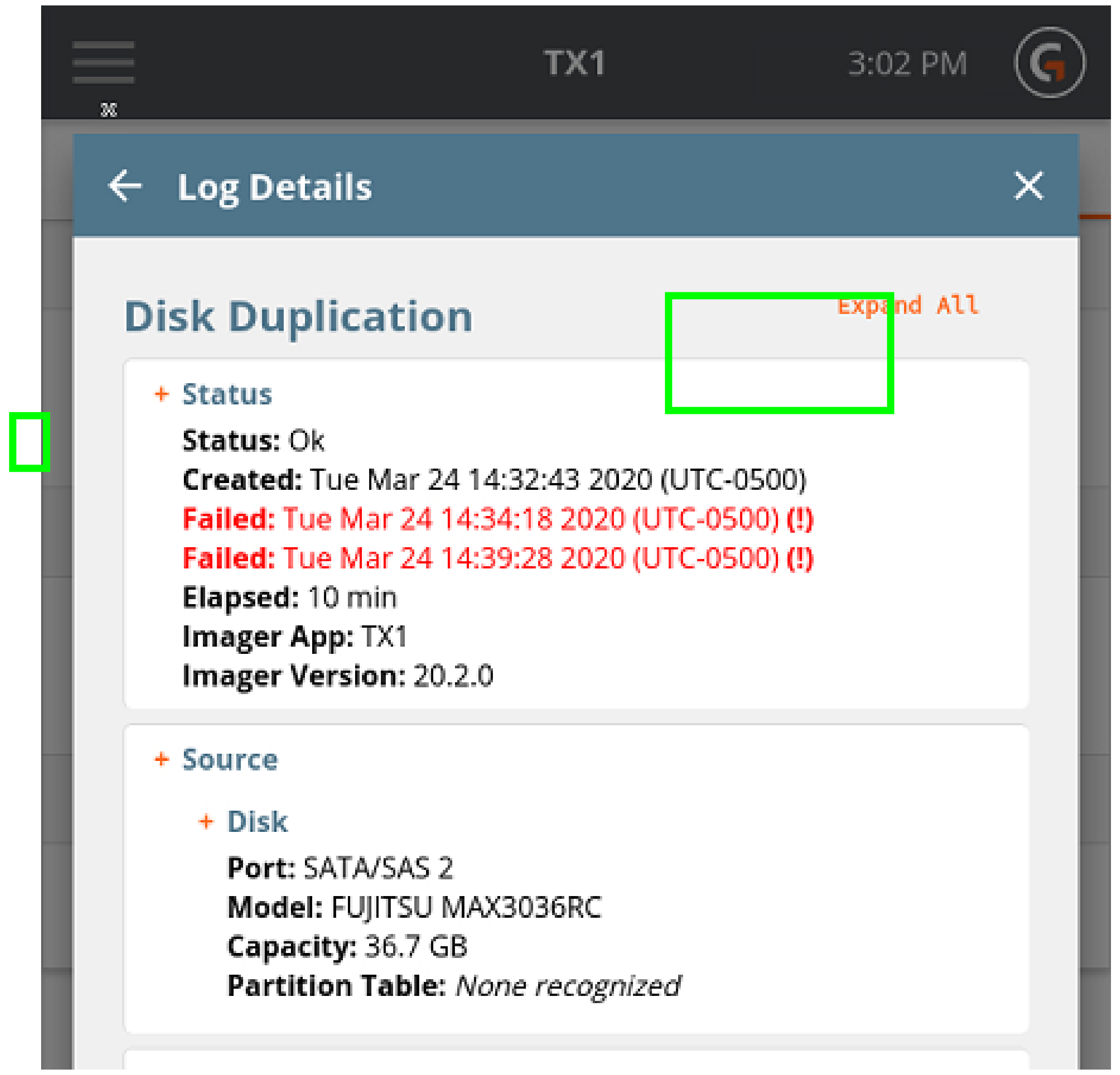
- Localization updates for the TX1 3.0 release changes



opentext™

HTML Logs

- Logs can now be created in either HTML or text format
  - ○ TX1 default is HTML logs



Disk Duplication

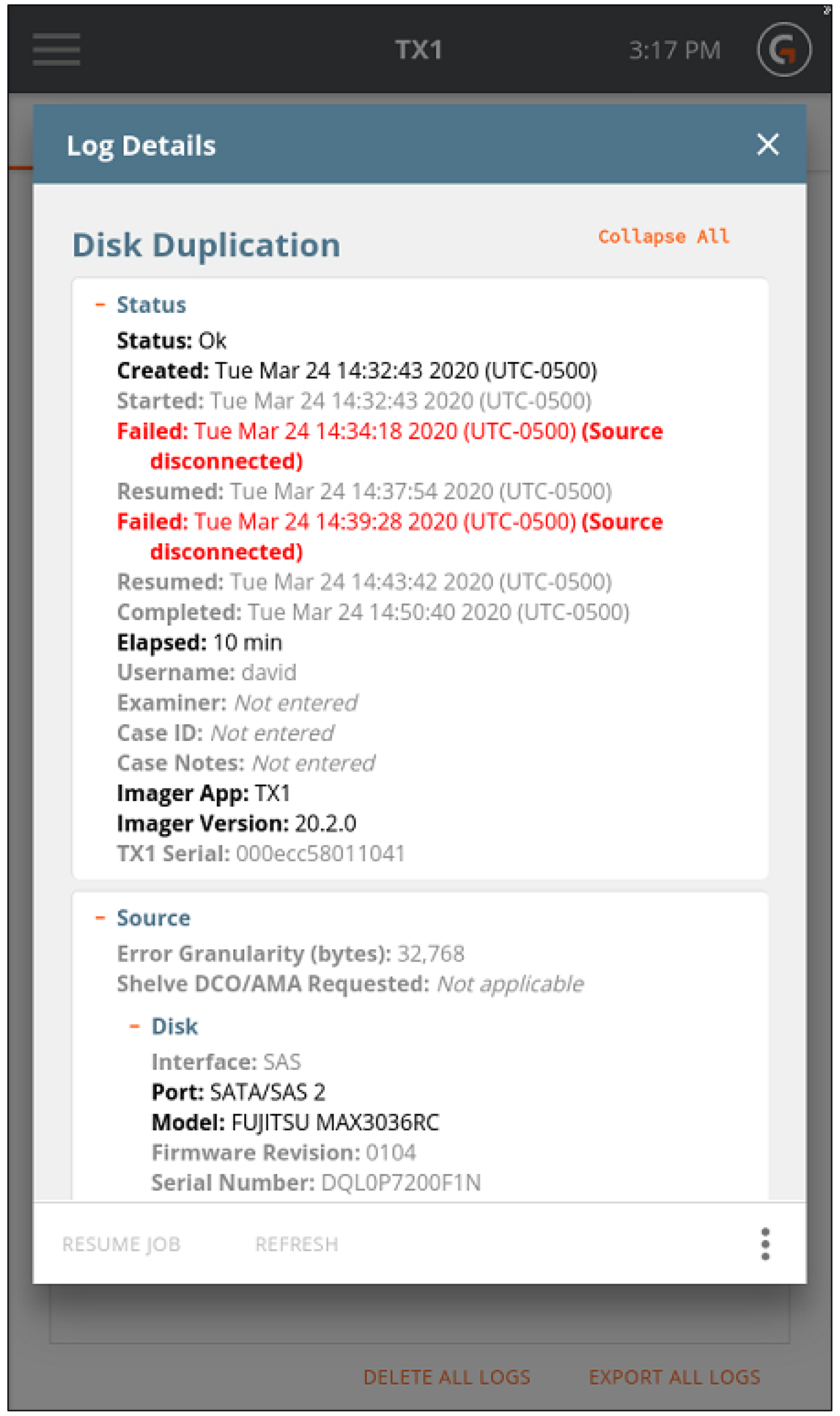
+ Status

Status: Ok
Created: Tue Mar 24 14:32:43 2020 (UTC-0500)
Failed: Tue Mar 24 14:34:18 2020 (UTC-0500) (!)
Failed: Tue Mar 24 14:39:28 2020 (UTC-0500) (!)
Elapsed: 10 min
Imager App: TX1
Imager Version: 20.2.0

+ Source

+ Disk

Port: SATA/SAS 2
Model: FUJITSU MAX3036RC
Capacity: 36.7 GB
Partition Table: *None recognized*



Disk Duplication

- Status

Status: Ok
Created: Tue Mar 24 14:32:43 2020 (UTC-0500)
Started: Tue Mar 24 14:32:43 2020 (UTC-0500)
Failed: Tue Mar 24 14:34:18 2020 (UTC-0500) **(Source disconnected)**
Resumed: Tue Mar 24 14:37:54 2020 (UTC-0500)
Failed: Tue Mar 24 14:39:28 2020 (UTC-0500) **(Source disconnected)**
Resumed: Tue Mar 24 14:43:42 2020 (UTC-0500)
Completed: Tue Mar 24 14:50:40 2020 (UTC-0500)
Elapsed: 10 min
Username: david
Examiner: *Not entered*
Case ID: *Not entered*
Case Notes: *Not entered*
Imager App: TX1
Imager Version: 20.2.0
TX1 Serial: 000ecc58011041

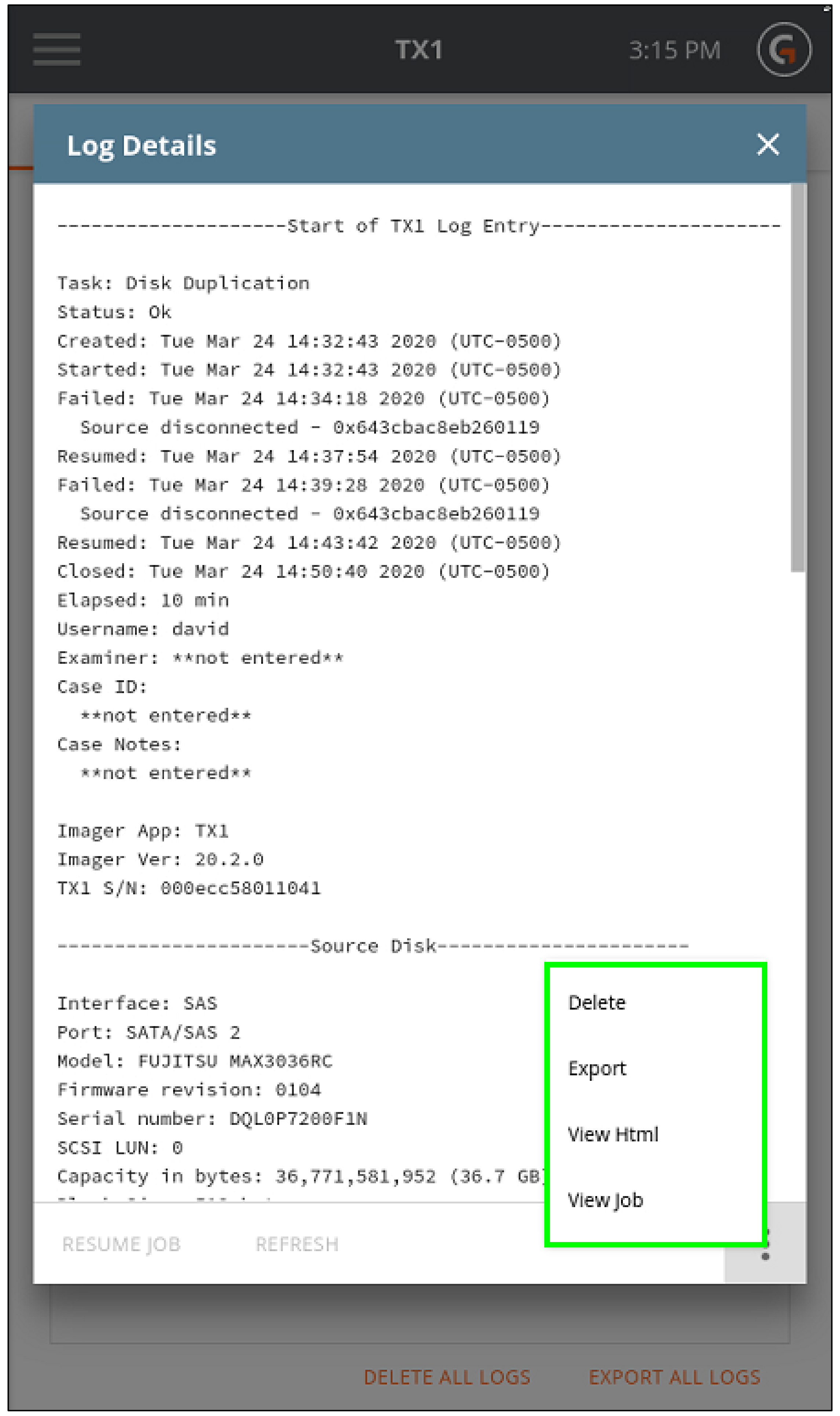
- Source

Error Granularity (bytes): 32,768
Shelve DCO/AMA Requested: *Not applicable*

- Disk

Interface: SAS
Port: SATA/SAS 2
Model: FUJITSU MAX3036RC
Firmware Revision: 0104
Serial Number: DQL0P7200F1N

