ZClone Xi Forensic User's Manual

Logicube, Inc.

Chatsworth, CA 91311

USA

Phone: 818 700 8488

Fax: 818 700 8466

Version: 1.0

Date: 04/29/16

MAN-ZXI_FORENSIC

Limitation of Liability and Warranty Information

Logicube Disclaimer

LOGICUBE IS NOT LIABLE FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO PROPERTY DAMAGE, LOSS OF TIME OR DATA FROM USE OF A LOGICUBE PRODUCT, OR ANY OTHER DAMAGES RESULTING FROM PRODUCT MALFUNCTION OR FAILURE OF (INCLUDING WITHOUT LIMITATION, THOSE RESULTING FROM: (1) RELIANCE ON THE MATERIALS PRESENTED, (2) COSTS OF REPLACEMENT GOODS, (3) LOSS OF USE, DATA OR PROFITS, (4) DELAYS OR BUSINESS INTERRUPTIONS, (5) AND ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE (OR FROM DELAYS IN SERVICING OR INABILITY TO RENDER SERVICE ON ANY) LOGICUBE PRODUCT.

LOGICUBE MAKES EVERY EFFORT TO ENSURE PROPER OPERATION OF ALL PRODUCTS. HOWEVER, THE CUSTOMER IS RESPONSIBLE TO VERIFY THAT THE OUTPUT OF LOGICUBE PRODUCT MEETS THE CUSTOMER'S QUALITY REQUIREMENT. THE CUSTOMER FURTHER ACKNOWLEDGES THAT IMPROPER OPERATION OF LOGICUBE PRODUCT AND/OR SOFTWARE, OR HARDWARE PROBLEMS, CAN CAUSE LOSS OF DATA, DEFECTIVE FORMATTING, OR DATA LOADING. LOGICUBE WILL MAKE EFFORTS TO SOLVE OR REPAIR ANY PROBLEMS IDENTIFIED BY CUSTOMER, EITHER UNDER WARRANTY OR ON A TIME AND MATERIALS BASIS.

Warranty

DISCLAIMER

IMPORTANT - PLEASE READ THE TERMS OF THIS AGREEMENT CAREFULLY. BY INSTALLING OR USING LOGICUBE PRODUCTS, YOU AGREE TO BE BOUND BY THIS AGREEMENT.

IN NO EVENT WILL LOGICUBE BE LIABLE (WHETHER UNDER THIS AGREEMENT, RESULTING FROM THE PERFORMANCE OR USE OF LOGICUBE PRODUCTS, OR OTHERWISE) FOR ANY AMOUNTS REPRESENTING LOSS OF PROFITS, LOSS OR INACCURACY OF DATA, LOSS OR DELAYS OF BUSINESS, LOSS OF TIME, COSTS OF PROCUREMENT OF SUBSTITUTE GOODS, SERVICES, OR TECHNOLOGY, PROPERTY DAMAGE, OR INDIRECT, CONSEQUENTIAL, OR PUNITIVE DAMAGES OF A PURCHASER OR USER OF LOGICUBE PRODUCTS OR ANY THIRD PARTY. LOGICUBE'S AGGREGATE LIABILITY IN CONTRACT, TORT, OR OTHERWISE (WHETHER UNDER THIS AGREEMENT, RESULTING FROM THE PERFORMANCE OR USE OF LOGICUBE PRODUCTS, OR OTHERWISE) TO A PURCHASER OR USER OF LOGICUBE PRODUCTS SHALL BE LIMITED TO THE AMOUNT PAID BY THE PURCHASER FOR THE LOGICUBE PRODUCT. THIS LIMITATION OF LIABILITY WILL BE EFFECTIVE EVEN IF LOGICUBE HAS BEEN ADVISED OF THE POSSIBILITY OF ANY SUCH DAMAGES.

LOGICUBE MAKES EVERY EFFORT TO ENSURE PROPER OPERATION OF ITS PRODUCTS. HOWEVER, THE PURCHASER IS RESPONSIBLE FOR VERIFYING THAT THE OUTPUT OF A LOGICUBE PRODUCT MEETS THE

PURCHASER'S REQUIREMENTS. THE PURCHASER FURTHER ACKNOWLEDGES THAT IMPROPER OPERATION OF LOGICUBE PRODUCTS CAN CAUSE LOSS OF DATA, DEFECTIVE FORMATTING, OR DEFECTIVE DATA LOADING. LOGICUBE WILL MAKE EFFORTS TO SOLVE OR REPAIR ANY PROBLEMS IDENTIFIED BY PURCHASER, EITHER UNDER THE WARRANTY SET FORTH BELOW OR ON A TIME AND MATERIALS BASIS.

LIMITED WARRANTY

FOR ONE YEAR FROM THE DATE OF SALE (THE "WARRANTY PERIOD") LOGICUBE WARRANTS THAT THE PRODUCT (EXCLUDING CABLES, ADAPTERS, AND OTHER "CONSUMABLE" ITEMS) IS FREE FROM MANUFACTURING DEFECTS IN MATERIAL AND WORKMANSHIP. THIS LIMITED WARRANTY COVERS DEFECTS ENCOUNTERED IN THE NORMAL USE OF THE PRODUCT DURING THE WARRANTY PERIOD AND DOES NOT APPLY TO: PRODUCTS DAMAGED DUE TO PHYSICAL ABUSE, MISHANDLING, ACCIDENT, NEGLIGENCE, OR FAILURE TO FOLLOW ALL OPERATING INSTRUCTIONS CONTAINED IN THE OPERATING MANUAL; PRODUCTS WHICH ARE MODIFIED; PRODUCTS WHICH ARE USED IN ANY MANNER OTHER THAN THE MANNER FOR WHICH THEY WERE INTENDED, AS SET FORTH IN THE OPERATING MANUAL; PRODUCTS WHICH ARE DAMAGED OR DEFECTS CAUSED BY THE USE OF UNAUTHORIZED PARTS OR BY UNAUTHORIZED SERVICE; PRODUCTS DAMAGED DUE TO UNSUITABLE OPERATING OR PHYSICAL CONDITIONS DIFFERING FROM THOSE RECOMMENDED IN THE OPERATING MANUAL OR PRODUCT SPECIFICATIONS PROVIDED BY LOGICUBE; ANY PRODUCT WHICH HAS HAD ANY OF ITS SERIAL NUMBERS ALTERED OR REMOVED; OR ANY PRODUCT DAMAGED DUE TO IMPROPER PACKAGING OF THE WARRANTY RETURN TO LOGICUBE. AT LOGICUBE'S OPTION, ANY PRODUCT PROVEN TO BE DEFECTIVE WITHIN THE WARRANTY PERIOD WILL EITHER BE REPAIRED OR REPLACED USING NEW OR REFURBISHED COMPONENTS AT NO COST. THIS WARRANTY IS THE SOLE AND EXCLUSIVE REMEDY FOR DEFECTIVE PRODUCTS. IF A PRODUCT IS HAS BECOME OBSOLETE OR IS NO LONGER SUPPORTED BY LOGICUBE THE PRODUCT MAY BE REPLACED WITH AN EQUIVALENT OR SUCCESSOR PRODUCT AT LOGICUBE'S DISCRETION. THIS WARRANTY EXTENDS ONLY TO THE END PURCHASER OF LOGICUBE PRODUCTS. THIS WARRANTY DOES NOT APPLY TO, AND IS NOT FOR THE BENEFIT OF, RESELLERS OR DISTRIBUTORS OF LOGICUBE PRODUCTS. UNLESS OTHERWISE AGREED IN WRITING BY LOGICUBE, NO WARRANTY IS PROVIDED TO RESELLERS OR DISTRIBUTORS OF LOGICUBE PRODUCTS.
IN ORDER TO RECEIVE WARRANTY SERVICES CONTACT LOGICUBE'S TECHNICAL SUPPORT DEPARTMENT VIA PHONE OR E-MAIL. PRODUCTS RETURNED TO LOGICUBE FOR REPAIR UNDER WARRANTY MUST REFERENCE A LOGICUBE RETURN MATERIAL AUTHORIZATION NUMBER ("RMA"). ANY PRODUCT RECEIVED BY LOGICUBE WITHOUT AN RMA# WILL BE REFUSED AND RETURNED TO PURCHASER. THE PURCHASER MUST CONTACT LOGICUBE'S TECHNICAL SUPPORT DEPARTMENT VIA E-MAIL (SUPPORT@LOGICUBE.COM) OR VIA PHONE AT +1-818-700-8488 OPT. 3 TO OBTAIN A VALID RMA#. THE PURCHASER MAY BE REQUIRED TO PERFORM CERTAIN DIAGNOSTIC TESTS ON A PRODUCT PRIOR TO LOGICUBE ISSUING AN RMA#. THE PURCHASER MUST PROVIDE THE PRODUCT MODEL, SERIAL NUMBER, PURCHASER NAME AND ADDRESS, EMAIL ADDRESS AND A DESCRIPTION OF THE PROBLEM WITH AS MUCH DETAIL AS POSSIBLE. AT LOGICUBE'S SOLE AND ABSOLUTE DISCRETION, REASONABLE TELEPHONE AND EMAIL SUPPORT MAY ALSO BE AVAILABLE FOR THE LIFE OF THE PRODUCT AS DEFINED BY LOGICUBE.

EXCEPT AS OTHERWISE SPECIFICALLY PROVIDED IN THIS AGREEMENT, LOGICUBE PRODUCTS ARE PROVIDED AS-IS AND AS-AVAILABLE, AND LOGICUBE DISCLAIMS ANY AND ALL OTHER WARRANTIES (WHETHER EXPRESS, IMPLIED, OR STATUTORY) INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT OF THIRD PARTY RIGHTS.
SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, OR LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, SO THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION.

RoHS Certificate of Compliance

LOGICUBE PRODUCTS COMPLY WITH THE EUROPEAN UNION RESTRICTION OF THE USE OF CERTAIN HAZARDOUS SUBSTANCES IN ELECTRONIC EQUIPMENT, ROHS DIRECTIVE (2002/95/EC).

THE ROHS DIRECTIVE PROHIBITS THE SALE OF CERTAIN ELECTRONIC EQUIPMENT CONTAINING SOME HAZARDOUS SUBSTANCES SUCH AS MERCURY, LEAD, CADMIUM, HEXAVALENT CHROMIUM AND CERTAIN FLAME-RETARDANTS IN THE EUROPEAN UNION. THIS DIRECTIVE APPLIES TO ELECTRONIC PRODUCTS PLACED ON THE EU MARKET AFTER JULY 1, 2006.

Logicube Technical Support Contact Information

1. By website: www.logicube.com
2. By email: techsupport@logicube.com
3. By telephone: 1 - (818) 700 8488 ext. 3 between the hours of 7am – 5pm PST, Monday through Friday, excluding U.S. legal holidays.

Table of Contents

1: Introduction

1.0 Introduction to the Logicube ZXi-Forensic

Digital forensic labs or organizations that routinely handle large amounts of evidence data for review or analysis can take advantage of the ZXi-Forensic's three Gigabit Ethernet ports, fast imaging speeds of over to 50GB/min* and advanced features to streamline processes. The solution provides a network "Push" feature that allows users to upload images from up to 3 evidence drives directly to a network repository simultaneously. Add the optional 3 drive expansion kit to push up to a total of 5 evidence drives. The ZXi-Forensic's ability to image up to 3 source/suspect drives directly to a network repository and at the same time image to 3 destination/evidence drives (add the expansion kit to image up to 6 destination drives) provides efficiency and quick access to forensic evidence data.

1.1 Features

- **Multi-target, volume imaging**: Image from 3 suspect drives simultaneously to network repositories using 3 Gigabit Ethernet connections; image from 3 source drives directly to 3 destination drives; image from 3 source drives to network repositories and simultaneously image to 3 destination hard drives. Use the optional expansion kit to add 3 additional destinations.
- Supports dd, ex01, e01, or native **imaging formats**. User selectable MD5, SHA-1, or SHA-256 **verification** is available.
- Use the **Network Push feature** to upload evidence drive images that were captured using the Forensic Falcon or the ZXi-Forensic to a network repository. Push from up to 3 evidence drives simultaneously on the base unit or add the optional expansion kit and push from up to 5 evidence drives. An MD5 or SHA-1 hash is performed during the process and a log file is generated for each push task.
- **Image to or from a network location.** Use the ZXi-Forensic to image to a network location using CIFS protocol and/or image from a network location using iSCSI. Users can use iSCSI as a source or destination drive.
- Supports imaging to and from **USB enclosures and USB thumb drives.** 1 USB 3.0 source port and 2 USB 3.0 Destination ports are available.
- **High speed imaging** at over 50GB/min*
- **Write-protected source drives.** All ZXi-Forensic source ports are automatically write-blocked to prevent any alteration to sensitive data on the source drive.
- The ZXi-Forensic has built-in support for 3.5”/2.5” **SAS or SATA** hard drives, 1.8”/2.5”/3.5” **IDE and IDE ZIF** drives, **eSATA**, **microSATA**, **mSATA**, and **CompactFlash** media are supported with optional adapters. The ZXi-Forensic supports SSDs.
- **Optional 3 drive expansion kit** provides an additional 2 SAS/SATA and 1 SATA for a total of **6 SATA or 5 SAS destinations**.
- **Remote Operation**. Connect the ZXi-Forensic to your network and allow remote access from any computer within the same network. **A web-based browser** interface provides easy navigation.
- **Write-blocked preview/triage hard drive contents**. Preview the drive contents directly on the ZXi-Forensic. The file browser feature provides logical access to source or destination drives connected to the ZXi-Forensic. Users can view the drive’s partitions and contents, and view text files, jpeg, PDF, XML, HTML files. Other file types (such as .doc and .xls) can be viewed by connecting the ZXi-Forensic to a network and via a workstation, download and view. Users can also use an iSCSI or SMB protocol to preview source drives via the network.
- **Wipe feature. Sanitizes** hard drives to DoD 7-pass specification, offers Secure Erase and custom pass settings.
- **Network services.** Users can disable various network services (such as HTTP, SSH, Telnet, CIFS/NETBIOS, iSCSI, Iperf, and Ping) for security purposes.

**The Zxi-Forensic achieves speeds of over 50GB/min using solid state "suspect" drives that contain a freshly installed Windows "X" OS and random data. Settings used are e01/ex01 image format, with compression and with verify "on". The specification and condition of the suspect hard drives as well as the mode, image format and settings used during the imaging process may affect the achieved speeds.*

- **Image from a desktop or laptop PC** without removing the hard drive. Create a forensic bootable USB flash drive that allows the user to image a source drive from a computer on the same network without booting the computer's native operating system.
- **Parallel Imaging.** Perform multiple imaging tasks from the same source drive to multiple destinations using different imaging formats. Image (e01, ex01, or dd) to a network location while simultaneously cloning to a destination drive.
- **Concurrent Image+Verify. The** ZXi-Forensic takes advantage of destination drives that are faster than the source drive and begins verification while the imaging process is occurring. Duration of total image plus verification process time may be reduced by up to half.
- The ZXi-Forensic can perform a **forensic, filter-based file copy**. Filter and then image specific file types by file extension such as .pdf, .doc, .jpg, .mov, etc.
- Secure sensitive evidence data with whole drive **AES-256 bit encryption**. Decryption can be performed using the ZXi-Forensic or by using open source software
- **Removable drive stations** are field replaceable.
- **Task Macro** feature. Set specific tasks to be performed sequentially, for example, image from source drives to destination drives and then push to a network repository. Set up your macro, press start, and all tasks within the macro will be performed automatically.
- Features an **Internal, removable storage drive** that stores OS and audit trail/logs. The drive is easily removed for secure/classified locations.
- **Audit Trail/Log files** provide detailed information on each operation. Log files can be viewed on the ZXi-Forensic or via a web browser, exported to XML, HTML, or PDF format to a USB drive. Users can print the log files directly from their PC when connected to ZXi-Forensic via a web browser.
- **Additional features** include HPA/DCO capture, drive "trim" feature to manipulate the DCO and HPA areas of destination drives, the ability to set password-protected user profiles and save configurations, drive "time-out" feature automatically puts drives in stand-by mode after a specified idle time, drive spanning, large 7" color touch screen display, on-screen keyboard, two USB 2.0 host ports for mouse or printer connectivity, a PS/2 keyboard port and an HDMI port to connect a projector or monitor.

1.2 In the Box

The ZXi-Forensic system includes the following:

- The Logicube ZXi-Forensic unit
- Power cable
- 6 SAS/SATA cables
- 3 CAT6 Network cable
- CD-ROM containing the user's manual

1.3 Options

The following options are available for the Forensic ZXi-Forensic:

- 3-target expansion kit (includes 1 SATA only drive station, 2 SATA/SAS drive stations, drive tray, 3 SATA/SAS data/power cables)
- USB to SATA adapter
- 2.5”/3.5” IDE to SATA adapter
- 1.8” IDE to SATA adapter
- 1.8” IDE ZIF to SATA adapter
- 1.8” microSATA adapter
- mSATA to SATA adapter
- eSATA 18” cable
- Flash card reader for compact flash media
- Replacement SAS/SATA cables
- USB cables
- Extended warranties

1.4 Specifications

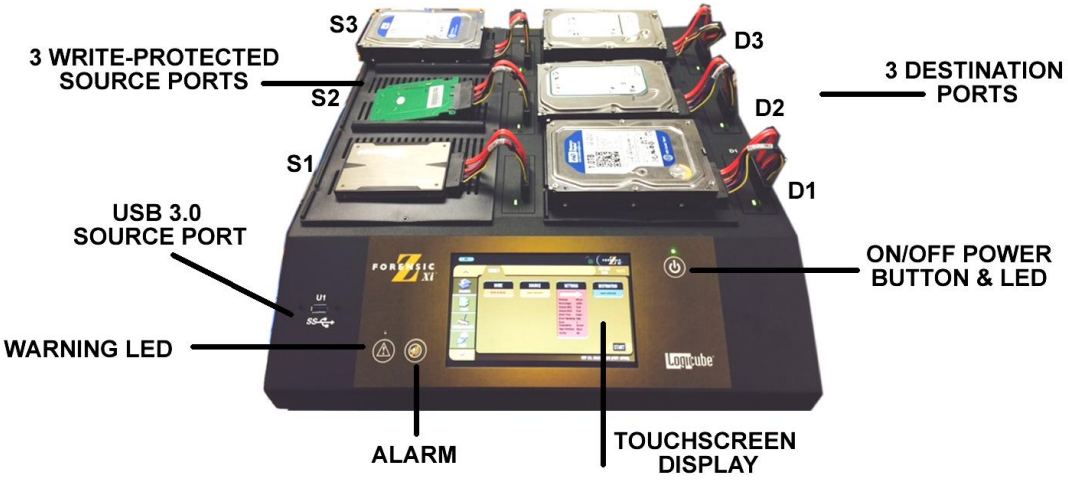
Power Requirements	Operating Temp	Storage Temp	Relative Humidity	Net Weight	Dimensions	Agency Approvals
110-240V 7.5A-3.5A 50-60Hz	32°- +122°F 0° to 50° c	-4 to +176F -20 to +80C	Operatin:g 85% RH, non-condensing Storage: 95% RH, non-condensing	14 lbs 6.4 kg	3.7”H X 19”D X 17.2”W 9.39cm X 48.26cm X 43.68cm	RoHs compliant

WARNINGS:

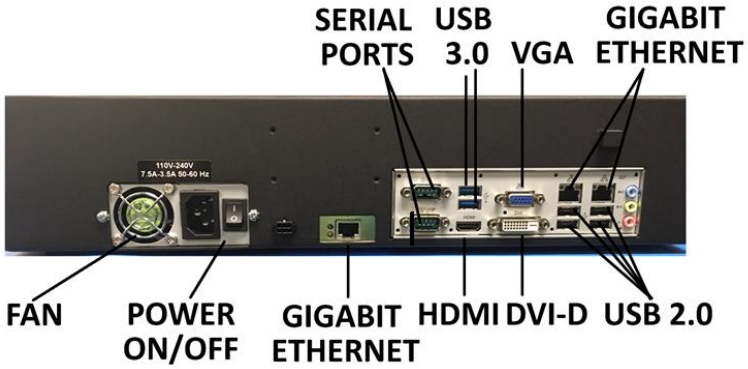
- Never connect a suspect drive to the Destination ports of the Forensic ZXi-Forensic as data may be overwritten.
- Incorrectly connecting the suspect drive to the system can result in data on the suspect drive to be lost forever.
- Avoid dropping the Logicube Forensic ZXi-Forensic or subjecting it to sharp jolts. When in use, place it on a flat surface.
- Keep the unit dry. If the Forensic ZXi-Forensic needs to be cleaned, use a lightly damp, lint free cloth. Avoid using soap or other cleaning agents particularly those containing bleach, ammonia, alcohol or other harsh chemicals.
- Do not attempt to service or open the Logicube Forensic ZXi-Forensic. Doing so may void the warranty. If the unit requires service, please contact Logicube Technical Support for assistance.

Warning and Informational Icons – Throughout this manual, there are two icons that can be seen. Please pay close attention when any of these two icons are found. These icons highlight additional information or important warnings on specific topics.

ZXI-FORENSIC



ZXi-Forensic Rear Panel



ZXi-FORENSIC
LEFT SIDE VIEW

ZXI-FORENSIC WITH OPTIONAL EXPANSION KIT

2.0 Turning the ZXi-Forensic on and off

The ZXi-Forensic comes with a standard power cable that connects to the back of the device. Attach the included power cable the power connector in the back of the ZXi-Forensic.

To turn the ZXi-Forensic on, make sure the power switch (located next to the power connector on the back of the unit) is set to the ON position, then press and release the power button located in front of the device. The ZXi-Forensic will turn on and start the boot process.

> It is normal for the fans to either turn off or slow down after the initial start-up sequence.

There are two ways to turn the ZXi-Forensic off:

- Use the Graphical User Interface (GUI) either on the touch screen or via a browser through a remote connection. Navigate to the ***Power Off*** screen and tap or click the ***Power Off*** icon.
- Press and release the power button located in front of the device.

> It is not recommended to use the power switch to turn the ZXi off. Using the ***Power Off*** icon in the GUI gracefully shuts down the ZXi's Operating System.

2.1 Connecting various drive types

Cables and adapters are available for the following drive types:

- SAS
- SATA
- USB (optional)
- 1.8” microSATA (optional)
- 2.5” and 3.5” PATA/IDE (optional)
- 1.8” ZIF (optional)
- 1.8” PATA/IDE (optional)
- eSATA (optional)
- mSATA (optional)
- Flash Media (optional)

2.1.1 Connecting Source Drives

Source drives (also called suspect drives) must be connected to the left side of the ZXi-Forensic. There are a total of four write-protected Source ports:

- S1 – SAS/SATA located front left
- S2 – SAS/SATA located middle left
- S3 – SAS/SATA located back/far left
- U1 – front USB 3.0

Any combination of drives can be connected, up to 4 Source drives. Source drives do not have to be connected in any order. For example, a single SATA Source drive does not have to be connected to the S1 port. It can be connected to the S2 port without having anything connected to the S1 port.

Never connect a suspect or Source drive to the Destination ports of the ZXi-Forensic. Data may be overwritten if a drive is connected to a Destination port.

