Falcon®-NEO User's Manual

Logicube, Inc.
Chatsworth, CA 91311
USA
Phone: 818 700 8488
Fax: 818 700 8466

Version: 2.3
Date: 10/22/2019
MAN-FALCON-NEO

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

- By website: www.logicube.com
- By email: techsupport@logicube.com
- By telephone: +1 - (818) 700 8488 ext. 3 between the hours of 8 a.m. – 5 p.m. PT, Monday through Friday, excluding U.S. legal holidays.

Table of Contents

1: Introduction

1.0 Introduction to the Logicube Falcon-NEO

The next-generation of our ground-breaking Falcon® forensic imager, the Falcon-NEO has been engineered specifically for digital forensic investigations. Delivering high performance and advanced features, the Falcon-NEO is designed to meet the challenges of digital investigations head-on. Efficient and secure digital evidence collection is accomplished with a feature-set that provides sophisticated functionality with a goal to shorten acquisition time. Future-focused, the Falcon-NEO sets new standards in digital forensic imaging technology.

1.1 Features

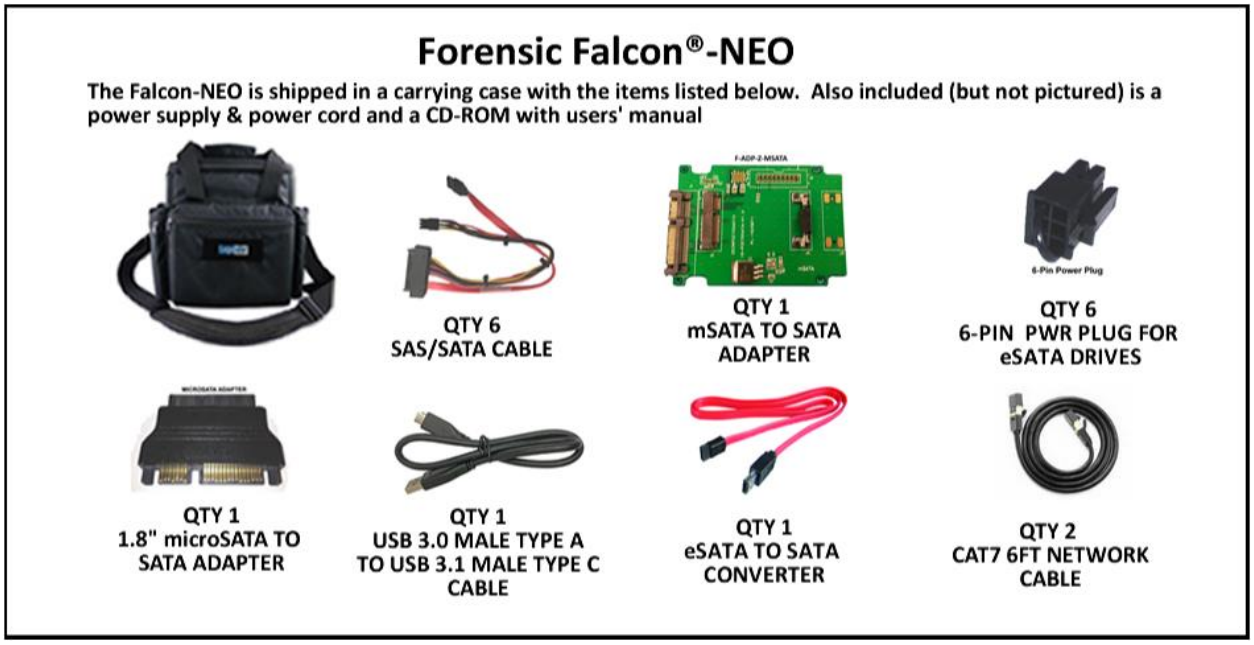
- The Falcon®-NEO achieves imaging speeds **surpassing 50GB/min** and can clone PCIe to PCIe at speeds at over 90GB/min.
- I**mage and verify to multiple image formats**; native copy, .dd, dmg, e01 and ex01. The Falcon-NEO provides MD5, SHA1, SHA256, and dual hash authentication at extremely fast speeds
- **6 write-blocked source ports** include 2 SAS/SATA,1 USB 3.0, 1 PCIe, 2 I/O ports for use with optional I/O cards including Thunderbolt™ 3/USB-C.
- **9 destination ports** include 2 SAS/SATA, 2 SATA, 3 USB 3.0 and 1 PCIe and 1 I/O port for use with optional I/O cards including Thunderbolt 3/USB-C.

- **Concurrent Image+Verify.** Imaging and verifying concurrently takes advantage of destination hard drives that may be faster than the source hard drive. Duration of total image+verify process time may be reduced by up to half.
- **Targeted/Logical Imaging shortens acquisition time.** Create a logical image by using pre-set, custom, or file signature filters, and/or keyword search function to select and acquire only the specific files you need. Format output to L01, LX01, ZIP, or directory tree.
- Image directly to/from **Thunderbolt™3/USB-C**, **USB 3.1 Gen 2 external drives and enclosures** with an optional I/O card. Organizations can take advantage of Thunderbolt 3 technology's fast transfer speeds when imaging directly to large capacity Thunderbolt 3 RAID storage enclosures for evidence data collection. The card connects to the Falcon-NEO's 2 write-blocked source I/O ports or 1 destination I/O port. The I/O card does not currently support imaging in TDM from Mac® systems, refer to the Falcon-NEO users' manual on how to image from Mac systems in TDM using USB ports or our iSCSI boot device.
- **Two 10GbE network ports** provide fast network imaging performance. Image to/from a network repository using CIFs or iSCSI. Connect to a 10GbE NAS as a source and connect to a network using the 2nd 10GbE port to minimize bottlenecks. Two ports provide a secure method to isolate the source network/NAS from the destination NAS/network.
- **APFS Support**. The Falcon-NEO supports logical imaging (using our file to file mode) from drives formatted to APFS (Apple File System). Requires use of *Advanced* set-up, reference our users' manual for complete information. The Falcon-NEO can also view and browse APFS files using our file browser feature.
- **Network Capture.** Capture network traffic, internet activity, and VOIP. Sniff data on a network and store captured packets on a hard drive connected to Falcon-NEO, data is saved to a .pcapng file format.
- **Image from a Mac® computer with USB-C ports** using a USB-C to USB-A cable and Target Disk Mode or use Logicube's USB boot device to image a source drive from a Mac computer on the same network without booting the Mac computer's native OS. The Falcon-NEO supports imaging from **MacBook Pro® systems.**
- **Image from a PC/laptop without removing hard drives.** Create a forensic bootable USB flash drive to image a source drive from a computer on the same network without booting the computer's native OS. Supports **Surface Pro 4 and above** laptops.
- **File Browser/Write-Blocked Drive Preview**. Provides logical access to source or destination drives and network repositories connected to Falcon-NEO. View the drive's partitions and contents and view text files, jpeg, PDF, XML, HTML files. View the contents of .dd, e01, ex01, dmg, L01 image files created by Falcon-NEO. Preview on a PC/laptop or over a network via SMB or as an iSCSI target.
- **Multi-Task.** Image from multiple sources to multiple destinations, including a network repository, simultaneously. Image to one destination while hashing and/or wiping a second drive at the same time. Perform up to 5 tasks concurrently.
- **Built-in support for SAS/SATA/USB3/PCIe** storage devices. Thunderbolt™ external storage solutions are supported with an optional I/O card. PCIe M.2, including NVMe drives, PCIe cards, IDE drives and flash drives require optional adapters. SCSI and FireWire® devices are supported with optional modules that connect to the Falcon-NEO's PCIe ports. Adapters for mSATA, micro SATA and eSATA drives are included with the unit.

- Format destination drives **to NTFS, exFAT, EXT4 or FAT32** file systems. Image from source drives formatted to any major file system.
- **Capture path selection**. Add folders to the destination repository and then select and image to the named folder. Empty folders can be deleted, and folders can be renamed.
- **Parallel Imaging.** Perform multiple imaging tasks from the same source drive to multiple destinations using different imaging formats.
- **BitLocker Support.** Image source drives that have been encrypted using BitLocker. Decrypt partitions (requires the recovery key or password) and then image the selected partitions. A password or a newly generated BEK (BitLocker Encryption Key) file is required to unlock FIPS-compliant BitLocker encryption.
- **Secure sensitive evidence data** with whole drive, open standard drive encryption using the NIST recommended **XTS-AES 256 cipher mode.** Decryption can be performed using the Falcon-NEO or by using open source software programs such as VeraCrypt, TrueCrypt or FreeOTFE.
- **Wipe drives to DoD specifications** or use secure erase to wipe drives. Wipe at speeds of 30GB/min for SATA drives and 72GB/min for PCIe drives.
- **Audit trail/Log files** provide detailed information on each operation. Log files can be viewed on Falcon-NEO or via a web browser, exported to XML, HTML or PDF format to a USB enclosure.
- **Additional features** include **remote operation, internal removable storage drive for secure/classified locations,** partition imaging, a task macro, a resume feature for interrupted tasks, image restore, reverse read, network "Push" feature, HPA/DCO capture, save configuration settings and set password-protected user profiles, image from CD/DVD Blu-Ray media, drive spanning, color touchscreen display, HDMI port, USB 3.0 ports for keyboard, mouse, or printer, blank disk check, drive trim, and S.M.A.R.T. data.

* The Forensic Falcon-NEO achieves speeds surpassing 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.

1.2 In the Box



The Falcon-NEO is shipped in a soft-sided carrying case that includes:

- The Logicube Falcon-NEO unit
- AC adapter/Power supply and US power cord
- QTY: 6 – SAS/SATA data & power cables
- QTY: 2 – CAT7 network cables
- eSATA to SATA cable (18")
- mSATA to SATA adapter
- micro SATA adapter
- USB 3.0 male type A to USB 3.1 male type C cable
- QTY: 6 – 6-pin power plugs for eSATA devices
- CD-ROM containing the user's manual

1.3 Options

The following options are available for the Falcon-NEO:

- The SCSI Module provides 1 68-pin SCSI port that can be used as either source (write-protected) or destination. Module connects to the PCIe ports on the Falcon®-NEO.
- The FireWire Module provides 1 FireWire port that can be used as either source (write-protected) or destination. Module connects to the PCIe ports on the Falcon-NEO.

- The Thunderbolt™ 3/USB-C I/O card provides support for Thunderbolt storage enclosures. Card connects to any of Falcon-NEO's I/O ports, including 2 write-protected source I/O ports and 1 destination I/O port.
- PCIe adapter kit includes adapters for M.2 PCIe, M.2 SATA, M.2 NVMe, mSATA, PCIe and mini-PCIe cards
- USB 3.0 4-port hub
- USB 3.0 to SATA adapter to connect SATA drives to the USB 3.0 ports
- USB Power cable eliminates the need for additional power supplies when using USB to SATA adapters connected to USB ports on the Falcon-NEO
- 2.5"/3.5" IDE, 1.8" IDE to SATA, 1.8" ZIF adapters, flash media reader
- 18" extended length SAS/SATA cable set
- Extended 1-year and 2-year warranties
- Hard case (Pelican type)

1.4 Specifications

Power Requirements	Power Consumption	Operating Temperature	Relative Humidity	Net Weight	Dimensions	Agency Approvals
12 VDC, grounded, 21 AMP	< 200W with drives	0 to 40°C (32 to 104°F)	20% to 80%	3.0lbs/1.36k	10" X 6.75" X 3.25" 25.4cm X17.1cm X 8.2cm	RoHs compliant FCC Part 15 Class A CE

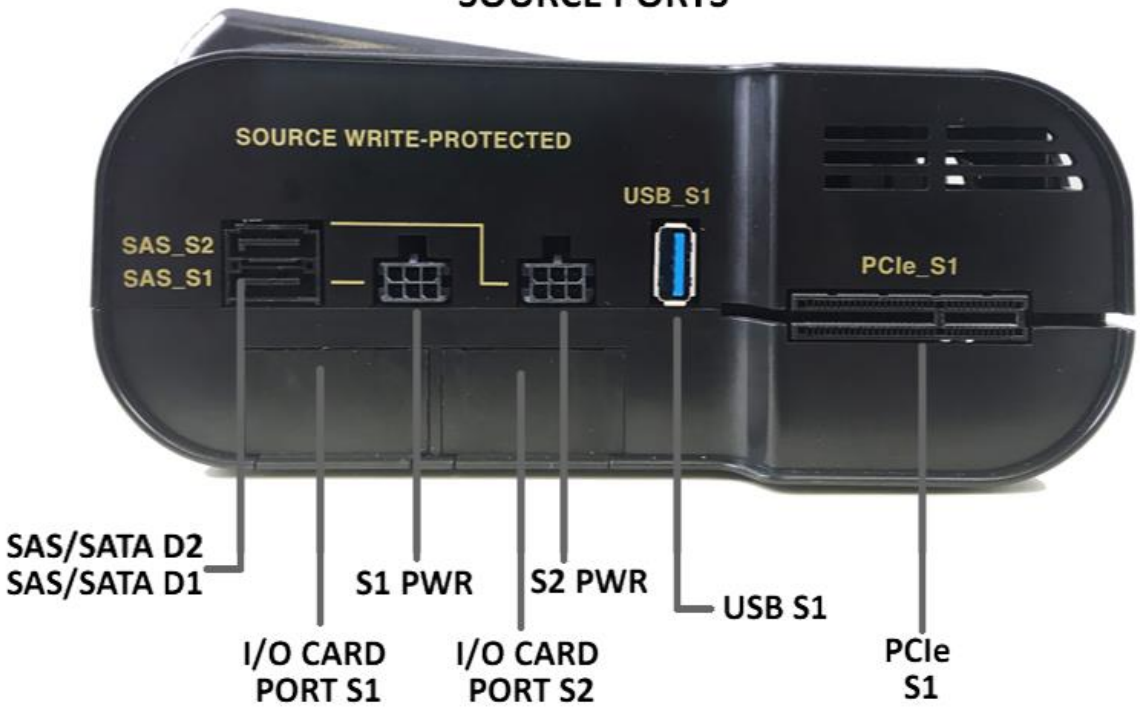
WARNINGS:

- Never connect a suspect drive to the Destination ports 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 device or subjecting it to sharp jolts. When in use, place it on a flat surface.
- Keep the unit dry. If the Logicube device 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 device. Doing so may void the warranty. If the unit requires service, please contact Logicube Technical Support for assistance.

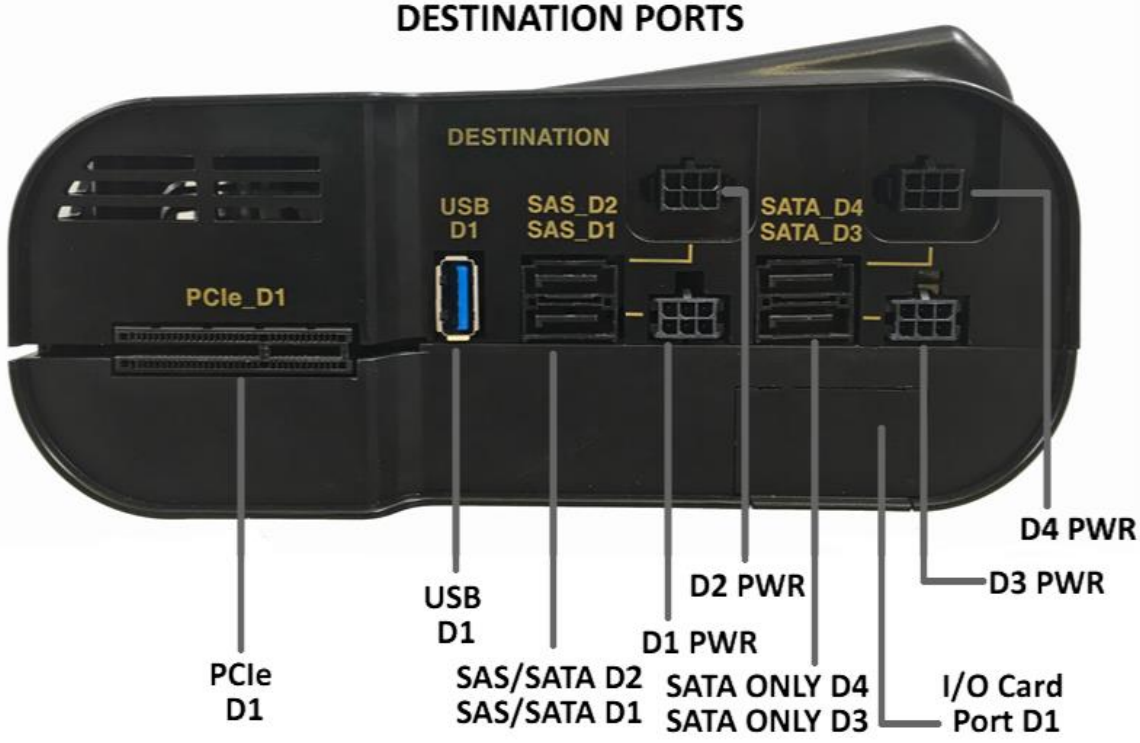
2.0 Overview of the Falcon-NEO

Special 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.

FALCON-NEO LEFT SIDE VIEW SOURCE PORTS



FALCON-NEO RIGHT SIDE VIEW DESTINATION PORTS



2.1 Turning the Falcon-NEO On and Off

The Falcon-NEO has two DC-IN ports located in the back of the device. Any of these two ports can be used. The second DC IN port is available for possible future increases in power requirements.

The Falcon-NEO also comes with a 12V grounded, 21A (output DC) power supply that connects to the back of the device. Attach the included power supply to any one of the two DC power ports in the back of the Falcon-NEO.

To turn the Falcon-NEO on, press and immediately release the power button located on the top right corner of the Falcon-NEO. The Falcon-NEO will turn on and start the boot process.

It is normal for the fans to slow down after the initial start-up sequence.

There are two ways of turning the Falcon-NEO off:

1. Press and immediately release the power button on the top right corner of the Falcon-NEO. The Falcon-NEO will begin the shutdown process and after a few seconds, the display and fans will turn off.
2. Using 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 the ***Power Off*** icon.

2.2 Connecting Various Drive Types

The Falcon-NEO supports a variety of drive types including the following types:

- SATA
- USB
- SAS
- eSATA
- mSATA
- 1.8″ Micro SATA
- 2.5″ and 3.5″ PATA/IDE (optional)
- 1.8″ ZIF (optional)
- 1.8″ PATA/IDE (optional)
- Flash media (optional)
- M.2 (NVMe, AHCI, SATA – optional)
- mPCIe (optional)
- SCSI (optional)
- FireWire (optional)
- Thunderbolt drive and enclosures (optional)

When connecting/disconnecting drives using drive adapters, it is recommended to keep the drive connected to the adapter, then connect/disconnect the adapter to/from the SAS/SATA cable, or connect/disconnect the SAS/SATA cable from the drive bay.

2.2.1 Connecting Source Drives

Source drives (also called suspect drives) must be connected to the left side of the Falcon-NEO. These ports are write-protected and are labeled as follows:

- **SAS_S1** – SAS/SATA data port for the Source 1 position.
- **SAS_S2** – SAS/SATA data port for the Source 2 position.
- **USB_S1** – USB 3.0 Source port.
- **PCIe_S1** – PCIe Source port (Depending on the type of PCIe drive, the optional PCIe kit, part number F-ADP-PCI-FN-KT may be required).
- **Not labeled:** Two 6-pin power ports for SAS_S1 and SAS_S2 that have lines corresponding to the proper data port.
- **Not labeled:** Two I/O ports for use with optional Logicube I/O expansion cards.

The Falcon-NEO Source ports are hot-swappable (including the PCIe ports).

> Although the Falcon-NEO ports are hot-swappable, 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.

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 SAS_S1 port. It can be connected to the SAS_S2 port without having anything connected to the SAS_S1 port.

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

Any combination of drives can be connected. For example, one SAS drive, one SATA drive, one USB drive, and one PCIe drive can all be connected at the same time.

2.2.2 Connecting Destination Drives

Destination drives (also called evidence drives) must be connected to the right side of the Falcon-NEO. These ports are labeled as follows:

- **SAS_D1 –** SAS/SATA data port for the Destination 1 position.

- **SAS_D2 –** SAS/SATA data port for the Destination 2 position.
- **SATA_D3 –** SATA only data port for the Destination 3 position.
- **SATA_D4 –** SATA only data port for the Destination 4 position.
- **USB_D1 –** USB 3.0 Destination port.
- **PCIe_D1 –** PCIe Destination port (Depending on the type of PCIe drive, the optional PCIe kit, part number F-ADP-PCI-FN-KT may be required).
- **Not labeled:** Four 6-pin power ports for SAS_D1, SAS_D2, SATA_D3, and SATA_D4 that have lines corresponding to the proper data port.
- **Not labeled:** One I/O port for use with optional Logicube I/O expansion cards.

Not shown: Two front USB 3.0 ports are available as Destination ports or input device ports for use with wired keyboards or mice.

The Falcon-NEO Destination ports are hot-swappable (including the PCIe ports).

Although the Falcon-NEO ports are hot-swappable, 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.

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 SAS_D1 port. It can be connected to the SATA_D4 port without having anything connected to any of the other ports.

Any combination of drives can be connected. For example, four SATA drives, one USB drive, and one PCIe drive can all be connected at the same time.

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

2.2.3 Using USB/eSATA Drives or Enclosures

It is recommended to leave the drive inside the enclosure. These enclosures may 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.

2.2.4 Connecting M.2/PCIe/mPCIe Drives

An optional PCIe adapter kit (part number F-ADP-PCI-FN-KT) is available for the Falcon-NEO which includes M.2 adapters, a mini PCIe adapter, and a PCIe extender cable.

2.2.5 Connecting an External Optical Drive (CD/DVD/Blu-ray)

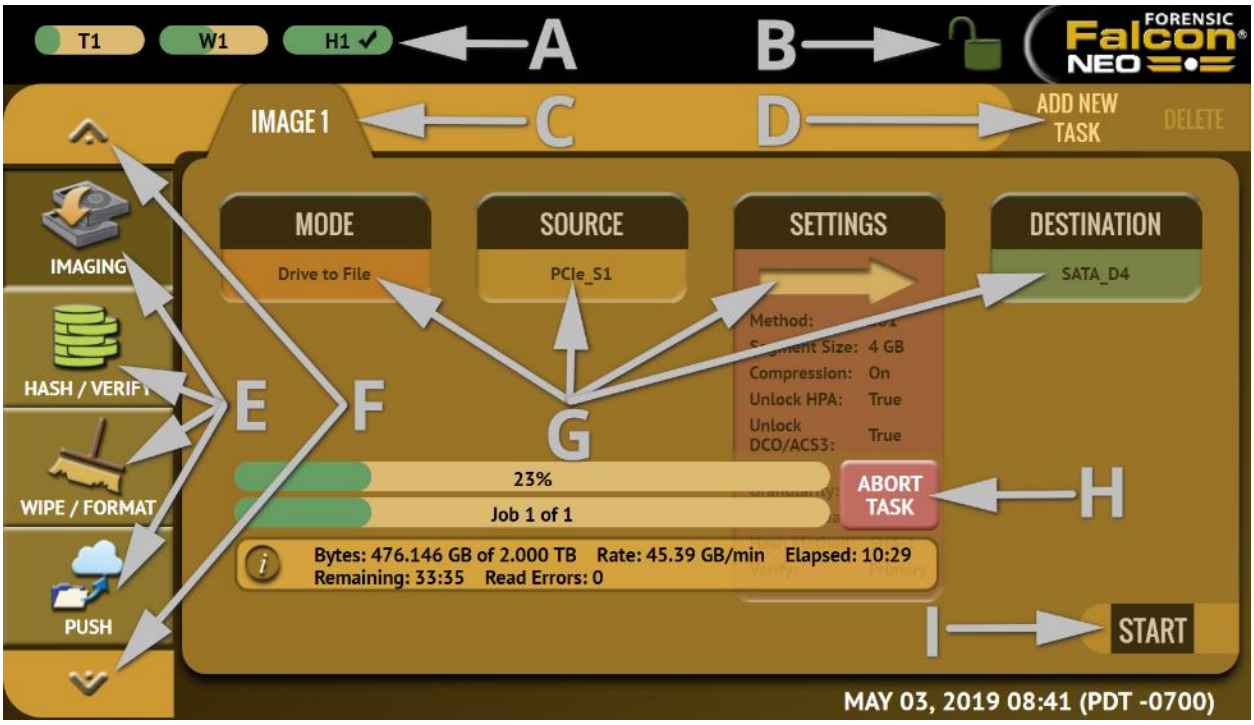
An optical drive can be connected to the Source USB port. The Falcon-NEO can then image the contents of the CD, DVD, or Blu-ray disc.

> Although most USB optical drives should work (may require external or additional power), Logicube has tested and qualified the following optical drive:
>
> - Pioneer BDR-XS06 with external power

Multisession support: The Falcon-NEO supports imaging from a multisession CD (as a Source). However, forensic analysis software may not support reading the multisession data. Please check with your forensic analysis software manufacturer to find out if it supports reading multisession data from CDs.

2.3 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 – Status Bar
I – Start icon

2.4 Front and Rear Ports

The Falcon-NEO has two front USB 3.0 ports, an HDMI port, two 10GbE ports, and two DC-IN power ports.

2.4.1 Front Ports

The Falcon-NEO has two front USB 3.0 ports. These ports serve two purposes:

- As two additional USB 3.0 Destination ports (USB_D2 and USB_D3).
- To connect peripherals such as USB keyboards and mice.

2.4.2 Rear Ports

The Falcon-NEO has two DC-IN power ports, two 10GbE ports, and an HDMI port.

2.4.2.1 DC IN Power Ports

The Falcon-NEO has two DC-IN ports. The included AC adapter/power supply can be connected to either DC-IN port to provide power to the Falcon-NEO. There are two DC-IN ports for possible future power scaling requirements.

2.4.2.2 Dual 10GbE Ports

The Falcon-NEO has two 10GbE (Gigabit Ethernet) ports (labeled LAN_1 and LAN_2) to provide fast network performance. Some of the possible uses for these ports include (but are not limited to) the following:

- Connect two NAS devices to each port.
- Connect a NAS to one port and the suspect's network to the other.
- Connect a work network (to control the Falcon-NEO remotely) and a NAS to the other port.

2.4.2.3 HDMI

The Falcon-NEO has a standard Type A HDMI port located on the back panel. Simply connect an HDMI cable from the Falcon-NEO to an external display that supports HDMI

and the Falcon-NEO will automatically show the display on both the Falcon-NEO and the external display.

To change the display resolution on the external display:

1. Connect a wired USB keyboard to one of the front USB host ports.
2. Press ALT+R. An on-screen display should appear on the external display that allows the display resolution to be changed.

2.5 Touch Screen

The Falcon-NEO features a 7" color LCD capacitive touch screen that allows the user to quickly input commands. The screen is bright, easy to read, and supports swipe gestures.

3.0 Quick Start Guide

This chapter gives a basic overview and steps on how to perform different types of operations using the Falcon-NEO (Image, Hash, Wipe, etc.). Complete details on each operation, menu, or selection, and the different screens can be found in ***Chapter 4: Imaging*** and ***Chapter 5: Types of Operation***.

The Falcon-NEO can perform up to five (5) tasks for each Image, Hash, and/or Wipe operation.

The passwords for built-in accounts can be changed. Instructions on how to change the passwords to the built-in user accounts can be found in ***Section 5.10.2.2***.