HTML log

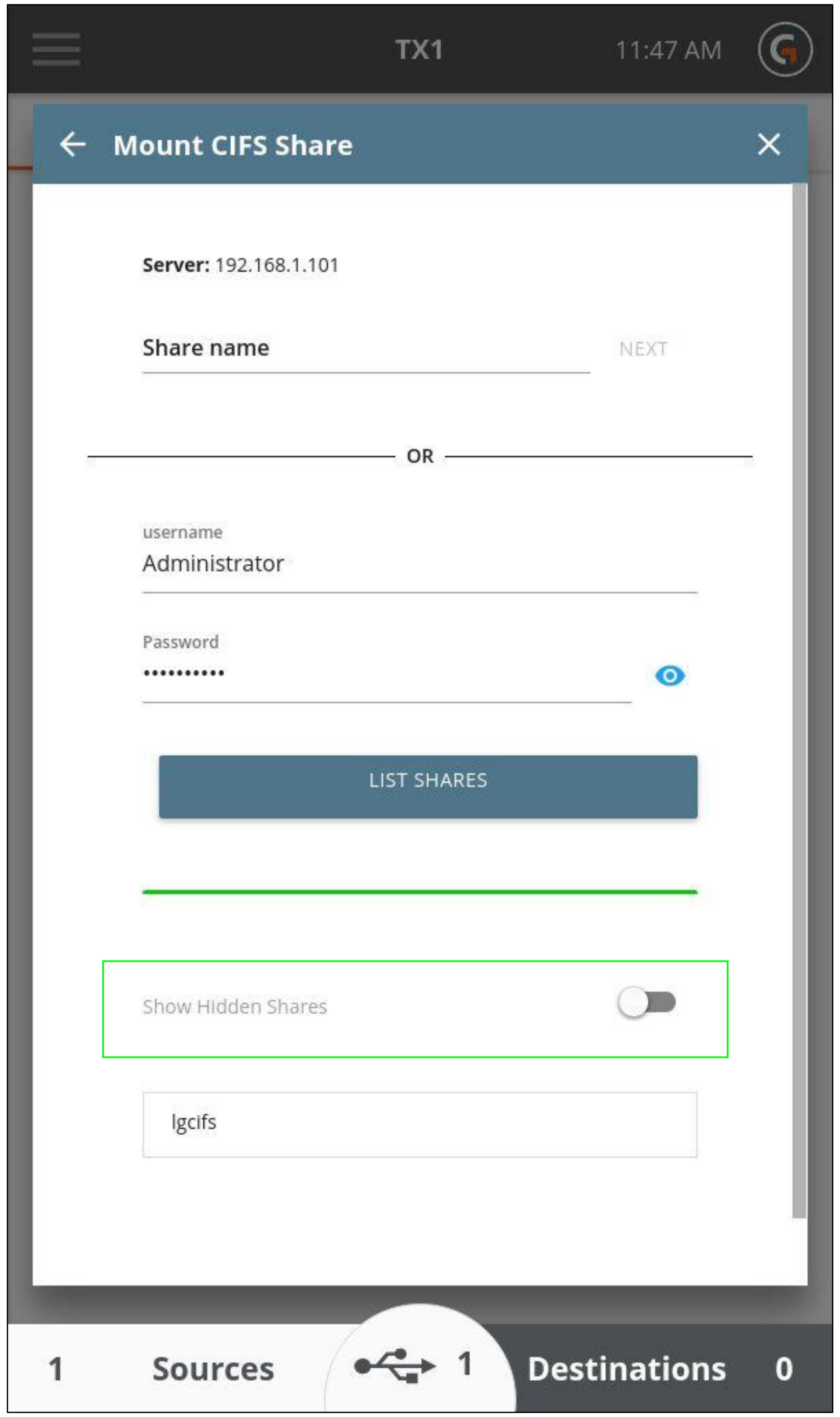


```
--------------------Start of TX1 Log Entry---------------------

Task: Disk Duplication
Status: Ok
Created: Tue Mar 24 14:32:43 2020 (UTC-0500)
Started: Tue Mar 24 14:32:43 2020 (UTC-0500)
Failed: Tue Mar 24 14:34:18 2020 (UTC-0500)
  Source disconnected - 0x643cbac8eb260119
Resumed: Tue Mar 24 14:37:54 2020 (UTC-0500)
Failed: Tue Mar 24 14:39:28 2020 (UTC-0500)
  Source disconnected - 0x643cbac8eb260119
Resumed: Tue Mar 24 14:43:42 2020 (UTC-0500)
Closed: Tue Mar 24 14:50:40 2020 (UTC-0500)
Elapsed: 10 min
Username: david
Examiner: **not entered**
Case ID:
  **not entered**
Case Notes:
  **not entered**

Imager App: TX1
Imager Ver: 20.2.0
TX1 S/N: 000ecc58011041

----------------------Source Disk----------------------

Interface: SAS
Port: SATA/SAS 2
Model: FUJITSU MAX3036RC
Firmware revision: 0104
Serial number: DQL0P7200F1N
SCSI LUN: 0
Capacity in bytes: 36,771,581,952 (36.7 GB)
```

Text log

Scan Local Network for Hosts with CIFS Shares

- When mounting a CIFS share, a user can now search the local network for hosts with configured CIFS shares
- Option to view admin/hidden shares



Server: 192.168.1.101

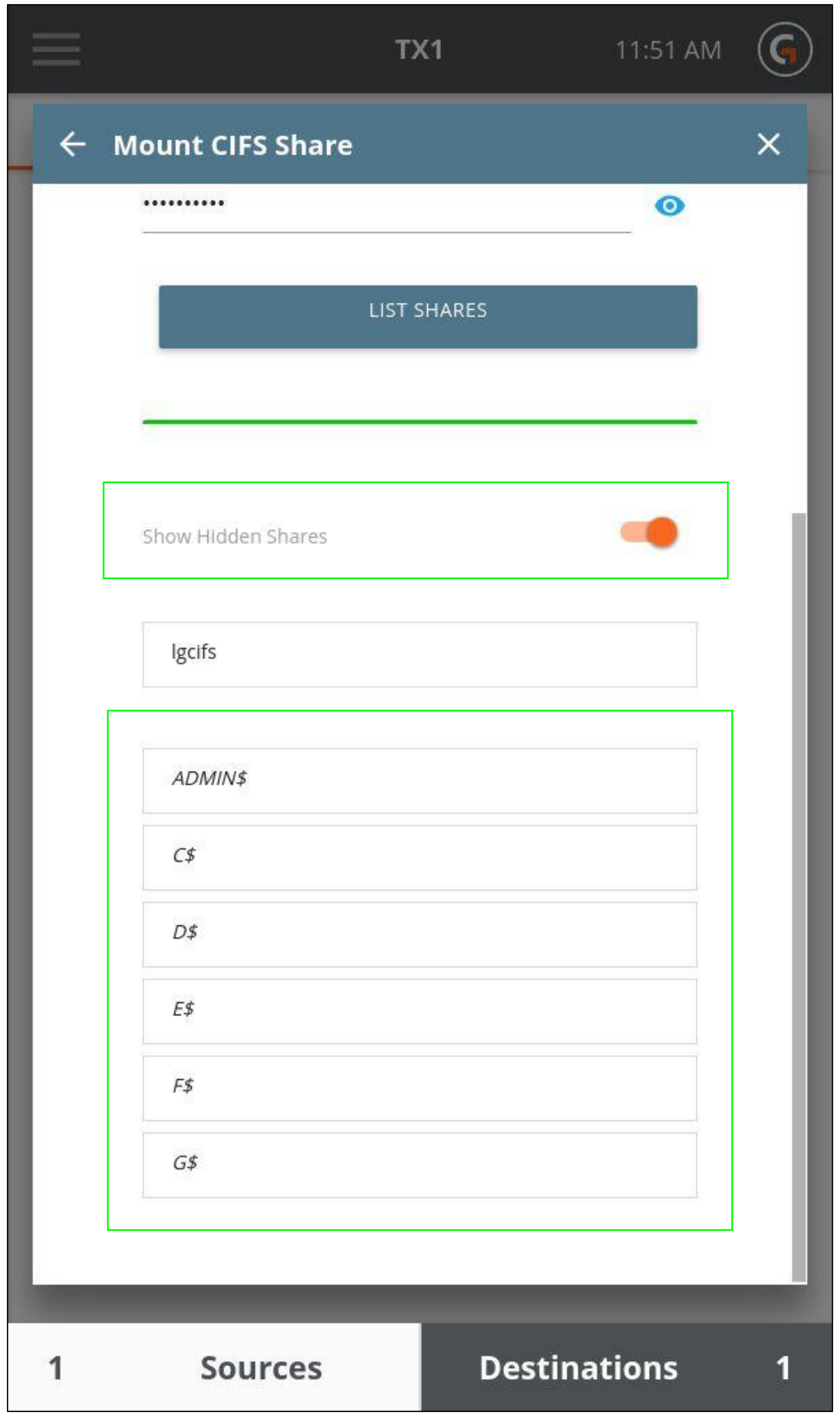
Share name

username
Administrator

Password
••••••••••

Show Hidden Shares ○

lgcifs



••••••••••

Show Hidden Shares ●

lgcifs

ADMIN$

C$

D$

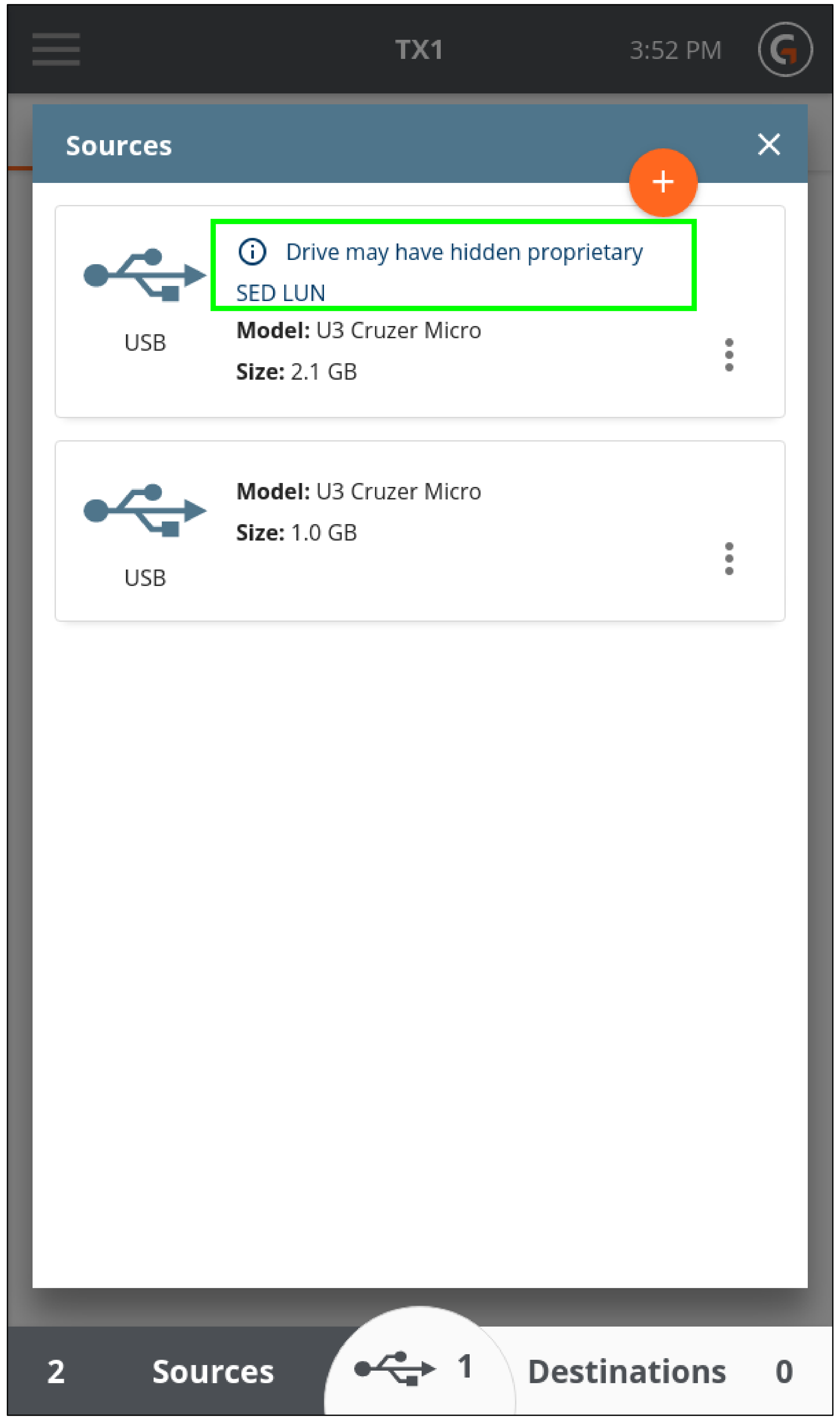
E$

F$

G$

Detect Proprietary Self-encrypting USB Drives

- Previously undetected by TX1
- TX1 now detects this to inform the user that:
  - Drive is not dead
  - Is a proprietary SED that can be unlocked with the right software
- If there is an unencrypted partition, TX1 will expose it and allow it to be imaged



Drive may have hidden proprietary SED LUN

Model: U3 Cruzer Micro

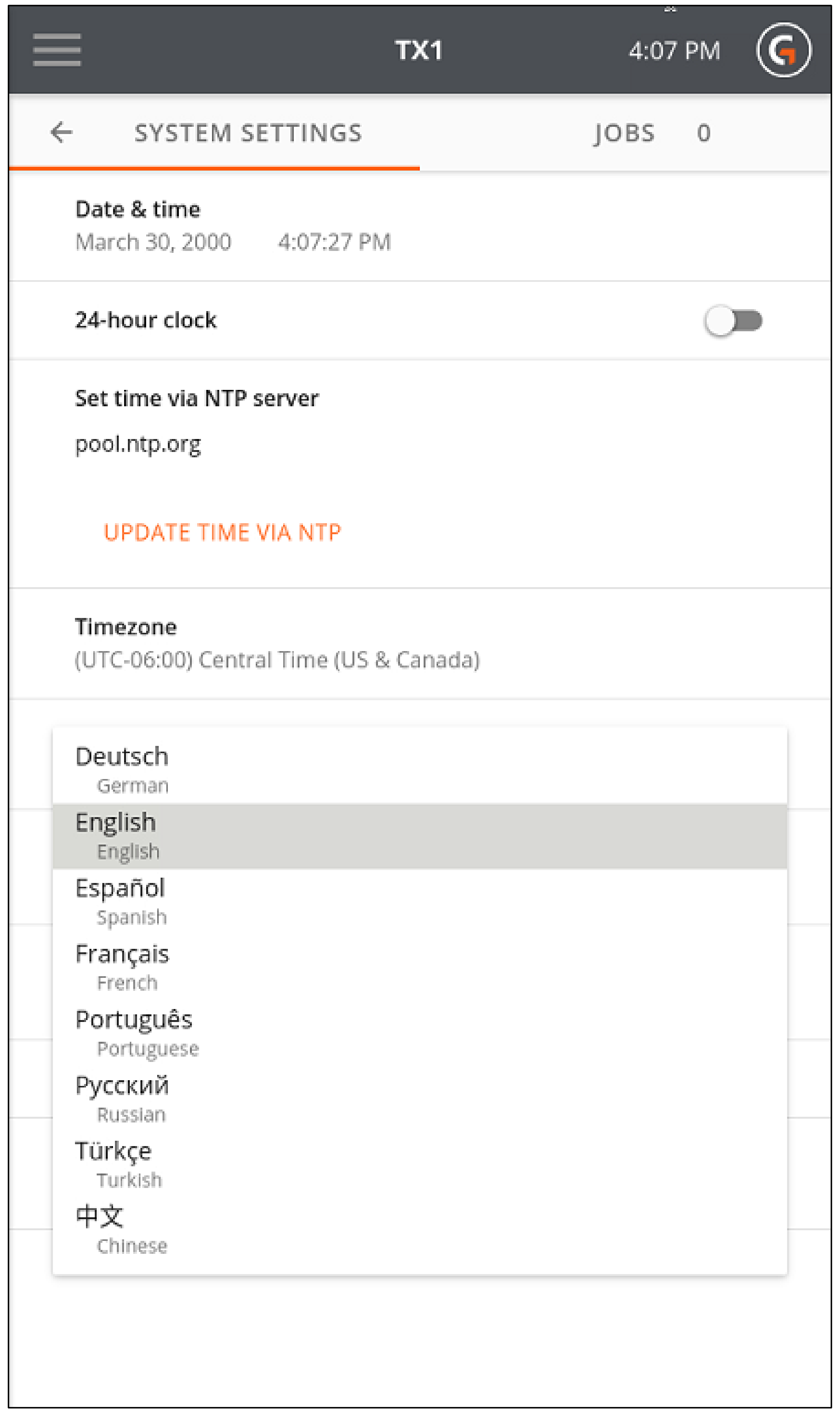
Size: 2.1 GB

Model: U3 Cruzer Micro

Size: 1.0 GB

Localization Updates

- For user-facing changes from TX1 3.0 and 20.1



TX1 4:07 PM

SYSTEM SETTINGS JOBS 0

Date & time
March 30, 2000 4:07:27 PM

24-hour clock

Set time via NTP server
pool.ntp.org

UPDATE TIME VIA NTP

Timezone
(UTC-06:00) Central Time (US & Canada)