2.1.2 Connecting Destination Drives

Destination drives (also called evidence drives) must be connected to the right side of the ZXi-Forensic (or to the rear USB 3.0 ports). These ports are labeled as follows:

- D1 – SAS/SATA located front right
- D2 – SAS/SATA located middle right
- D3 – SAS/SATA located back/far right
- U2 – Top Rear USB 3.0
- U3 – Bottom Rear USB 3.0

Any combination of drives can be connected, up to 5 Destination drives (8 with expansion kit). Destination drives do not have to be connected in order. For example, a single SATA Destination drive does not have to be connected to the D1 port. It can be connected to the D2 port without having anything connected to the D1 port.

The ZXi-Forensic ports are hot swappable. Drives that are not being used in any task (image, hash, wipe, etc.) can be disconnected any time.

Some drives are not hot swappable. Please check with the drive manufacturer to find out if the drive being used does not support hot swapping.

When disconnecting drives, it is very important to make sure the drives are not being used on any task. Disconnecting drives while the ZXi-Forensic is using the drive for a task may cause data loss.

2.1.3 Connecting USB 3.0 Drives

USB 3.0 is a new technology and USB 3.0 controller manufacturers may have variations in device designs that have inconsistent adherence to USB 3.0 specification. This may result in non-detection of the USB 3.0 device on certain equipment (including desktops, laptops or the ZXi-Forensic). If a USB 3.0 device cannot be detected on the ZXi-Forensic USB ports we have found that using a USB 3.0 hub may stabilize and regulate the communication between the USB 3.0 device and the ZXi-Forensic, allowing the device to be detected properly. We have identified and qualified a USB 3.0 hub which is available as an option. For more information on the USB 3.0 hub, please see **Section 9.5**.

2.1.4 Using USB/eSATA enclosures

When using USB or eSATA enclosures, it is highly recommended to leave the drive inside the enclosure. USB enclosures typically have an on-board controller that may be necessary to read the drive properly. Taking the drive out of the enclosure could cause any device (including computers) not to read the drive contents properly.

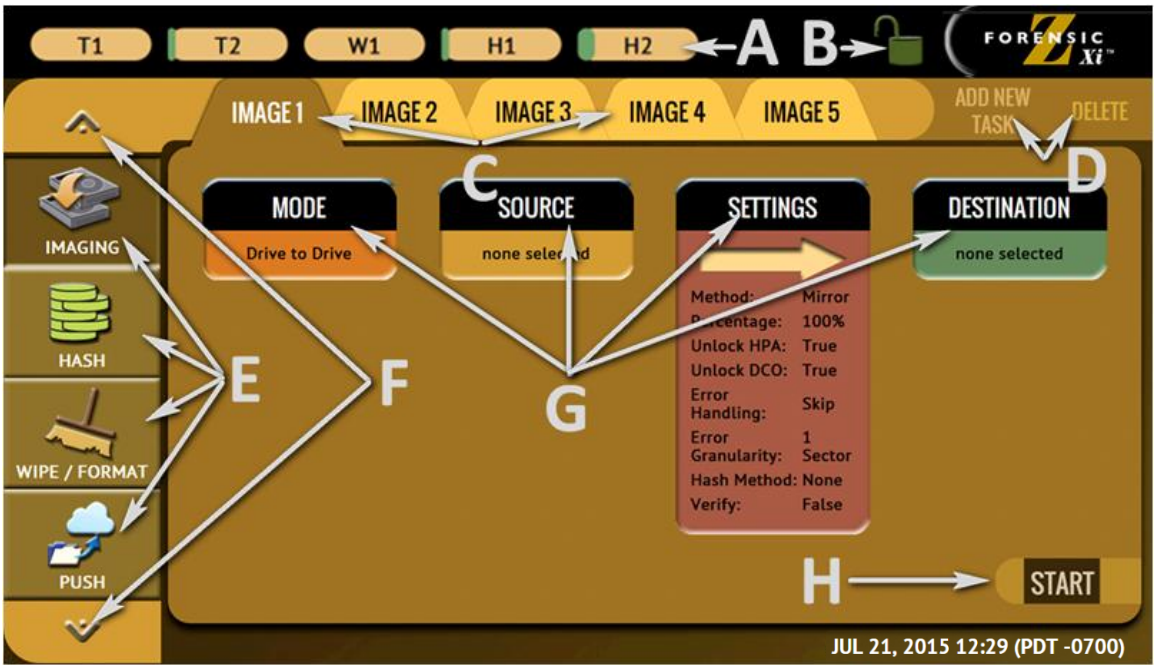
2.1.5 Connecting SATA Drives using a USB-to-SATA adapter

Logicube has qualified a USB 3.0 to SATA adapter for use with the ZXi-Forensic. This adapter provides the capability to connect SATA drives to the USB 3.0 ports on the ZXi-Forensic and uses a USB 3.0 to SATA converter. USB 3.0 is a new technology and USB 3.0 controller manufacturers may have variations in device designs that have inconsistent adherence to USB 3.0 specifications. This adapter and other USB 3.0 enclosures may experience communication disruption between devices. If the adapter is not detected properly we have found that using a USB 3.0 hub may stabilize and regulate the communication between the Adapter or USB 3.0 enclosure, and the ZXi-Forensic, allowing the device to be detected properly. We have identified and qualified a USB 3.0 hub which is

available as an option. For more information on the USB 3.0 to SATA adapter, please see **Section 9.4**. For more information on the USB 3.0 hub, please see **Section 9.5**.

2.2 The user interface

The user interface (UI) has been designed to quickly and easily input commands. It is simple and intuitive showing common icons such as tasks, modes of operation, and scroll icons on the screen. The UI is designed to be easily followed, going from left to right across the screen.



A – Operations/Tasks currently running (displays up to 5 total tasks)

B – Lock indicator/shortcut

C – Operations/Tasks

D – Add or delete tasks

E – Types of Operations

F – Up and down scroll arrows

G – Operations options and settings

H – Start icon

2.3 Touch screen

The ZXi-Forensic features a 7” color LCD capacitive touch screen that allows the user to quickly input commands. The screen is bright and easy to read.

3: Quick Start

3.0 Quick Start Guide – Networking Setup and Imaging

This chapter gives an overview and steps on how to perform Imaging tasks to a network location/repository.

> Complete details on other operations and the different screens can be found in **Chapter 4: Imaging** and **Chapter 5: Types of Operation**.

The ZXi-Forensic comes with three Gigabit Ethernet ports which allow the ZXi-Forensic to image Source drives to up to three network repositories at the same time.

The ZXi-Forensic can also image to 3 Destination drives connected directly to the ZXi (3 additional Destination ports are available with an optional expansion kit).

It can also image to different multiple Destinations at the same time (e.g. From Source S1 to Destination D1 and to a network repository), and with Parallel imaging, the output for each Destination can be different. For example, you can image to E01 format to a network repository and to DD format to a Destination drive on D1 all in the same task.

This chapter will show how to set up the ZXi-Forensic to be used with a network repository (network location, shared folder, NAS, etc.) along with how to perform imaging and push tasks.

- **NETWORK REPOSITORY SETUP**
- **IMAGING**
- **PUSH**

3.1 Network Repository Setup

For the initial setup, it is recommended to reboot the ZXi-Forensic or turn it on without changing any other setting. A repository (network location, shared folder, NAS, etc.) must be configured on the ZXi-Forensic so images can be created, saved, or pushed to the repository.

There are two main steps required:

1. Configure the network repository.
2. Save the current configuration so that the repository can be accessible on future sessions.

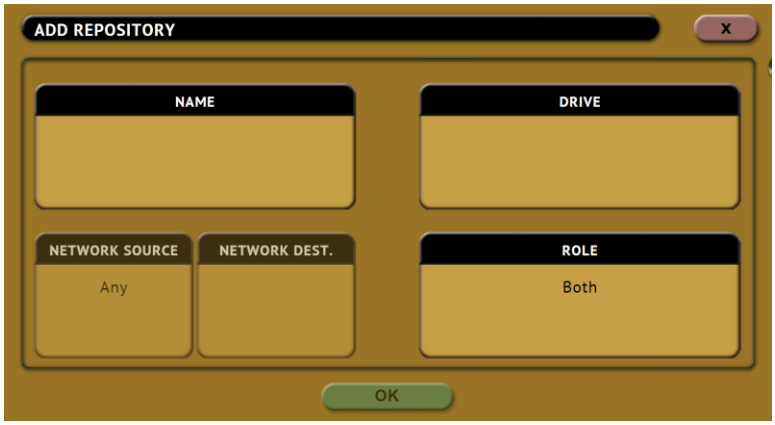
Networks are configured differently and may require the assistance of a Network or Systems Administrator.

3.1.1 Configuring a Network Repository – CIFS & SMB

To configure a CIFS or SMB share as a network repository, the following information is needed:

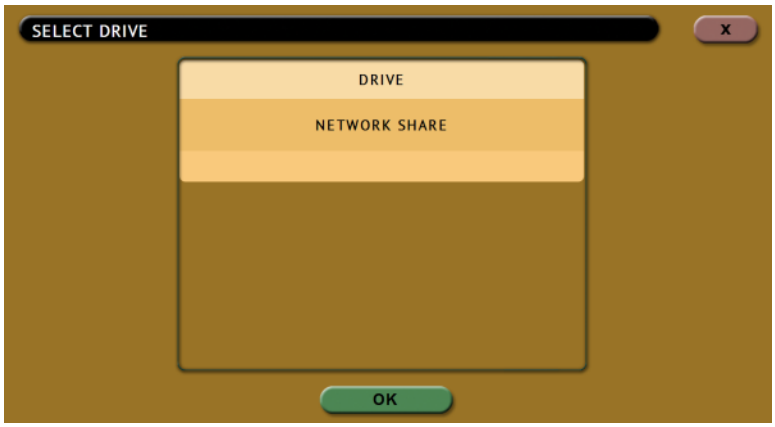
- The directory or folder's shared path and name
- A username and password with full access/rights to the shared directory/folder.
- Whether the repository is on domain or a workgroup

1. From the list of operations on the left side, navigate to ***Manage Repositories***.
2. Tap ***Add Repository***. The Add Repository window will appear.



3. Tap ***Name*** to set the name of the repository. Tap the ***OK*** icon when finished.

4. Tap ***Drive*** then tap ***Network Share*** set a network share as a repository. Tap the ***OK*** icon when finished.



5. Tap ***Network Source*** to specify which Ethernet port to use for this repository. Tap the ***OK*** icon when finished.

ETH0 is the port furthest from the edge (by itself). ETH1 is the middle port, and ETH2 is the port closest to the back left edge.

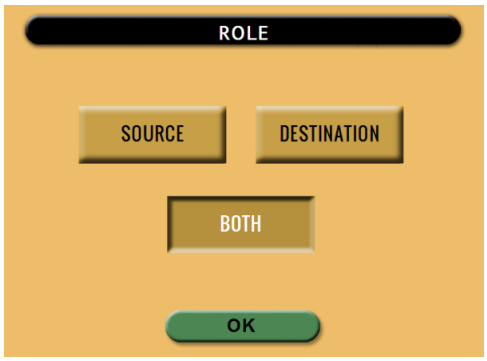
6. Tap ***Network Dest.*** to enter the network settings. See the example below. Tap the ***OK*** icon when finished.

For the path, enter the IP address or hostname followed by a slash (/) then the share name. For example: ***ip_or_hostname/sharename***

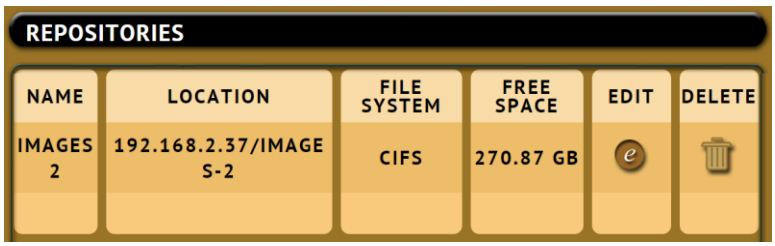
It is recommended to use the IP address instead of host name when the repository (computer, server, or NAS for example) has multiple Ethernet ports that can be accessed by the ZXi-Forensic.

Hidden Samba network shares (shares ending with $ can be mounted by adding the $ at the end of the share name. For example: ***ip_or_hostname/sharename$***

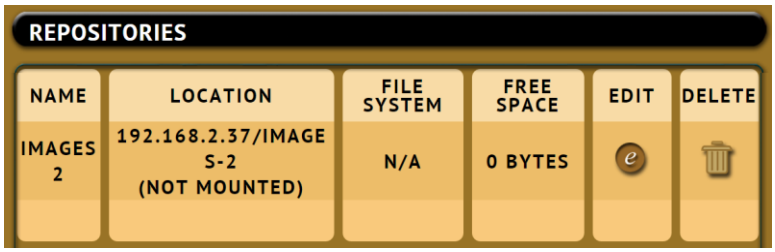
7. Tap ***Role*** and input the role for this repository. Tap ***OK*** when finished.



Below is an example of a properly configured repository:



If the repository is not configured properly, the location will show **(NOT MOUNTED)**.

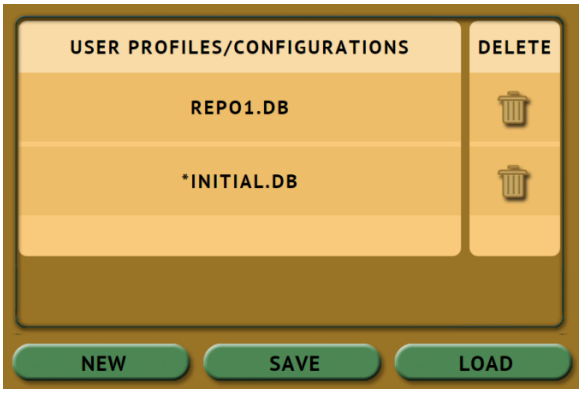


8. Repeat steps 2 through 7 to add additional repositories.

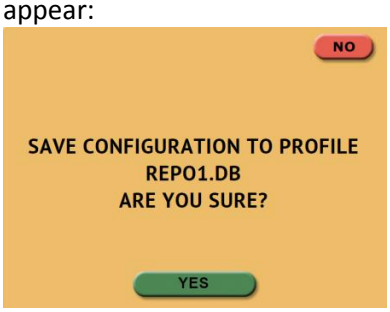
3.1.2 Saving the configured repository

Now that the repository (or repositories) has been set, the repository (or repositories) needs to be saved to a profile/configuration so that each time the ZXi-Forensic is turned on, the repositories will already be configured. The steps below show how to save and load a profile/configuration:

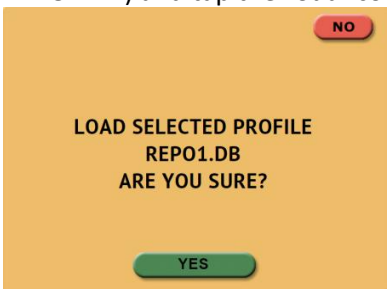
1. From the list of operations on the left side, navigate to ***System Settings***.
2. In the ***User Profiles/Configurations*** tab, tap the ***New*** icon.
3. Type a name for this profile. For example, ***repo1*** and tap the ***OK*** icon. The profile name should appear on the screen.



4. Tap the newly saved profile and tap ***Save***. A confirmation screen will appear:



5. Tap the ***Yes*** icon to save the profile.
6. Make sure the profile to be loaded is highlighted (in this case, REPO1.DB) and tap the ***Load*** icon. A confirmation screen will appear:



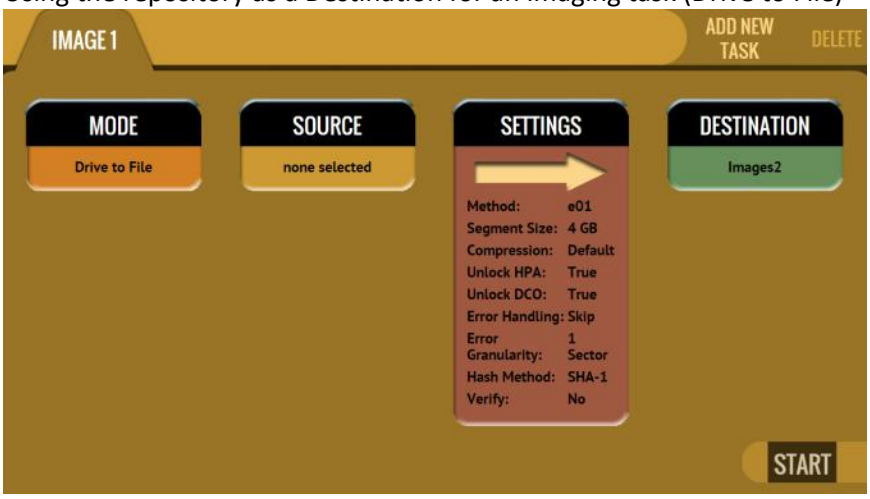
7. The next time the ZXi-Forensic is turned on it will load the REPO1.DB profile and will contain the repository (or repositories) that were configured and saved.

Do not highlight and save over the INITIAL.DB configuration. This is the default configuration of the ZXi-Forensic and is used to reset the ZXi-Forensic to the factory default settings.

3.1.3 Using the repositories

The repositories can now be used as a Destination. The two typical operations that use the repositories are seen below. Details on each of these can be found in the next sections: **Section 3.2** and **Section 3.3**.

- Using the repository as a Destination for an Imaging task (Drive to File)



- As a Destination for a Push task

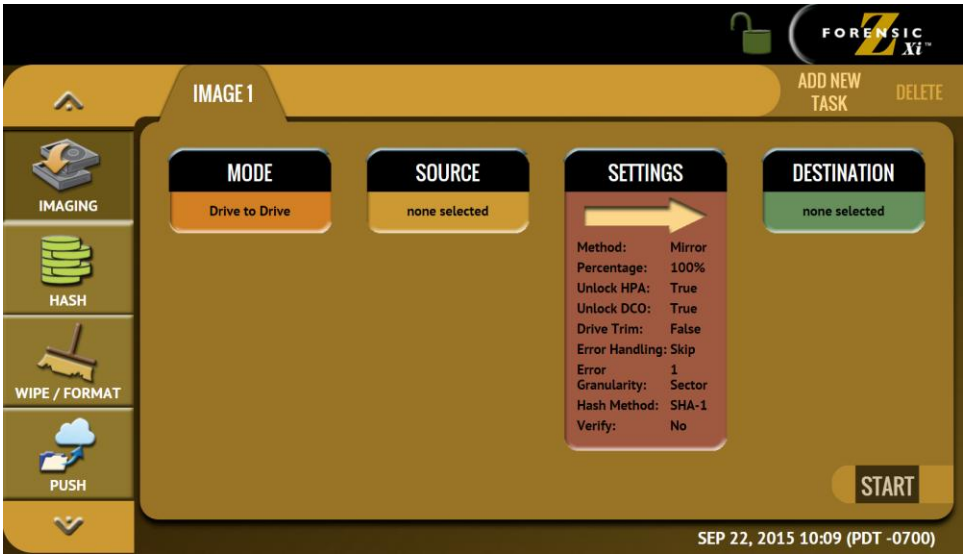
3.2 Imaging

This type of operation allows the imaging of a Source drive to one or more Destinations. There are three (3) different imaging modes and several settings to choose from:

- **Drive to Drive** – Performs a bit-for-bit copy of the Source producing an exact duplicate of the Source drive. This is also known as a native copy or mirror copy.
- **Drive to File** – Images the Source to any of the following image output file formats: ***DD***, ***E01***, or ***EX01***. Compression is available for E01 and EX01 formats.
- **File to File** – Image specific files (by filename or extension). The files will be sorted by path (based on where the file is located on the Source). If a hash method is selected, each file will be hashed.

This section shows how to perform an E01, EX01, or DD image from Source drives to a network repository using ***Drive to File***.

3.2.1 Step-by-step instructions – Imaging



1. Select ***Imaging*** from the types of operation on the left side.
2. Tap the ***Mode*** icon and select ***Drive to File*** then tap the ***OK*** icon.
3. Tap the ***Source*** icon and choose the source from the list of connected drives then tap the ***OK*** icon.

> All drives connected to S1, S2, S3, and U1 will appear in the ***Source*** window.

4. Tap the ***Settings*** icon and adjust the settings as needed (*Case Info*, *File Image Method Settings or Mirror Settings*, *HPA/DCO*, *Error Handling*, *Hash/Verification Method*, *etc.*) then tap the *OK* icon.

- **CASE INFO –** CASE INFO allows users to enter information about the case. This is optional and is not required to start an imaging operation.

  Information entered here will appear in the logs. In addition, some forensic analysis software can import the information when the image files are opened.

  Tap any of the boxes and an on-screen keyboard will appear allowing information to be entered. After entering the information, tap the ***OK*** icon to go back to the previous screen.

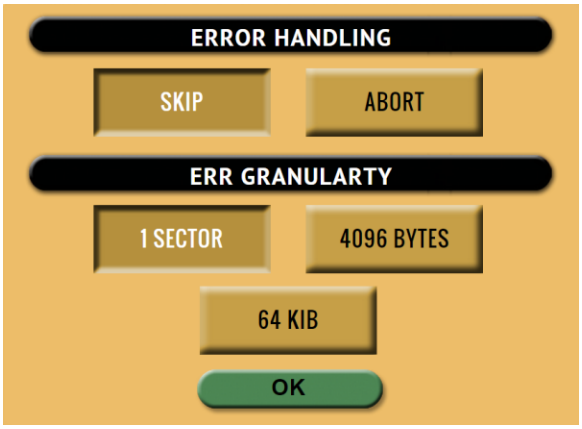
Log names and file names can be customized by entering a ***Case/File Name***. For example, if a DD or E01 image is performed, and the Case/File Name is set to ***TestCase***, the log name and file name will be called ***TestCase***. Subsequent Case/File Names that are the same will be identified with a dash, then the next image number, for example, TestCase-1, TestCase-2, etc.

The ZXi-Forensic will convert any non-POSIX portable characters used in ***Case/File Name*** field to underscores "_" when creating the log or file names.

POSIX portable characters are:

Uppercase A to Z	Period (.)
Lowercase a to z	Underscore (_)
Numbers 0 to 9	Hyphen/Dash (-)

- **FILE IMAGE METHOD SETTINGS –** There are up to 3 settings to choose from:
  - **METHOD**
    - DD
    - E01
    - EX01
  - **SEGMENT SIZE**
    - 2 GB
    - 4 GB
    - 8 GB
    - 16 GB
    - Whole Disk (DD only)
  - **COMPRESSION** (E01 & EX01 only)
- **HPA/DCO/TRIM –** By default, the ZXi-Forensic will unlock and image any HPA and/or DCO on the Source drive(s). TRIM is only available when using Drive to Drive mode.
- **ERROR HANDLING –** When bad sectors are encountered on the Source drive, ZXi-Forensic can either skip the bad sectors or abort the imaging operation. This allows flexibility on what to do when bad sectors are found on the Source drive.



When bad sectors are encountered, and error handling is set to ***Skip***, a zero on the corresponding sector or position will be written on the Destination drive or file.

ZXi-Forensic also has a setting for error granularity. There are 3 options:

- 1 sector (512 Bytes)
- 4096 Bytes (8 sectors)
- 64 KIB (128 sectors)

When a bad sector on the source drive is found, by default, it will skip that sector. Changing the granularity allows more sectors to be skipped.

A cluster size represents the smallest amount of disk space that can be used to hold a file. The most common cluster size for an NTFS volume, for example, is 4KB (4096 Bytes). This means that the smallest amount of space that will be used for a file is 4096 Bytes.

As an example, if 4096 Bytes is chosen, and one of the 8 sectors in that cluster size contains a bad sector, the ZXi-Forensic will skip the entire cluster (or 4096 bytes or 8 sectors).