The Falcon-NEO imaging, hash, and wipe speeds are determined by several factors including the following:

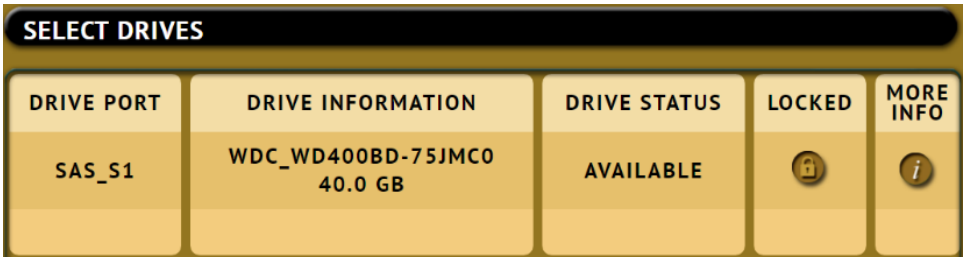
- The manufacturer specifications of the drive(s) being used
- The age of the drive (manufactured date)
- How often that drive has been used

For example, a 2 TB drive with 64MB of cache produced by the manufacturer 2 years ago is most likely slower than a 2 TB drive that the same manufacturer just released this year, even though they are both 7200RPM with 64MB of cache, and both are SATA III.

3.0.1 ATA Security Locked Drives

With Falcon-NEO software version 1.2 (and newer), drives that are locked with the ATA security standard can be temporarily unlocked. The password used to lock the drive is required to unlock the drive.

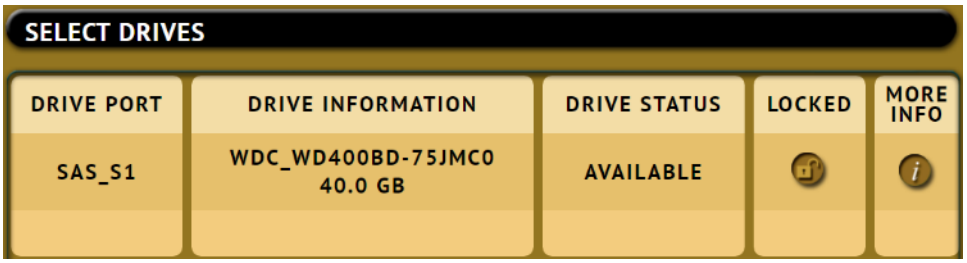
Drives that are locked with the ATA security standard will show a locked icon in the ***LOCKED*** column when selecting drives (Master or Target).



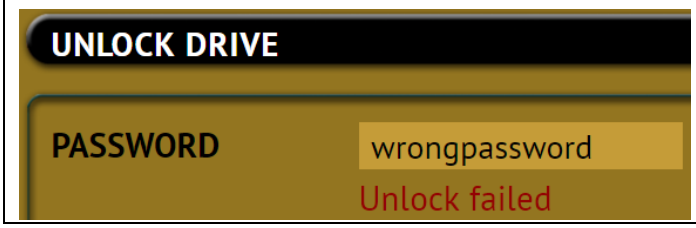
When the drive is locked, the contents of the drive are not accessible. Locked drives cannot be cloned (as Source or Destination), hashed, or wiped without first being unlocked.

To unlock the drive, tap the locked icon, The UNLOCK DRIVE screen will appear:

Enter the password to unlock the drive. If the entered password is correct, the screen will change to show an UNLOCKED icon:



If the wrong password was entered, an 'Unlock failed' message will appear:



Once the drive is unlocked, it can be used for a clone task (as Master or Target), a hash task, or a wipe task.

The drive will remain unlocked temporarily until the drive is disconnected or powered down. If the drive is disconnected then reconnected, it will be locked again.

While the drive is unlocked, a Secure Erase wipe will permanently remove the password lock.

3.1 Imaging

This type of operation allows the imaging of a Source drive to one or more Destinations. There are six (6) different imaging modes and several settings to choose from. These selections should be performed in order from left to right.

Details on the different screens found in the Imaging operation can be found in ***Chapter 4: Imaging***.

DD, E01, EX01, and DMG files created on the Destination may be smaller than the selected Segment size. For example, if 4GB segment size selected, some files may be less than 4GB. This occurs when there is a lot of blank space on the Source drive.

- **Drive to File –** Images the Source to any of the following image output file formats: ***DD***, ***E01***, ***EX01***, or ***DMG***. Compression is available for E01 and EX01 formats.
- **File to File - (Targeted Imaging feature) –** The Falcon-NEO can shorten acquisition time by creating a logical image by using pre-set filters, custom filters, file signatures filter, and/or keywords search function to select and acquire only the specific files needed. Output formats available are: Directory tree, MFT report, L01 archive, LX01 archive, and ZIP archive. The MFT report contains a list of deleted files (if present) that can potentially be restored or recovered.

  Software 2.3 or newer adds the ability to image APFS (Apple File System) when using ***File to File***. To image APFS using ***File to file***, users must go to the ***System Settings*** screen, then the ***Advanced*** tab and set ***APFS*** to ***ON*** before starting the task.

- **Partition to File (Logical Imaging) –** Images one partition from the Source drive to any of the following image output file formats: ***DD***, ***E01***, ***EX01***, and ***DMG***. Compression is available for E01 and EX01 formats. It also allows BitLocker decryption (requires the BitLocker passphrase/password, recovery key, or BEK file) so the image file(s) created will not have encrypted data.
- **Net Traffic to File –** Captures network traffic, internet activity, and VOIP. Sniff data on a network and store captured packets on a Destination drive connected to Falcon-NEO. Captured data are saved to .pcapng file format.
- **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.
- **File to Drive (Image Restore) –** Restores DD, E01, EX01, and DMG images created by the Falcon-NEO to another drive.

Any HPA, DCO, or ACS3 can be unlocked when imaging with the following modes:

- Drive to File
- Partition to File
- Drive to Drive

The Falcon-NEO uses a concurrent Image+Verify process. When Verify is set, the Falcon-NEO images and verifies concurrently and takes advantage of destination hard drives that may be faster than the source hard drive. The duration of the total image process time may be reduced by up to half.

3.1.1 Step-By-Step Instructions – Imaging

> Details on each selectable option on the Image screen can be found in ***Chapter 4: Imaging***.

1. Select ***Imaging*** from the types of operation on the left side.
2. Tap the ***Mode*** icon and select one of the six modes 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.
4. Tap the ***Settings*** icon and adjust the settings as needed (***Case Info***, ***File Image Method Settings*** or ***Mirror Settings***, ***HPA/DCO/ACS3/TRIM***, ***Error Handling***, ***Hash/Verification Method***, etc.) then tap the ***OK*** icon.

> The Settings screen will be different for each of the two modes. Details on the different Settings screens can be found in ***Chapter 4: Imaging***.
>
> Log file names can be set in ***Settings*** in the ***Case Info*** screen by entering a Case/File name. See ***Section 4.3.1*** for more information.
>
> The Falcon-NEO 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:

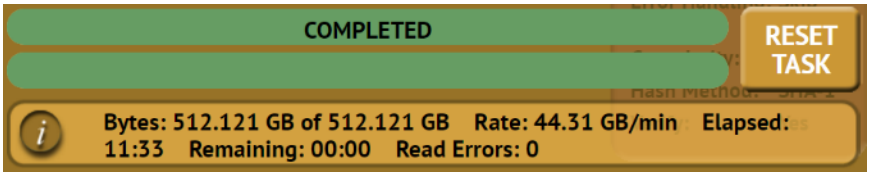
Uppercase A to Z	Period (.)
Lowercase a to z	Underscore (_)
Numbers 0 to 9	Hyphen/Dash (-)

5. Tap the ***Destination*** icon and select the destination(s) to be used then tap the ***OK*** icon.

> For DD, E01, Ex01, and DMG, the Falcon-NEO must be used to format drives. If the Destination drive is not formatted by the Falcon-NEO, the ***Location*** will appear as "***(NOT_MOUNTED)***" and a format icon will appear in the Format column. Tap the ***(Format)*** icon to format the Destination drive.
>
> Encrypted drives will have the following symbol: in the Format column.

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

8. When finished, the status will show "COMPLETED". It is recommended to tap ***Reset Task*** to reset the task, so the drive bays properly reset and not show as being used or assigned for other tasks.



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

3.1.2 Imaging BitLocker Encrypted Drives

Source drives encrypted with BitLocker can be decrypted so that the data in the DD, E01, EX01, or DMG image files is not encrypted. One of the following two are required to unlock the drive:

- The Password/Recovery Key, or
- A *.BEK file (BitLocker Encryption Key)

> Parallel imaging is not supported with unlocked BitLocker encrypted drives. Parallel imaging is supported if the encrypted partitions are not unlocked.

Drives can be encrypted using BitLocker encryption. FIPS-compliant encryption can also be used. When a drive is encrypted, a recovery key and a password are created, and the password can be generated by the administrator or by the end user.

With software release 2.1, the Falcon-NEO can unlock and image FIPS compliant encrypted drives if the Falcon-NEO user can create a new *.BEK (BitLocker Encryption Key) file in Windows. To create a new *.BEK file:

- The user would need to have the original Recovery Key or the password associated with the drive.
- The BitLocker encrypted drive will need to be connected to a Windows computer (the user must have administrative rights).
- A 2nd encryption key will need to be created, then saved to an external storage device (such as a USB flash drive) or to a computer connected to the same network the Falcon-NEO is connected to.

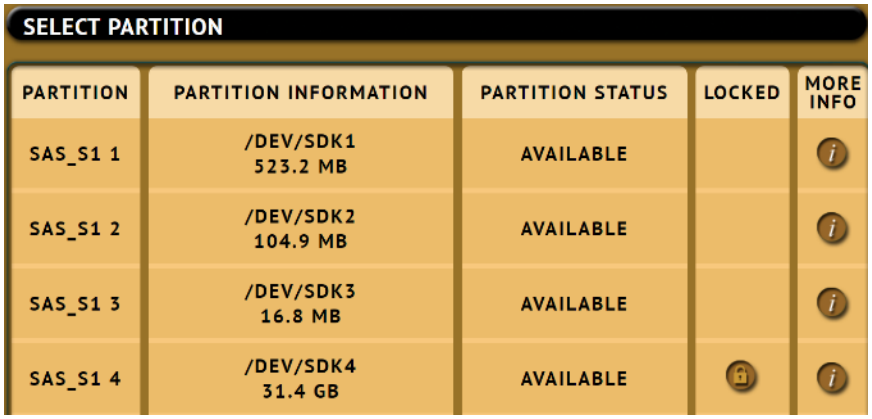
> See ***Section 3.1.2.2*** for details on how to create the *.BEK file using the original Recovery Key or password associated with the drive.

Since BitLocker encrypts volumes, and a volume is a formatted partition, unlocking the BitLocker encrypted volume requires going through the ***Partition to File*** mode.

1. Select ***Imaging*** from the types of operation on the left side.
2. Tap the ***Mode*** icon and select ***Partition to File*** then tap the ***OK*** icon.

3. Tap the ***Source*** icon and choose the BitLocker encrypted source drive from the list of connected drives then tap the ***OK*** icon.

4. The 'Select Partition' screen will appear. Any BitLocker encrypted partition will have the 'Locked' icon showing in the LOCKED column.



5. To unlock the encrypted volume, choose a partition that is encrypted with BitLocker to be imaged by tapping the LOCKED icon.

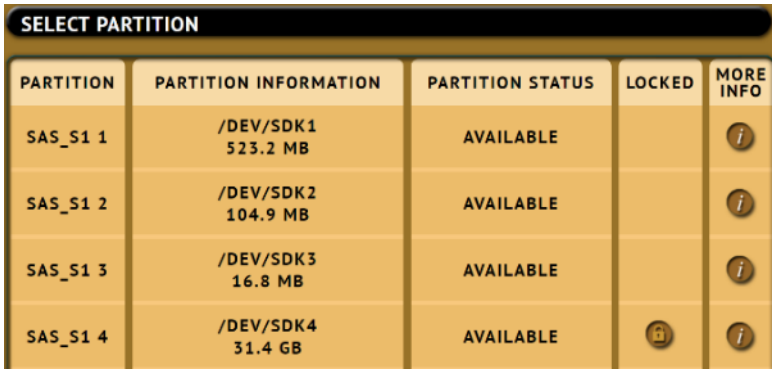
6. The following screen will appear allowing you to choose how to unlock the partition:

3.1.2.1 Password/Key

When the Password/Key is selected, the following screen will appear:

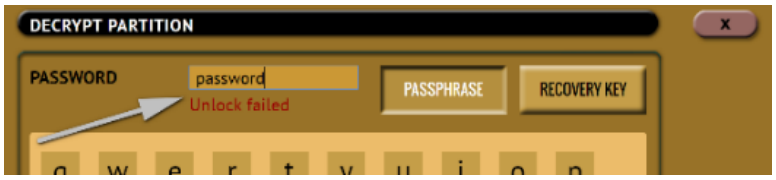
1. In the DECRYPT PARTITION screen, tap the ***Passphrase*** icon then enter the BitLocker password. You can also use the long recovery key by tapping ***Recovery Key*** then entering the BitLocker Recovery Key. When finished, tap the ***OK*** icon to continue.

   If the password is correct, the screen will go back to the 'Select Partition' screen.

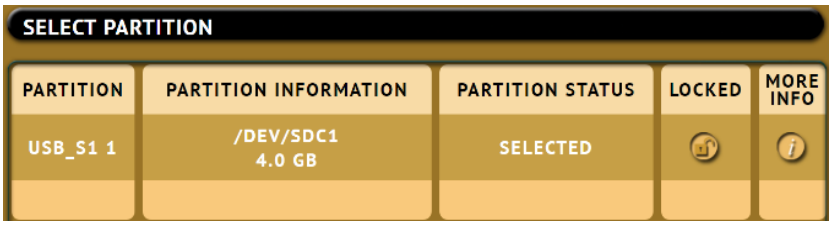


   The icon in the 'Locked' column may still appear to be locked, even though the partition is unlocked, but the partition will be unlocked.

   If the password is incorrect, a message will appear below the Password field showing 'Unlock failed'.



2. Once the partition is unlocked, select the partition to be imaged then tap the ***OK*** icon to continue.



   Once the BitLocker encrypted partition has been unlocked, you can proceed with the Partition to File image task or change the mode to perform a Drive to File image task to Image all other partitions that may be on the drive. Since the encrypted partition has been unlocked, selecting the whole source drive using Drive to File will image the whole drive including the unlocked partition.

3. Tap the Settings icon and adjust the settings as needed (Case Info, File Image Method Settings or Mirror Settings, HPA/DCO/ACS3/TRIM, Error Handling, Hash/Verification Method, etc.) then tap the OK icon.

4. Tap the ***Destination*** icon and select the destination(s) to be used then tap the ***OK*** icon.
5. Tap the ***Start*** icon to start the imaging task.
6. A progress bar will appear at the bottom of the screen showing the bytes processed, the rate (speed), elapsed time, and time remaining.
7. When finished, the status will show "COMPLETED". It is recommended to tap ***Reset Task*** to reset the task, so the drive bays properly reset and not show as being used or assigned for other tasks.

3.1.2.2 BEK File

A 2nd *.BEK file is needed to unlock FIPS compliant BitLocker encrypted drives. The following steps outline the procedure to create a 2nd *.BEK file:

> Since a second BitLocker Encryption Key is being added to the BitLocker header of the encrypted drive, the drive cannot be connected through a write blocker or write protection device.

1. Connect the BitLocker encrypted drive to a Windows computer.

> The Windows computer must be used with an account that has administrative rights.

2. Unlock the drive using the password or Recovery Key.
3. Open a command prompt with administrator privileges.
4. Run the following command to add a new Recovery Key:

manage-bde -protectors -add d: -RecoveryKey c:\download

> Where d: is the drive letter of the BitLocker encrypted drive and c:\download is the location to save the Recovery Key.

5. Run the following command to save the external key (*.BEK file):

manage-bde -protectors -get d: -sek c:\download

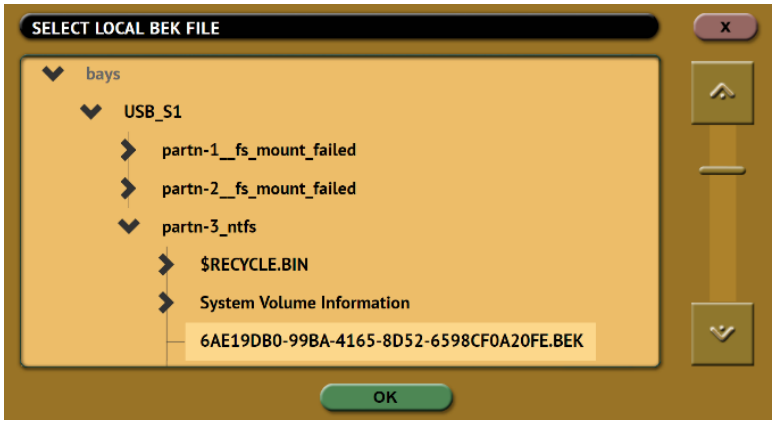
> To view the *.BEK file in Windows, the following folder view options need to be set:
> - Set "Show hidden files, folders, and drives"
> - Uncheck "Hide protected operating system files (Recommended)"

6. The *.BEK file can be saved to an external storage device (such as a USB flash drive) or to a computer connected to the same network the Falcon-NEO is connected to.

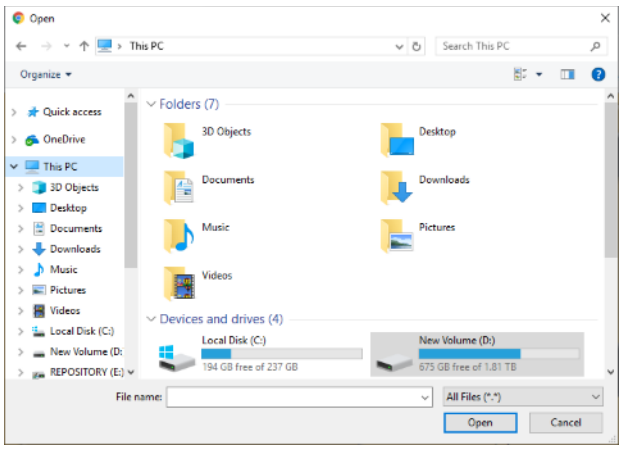
To unlock a FIPS compliant BitLocker encrypted drive, choose BEK file. When the Password/Key is selected, the following screen will appear:

There are two selections on this screen:

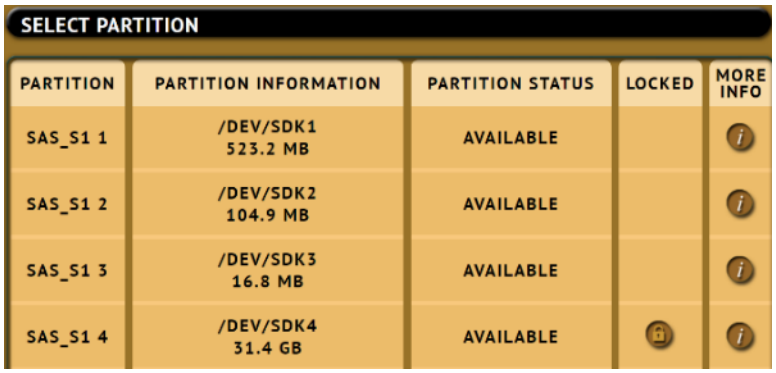
- **SELECT LOCAL FILE –** Choose this If the BEK file is on a drive connected to one of the Source ports on the Falcon-NEO. A file browser screen will appear allowing the user to locate and select the BEK file:



- **UPLOAD FROM PC –** This is only available from a web interface using a supported browser from a computer on the same network that the Falcon-NEO is connected to. Depending on the Operating System on the computer, a window will appear allowing the user to locate and choose the BEK file:



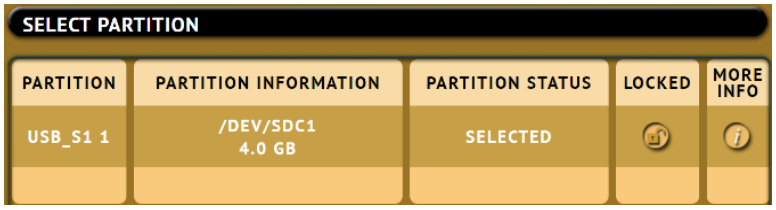
If the correct BEK file is used, the screen will go back to the 'Select Partition' screen.



The icon in the 'Locked' column may still appear to be locked, even though the partition is unlocked, but the partition will be unlocked.

If the incorrect BEK file is used, a message will appear below the Password field showing 'Unlock failed'.

Once the partition is unlocked, select the partition to be imaged then tap the ***OK*** icon to continue.



Once the BitLocker encrypted partition has been unlocked, you can proceed with the ***Partition to File*** image task or change the mode to perform a ***Drive to File*** image task to Image all other partitions that may be on the drive. Since the encrypted partition has been unlocked, selecting the whole source drive using ***Drive to File*** will image the whole drive including the unlocked partition.

1. Tap the Settings icon and adjust the settings as needed (Case Info, File Image Method Settings or Mirror Settings, HPA/DCO/ACS3/TRIM, Error Handling, Hash/Verification Method, etc.) then tap the OK icon.

2. Tap the ***Destination*** icon and select the destination(s) to be used then tap the ***OK*** icon.
3. Tap the ***Start*** icon to start the imaging task.
4. A progress bar will appear at the bottom of the screen showing the bytes processed, the rate (speed), elapsed time, and time remaining.
5. When finished, the status will show "COMPLETED". It is recommended to tap ***Reset Task*** to reset the task, so the drive bays properly reset and not show as being used or assigned for other tasks.

3.1.3 Targeted/Logical Imaging

The Falcon-NEO has the capability to perform targeted or logical imaging using File to File mode. Using various filters, the Falcon-NEO can image only the files found within the filters. Output formats include L01, LX01, Directory Tree, and Zip Archive. An MFT report can be generated which will list files that can potentially be restored or recovered.

1. Select ***Imaging*** from the types of operation on the left side.
2. Tap the ***Mode*** icon and select ***File to File*** then tap the ***OK*** icon.
3. Tap the ***Source*** icon and select the Source then tap the ***OK*** icon.
4. Tap the ***Settings*** icon and choose the desired settings.

> For details on the different settings in File to File mode, please see ***Section 4.3.8*** of this manual.

5. Tap the ***Destination*** icon and select the destination(s) to be used then tap the ***OK*** icon.
6. Tap the ***Start*** icon to start the imaging task.
7. A progress bar will appear at the bottom of the screen showing the bytes processed, the rate (speed), elapsed time, and time remaining.
8. When finished, the status will show "COMPLETED". It is recommended to tap ***Reset Task*** to reset the task, so the drive bays properly reset and not show as being used or assigned for other tasks.

3.1.4 Imaging To or From a Network

A network repository or location must be set for the Falcon-NEO to be able to image to or from a network repository/location. Depending on the type of repository added (for example SMB, CIFS or iSCSI), the repository will appear as a Source, Destination, or both.

> For details on how to add a network repository/location, please see ***Section 5.9*** of this manual.

3.1.5 Imaging Net Traffic

The Falcon-Neo can capture network traffic data using the ***Net Traffic to File*** imaging mode. Network traffic that can be captured can include local network activity, internet activity, and VOIP activity. The data is saved and stored to a *.pcanpg file format which can be analyzed by various software such as Wireshark.

> Advanced networking knowledge is required for the setup of capturing network traffic and data analysis.
>
> When performing a Net Traffic to File imaging task, it is highly recommended not to use the network port used as the Source (LAN1 or LAN2) for any other imaging task or for remote access to the Falcon-NEO.

1. Select ***Imaging*** from the types of operation on the left side.
2. Tap the ***Mode*** icon and select ***Net Traffic to File*** then tap the ***OK*** icon.
3. Tap the ***Source*** icon and choose a network port to capture with (LAN1 or LAN2).
4. Tap the ***Settings*** icon and choose the desired settings.

   > For more information on the Net Traffic to File Settings, please see ***Section 4.3.9***. Additional notes on Net Traffic Imaging can be found in ***Chapter 11: Net Traffic***.

5. Tap the ***Destination*** icon and select the destination(s) to be used then tap the ***OK*** icon.
6. Tap the ***Start*** icon to start the imaging task.
7. A progress bar will appear at the bottom of the screen showing the bytes processed, number of packets, segments, and dropped packets.

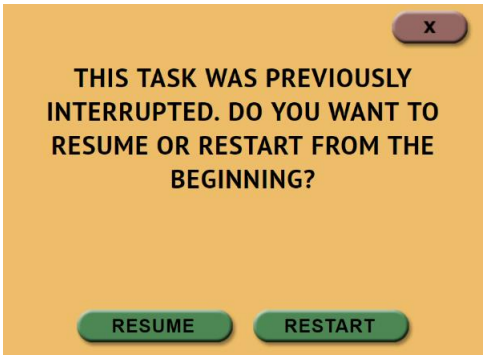
3.1.6 Drive to Drive Resume Feature

Software version 2.1 and newer includes a resume feature when using the Drive to Drive mode. This feature will give the user the option to resume or restart a Drive to Drive image when any of the following interruptions occur:

- The task is aborted
- Power to the Falcon-NEO is interrupted

To resume a Drive to Drive imaging task:

1. Make sure the same drives are connected to the same ports.
2. Make sure the Imaging settings are set the same as when the task was interrupted.
3. Start the task. When the same imaging task is setup with the same drives (connected to the same ports) connected when the task was interrupted, and the task is started, the following screen should appear:



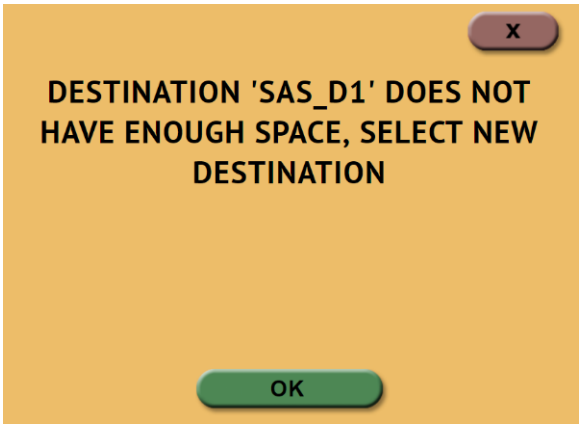
The audit log file will contain the original date and time along with the date and time the task was resumed.

3.1.7 Drive Spanning

The Falcon-NEO can automatically span to two (or more) Destination drives when using ***Drive to File, File to File, Partition to File, or Net Traffic to File*** mode (DD, E01, EX01, or DMG).

When the task is started, and there may not be enough space on the Destination drive, the following prompt will appear warning that there might not have sufficient free space on the Destination drive:

When the Destination drive is full and the remaining data to be will not fit, Falcon-NEO will prompt for another drive.



When the screen above appears, tap the ***OK*** icon and the ***Select Repository*** screen will appear. The Destination drive that is full can be disconnected, and replaced with another drive, or a different Destination drive port or repository can be selected. After selecting the next Destination/Repository to be used, tap the ***OK*** icon.

When the imaging operation is finished, all subsequent Destinations/Repositories used will contain the same Case/File name and the next DD, E01, EX01, or DMG file. For example, if the last file on the first Destination used is *.E23, the next Destination/Repository used will start with file *.E24.

3.1.8 Parallel Imaging

Falcon-NEO can perform Parallel Imaging. A user can simultaneously perform multiple imaging tasks from the same source drive to multiple destinations using different imaging formats. For example, image to a network location or a destination drive using the E01 format while imaging to a different destination drive using native/mirror or DD format.

Parallel imaging is not supported with unlocked BitLocker encrypted drives. Parallel imaging is supported if the encrypted partitions are not unlocked.

For parallel imaging, prior to starting the imaging first task, users must set all other imaging tasks that need to be run in parallel.

When a task is started, and the same Source drive is selected on other imaging tasks, a screen will appear notifying the user that there are tasks that may be started in parallel. The user can then select one or more of the tasks to run.