Deutsch
German

English
English

Español
Spanish

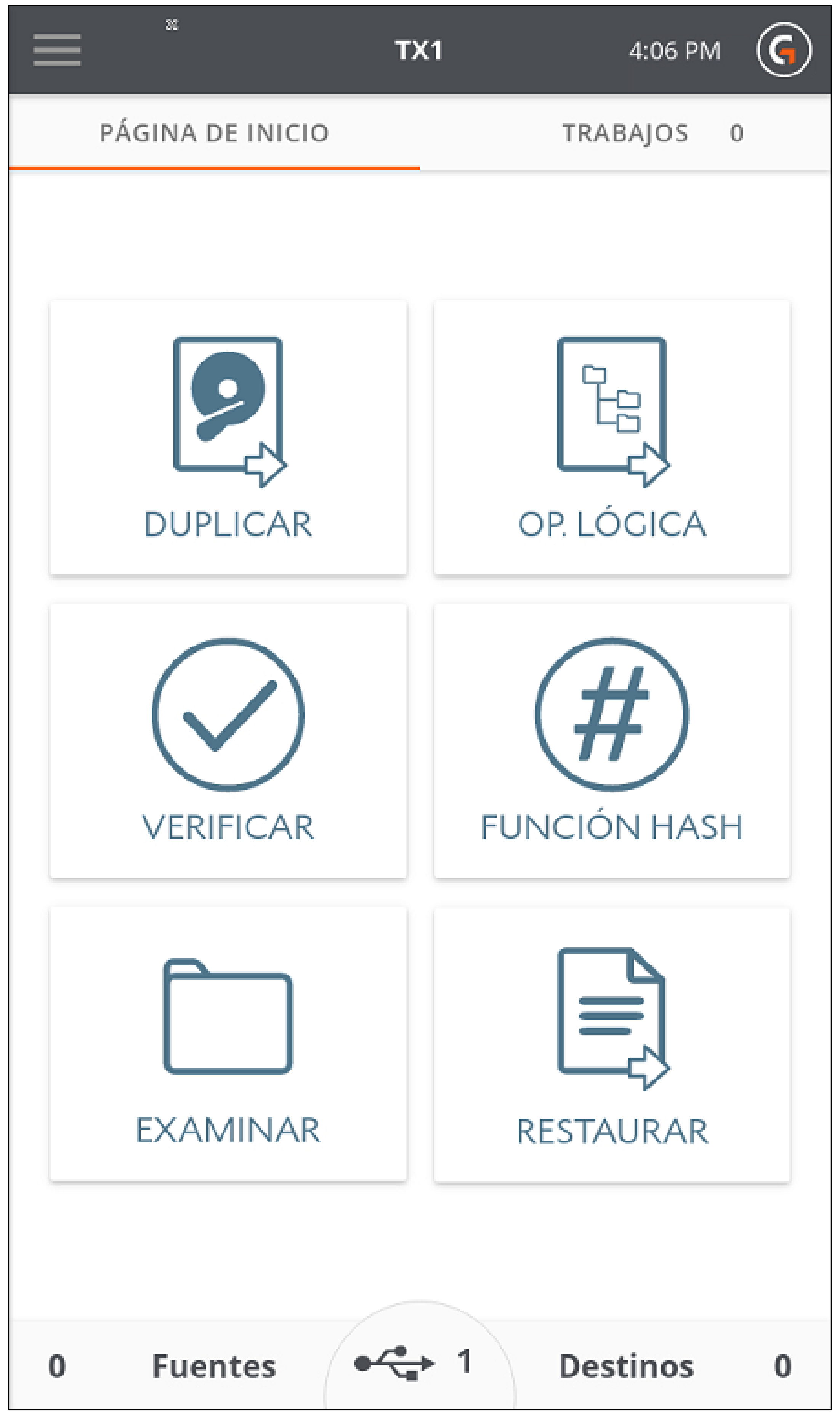
Français
French

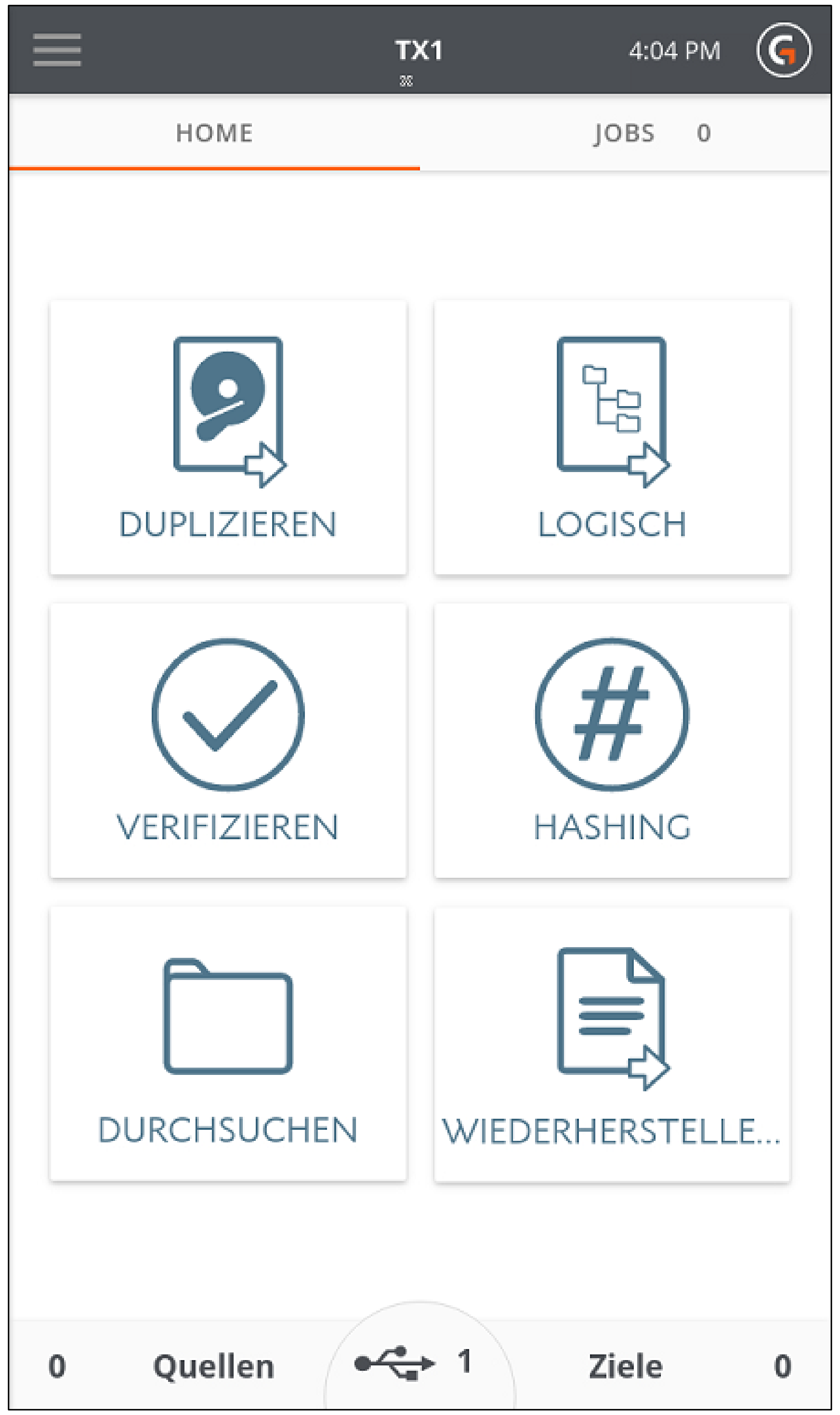
Português
Portuguese

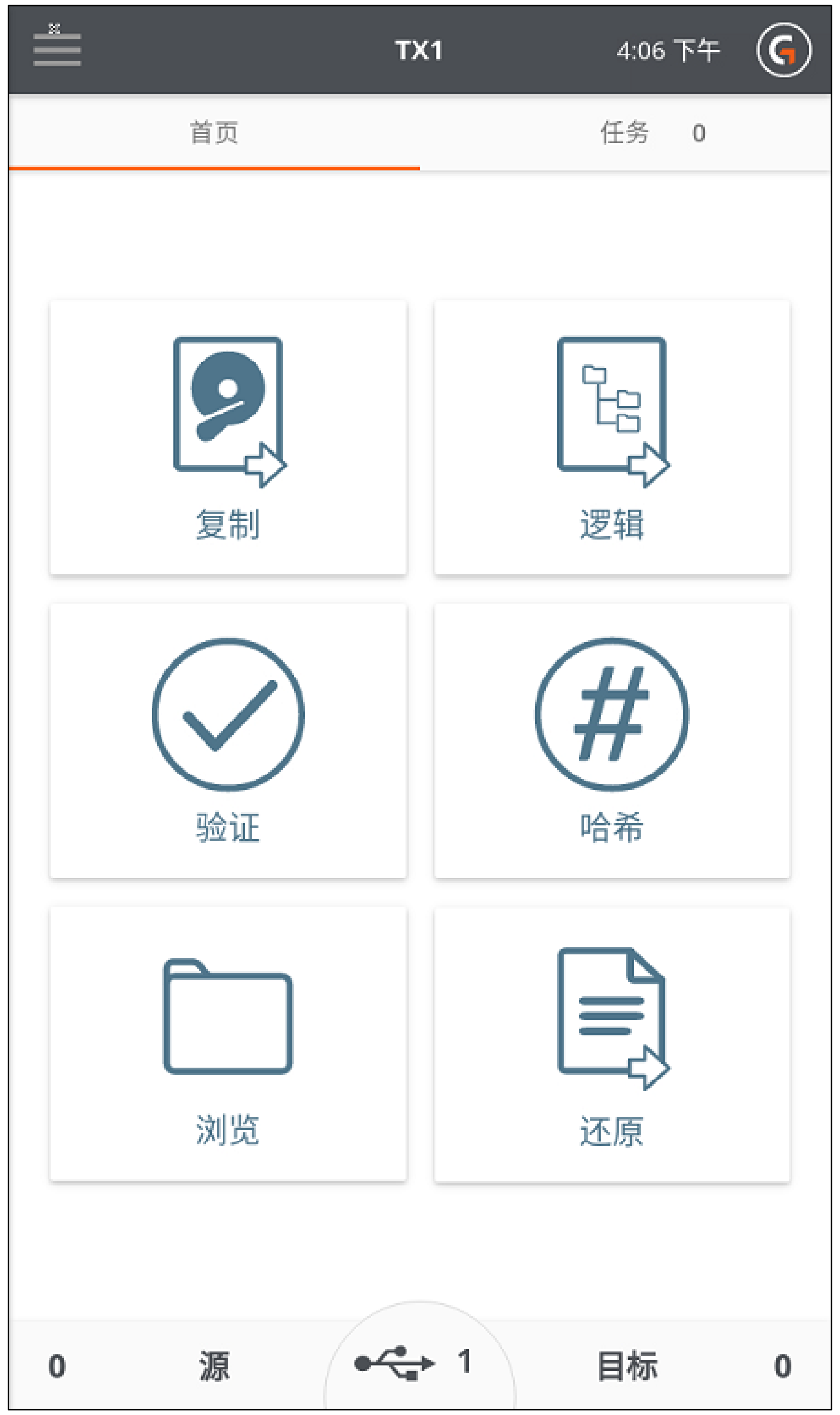
Русский
Russian

Türkçe
Turkish

中文
Chinese





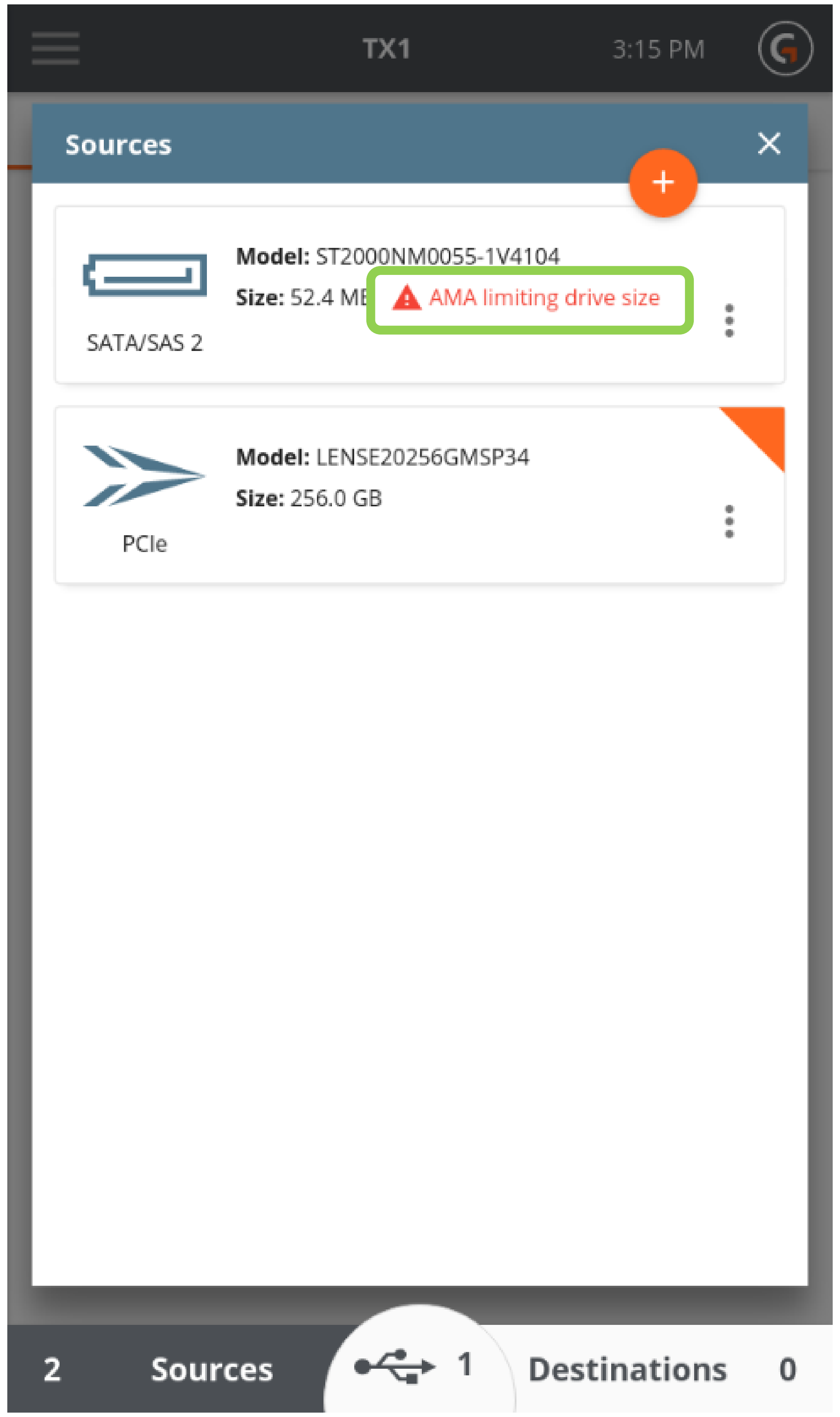


What is AMA? (And why should I care?)

- Accessible Max Address (AMA), also known as Accessible Max Address Configuration (AMAC) is a new command set that was introduced in ATA Command Set 3 (ACS-3) by the T13 storage industry committee.
- AMA is optional, but supported by many newer ATA (SATA) drives
- Replaces HPA and DCO to limit size of drive (create hidden areas)
  - Like DCO, “unlocking” a hidden AMA partition will require a deterministic write
- As of Feb 2020, all current Tableau bridges (using TIM 1.3) and duplicators/imagers support the detection and removal of AMA settings!
  - TIM 1.3 and TD2u 2.0 support AMA detection and removal
  - TX1 2.2 supports AMA detection, removal, restore and trim