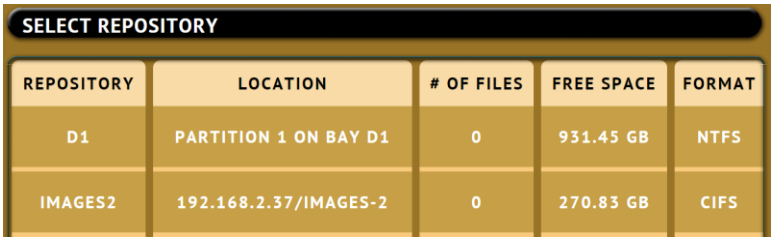
- **HASH/VERIFICATION METHOD -** This setting allows the user to set a hash and/or a verification method. The ZXi-Forensic will hash the Source drive with the selected method. There are several hash algorithm options available, depending on which mode is selected:

  - **None –** No hash of the Source will be performed.
  - **SHA-1 –** Uses the SHA-1 algorithm to hash the Source.
  - **SHA-256 –** Uses the SHA-256 algorithm to hash the Source. This is only available when using the Drive to Drive Imaging mode.
  - **MD5 –** Uses the MD5 algorithm to hash the Source.

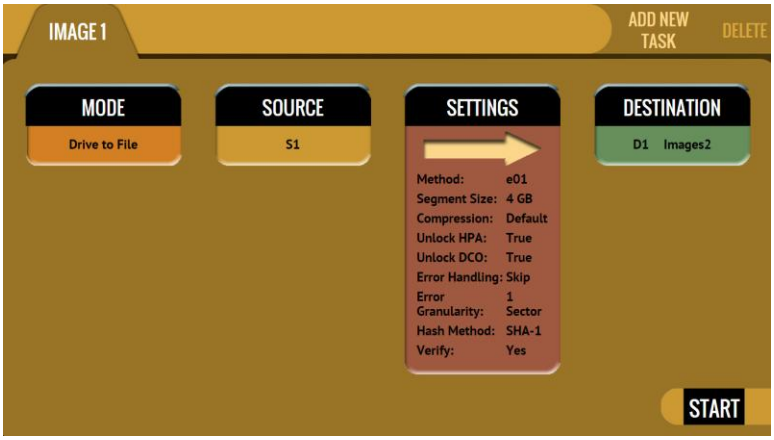
Verification Method – Select ***YES*** to hash the Destination and verify that hash with the selected Source hash.

5. Tap the ***Destination*** icon and select the destination(s) to be used then tap the ***OK*** icon. Any repository previously set up will appear on this screen.

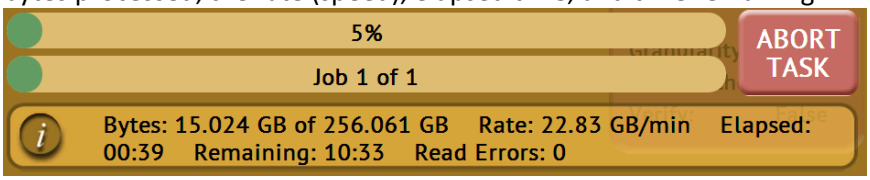
   More than one Destination can be selected. For example, a Destination drive on bay D1 and the repository can both be selected.



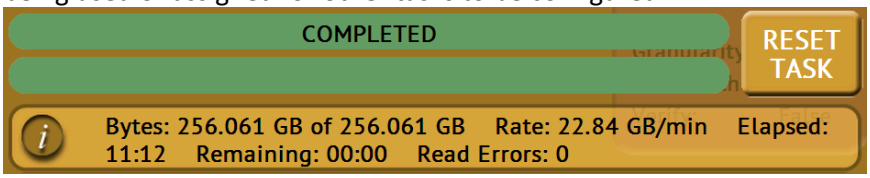
6. When ready, the Imaging screen should look like the following:



7. Tap the ***Start*** icon to start the imaging task.
8. A progress bar will appear at the bottom of the screen showing the bytes processed, the rate (speed), elapsed time, and time remaining.



9. When finished, the status will show "COMPLETED". At this point, it is recommended to tap ***Reset Task*** to reset the task, and also to delete the task in order for the drive bays to be properly reset and not show as being used or assigned for other tasks to be configured.



The number of bytes shown on the progress bar is not the actual size of the drive. This is the actual data being processed. When 'Verify' is set to "Yes", the reported number will double in size.

3.3 Push

The network Push operation gives users the ability to push ZXi-Forensic (or Forensic Falcon) created evidence files from destination drives connected to the ZXi-Forensic to a network location/repository.

The Push feature provides a more secure method than simply copying files through a computer by performing an SHA-1 or MD5 hash during the push process. Additionally users can select to verify the file transfer to ensure data integrity. The ZXi-Forensic will generate a log file for each push process.

3.3.1 Step-by-step instructions - Push

Follow these steps to set up a Push operation:

1. Select ***Push*** from the types of operation on the left side.
2. Tap the ***Source*** icon and select the drive that contains the files to be pushed then tap the ***OK*** icon.

   The Source selection will only show drives connected to the Destination ports, or locations set up as a repository.

3. A 'Select Cases' screen will appear showing each case name located on the selected source. Select one or more cases by tapping each case name. When finished, tap the ***OK*** icon.
4. Tap the ***Settings*** icon to select the hash method or algorithm. Choose from NONE, SHA-1, or MD5 and choose whether to verify the data or not (YES or NO). Tap the ***OK*** icon to continue.
5. Optional: Tap ***Case Info*** to set the Case/File Name, Case ID, Examiner, Evidence ID, or Case Notes.
6. Verify the settings then tap the ***OK*** icon to continue.
7. Tap the ***Destination*** icon and select the destination or repository to push the images to. Tap the ***OK*** icon to continue. Only one Destination can be selected when using the Push operation.
8. Tap the ***Start*** icon to start the push task.
9. When finished, the status will show "COMPLETED". At this point, it is recommended to tap Reset Task to reset the task, and also to delete the task in order for the drive bays to be properly reset and not show as being used or assigned for other tasks to be configured.

Push speeds will vary depending on network conditions.

4: IMAGING

4.0 Imaging

This type of operation allows the imaging of a Source drive to a Destination. There are three different imaging modes and several settings to choose from. These selections should be performed in order from left to right.

There are four selections when performing an image:

- Mode
- Source
- Settings
- Destination

4.0.1 Mode

Tap this icon to choose between the following three imaging modes:

- **Drive to Drive –** Performs a bit-for-bit copy of the Source producing an exact duplicate of the Source drive.

- **Drive to File –** Images the Source to any of the following image output file formats: ***DD***, ***E01***, or ***EX01***. Compression is available for E01 and EX01 modes.
- **File to File –** Image specific files (by filename, extension, etc.). The files will be sorted by path (based on where the file is located on the Source. If a hash method is selected, each file will be hashed.

4.0.2 Source

SOURCE

Tap this icon to select the Source drive to be imaged. ZXi-Forensic will list all the drives connected to the Source position(s).

When ***Drive to Drive*** or ***Drive to File*** mode is selected, the Source window will show all drives connected to the Source positions.

When ***File to File*** mode is selected, the Source window will show all drives connected to the Source positions and any repository added with the Source role (Source or Both Source and Destination).

The ***(More Info)*** icon displays more information on the drive. The drive details window will appear showing information about the drive.

4.0.3 Settings

SETTINGS

Tap the ***Settings*** icon to change the image settings. Depending on what Mode was selected (Drive to Drive, Drive to File, or File to File), different screens will appear.

COMMON SETTINGS – The following settings are found on all three modes:

- Case Info
- HPA/DCO
- Error Handling / Error Granularity
- Hash/Verification Method

SHA-256 verification is only available when using ***Drive to Drive*** mode.

4.0.3.1 Case Info (Common Setting)

Case Info allows users to enter information about the case. This is optional and is not required to start an imaging operation.

Information entered here will appear in the logs. In addition, some forensic analysis software can import the information when the image files are opened.

Tap any of the boxes and an on-screen keyboard will appear allowing information to be entered. After entering the information, tap the ***OK*** icon to go back to the previous screen.

Log names and file names can be customized by entering a ***Case/File Name***. For example, if a DD or E01 image is performed, and the Case/File Name is set to ***TestCase***, the log name and file name will be called ***TestCase***. Subsequent Case/File Names that are the same will be identified with a dash, then the next image number, for example, TestCase-1, TestCase-2, etc.

The ZXi-Forensic will convert any non-POSIX portable characters used in ***Case/File Name*** field to underscores "_" when creating the log or file names.

POSIX portable characters are:

Uppercase A to Z	Period (.)
Lowercase a to z	Underscore (_)
Numbers 0 to 9	Hyphen/Dash (-)

4.0.3.2 HPA, DCO (Common Setting) and Drive Trim

Some computer manufacturers will use a utility that creates an HPA or DCO configuration on a hard drive. These configurations are designed to change drive characteristics such as drive capacity, speed and other settings as they are reported to the computer's BIOS.

The HPA/DCO setting allows the user to set whether a drive's HPA or DCO is to be unlocked and imaged.

Select ***YES*** to unlock and image a Host Protected Area (HPA) or Device Configuration Overlay (DCO).

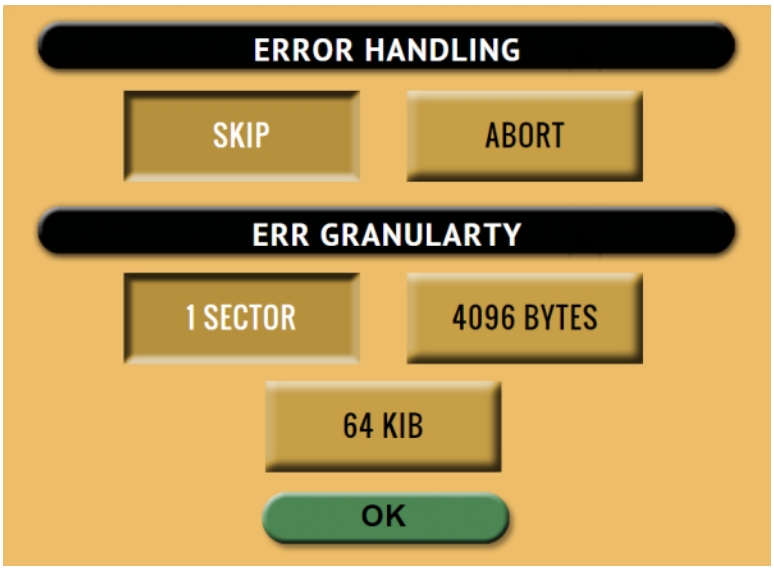
HPA – Host Protected Area can limit the size of a hard drive, but it can also change many other settings such as speed and S.M.A.R.T. status.

DCO – Device Configuration Overlay limits the size of a drive only. For example, a 160GB drive can be made to look like a 100GB drive to a computer.

Drive Trim is a special setting when the mode is set to Drive to Drive. For more information on Drive Trim, please see ***section 4.0.3.5.1 Special Settings for Drive to Drive***.

4.0.3.3 Error Handling (Common Setting)

When bad sectors are encountered on the Source drive, ZXi-Forensic can either skip the bad sectors or abort the imaging operation. This allows flexibility on what to do when bad sectors are found on the Source drive.



When bad sectors are encountered, and error handling is set to ***Skip***, a zero on the corresponding sector or position will be written on the Destination drive or file.

ZXi-Forensic also has a setting for error granularity. There are 3 options:

- 1 sector (512 Bytes)
- 4096 Bytes (8 sectors)
- 64 KIB (128 sectors)

When a bad sector on the source drive is found, by default, it will skip that sector. Changing the granularity allows more sectors to be skipped.

A cluster size represents the smallest amount of disk space that can be used to hold a file. The most common cluster size for an NTFS volume, for example, is 4KB (4096 Bytes). This means that the smallest amount of space that will be used for a file is 4096 Bytes.

As an example, if 4096 Bytes is chosen, and one of the 8 sectors in that cluster size contains a bad sector, the ZXi-Forensic will skip the entire cluster (or 4096 bytes or 8 sectors).

4.0.3.4 Hash/Verification Method (Common Setting)

This setting allows the user to set a hash and/or a verification method.

Hash – Will hash the Source drive with the selected method. There are two, three, or four hash algorithm options available,

depending on which Imaging mode or File Image Method is selected:

- **None –** No hash of the Source will be performed.
- **SHA-1 –** Uses the SHA-1 algorithm to hash the Source.
- **SHA-256 –** Uses the SHA-256 algorithm to hash the Source. This is only available when using the Drive to Drive Imaging mode.
- **MD5 –** Uses the MD5 algorithm to hash the Source.

Verification Method – Select ***YES*** to hash the Destination and verify that hash with the selected Source hash.

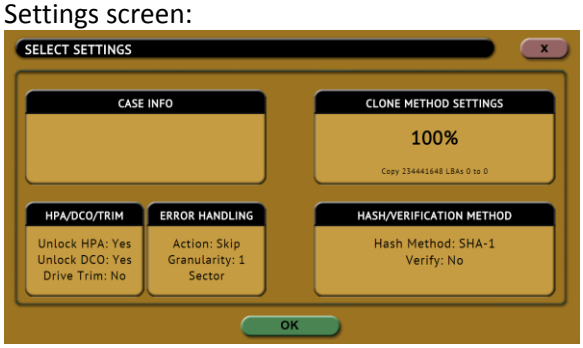
4.0.3.5 Special Settings

The Settings screen changes depending on which of the three ***Modes*** (Drive to Drive, Drive to File, or File to File) is selected. Each of the three modes has their own different ***Settings*** screen.

4.0.3.5.1 Special Settings for Drive to Drive

When ***Drive to Drive*** mode is selected, ***Mirror Settings*** will appear on the top-right of the

Settings screen:



DRIVE TRIM – This user selectable function allows the ZXi-Forensic to manipulate the Device Configuration Overlay (DCO) and Host Protected Area (HPA) of the destination drive using the *Device Configuration Set* command for DCO and *Set Max Address* command for HPA so that the Destination drive's total native capacity matches the Source drive. For example, if the Source drive is a 120GB drive and the Destination drive is a 500GB drive, the ZXi-Forensic will limit the Destination drive's capacity to 120GB to match the Source drive exactly.

SAMPLE SOURCE DRIVE:

Bay:	
Role:	Master
Model:	KINGSTON_SH103S3120G
SerialNumber:	50026B733200CA0C
Size:	120034123776
PhysicalSectors:	234441648
LogicalSectors:	234441648
LogicalSectorsSize:	512
Cylinders:	14593
Heads:	255
Sectors:	63

SAMPLE DESTINATION DRIVE PRIOR TO DRIVE TRIM:

Bay:	
Role:	Target
Model:	WDC_WD10EZEX-08M2NA0
SerialNumber:	WD-WCC3F0914869
Size:	1000204886016
PhysicalSectors:	1953525168
LogicalSectors:	1953525168
LogicalSectorsSize:	512
Cylinders:	56065
Heads:	255
Sectors:	63

SAMPLE DESTINATION DRIVE AFTER DRIVE TRIM:

Bay:	
Role:	Target
Model:	WDC_WD10EZEX-08M2NA0
SerialNumber:	WD-WCC3F0914869
Size:	120034123776
PhysicalSectors:	234441648
LogicalSectors:	234441648
LogicalSectorsSize:	512
Cylinders:	14593
Heads:	255
Sectors:	63

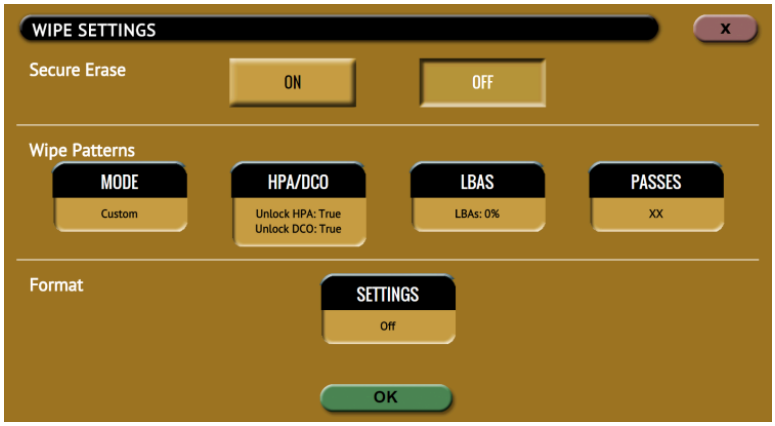
Drive Trim is only available in ***Drive to Drive*** mode and by default is set to ***NO***.

Drive Trim only works with ATA drives and will not work with USB external drives (or drives connected via USB), SAS or SCSI drives.

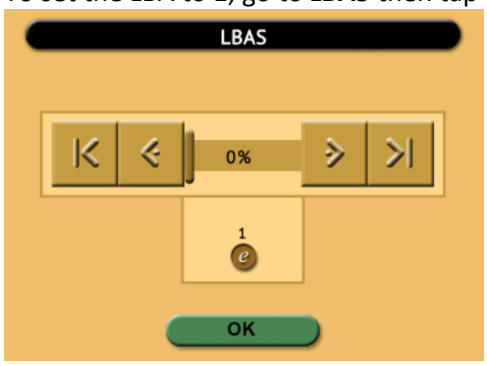
Restoring a trimmed drive – To restore a trimmed drive to its original capacity, perform a custom wipe (single pass) and set the WIPE DCO and WIPE HPA settings to YES.

RESTORING A TRIMMED DRIVE:

1. Navigate to the Wipe/Format mode of operation.
2. Select the drive to restore.
3. In the Wipe Settings:
   a. Set Secure Erase to OFF
   b. Set Wipe Patterns to:
      - Mode: Custom
      - HPA/DCO: YES (TRUE)
      - LBAS: Edit to 1 LBA
      - PASSES: Edit the number of passes to any value for 1 pass

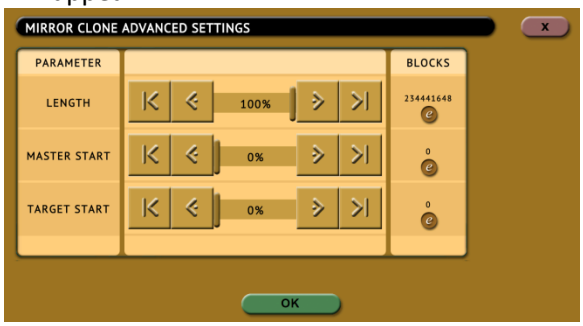


To set the LBA to 1, go to ***LBAS*** then tap the edit icon and enter the value: 1



Start the wipe task. The task should finish quickly as it is resetting just wiping the HPA/DCO and 1 LBA.

Tap ***Mirror Settings*** and the following screen will appear:

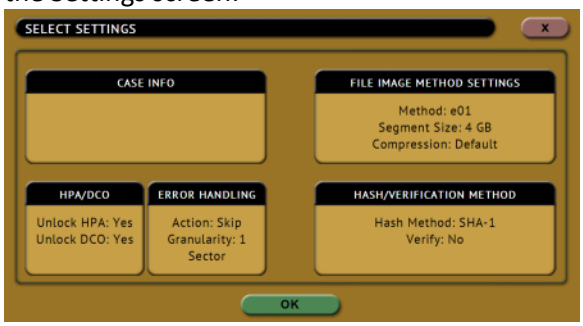


- **Length –** Set the percentage or number of blocks to clone. For forensic purposes, this is typically set to 100% of the Source.
- **Master Start –** Set the percentage or number of blocks from the start of the Source (Master). For forensic purposes, this is typically set to 0%, or the beginning of the Source (Master).
- **Target Start** – Set the percentage or number of blocks from the start of the Destination (Target). For forensic purposes, this is typically set to 0%, or the beginning of the Destination (Target).

Alternatively, the specific number of blocks can be set for each of the options by tapping the: ***(edit)*** icon.

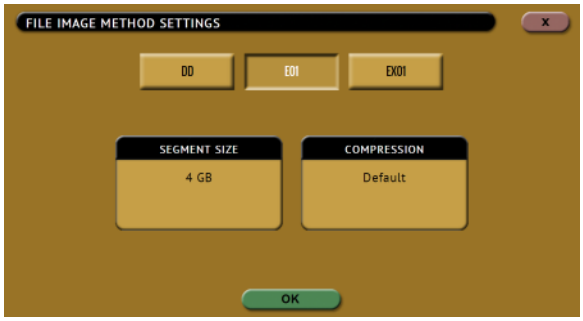
4.0.3.5.2 Special Settings for Drive to File

When ***Drive to File*** mode is selected, ***File Image Method Settings*** will appear on the top-right of the Settings screen:



Tap ***File Image Method Settings*** and the following screen will appear when DD is selected:

The following screen will appear when E01 or EX01 is selected:



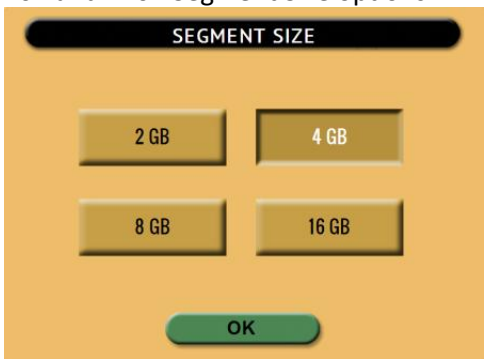
One of three different images methods can be selected:

- **DD –** Uncompressed raw image files readable by many forensic programs.
- **E01 –** Compressed or uncompressed EnCase legacy evidence file format.

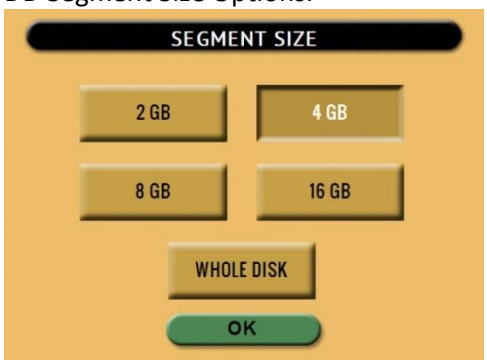
- **EX01 –** Compressed or uncompressed EnCase evidence file format.

SEGMENT SIZE – Available for DD, E01, and EX01. Allows the user to set the output segment size (file size). Choose from **2 GB**, **4 GB**, **8 GB**, **or 16 GB**. A **Whole Disk** option is available for DD only.

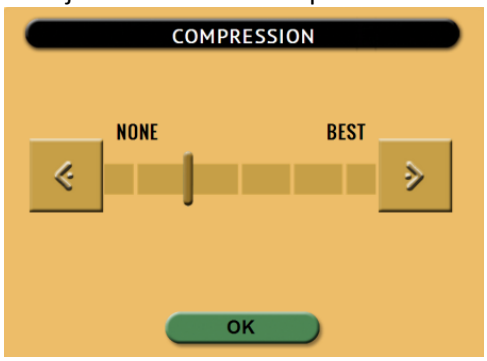
E01 and EX01 Segment Size options:



DD Segment Size Options:

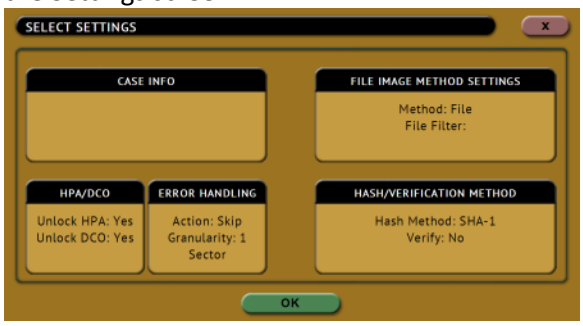


COMPRESSION – Available for E01 and EX01 only. Sets the compression level for E01 or EX01 imaging. When selecting Compression, the following screen will appear. Use the slider bar to adjust the desired compression level.