3.1.9 Blank Disk Check

The Falcon-NEO can check a drive to see if it has been wiped by the Falcon-NEO. This check will not be accurate if Secure Erase or Pattern Buffers were used to wipe the drive. To perform a blank disk check:

1. Connect a drive to the Falcon-NEO.
2. Choose Imaging, Hash, or Wipe/Format.
3. Choose Source, Destination, or Drives to list the connected drives.
4. Tap the ***More Info*** icon to display more information about the drive.

> The More Info icon will not appear in the Destination screen when using Drive to File, File to File, Partition to File, or Net Traffic to File.

5. Tap the down arrow located to the right of the screen to scroll down to the second page of information.
6. Locate the line that shows "Wiped". This will either show ***True*** (drive is blank) or ***False***.

3.2 Hash / Verify

A hash or verify operation can be performed to any drive or case (any Falcon-NEO created DD, E01, EX01, or DMG image). Performing a hash or verify task will instruct the Falcon-NEO to calculate the hash for the specified drive or case. There are two modes available:

> Details on the different screens found in the Hash/Verify operation can be found in ***Section 5.2: Hash/Verify***.

- **DRIVE HASH –** This mode will hash any connected drive on an active Source or Destination port. This mode 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 Falcon-NEO 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.
- **CASE VERIFY –** This mode will hash cases/images created by the Falcon-NEO (DD, E01, Ex01, DMG) for verification purposes. There are two settings for this mode:
    - **Primary –** This will verify the primary hash of the image. Use this if only on hash value was selected when the case was imaged.

- **Both –** This will verify both primary (SHA-1) and secondary hash (MD5) of the image. Use this if ***SHA1+MD5*** was used when the case was imaged.

3.2.1 Step-By-Step Instructions – Drive Hash or Case Verify

1. Select ***Hash*** from the types of operation on the left side.
2. Tap the ***Modes*** icon and select the desired mode (Drive Hash or Case Verify).
3. Tap the ***Drives*** icon and select the drive(s) to be hashed then tap the ***OK*** icon.
4. Tap the ***Settings*** icon to choose the different settings based on the Mode. Details for every setting can be found in ***Section 5.2.3***.
5. Change any of the optional settings (LBA settings or percentage of the drive to be hashed) if needed.

Optional: Tap Case Info to set the Case/File Name, Case ID, Examiner, Evidence ID, or Case Notes.

6. Tap the ***Start*** icon to start the hash task
7. When finished, the status will show "COMPLETED". It is recommended to tap ***Reset Task*** to reset the task, so the drive bays properly reset and not show as being used or assigned for other tasks.

3.3 Wipe/Format

Destination drives can be wiped and formatted using the Falcon-NEO. To use a drive as a Destination drive (using ***Drive to File, File to File, Partition to File, or Net Traffic to File***), the Destination will need to be formatted by the Falcon-NEO. The following methods are available in the Wipe menu:

Details on the different screens found in the Wipe/Format operation can be found in ***Section 5.3: Wipe/Format***.

- ***Secure Erase*** – Sends a command to the drive instructing it to wipe the drive based on the hard drive manufacturer's specifications for the Secure Erase command.

  Contact the hard drive manufacturer for Secure Erase specifications for each model/type of hard drive.

  Secure Erase will not work on drives connected through the USB, PCIe, or I/O ports (Thunderbolt).

- ***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. The Falcon-NEO can verify each pass value through a setting. Any HPA, DCO, or ACS3 can also be wiped.
- ***Format –*** Instructs the Falcon-NEO to format a drive (with or without encryption). The Falcon-NEO can format the drive using the following file systems: ***EXT4, NTFS, exFAT, FAT32***.

For in-depth information regarding drive encryption, please see ***Chapter 7: Drive Encryption and Decryption***. Windows does not have native support for EXT4.

3.3.1 Step-By-Step Instructions – Wipe/Format

1. Select ***Wipe*** from the types of operation on the left side.
2. Tap the ***Destination*** icon and select one or more drives then tap the ***OK*** icon.

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

3. Tap the ***Settings*** icon and 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).
4. If the drive has an HPA, DCO, or ACS3 area that needs to be wiped, tap the ***HPA/DCO/ACS3/TRIM*** icon and select ***Yes*** to wipe the HPA/DCO/ACS3 area of the drive.
5. Tap the ***Passes*** icon to edit the number of passes and what gets written on each pass.
6. If the drive needs to be formatted, tap the ***Settings*** icon to change the Format settings then tap the ***OK*** icon.
   - **FORMAT –** Select ON to format the drive.
   - **FILE SYSTEM –** Select which file system the Falcon-NEO will use to format the drive.
   - **ENCRYPTION –** Select whether to encrypt the drive (ON) or not (OFF).

     For more information on encrypted Destination drives, please see ***Chapter 7: Drive Encryption and Decryption***.

Optional: Tap Case Info to set the Case/File Name, Case ID, Examiner, Evidence ID, or Case Notes.

7. Tap the ***Start*** icon to start the wipe task. The Falcon-NEO will perform a Secure Erase first (if selected), then a Wipe Pattern (if selected), then finally a Format (if selected).
8. When finished, the status will show "COMPLETED". It is recommended to tap ***Reset Task*** to reset the task, so the drive bays properly reset and not show as being used or assigned for other tasks.

3.4 Push

The Push operation gives users the ability to push Falcon-NEO created evidence files to or from drives connected to the Falcon-NEO or a Falcon-NEO repository or network location. The Push feature provides a more secure method than simply copying files

through a computer by allowing the ability to verify the data that is pushed. The Falcon-NEO will generate a log file for each push process.

> Details on the different screens found in the Wipe/Format operation can be found in ***Section 5.4: Push***.

3.4.1 Step-By-Step Instructions - Push

> 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 5.9.1***.

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 both drives connected to the Source or 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 then tap the Verification icon to change the verification setting to Yes or No. Tap the ***OK*** icon to continue.

Optional: Tap ***Case Info*** to set the Case/File Name, Case ID, Examiner, Evidence ID, or Case Notes.

5. Verify the settings then tap the ***OK*** icon to continue.
6. Tap the ***Destination*** icon and select the destination or repository to push the images to. Tap the ***OK*** icon to continue.
7. Tap the ***Start*** icon to start the push task.
8. When finished, the status will show "COMPLETED". It is recommended to tap ***Reset Task*** to reset the task, so the drive bays properly reset and not show as being used or assigned for other tasks.

3.5 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, and then Hash.

Details on the different screens found in the Wipe/Format operation can be found in ***Section 5.5: Task Macro***.

3.5.1 Step-By-Step Instructions – Task Macros

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.

1. Select ***Task Macro*** from the types of operation on the left side.
2. Select a macro (Macro 1 through Macro 5).
3. Tap the ***Task*** icon to select up to nine (9) operations.
4. Set up to 9 operations by tapping on each operation in order (Operation 1, Operation 2, etc.)
5. When all the operations have been set, tap the ***OK*** icon.
6. Tap the ***Start*** icon to execute the macro and perform all the operations within that macro.
7. When finished, the status will show "COMPLETED". It is recommended to tap ***Reset Task*** to reset the task, so the drive bays properly reset and not show as being used or assigned for other tasks.

3.6 File Browser

The contents of connected Source and Destination drives on the Falcon-NEO can be previewed using the Falcon-NEO's file browser. The Falcon-NEO will show the partitions and the contents of each partition. Only some files can be opened by the Falcon-NEO. Files opened by the file browser will not alter the drive in any way.

With software version 2.1 or newer, the Falcon-NEO can show the contents of DD, E01, EX01, and DMG image files created by the Falcon-NEO.

Software 2.2 or newer adds the ability to view L01 image files and network repositories within the File Browser.

For detailed information on how to use the file browser and important notes, see ***Section 5.6*** of this manual.

For Source drives, the Falcon-NEO will show all the partitions that can be read.

For Destination drives, the only tabs displayed are drives formatted by the Falcon-NEO and will show any DD, E01, EX01, DMG, L01, LX01, ZIP, and Directory Tree files created by the Falcon-NEO.

3.6.1 Step-By-Step Instructions – File Browser

1. From the File Browser screen, select the drive to browse by tapping the corresponding tab at the top of the screen.
2. Tap the partition or folder to browse. The Falcon-NEO will show the contents (folders/directories and files) of the selected partition or folder on the Destination drive.
3. To view a file, tap the filename. The Falcon-NEO will attempt to open the file.
   - If the Falcon-NEO can open the file, it will be displayed on the screen.
   - If the Falcon-NEO cannot open the file, a message will appear stating "File viewer cannot view file type:"
   - To view the contents of the DD, E01, EX01, DMG, or L01 image file, tap the first segment of the image file (for example, DDCapture.001, E01Capture.E01, Ex01Capture.Ex01, or DMGCapture.dmg). A new tab will appear showing the contents of the image file.

3.7 Logs

The Falcon-NEO keeps logs of all imaging, hash, wipe (or format), and push operations. Logs can be viewed directly on the Falcon-NEO or from a computer's browser (if the Falcon-NEO is connected to a network). In addition to viewing, the logs can be exported to an external USB drive. Logs are exported in PDF, HTML and XML format.

Details for the Logs screen can be found in ***Section 5.7: Logs***.

When using Drive to File mode (DD, E01, EX01, or DMG), 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.

The log files may contain a "partial hash". This hash is for Falcon-NEO's internal purposes only and cannot be validated by any other means.

3.7.1 Step-By-Step Instructions – Viewing or Exporting Logs

To view the log files:

1. Select ***Logs*** from the types of operation on the left side. A list of log files will appear sorted by date (newest on top).
2. Select the log file to view by tapping the name of the log file. This will highlight the log file chosen.
3. Tap the ***View*** icon to view the log file on-screen.

The log files can also be exported to a USB drive. To export the log files:

1. Select ***Logs*** from the types of operation on the left side. A list of log files will appear sorted by date (newest on top).

2. Select the log file to export by tapping the name of the log file. This will highlight the log file chosen.
3. Connect a formatted USB drive (USB flash drive or USB external drive) to one of the two USB ports located on the front of the Falcon-NEO.

> The USB drive connected to the front USB port must be formatted in Windows using the NTFS, FAT32, or FAT file system.

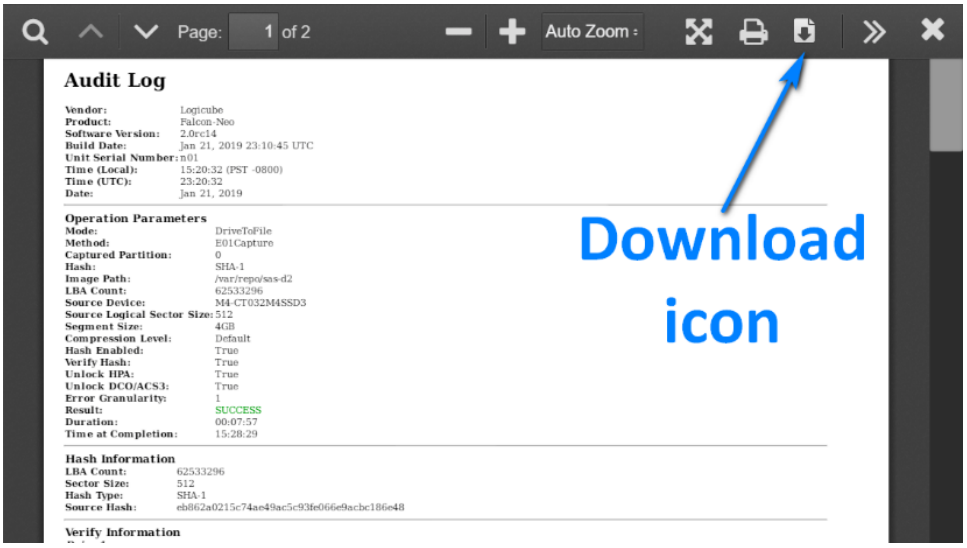
4. Tap the ***Export*** icon to export the log file via USB. The log will be exported/copied to the attached USB drive and will be in HTML, PDF, and XML formats.

Repeat steps 2 and 3 if other log files need to be exported or viewed. Alternatively, all the log files can be exported by tapping the ***Select All*** button to select all the log files. Once all log files are selected, they can be exported in a single operation.

To print the log files, it is recommended to use the web interface as described in ***Chapter 9: Remote Operation*** and click the print icon on the upper-right corner of the screen. The browser's print menu will appear, and the log can be printed to an available printer configured on the computer.

3.7.2 Viewing and downloading Log Files from the web interface

When using the web interface (see ***Section 9.1*** for details on the web interface), the log file will be viewed on a web browser. There is a download icon on the browser that can be used to download the log file being viewed.



3.7.3 Deleting Log Files

Log files can be deleted one at a time or all at once.

- To delete a single log file, tap the log file to highlight the log file to be deleted. Tap the ***Delete*** icon to delete the selected log file.

- To delete all the log files, tap the ***Select All*** icon to select all the log files, then tap the ***Delete*** icon.

A log file deletion password can be set to add a layer of security when deleting log files. If a password was set, log files cannot be deleted without entering the correct password.

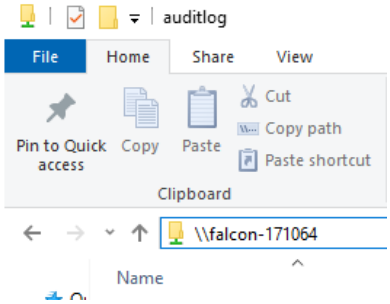
- If a log file deletion password was not created, a confirmation screen will appear confirming to delete the single log file or all log files.
- If a log file deletion password was created, a screen will appear prompting to enter the log file deletion password. Enter the log file deletion password. Tap the ***OK*** icon to delete the single log file or all the log files (depending on which was selected).

> The password can be set in the ***Systems Settings***. More information about the log file deletion password can be found in ***Section 5.10.2***.

3.7.4 Accessing the Logs Over a Network

The log files can also be accessed through a network on a computer if the Falcon-NEO is connected on the same network.

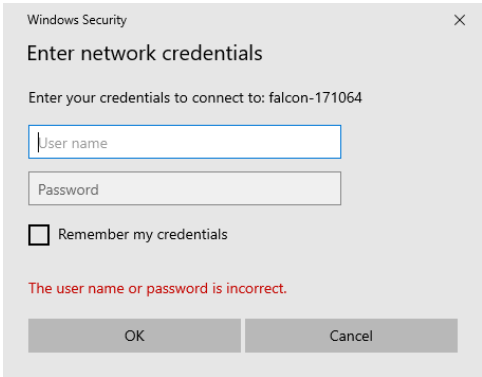
1. Open File Explorer or a similar window and browse to the hostname or the IP address found in the Statistics screen. See ***Section 5.8*** for more information on the Statistics screen.



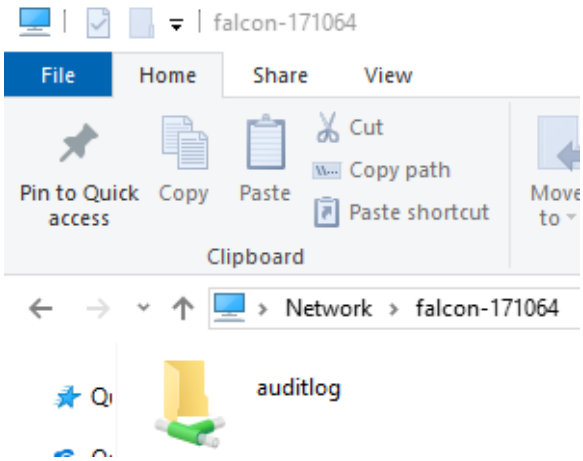
2. A Windows security screen will appear prompting to enter a User name and Password to connect to the Falcon-NEO. Login with the following credentials:

   User name: ***it***

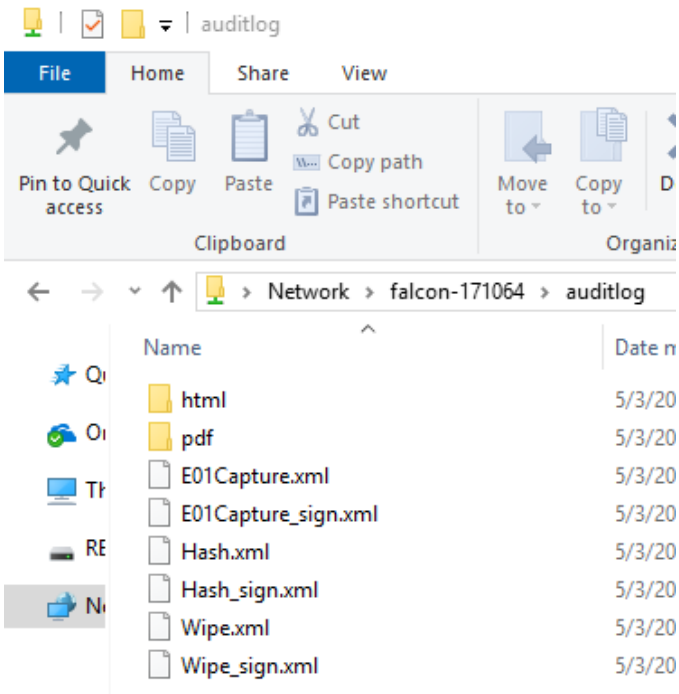
   Password ***it***



3. Once connected, an ***auditlog*** folder will appear. Open the ***auditlog*** folder.



4. The auditlog folder contains the HTML, PDF, and XML files for each of the log files. There will be two folders (html and pdf) that contain either the HTML or PDF versions of the log files. The XML files can be used with any XML viewer which allows for some customization on how the information can be viewed.



3.8 Statistics

This will display the following tabs: ***About***, ***Adv. Drive Statistics***, ***Network Interface Stats***, ***Debug Logs***, and ***Help***.

Details on the different Statistics screens can be found in ***Section 5.8: Statistics***.

About – This screen will show information about the Falcon-NEO including the current software installed. Additionally, a QR code can be found on this page. When the QR code is scanned on a device connected to the same network the Falcon-NEO is connected to, it will open a web browser to the Falcon-NEO's IP address to access the web interface.

Adv. Drive Statistics – Displays S.M.A.R.T. information taken directly from what the drive is reporting.

Network Interface Stats – Displays the Network Interface statistics (Receive and Transfer bytes, packets, drops, and errors, and the link status).

Debug Logs – Allows the export of debug logs for support purposes.

Help – Contains a QR code linking to the user's manual.

3.9 Manage Repositories

Repositories can be added to the Falcon-NEO in this operation. Repositories can be drives connected to the Destination ports of the Falcon-NEO (automatically shown) or shared folders over a network. SMB/CIFS and iSCSI protocols are supported.

Details on the different Manage Repositories screens can be found in ***Section 5.9: Manage Repositories***.

3.10 System Settings

The ***System Settings*** screen allows users to configure different settings for the Falcon-NEO:

Details on the different System Settings screens can be found in ***Section 5.10: System Settings***.

- Profiles
- Passwords
- Encryption
- Language/Time Zone
- Display
- Notifications
- Debug

3.11 Network Settings

The following tabs are seen in the Network settings screen:

Details on the different Network Settings screens can be found in ***Section 5.11: Network Settings***.

- **Interfaces –** Interfaces – Allows the configuration of the network interface which includes setting a static IP address and allows certain network services to be enabled or disabled.
- **HTTP Proxy –** For the Falcon-NEO to be able to update software from a network (over the internet), proxy settings may need to be set. Networks that have a proxy server for internet access will require proxy settings for devices like the Falcon-NEO to connect to the Internet. This typically includes a server (or IP address), a host port, a username, and a password.

3.12 Software Updates

New and improved software will be released from time to time. There are two ways to update the software on the Falcon-NEO: From the web via a network connection or from a USB drive.

Details on how to perform a software update, software re-load, or firmware update can be found in ***Chapter 8: Updating/Loading/Re-loading Software***.

3.13 Power Off

There are two tabs in the Power Off screen:

Details on the different Network Settings screens can be found in ***Section 5.13: Power Off***.

POWER OFF – The Falcon-NEO can be remotely turned off or restarted by going to this tab. Additionally, the Falcon-NEO screen can be refreshed.

DRIVE POWER – Inactive drives connected to the Falcon-NEO can be set to go to standby mode in this tab. The default is set to 0 minutes (OFF).

4: Imaging

4.0 Imaging - Introduction

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
- Drives
- Settings
- Destination

4.1 Mode

Tap this icon to choose between the following imaging modes:

- **Drive to File –** Images the Source to any of the following image output file formats: ***DD***, ***E01***, ***EX01***, *or* ***DMG***.
- **File to File (Targeted Imaging feature) –** Create logical images by using preset filters, custom filters, file signatures filter, and/or keywords search function to select and acquire only the specific

files needed. Output formats available are LX01, ZIP, or directory tree. Optionally an MFT report can be generated, which contains a list of deleted files (if present) that can potentially be restored or recovered.

> Software 2.3 or newer adds the ability to image APFS (Apple File System) when using ***File to File***. To image APFS using ***File to file***, users must go to the ***System Settings*** screen, then the ***Advanced*** tab and set ***APFS*** to ***ON*** before starting the task.

- **Partition to File (Logical Imaging) –** Images one partition from the Source drive to any of the following image output file formats: ***DD***, ***E01***, or ***EX01***. Compression is available for E01 and EX01 formats. It also allows BitLocker decryption (requires the BitLocker password) so the image file(s) created will not have encrypted data. Since BitLocker encrypts volumes, and a volume is a formatted partition, unlocking the BitLocker encrypted volume requires going through the ***Partition to File*** mode.
- **Net Traffic to File –** Falcon-Neo can capture network traffic data using the Net Traffic to File imaging mode. Network traffic that can be captured can include local network activity, internet activity, and VOIP activity. The data is saved and stored to a *.pcanpg file format.
- **Drive to Drive –** Performs a bit-for-bit copy of the Source producing an exact duplicate of the Source drive.

> Software version 2.1 and newer includes a resume function when using Drive to Drive. See ***Section 3.1.6*** for details on the resume feature.

- **File to Drive (Image Restore) –** Restores DD, E01, EX01, and DMG images created by the Falcon-NEO.

4.2 Source or Case

When ***Drive to Drive***, ***Drive to File***, ***or Partition to File*** mode is selected, the Source window will show all drives connected to the Source positions. Tap this icon to select the Source drive to be imaged. Falcon-NEO will list all the drives connected to the Source position(s).

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).

When ***Net Traffic to File*** mode is selected, the Source Interface window will appear showing both LAN ports (LAN 1, LAN 2).

When ***File to Drive*** mode is selected, the Case window will show all drives (connected to Source or Destination) that have DD, E01, or Ex01 images created by the Falcon-NEO.

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

4.3 Settings

Tap the ***Settings*** icon to change the image settings. Depending on the selected mode, different screens will appear.

- **Case Info –** Available in all modes. See ***Section 4.3.1***.
- **HPA/DCO/ACS3/TRIM –** Available in the following modes: (Trim is available only in Drive to Drive mode). See ***Section 4.3.2***.
    - Drive to File
    - Partition to File
    - Drive to Drive
- **Error Handling –** Available in the following modes (See ***Section 4.3.3***):
    - Drive to File
    - Partition to File
    - Drive to Drive
- **Hash/Verification Method –** Available in the following modes (See ***Section 4.3.4***):
    - Drive to File
    - File to File
    - Partition to File
    - Drive to Drive
- **File Image Method Settings –** Available in the following modes (See ***Section 4.3.5)***:
    - Drive to File
    - Partition to File
- **Clone Method Settings –** Available in Drive to Drive mode. See ***Section 4.3.6***.
- **Verify Hash –** Available in File to Drive mode. See ***Section 4.3.7***.
- **Special settings in File to File Mode –** Only available in File to File mode and includes ***Output Format*****,** and ***Filter Settings***. See ***Section 4.3.8***.
- **Special Settings in Net Traffic to File Mode –** Only available in Net Traffic to File mode and includes ***Number of Segments***, and ***Segment Ring Buffer***. See ***Section 4.3.9***.

4.3.1 Case Info

Case Info is available in all Imaging modes and allows users to enter information about the case. Case Info 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 Falcon-NEO 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 (-)

4.3.2 HPA/DCO/ACS3/TRIM

HPA/DCO/ACS3 is available in the following modes: ***Drive to File***, ***Partition to File***, and ***Drive to Drive***. TRIM is available only in Drive to Drive mode.

The HPA/DCO/ACS3 setting allows the user to set whether a drive's HPA, DCO, or Accessible Max Address is to be unlocked and imaged. Select ***YES*** to unlock and image a Host Protected Area (HPA), Device Configuration Overlay (DCO), or Accessible Max Address (ACS3).

HPA – If supported by the drive, HPA is set with the SET MAX ADDRESS command. The Host Protected Area is an area of a drive that is normally not visible to an Operating System, BIOS, or the user.

DCO – If supported by the drive, DCO is typically set by using the DCO MODIFY or DEVICE CONFIGURATION SET command. The 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. Like HPA, this hidden area is normally not visible to an Operating System, BIOS, or the user.

ACS3 – If supported by the drive, this is set using the ACCESSIBLE MAX ADDRESS command as specified by the ATA/ATAPI Command Set. This is the maximum LBA that is accessible by read commands and write commands that return command completion without error.

4.3.2.1 DRIVE TRIM

Destination Drive Trim is available only in Drive to Drive mode and is a user-selectable function that allows the Falcon-NEO to manipulate the destination drive using the DEVICE CONFIGURATION SET command for DCO, SET MAX ADDRESS command for HPA, or ACCESSIBLE MAX ADDRESS command for ACS3 so that the Destination drive's total native capacity matches the Source drive. For example, if the Source drive is a 128 GB drive and the Destination drive is a 6 TB drive, the Falcon-NEO will limit the Destination drive's capacity to 128 GB to match the Source drive exactly.

SAMPLE SOURCE DRIVE:

Bay:	SAS_S1
Role:	Master
Model:	Samsung_SSD_850_PRO_128GB
SerialNumber:	S24ZNSAG417968R
Size:	128035676160
PhysicalSectors:	250069680
LogicalSectors:	250069680
LogicalSectorSize:	512
Cylinders:	15566
Heads:	255

SAMPLE DESTINATION DRIVE PRIOR TO DRIVE TRIM:

Bay:	SAS_D1
Role:	Target
Model:	WDC_WD60EZRX-00MVLB1
SerialNumber:	WD-WX21D1403007
Size:	6001175126016
PhysicalSectors:	11721045168
LogicalSectors:	11721045168
LogicalSectorSize:	512
Cylinders:	65535
Heads:	255

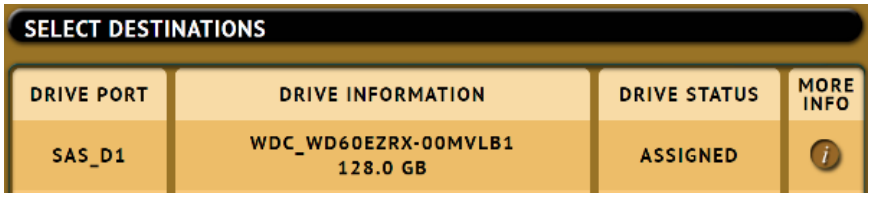
SAMPLE DESTINATION DRIVE AFTER DRIVE TRIM:

Bay:	SAS_D1
Role:	Target
Model:	WDC_WD60EZRX-00MVLB1
SerialNumber:	WD-WX21D1403007
Size:	128035676160
PhysicalSectors:	250069680
LogicalSectors:	250069680
LogicalSectorSize:	512
Cylinders:	15566
Heads:	255

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

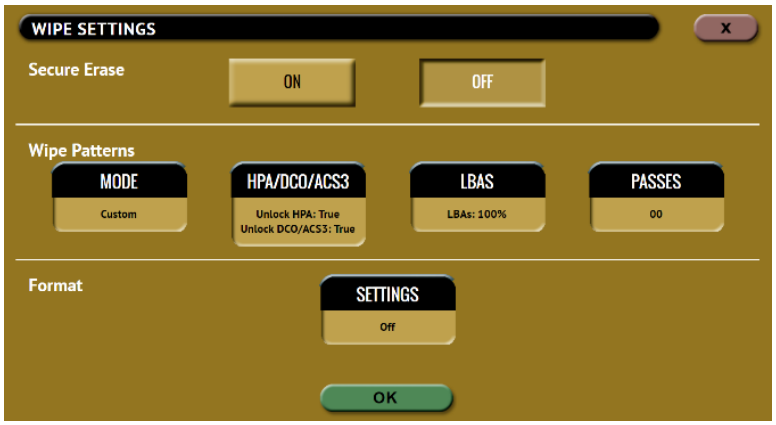
Drive Trim only works with ATA drives connected to the SAS/SATA Destination ports. Drive trim will not work with SAS drives or drives connected to the USB, PCIe, or I/O ports.