  - T35u & T3iu recently updated to support AMA detection and removal in Feb via TFU 20.1

TX1 V2.2 RELEASE

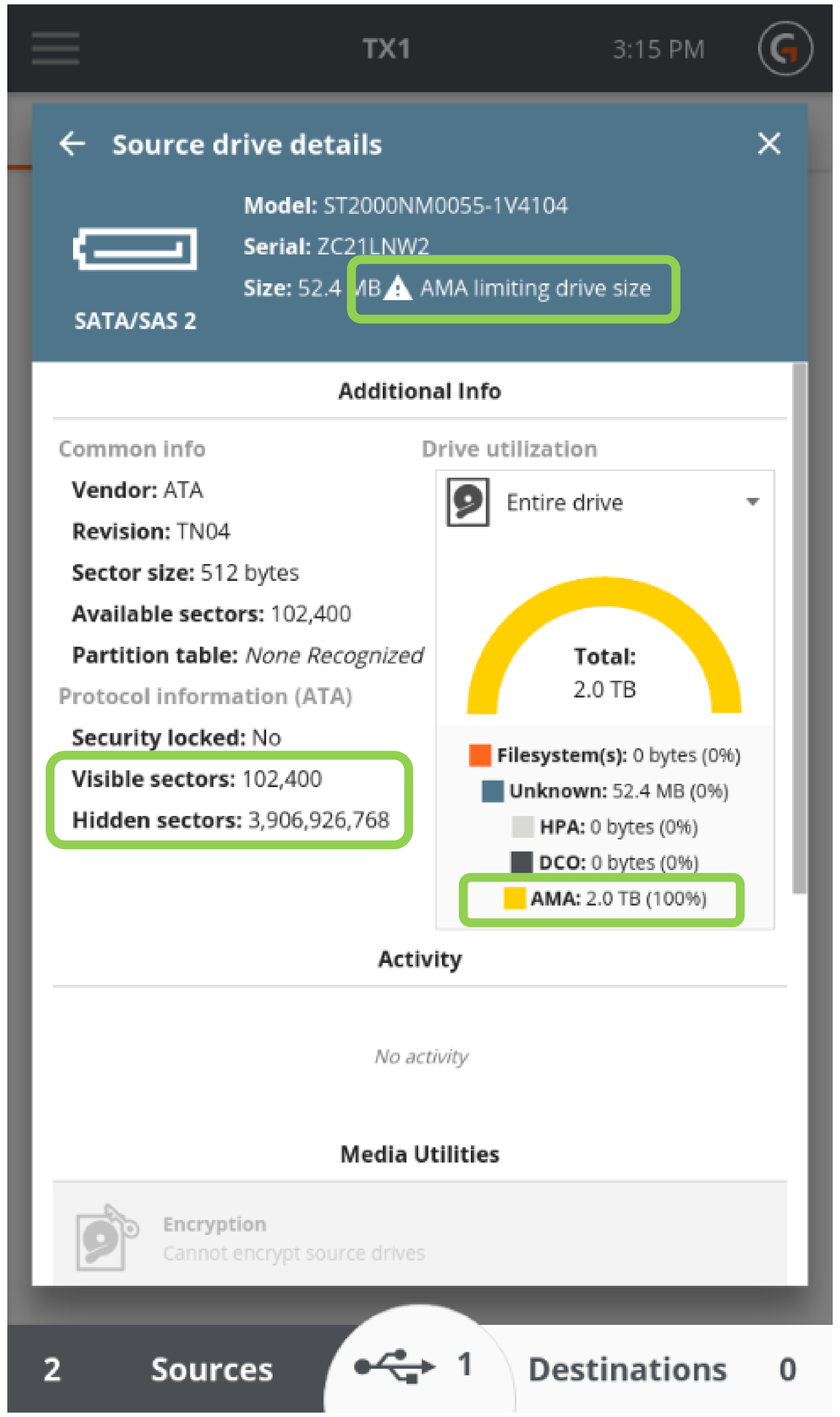
AMA (Accessible Max Address) support



Sources

Model: ST2000NM0055-1V4104
Size: 52.4 MB ⚠ AMA limiting drive size
SATA/SAS 2

Model: LENSE20256GMSP34
Size: 256.0 GB
PCIe



Source drive details

Model: ST2000NM0055-1V4104
Serial: ZC21LNW2
Size: 52.4 MB ⚠ AMA limiting drive size
SATA/SAS 2

Additional Info

Common info
Vendor: ATA
Revision: TN04
Sector size: 512 bytes
Available sectors: 102,400
Partition table: *None Recognized*

Protocol information (ATA)
Security locked: No
Visible sectors: 102,400
Hidden sectors: 3,906,926,768

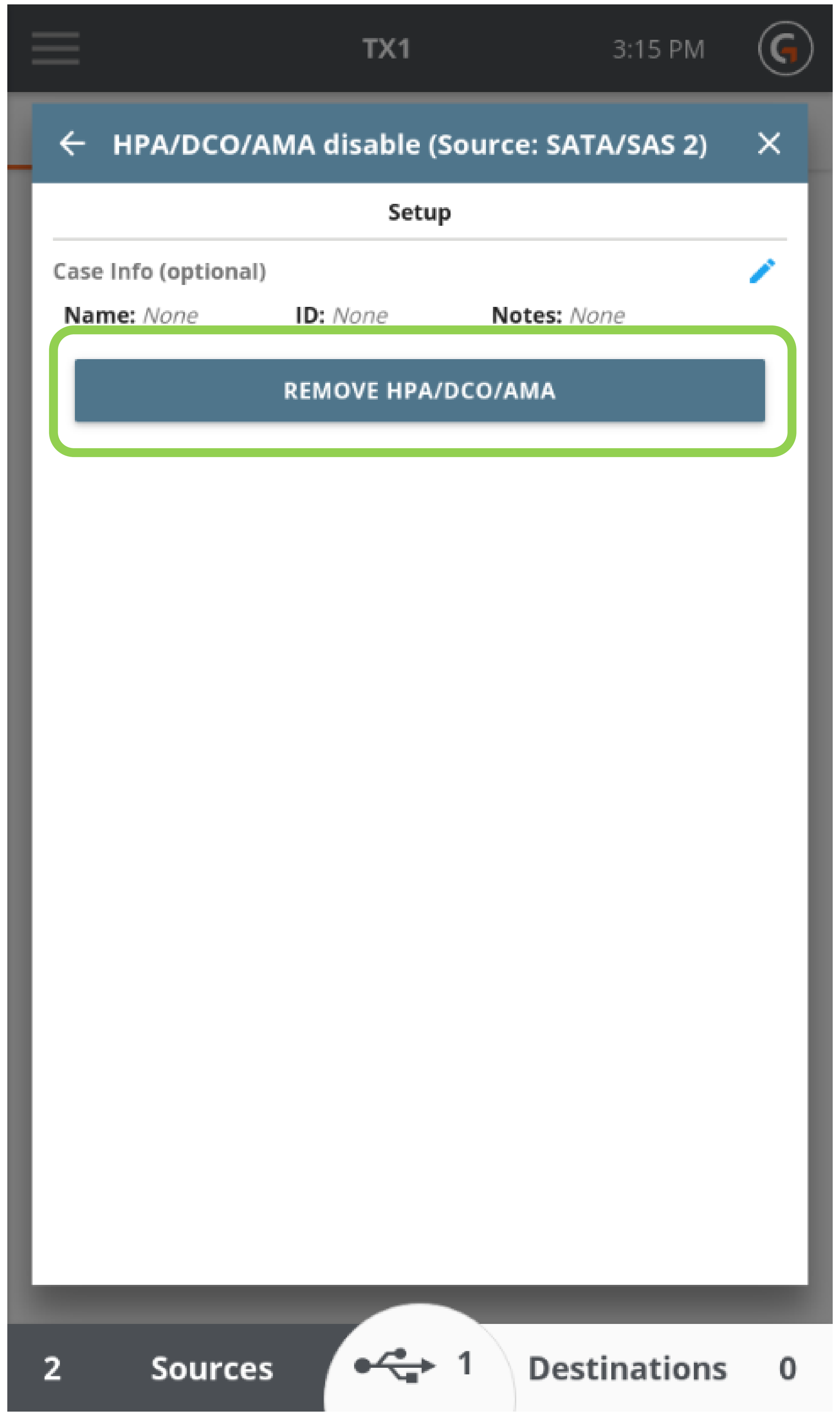
Drive utilization
Entire drive
Total: 2.0 TB
🟧 **Filesystem(s):** 0 bytes (0%)
🟦 **Unknown:** 52.4 MB (0%)
⬜ **HPA:** 0 bytes (0%)
⬛ **DCO:** 0 bytes (0%)
🟨 **AMA:** 2.0 TB (100%)

Activity

No activity

Media Utilities

Encryption
Cannot encrypt source drives

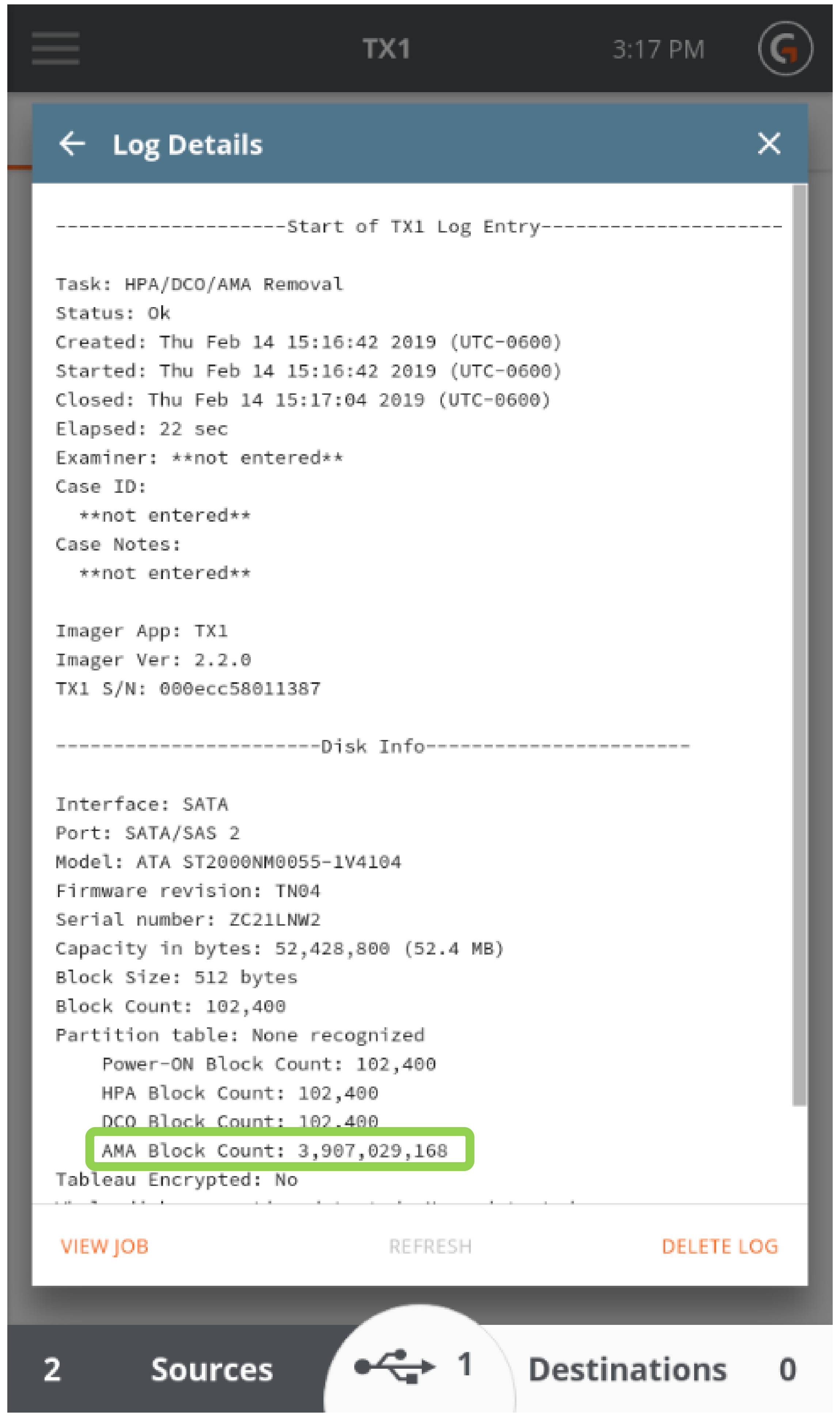


HPA/DCO/AMA disable (Source: SATA/SAS 2)