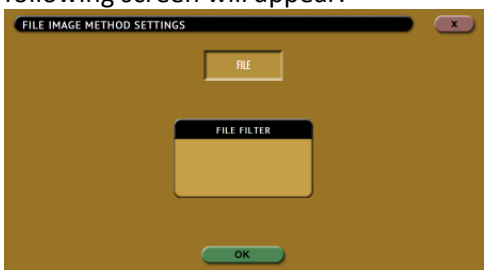


4.0.3.5.3 Special Settings for File to File

When File to File mode is selected, ***File Image Method Settings*** will appear on the top-right of the Settings screen:



Tap ***File Image Method Settings*** and the following screen will appear:



Tap ***File Filter*** to input the filter. Input the file extension filter desired, for example: ***.jpg***.

Multiple files can be specified by using a comma and no spaces, for example, ***.jpg,.zip,.mov,.mp3***

4.0.4 Destination / Image File

Tap the Destination or Image File icon to select the Destination drive or Image File. ZXi-Forensic will list all the drives connected to the Destination position(s) and any repository configured as a Destination. When ***Drive to Drive*** mode is selected, the Destination screen will show all drives connected to the Destination positions.

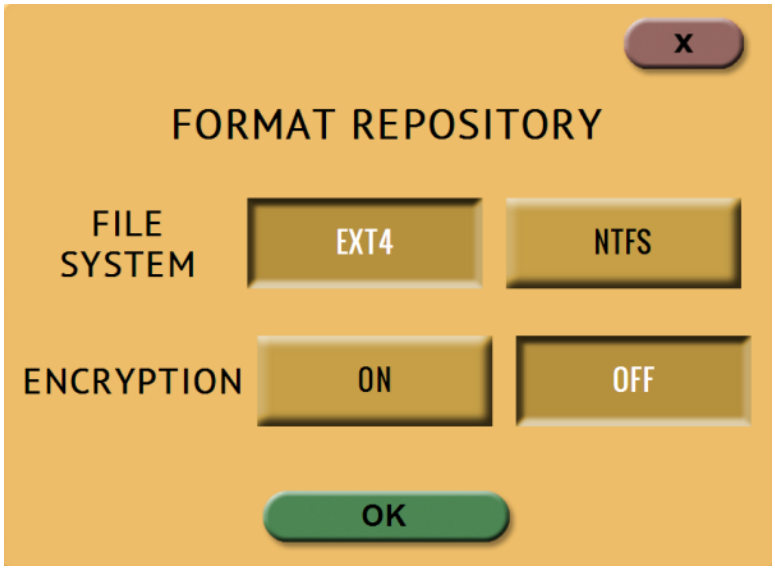
When ***Drive to File*** or ***File to File*** mode is selected, the Destination screen will show all drives connected to the Destination positions and any repository added with the Destination role (Destination or Both Source and Destination).

For DD, E01, Ex01, and File to File mode, the ZXi-Forensic uses the EXT4 file system or NT file system (NTFS) to format drives. If the Destination drive is not formatted properly, the ***Location*** will appear as "***(NOT_MOUNTED)***" and a format icon will appear in the Format column. Tap the ***(Format)*** icon the Destination drive.

For Drive to File or File to File, the ZXi-Forensic will display drives connected to the Destination ports and any added repository.

Encrypted drives will have the following symbol in the Format column:

When formatting the drive from this screen, a prompt will appear to format the drive.



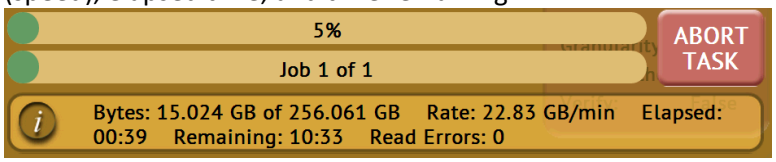
Select which file system to use (EXT4 or NTFS) and whether to format with encryption (ON) or without encryption (OFF). Details on encryption can be found in Chapter 8 of the ZXi-Forensic User's Manual. For details on formatting a drive, see ***Section 5.0.3.2.3***. Formatting the drive may take up to two minutes. Tap the ***OK*** icon to continue.

For in-depth information regarding drive encryption, please see **Chapter 6: Drive Encryption and Decryption**

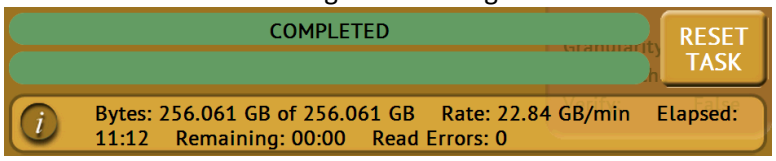
4.1 Starting the Imaging Operation

Once all the settings and options have been selected or set, tap the START ***(Start)*** icon to begin the imaging. A confirmation screen will appear. Tap the ***Yes*** icon to continue.

A progress bar will appear at the bottom of the screen showing the bytes processed, the rate (speed), elapsed time, and time remaining.



When finished, the status will change to COMPLETED. At this point, it is recommended to tap Reset Task to reset the task, and also to delete the task in order for the drive bays to be properly reset and not show as being used or assigned for other tasks to be configured.



The number of bytes shown on the progress bar is not the actual size of the drive. This is the actual data being processed. When 'Verify' is set to "Yes", the reported number will double in size.

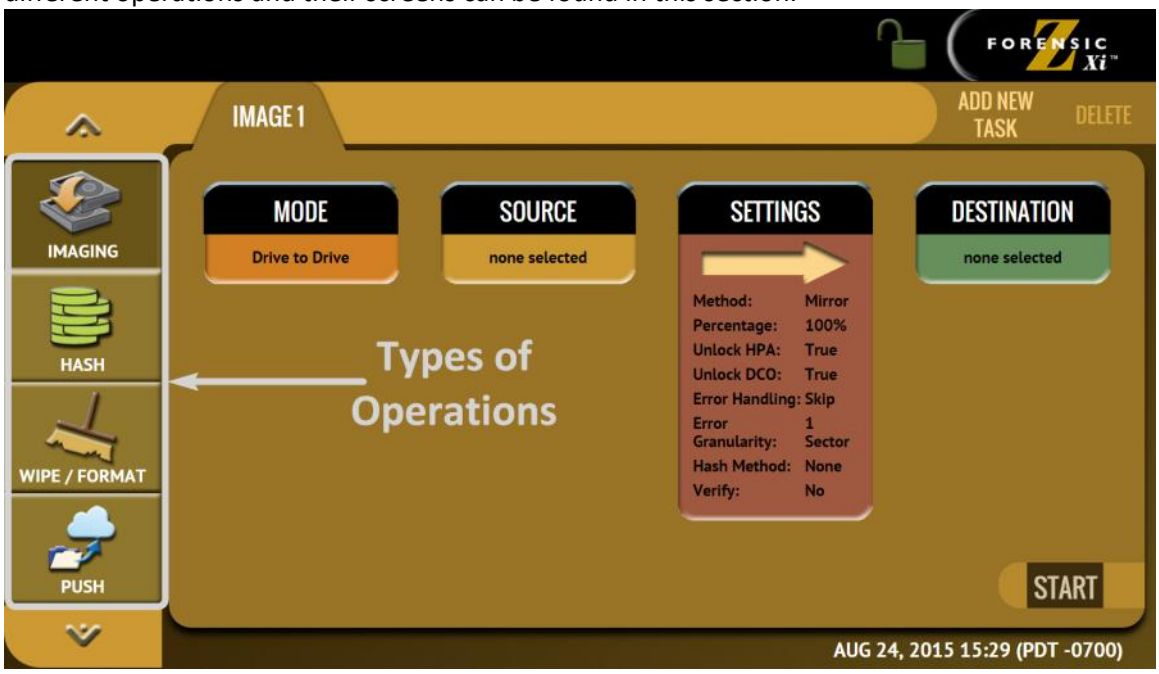
For parallel imaging, prior to starting the first task, users must set all other tasks that need to be run in parallel. When all other tasks to be run in parallel are set, a confirmation screen will appear stating there are multiple tasks setup with the same Source drive.

ZXi-Forensic can automatically span to two (or more) Destination drives when using Drive to File mode (DD, E01, EX01). When the Destination drive is full and the remaining data to be imaged will not fit, ZXi-Forensic will prompt for another drive. Information on Drive Spanning can be found in ***Section 3.1.1.1***.

5: Types of Operations

5.0 Types of Operations

There are thirteen (13) types of operation available on the ZXi-Forensic. The left side of the screen shows the different operation types that can be set. Detailed information on all of the different operations and their screens can be found in this section.



1. **IMAGING –** Performs an image from a Source to a Destination. There are three modes available:
    a. **Drive to Drive** – Performs a bit-for-bit copy of the Source producing an exact duplicate of the Source drive.
    b. **Drive to File** – Images the Source to any of the following image output formats: ***DD***, ***E01***, ***EX01***, or ***File***. Compression is available for E01 and EX01 formats.
    c. **File to File** – Image specific files (by filename, extension, etc.). The files will be sorted by path (based on where the file is located on the Source and each file will be hashed.

    Details on the different screens found in the Imaging operation can be found in ***Chapter 5: Imaging*****.**

2. **HASH –** Perform a SHA1, SHA-256, or MD5 hash of a drive. This can also verify the hash of the drive by entering an "expected value" for the hash.

3. **WIPE –** This type of operation is used to erase, wipe, and/or format drives. There are three main settings:
    - **Secure Erase –** Sends a command to the drive instructing it to perform a secure erase based on the drive manufacturer's specifications.
    - **Wipe Patterns –** Allows the user to set a specific pattern to use for wiping the drive. The number of passes is customizable (up to 7 passes) along with the type of data written for each pass. In addition, a 7-pass DoD wipe can be set.
    - **Format –** Formats the Destination using the EXT4 file system or NT file system (NTFS) either with or without AES-256 encryption.
4. **PUSH –** The network Push feature gives users the ability to push evidence files from destination drives connected to the ZXi-Forensic or from a ZXi-Forensic repository to a network location. The Push feature provides a more secure method than simply copying and pasting to the analysis computer by performing an MD5 or SHA hash during the push process. Additionally users can select to verify the file transfer to ensure data integrity. Network users can then quickly preview data or copy data to a local drive or to any other directory on the network. The ZXi-Forensic will create a log file for each push process.
5. **TASK MACRO –** Set up to nine (9) different tasks to perform sequentially (one after another). For example, a macro can be set to perform these tasks in order: Wipe, image, hash, push, then wipe again.
6. **FILE BROWSER –** Preview the contents of all connected Source or Destination drives on the ZXi-Forensic. The ZXi-Forensic will show all viewable partitions and the contents of each partition.
7. **LOGS –** Display logs of each task that has been performed on the ZXi-Forensic.
8. **STATISTICS –** This will display information about the ZXi-Forensic including the current software installed. In addition, the Statistics screen has an ***Advanced Drive Statistics*** tab that shows raw S.M.A.R.T. data on any drive connected to the ZXi-Forensic and a ***Network Interface Stats*** tab that displays statistics for all three network ports.
9. **MANAGE REPOSITORIES –** Allows the user to add a network location as a repository that can be used as a Destination for imaging or pushing images (or a Source when using the ***File to File*** mode).
10. **SYSTEM SETTINGS –** This mode allows changes to the system settings on the ZXi-Forensic which include the following:
    - **User profiles/configurations –** Allows the user to create, save, apply, or delete user profiles/configurations.
    - **Passwords –** Allows the user to set a password to lock the ZXi-Forensic from any configuration changes.
    - **Encryption Settings –** Sets the cipher mode (TC-XTS, CBC, or ECB), Cipher, IV Generation, and the encryption password.
    - **Language/Time Zone –** Sets the language on the ZXi-Forensic's menu and change the system's Time Zone.
11. **NETWORK SETTINGS –** Allows certain services to be enabled or disabled. Also, allows the user to set proxy settings (if required by their network).

12. **SOFTWARE UPDATES –** Perform software updates on the ZXi-Forensic. Software can be updated over an internet connection (from network) or from a USB flash drive.
13. **POWER OFF –** Allows the user to turn the ZXi-Forensic unit off by using the Graphical User Interface (GUI). Also allows a drive timeout to be set, powering down drives when not in use.

5.0.1 Imaging

This type of operation allows the imaging of a Source to a Destination. There are three different imaging modes and several settings to choose from. These selections should be performed in order from left to right.

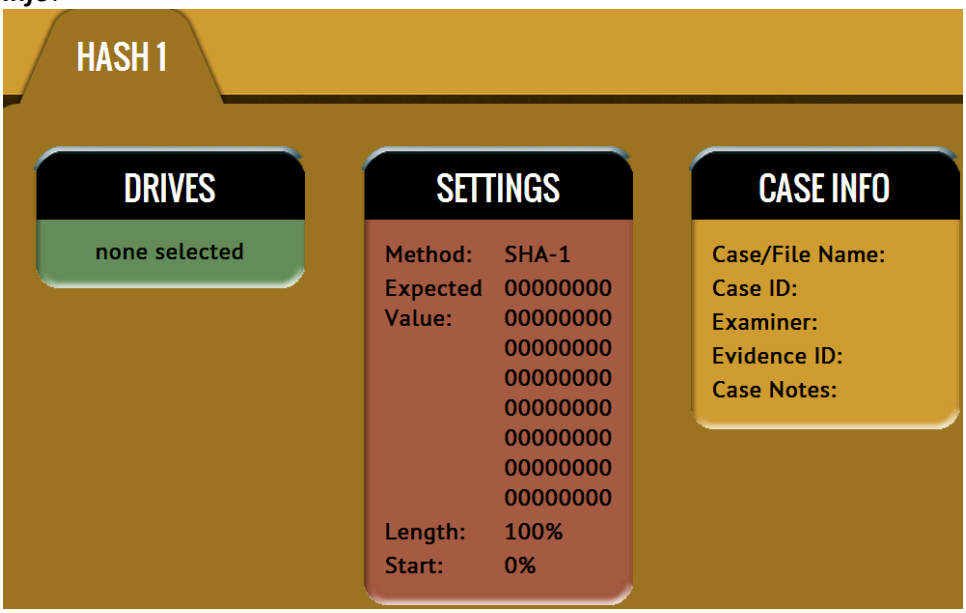
In-depth details on the different screens found in the Imaging operation can be found in **Chapter 5: Imaging**.

5.0.2 Hash

This type of operation allows the hashing of any connected drive using one of the following algorithms:

- SHA-1
- SHA-256
- MD5

There are three selections when performing a hash: ***Drives***, ***Settings***, and ***Case Info***.



5.0.2.1 Drives

DRIVES Tap this icon to choose a drive to hash. ZXi-Forensic will show all connected Source and Destination drives. Tap the drive to be hashed then tap ***OK***.

5.0.2.2 Settings

SETTINGS Tap this icon to choose a drive to adjust the hash settings. The Hash Settings screen will appear:

HASH VALUES Tap this icon to set the hash method (SHA-1, SHA-256, or MD5) and to set the expected hash value (if desired). Setting the expected hash value instructs the ZXi-Forensic to hash the drive then verify the hash with the expected value set.

> Each hash task is Logical Block Address (LBA) based and will hash drives based on the number of LBAs. If multiple drives are selected to be hashed, the ZXi-Forensic will hash up to the LBA value of the smallest capacity drive. If drives with different capacities need to be hashed, it is recommended to start one task per drive.

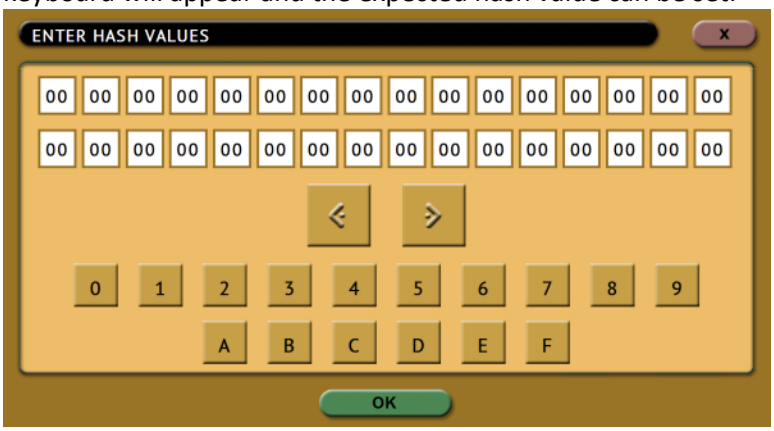
Hash Method Select one of the following hash methods:

- **SHA-1 –** Select this to hash or verify the Target drives using the SHA-1 algorithm.
- **SHA-256 –** Select this to hash or verify the Target drives using the SHA-256 algorithm.
- **MD5 –** Select this to verify the Target drives using the MD5 algorithm.

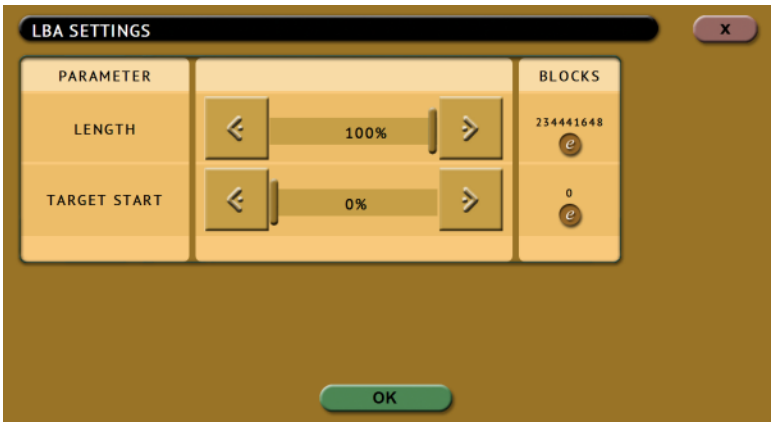
The recommended method is SHA-1 or SHA-256.

Hash Values By default, this value will have 0s (zeros). If this is not changed, or no value is entered, this will instruct the ZXi-Forensic to hash the drive using the selected algorithm in the previous step. If a value is entered, the ZXi-Forensic will hash the selected drive and verify hash with the value entered/edited.

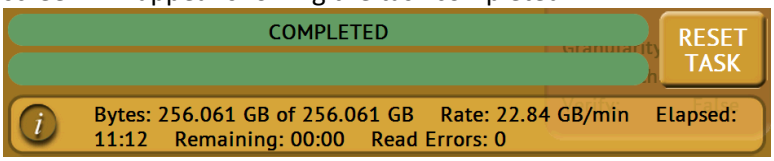
To set the expected value, tap the ***(edit)*** icon. The on screen keyboard will appear and the expected hash value can be set.



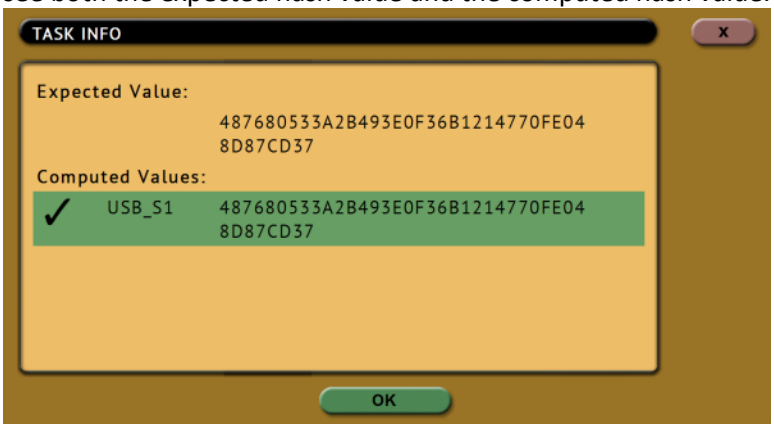
LBA The LBA icon will bring up the LBA settings screen. On this screen the user can adjust the percentage or the number of blocks of the drive to hash and also where to start the hash. By default the length is set to 100% (whole drive) and the starting percentage is set to 0% (start of the drive).



When the ZXi-Forensic finishes hashing the drive, the following screen will appear showing the task completed.



Tap the ***(Info)*** icon on the left of the completed screen to see both the expected hash value and the computed hash value.



5.0.2.3 Case Info

The Case Info setting allows users to enter some information about the case. This is optional and is not required to start a Hash operation.

Information entered here will appear in the logs. More information on the Case Info screen can be found in ***Section 5.0.3.1***.

Tap any of the boxes and an on-screen keyboard will appear allowing information to be entered. After entering the information, tap the ***OK*** icon to go back to the previous screen.

The ZXi-Forensic will convert any non-POSIX portable characters used in ***Case/File Name*** field to underscores "_" when creating the log or file names.

POSIX portable characters are:

Uppercase A to Z	Period (.)
Lowercase a to z	Underscore (_)
Numbers 0 to 9	Hyphen/Dash (-)

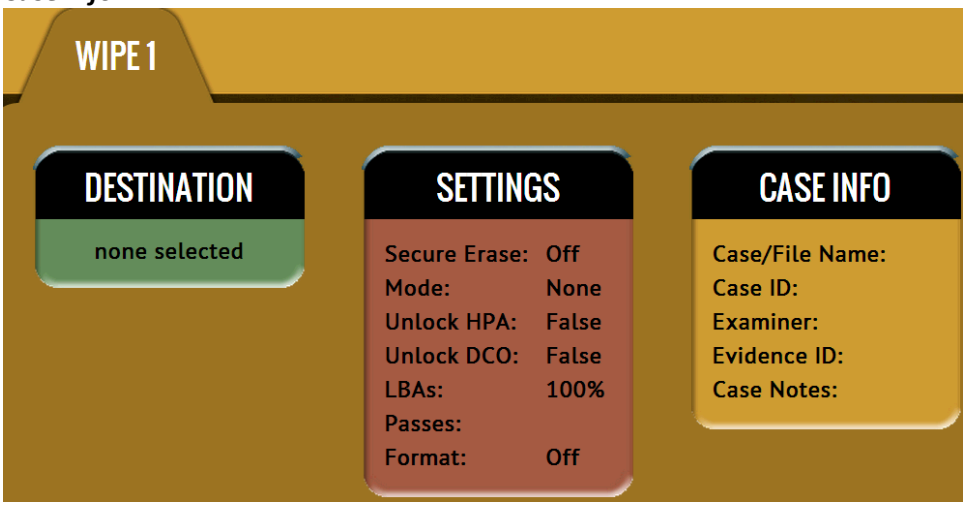
5.0.3 Wipe

This type of operation allows the user to erase, wipe, and/or format one or more Destination drives. There are three main settings: Secure Erase, Wipe Mode, and Format.

- **Secure Erase –** Sends a command to the drive instructing it to perform a secure erase based on the drive manufacturer's specifications for the secure erase command.
- **Wipe Patterns –** Allows the user to set a specific pattern to use for wiping the drive. The number of passes is customizable (up to 7 passes) along with the type of data written for each pass. In addition, a 7-pass DoD wipe can be set with pre-selected pass values.
- **Format –** Formats the Destination drive with an EXT4 file system or NT file system (NTFS) with or without AES-256 encryption.

More information on encryption can be found in ***Chapter 8***.

There are three selections when performing a wipe: ***Destination***, ***Settings***, and ***Case Info***.



5.0.3.1 Destination

Tap this icon to choose a drive to erase, wipe, and/or format.