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.

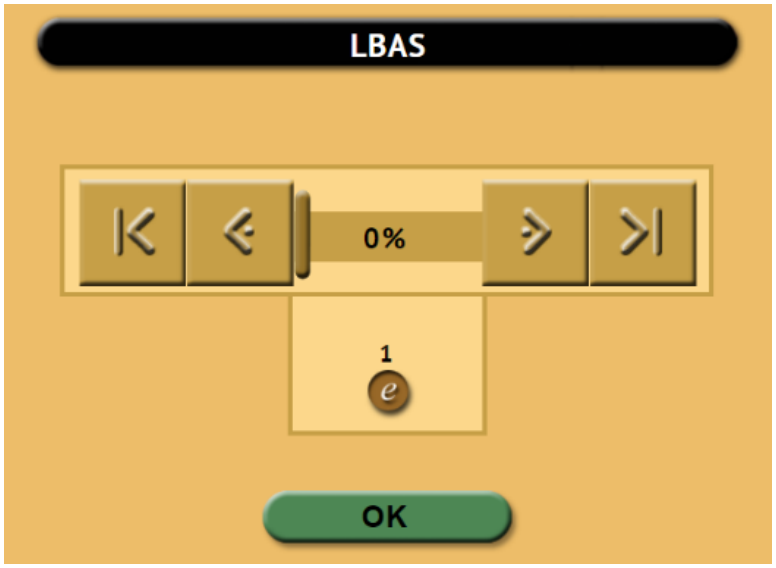


IN THE WIPE SETTINGS:

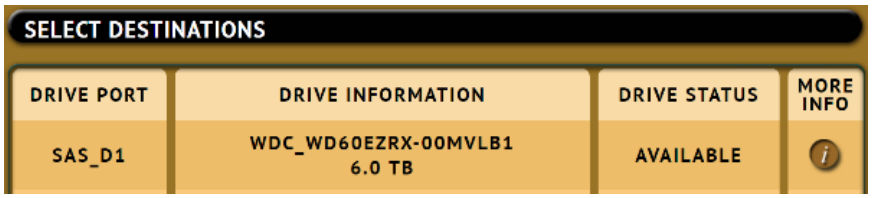
- Set Secure Erase to OFF
- Set Wipe Patterns to:
  - Mode: Custom
  - HPA/DCO/ACS3/TRIM: YES (TRUE)
  - LBAS: Edit to at least 1 LBA
  - PASSES: By default, this will have a value of 00



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 just wiping the HPA/DCO/ACS3 and 1 LBA. When the Wipe task finishes, the drive should be back to its original capacity.



4.3.3 Error Handling

Error Handling is available in the following modes: ***Drive to File***, ***Partition to File***, and ***Drive to Drive***.

In ***Drive to Drive*** mode, when bad sectors are encountered on the Source drive, Falcon-NEO 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***, Falcon-NEO will write a zero on the corresponding sector or position in the Destination drive or file.

In ***Drive to File*** and ***Partition to File***, Falcon-NEO also has a setting for **Error Granularity** and **Reverse Read**:

4.3.3.1 Error Granularity

In ***Drive to File*** and ***Partition to File*** bad sectors are skipped. Changing the granularity allows more sectors to be skipped. The following options are available:

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

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 Falcon-NEO will skip the entire cluster (or 4096 bytes or 8 sectors).

4.3.3.2 Reverse Read

Reverse Read is available in ***Drive to File***, ***Partition to File***, and ***Drive to Drive***. When this is set to YES and the Falcon encounters a bad sector, this will instruct the Falcon-NEO will skip past the block (based on the Error Granularity) then read backwards, potentially capturing data that may not necessarily be read when skipping the entire block.

4.3.4 Hash/Verification Method

The Hash/Verification method is available in all modes. Hash is selectable only in the following modes: ***Drive to File***, ***File to File***, ***Partition to File***, and ***Drive to Drive***. Verification is available in all modes. 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 is selected:

- **None –** No hash of the Source will be performed. This is available only when using the following mode:
  - Drive to Drive
- **SHA-1 –** Uses the SHA-1 algorithm to hash the Source. This is available in the following modes:
  - Drive to Drive
  - Drive to File
  - File to File
  - Partition to File
  - Net Traffic to File
- **SHA-256 –** Uses the SHA-256 algorithm to hash the Source. This is available in the following modes:
  - Drive to Drive
  - When using DD or DMG methods in Drive to File
  - When using DD or DMG methods in Partition to File
  - Net Traffic to File
- **MD5 –** Uses the MD5 algorithm to hash the Source. This is available in the following modes:
  - Drive to Drive
  - Drive to File
  - File to File
  - Partition to File
  - Net Traffic to File
- **SHA1+MD5 –** Dual Hash. Uses both SHA-1 and MD5 algorithms to hash the Source. This is available when using the following modes:
  - Drive to File
  - Partition to File
- **SHA1+SHA256 –** Dual Hash. Uses both SHA-1 and SHA-256 algorithms to hash the Source. This is available when using the following modes:
  - Drive to File (EX01 only)

  - Partition to File (EX01 only)
- **MD5+SHA256 –** Dual Hash. Uses both MD5 and SHA-256 algorithms to hash the Source. This is available when using the following modes:
  - Drive to File (EX01 only)
  - Partition to File (EX01 only)

Verification Method/Verify – One of the two screens will appear:

- **YES / NO –** Select ***YES*** to hash the Destination and verify that hash with the selected Source hash.
- **NO / PRIMARY / BOTH –** Select ***PRIMARY*** to verify just one hash value (For example, if SHA-1 or MD5 was selected in the image process). Select ***Both*** to verify both SHA-1 and MD5 if the ***SHA-1+MD5*** hash was selected in the image process.

4.3.5 File Image Method Settings

The File Image Method Settings screen allows the user to select a file image output. One of four different images methods can be selected:

- **DD –** 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.
- **DMG –** Raw disk image files commonly used in Mac OS X.

SEGMENT SIZE – This allows the user to set the output segment size (file size). Choose from the following segment sizes: 2 GB, 4 GB (Default), 8 GB, 16 GB, or Whole Disk.

> DD, E01, EX01, and DMG files created on the Destination may be smaller than the selected Segment Size if compression is on. For example, if 4 GB segment size is selected, some files may be less than 4 GB.

COMPRESSION –Available for E01 and EX01 only. Set compression to either ON or OFF.

4.3.6 Clone Method Settings

When ***Drive to Drive*** mode is selected, ***Clone Method Settings*** will appear on the top-right of the Settings screen. The Clone Method Settings screen has three settings:

- **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).

The specific number of blocks can be set for each of the options by tapping the: icon.

4.3.7 Verify Hash

In ***File to Drive*** (Image Restore) mode, ***Verify Hash*** will appear on the top-right side of the Settings screen. This screen allows the user to set the verification of the task.

4.3.8 Special Settings in File to File mode

The following are special settings screens in File to File Mode:

- Output Format Settings
- Filter Settings

4.3.8.1 Output Format Settings

The Output format screen shows the following selections:

- **L01 Archive –** Results will be in Encase L01 archive format.
- **LX01 Archive –** Results will be in Encase LX01 archive format.
- **Directory Tree –** All results will be written in a directory tree format. All files will appear in the same directory structure as found on the Source drive.
- **MFT Report –** Results will list deleted files (if present) in the auditlog file that can potentially be restored or recovered.
- **Zip Archive –** Results will be in a Zip archive format.

In addition to the output format, two additional settings are available when **L01 Archive** or **LX01 Archive** is selected:

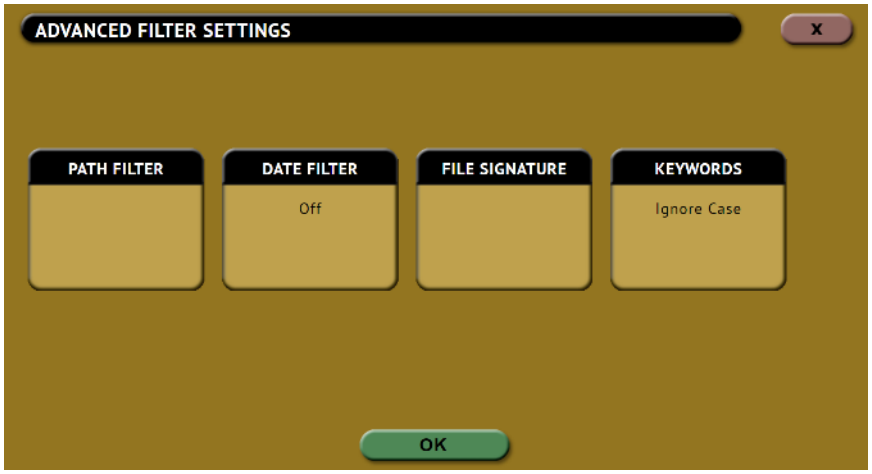
- **Segment Size –** Allows the user to set the output segment size (file size). Choose from the following segment sizes: 2 GB, 4 GB (Default), 8 GB, 16 GB, or Whole Disk.

The actual file size may be smaller than the selected Segment Size if compression is on. For example, if 4 GB segment size is selected, some files may be less than 4 GB.

- **Compression –** Set compression to either ON or OFF.

4.3.8.2 Filter Settings

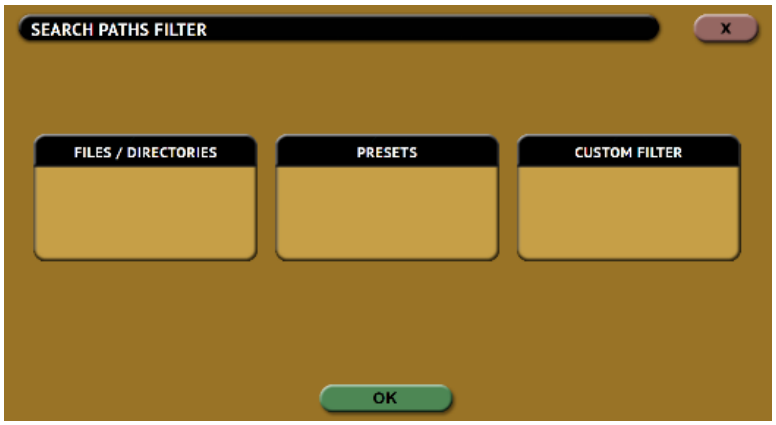
The Filter Settings screen shows the following selections:



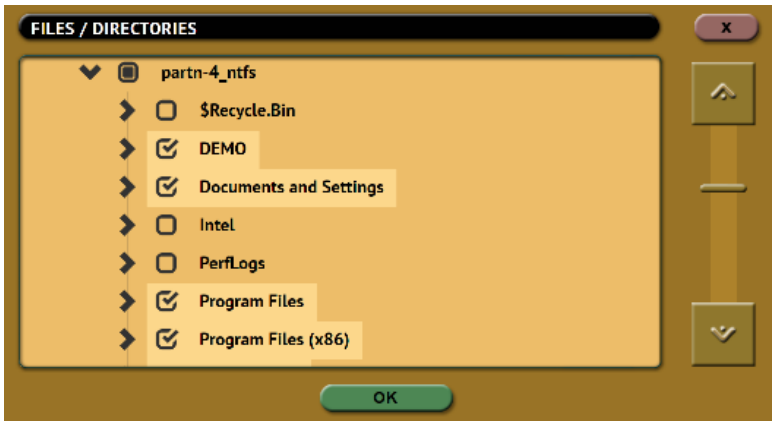
This screen allows the user to set several filters. Setting an incorrect filter or setting the filter too narrow may adversely affect results. Each filter narrows down the results. For example, if only video files are selected in the ***Signature-Based File Category*** filter, it will narrow down the results of the ***path filter*** to only video files within the results of the first filter.

4.3.8.2.1 Path Filter

This allows the user to choose files or directories, set preset filters, or specify a preset filter and/or custom filter. This is the first level of filtering.



The Files/Directories window allows the user to select files or directories to image.



The ***PRESETS*** window will show the available preset filters.

The ***CUSTOM FILTER*** uses the POSIX Extended Regular Expressions standard for syntax.

There are several websites with articles explaining the different expressions than can be used. Simply search the Internet for "POSIX Extended Regular Expressions."

Below are some examples of what can be entered in the ***Custom Filter***:

Example 1: A single keyword

If all filenames with "pic" are desired, the custom filter would be (similar to *pic* where * are wildcards):

.*(pic)

This will find any file with "pic" in the name like:

mypic.jpg

picture.jpg

baby.pic

Example 2: Multiple keywords

Multiple keywords can be used. If all filenames with "pic" or "txt" are desired, the custom filter would be:

.*(pic|txt)

This will find all files with "pic" or "txt" in the name.

Example 3: File extension keywords

For file extensions, **\.** must be placed at the end of the syntax:

.*\.(pic)

This will find all files with "pic" in the extension such as:

filename.pic

filename.pict

Example 4: File extensions without a wildcard at the end

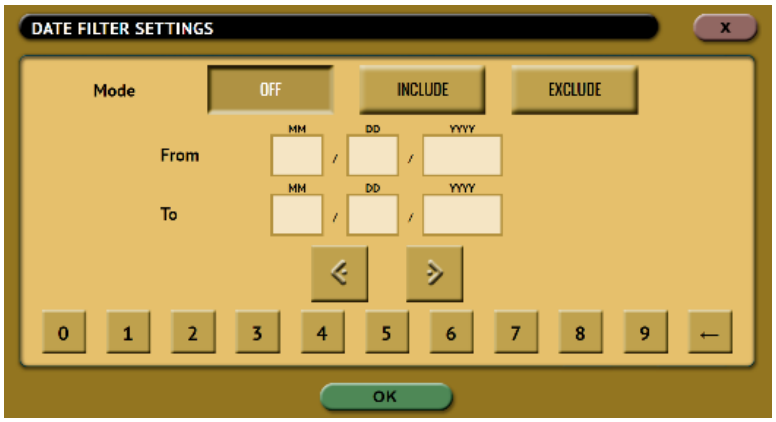
If a search is desired for a specific filename without any wildcard afterward, a ***$*** symbol must be added to the syntax. Using the example above (in example 3), you can use the following syntax:

.*\.(pic)$

This will find all files with the "pic" extension and nothing afterward. Using the examples above, it will find "filename.pic" but not "filename.pict".

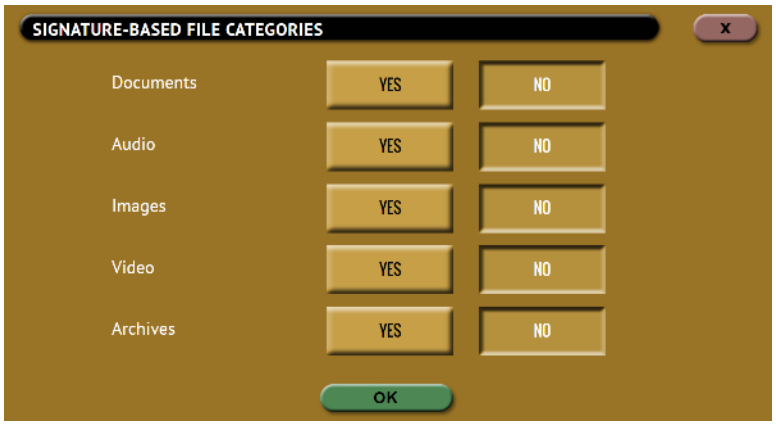
4.3.8.2.2 Date Filter

This allows a date filter to be set. By default, this is set to OFF. Set an ***Include*** date range to only include files modified within the specified date range. If ***Exclude*** is selected, all files modified within the specified date range will not be imaged.



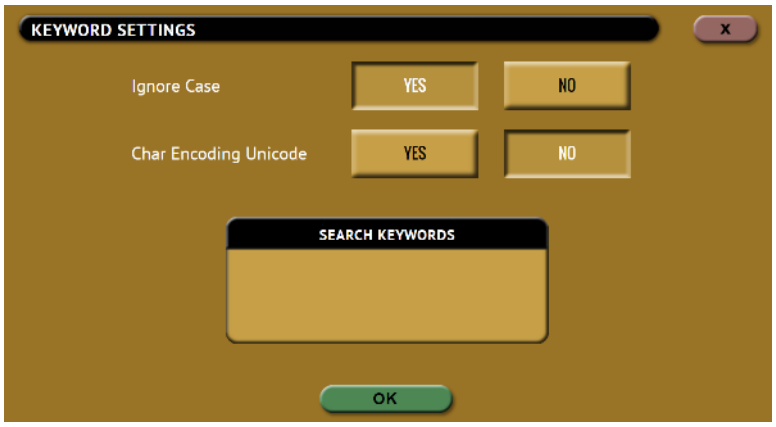
4.3.8.2.3 File Signature

This allows the user to set signature-based file categories. This is the second level of filtering and will narrow down the results of the first filter to only the selected file categories if selected.



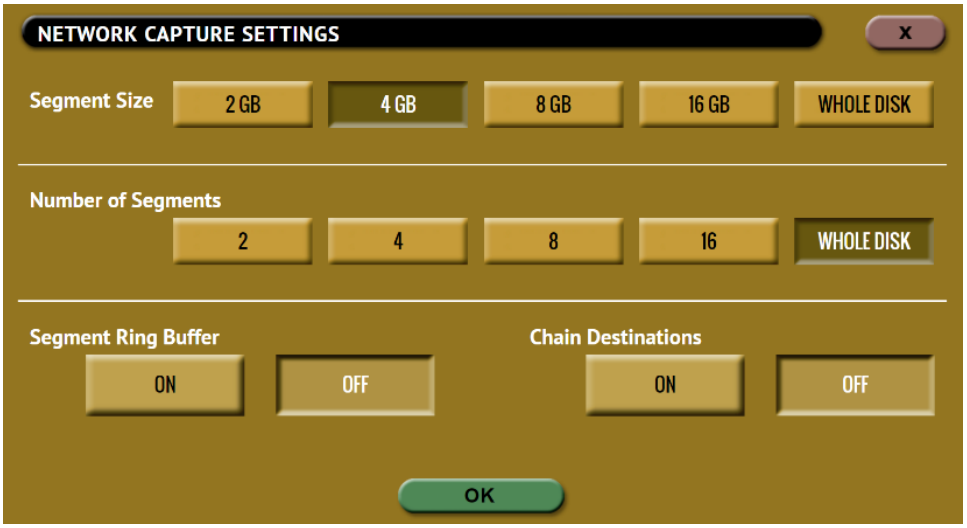
4.3.8.2.4 Keywords

This allows the user to set specific keywords. The Falcon-NEO will search specific keywords within the results of the previous filters.



4.3.9 Special Settings in Net Traffic to File Mode

There are special settings available when selecting the ***Net Traffic to File*** mode:



- Segment Size
- Number of Segments
- Segment Ring Buffer
- Chain Destinations

4.3.9.1 Segment Size

This allows the user to set the output segment size (file size). Choose from the following segment sizes: 2 GB, 4 GB (Default), 8 GB, 16 GB, or Whole Disk.

4.3.9.2 Number of Segments

This allows the user to select how many segment files to create. For example, if the Segment Size is set to 4 GB and the Number of Segments is set to 2, two segment files that are up to 4 GB will be created. The options available are 2, 4, 8, 16, or Whole Disk (Default).

4.3.9.3 Segment Ring Buffer

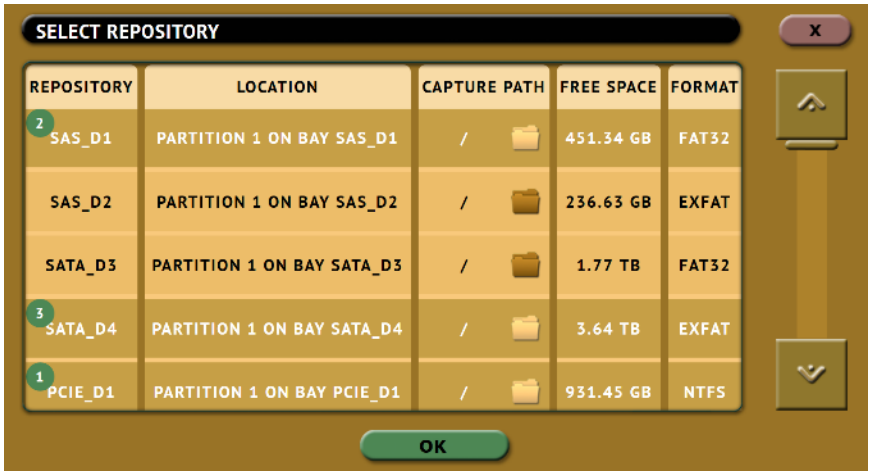
This setting determines what the Falcon-NEO will do when it reaches the total number of segments on all selected repositories (Destination drives).

- ***ON –*** When this is set to ON, the Falcon-NEO will continuously capture network traffic until the task is aborted. For example, if the ***Number of Segments*** is set to 2 and the ***Segment Ring Buffer*** is set to ON after the 2nd segment is finished, it will delete the 1st segment, then continue capturing network traffic, and create a new first segment file. If more than one repository is selected, it will keep cycling through both repositories, overwriting the oldest segment until the task is aborted.

- ***OFF –*** This is the default setting. When this is set to OFF, once the Falcon-NEO reaches the number of segments set and the last repository is filled, it will stop the task.

4.3.9.4 Chain Destinations

This setting allows the user to span the Net Traffic to File images over two or more repositories (such as Destination drives) continuously. When this is set to YES, all selected Destination drives will be used in the order they were selected. When the drive on the first repository is full, it will continue with the next selected repository.



> To enable Chain Destinations, Ring Buffer must be set to OFF.
>
> Drives must be formatted (by the Falcon-NEO) before starting the Net Traffic to File Imaging task.

After the first repository is full, the Destination drive on that repository can be swapped with a new Destination drive.

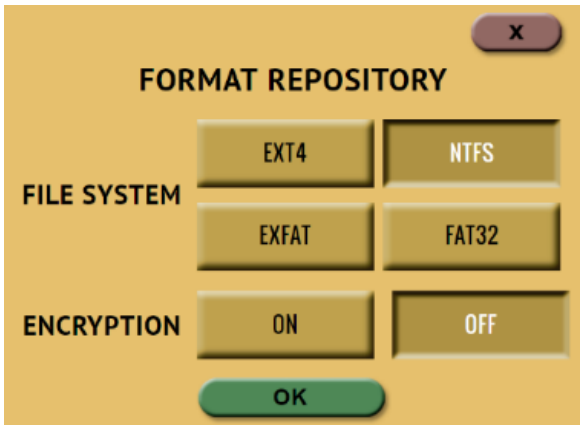
Replacing full repositories with a new Destination drive allows the Falcon-NEO to continuously capture Net Traffic until all the repositories are full. When all repositories are full, the task will finish showing a status of completed.

4.4 Destination/Image File

Tap the Destination or Image File icon to select the Destination drive or Image File. The Destination or Repository screen will show all drives connected to the Destination positions.

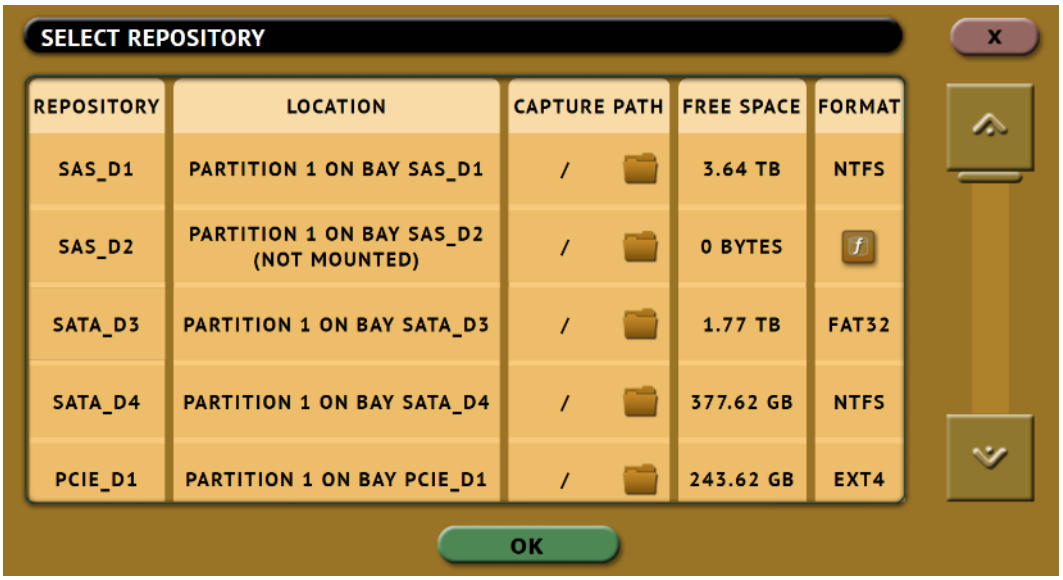
> When using Drive to File, File to File, Partition to File, or Net Traffic to File, if the Destination drive is not formatted properly, the ***Location*** will appear as "***(NOT_MOUNTED)***" and a format icon will appear in the Format column. Tap the ***(Format)*** icon the Destination drive.
>
> Drives encrypted by the Falcon-NEO will have the following icon:

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



Select which file system to use and whether to format with encryption (ON) or without encryption (OFF). For details on formatting a drive, see ***Section 5.3.2.3***. Formatting the drive may take several minutes, especially with encryption. Tap the ***OK*** icon to continue.

The default selection for the screen above can be changed in the ***Manage Repositories – Configuration*** screen. See ***Section 5.9.3*** for more information.



Software release v2.2 adds the ability to specify a capture path allowing users to save image files to specific folders within the selected repository/destination drive.

Tap or click the ***Capture Path*** column on the desired drive or repository and a Capture Path selection screen will appear.

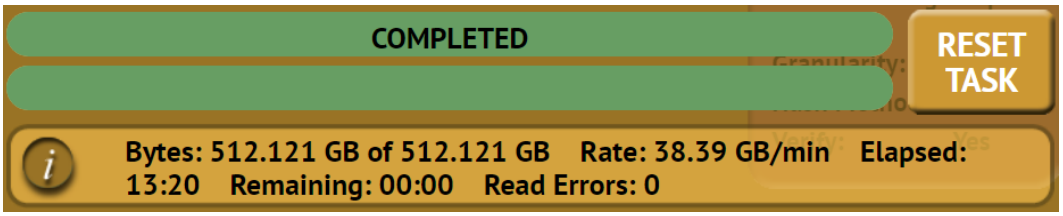
There are four buttons on the Capture Path selection screen:

- **Add Folder –** This is used to add a folder or sub-folder.
- **Delete Folder –** This is used to delete an empty folder. Folders that contain any files cannot be deleted with this method.
- **Rename Folder –** This will rename any folder.
- **OK –** Use this button when all desired changes have been completed.

Creating a folder or sub-folder is optional. If none are created, simply tap the ***OK*** button to continue. The image file will be saved on the root of the drive/partition.

4.5 Starting the Imaging Operation

Once all the settings and options have been selected or set, tap the ***Start*** icon to begin the imaging task. 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, time remaining, and any read errors. When finished, the status will show "COMPLETED". It is recommended to tap ***Reset Task*** to reset the task, so the drive bays properly reset and not show as being used or assigned for other tasks.