Setup

Case Info (optional)
Name: *None* **ID:** *None* **Notes:** *None*

REMOVE HPA/DCO/AMA



Log Details

```
--------------------Start of TX1 Log Entry---------------------

Task: HPA/DCO/AMA Removal
Status: Ok
Created: Thu Feb 14 15:16:42 2019 (UTC-0600)
Started: Thu Feb 14 15:16:42 2019 (UTC-0600)
Closed: Thu Feb 14 15:17:04 2019 (UTC-0600)
Elapsed: 22 sec
Examiner: **not entered**
Case ID:
  **not entered**
Case Notes:
  **not entered**

Imager App: TX1
Imager Ver: 2.2.0
TX1 S/N: 000ecc58011387

----------------------Disk Info----------------------

Interface: SATA
Port: SATA/SAS 2
Model: ATA ST2000NM0055-1V4104
Firmware revision: TN04
Serial number: ZC21LNW2
Capacity in bytes: 52,428,800 (52.4 MB)
Block Size: 512 bytes
Block Count: 102,400
Partition table: None recognized
    Power-ON Block Count: 102,400
    HPA Block Count: 102,400
    DCO Block Count: 102,400
    AMA Block Count: 3,907,029,168
Tableau Encrypted: No
```

VIEW JOB REFRESH DELETE LOG

opentext™

Tableau Drive Adapters (TDA3-3, TDA7-4, TDA7-7)

New Tableau Drive Adapters

Provide users the ability to connect physical media with non-standard connectors to Tableau Forensic Bridges or Duplicators.

mSATA / M.2 SATA SSD adapter

TDA3-3

PCIe U.2 SSD adapter cable

TDA7-4

Apple 2016+ PCIe SSD adapter

TDA7-7

Updated Adapter Bundles

TKDA-SATA-IDE-7PC
TKDA-PCIE-5PC
TK7U-BNDLC

More New Tableau Drive Adapters! (Feb 2020)

- Connect physical media with non-standard connectors to our Tableau Forensic Bridges and Duplicators.
- We’re adding new adapters to the family: SATA, PCIe and Mac.

SATA and IDE adapters

PCIe adapters and cable

Mac Adapters

New Tableau Drive Adapters Overview

- Tableau drive adapters allow users to connect physical media with non-standard connectors to our Tableau Forensic Bridges or Duplicators so that they can preview or create forensic copies of the data on the drives.

mSATA / M.2 SATA SSD adapter

model TDA3-3

PCIe U.2 SSD adapter cable

model TDA7-4

Apple 2016+ PCIe SSD adapter

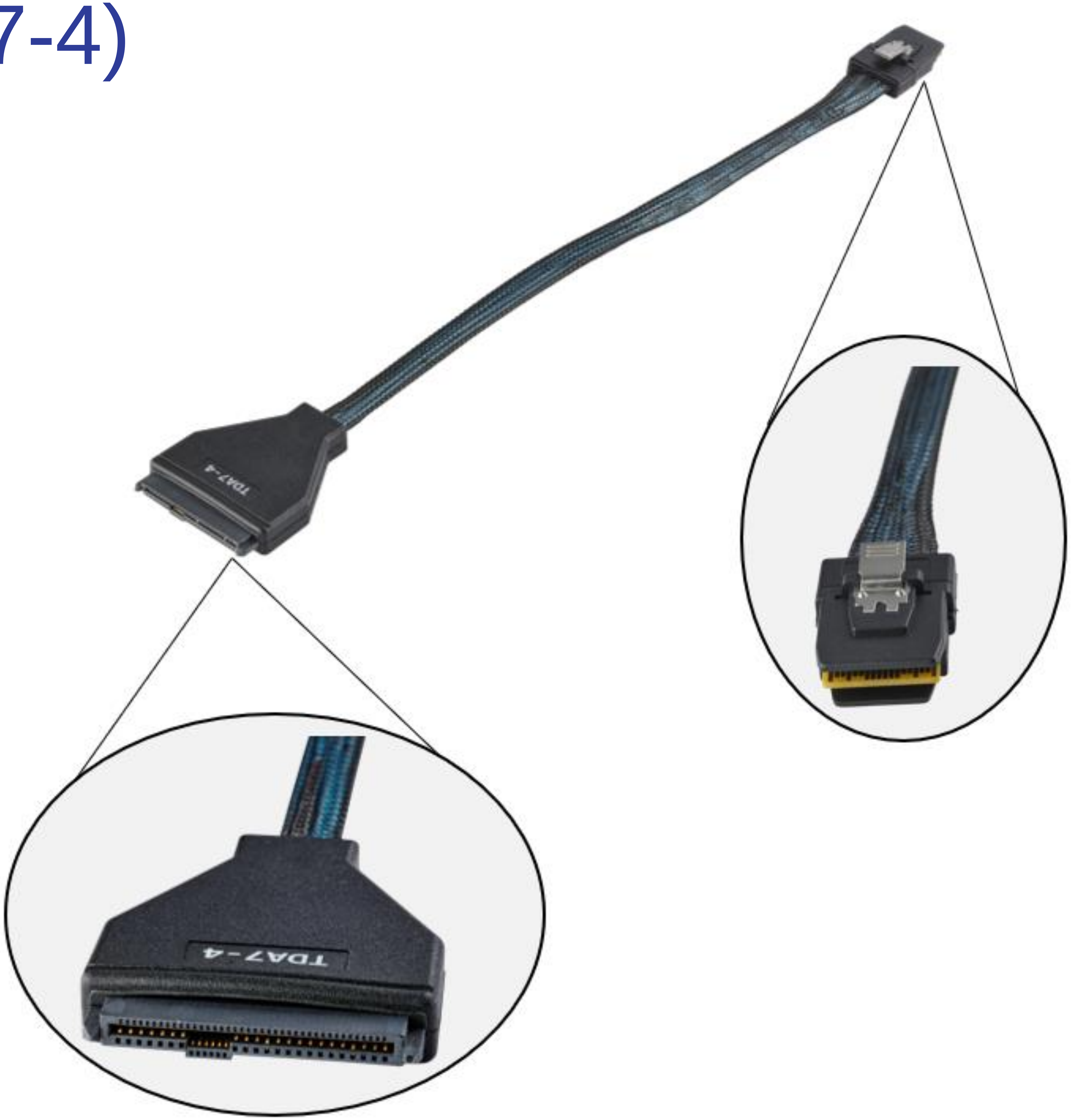
model TDA7-7

mSATA / M.2 SATA SSD Adapter (TDA3-3)

- Adapts from mSATA *or* M.2 SATA SSD to standard SATA
- SATA signal/power cable connects the adapter to a core SATA product
- Only one media type (mSATA or M.2 SATA) can be connected at a time
- Compatible with all Tableau SATA products – **NOT** compatible with PCIe
- Compatible with most non-Tableau products
- Includes thumbscrews to secure drives - No special OS drivers or tools required for operation

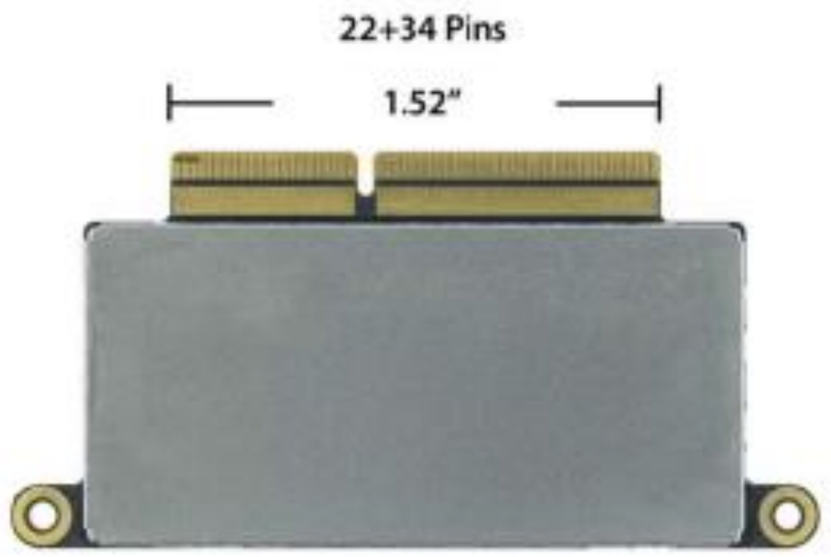
PCIe U.2 SSD Adapter (TDA7-4)

- Adapts from PCIe U.2 SSD to a Tableau PCIe Connector
- No special OS drivers, tools or cables required for operation
- Only compatible with Tableau products

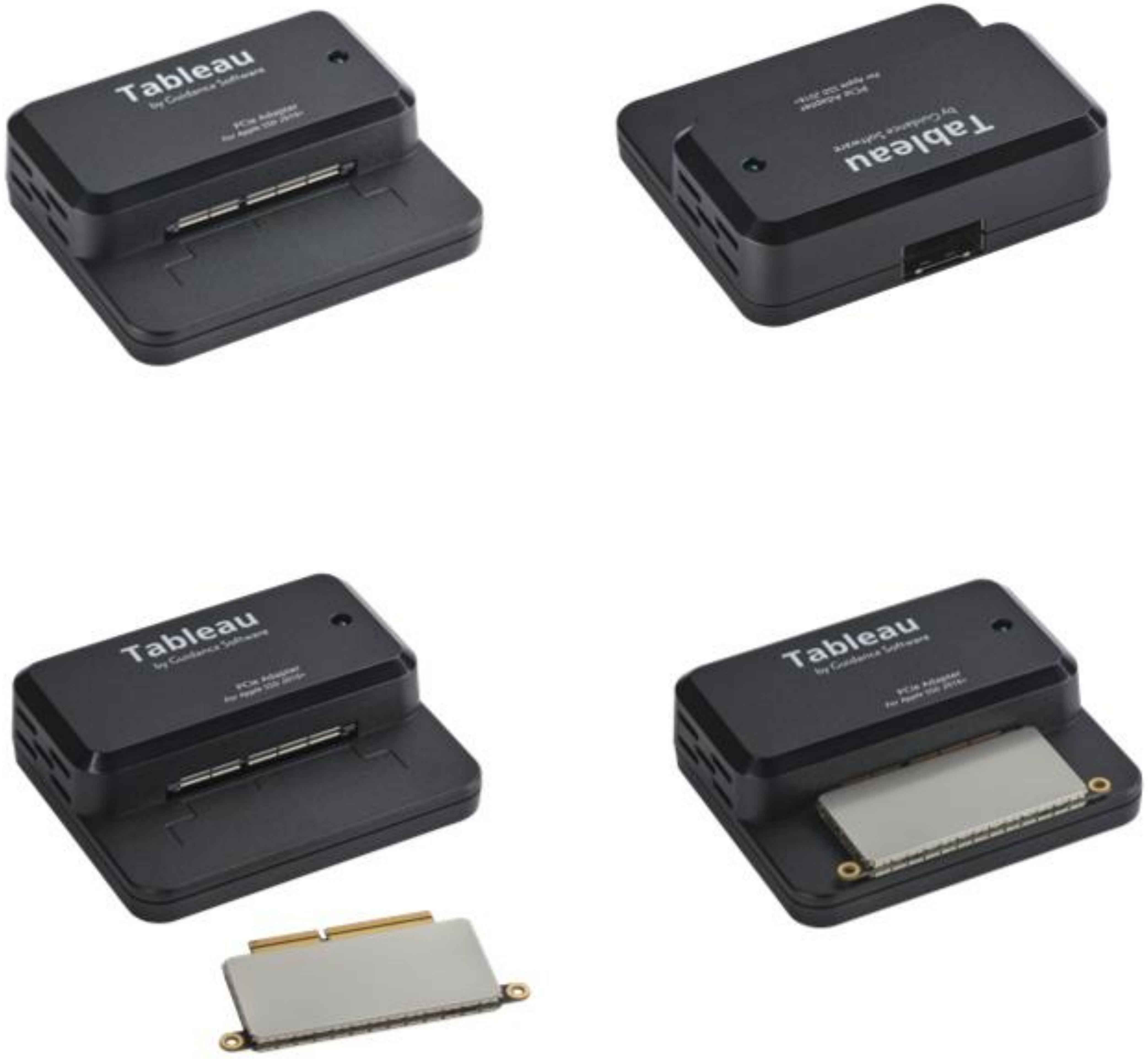


Apple 2016+ PCIe SSD Adapter (TDA7-7)

- Apple released yet another new custom SSD, which is used in MacBooks and Macbook Pros without a touch bar from 2016 and later:



- TDA7-7 Adapts fr pple PCIe SSD to a Tableau PCIe c au PCIe cable
- We are **first-to-market** for adapting this form factor SSD and currently* Tableau offers the only solution for direct forensic acquisition of these types of drives
- Adapter is only compatible with Tableau PCIe products
- No special OS drivers or tools required for operation



*As of January 2020

New Tableau Bags

- The new Tableau bags are used to transport and protect the Tableau PCIe adapters and related items when they are sold together as a complete bundle and are a differentiating convenience our customers love and expect from us. Construction is soft nylon with a side zipper.