A screen will appear, allowing the selection of one or more destinations. Tap the drive(s) to be erased, wiped, and/or formatted then tap ***OK***.

5.0.3.2 Settings

Tap this icon to choose a drive to set the wipe settings. The Wipe Settings screen will appear.

There are three sections in the ***Settings*** screen:

- Secure Erase
- Wipe Patterns
- Format

The ZXi-Forensic will perform each of the settings sequentially. For example, if Secure Erase is set to ON, a Wipe Pattern mode is specified, and Format is set to On, the ZXi-Forensic will first secure erase the drive, then wipe the drive according to the mode specified, then format the drive.

5.0.3.2.1 Secure Erase

Secure Erase Choose ***ON*** to Secure Erase the selected Destination drive(s). Most drives support this function. Secure Erase will send a command to the drive instructing it to reset itself to the specifications the drive manufacturer has set. For information on what happens when the Secure Erase command is sent, please contact the drive manufacturer. If the secure erase process fails, contact the drive manufacturer to find out if Secure Erase is supported on that specific drive.

For SAS (Serial Attached SCSI) drives, Secure Erase sends a 'Format' command. For SATA (Serial-ATA) drives, Secure Erase sends a 'Security Erase Unit' command. For SATA drives that support 'Enhanced Security Erase Unit' commands, the enhanced command will be sent. For questions on how each drive supports these features, or what the drive will do with these commands, please contact the drive manufacturer.

If errors appear when performing Secure Erase, contact the drive manufacturer to check if the drive supports Secure Erase. For Secure Erase specifications (what happens when the drive receives the Secure Erase command), contact the drive manufacturer.

5.0.3.2.2 Wipe Patterns

Wipe Patterns This setting allows the user to set a specific wipe pattern or patterns to use for wiping the drive. The number of passes is customizable (up to 7 passes) along with the type of data written for each pass. In addition, a 7-pass DoD wipe can be set with pre-selected pass values.

There are 4 selections when setting a wipe pattern:

- MODE
- HPA/DCO
- LBAS
- PASSES

> It is recommended to use the same capacity drive per task. When smaller capacity drives are wiped together with larger capacity drives, the smaller drives will finish first. However, the drive bays will not be available until the entire task is finished.

MODE Selecting this will open the Wipe Mode screen showing 3 options:

- **NONE –** Choosing this will instruct the ZXi-Forensic not to perform a wipe using Wipe Mode.
- **DOD –** Choosing this will instruct the ZXi-Forensic to perform a 7-pass wipe conforming to the DoD M-5220 standards.

- **CUSTOM –** Choosing this will allow the user to specify how many wipe passes will be performed and what values each pass will be written on each of the passes selected.

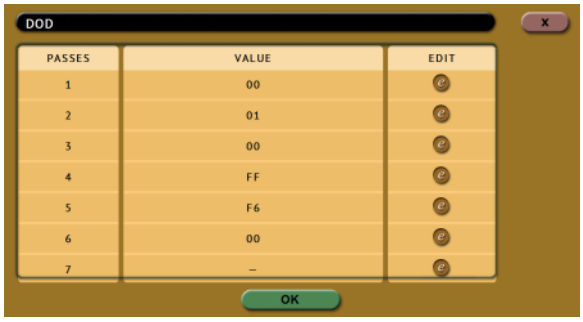
HPA/DCO This will open the HPA/DCO option for wiping. If the drive to be wiped has HPA and/or DCO that needs to be wiped, select ***Yes*** for the corresponding option.

LBA By default, this is set to 100% which will wipe all Logical Block Addresses (LBAs) and will wipe the entire drive (100%).

PASSES This Wipe Setting will change depending on the Wipe Pattern ***Mode*** selected.

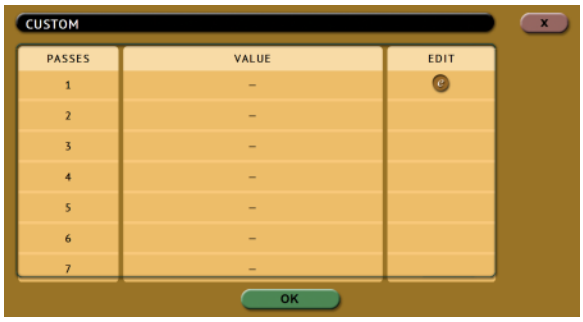
- If ***None*** was selected, this is not selectable.
- If ***DoD*** was selected, the first six pass values will be filled automatically by default. It is mandatory that the user enter the 7th pass value by tapping the (edit) icon or the operation will fail.
- If ***Custom*** was selected, no passes will be filled out. It is mandatory that the user set the value for at least one pass or the wipe operation will fail. The pass value can be set by tapping the ***(edit)*** icon.

Passes screen when DOD is selected:



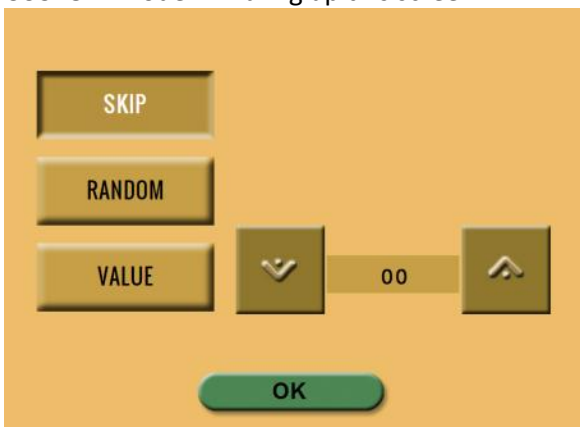
The ZXi-Forensic automatically enters default values for pass numbers 1 through 6. It is mandatory that the user enters a value for the 7th pass or the ZXi-Forensic will not proceed with the wipe operation. Values can be changed or added by tapping the ***(edit)*** icon.

Passes screen when Custom is selected:



There is no default value entered for any passes. It is mandatory that the user select a value for at least the first pass or the ZXi-Forensic will not proceed with the wipe operation. Values can be changed or added by tapping the ***(edit)*** icon.

Editing one or more of the passes in DOD or CUSTOM mode will bring up this screen:



- **SKIP –** Instructs the ZXi-Forensic to skip the pass.
- **RANDOM –** Instructs the ZXi-Forensic to perform a random pattern or value.
- **VALUE –** Instructs the ZXi-Forensic to use the specified hex value to be written for the pass. The values can range anywhere from 00 to FF.

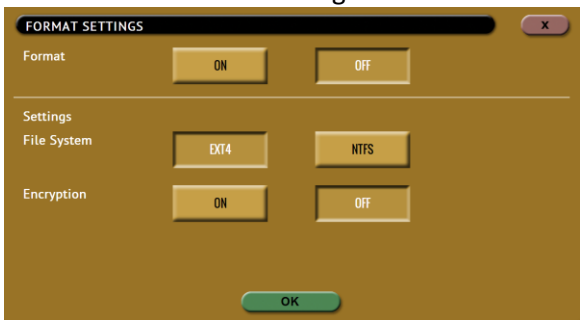
5.0.3.2.3 Format

Format Formats the Destination using the EXT4 file system or NT file system (NTFS) either with or without AES-256 encryption. To format the drive (with or without encryption) tap the ***Settings*** icon.

The ZXi-Forensic will check the Destination drive for proper formatting prior to being used as a Destination or Repository for Imaging using ***Drive to File*** or ***File to File***. If it is not properly formatted, Destination drive must be formatted using the ZXi-Forensic prior to being used as a Destination or Repository for Imaging using ***Drive to File*** or ***File to File***.

SETTINGS Tap this icon to set the ZXi-Forensic to format the drive (with or without encryption). Three settings are available:

- **Format –** When set to ***ON***, the ZXi-Forensic will format the Destination drive with or without encryption. The drive will be formatted with the EXT4 file system or NT file system (NTFS), depending on which file system is chosen. When set to ***OFF***, the ZXi-Forensic will not format or encrypt the selected drive.
- **File System –** Select ***EXT4*** to format the Destination using the EXT4 file system. Select ***NTFS*** to format using the NT file system (NTFS).
- **Encryption –** Select ***ON*** to format the drive with encryption. The drive will be formatted with the EXT4 file system or NT file system (NTFS) and encrypted with the AES-256 algorithm.



For more information on encrypted Destination drives, please see **Chapter 6: Drive Encryption and Decryption**.

5.0.3.3 Case Info

CASE INFO The Case Info setting allows users to enter some information about the case. This is optional and is not required to start a Wipe operation.

Information entered here will appear in the logs. More information on the Case Info screen can be found in ***Section 5.0.3.1***.

Tap any of the boxes and an on-screen keyboard will appear allowing information to be entered. After entering the information, tap the ***OK*** icon to go back to the previous screen.

The ZXi-Forensic will convert any non-POSIX portable characters used in ***Case/File Name*** field to underscores "_" when creating the log or file names.

POSIX portable characters are:

Uppercase A to Z	Period (.)
Lowercase a to z	Underscore (_)
Numbers 0 to 9	Hyphen/Dash (-)

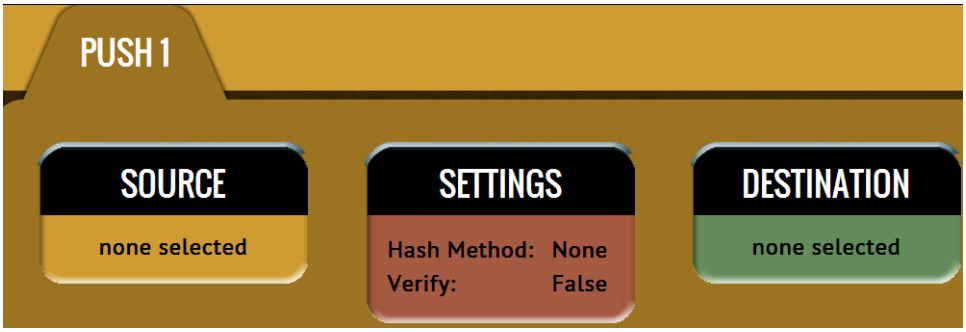
5.0.4 Push

The network Push feature gives users the ability to push evidence files from destination drives connected to the ZXi-Forensic or from a ZXi-Forensic repository to a network location or a Destination drive connected to the ZXi-Forensic. The Push feature provides a more secure method than simply copying and pasting to the analysis computer by performing an MD5 or SHA hash during the

push process. Users can also select to verify the file transfer to ensure data integrity. The ZXi-Forensic will create a log file for each push process.

There are three selections when performing a push:

- Source
- Settings
- Destination



To push files to a network location, a network repository must be set up. Details on how to add a repository can be found in ***Section 3.9 Manage Repositories***.

5.0.4.1 Source

SOURCE

Tap this icon to select the drive or repository where the files are to be pushed from (where the files to push are located). This will only show drives connected to the Destination ports or locations set up as a repository where the DD, E01, or EX01 images are located.

After selecting the Source, a list of cases found on the drive will be displayed. Select one or more cases to push then tap the ***OK*** button to continue. If no cases are selected, all cases found on the drive or repository will be pushed.

5.0.4.2 Settings

SETTINGS (Optional) Tap this icon to enter case info, set a hash method, and to set the verify option. The case info screen is similar to previous case info screens.

There are four hash methods available for this operation:

- **None –** No hash will be performed.
- **SHA-1 –** The SHA-1 algorithm will be performed on each file from the source location.
- **MD5 –** The MD5 algorithm will be performed on each file from the source location.

SHA-1 is the recommended method.

There are two verify settings available:

- **Yes –** Each file that was copied (on the Destination location) will be verified using the selected hash method/algorithm selected.
- **No –** No verification will be made.

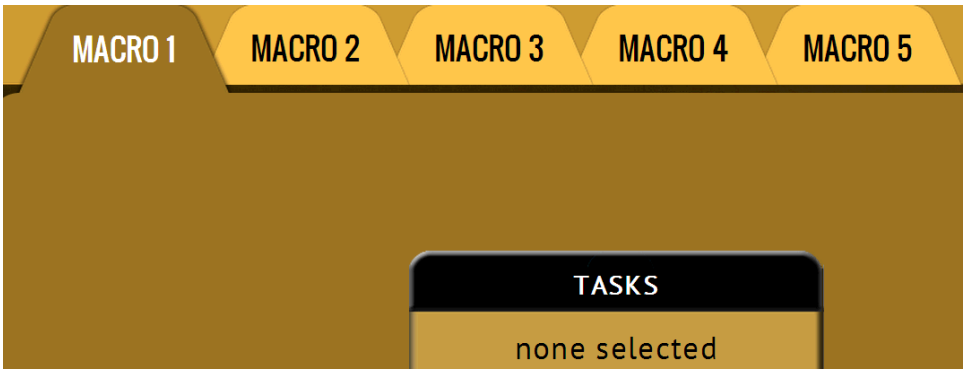
5.0.4.3 Destination

DESTINATION Tap this icon to select the drive or repository where the files are to be pushed to (where the files to push will be pushed/copied to). This will only show drives connected to the Destination ports or locations set up as a repository where the DD, E01, or EX01 images will be pushed to.

5.0.5 Task Macro

This operation allows up to five (5) macros that can be set. Each macro can run up to nine (9) tasks sequentially (one after another). For example, a macro can be set to perform these tasks in order: Wipe, image, hash, push, then wipe again.

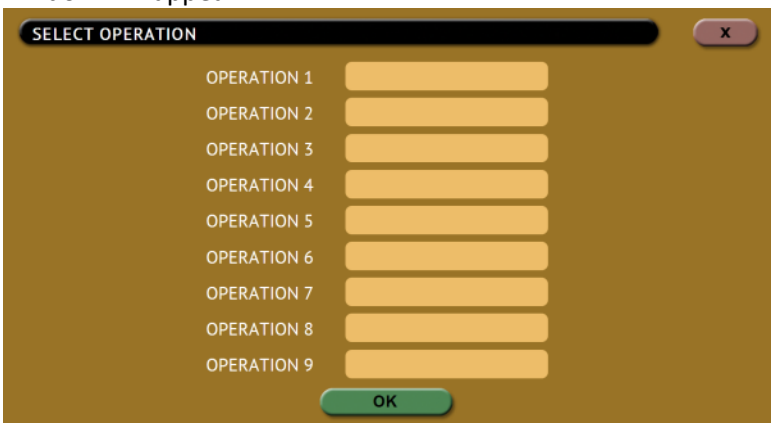
Each of the five macros can be set by tapping on the Macro number as seen in the next picture:



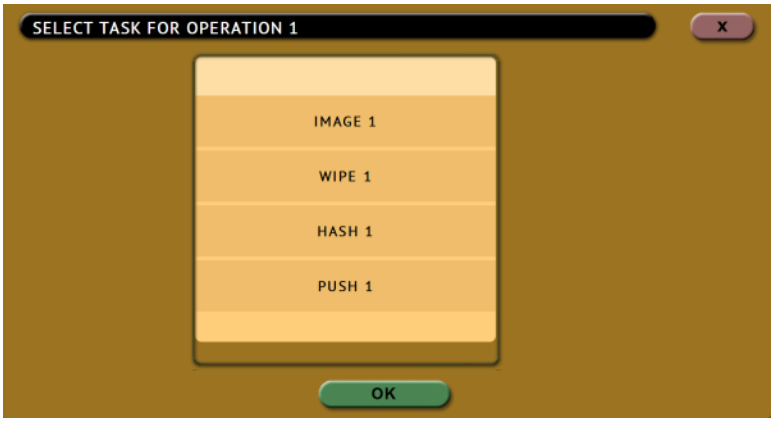
Each task or operation must be set up before setting up the macro. For example, to set up a Task Macro that will perform a wipe, then image, users must first set up both the wipe and image tasks. Once the wipe (for example, Wipe 1) and image (for example, Image 1) has been set up, the Task Macro can be set.

5.0.5.1 Tasks

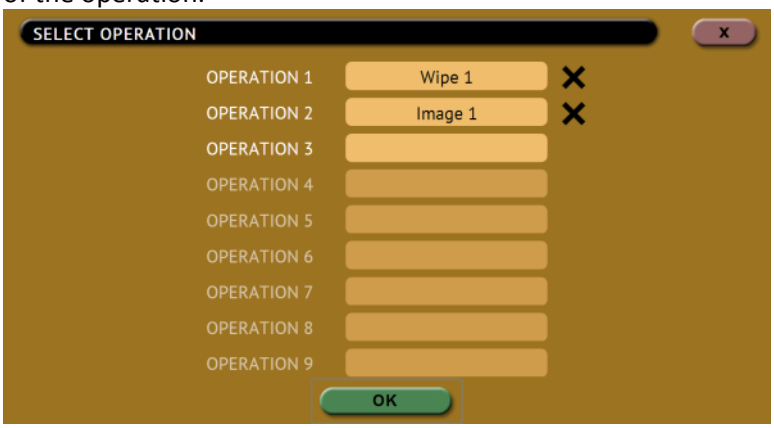
Tapping this icon allows the user to set specific tasks for each macro. The following window will appear:



Tap ***Operation 1*** to set the first operation in the macro. The following screen will appear allowing the user to choose the task. Tap the ***OK*** icon to continue.



Continue adding operations desired. Each operation added will appear on the list. To delete an operation, tap the ***X*** to the right of the operation.



When finished, tap the ***OK*** icon. A summary of the macro will be seen:

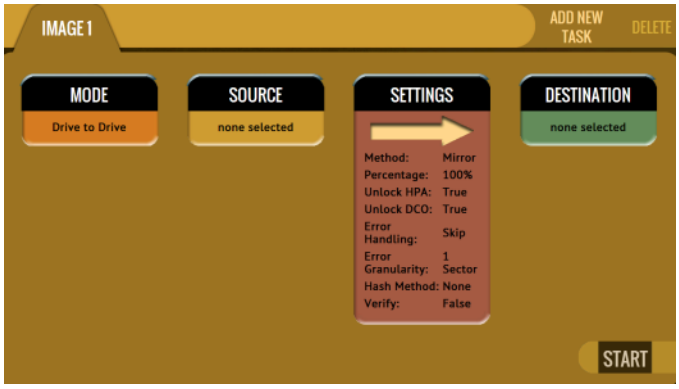
To start the macro and have the ZXi-Forensic perform all the operations on the task list, tap the ***Start*** icon.

Example: Setting up a Macro for a Wipe using Secure Erase then perform a Drive to Drive Image

To set a macro to perform a Wipe using Secure Erase on D1, immediately followed by performing a Drive to Drive image from S1 to the newly wiped (secure erased) D1, the Wipe and Imaging Tasks first need to be set up.

1. First, set the Wipe task. Select D1 as the Destination and change the setting to perform a Secure Erase (Wipe Patterns and Format set to off). Do not start this task.

2. Next, set the Imaging task. Select Drive to Drive as the Mode. Select S1 as the Source. Change the settings as needed. Select D1 as the Destination. Do not start this task.



3. Choose ***Task Macro*** from the list of operations on the left side.
4. Tap the ***Tasks*** icon to select the different tasks for the macro.
5. Tap the field next to ***Operation 1*** to set the first operation. Since the first task to be run is the Wipe task, select ***Wipe 1*** then tap ***OK***.
6. Tap the field next to ***Operation 2*** to set the second operation. Since the second task to be run is the Drive to Drive Imaging task, select ***Image 1*** then tap ***OK***.

7. The screen should now show ***Wipe 1, Image 1*** as the Tasks for Macro 1.

8. Tap the ***Start*** icon to begin the macro. The macro will run the Wipe 1 task first, then Image 1.

5.0.6 File Browser

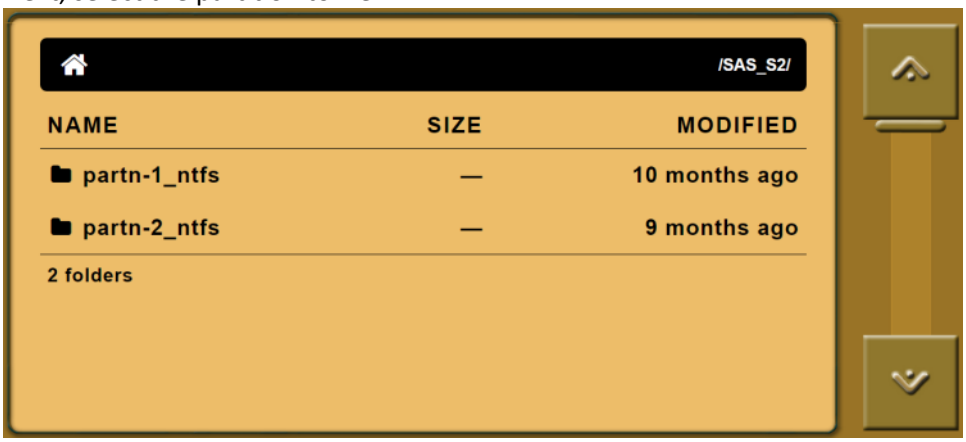
The contents of all connected Source or Destination drives on the ZXi-Forensic can be viewed using the ZXi-Forensic's file browser. The ZXi-Forensic will show the partitions and the contents of each partition. Note that only some files can be opened by the ZXi-Forensic.

For Destination drives, only drives formatted by the ZXi-Forensic can be previewed. Contents of Destination drives that were used in a 'Drive to Drive' image will not be seen.

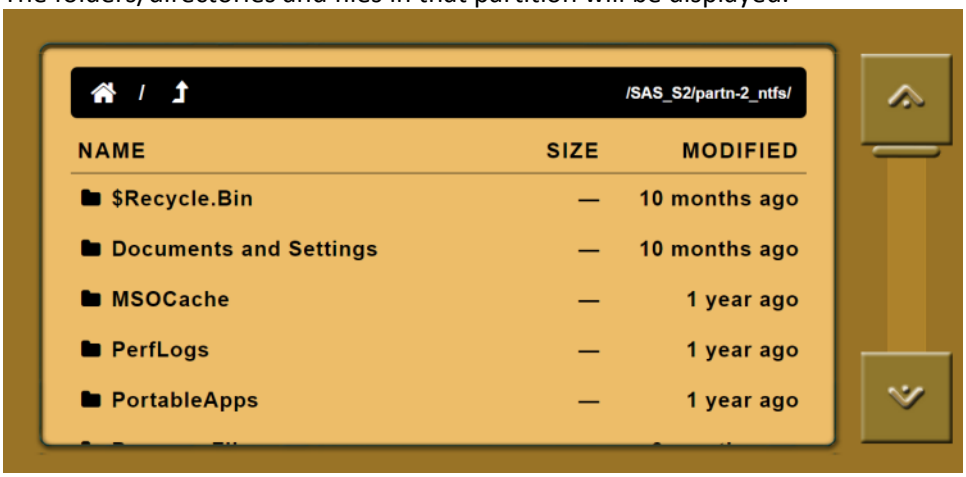
Drives connected to the Source ports (S1, S2, S3, and U1) – Drives connected to the Source ports are always write-protected. Using the File Browser function will not alter the drive or its contents in any way.

Drives connected to the Destination ports (D1, D2, D3 U2, and U3) – Drives connected to the Destination ports are not write-protected. The File Browser function only opens a file and does not modify the contents of the file. The only change to the contents of the destination drive will be the file's accessed date and time.