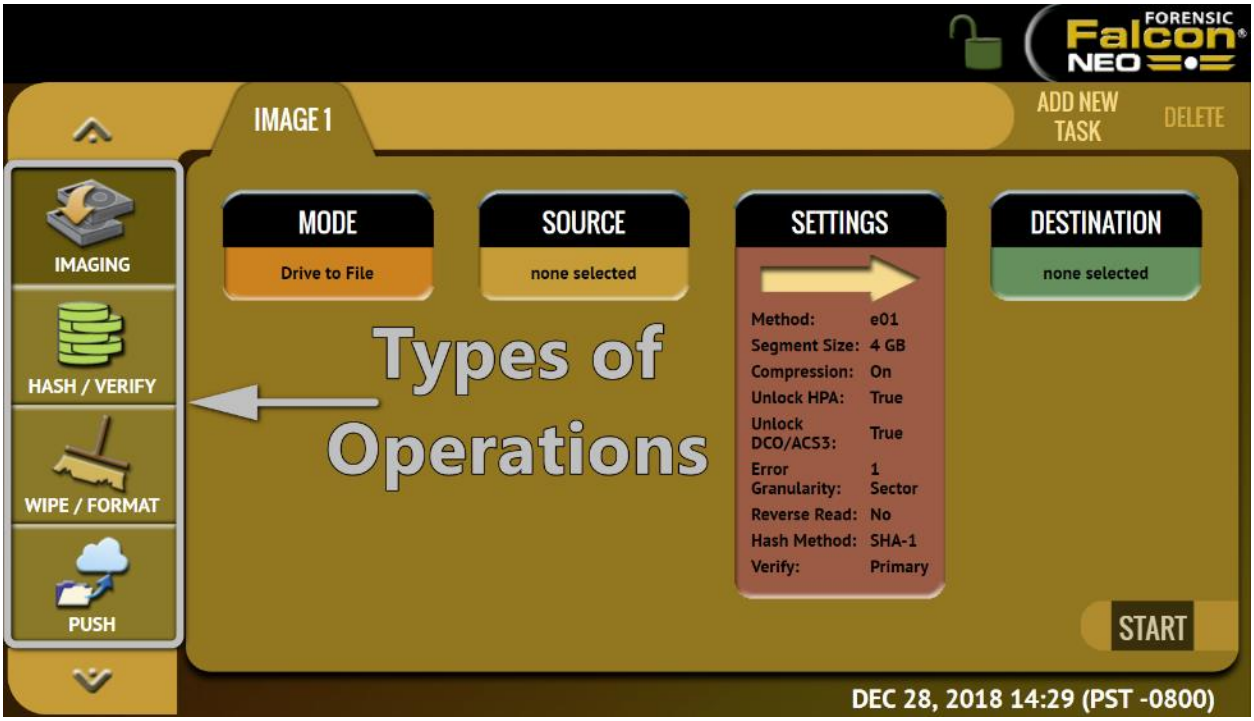


The number of bytes shown on the progress bar is not the actual size of the drive. This is the actual data being processed. When 'Verify' is set to "Yes", the reported number will double in size.

The Falcon-NEO can automatically span to two (or more) Destination drives when using Drive to File mode (DD, E01, EX01, or DMG). When the Destination drive is full and the remaining data to be imaged will not fit, Falcon-NEO will prompt for another drive. Information on Drive Spanning can be found in ***Section 3.1.7***.

5.0 Types of Operations - Introduction

There are thirteen (13) types of operation available on the Falcon-NEO. The left side of the screen shows the different operation types that can be set. Detailed information on all 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 six modes available:
   - **Drive to File –** Images the Source to any of the following image output file formats: ***DD***, ***E01***, ***EX01***, *or* ***DMG***.
   - **File to File (Targeted Imaging feature) –** Create logical images by using preset filters, custom filters, file signatures filter, and/or keywords search function to select and acquire only the specific files needed. Output formats available are LX01, ZIP or directory tree. Optionally an MFT report can be generated, which contains a list of deleted files (if present) that can potentially be restored or recovered.
   - **Partition to File (Logical Imaging) –** Images one partition from the Source drive to any of the following image output file formats: ***DD***, ***E01***, or ***EX01***. Compression is available for E01 and EX01 formats. It also allows BitLocker decryption (requires the BitLocker password) so the image file(s) created will not have encrypted data. Since BitLocker encrypts volumes, and a volume is a formatted partition, unlocking the BitLocker encrypted volume requires going through the ***Partition to File*** mode.

- **Net Traffic to File –** Capture network traffic data using this imaging mode. Network traffic that can be captured can include local network activity, internet activity, and VOIP activity. The data is saved and stored to a *.pcanpg file format.
- **Drive to Drive –** Performs a bit-for-bit copy of the Source producing an exact duplicate of the Source drive.
- **File to Drive (Image Restore) –** Restores DD, E01, EX01, and DMG images created by the Falcon-NEO.

Details on the different screens found in the Imaging operation can be found in ***Chapter 4: Imaging*.**

2. **HASH/VERIFY –** Perform a SHA-1, SHA-256, or MD5 hash of a drive or verify the file hash of a case (image) created by the Falcon-NEO.
3. **WIPE/FORMAT –** 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 any of the following file systems (with or without AES-256 encryption):
        - EXT4
        - NTFS
        - EXFAT
        - FAT32
4. **PUSH –** The network Push feature gives users the ability to push evidence files from destination drives connected to the Falcon-NEO or from a Falcon-NEO 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 Falcon-NEO 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 Falcon-NEO. The Falcon-NEO will show all viewable partitions and the contents of each partition.
7. **LOGS –** Display logs of each imaging, hash/verify, or wipe/format task that has been performed on the Falcon-NEO.
8. **STATISTICS –** This will display several tabs that include:
    - **About –** Displays information about the Falcon-NEO. Additionally, a QR code can be found on this page. When the QR code is scanned on a device connected to the same

network the Falcon-NEO is connected to, it will open a web browser to the Falcon-NEO's IP address to access the web interface.

- **Advanced Drive Statistics –** Shows raw S.M.A.R.T. data (if supported) on any drive connected to the Falcon-NEO.
- **Network Interface Stats –** Shows statistics and information on the Network Interface
- **Debug Logs –** Logicube Support may request to export debug log files to a USB flash drive.
- **Help –** Displays a QR code that links to the user's manual online.

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. This will display three tabs that include:
    - **Add/Remove –** Allows the user to add, remove, or edit networked repositories.
    - **iSCSI –** Allows the user to set ISCSI protocol settings.
    - **Configuration –** Allows the user to change the default format option for drives that are not formatted by the Falcon-NEO.
10. **SYSTEM SETTINGS –** This mode allows changes to the system settings on the Falcon-NEO which include the following:
    - **Profiles –** Allows the user to create, save, apply, or delete user profiles/configurations.
    - **Passwords –** Allows the user to set passwords or keys to lock the unit from any configuration changes, local access, HTTP access, or log file deletions. Local account passwords can also be changed on this screen.
    - **Encryption –** Sets the cipher mode (VCRPYT, TC-XTS, CBC, or ECB), Cipher, IV Generation, and the encryption password.
    - **Language/Time Zone –** Sets the language on the Falcon-NEO's menu and change the system's Time Zone.
    - **Display –** Sets the Falcon-NEO's display/screen brightness and enable/disable Stealth Mode.
    - **Notifications –** Sets audible beeps/notifications for when a task successfully completes or if an error appears.
    - **Advanced –** Allows the user to enable imaging APFS source drives when using ***File to File*** mode.
    - **Debug –** Reserved. Do not change any settings in this tab without instructions from Logicube Technical Support.
11. **NETWORK SETTINGS –** Allows the editing of various network configurations. Two tabs are available:
    - **Interfaces –** Edit TCP/IP and enable or disable certain network services.
    - **HTTP Proxy –** Set proxy settings (if required by the user's network).
12. **SOFTWARE UPDATES –** Perform software and firmware updates on the Falcon-NEO. Software can be updated over an internet connection (from network) or from a USB flash drive. Two tabs will be displayed:

- **Software Updates –** This is the screen where users can check for new software and update or reload the software.
- **Firmware Update –** Firmware for the Falcon-NEO (if available) can be updated on this screen.

13. **POWER OFF –** Turn the Falcon-NEO off or refresh the Graphical User Interface (GUI) and set a drive timeout, powering down drives when not in use. Two tabs are available:
    - **Power Off –** The Falcon-NEO can be turned off on this screen. This can be useful when using the web interface. The User Interface can also be refreshed in this screen.
    - **Drive Power –** Drives can be powered down automatically when not in use.

5.1 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 4: Imaging***.

5.2 Hash / Verify

This type of operation allows the hashing of any connected drive using one of the following algorithms: ***SHA-1***, ***SHA-256***, or ***MD5***. Case (Image) files created by the Falcon-NEO can also be verified.

There are four selections when performing a Hash or Verify: ***Mode***, ***Drives / Case***, ***Settings***, and ***Case Info***.

5.2.1 Mode

Tap this icon to choose the mode.

- **Drive Hash –** Hash a drive based on Logical Block Addresses (LBA) or Sectors.
- **Case Verify –** Verify the hash of a case (image) file. The Falcon-NEO can verify the following case/image file types: **DD**, **E01**, **EX01**, and **DMG**.

5.2.2 Drives

Tap this icon to choose the drive to be hashed or the drive that contains the case (image) files to be verified.

5.2.3 Settings

Tap this icon to choose a drive to adjust the hash or verify settings.

5.2.3.1 Drive Hash Settings

If Drive Hash mode was chosen, the Hash Settings screen will appear. Tap the ***Hash Values*** 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 Falcon-NEO 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 Falcon-NEO 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.

5.2.3.1.1 Hash Method

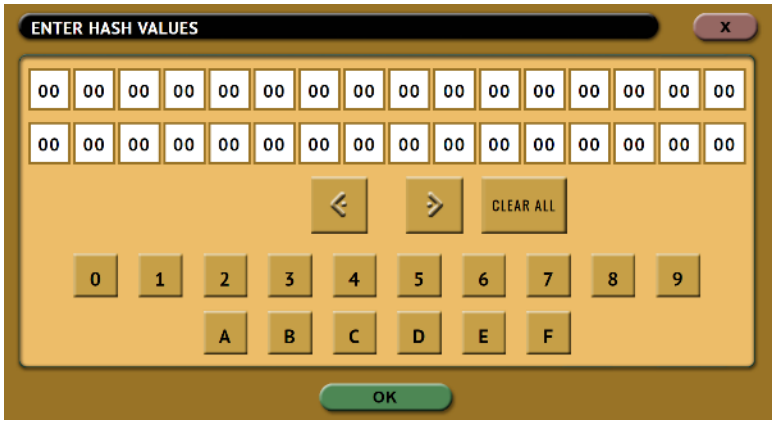
Select one of the following hash methods:

- SHA-1
- SHA-256
- MD5

5.2.3.1.2 Hash Values

By default, this value will have 0s (zeros). If this is not changed, or no value is entered, this will instruct the Falcon-NEO to hash the drive using the selected algorithm in the previous step. The Falcon-NEO will use the result as the expected value. If a value is entered, the Falcon-NEO will hash the selected drive and verify hash with the value entered/edited.

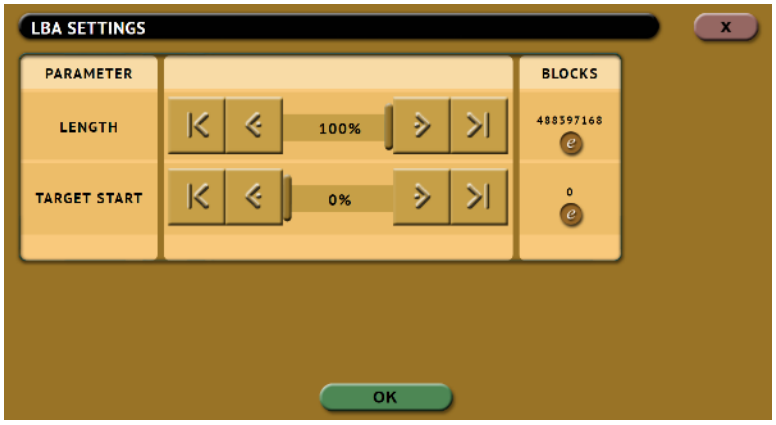
To set the expected value, tap the ***(edit)*** icon. The on-screen keyboard will appear, and the expected hash value can be set.



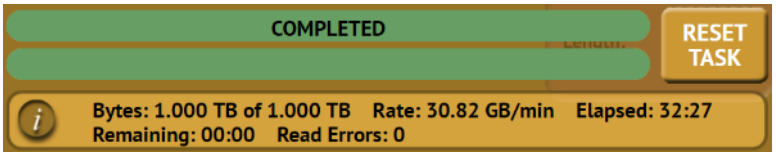
There is a ***Clear All*** button to easily clear all values.

5.2.3.1.3 LBA

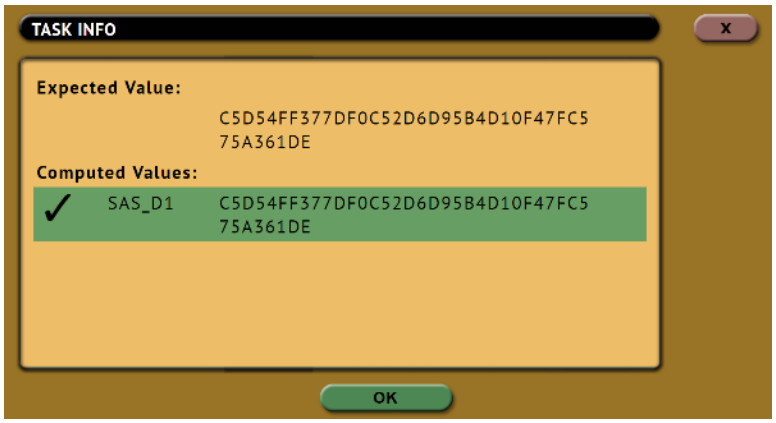
The LBA icon will bring up the LBA settings screen. The user can adjust the percentage or the number of blocks of the drive to hash and where to start the hash. By default, the length is set to 100% (whole drive) and the starting percentage is set to 0% (start of the drive).



When the Falcon-NEO 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.



5.2.3.2 Case Verify

There are two settings in the Verify Hash screen:

- **Primary –** Will verify just one hash value (For example, if SHA-1 or MD5 was selected during the image process).
- **Both –** Will verify both SHA-1 and MD5 if the ***SHA-1+MD5*** hash was selected during the image process.

5.2.4 Case Info

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

Information entered here will appear in the logs. More information on the Case Info screen can be found in ***Section 4.3.1***.

5.3 Wipe / Format

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 Patterns, 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.

> Secure erase will not work on drives connected through the USB or PCIe ports.

- **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. The Falcon-NEO can verify each pass value through a setting. Any HPA, DCO, or ACS3 can be unlocked and wiped in these settings.

- **Format –** Formats the Destination drive with one of the following user-selectable file systems (with or without encryption): EXT4, NTFS, exFAT, or FAT32.

There are three selections when performing a wipe:

- Destination
- Settings
- Case Info

5.3.1 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***.

5.3.2 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***, and ***Format***.

The Falcon-NEO 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 Falcon-NEO will first secure erase the drive, then wipe the drive according to the mode specified, then format the drive.

5.3.2.1 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 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.

Secure Erase will not work on drives connected through the USB or PCIe ports.

Since Secure Erase is controlled by the drive, for questions on how each drive supports these features, or what the drive will do with these commands, please contact the drive manufacturer.

5.3.2.2 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/ACS3
- LBAS
- PASSES

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

5.3.2.2.1 Mode

Selecting ***Mode*** will open the Wipe Mode screen showing 3 options:

- **NONE –** Choosing this will instruct the Falcon-NEO not to perform a wipe using Wipe Mode.
- **DOD –** Choosing this will instruct the Falcon-NEO to perform a 7-pass wipe conforming to the DoD 5220.22-M 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.

5.3.2.2.2 HPA/DCO/ACS3

The HPA/DCO/ACS3 button will open the HPA/DCO/ACS3 option for wiping. If the drive to be wiped has HPA, DCO, and/or ACS3 that need to be wiped, select Yes for the corresponding option.

5.3.2.2.3 LBA

By default, this is set to 100% which will wipe all Logical Block Addresses (LBAs) and will wipe the entire drive (100%). The LBA count can be adjusted by tapping the ***edit*** icon.

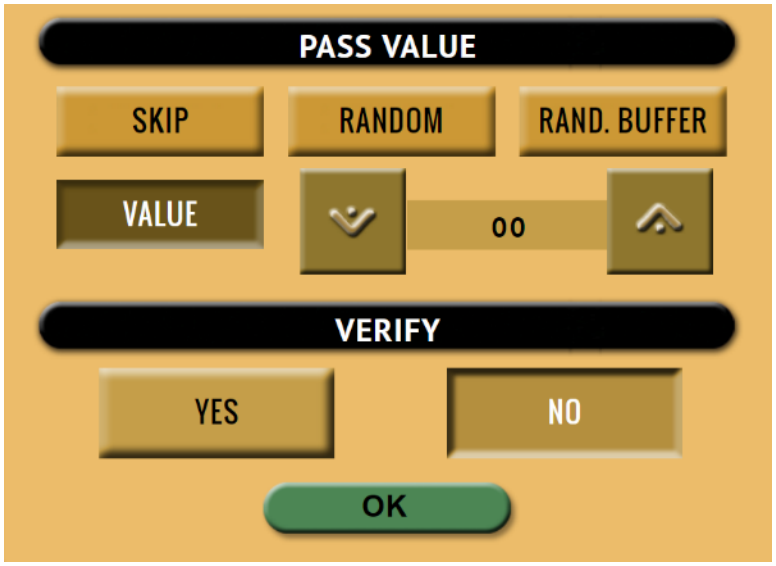
5.3.2.2.4 PASSES

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

- If ***None*** was selected, ***Passes*** is not selectable.
- If ***DoD*** was selected, all 7 passes will be pre-filled. Users can edit the pass values by tapping the ***edit*** icon. The default values are: 00, 01, 00, FF, F6, 00, XX (random).

- If ***Custom*** was selected, one pass will be pre-filled with a specified value. Users can edit the pass values if desired by tapping the ***edit*** icon. The default value for a custom pass is 00.

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



- **SKIP –** Instructs the Falcon-NEO to skip the pass.
- **RANDOM –** Writes one random hexadecimal value (from 00 - FF) to all the selected Logical Block Addresses.
- **RAND. BUFFER –** The Falcon-NEO will create an 8MB block filled with random values (each byte in the 8MB block will contain a random value). The 8MB block will be written repeatedly to fill the entire drive.
- **VALUE –** Instructs the Falcon-NEO to use the specified hexadecimal value to be written for the pass. The values can range anywhere from 00 to FF.
- **VERIFY –** Select ***YES*** to verify each wipe pass value the Falcon-NEO performs.

When ***Verify*** is set to ***YES***, the total time to wipe the drive will double.

5.3.2.3 Format

Formats the Destination using the EXT4, NTFS, exFAT, or FAT32 file system with or without encryption. To format the drive (with or without encryption) tap the ***Settings*** icon.

The Falcon-NEO will check the Destination drive for formatting prior to being used as a Destination or Repository for Imaging using ***Drive to File***, ***File to File***, ***Partition to File***, or ***Net Traffic to File***. If the drive has not been formatted by the Falcon-NEO, the Destination drive must be formatted using the Falcon-NEO prior to being used as a Destination for Imaging using the modes above.

Tap this icon to set the Falcon-NEO to format the drive (with or without encryption). The following settings are available:

- **Format –** When set to ***ON***, the Falcon-NEO will format the Destination drive with or without encryption. The drive will be formatted with the user's choice of file system (EXT4, NTFS, exFAT, or FAT32). When set to ***OFF***, the Falcon-NEO will not format or encrypt the selected drive.
- **File System –** Select the file system to be used to format the Destination drive. Users can select from EXT4, NTFS, exFAT, or FAT32.
- **Encryption –** Select ***ON*** to format the drive with encryption.

For more information on encrypted Destination drives, please see ***Chapter 7: Drive Encryption and Decryption***.

5.3.3 Case Info

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

Information entered here will appear in the logs. More information on the Case Info screen can be found in ***Section 4.3.1***.

5.4 Push

The network Push feature gives users the ability to push Falcon-NEO created evidence files from drives connected to the Falcon-NEO or from a Falcon-NEO repository to a network location or a Destination drive connected to the Falcon-NEO. The Push feature provides a more secure method than simply copying and pasting to the analysis computer by verifying the MD5 or SHA hash value (created during the imaging process) during the push process. The Falcon-NEO will create a log file for each push process.

There are three selections when performing a push:

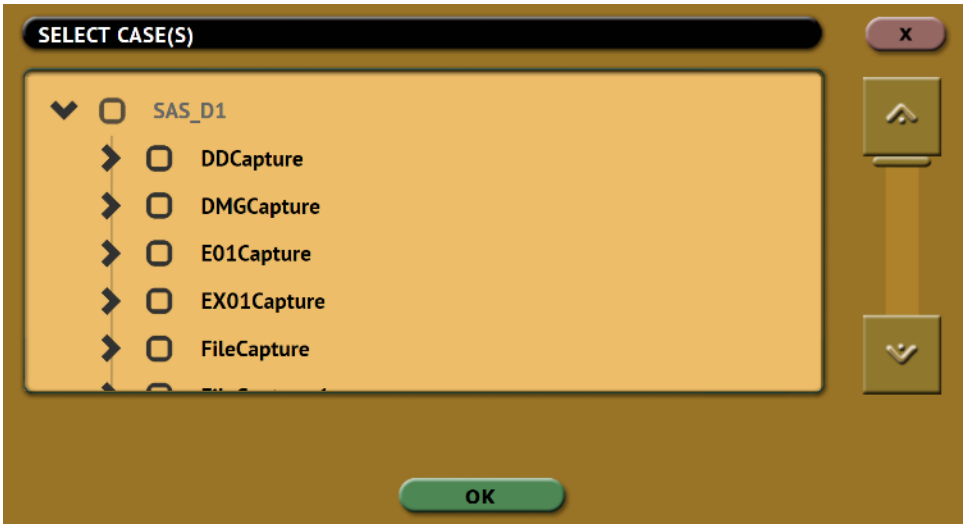
- Source
- Settings
- Destination

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 5.9.1***.

5.4.1 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).

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.



The Push feature will only push DD, E01, EX01, and DMG files.

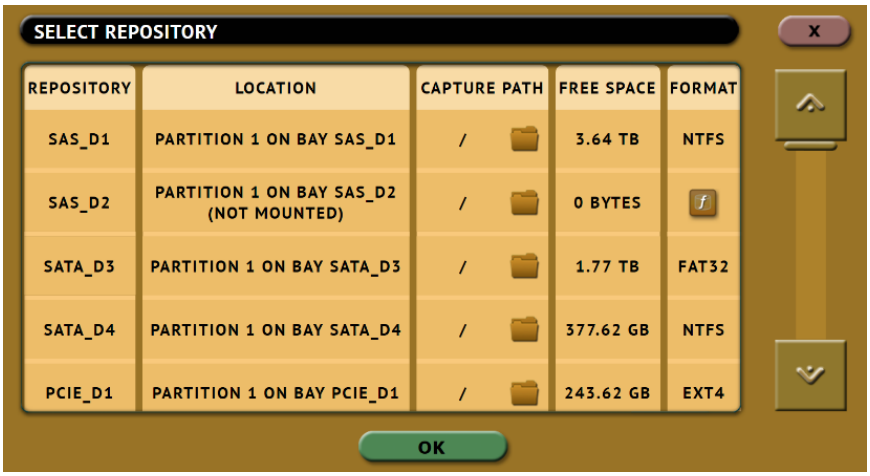
5.4.2 Settings

(Optional) Tap this icon to enter case info and to set the verify option. There are two verify settings available:

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

5.4.3 Destination

Tap this icon to select the drive or repository where the DD, E01, EX01, or DMG images will be pushed to (where the files to push will be pushed/copied to). This will only show drives connected to the Destination ports or repositories set up through the Manage Repositories screen.



Software release v2.2 adds the ability to specify a capture path allowing users to save image files to specific folders within the selected repository/destination drive.

Tap or click the ***Capture Path*** column on the desired drive or repository and a Capture Path selection screen will appear.

There are four buttons on the Capture Path selection screen:

- **Add Folder –** This is used to add a folder or sub-folder.
- **Delete Folder –** This is used to delete an empty folder. Folders that contain any files cannot be deleted with this method.
- **Rename Folder –** This will rename any folder.
- **OK –** Use this button when all desired changes have been completed.

> Creating a folder or sub-folder is optional. If none are created, simply tap the ***OK*** button to continue. The image file will be saved on the root of the drive/partition.

5.5 Task Macro

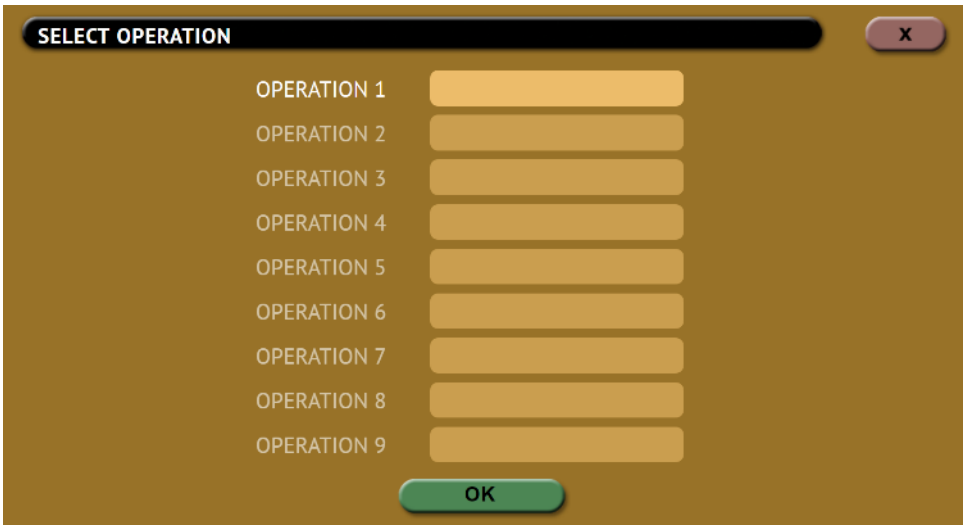
This operation allows up to five (5) macros that can be set. Each macro can run up to nine (9) tasks sequentially (one after another). For example, a macro can be set to perform these tasks in order: Wipe, image, hash, push, then wipe again.

Each of the five macros can be set by tapping on the Macro tabs on the top of the screen.

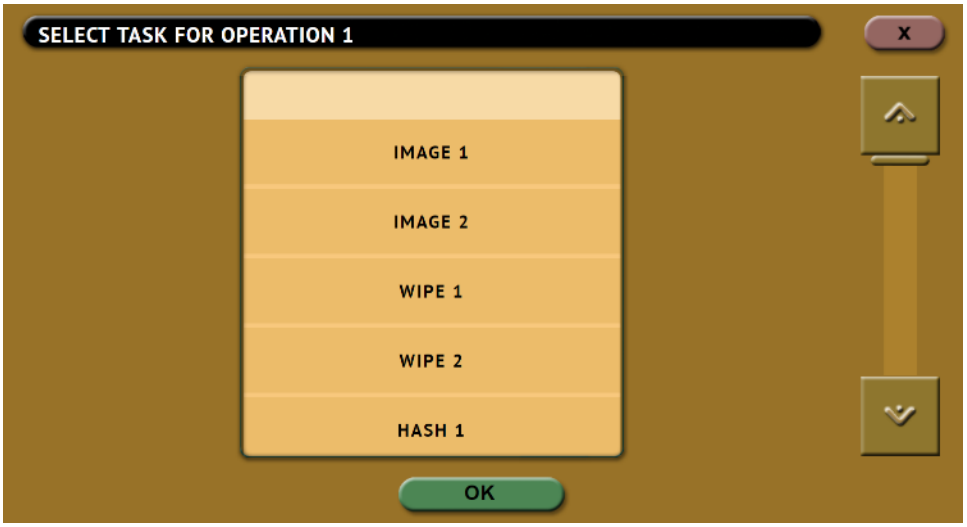
Each task or operation must be set up before setting up the macro. For example, to set up a Task Macro that will perform a wipe, then image, users must first set up both the wipe and image tasks. Once the wipe (for example, Wipe 1) and image (for example, Image 1) has been set up, the Task Macro can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

5.5.1 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 Falcon-NEO perform all the operations on the task list, tap the ***Start*** icon.