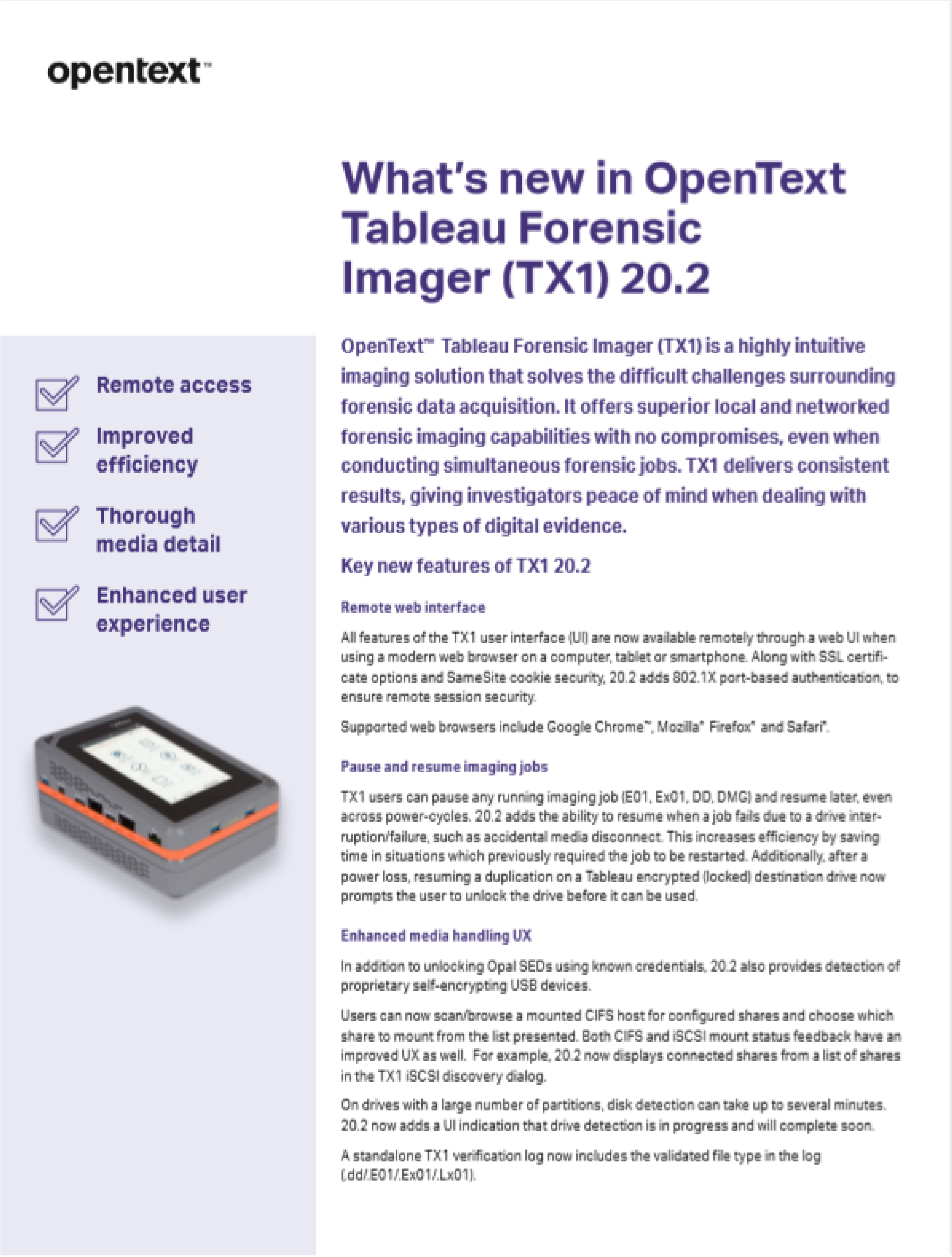
Model	Description	Photos
TB6	Slightly larger version of the existing TB5 bag and has room for all five PCIe adapters and a 4-inch PCIe cable.	
TB7	Slightly larger than the TB6 bag and has room for all five PCIe adapters plus a Tableau Forensic PCIe Bridge (T7u), the required power supply, and cables for operation.	

Where to find more information

- Product webpage

  https://www.opentext.com/products-and-solutions/products/security

Product Information



opentext™

What's new in OpenText Tableau Forensic Imager (TX1) 20.2

- ☑ Remote access
- ☑ Improved efficiency
- ☑ Thorough media detail
- ☑ Enhanced user experience

OpenText™ Tableau Forensic Imager (TX1) is a highly intuitive imaging solution that solves the difficult challenges surrounding forensic data acquisition. It offers superior local and networked forensic imaging capabilities with no compromises, even when conducting simultaneous forensic jobs. TX1 delivers consistent results, giving investigators peace of mind when dealing with various types of digital evidence.

Key new features of TX1 20.2

Remote web interface

All features of the TX1 user interface (UI) are now available remotely through a web UI when using a modern web browser on a computer, tablet or smartphone. Along with SSL certificate options and SameSite cookie security, 20.2 adds 802.1X port-based authentication, to ensure remote session security.

Supported web browsers include Google Chrome™, Mozilla® Firefox® and Safari®.

Pause and resume imaging jobs

TX1 users can pause any running imaging job (E01, Ex01, DD, DMG) and resume later, even across power-cycles. 20.2 adds the ability to resume when a job fails due to a drive interruption/failure, such as accidental media disconnect. This increases efficiency by saving time in situations which previously required the job to be restarted. Additionally, after a power loss, resuming a duplication on a Tableau encrypted (locked) destination drive now prompts the user to unlock the drive before it can be used.

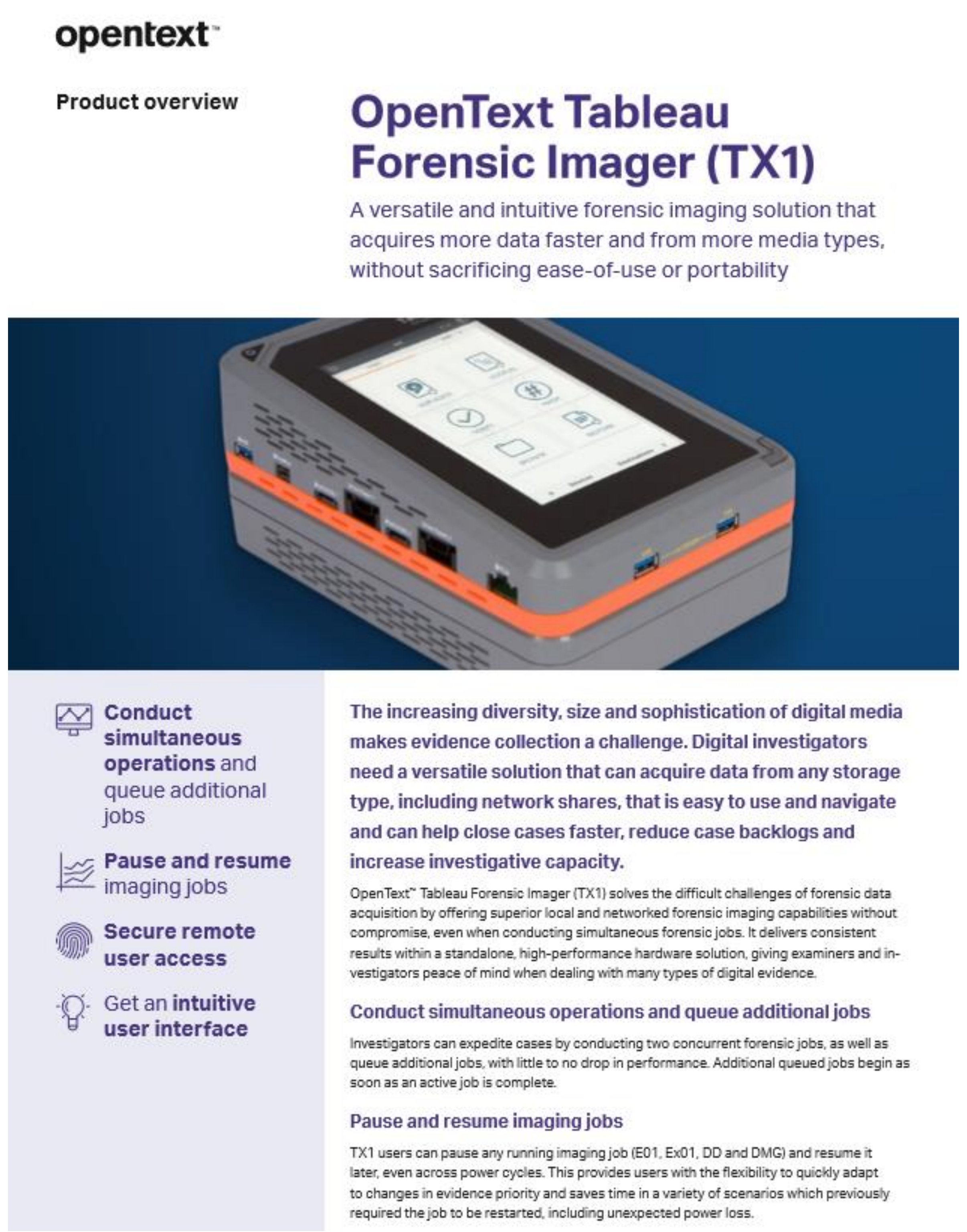
Enhanced media handling UX

In addition to unlocking Opal SEDs using known credentials, 20.2 also provides detection of proprietary self-encrypting USB devices.

Users can now scan/browse a mounted CIFS host for configured shares and choose which share to mount from the list presented. Both CIFS and iSCSI mount status feedback have an improved UX as well. For example, 20.2 now displays connected shares from a list of shares in the TX1 iSCSI discovery dialog.

On drives with a large number of partitions, disk detection can take up to several minutes. 20.2 now adds a UI indication that drive detection is in progress and will complete soon.

A standalone TX1 verification log now includes the validated file type in the log (.dd/.E01/.Ex01/.Lx01).



opentext™

Product overview

OpenText Tableau Forensic Imager (TX1)

A versatile and intuitive forensic imaging solution that acquires more data faster and from more media types, without sacrificing ease-of-use or portability

- **Conduct simultaneous operations** and queue additional jobs
- **Pause and resume** imaging jobs
- **Secure remote user access**
- Get an **intuitive user interface**

The increasing diversity, size and sophistication of digital media makes evidence collection a challenge. Digital investigators need a versatile solution that can acquire data from any storage type, including network shares, that is easy to use and navigate and can help close cases faster, reduce case backlogs and increase investigative capacity.

OpenText™ Tableau Forensic Imager (TX1) solves the difficult challenges of forensic data acquisition by offering superior local and networked forensic imaging capabilities without compromise, even when conducting simultaneous forensic jobs. It delivers consistent results within a standalone, high-performance hardware solution, giving examiners and investigators peace of mind when dealing with many types of digital evidence.

Conduct simultaneous operations and queue additional jobs

Investigators can expedite cases by conducting two concurrent forensic jobs, as well as queue additional jobs, with little to no drop in performance. Additional queued jobs begin as soon as an active job is complete.

Pause and resume imaging jobs

TX1 users can pause any running imaging job (E01, Ex01, DD and DMG) and resume it later, even across power cycles. This provides users with the flexibility to quickly adapt to changes in evidence priority and saves time in a variety of scenarios which previously required the job to be restarted, including unexpected power loss.

opentext™

OpenText™ EnCase™ Forensic / Tableau Training Bundle

OpenText™ EnCase™ Forensic and Tableau Hardware bundle

OpenText™ is pleased to announce the release of a new bundle offering comprising of these key digital forensic products at 15% discount until 30th June 2020

EnCase™ Forensic

+

Tableau Hardware

+

Training

Bundle contents

- **EnCase Forensic**
  - Perpetual license with physical key (dongle/electronic if requested)
  - 1 year SMS (23% of license price)

- **Tableau Hardware**
  - Tableau Forensic Imager (TX1) Kit
  - Tableau PCIe M.2 SSD adapter (TDA7-2)

- **OpenText™ EnCase Training options (can choose one)**
  - Option (1) ~~Single Live Classroom (at OpenText Facilities)~~ /Virtual training (streams live)
    - Customer can select one training from the list provided
  - Option (2) Annual Training Passport
  - Option (3) OnDemand Annual Training Passport

Training Options

OPTION 1 - OpenText™ EnCase training selection for a single live/virtual training at OpenText™ facilities

- DF120-Foundations in Digital Forensics with EnCase
- DF210-Building an Investigation with EnCase
- DF320-Advanced Analysis of Windows Artifacts with EnCase
- DF410-NTFS Examinations with EnCase
- DFIR350-Internet-based Investigation with EnCase

Training Options

OPTION 2 - Annual Training Passport
Pay one discounted annual rate for unlimited training

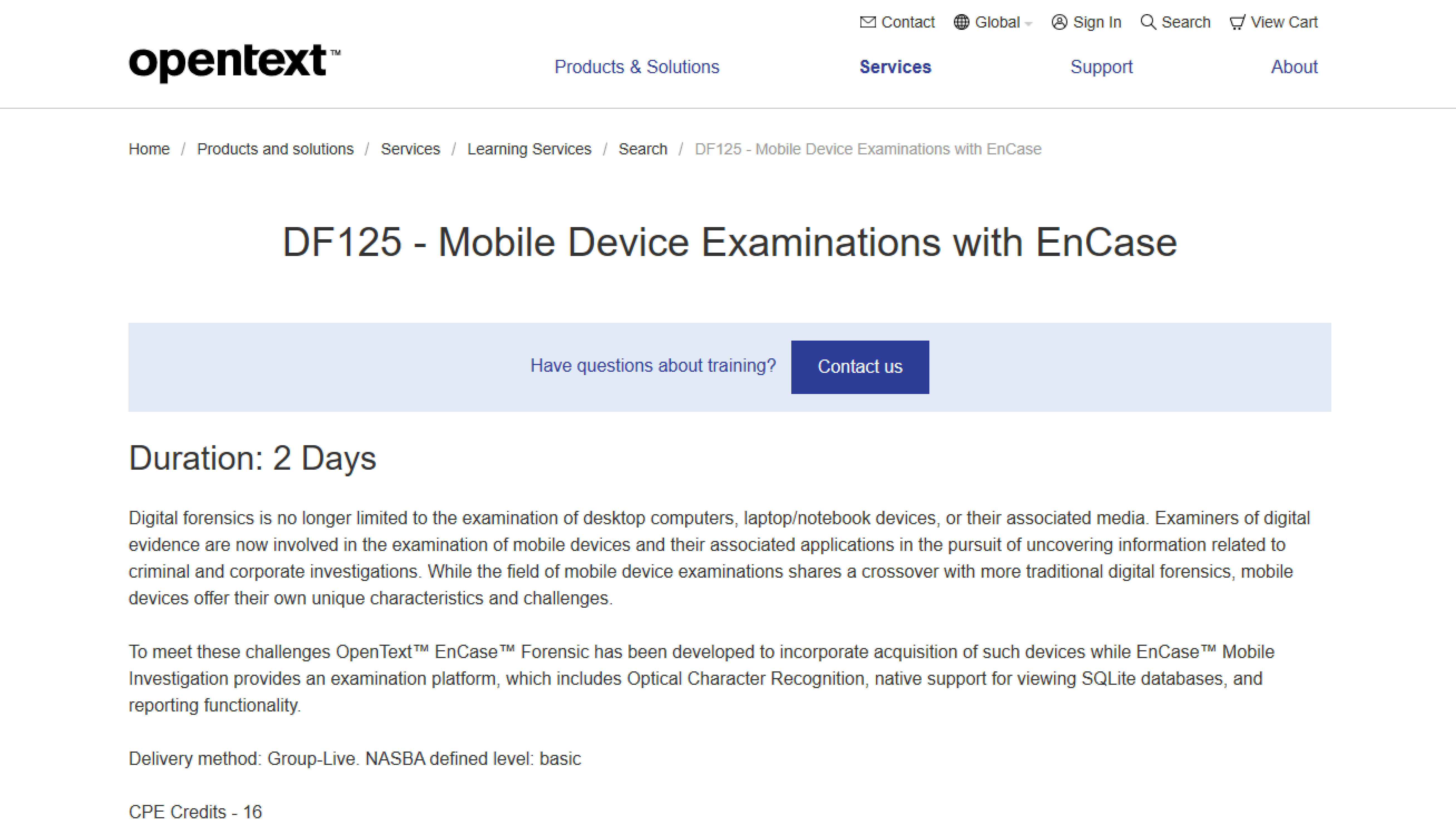
- Annual Passport holders are entitled to attend unlimited EnCase Training courses.
- Combine ~~classroom~~, vClass and OnDemand delivery methods for maximum flexibility.