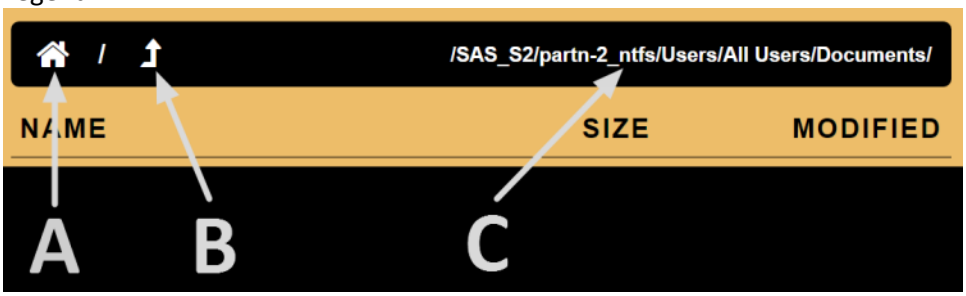
In the File Browser screen, select the drive to view by selecting one of the tabs. Next, select the partition to view:



The folders/directories and files in that partition will be displayed:



Legend:



A – Home – Tap the Home icon to bring you to the top-level of the drive.

B – Up One Level – Tap this icon to go up one level (one folder/directory).

C – Path – Displays the current path to the folder/directory being viewed.

ZXi-Forensic can open and preview certain files. Some of the files it can preview are:

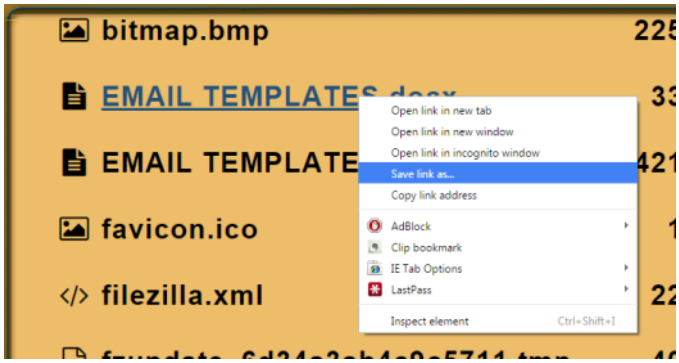
*.jpg	*.txt
*.gif	*.pdf
*.png	*.html

If the ZXi-Forensic cannot preview a file, a message will appear stating "**File viewer cannot view file type:**"

5.0.6.1 Viewing files from the web interface

The ZXi-Forensic's File Browser can also be used from the web interface. Using the web interface gives the ability to open files that the ZXi-Forensic cannot preview by downloading the file to a computer (where the ZXi-Forensic is being browsed from).

1. Using a compatible web browser, connect to the ZXi-Forensic's web interface (see ***Section 8.1*** for more information on how to connect to the ZXi-Forensic's web interface).
2. From the ZXi-Forensic's web interface, navigate to ***File Browser***.
3. Select the drive to view.
4. Navigate through the file browser and locate the file to download and open.
5. From the File Browser screen, right-click on the file and select ***"Save link as…"*** and save the file to the local computer.



6. The file can then be opened on the computer where it was downloaded to.

> Your computer will need to be able to open the type of file that was downloaded. For example, if a Word document was downloaded, the computer needs to have software that can open a Word document.

5.0.6.2 Important notes about using the File Browser

When using the ZXi-Forensic's File Browser, there are several things to take note of:

- Drives connected to the Source positions are write-protected.
- When using the ZXi-Forensic on-screen GUI, opening a file will not alter the forensic integrity of the Source drive connected to the ZXi-Forensic.
- When using the web interface, opening a file or saving a file to a computer will not alter the forensic integrity of the Source drive connected to the ZXi-Forensic.
- The ZXi-Forensic file browser is not able to open every file to preview. When a file cannot be opened directly on the ZXi-Forensic, the file can be saved on a computer by connecting to the ZXi-Forensic's web interface.

5.0.7 Logs

The ZXi-Forensic keeps logs of all imaging, hash, wipe, format, and push operations. Logs can be viewed directly on the ZXi-Forensic or from a computer's browser (if the ZXi-Forensic is connected to a network).

When using Drive to File mode (DD, E01, or EX01), log files are also stored in the Destination drive in the same folder as the image files.

The log files in the Destination drive are available in PDF, HTML, and XML formats.

In addition to viewing, the logs can be exported to an external USB location such as a USB flash drive. Logs are exported in PDF, HTML and XML format.

From this screen, log files can also be deleted one at a time or all at once.

The log file may contain several sections, depending on what settings and options were chosen during the operation, including:

- Information on the ZXi-Forensic and its settings
- Case info (if entered)
- Source and Destination hashes

5.0.8 Statistics

This will display two tabs: ***About*** and ***Adv. Drive Statistics***. The ***About*** screen will show information about the Forensic ZXi-Forensic including the current software installed.

The ***Adv. Drive Statistics*** tab shows S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) information taken directly from what the drive is reporting. Navigate between drives by using the left and right scroll arrows. The up and down scroll arrows scroll through the different information. The information shown is the raw value tracked by the drive and is not translated.

The ***Network Interface Stats*** tab displays information on each of the three network interfaces.

5.0.9 Manage Repositories

Repositories can be added to the ZXi-Forensic in this operation. Repositories can act as a Source or Destination.

When ***Manage Repositories*** is selected, two tabs are available at the top of the screen:

- Add/Remove (using the SMB (Server Message Block) and CIFS (Common Internet File System) protocols)
- iSCSI (Internet Small Computer System Interface protocol)

Networks are configured differently and may require the assistance of a Network or Systems Administrator.

Step-by-step details for the ManageRepositories screen can be found in the Quick Start section: ***Section 3.9 Manage Repositories***.

5.0.10 System Settings

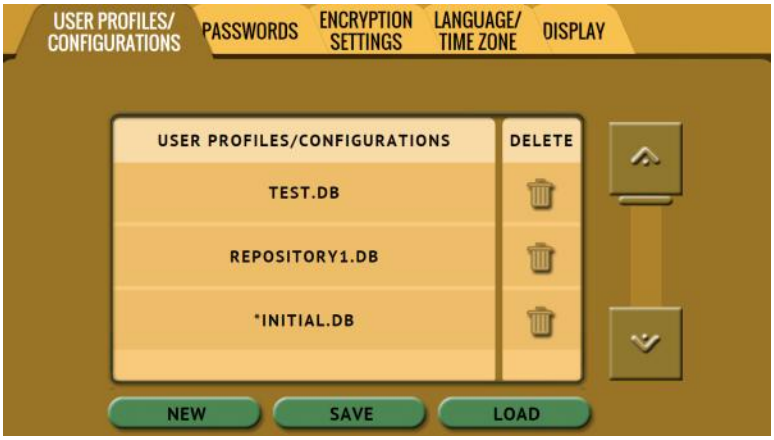
The ***System Settings*** screen allows users to configure five different settings for the ZXi-Forensic:

- User Profiles/Configurations
- Passwords
- Encryption Settings
- Language/Time Zone
- Display

5.0.10.1 User Profiles/Configurations

This screen shows all user profiles/configurations for the ZXi-Forensic. There are three options in this screen:

- **New –** Allows the user to create a new profile/configuration name.
- **Save –** Saves the selected profile/configuration.
- **Load –** Loads the selected profile/configuration.



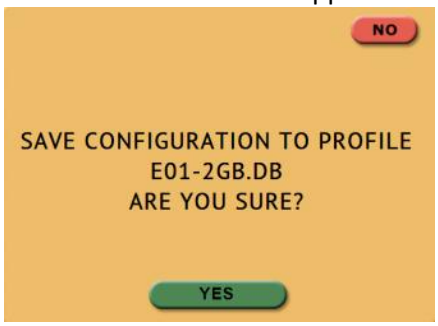
The ZXi-Forensic will boot with the profile/configuration that has an asterisk (*) next to the name.

Profiles/configurations allow users to create different profiles or configurations. The profile/configuration can then be saved.

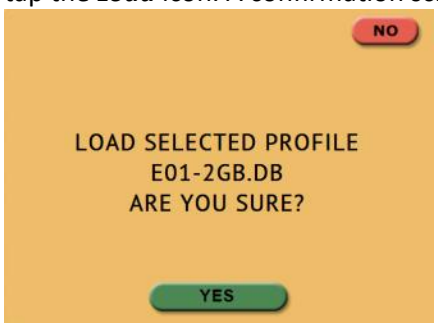
When a profile/configuration is loaded using the ***Load*** icon, the ZXi-Forensic will load that configuration during its boot process.

For example, if the user wants the ZXi-Forensic to always boot up with the default imaging mode to ***Drive to File*** with the setting of ***E01*** with a segment size of ***2GB***:

8. Turn the ZXi-Forensic off then back on. This will reset all settings to its default configuration. This is an important step to help ensure only the changes desired will be the changes saved.
9. Go to the ***Imaging*** screen and set the ***Mode*** to 'Drive to File.
10. In the ***Settings***, set the image to ***E01*** and set the segment size to ***2GB***.
11. In the ***System Settings***, go to ***User Profiles/Configurations*** and tap the ***New*** icon.
12. Type a name for this profile. For example, E01-2GB and tap the ***OK*** icon. The profile name should appear on the screen.
13. Tap the newly saved profile and tap ***Save***. A confirmation screen will appear:



14. Tap the ***Yes*** icon to save the profile.
15. Make sure the profile to be loaded (during the boot process) is highlighted (in this case, E01-2GB.DB) and tap the ***Load*** icon. A confirmation screen will appear:



16. The next time the ZXi-Forensic is turned on it will load the E01-2GB.DB profile.

To delete a profile, tap the (delete) icon. A confirmation screen will appear. Tap the ***Yes*** icon to delete the selected profile.

It is highly recommended that the ZXi-Forensic is turned off then back on before making any changes to the profiles/configurations. This helps ensure that only the desired changes are saved.

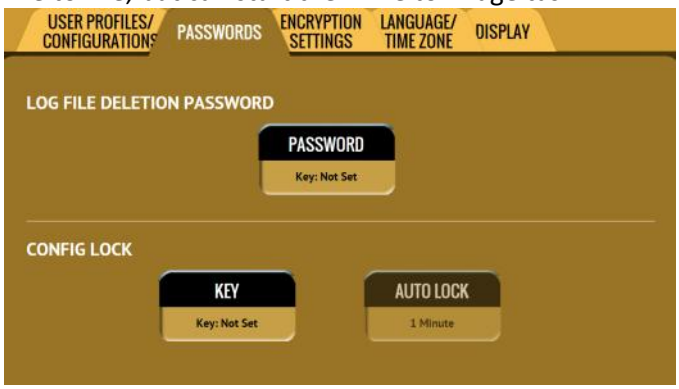
Do not highlight and save over the INITIAL.DB configuration. This is the default configuration of the ZXi-Forensic and is used to reset the ZXi-Forensic to the factory default settings.

5.0.10.2 Passwords

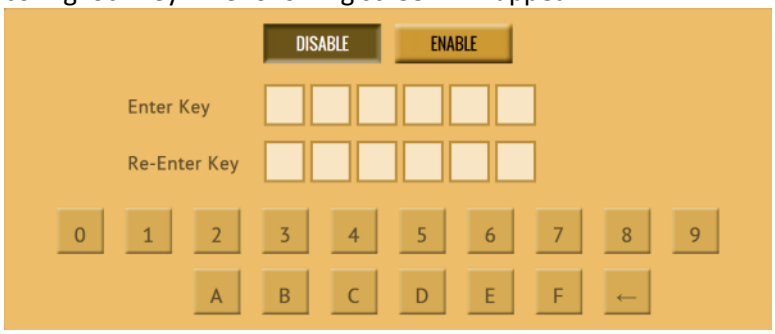
There are two sets of passwords that can be entered on the ZXi-Forensic.

- **Log File Deletion Password –** A password can be set as an extra layer of protection when deleting log files. If this password is set, ZXi-Forensic will prompt for the password before any log files can be deleted.
- **Config Lock –** The ZXi-Forensic can be configured to lock out any configuration changes. When this is enabled, changes to the different types of operations cannot be made without entering the correct key or password. Different types of operations can still be started.

  For example, when the ZXi-Forensic is locked, and it is configured for Drive to Image Imaging mode, the user will be unable to change this mode to Drive to Drive or File to File, but can start the Drive to Image task.



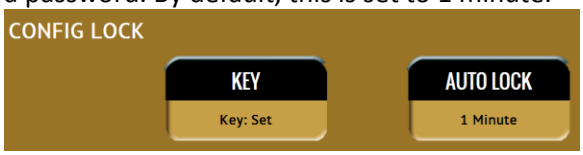
Tap ***Password*** or ***Key*** to enter a log file deletion password or a config lock key. The following screen will appear.



Tap the ***Enable*** icon to enter a password or key. The available characters are 0 through 9 and A through F.

5.0.10.2.1 Additional information for Config Lock

Tap the ***Auto Lock*** icon to set the time to automatically lock the configuration and require a password. By default, this is set to 1 minute.



A shortcut (and indicator) to the ***config lock*** can always be seen on the ZXi-Forensic's screen. It is located on the top-right of the screen, next to the ZXi-Forensic logo.

While in a locked state, the following operations will be affected as follows:

- **Imaging –** An imaging task can be started, but no settings can be changed. Additionally, no new task can be added, and no task can be deleted without the unlock key.
- **Hash –** A hash task can be started, but no settings can be changed. Additionally, no new task can be added, and no task can be deleted without the unlock key.
- **Wipe –** A wipe task can be started, but no settings can be changed. Additionally, no new task can be added,

and no task can be deleted without the unlock key.

- **Task Macro –** A task macro can be started, but no settings can be changed. Additionally, no new macro can be set or edited without the unlock key.
- **File Browser –** The file browser cannot be accessed without the unlock key.
- **Logs –** Since there are no settings or configurations for this operation, it is not affected by Config Lock.
- **Statistics –** Since there are no settings or configurations for this operation, it is not affected by Config Lock.
- **Manage Repositories –** A managed repository cannot be added without the unlock key. At this time, a managed repository can be deleted without the unlock key. A future software update will require the unlock key to delete a managed repository.
- **System Settings –** This entire section cannot be accessed without the unlock key.
- **IP Settings –** This entire section cannot be accessed without the unlock key.
- **Software Updates –** This entire section cannot be accessed without the unlock key.
- **Power Off –** This entire section cannot be accessed without the unlock key.

The Passwords can be saved into a user profile/configuration and loaded each time the ZXi-Forensic is turned on. See **Section 5.0.10.1** for more information on saving and loading a user profile/configuration.

The ZXi-Forensic can still be turned off without the unlock key by using the power switch located in the back of the ZXi-Forensic.

Remember the Config Lock Key! If the ZXi-Forensic is configured to load with the Config Lock set (enabled) the only way to delete the Config Lock is to reset the ZXi-Forensic using the Command Line Interface (CLI).

5.0.10.2.2 Forgotten password or config lock key

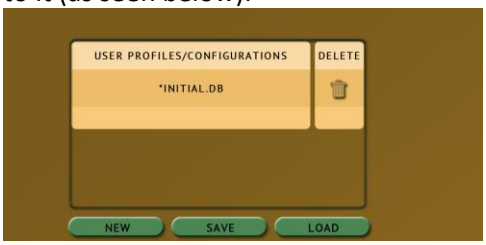
If the Log File Deletion password or Config Lock key is forgotten, the ZXi-Forensic will need to be reset using the Command Line Interface (CLI). See **Section 8.2** for more information on how to connect to the ZXi-Forensic using the CLI.

Once connected to the CLI:

1. Login with the username "***it***" (without the quotes) and the password "***it***" (without the quotes).
2. From the main prompt, type ***command*** then press the enter key.
3. Type ***config*** then press the enter key.
4. Type ***db list*** then press the enter key. This will show a list of databases or configurations saved. The example below shows two databases (the default initial.db and Lock.db). The db that shows an asterisk (*) before the name is the current database or configuration being loaded each time the ZXi-Forensic is turned on.
5. Type ***db load initial.db*** then press the Enter key to load the default database. There should be a response showing "Command (DbManagement) Successful".
6. Type ***db list*** again and there should be an asterisk (*) on initial.db.
7. Turn the ZXi-Forensic off using the power switch located in the back of the

device, and close the Telnet/SSH application.

8. Wait for the ZXi-Forensic to completely turn off then turn it back on. When the ZXi-Forensic boots up, it will load the default configuration. The default configuration can be checked by going to ***System Settings*** and looking at the ***User Profiles/Configurations*** tab. INITIAL.DB should have an asterisk next to it (as seen below).



5.0.10.3 Encryption Settings

The ZXi-Forensic allows imaging drives onto a Destination where the data on the Destination drive is encrypted. Destination drives that are encrypted by the ZXi-Forensic can be decrypted by using the ZXi-Forensic or third party software (TrueCrypt or FreeOTFE).

For in-depth information on encrypting and decrypting a drive using the ZXi-Forensic, or decrypting a drive using TrueCrypt or FreeOTFE, please see **Chapter 6: Drive Encryption and Decryption.**

There are 4 parameters that must be configured before encryption can be used. These 4 parameters are necessary to decrypt and read the Destination drive properly:

- **Cipher Mode** – Users can choose between ***TC-XTS***, ***CBC*** (cbc-plain64.) or ***ECB*** (cbc-essiv:sha256) cipher modes.
- **Cipher** – At this time, only the ***AES-256*** cipher is supported.
- **IV Generation** – Unavailable when TC-XTS cipher mode is selected. If CBC or ECB cipher mode is selected, users can choose between ***PLAIN64*** and ***ESSIV:SHA256***.
- **Encryption** (Password or Key) – Users must choose their own encryption password/key.

There are 2 imaging modes in which encryption can be used:

- **Drive to File** – Images the Source to any of the following image output formats: ***DD***, ***E01***, and ***EX01***. This will have a partition level encryption where only the partition (on the Destination or Repository) where the images are created will be encrypted.
- **File to File** – Image specific files (by filename, extension, etc.). The files will be sorted by path (based on where the file is located on the Source and each file will be hashed. This will have a partition level encryption where only the partition (on the Destination or Repository) where the images are created will be encrypted.

There are many articles on the Internet about AES-256 encryption and the different modes and settings that come with encryption.

5.0.10.4 Language/Time Zone

The ZXi-Forensic's menu system's language can be changed. At this time, the available languages are English, Chinese (中文), Korean (한국어), and Japanese (日本語).

This screen also allows the time zone to be set.

5.0.10.4.1 Language

Four languages are available at this time. Select English, Chinese (中文), Korean (한국어), or Japanese (日本語) to change the language displayed. As soon as the selection is made, the ZXi-Forensic's screen (or the computer's Internet browser) will automatically refresh and display the selected language.

The ***Custom*** button is reserved for future language releases.

5.0.10.4.2 Time Zone

The ZXi-Forensic utilizes NTP (Network Time Protocol). Each time the ZXi-Forensic is connected to a network with internet access, it will automatically check for the correct time using NTP and adjust the time as needed.

The ZXi-Forensic also has a time zone setting. Tap ***Time Zone*** to select the time zone region. Tap the ***OK*** icon to continue.

After selecting the region, select the time zone where the ZXi-Forensic is located. Tap the ***OK*** icon to set the time zone.

5.0.11 Network Settings

The Network settings screen allows certain services to be enabled or disabled in the ***Services*** tab. There is also an ***HTTP Proxy*** tab where proxy server information can be entered.

5.0.11.1 Services

There are 7 services that can be disabled (enabled by default):

- **SSH –** Disabling this will block Secure Shell (SSH) traffic.

- **Telnet –** Disabling this will block Telnet traffic.
- **HTTP –** Disabling this will block web browser connections to the ZXi-Forensic.
- **CIFS/NETBIOS –** Disabling this will block any CIFS or NETBIOS connection to the ZXi-Forensic (for example, Windows Explorer).
- **iSCSI –** Disabling this will block iSCSI connections.
- **Iperf –** Disabling this will block Iperf traffic (a network tool to measure bandwidth performance).
- **Ping –** Disabling this will block ping access to the ZXi-Forensic.

Disabling any of the services above will disallow the types of communication controlled by those services. For example, if HTTP is disabled, users will not be able to see the ZXi-Forensic through a web browser over the network.

Please contact your Network or Systems Administrator before changing any of these services.

5.0.11.2 Interfaces

The Interfaces screen will show the MAC address, configuration type (DHCP or STATIC), MTU speed, and the status of each of the three Ethernet ports.

5.0.11.3 HTTP Proxy

If the network the ZXi-Forensic is connected to uses an HTTP proxy server to access the Internet, a proxy settings may need to be set in order for the ZXi-Forensic to be able to update software from a network (over the internet),. This typically includes a server (or IP address), a host port, a username and password.

5.0.11.3.1 Server

Tap the Server icon to set the IP address (or server name) and port of the proxy server.

5.0.11.3.2 Username/Password

If the proxy server requires a username and password for authentication, tap the ***Username/Password*** icon to set this information.

5.0.12 Software Update

This section is reserved. Please contact Logicube Technical Support for questions regarding software (support@logicube.com or 818.700.8488, opt. 3).

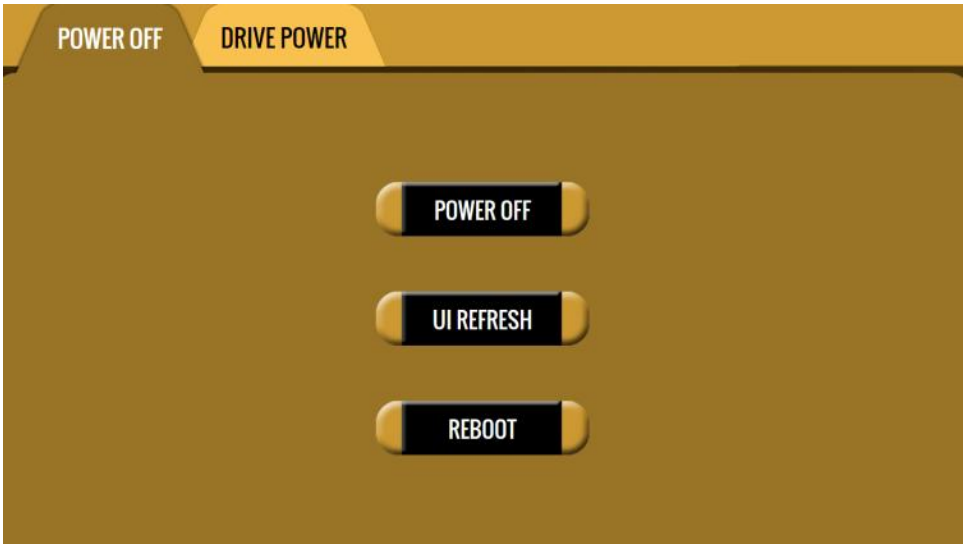
5.0.13 Power Off

There are two tabs in the ***Power Off*** screen:

POWER OFF – The ZXi-Forensic can be remotely turned off or restarted by going to this tab. Additionally, the Graphical User Interface (GUI) can be refreshed.

DRIVE POWER – Inactive drives connected to the ZXi-Forensic can be set to go to standby mode in this tab. The default is set to disabled (0 minutes, or OFF).

Power Off screen:



A confirmation screen will appear. Select ***Yes*** to confirm the selection.

Drive Power screen:

6: Drive Encryption and Decryption

6.0 Introduction – Drive encryption and decryption

The Forensic ZXi-Forensic allows imaging drives onto a Destination or Repository where the data on the Destination drive is encrypted. There are two different modes where Encryption is supported: Drive to File and File to File.

- **Drive to File –** Images the Source to any of the following image output formats: ***DD***, ***E01***, and ***EX01***. This will have a partition level encryption where only the partition (on the Destination or Repository) where the images are created will be encrypted.
- **File to File -** Image specific files (by filename, extension, etc.). The files will be sorted by path (based on where the file is located on the Source and each file will be hashed. This will have a partition level encryption where only the partition (on the Destination or Repository) where the images are created will be encrypted.