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

To set a macro to perform a Wipe using Secure Erase on SAS_D1, immediately followed by performing a Drive to Drive image from SAS_S1 to the newly wiped (secure erased) SAS_D1, the Wipe and Imaging Tasks first need to be set up.

1. First, set the Wipe task. Select SAS_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 the Source. Change the settings as needed. Select a 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.

5.6 File Browser

The Falcon-NEO has a built-in file browser. The File Browser allows the user to view the Source drive's partitions and its contents or image files created by the Falcon-NEO on the Destination drives. The file browser can also open several types of files including .jpg, .png, .gif, .txt, .html, and .pdf. This method can be very useful when the Falcon-NEO is out on the field and there are no computers to analyze or triage the contents of drives.

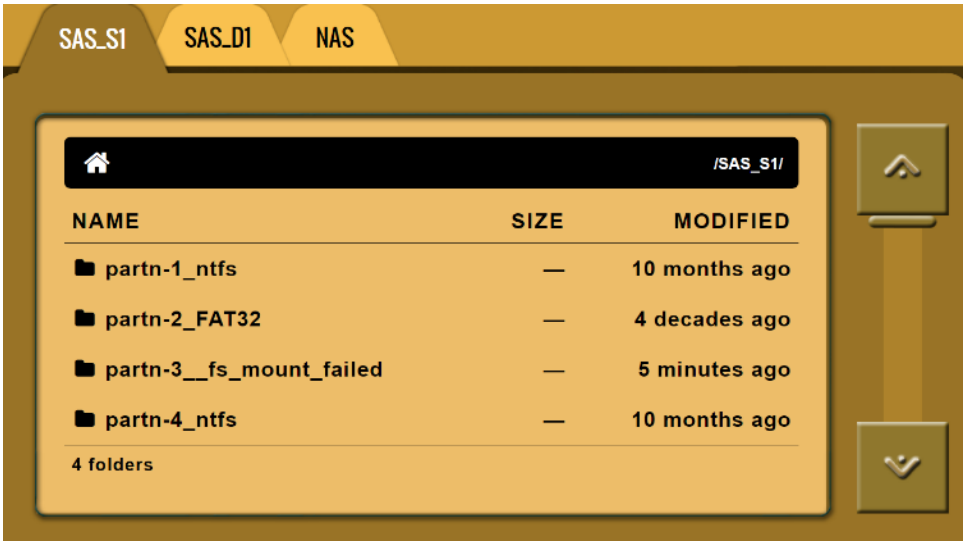
Software version 2.1 or newer adds the ability to view the contents of DD, E01, EX01, and DMG image files created by the Falcon-NEO.

Software 2.2 or newer adds the ability to view L01 image files and network repositories within the File Browser.

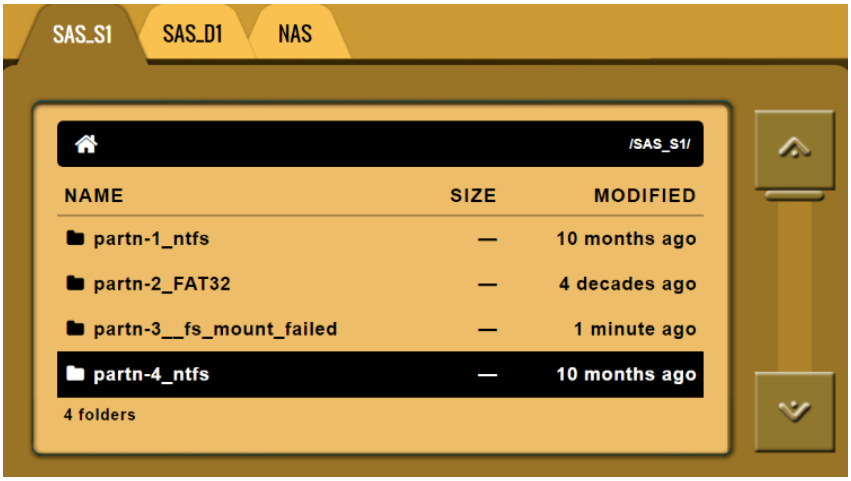
Software 2.3 or newer adds the ability to view APFS source drives.

5.6.1 Viewing Source Drives or Network Repositories

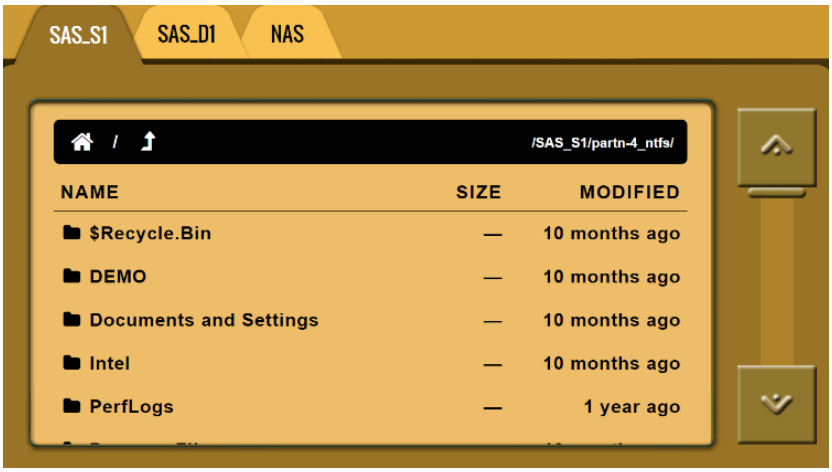
In the File Browser screen, select the Source Drive or Network Repository to view by tapping or clicking one of the tabs on the top of the screen:



If the drive has partitions, Select the partition to view:

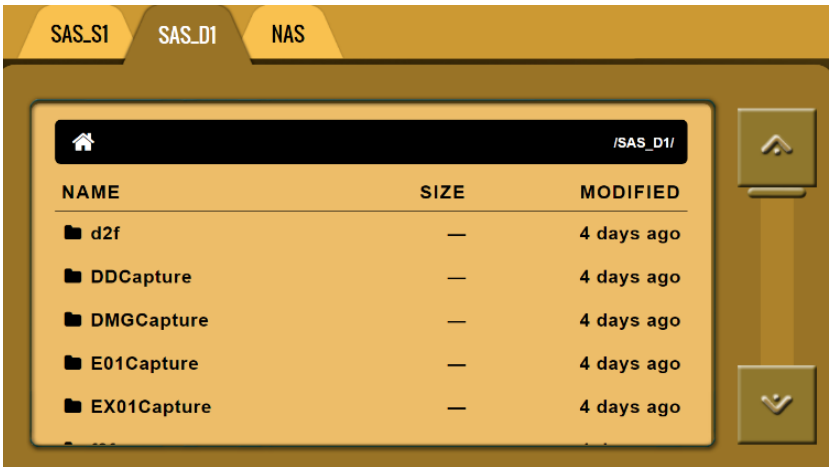


The folders/directories and files in that partition will be displayed:

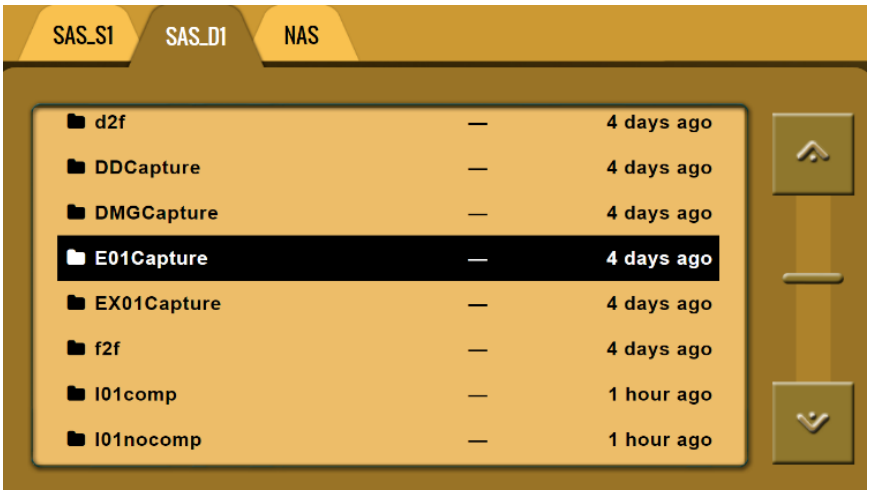


5.6.2 Viewing DD, E01, EX01, DMG, and L01 Images

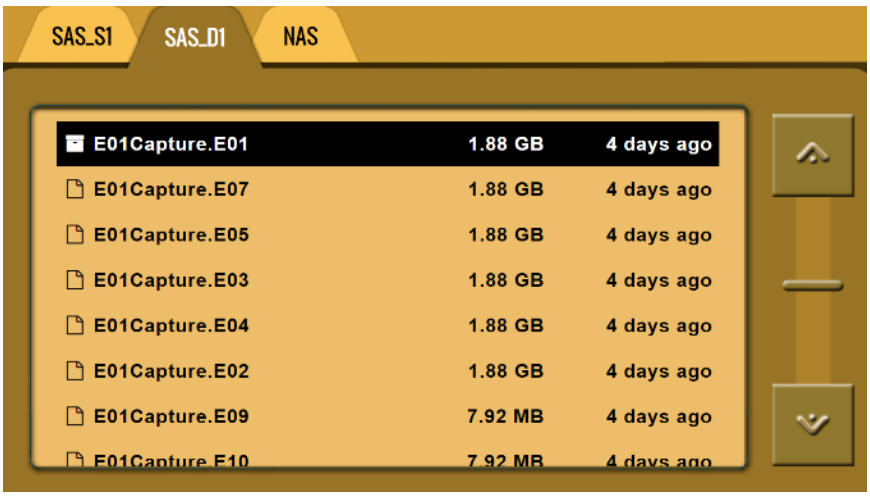
In the File Browser screen, select the Drive or Network Repository to view by tapping or clicking one of the tabs on the top of the screen:



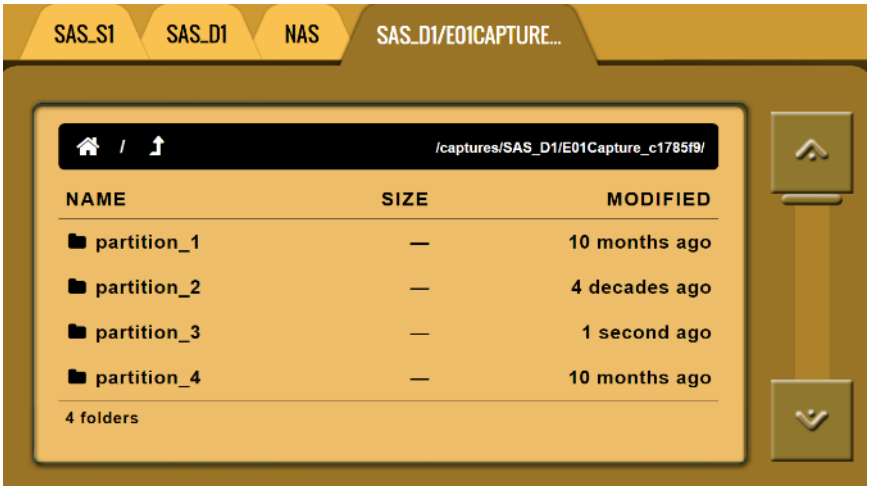
Select the folder where the image is located:



The captured image files will be displayed. To view the contents of the image file, select the first segment of the image file (for example, DDCapture.001, E01Capture.E01, Ex01Capture.Ex01, or DMGCapture.dmg.

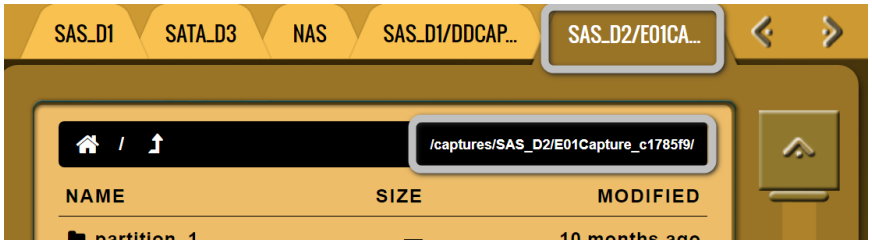


A new tab will appear showing the contents of the image file:

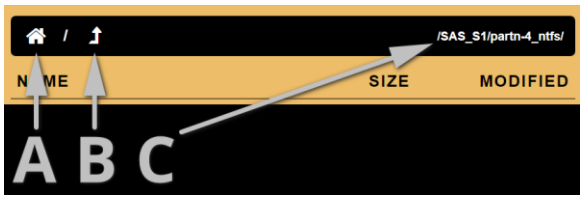


5.6.3 Additional Notes About Using the File Browser

- The tab label may not display the entire path and image file name. When this happens, the entire path and image file name can be seen on the top-right side of the window.



- Legend:



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

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

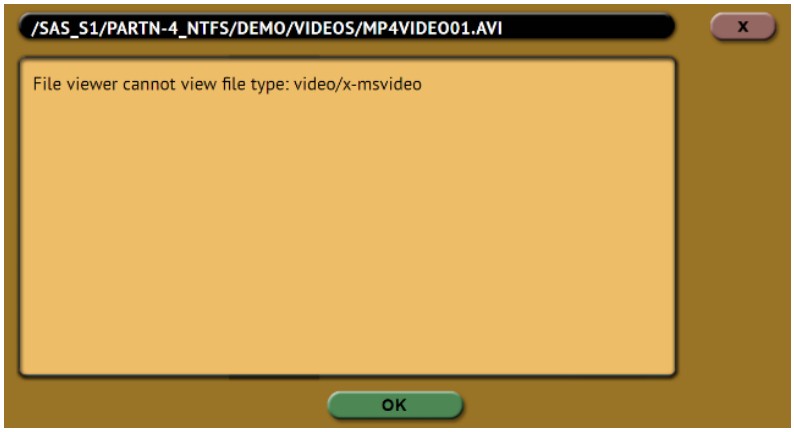
C – Path – Displays the current path to the folder/directory/file being viewed.

The Falcon-NEO can open and preview certain files. Some of the files it can preview are:

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

- When more than 5 tabs are available for browsing, use the ***Left*** and ***Right Arrows*** located on the top-right of the screen:

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

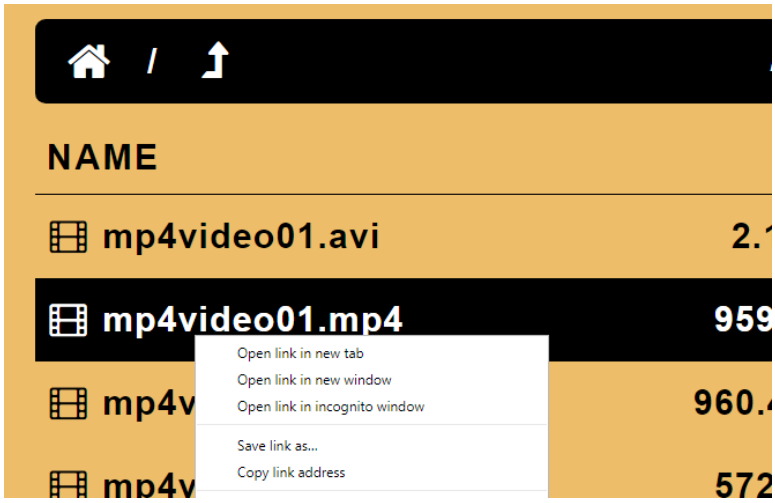


- Encrypted drives/volumes/partitions will show "fs_mount_failed" and must be decrypted before viewing the contents using the File Browser.
- Using the File Browser function to view a file only opens the file and does not modify the contents of the file. The only change to the contents of the destination drive will be the file's accessed date and time.

5.6.4 Viewing Files from the Web Interface

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

1. Using a compatible web browser, connect to the Falcon-NEO's web interface (see ***Section 9.1*** for more information on how to connect to the Falcon-NEO's web interface).
2. From the Falcon-NEO'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..."*** (other browsers may call this selection something different) and save the file to the local computer.



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

> The computer will need to be able to open the type of file that was downloaded. For example, if an MP4 file was downloaded, the computer needs to have software that can open an MP4 file.

5.7 Logs

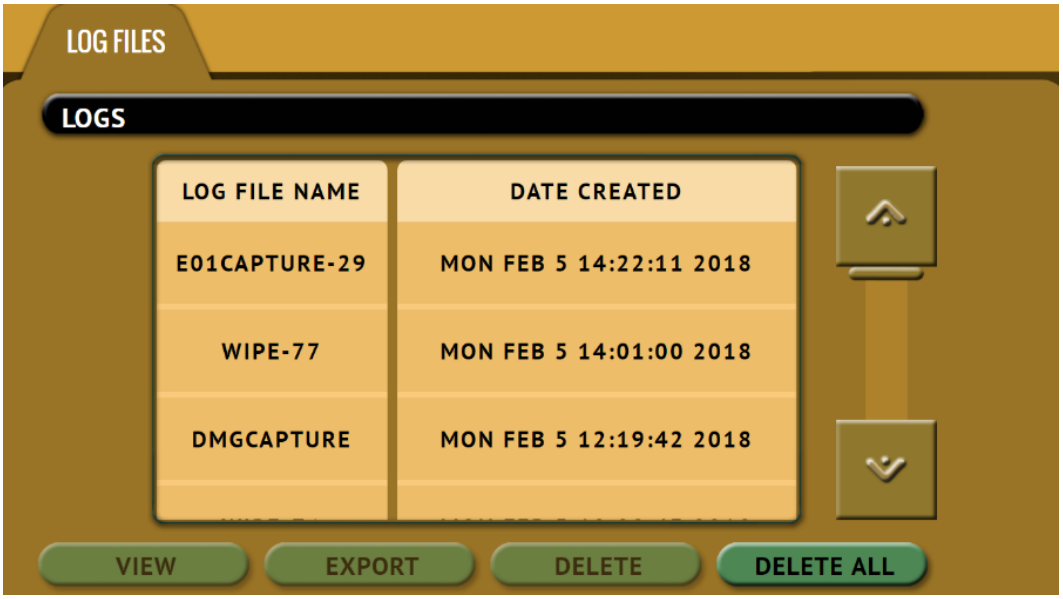
The Falcon-NEO keeps logs of all imaging, hash, wipe, format, and push operations. Logs can be viewed directly on the Falcon-NEO or from a computer's browser (if the Falcon-NEO is connected to a network).

When using Drive to File mode (DD, E01, EX01, or DMG), 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 Falcon-NEO and its settings
- Case info (if entered)
- Source and Destination hashes (if verify was set to YES)

See ***Section 3.7.1*** for instructions on how to export the log files.

See ***Section 3.7.2*** for instructions on how to download the log file from the web interface.

See ***Section 3.7.3*** for instructions on how to delete the log files.

See ***Section 3.7.4*** for instructions on how to access the logs over a network.

5.8 Statistics

This will display the following tabs: About, Adv. Drive Statistics, Network Interface Stats, Debug Logs, and Help.

5.8.1 About Screen

The ***About*** screen will show information about the Falcon-NEO including the current software installed, host name, and IP address. There is a QR code that can be scanned on a phone or tablet. If the phone or tablet is connected to the same network the Falcon-NEO is connected to, it will open a web browser and connect to the IP address or hostname of the Falcon-NEO.

5.8.2 Adv. Drive Statistics

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.

5.8.3 Network Interface Stats

This screen displays the Network Interface statistics (Receive and Transfer bytes, packets, drops, errors, and link status).

5.8.4 Debug Logs

There may be times when Logicube Technical Support will ask for debug logs. This tab allows the user to export the debug logs to a USB flash drive (connected to one of the two front USB ports). To export the debug logs:

1. Connect a formatted USB flash drive to one of the two front USB ports.

   The USB flash drive must be formatted in Windows using the NTFS, FAT32, or FAT file system.

2. Disconnect any other drive connected to the other front USB port.
3. From the Debug Logs screen, tap ***Export***.
4. The Debug Logs will be exported to the USB flash drive and can be zipped/compressed and sent to Technical Support.

5.8.5 Help

The Help tab contains a QR code that links to the user's manual online. There are several ways to view the manual through the QR code such as:

- From the touch screen (if the Falcon-NEO is connected to a network with Internet access), simply tap the QR code.
- Through a web browser, when using the web interface (see ***Section 9.1*** for more information on the web interface), click the QR code.
- Scan the QR code from a mobile phone or tablet that has internet access.

5.9 Manage Repositories

Repositories can be added to the Falcon-NEO using this operation.

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

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

The following information is required to set up an SMB/CIFS repository:

- **Path –** Also called the Network Path (The IP address/Hostname and sharename).
- **Domain –** If the shared resource is in a domain. If not, use the workgroup name.
- **Username –** The username with full permissions to the shared resource (read and write access).
- **Password –** The password for the username.

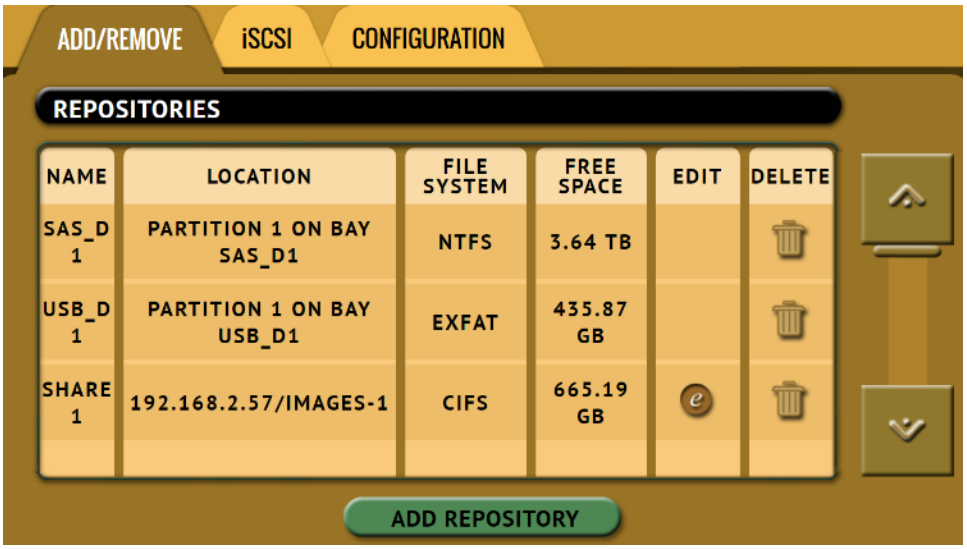
The following information is required to set up an iSCSI repository:

- **Portal –** The IP address or host name of the iSCSI Target.
- **Username –** The username with full permissions to the shared resource (read and write access).
- **Password –** The password for the username.

Please consult your Network or Systems Administrator to ensure the above requirements are available or set up properly.

5.9.1 Add/Remove

A list of repositories will be shown. The user has the option of adding or deleting a repository. This will include all drives attached to the Falcon-NEO (Destination ports) and any networked repository.

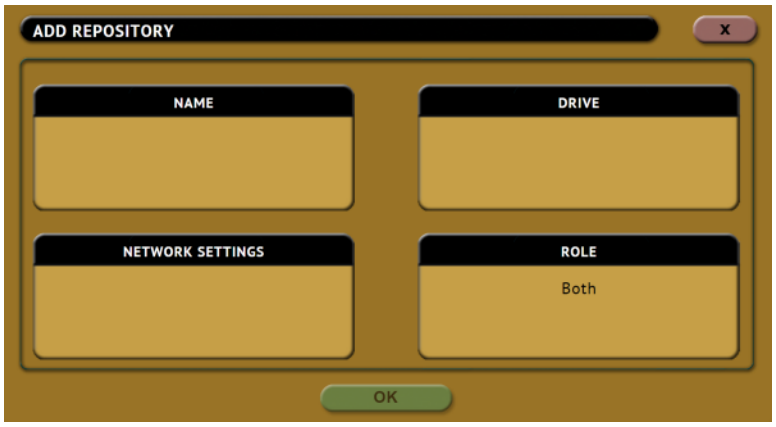


If a repository location shows ***(NOT MOUNTED)***, it is because the drive attached is not formatted by the Falcon-NEO or the Falcon-NEO cannot connect to the shared network resource, or the drive needs to be formatted (if it is a connected drive).

In order for a repository to remain configured when the Falcon-NEO is turned off, the changes must be saved and loaded to a profile. Details on profiles can be found in ***Section 5.10.1***.

5.9.1.1 Adding a Repository Using CIFS or SMB

1. Tap ***Add Repository*** to add a repository. The Add Repository window will appear.



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

3. Tap ***Drive*** to select ***network share*** to set as a repository. Tap the ***OK*** icon when finished.

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

For the ***Path***, make sure the forward-slash (/) is used and not the backslash symbol (\ ).

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

5.9.1.2 Editing or Deleting/Removing a Repository

To edit a repository, tap the ***edit*** icon. To delete a repository, tap the ***delete*** icon. A confirmation screen will appear. Tap ***Yes*** to permanently delete the repository from the list.

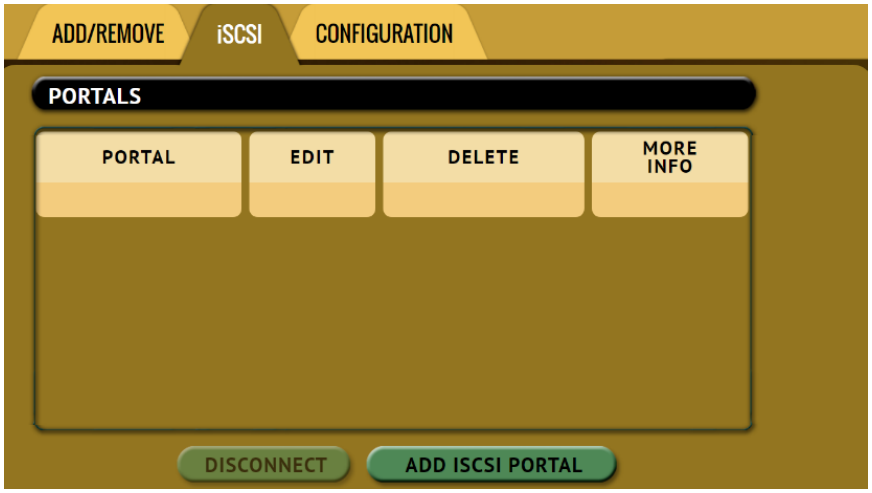
5.9.2 iSCSI

This screen allows a user to add repositories using the iSCSI protocol.