OPTION 3 - OnDemand Annual Training Passport

- Attend all EnCase Training OnDemand offerings for one discounted annual rate.

Learning Services – Training Only Option

- Training Only is 25% discount
- DF125 Mobile Device Examinations Virtual class starts 1st June 2020
- Online access to courses provided in the classroom


Contact
Global
Sign In
Search
View Cart
opentext
Products & Solutions
Services
Support
About
Home / Products and solutions / Services / Learning Services / Search / DF125 - Mobile Device Examinations with EnCase

DF125 - Mobile Device Examinations with EnCase

Have questions about training?
Contact us

Duration: 2 Days

Digital forensics is no longer limited to the examination of desktop computers, laptop/notebook devices, or their associated media. Examiners of digital evidence are now involved in the examination of mobile devices and their associated applications in the pursuit of uncovering information related to criminal and corporate investigations. While the field of mobile device examinations shares a crossover with more traditional digital forensics, mobile devices offer their own unique characteristics and challenges.

To meet these challenges OpenText™ EnCase™ Forensic has been developed to incorporate acquisition of such devices while EnCase™ Mobile Investigation provides an examination platform, which includes Optical Character Recognition, native support for viewing SQLite databases, and reporting functionality.

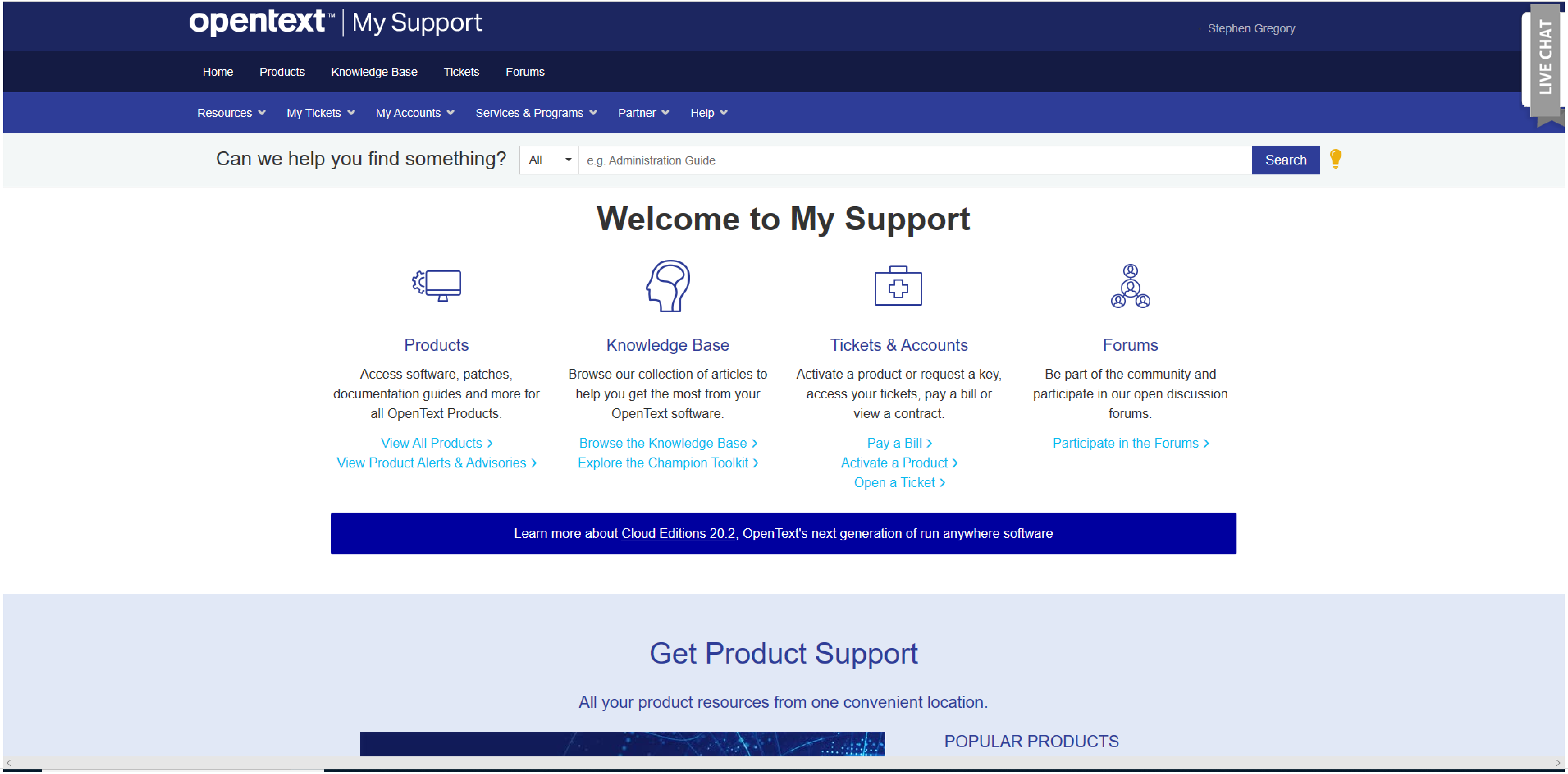
Delivery method: Group-Live. NASBA defined level: basic

CPE Credits - 16

opentext™

My Support

My Support



Can we help you find something?

Welcome to My Support

Products

Access software, patches, documentation guides and more for all OpenText Products.

View All Products ›
View Product Alerts & Advisories ›

Knowledge Base

Browse our collection of articles to help you get the most from your OpenText software.

Browse the Knowledge Base ›
Explore the Champion Toolkit ›

Tickets & Accounts

Activate a product or request a key, access your tickets, pay a bill or view a contract.

Pay a Bill ›
Activate a Product ›
Open a Ticket ›

Forums

Be part of the community and participate in our open discussion forums.

Participate in the Forums ›

Learn more about Cloud Editions 20.2, OpenText's next generation of run anywhere software

Get Product Support

All your product resources from one convenient location.

POPULAR PRODUCTS

Working with Technical Support

Best Practice Guide

Engaging Technical Support

Technical Support is available 24 hours, 7 days a week – depending on your contact type. We are ready to assist when you need us. Using our MySupport, with 4 easy Steps, you are directed to a Technician.

How do you Connect with Technical Support?

- Email
- Phone
- Support.opentext.com portal

Recommended Best Practice – My Support Portal

- Open or Update cases directly on the portal to avoid email delays
- Customer controls the captured content in the ticket
- Less or No L1/CSR interaction Required = Direct to Tech

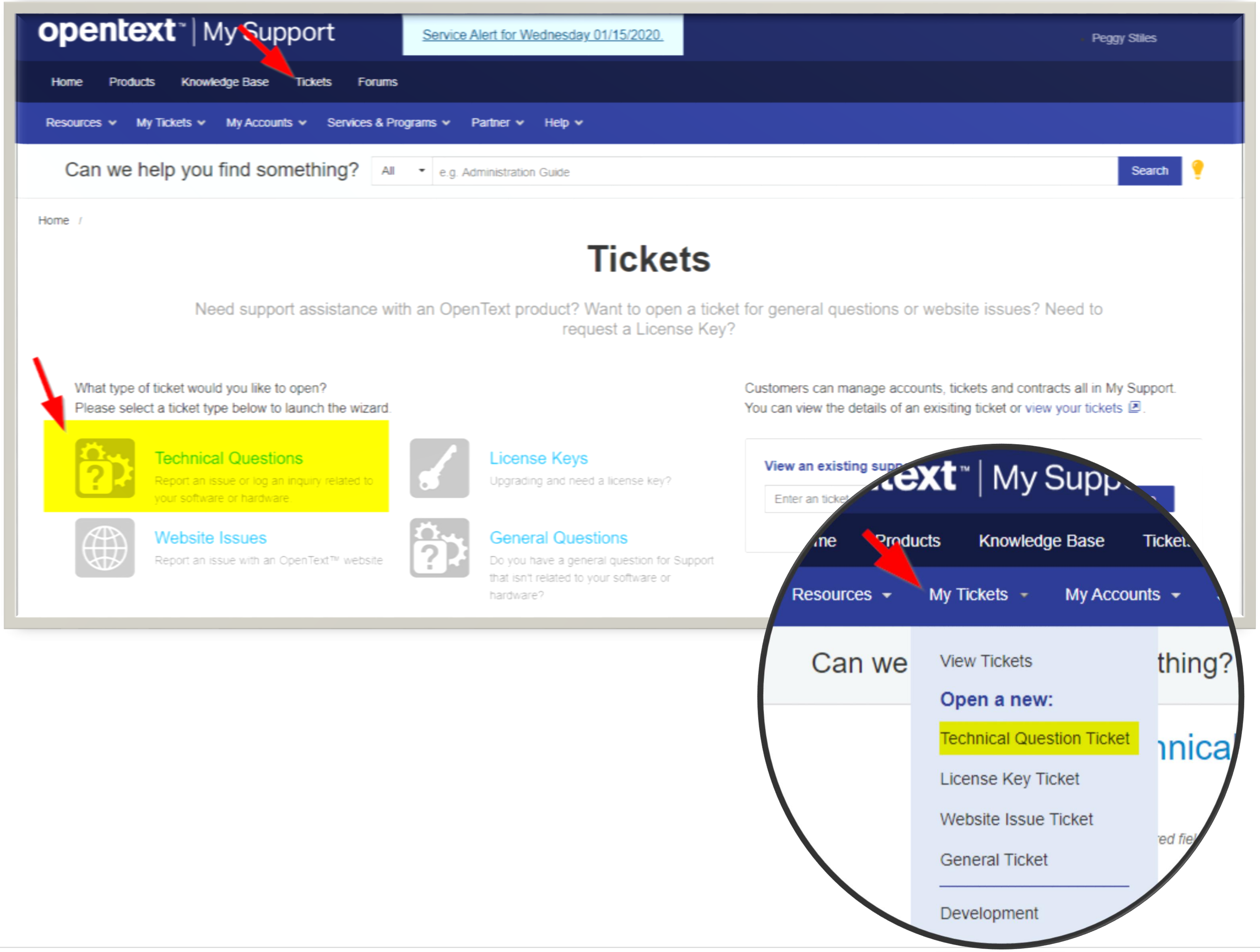
Best-practice MySupport workflow can be found in the Appendix to this slide deck!

Opening a Ticket Process

Step 1

Accessing the Portal and Selecting the correct ticket type

- Portal is located on MySupport: http://Support.opentext.com
- When looking for Technical Support, use the **Technical (Question) Ticket Type**
- Direct link to the Technical Ticket option: https://support.opentext.com/portal/site/css?customView=newTicketTechnical



Tickets

Need support assistance with an OpenText product? Want to open a ticket for general questions or website issues? Need to request a License Key?

What type of ticket would you like to open?
Please select a ticket type below to launch the wizard.

Technical Questions
Report an issue or log an inquiry related to your software or hardware

License Keys
Upgrading and need a license key?

Website Issues
Report an issue with an OpenText™ website

General Questions
Do you have a general question for Support that isn't related to your software or hardware?

Customers can manage accounts, tickets and contracts all in My Support. You can view the details of an exisiting ticket or view your tickets.