Third party utilities can be used to decrypt a drive encrypted by the ZXi-Forensic; TrueCrypt and FreeOTFE.

In the ***System Settings*** screen, there is an ***Encryption Settings*** tab used to configure the ZXi-Forensic for encryption. There are four (4) parameters that must be configured before encryption can be used. These parameters are necessary to decrypt and read the Destination drive and can be configured in the ***Encryption Settings*** page on the ZXi-Forensic:

- **Cipher Mode –** Users can choose between ***TC-XTS***, ***CBC*** or ***ECB*** cipher modes.

> TC-XTS cipher mode can be decrypted using the ZXi-Forensic or TrueCrypt.
>
> CBC or ECB cipher modes can be decrypted using the ZXi-Forensic or FreeOTFE.
>
> The ZXi-Forensic encrypts drives using AES 256 encryption regardless of what cipher mode is used. If TC-XTS is used, ZXi-Forensic uses a TrueCrypt friendly format and **does not** use TrueCrypt to encrypt the drive. The encryption key is not stored on the Destination drive.
>
> There are many articles on the Internet about AES-256 encryption and the different modes and settings that come with encryption.

- **Cipher –** At this time, only the ***AES-256*** cipher is supported.
- **IV Generation –** Initialization Vector. Unavailable when TC-XTS cipher mode is selected. If CBC or ECB cipher mode is selected, users can choose between ***PLAIN64*** and ***ESSIV:SHA256***.
- **Encryption** (Password or Key) **–** Users must choose their own encryption password/key.

6.1 Encrypting a Destination

To encrypt a Destination, the Encryption settings must be set and the drive will need to be formatted using the ZXi-Forensic. These steps must be performed prior to an Imaging operation.

6.1.1 Step-by-step Instructions

1. Select ***System Settings*** from the types of operation on the left side.
2. Tap the ***Encryption Settings*** tab.
3. Set the ***Cipher Mode***, ***Cipher***, ***IV Generation***, ***and Password***.
4. Select ***Wipe*** from the types of operation on the left side.
5. Tap the ***Destination*** icon and select the Destination drive to be formatted and encrypted.
6. Tap the ***Settings*** icon.

- If the Destination needs to be wiped, choose the type of wipe to be performed (Secure Erase and/or Wipe Patterns). If Wipe Patterns is selected, choose the type of Wipe Pattern to perform (DoD or Custom).
- If the drive has an HPA or DCO area that needs to be wiped, tap the ***HPA/DCO*** icon and select ***Yes*** to wipe the HPA or DCO area of the drive.
- If a Wipe Pattern was selected, tap the ***Passes*** icon to edit the number of passes and what gets written on each pass. If DoD was selected, a 7th pass value must be chosen.

7. Tap the ***Format Settings*** icon to change the Format setting.
   a. Set ***Format*** to ***ON***.
   b. Select the desired ***File System*** (***EXT4*** or ***NTFS***).
   c. Set ***Encryption*** to ***ON***. When finished, tap the ***OK*** icon.

The ZXi-Forensic will perform each of the settings sequentially. For example, if Secure Erase is set to ON, a Wipe Pattern mode is specified, and Format is set to On, the ZXi-Forensic will first secure erase the drive, then wipe the drive according to the mode specified, then format the drive.

8. Tap the ***Start*** icon to start the wipe task. The ZXi-Forensic will perform a Secure Erase first (if selected), then a Wipe Pattern (if selected), then finally a Format with encryption.

6.1.2 Using previously encrypted Destination drives

If a previously encrypted Destination drive is going to be used and the ZXi-Forensic has been turned off since the last time the encrypted drive was used, the encryption settings must be set with the same encryption settings previously used before connecting the drive.

1. Turn the ZXi-Forensic on. Make sure the previously encrypted Destination drive is not connected.
2. From the main menu, select ***System Settings*** from the types of operations on the left side.
3. Tap the ***Encryption Settings*** tab.
4. Set the ***Cipher Mode***, ***Cipher***, ***IV Generation***, and ***Password*** that was used for the previously encrypted Destination drive.
5. Connect the previously encrypted Destination drive to one of the Destination ports.

6.2 Decrypting a previously encrypted drive

In order to mount and read an encrypted Destination drive in Windows, Logicube recommends one of two third-party utilities called ***TrueCrypt*** or ***FreeOTFE***. Other utilities may work, but are not supported or tested by Logicube.

TrueCrypt can be downloaded from (for decryption purposes only):
http://truecrypt.sourceforge.net/

FreeOTFE can be downloaded from:
http://sourceforge.net/projects/freeotfe.mirror/files/latest/download

To install FreeOTFE the verification of signed drivers must be disabled. Here is a link that might help:
http://en.kioskea.net/faq/3914-windows-7-disable-signature-verification-of-drivers

There are other ways of installing unsigned drivers. Several different ways can be found by searching the Internet for “install unsigned drivers”.

If the Destination drive was formatted with the EXT4 file system, please read ***Chapter 7*** for information on how to view EXT4 in Windows.

6.2.1 Which decryption software to use?

The decryption software to use (TrueCrypt or FreeOTFE) depends on how the Destination drive was encrypted.

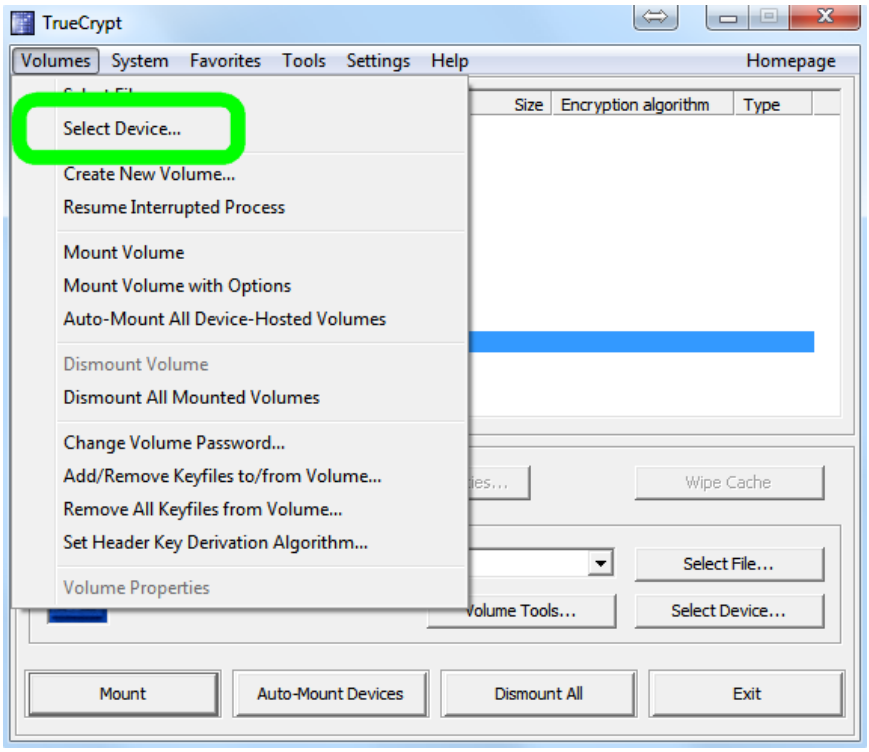
- **TrueCrypt –** Use this software if the Destination drive was encrypted with the ***TC-XTS*** cipher mode.
- **FreeOTFE –** Use this software if the Destination drive was encrypted with the ***CBC*** or ***ECB*** cipher mode.

6.2.2 Decrypting using TrueCrypt

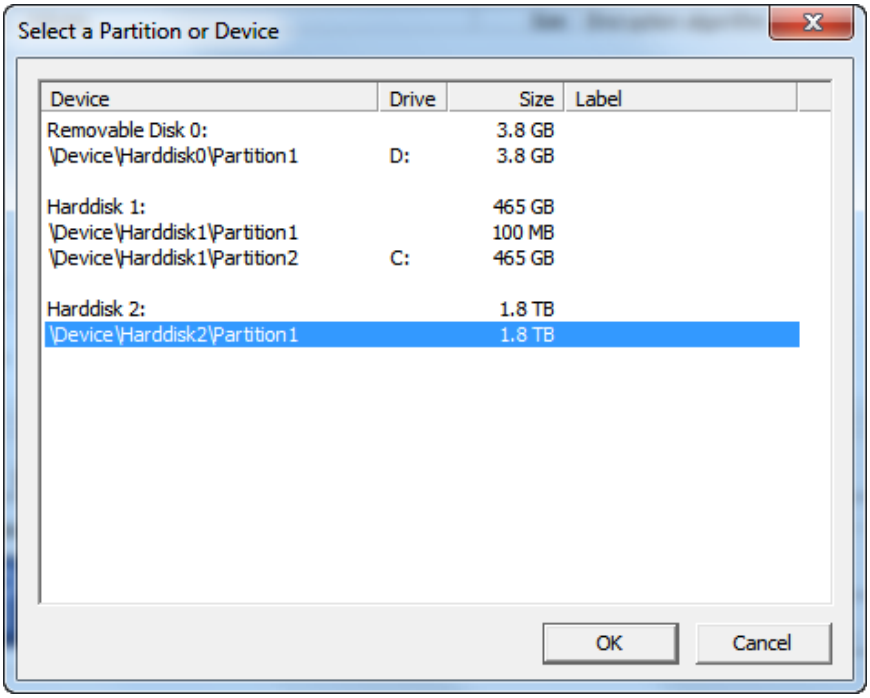
Requirements:

- TrueCrypt properly installed.
- A drive encrypted by the ZXi-Forensic using the TC-XTS cipher mode connected to the computer with TrueCrypt.

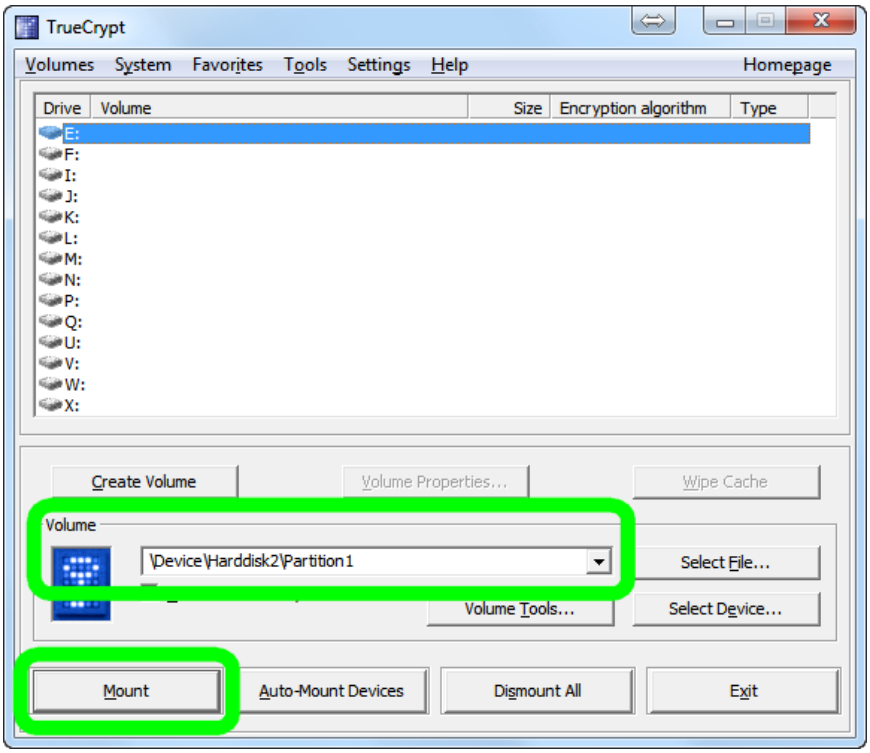
1. Open TrueCrypt and select ***Volumes*** from the menu system, then click ***Select Device…***



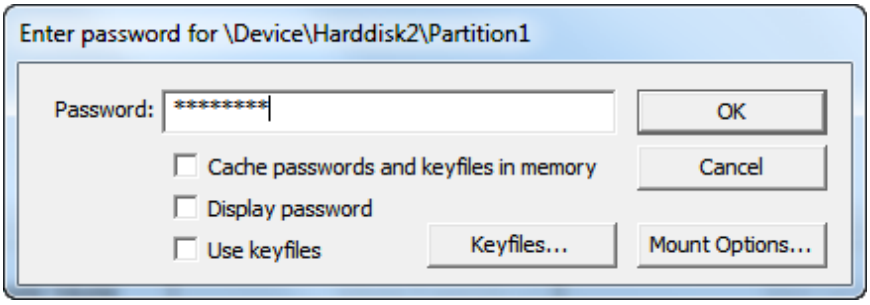
2. The 'Select a Partition or Device' window will appear. Select the partition of the drive. Do not select the actual drive itself. Click ***OK*** to continue.



3. Verify the ***Volume*** shows the correct device and partition. Click ***Mount*** to continue.

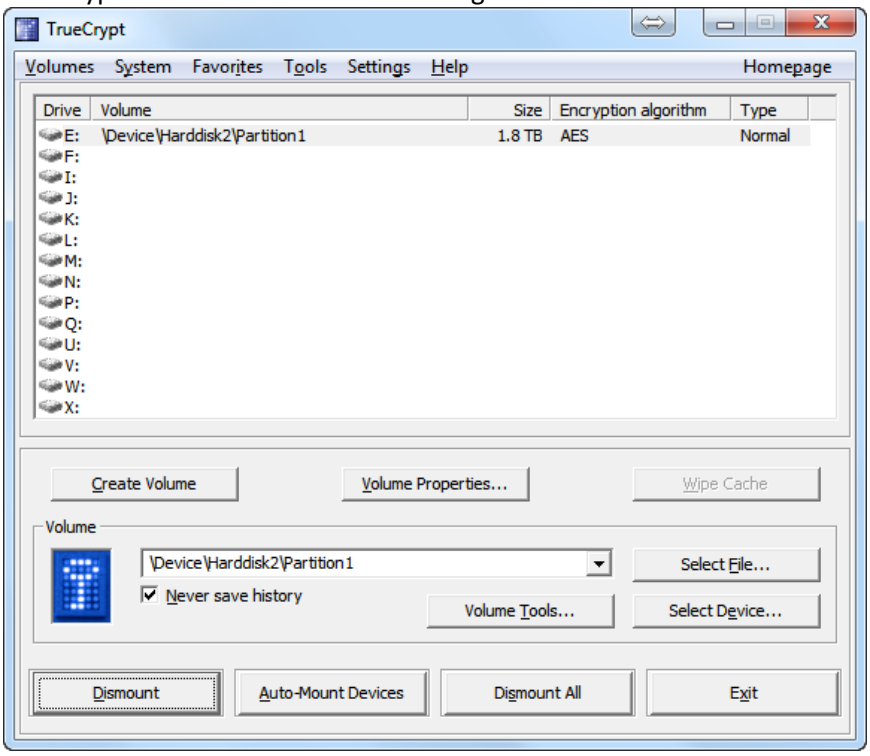


4. The password screen will appear. Enter the password used to encrypt the drive then click ***OK*** to continue.

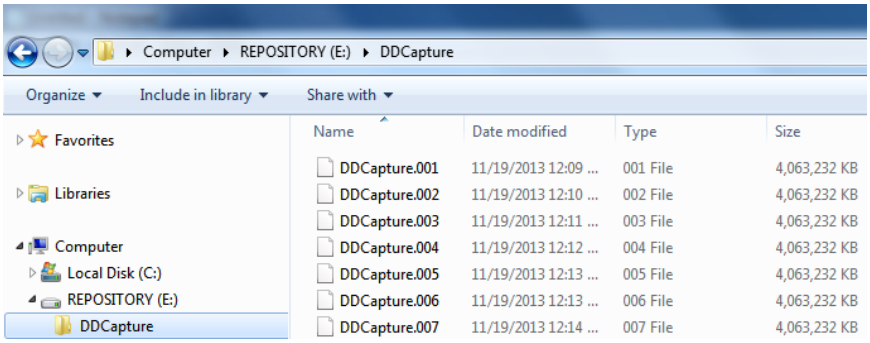


TrueCrypt has a setting to mount the drive as "read-only" which is a software write-block. This setting can be found by clicking ***Mount Options…*** A hardware write-block device may be used instead, if needed.

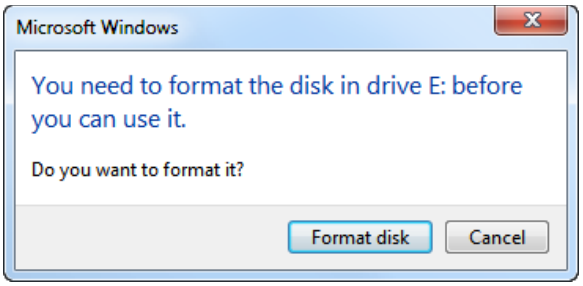
5. TrueCrypt will mount the drive and assign it a drive letter.

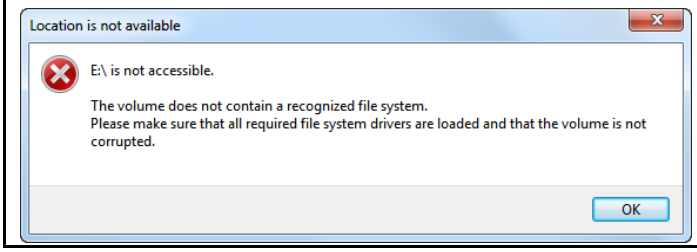


6. The Destination drive should now be accessible in Windows.



If the Destination drive was formatted with the EXT4 file system, and Ext2Fsd is not installed, the following messages may appear in Windows. Make sure Ext2Fsd is installed if the Destination drive was formatted with the EXT4 file system.



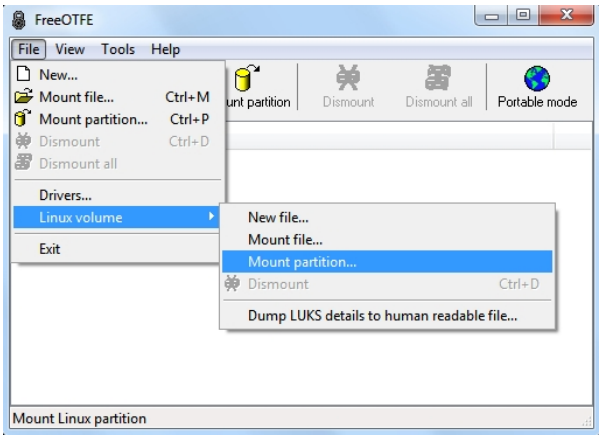


6.2.3 Decrypting using FreeOTFE

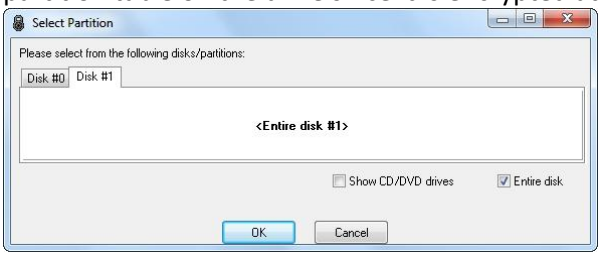
Requirements:

- FreeOTFE properly installed
- A drive encrypted by the ZXi-Forensic using the CBC or ECB cipher mode connected to the computer with FreeOTFE.

1. Open FreeOTFE. In the main window, click ***File*** then ***Linux volume*** then ***Mount partition…***

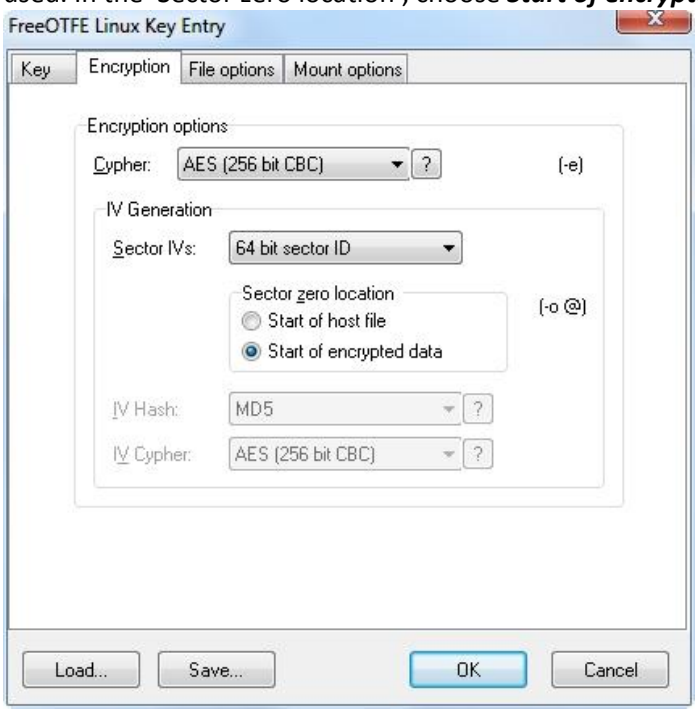


2. Select the encrypted disk to mount (in this example, it is Disk #5). Place a check mark on the ***Entire disk*** option. FreeOTFE cannot read the partition table on the drive since it is encrypted at this time.

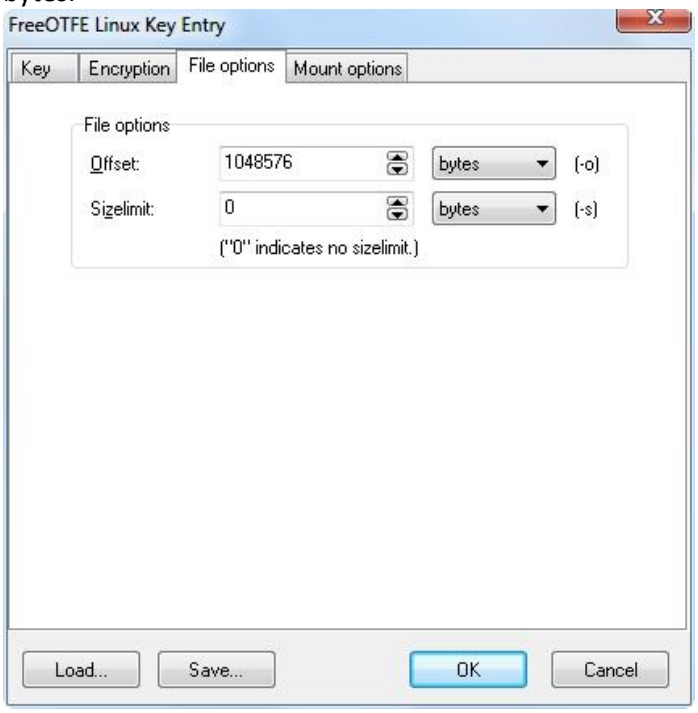


3. In the Key tab, enter the Key (password) and make sure the ***Hash*** is set to ***RIPEMD-160***.

4. In the Encryption tab, set the ***Cipher*** to ***AES (256 bit CBC)***. Set the ***Initialization Vector (IV) generation*** method to match what was used in the ***IV Generation*** on the ZXi-Forensic. In this example, "plain64' was used. In the 'Sector zero location', choose ***Start of encrypted data***.