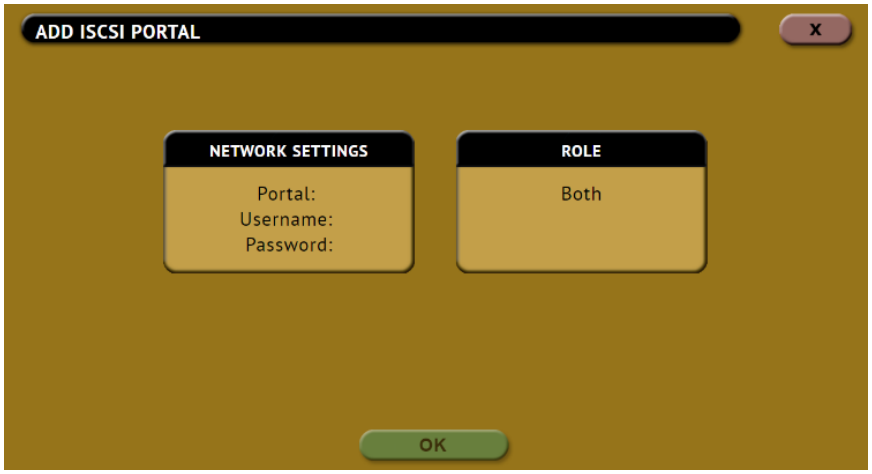
To add a repository using the iSCSI protocol, an iSCSI Target must be set up on the remote system. Since networks are configured differently, a Systems Administrator or Network Administrator may be needed to set up the iSCSI protocol.

Once the iSCSI Target has been setup:

1. Tap ***Add iSCSI Portal***.



2. The ***Add iSCSI Portal*** window should appear:



3. Tap ***Network Settings*** and input the ***Portal*** (IP address or hostname), ***Username***, and ***Password***. Tap the ***OK*** icon when finished.

4. Optional: Tap ***Role*** and input the role for this repository.
5. Tap ***OK*** when finished. The screen will go back to the ***Portals*** screen.
6. In the ***Portals*** screen, tap the iSCSI portal to highlight it, then tap ***Connect***.
7. The Falcon-NEO will attempt to connect to the iSCSI target. If successful, a "connected" screen will appear. Tap ***OK*** to continue.

> Multiple iSCSI connections can be added. To disconnect an iSCSI connection, highlight the portal to disconnect, then tap ***Disconnect***. To edit or delete an iSCSI connection, tap ***Edit*** or ***Delete***.

5.9.3 Configuration

This screen allows a user to set a default file system when formatting a drive. This setting only configures the ***Format Repository*** screen that appears in the ***Imaging*** task when ***Drive to File***, ***File to File***, ***Partition to File***, or ***Net Traffic to File*** is used, and the Destination drive is not formatted.

5.10 System Settings

The ***System Settings*** screen allows users to configure the following settings for the Falcon-NEO:

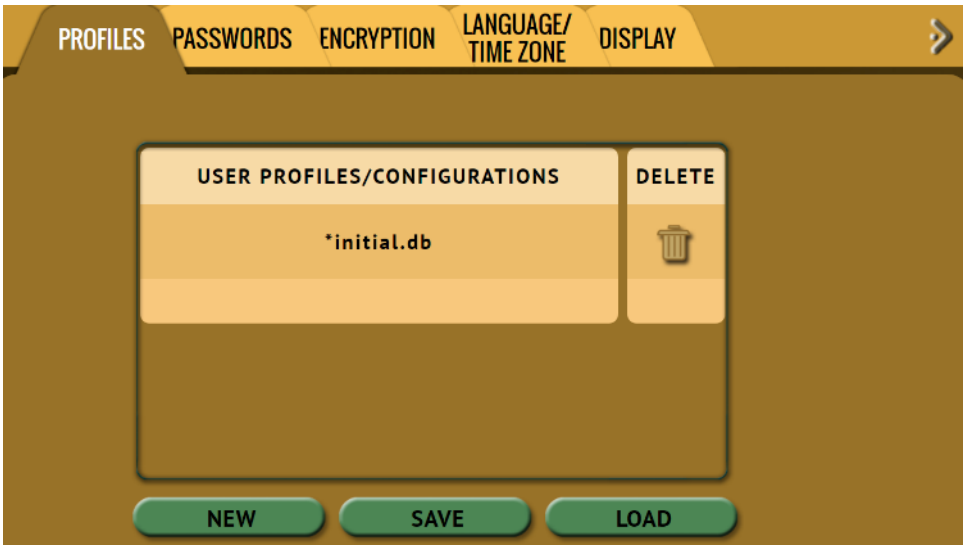
- Profiles
- Passwords
- Encryption
- Language/Time Zone
- Display
- Notifications
- Debug

5.10.1 Profiles

Do not highlight and save over the INITIAL.DB profile. This is the default profile of the Falcon-NEO and is used to reset the Falcon-NEO to the factory default settings.

This screen shows all user profiles for the Falcon-NEO. There are three selections in this screen:

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



The Falcon-NEO will boot with the profile that has an asterisk (*) next to the name.

After loading a profile, it is recommended to refresh the User Interface. This can be done one of several ways:

- From the touch screen, go to the POWER OFF menu and tap the ***Refresh*** button.

- If a web browser is used for remote operation, press the F5 key on the computer's keyboard or locate the ***Refresh*** icon on the browser.

The Profiles tab allows users to create, save, and load different profiles with different configurations. When a profile is loaded using the ***Load*** icon, the Falcon-NEO will load that profile during its boot process.

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

1. Turn the Falcon-NEO off then back on. This is an important step to help ensure only the changes desired will be the changes saved.
2. Go to the ***Imaging*** screen and set the ***Mode*** to 'Drive to File.
3. In the ***Settings***, set the image to ***E01*** and set the segment size to ***2GB***.

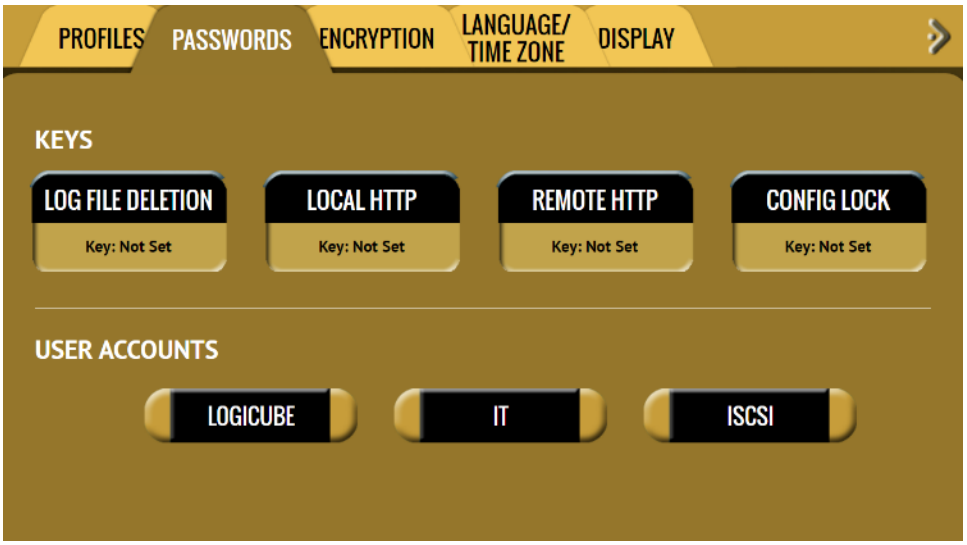
4. In the ***System Settings***, go to ***Profiles*** and tap the ***New*** icon.
5. Type a name for this profile. For example, E01-2GB and tap the ***OK*** icon. The profile name should appear on the screen.
6. Tap the newly saved profile and tap ***Save***. A confirmation screen will appear asking if you are sure you want to save the configuration.
7. Tap the ***Yes*** icon to save the profile.
8. 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. Tap the ***Yes*** icon to confirm.
9. The profile is now loaded. Also, the next time the Falcon-NEO 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.

When loading a profile, the Falcon-NEO will take several seconds to completely load the different settings.

5.10.2 Passwords

There are seven keys or passwords that can be set on the Falcon-NEO.



- **Key: Log File Deletion –** A key can be set as an extra layer of protection when deleting log files. If this key is set, a prompt will appear, and the correct key must be entered before any log files can be deleted.
- **Key: Local HTTP –** A key can be set to lock the local touch screen on the Falcon-NEO. If this key is set, a key prompt will appear, and the correct key must be entered before allowing access to the local touch screen.

- **Key: Remote HTTP –** A key can be set to lock remote HTTP access (through a web browser). If this key is set, a key prompt will appear, and the correct key must be entered before allowing access through a web browser.
- **Key: Config Lock –** A key can be set to lock out any configuration changes. If this key is set, changes to the different types of operations cannot be made without entering the correct key. Different types of operations can still be started.

  For example, if the Config Lock key is set, and the IMAGE task is configured for Drive to File imaging, the user will be unable to change the mode to Drive to Drive but can start the Drive to File task.
- **User Account: LOGICUBE –** Allows the user to change the ***logicube*** local account.
- **User Account: IT –** Allows the user to change the ***it*** local account.
- **User Account: ISCSI** – Allows the user to change the ***iscsi*** local account.

5.10.2.1 Setting Key Passwords

To set a key for ***Log File Deletion, Local HTTP, Remote HTTP, or Config Lock***, tap one of the buttons. 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.

The ***Auto Lock*** button is available for the following keys:

- Local HTTP
- Remote HTTP
- 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.

> The keys for ***Log File Deletion***, ***Local HTTP***, ***Remote HTTP***, and ***Config Lock*** can be saved into a user profile and loaded each time the Falcon-NEO is turned on. See ***Section 5.10.1*** for more information on saving and loading a user profile.

Remember the various keys! If the Falcon-NEO is configured to load a user profile with any key set (enabled) and the key is forgotten, the only way to reset the key is to load the ***initial.db*** profile using the Command Line Interface. See ***Section 5.10.2.1.2*** for more information.

If the ***initial.db*** has a key configured, and the key was forgotten, contact Tech Support assistance.

5.10.2.1.1 Config Lock Notes

A shortcut (and indicator) to the ***config lock*** can always be seen on the Falcon-NEO's screen. It is located on the top-right of the screen, next to the Falcon-NEO 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 Config lock unlock key.
- **Hash/Verify –** 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 Config lock unlock key.
- **Wipe/Format –** 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 Config lock unlock key.
- **Push –** A push 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 Config lock 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 Config lock unlock key.
- **Logs –** Logs are 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, edited, or deleted without the Config lock unlock key.
- **System Settings –** This entire section cannot be accessed without the Config lock unlock key.
- **Network Settings –** This entire section cannot be accessed without the Config lock unlock key.

- **Software Updates –** This entire section cannot be accessed without the Config lock unlock key.
- **Power Off –** This entire section cannot be accessed without the Config lock unlock key.

> The Falcon-NEO can still be turned off without the unlock key by using the power button located on the top of the Falcon-NEO.

5.10.2.1.2 Forgotten password for any keys

If any of the keys are forgotten, the INITIAL.DB profile will need to be loaded using the Command Line Interface (CLI). See ***Section 9.2*** for more information on how to connect to the Falcon-NEO using the CLI.

> This method will only work if the INITIAL.DB profile does not have a Config Lock Key saved. If the INITIAL.DB has a Config Lock Key configured, and the password was forgotten, contact Tech Support assistance.

Once connected to the Command Line Interface (CLI):

1. Log in 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 profiles (or databases) saved. The Falcon-NEO has one default profile called ***initial.db***. Any profiles added by users will appear in this list. The db that shows an asterisk (*) before the name is the current database or configuration being loaded each time the Falcon-NEO is turned on.

```
it@falcon-171038(command-config)> db list
Number of DB's: 2
0: *lock.db
1: initial.db
```

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 Falcon-NEO off using the power button, then close the Telnet/SSH application.
8. Turn the Falcon-NEO on. When the Falcon-NEO boots up, it will load the default configuration (INITIAL.DB).

5.10.2.2 User Account Passwords

The Falcon-NEO comes with three built-in user accounts:

- logicube
- it
- iscsi

All user account passwords can be changed on this screen. To change the password for any of the accounts, tap the ***LOGICUBE***, ***IT***, or ***ISCSI*** button. A screen will appear:

1. Enter the current password.

> The default password for each account is:
>
> **LOGICUBE:** logicube
> **IT:** it
> **ISCSI:** logicube@19755

2. Enter a new password.
3. Enter the new password again in the 'confirm password' box.
4. Tap the ***OK*** icon when finished.

> The ***User Account Passwords*** **<u>do not need to be saved into a user profile</u>**. Changing any of these two passwords will take effect immediately. If the User Account password is forgotten, contact Tech Support assistance.

5.10.3 Encryption

The Falcon-NEO can secure sensitive evidence data with whole disk drive encryption using the NIST recommended XTS-AES-256 cipher mode. Destination drives that are encrypted by the Falcon-NEO can be temporarily decrypted by using the Falcon-NEO or third-party software (VeraCrypt, TrueCrypt, or FreeOTFE).

> For in-depth information on encrypting and decrypting a drive using the Falcon-NEO, or decrypting a drive using VeraCrypt, TrueCrypt, or FreeOTFE, please see ***Chapter 7: 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 ***VCRYPT***, ***TC-XTS***, ***CBC***, or ***ECB*** cipher modes.
- **Cipher –** At this time, only the ***AES-256*** cipher is supported.
- **IV Generation –** Initialization Vector. Unavailable when VCRYPT or 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.

Falcon-NEO encrypted drives can be used with the following image modes:

- Drive to File
- File to File
- Partition to File
- Net Traffic to File

Remember the password used to encrypt the Destination drive! Logicube cannot retrieve or unlock the encrypted drive without the password.

5.10.4 Language/Time Zone

The Falcon-NEO's menu system's language can be changed. 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.

5.10.4.1 Language

The following languages are available:

- English
- Chinese (中文)
- Korean (한국어)
- Japanese (日本語)

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

To change the language displayed. As soon as the selection is made, the Falcon-NEO's screen (or the computer's Internet browser) will automatically refresh and display the selected language.

The language selection is independent of the display. For example, if the language is changed on the Falcon-NEO's screen, the web browser's language will not change unless it is changed through the web browser.

The language selection does not need to be saved to a profile. Any change in the language selection will stay the same until it is changed again, even after the Falcon-NEO is turned off.

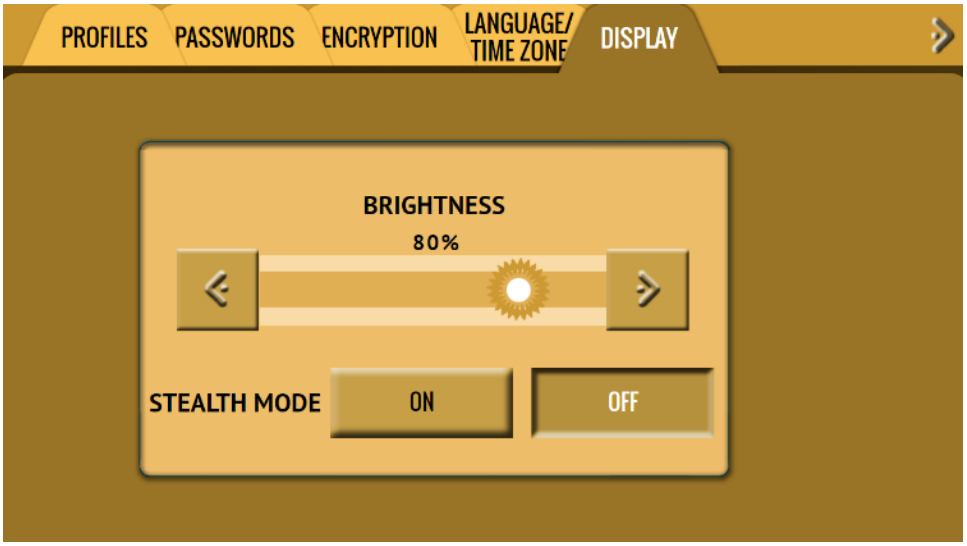
5.10.4.2 Time Zone

The Falcon-NEO utilizes NTP (Network Time Protocol). Each time the Falcon-NEO 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 Falcon-NEO 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 Falcon-NEO is located. Tap the ***OK*** icon to set the time zone.

5.10.5 Display



Brightness – The Falcon-NEO's screen's brightness may need to be adjusted, depending on the user's preference. To adjust the brightness, use the left or right arrow icons on the screen. The screen's brightness will adjust accordingly.

> The screen brightness cannot be saved and loaded as a user profile. Each time the Falcon-NEO boots, the brightness will be reset to 80%.

Stealth Mode – Stealth mode turns the Falcon-NEO's screen off, allowing privacy so no one can see what the Falcon-NEO is doing. When Stealth mode is activated, currently running operations continue to run.

To turn Stealth mode on, tap ***ON***.

To turn Stealth mode off and restore the Falcon-NEO's display, tap anywhere on the screen.

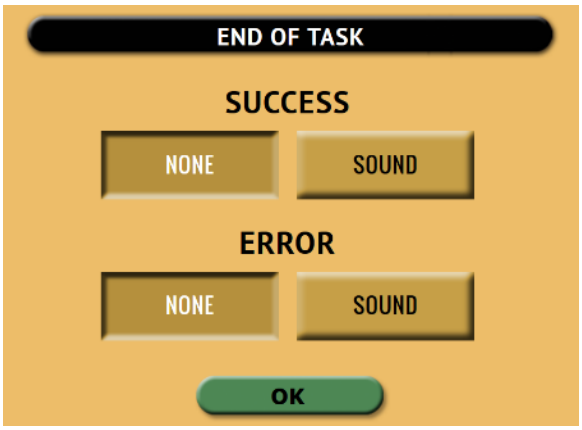
> Stealth mode will not have any effect when using the Graphical User Interface through a computer's Internet browser.

5.10.6 Notifications

To access the Notifications tab in the System Settings screen, tap the right navigation arrow below the Falcon-NEO logo (located on the top-right of the screen). To see the previous tabs, tap the left navigation arrow.

The Falcon-NEO can produce audible notification (beeps) when a task finishes successfully or if an error appears.

1. Tap ***End of Task*** to configure the notifications.
2. Select ***None*** or ***Sound*** for when the Falcon-NEO has a successful task or if the task has an error.



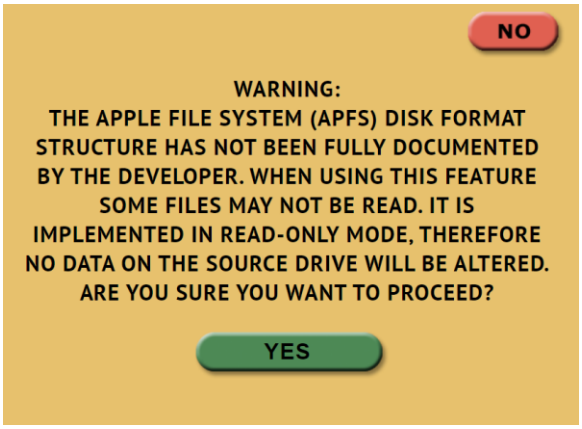
3. Tap the ***OK*** icon when finished.

End of Task notifications can be saved into a user profile and loaded each time the Falcon-NEO is turned on. See ***Section 5.10.1*** for more information on saving and loading a user profile.

5.10.7 Advanced

To access the Advanced tab in the System Settings screen, tap the right navigation arrow below the Falcon-NEO logo (located on the top-right of the screen). To see the previous tabs, tap the left navigation arrow.

On this screen, users can enable APFS ***File to File*** imaging. Set APFS to ***ON*** before starting a ***File to File*** imaging task with a Source drive that contains the Apple File System (APFS). A warning screen will appear:



5.10.8 Debug

To access the Debug tab in the System Settings screen, tap the right navigation arrow below the Falcon-NEO logo (located on the top-right of the screen). To see the previous tabs, tap the left navigation arrow.

This screen may adversely affect PCIe and/or NVMe performance. No changes should be made on this screen unless instructed to by Logicube Technical Support.

5.11 Network Settings

The Network settings screen has two tabs: ***Interfaces*** and ***HTTP Proxy***. The ***Interfaces*** tab allows the configuration of the network interface which includes setting a static IP (DHCP is set by default) and allows certain services to be enabled or disabled. There is also an ***HTTP Proxy*** tab where proxy server information can be entered.

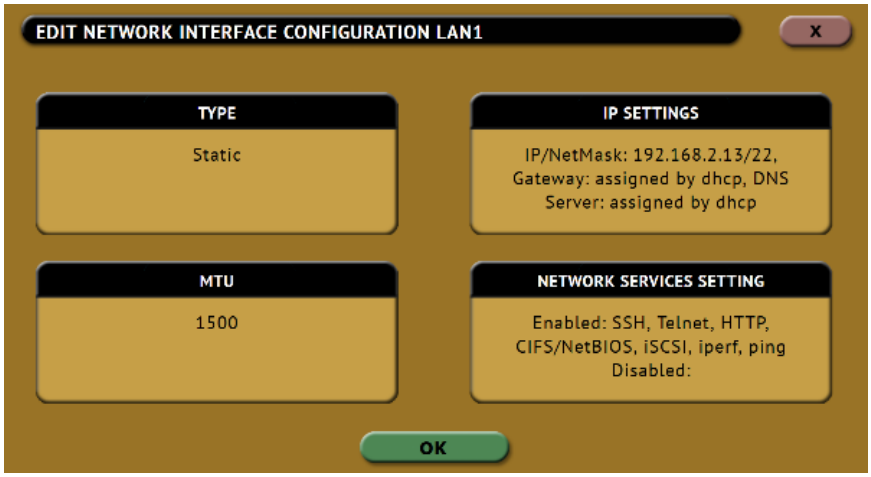
5.11.1 Interfaces

The Interfaces tab displays the network interface information (MAC Address, Configuration type (DHCP or Static), MTU, and status. This tab also allows enabling or disabling certain services. To edit the network interface configuration, tap the Ethernet adapter name (LAN1 or LAN2) then tap the ***Edit Configuration*** button.

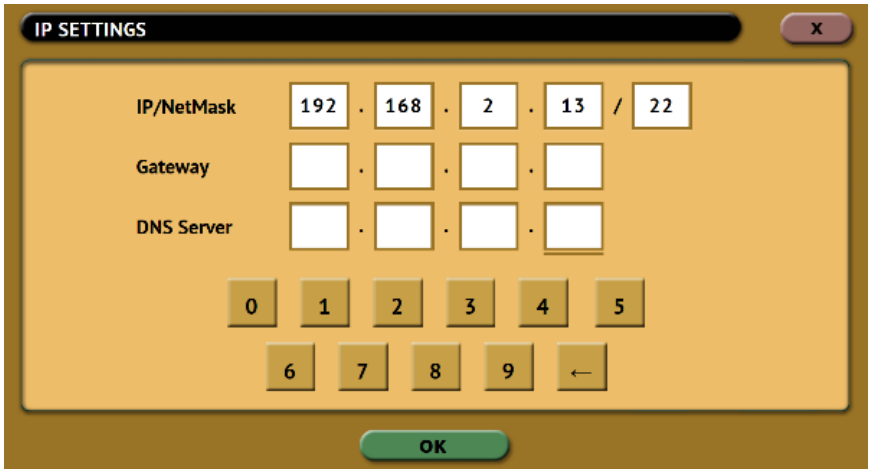
5.11.1.1 Configuring a Static IP address

The Falcon-NEO is DHCP enabled by default. The Falcon-NEO can be configured with a static IP.

1. From the ***Interfaces*** tab, select the network interface to edit (LAN1 or LAN2) then tap ***Edit Configuration***. The ***Edit Network Interface Configuration*** screen should appear.
2. From the ***Edit Network Interface Configuration*** screen, tap the ***Type*** box and select ***STATIC*** then tap the ***OK*** icon. The ***IP SETTINGS*** box should now be selectable.



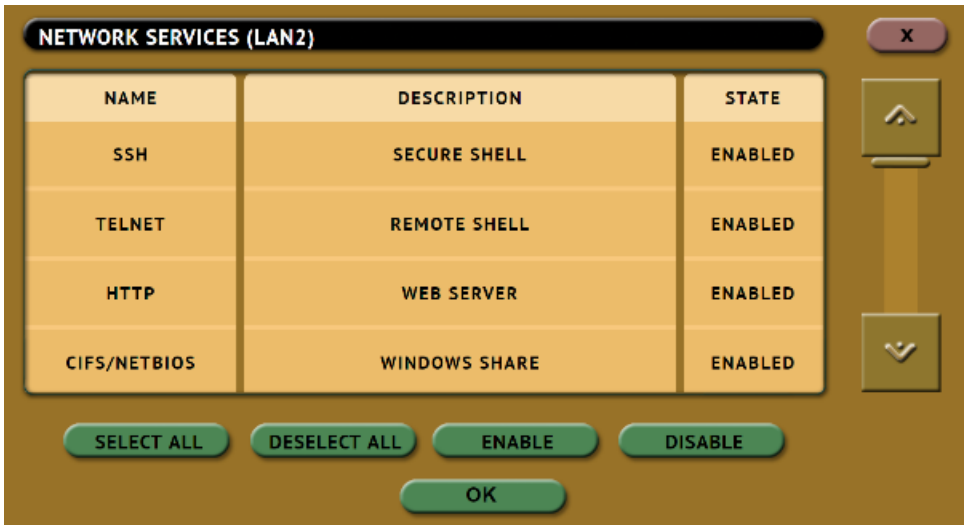
3. Tap the ***IP SETTINGS*** box to manually set the IP address, NetMask, Gateway, and DNS Server. When finished, tap the ***OK*** icon.



To save the settings so that the Falcon-NEO boots up with the static IP address, see ***Section 5.10.1*** for more information on saving and loading a user profile.

5.11.1.2 Enabling/Disabling Network Services

Network Services are enabled by default. To enable or disable specific network services, go to the ***Edit Network Interface Configuration Screen*** and tap ***Network Services Setting***. The ***Network Services*** screen will appear:



Tap each network service to be enabled or disabled then tap the ***Enable*** or ***Disable*** icon.

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 Falcon-NEO.
- **CIFS/NETBIOS –** Disabling this will block any CIFS or NETBIOS connection to the Falcon-NEO (for example, Windows Explorer).
- **iSCSI –** Disabling this will block any iSCSI (Internet Small Computer System Interface) traffic.
- **Iperf –** Disabling this will block Iperf traffic (a network tool to measure bandwidth performance).
- **Ping –** Disabling this will block ping access to the Falcon-NEO.

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 Falcon-NEO through a web browser over the network.

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

5.11.2 HTTP Proxy

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

5.11.2.1 Server

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

5.11.2.2 Username/Password

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

5.12 Software Update

New and improved software will be released from time to time. There are two ways to update the software on the Falcon-NEO: From the web through a network connection or from a USB drive.

For the latest step-by-step instructions on how to update the Falcon-NEO software, please read the ***Falcon-NEO Software readme*** file located on the Falcon-NEO Support page on the Logicube website at http://www.logicube.com/knowledge/forensic-falcon-neo.

In-depth information on updating the Falcon-NEO software can be found in ***Chapter 8: Updating/Loading/Re-loading Software***.

5.13 Power Off

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

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

DRIVE POWER – Inactive drives connected to the Falcon-NEO can be set to go to standby mode in this tab. The default is set to 0 minutes (Off/Disabled).

6.0 Previewing Drives - Introduction

Contents of drives connected to both Source and Destination ports can be previewed. There are 4 different methods available to preview drive contents with the Falcon-NEO:

- Falcon-NEO's native File Browser
- A computer with the Falcon-NEO's File Browser
- SMB protocol (Using a file explorer)
- iSCSI protocol – Source drives only (Using a file explorer)

Drives connected to the Source ports are always write-protected. Previewing the contents of these drives will not alter the drive or its contents in any way.

	Physical Access to the Drive	Logical Access to the Drive	Access to Source Drives	Access to Dest. Drives	Concurrent Multi-User Connection	Concurrent Multi-Drive Access	Use of Third-Party Analysis Tools or Software
File Browser		✓	✓	✓			
Computer + File Browser		✓	✓	✓	✓	✓	Very Limited[1]
SMB		✓	✓	✓	✓	✓	✓
iSCSI	✓	✓	✓		✓	✓	✓

[1] Files must be downloaded from the Falcon-Neo to the computer one file at a time before it can be analyzed.