View an existing supp
Enter an ticket

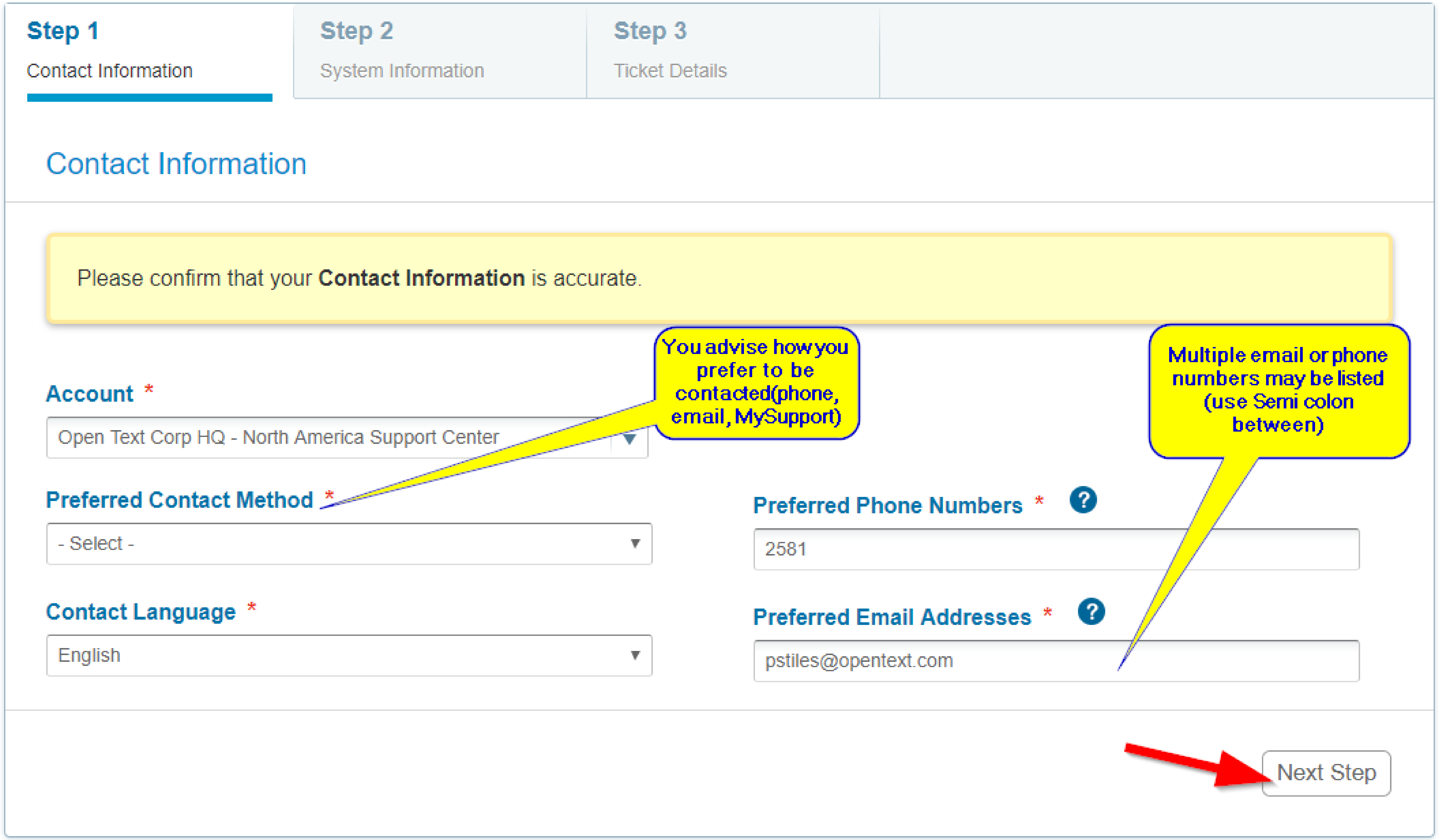
Opening a Ticket Process

Contact Information:

You have control over Who and How we contact.

Tip:

Preferred Email Address field can contain multiple email addresses (separated by a Semi Colon)



Contact Information

Please confirm that your **Contact Information** is accurate.

Account *
Open Text Corp HQ - North America Support Center

Preferred Contact Method *
- Select -

Contact Language *
English

Preferred Phone Numbers *
2581

Preferred Email Addresses *
pstiles@opentext.com

You advise how you prefer to be contacted(phone, email, MySupport)

Multiple email or phone numbers may be listed (use Semi colon between)

Opening a Ticket Process

Step 3

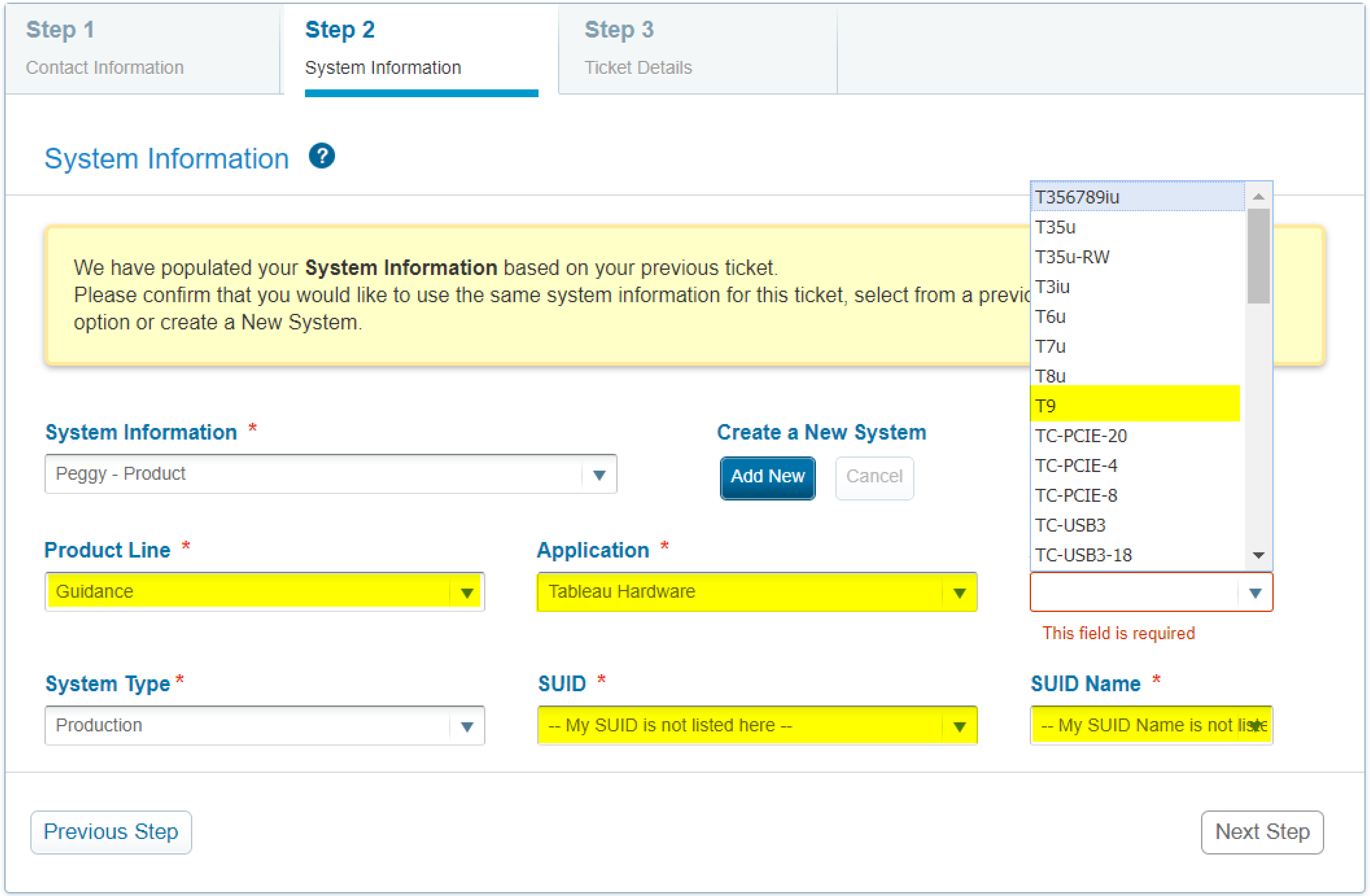
Tell us about your System

This step is key in accelerating your ticket through to the correct Tech (Direct to Tech).

Tips:

1. Select Guidance from Product Line
2. Select Tableau Hardware under the Application Field
3. In Application Versions select the hardware model you need assistance with

The SUID does not apply for Tableau Hardware. Since it's a required field, select "–My SUID is not listed here –"



We have populated your **System Information** based on your previous ticket.
Please confirm that you would like to use the same system information for this ticket, select from a previc
option or create a New System.

System Information *: Peggy - Product

Create a New System: Add New | Cancel

Product Line *: Guidance

Application *: Tableau Hardware

T356789iu
T35u
T35u-RW
T3iu
T6u
T7u
T8u
T9
TC-PCIE-20
TC-PCIE-4
TC-PCIE-8
TC-USB3
TC-USB3-18

This field is required

System Type *: Production

SUID *: -- My SUID is not listed here --

SUID Name *: -- My SUID Name is not liste

Opening a Ticket Process

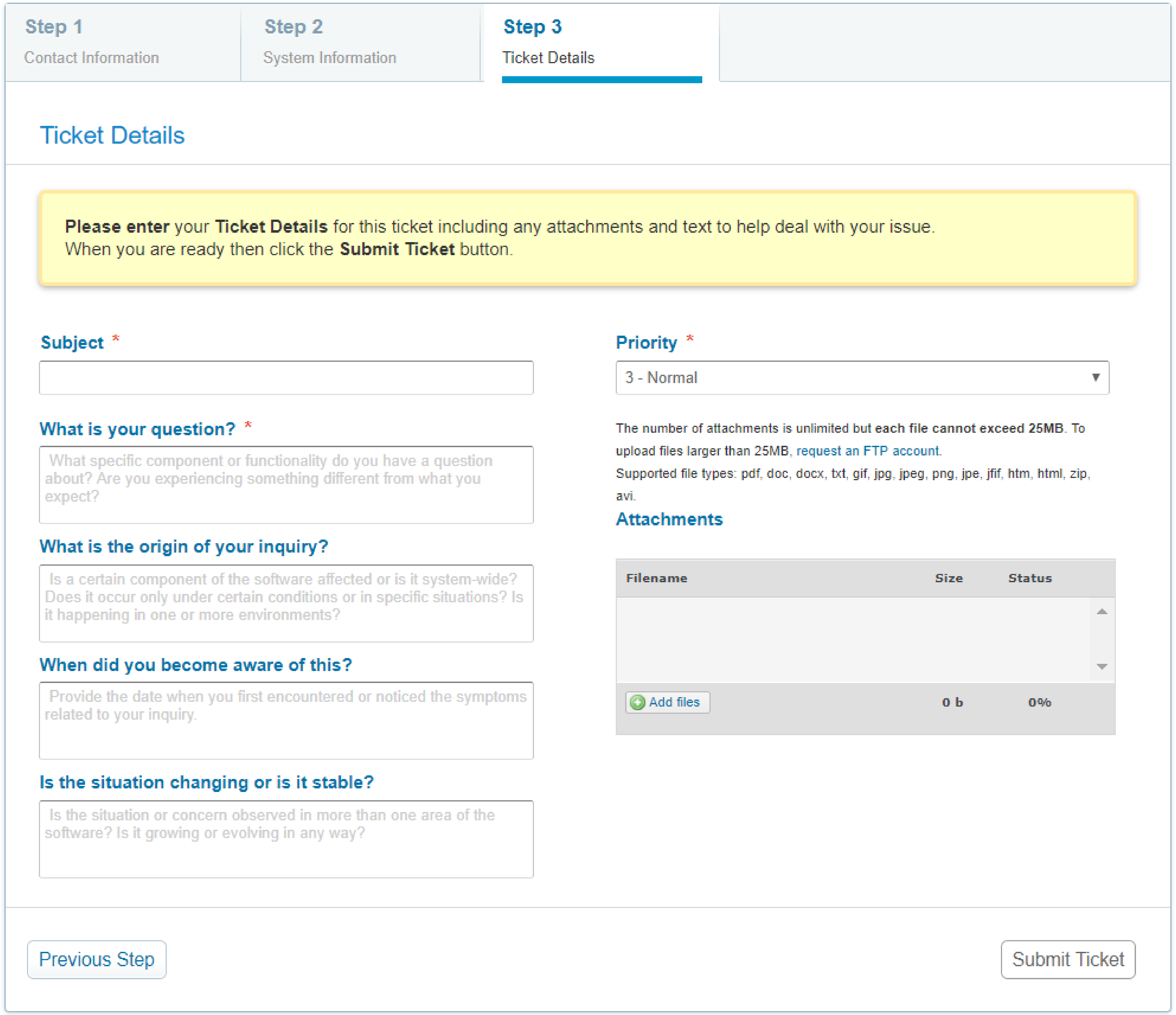
Step 4

Last Step

Tells us about the reason for the ticket. You control the priority of your tickets

Tips:

1. Provide as much detail as possible to accelerate through Scoping to resolution
2. Attach files if applicable



Step 1 Contact Information | Step 2 System Information | Step 3 Ticket Details

Ticket Details

Please enter your **Ticket Details** for this ticket including any attachments and text to help deal with your issue.
When you are ready then click the **Submit Ticket** button.

Subject *

What is your question? *
What specific component or functionality do you have a question about? Are you experiencing something different from what you expect?

What is the origin of your inquiry?
Is a certain component of the software affected or is it system-wide? Does it occur only under certain conditions or in specific situations? Is it happening in one or more environments?

When did you become aware of this?
Provide the date when you first encountered or noticed the symptoms related to your inquiry.

Is the situation changing or is it stable?
Is the situation or concern observed in more than one area of the software? Is it growing or evolving in any way?

Priority *
3 - Normal ▾

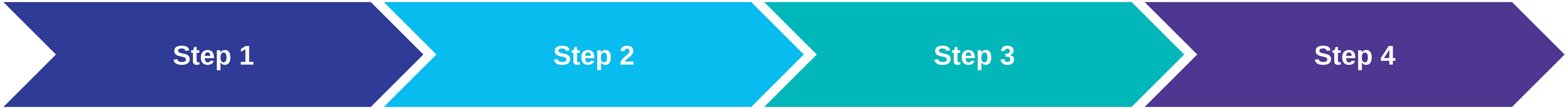
The number of attachments is unlimited but each file cannot exceed 25MB. To upload files larger than 25MB, request an FTP account.
Supported file types: pdf, doc, docx, txt, gif, jpg, jpeg, png, jpe, jfif, htm, html, zip, avi.

Attachments

Filename	Size	Status
Add files	0 b	0%

Previous Step | Submit Ticket

Review.



Step 1

Accessing the Portal and Selecting the correct ticket type

- Portal is located on MySupport: http://Support.opentext.com
- When looking for Technical Support, use the **Technical (Question) Ticket Type**
- Direct link to the Technical Ticket option: https://support.opentext.com/portal/site/css?customView=newTicketTechnical

Step 2

Contact Information:

You have control over Who and How we contact.

Tips:

Preferred Email Address field can contain multiple email addresses (separated by a Semi Colon)

Step 3

Tell us about your System

This step is key in accelerating your ticket through to the correct Tech (Direct to Tech).

Tips:

1. Select Guidance from Product Line
2. Select Tableau Hardware under the Application Field
3. In Application Versions select the hardware model you need assistance with

The SUID does not apply for Tableau Hardware. Since it’s a required field, select “–My SUID is not listed here –”

Step 4

Last Step

Tells us about the reason for the ticket. You control the priority of your tickets

Tips:

1. Provide as much detail as possible to accelerate through Scoping to resolution
2. Attach files if applicable

opentext™

DataExpert

Thank you

twitter.com/opentext

facebook.com/opentext

linkedin.com/company/opentext

opentext.com