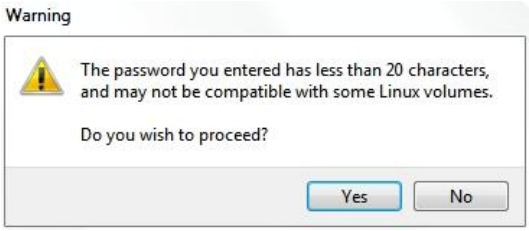


5. In the ***File options*** tab, set the ***Offset*** to 1048576. Since the ZXi-Forensic uses the EXT4 file system, the offset is at 2048 sectors, or 1048576 bytes.

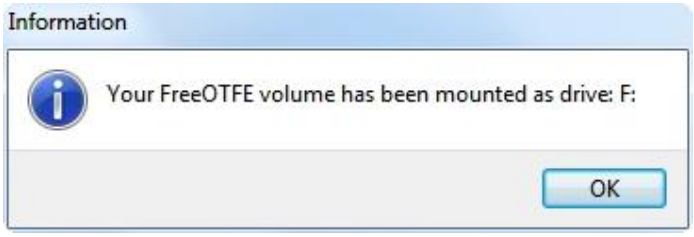


OPTIONAL: In the ***Mount options*** tab, the disk can also be mounted with write protection. To do so, make sure the ***Mount readonly*** option is checked. Windows may not mount the drive if this option is checked. If this is the case, use a write-protect device and uncheck the ***Mount readonly*** option.

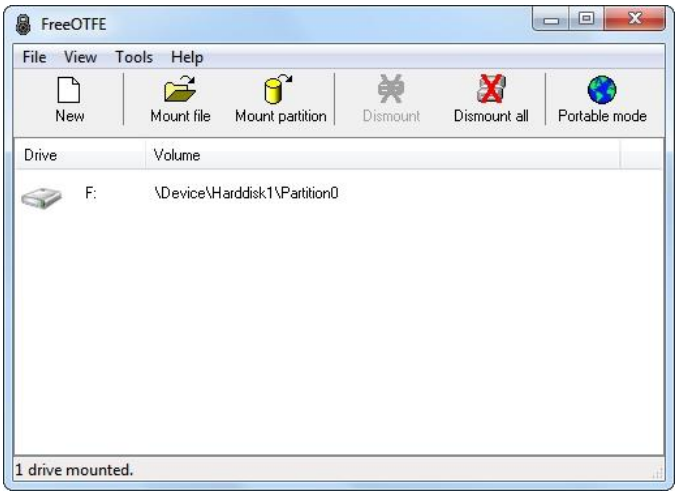
6. Click the ***OK*** button. The following warning screen may appear. Click the ***Yes*** button to continue.



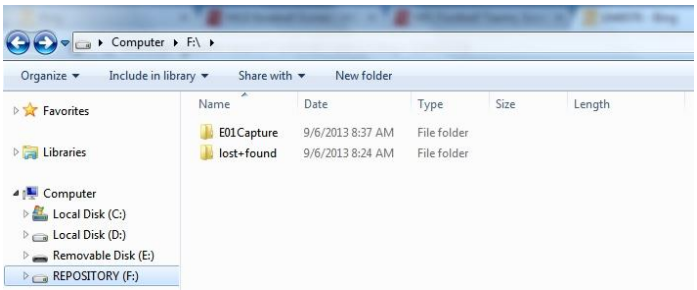
7. FreeOTFE will mount the drive and assign a drive letter.



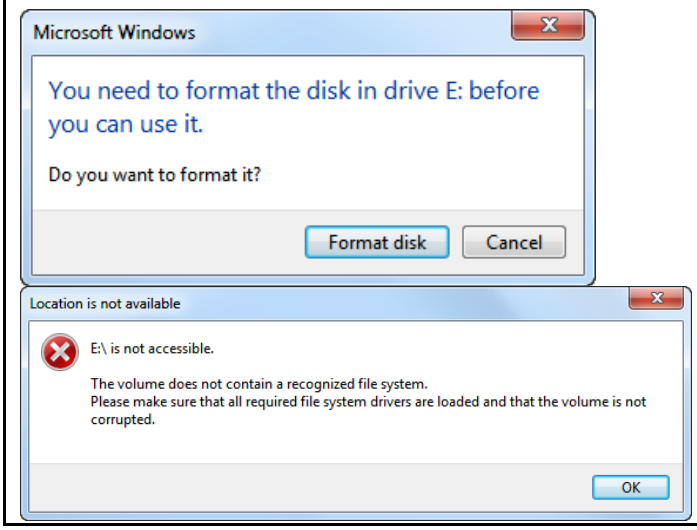
8. Click the ***OK*** button to continue. The drive should appear in the FreeOTFE window.



9. The Destination drive should now be accessible in Windows.



If the Destination drive was formatted with the EXT4 file system, and Ext2Fsd is not installed, the following messages may appear in Windows. Make sure Ext2Fsd is installed if the Destination drive was formatted with the EXT4 file system.



7: Updating the ZXi-Forensic Software

7.0 Loading New Software

This section is reserved. Please contact Logicube Technical Support for questions regarding software (support@logicube.com or 818.700.8488, opt. 3).

8: Remote Operation

8.0 Remote Operation – Introduction

The ZXi-Forensic comes with a gigabit network connection in the back of the unit. Connecting the ZXi-Forensic to a network allows remote access to the ZXi-Forensic from any computer within the same network.

The ZXi-Forensic is configured for DHCP by default. See **Section 8.5** for instructions on how to configure the ZXi-Forensic with a Static IP address.

The ZXi-Forensic is setup with a Zero Configuration Network (Zeroconf). There are two ways to access the ZXi-Forensic:

- Web interface – A graphical interface using an Internet browser where the screens are shown exactly the way they appear on the ZXi-Forensic
- Command Line Interface (CLI) – A text only command line interface that can be accessed one of two ways:
  i. Telnet (via a network connection)
  ii. SSH (Secure Shell via a network connection)

BROWSER COMPATIBILITY: Google Chrome or Mozilla Firefox is recommended. Other browsers may not compatible.

8.1 Web Interface

Using a web browser, go to the IP address or the name of the ZXi-Forensic with its serial number. Both IP address and serial number can be found by going to the ***Statistics*** screen on the ZXi-Forensic. For example, browse to http://192.168.1.100 or http://ZXif-XXXXXX/ where XXXXX is the 6 digit serial number of the ZXi-Forensic. The ZXi-Forensic's web interface will appear on the browser screen. All screens and operations available on the ZXi-Forensic will be available on the browser.

On some browsers or Operating Systems, the ZXi-Forensic will need to be accessed by browsing to http://ZXif-XXXXXX.local/.

The ZXi-Forensic can be controlled by clicking on the icons appearing on the browser window.

8.2 Command Line Interface (CLI)

The ZXi-Forensic also has a CLI, or Command Line Interface. This interface has no graphical content and is all command line (text) based and is for advanced users who have knowledge of command line functions. This type of connection requires a Telnet or SSH client. There are several telnet and SSH clients available from different software companies. Microsoft Windows also has a built-in Telnet client that can be used.

- Windows Vista, 7, 8, and 8.1 have a built-in Telnet client but is not installed by default. Installing the Telnet client may require the assistance of a Network or Systems Administrator. Other third party Telnet programs are available.
- All versions of Windows do not have a built-in SSH client.
- The instructions in this manual only refer to the clients that come with Windows. There are many third party Telnet or SSH clients available. For instructions and support for third party clients, please contact the software manufacturer.

8.3 Installing the Telnet client in Windows Vista, 7, 8, or 8.1

By default, the Telnet Client is not installed with Windows, but it can be installed it by following the steps below:

1. Open ***Control Panel*** and select either ***Programs & Features*** or ***Programs***.
2. Click ***Turn Windows features on or off***. If a prompt for an administrator password or confirmation, type the administrator password or provide confirmation (A Network or Systems Administrator may be required for administrator access).
3. In the Windows Features dialog box, select the Telnet Client check box.
4. Click OK. The installation might take several minutes.

8.3.1 Connecting via Telnet

Once the Telnet client is installed, follow the steps below to connect using the Windows Telnet client.

1. Connect the ZXi-Forensic to the network by attaching a network cable (CAT 6 type) to the RJ45 connector in the back of the ZXi-Forensic.
2. Turn the ZXi-Forensic on and allow it to boot up completely.
3. Open the Telnet client. For Windows Vista or 7, click ***Start*** and in the ***Search*** field, type ***Telnet***. Telnet should appear in search results.
4. Type ***open*** followed by the IP address or name of the ZXi-Forensic. For example ***open 192.168.1.100*** or ***open ZXif-XXXXXX*** where XXXXXX is the 6 digit serial number of the ZXi-Forensic, then press Enter. The ZXi-Forensic login screen should appear.

   Note: On some Operating Systems, the ZXi-Forensic will need to be accessed by opening ZXif-XXXXXX.local.

5. Login with the username "***it***" (without the quotes) and the password "***it***" (without the quotes).
6. The following prompt should appear in the Telnet window:
7. The ZXi-Forensic can now be configured or managed via the command line interface.

8.3.2 Connecting via SSH

Connecting to the ZXi-Forensic via SSH (Secure Shell) is very similar to connecting via Telnet. Since Windows does not have a built-in SSH client, a third party SSH client will need to be downloaded and installed to connect via SSH. For instructions and support on how to use third party SSH clients, please contact the SSH client's manufacturer.

1. Connect the ZXi-Forensic to the network by attaching a network cable (CAT 6 type) to the RJ45 connector in the back of the ZXi-Forensic.
2. Turn the ZXi-Forensic on and allow it to boot up completely.
3. Open the SSH client and select an SSH connection.
4. Connect to the ZXi-Forensic either by IP address or by name. The name of the ZXi-Forensic will be **ZXif-*XXXXXX*** where XXXXXX is the serial number of the ZXi-Forensic).

   On some Operating Systems, the ZXi-Forensic will need to be accessed by opening ZXif-XXXXXX.local.

5. Login with the username "***it***" (without the quotes) and the password "***it***" (without the quotes).
6. The following prompt should appear in the SSH window:
7. The ZXi-Forensic can now be configured or managed via the command line interface.

8.4 Zero Configuration Networking (Zeroconf)

The ZXi-Forensic has the capabilities for Zero Configuration Networking (Zeroconf). Zeroconf allows devices to automatically create a usable computer network based on the Internet Protocol Suite (TCP/IP).

For example, when the ZXi-Forensic is connected (connected via a network cable) directly to a Windows based computer that is DHCP enabled, both the ZXi-Forensic and the Windows based computer will automatically configure themselves to be seen by each other using TCP/IP.

8.5 Configuring the ZXi-Forensic with a static IP address

The ZXi-Forensic is DHCP enabled by default. Some networks do not support DHCP and require a static IP address. The ZXi-Forensic can be configured with a static IP address and needs to be connected to a network with DHCP first.

8.5.1 Step-by-step instructions – Static IP address

1. Connect the ZXi-Forensic to a network with DHCP.
2. Turn the ZXi-Forensic on. The ZXi-Forensic should automatically assign itself an IP address that the Windows computer can see. Go to the ***Statistics*** screen on the ZXi-Forensic and take a look at the HostName and IPAddress.
3. Using Telnet or SSH, connect to the ZXi-Forensic. Instructions on how to connect via Telnet or SSH can be found in **Section 10.3.1 or 10.3.2**.
4. Once logged in to the ZXi-Forensic via CLI, follow these steps to set the IP address to a static IP:
    a. From the main prompt, type ***command*** then press the enter key.
    b. Type ***config*** then press the enter key.
    c. Type ***net del -n eth0*** to delete the current network configuration.
    d. The following information is required: a static IP, the netmask, network gateway, the network nameserver, the domain. For example:
        i. IP Address: 192.168.1.123
        ii. Netmask: 255.255.255.0
        iii. Gateway: 192.168.1.10
        iv. Nameserver: 192.168.1.10 (typically the same as the gateway unless the network has a specific nameserver IP.
        v. Domain: LG

> Networks are configured differently and the necessary settings may require the assistance of a Network or Systems Administrator.

    e. Based on the info above, the example for this line will be to type (case sensitive): ***net add -n eth0 -t static -a 192.168.1.143 -m 255.255.255.0 -g 192.168.1.1 -N 192.168.1.1 -d lg*** then press the enter key.
    f. The ZXi-Forensic should respond with the following: Command (DbNetworkConfig) Successful

g. Now we need to save the configuration. Type ***db save staticip.db*** then press the enter key. A “Successful” message should appear.

h. Type ***db load staticip.db*** to load the database configuration.

i. Perform a full shut down on the ZXi-Forensic. Wait about 30 seconds then turn the ZXi-Forensic back on. The ZXi-Forensic should load the new configuration. The IP address can be checked by going to the Statistics screen.

9: Security – Changing the default passwords

9.0 Changing the default passwords - Introduction

The ZXi Forensic comes with default accounts for the Command Line Interface. It is highly recommended to change the default passwords for security purposes.

- logicube
- it

If the new password(s) cannot be remembered, a system recovery must be performed to reset the passwords back to the default values.

9.0.1 Changing the *logicube* password

For the username: logicube

1. Telnet or SSH to the ZXi Forensic and login using the user ***logicube*** and the password ***logicube***. Alternatively, you can connect a USB keyboard one of the four USB ports in the back of the ZXi-Forensic then use the following key combinations: ***Alt+2*** then ***Alt+Shift+Enter***.
2. Once logged in and/or the logicube prompt appears, type the following commands, one line at a time (Press the Enter key after each command/line):
   sudo mount -o remount,rw /
   passwd
3. The following prompt will appear:
   Changing password for logicube.
   (current) UNIX password:
4. Type the current password (by default, “logicube” without the quotes) then press the Enter key. The following prompt will appear:
   Enter new UNIX password:
5. Type a new password then press the Enter key. The following prompt will appear:
   Retype new UNIX password:
6. Type the new password again then press the Enter key. The following response should appear:
   passwd: password updated successfully

7. Type the following command then press the Enter key:
   sudo mount -o remount,ro /
8. Close the Telnet or SSH client or if you are directly connected to the ZXi Forensic with a USB keyboard, use the following key combinations:
   Alt+1

9.0.2 Changing the *it* password

To change these passwords, you will need to telnet or SSH to the ZXi Forensic (see ***sections 8.3.1 and 8.3.2*** for instructions on how to connect via Telnet or SSH).

1. Login with the username ***it*** and the default password ***it***. The Command Line Interface (CLI) should appear.
2. Type the following commands one line at a time (Press the Enter key after each command/line):
   command
   config
   user set –n it –p xxxxx –g itgrp

   xxxxx would be the new password you would like to use for the IT user account.

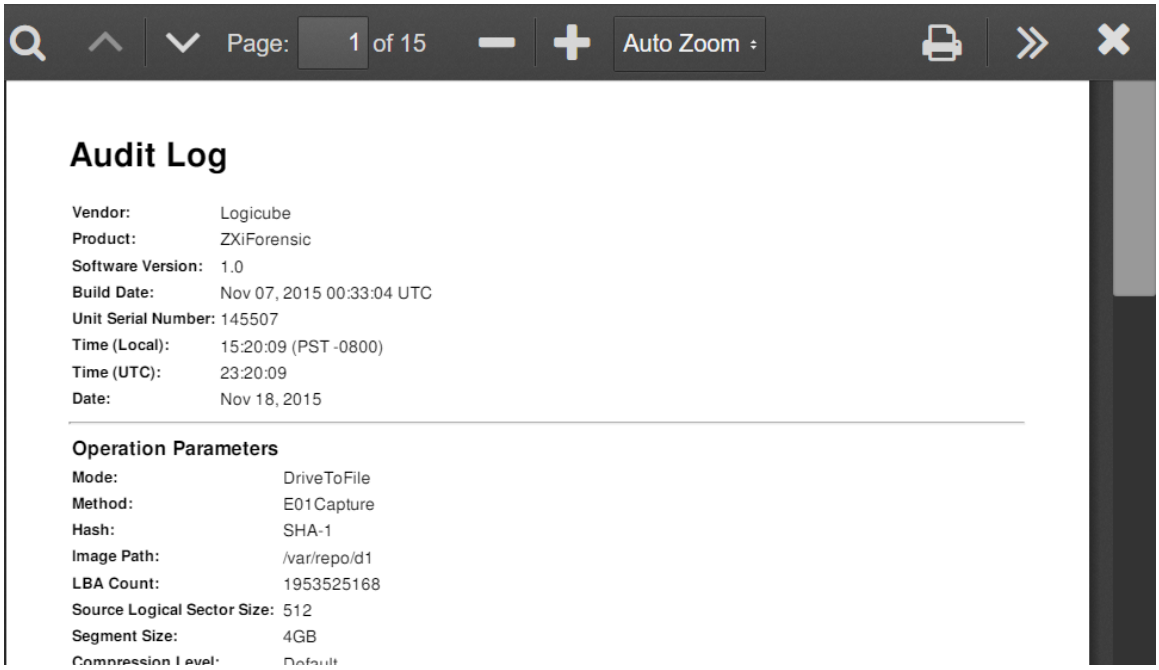
3. Once the new password is entered, the telnet or SSH connection should be terminated/disconnected.

10: Printing Log Files

10.0 Printing Log Files - Introduction

When viewing log files through the ZXi Forensic touch screen or web interface, there is a Print icon located on the top right of the screen. This icon allows the printing of the currently viewed log file. There are two ways to print log files:

- Recommended - From the Web Interface using a computer on the same network the ZXi Forensic is connected to (see ***Section 8.1 – Web Interface***). This will allow the printing to any printer already set up on the computer being used.
- From the touch screen on the ZXi Forensic. This will print to a configured local printer (connected via USB to the ZXi Forensic) or to a networked printer. See ***Section 10.2 – Configuring a local or networked printer*** for instructions on how to set up a local or networked printer on the ZXi Forensic.



10.1 Printing from the Web Interface

When the ***print icon*** is used on the web interface, the browser's print dialog screen will appear. This will allow printing to any configured printer on the computer, as it is using the computer's web browser and Operating System to print.

10.2 Configuring a local or networked printer

The ZXi Forensic can also print to a local (through USB) or networked printer. The printer has to be configured using the Command Line Interface (CLI, see ***Section 8.3.1*** and ***Section 8.3.2*** for instructions on how to connect to the CLI using a Telnet or SSH client).

Local printers will need to be connected to the ZXi-Forensic through an available USB 2.0 port in the back of the ZXi-Forensic.

Networked printers will be seen by the ZXi-Forensic when connected to the same network.

Once the printers are set up and configured, the configuration must be saved.

10.2.1 Step-by-step – Configuring a local or networked printer

1. Connect the ZXi-Forensic to a network with DHCP. For networked printers, make sure the ZXi-Forensic is connected to the same network. For local printers, connect the printer to an available USB 2.0 port located in the back of the ZXi-Forensic.
2. Turn the ZXi-Forensic on. The ZXi-Forensic should automatically assign itself an IP address that the Windows computer can see. Go to the ***Statistics*** screen on the ZXi-Forensic and take a look at the HostName and IPAddress.
3. Using Telnet or SSH, connect to the ZXi-Forensic. Instructions on how to connect via Telnet or SSH can be found in **Section 7.3.1 or 7.3.2**.
4. Once logged in to the ZXi-Forensic via CLI, type ***command*** then press theenter key.
5. Type ***config*** then press the enter key.
6. Type ***printer search*** then press the enter key. This will instruct the ZXi-Forensic to search for all local and networked printers.

   Here is an example of the search results:

```
class        : network
make_model   : HP Color LaserJet 3600
uri          : socket://192.168.1.158

class        : network
make_model   : HP LaserJet P4015
uri          : socket://192.168.2.41
```

```
class        : network
make_model   : EPSON WF-2530 Series
uri          : lpd://192.168.2.48:515/PASSTHRU

class        : network
make_model   : Brother HL-4150CDN series
uri          : lpd://BRN001BA9A8F7EA/BINARY_P1
```

7. Add the printer using the following syntax (case sensitive):

printer add –n <name_for_the_printer> -N –u <uri> -m <make_model>
Or
printer add –n <name_for_the_printer> -D –u <uri> -m <make_model>

For example, to add the networked HP Color LaserJet 3600, type the following:
printer add -n 3600 -N -u "socket://192.168.1.158" -m "HP Color LaserJet 3600"

The CLI should respond with: ***Command (DbPrinterConfig) Successful***

8. To save the printer configuration, ***db save printer.db*** (or you can use any name.db you prefer) then press the enter key. A “Successful” message should appear.
9. Type ***db load printer.db*** to load the database configuration. Each time the ZXi-Forensic is turned on, the local or networked printer should be available on the ZXi-Forensic’s touch screen.

11: Optional Adapters

11.0 Optional Adapters – Introduction

Logicube has many different adapters that allow the imaging of almost any drive. This chapter lists some of the available optional adapters that can be used with the ZXi-Forensic.

11.1 mSATA (mini-SATA) Drives

mSATA (mini-SATA) drives can be connected using the adapter shown above. This mSATA adapter has a standard SATA connector that can connect to the ZXi-Forensic using the standard SATA cables included.

11.2 eSATA Drives

eSATA drives can be connected using Logicube's eSATA cable. Connect the SATA end of the eSATA cable to the ZXi-Forensic and connect the eSATA end of the cable to the eSATA drive. Power to the eSATA drive should come with the drive (typically some type of external AC adapter or power cable).

11.3 Flash Memory Reader

Flash memory cards can be connected using the adapter shown above.

> Third party multi-card readers are not supported and may not work with the ZXi-Forensic.

The multi-card reader supports the following formats:

- CF (CompactFlash)
- SD/SDXC/MMC
- Micro SD
- Memory Stick (MS)
- Memory Stick Duo (M2)
- X-Card

> Attach only one flash memory card to the multi-card reader at a time.

11.4 USB 3.0 to SATA Adapter

Logicube has qualified a USB 3.0 to SATA Adapter for use with the ZXi-Forensic. This adapter provides the capability to connect SATA drives to the USB 3.0 ports on the ZXi-Forensic and uses a USB 3.0 to SATA converter. USB 3.0 is a new technology and USB 3.0 controller manufacturers may have variations in device designs that have inconsistent adherence to USB 3.0 specifications. This adapter and other USB 3.0 enclosures may experience communication disruption between devices. If the adapter is not detected properly we have found that using a USB 3.0 hub may stabilize and regulate the communication between the Adapter or USB 3.0 enclosure, and the ZXi-Forensic, allowing the device to be detected properly. For information on the USB 3.0 hub, please see **Section 9.5**.

11.5 USB 3.0 Hub

Some USB 3.0 is a new technology and USB 3.0 controller manufacturers may have variations in device designs that have inconsistent adherence to USB 3.0 specification. This may result in non-detection of the USB 3.0 device on certain equipment (including desktops, laptops or the ZXi-Forensic). If a USB 3.0 device cannot be detected on the ZXi-Forensic USB ports we have found that using a USB 3.0 hub may stabilize and regulate the communication between the USB 3.0 device and the ZXi-Forensic, allowing the device to be detected properly. We have identified and qualified a USB 3.0 hub which is available as an option.

12: FREQUENTLY ASKED QUESTIONS

12.0 FAQs

This section is reserved.

13: Index

Technical Support Information

For further assistance please contact

Logicube Technical Support at: (**001) 818 700 8488 7am-5pm PST, M-F (excluding US legal holidays)**
or by email to **techsupport@logicube.com**

Software Attribution

Ubuntu 12.04 LTS (http://www.ubuntu.com)
Linux Kernel (3.2.48) (GPL v2) (http://www.kernel.org) (modified)
libcli (1.9.5) (LGPL v2.1) (https://github.com/dparrish/libcli) (modified)
monitorix (3.2.1) (GPL v2) (http://www.monitorix.org) (modified)