FORENSIC Z Xi™

Exceptional Performance, Network-Capable, High-Volume Forensic Imager & Uploader

- **Blazing fast imaging speeds of over 50GB/min**
- **Designed for digital forensic labs**
- **Three Gigabit Ethernet ports**
- **Network "Push" feature to upload images to a network repository from 3 evidence drives simultaneously**
- **Image from 3 suspect to a network repository or 3 evidence drives simultaneously**
- **Optional expansion kit adds 3 additional destination drives**

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 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.

FEATURES

- **High speed imaging** at over 50GB/min*
- **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 or SHA-1 or SHA-256 **verification** is available. Dual hash (MD5+SHA-1) planned for a future release
- 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.
- **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 **compact flash 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 of hard drive contents**. Preview/triage 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 files types (such as .doc and .xls) can be viewed by connecting 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.

FEATURES cont'd.

- **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.
- **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.
- **Image restore feature**. File to drive mode restores DD, E01, EX01 images created by the ZXi- Forensic to another drive. Planned for a future release.
- 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, .jpeg, .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 programs such as FreeOTFE or TrueCrypt. VeraCrypt support is planned for a future release.
- **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 O/S 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 enclosure. 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 manipulates the DCO and HPA areas of destination drives, the ability to set password-protected user profiles and save configurations, drive "timeout" feature automatically puts drives in stand-by mode after a specified idle time, drive spanning, end of task audible beep (planned for future release),blank disk check (planned for a future release), large 7" color touch screen display, on-screen keyboard, four USB 2.0 host ports for mouse or printer connectivity, an HDMI port to connect a projector or monitor.

IN THE BOX

The following items are included with the ZXi Forensic:

- Power supply & power cord
- 6 SAS/SATA data/power cables
- 3 CAT-6 network cables
- Users' manual on CD-ROM

OPTIONS

The following options are available with the ZXi Forensic:

- 3-target expansion kit (includes 1 SATA only drive stations, 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

SPECIFICATIONS

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

*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.