	Viewable File Types	Additional Comments
File Browser	Text, PDF, HTML, and some image files only	Drives can only be accessed on the Falcon-NEO unit itself.
Computer + File Browser	All files supported by the OS or installed software	Drives can be accessed from multiple computers if connected to a network. More powerful viewing capabilities through the computer's Operating System compared to using the File Browser alone.
SMB	All files supported by the OS or installed software	Logical access to partitions viewable by the computer's Operating System. Partitions are searchable using the Operating System's search functions. Third-party analysis tools and software can be used easily since partitions are mounted.
iSCSI	All files supported by the OS or installed software	Requires an iSCSI Target. Drives will appear in Disk Management and can be accessed on the physical level. Partitions are searchable using the Operating System's search functions. Third-party analysis tools and software can be used easily since partitions are mounted.

6.1 File Browser

See ***Section 5.6*** for details on how to use the File Browser.

6.2 Computer + File Browser

The Falcon-NEO can be accessed from a computer (through a direct network cable connection or through a network). Using a computer with the Falcon-NEO's file browser allows more files to be previewed by using the computer's Operating System and installed software. Connecting the two devices directly together with a network cable or onto a network and using the Falcon-NEO's web interface (See ***Section 9.1*** for more information on the web interface) allows the user to be able to open files that the Falcon-NEO cannot open using the file browser alone. See ***Section 5.6.1*** for details on how to use the File Browser using the web interface.

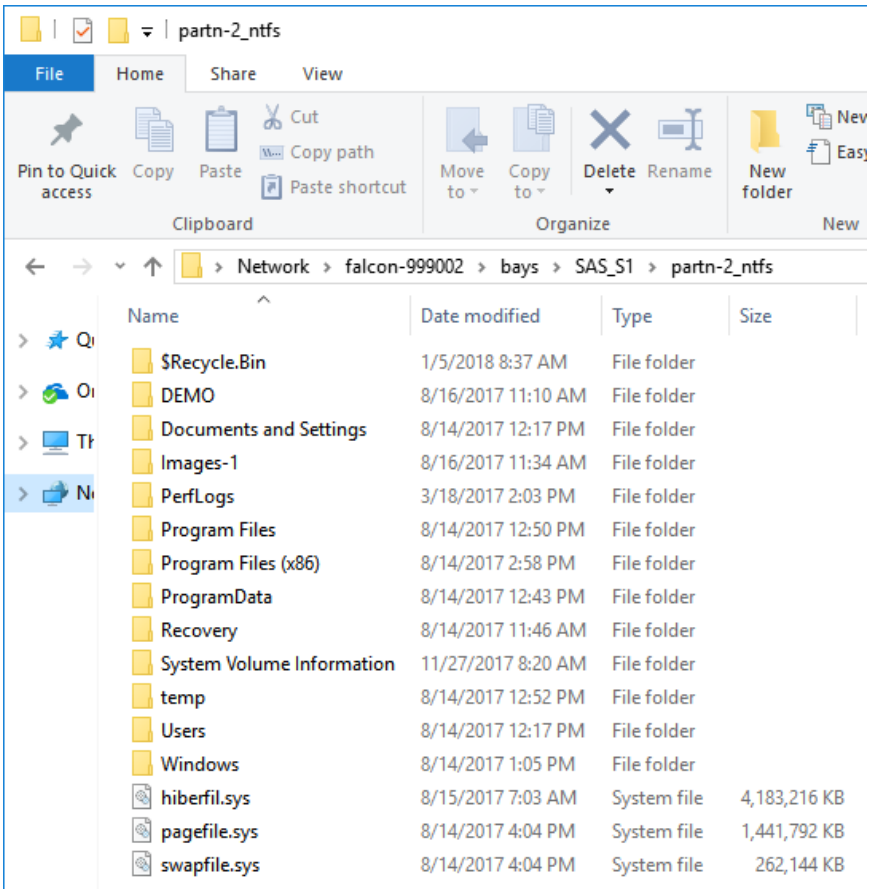
6.3 SMB

The Falcon-NEO can be accessed from a computer (through a direct network cable connection or through a network). One of the ways to access Source or Destination drives over the network is to use the SMB protocol. When using this method, all viewable/compatible partitions will be viewable on the computer. This method will give logical access to the contents of the drive.

See ***Section 10.1*** for details on how to view Source or Destination drives over the network using SMB.

Some advantages of using this method are:

- The contents of the drive are searchable using the Operating System's search functions.
- Third-party analysis tools and software can be used with the logical partition.



6.4 iSCSI

Another way to access Source drives from a computer (through a direct network cable connection or through a network) is through the iSCSI protocol. This method allows both physical and logical access to the drives but may require additional software installed and configured on the computer. To use the iSCSI protocol, an iSCSI initiator must be installed and configured to view the contents of drives connected to the Falcon-NEO over a network.

Like using SMB, some advantages of using this method are:

- The contents of the drive are searchable using the Operating System's search functions.
- Third-party analysis tools and software can be used with the logical partition.

See ***Section 10.2*** for details on how to view Source drives over the network using iSCSI.

7: Drive Encryption and Decryption

7.0 Drive Encryption/Decryption - Introduction

The Falcon-NEO can secure sensitive evidence data with whole disk drive encryption using the NIST recommended XTS-AES-256 cipher mode. Destination drives that are encrypted by the Falcon-NEO can be temporarily decrypted by using the Falcon-NEO or third-party software (VeraCrypt, TrueCrypt, or FreeOTFE).

In the ***System Settings*** screen, there is an ***Encryption*** tab used to configure the Falcon-NEO for encryption. There are up to 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*** page on the Falcon-NEO:

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

  - VCRYPT cipher mode can be decrypted using the Falcon-NEO or VeraCrypt.
  - TC-XTS cipher mode can be decrypted using the Falcon-NEO or TrueCrypt.
  - CBC or ECB cipher modes can be decrypted using the Falcon-NEO or FreeOTFE.

  The Falcon-NEO encrypts drives using AES-256 encryption regardless of what cipher mode is used. If TC-XTS is used, Falcon-NEO uses a TrueCrypt friendly format and **does not** use TrueCrypt to encrypt the drive. The encryption key is not stored on the Destination drive.

- **Cipher –** At this time, only the ***AES-256*** cipher is supported.
- **IV Generation –** Initialization Vector. Unavailable when VCRYPT or 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.

Remember the password used to encrypt the Destination drive! Logicube cannot retrieve or unlock the encrypted drive without the password.

7.1 Encrypting a Destination

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

7.1.1 Step-By-Step Instructions

1. Select ***System Settings*** from the types of operation on the left side.
2. Tap the ***Encryption*** 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.
7. Tap the ***Format Settings*** icon to change the Format settings to the following:
   a. Set ***Format*** to ***ON***.
   b. Select the desired ***File System*** (***EXT4***, ***NTFS***, ***exFAT***, or ***FAT32***).
   c. Set ***Encryption*** to ***ON***. When finished, tap the ***OK*** icon.

8. Tap the ***Start*** icon to start the wipe task. The Falcon-NEO will format the selected drive(s) with encryption.

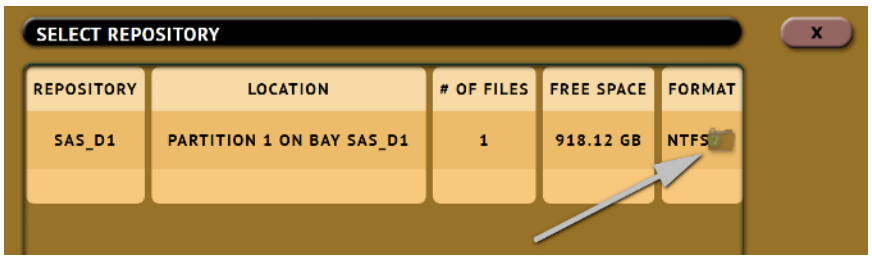
7.1.2 Using Previously Encrypted Destination Drives

If a previously encrypted Destination drive is going to be used and the Falcon-NEO 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.

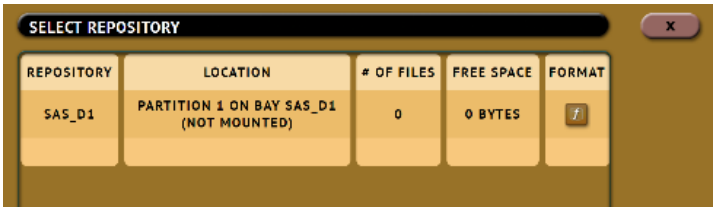
> If the same encryption settings are commonly used, the encryption settings and configuration can be saved as a profile, so they do not have to be entered manually all the time.

1. Make sure the previously encrypted Destination drive is not connected, then turn the Falcon-NEO on.
2. From the main menu, select ***System Settings*** from the types of operations on the left side.
3. Tap the ***Encryption*** 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. Go to Imaging and choose an imaging mode (Drive to File, File to File, Partition to File, or Net Traffic to File).
7. Choose a ***Source*** drive.
8. Adjust the ***Settings*** as needed.
9. Select the ***Destination***. Make sure the drive's encryption is detected and decrypted properly. The drive should look something like this:



Make sure the drive's encryption is detected and decrypted properly. If the Falcon-NEO did not decrypt the drive properly, it will show as ***(NOT MOUNTED)***:



If the drive is not decrypted properly, disconnect the drive from the Falcon-NEO, then double-check the encryption settings and repeated steps 2 through 9.

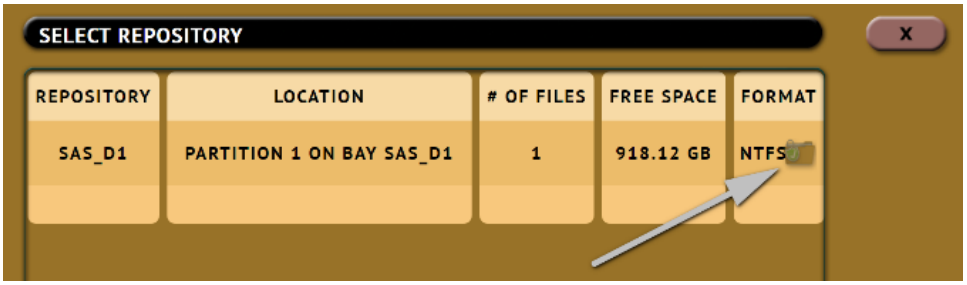
7.2 Decrypting a Falcon-NEO Encrypted Drive with a Falcon-NEO

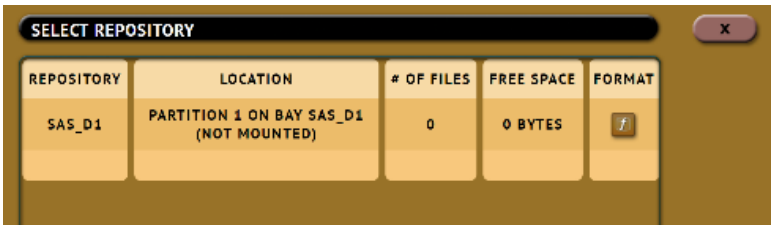
Falcon-NEO can decrypt a Destination drive encrypted by the Falcon-NEO. To decrypt the drive using a Falcon-NEO, follow these steps:

1. Make sure the previously encrypted Destination drive is not connected, then turn the Falcon-NEO on.
2. From the main menu, select ***System Settings*** from the types of operations on the left side.
3. Tap the ***Encryption*** 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.

> Although no imaging will be done, the next two steps should be followed to help ensure the Falcon-NEO is detecting and decrypting the Destination drive properly.

6. Go to ***Imaging*** and select the ***Drive to File*** mode.
7. Select the ***Destination***. Make sure the drive's encryption is detected and decrypted properly. The drive should look something like this:



> Make sure the drive's encryption is detected and decrypted properly. If the Falcon-NEO did not decrypt the drive properly, it will show as ***(NOT MOUNTED)***:
>
> 
>
>
> If the drive is not decrypted properly, disconnect the drive from the Falcon-NEO, then double-check the encryption settings and repeated steps 2 through 7.

8. Once the Falcon-NEO decrypts the destination drive, the drive can be accessed using SMB. See ***Section 10.1*** for details on how to view Source or Destination drives over the network using SMB.

7.3 Decrypting a Falcon-NEO Encrypted Drive without a Falcon-NEO

To mount and read an encrypted Destination drive in Windows, without using a Falcon-NEO, the following third-party utilities can be used depending on how the Destination drive was encrypted: ***VeraCrypt***, ***TrueCrypt*** or ***FreeOTFE***. Other utilities may work but are not supported or tested by Logicube.

> Logicube cannot offer support for third-party utilities. Please contact the software manufacturer for support, if needed.

7.3.1 Which Decryption Software to Use?

Choosing which decryption software to use (such as VeraCrypt, TrueCrypt or FreeOTFE) depends on how the Destination drive was encrypted.

- **VeraCrypt –** Use this software if the Destination drive was encrypted with the ***VCRYPT*** cipher mode.
- **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*** cipher mode.

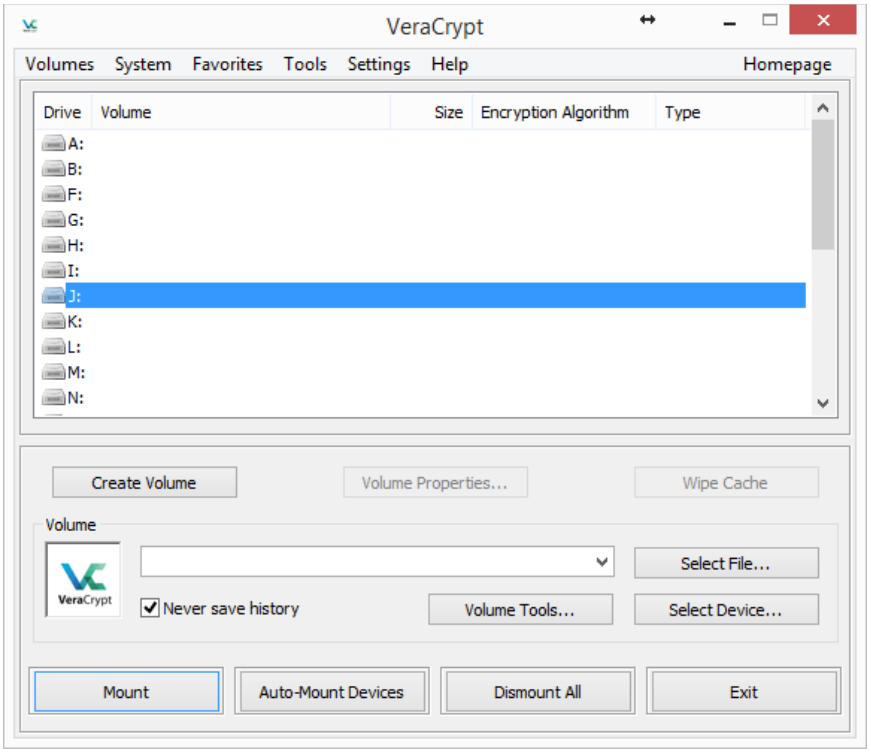
If the ***ECB*** cipher mode was used to encrypt the Destination drive, the Falcon-NEO must be used to decrypt the drive.

7.3.2 Decrypting Using VeraCrypt

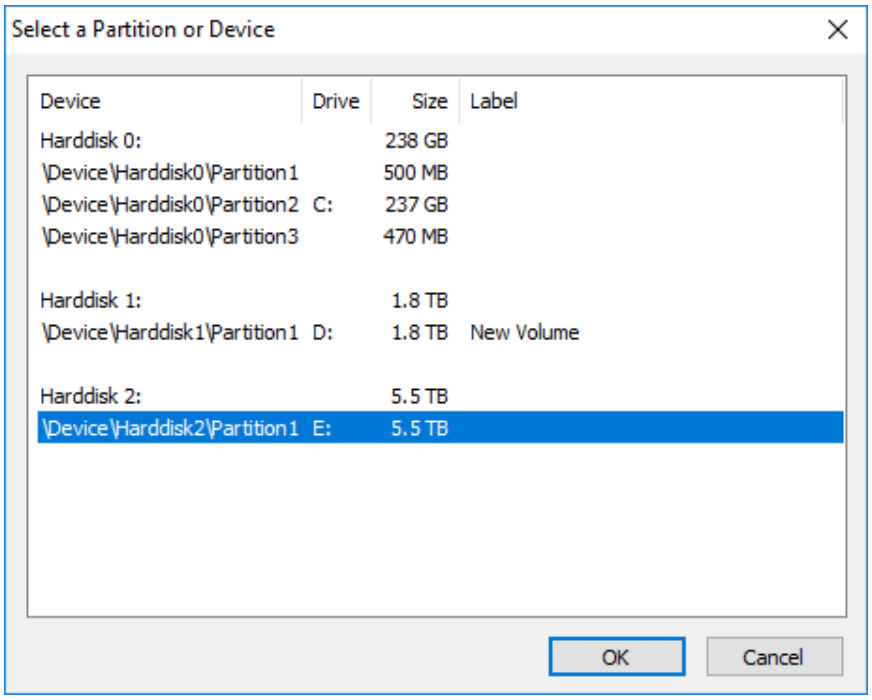
Requirements:

- VeraCrypt installed.
- A drive encrypted by the Falcon-NEO using the VCRYPT cipher mode connected to the computer with VeraCrypt.

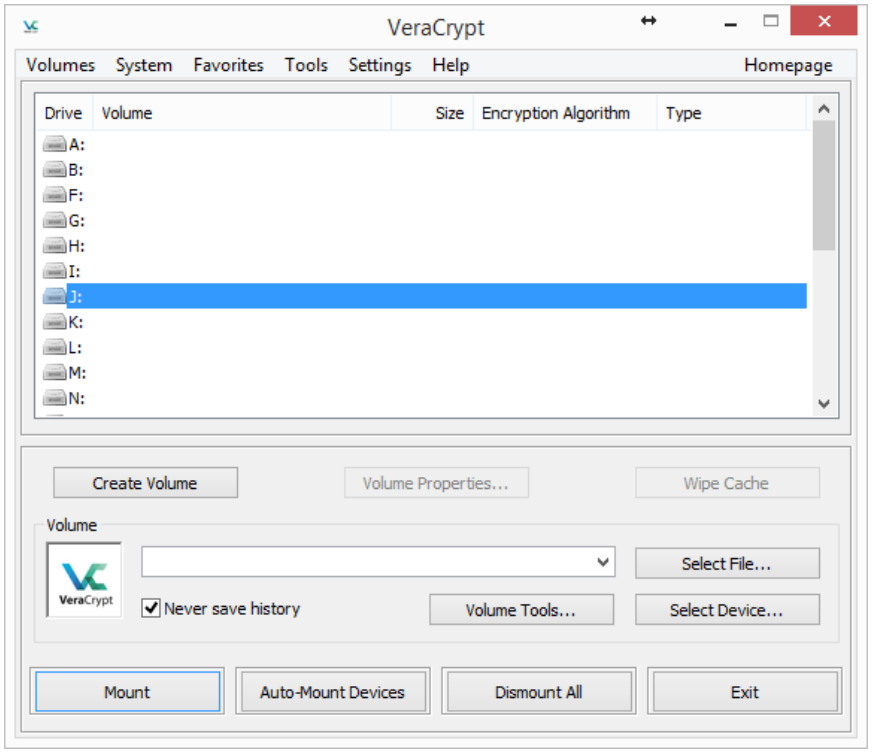
1. Once the drive is connected to the computer, Open VeraCrypt.



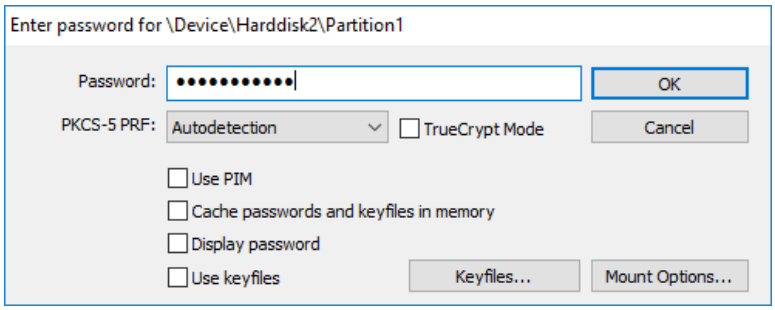
2. Click ***Select Device*** and choose the partition of the connected drive then click ***OK***.



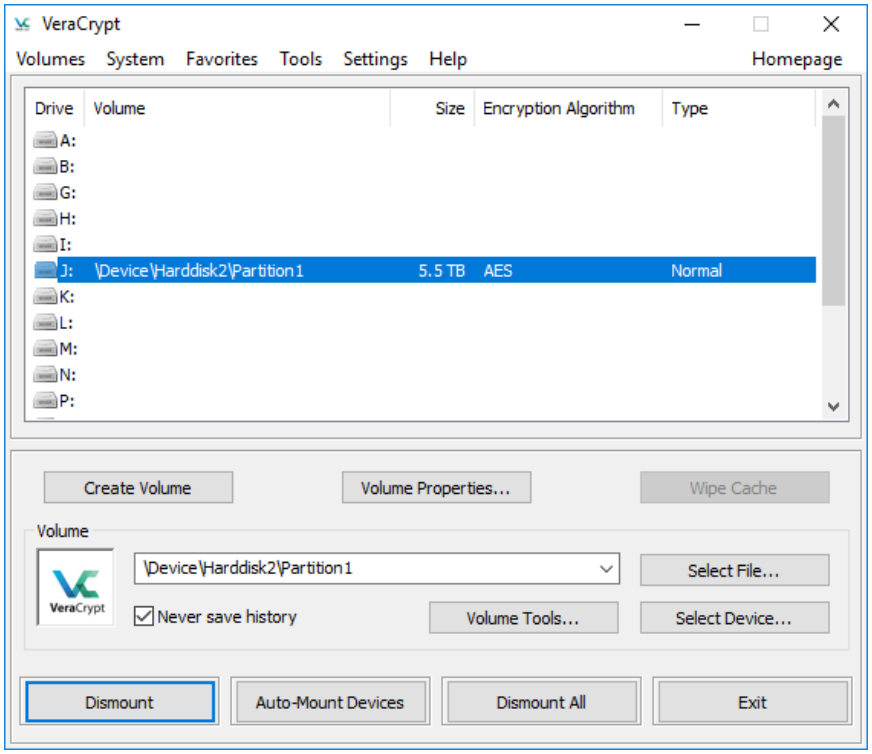
3. Click ***Mount***.



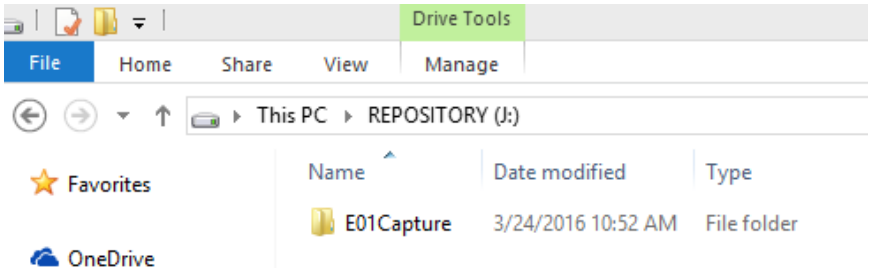
4. Type the encryption password in the ***Password*** field then click ***OK***.



5. The drive should now be mounted and assigned a drive letter.



6. The drive should now be accessible in Windows.



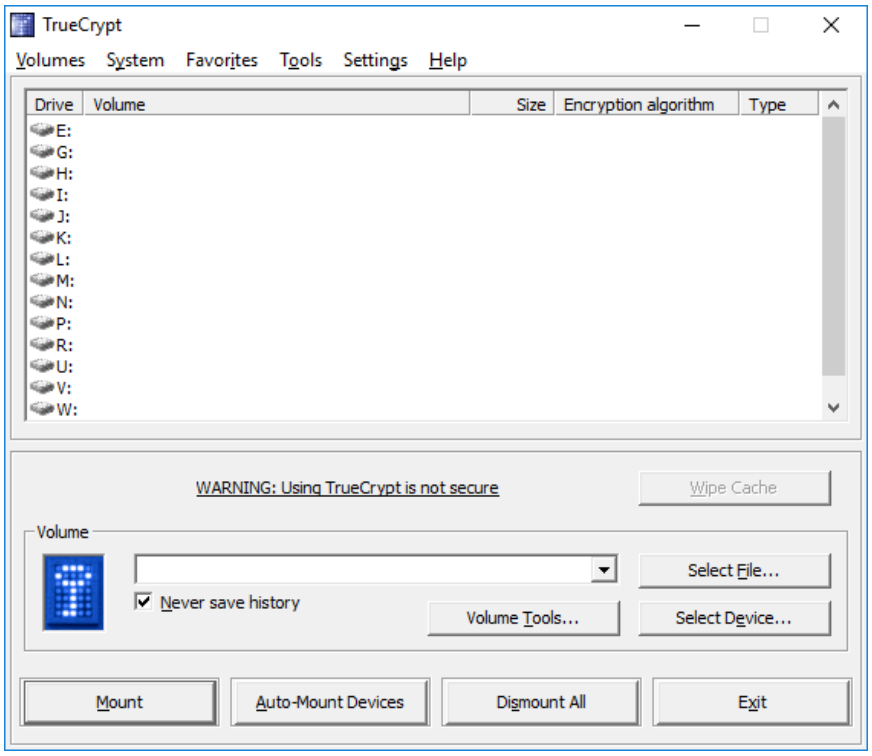
7.3.3 Decrypting Using TrueCrypt

Requirements:

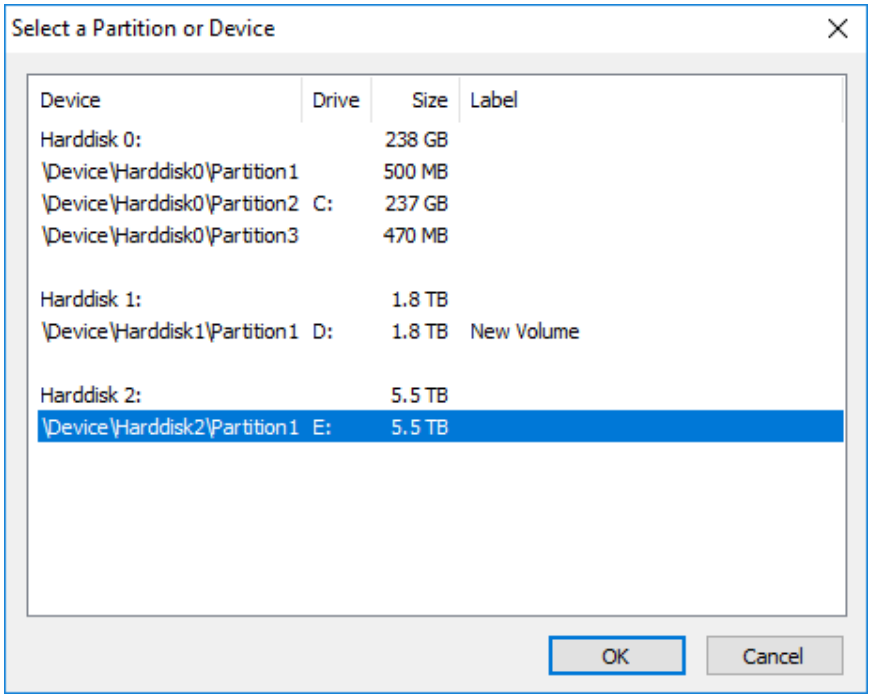
- TrueCrypt properly installed.

- A drive encrypted by the Falcon-NEO using the TC-XTS cipher mode connected to the computer with TrueCrypt.

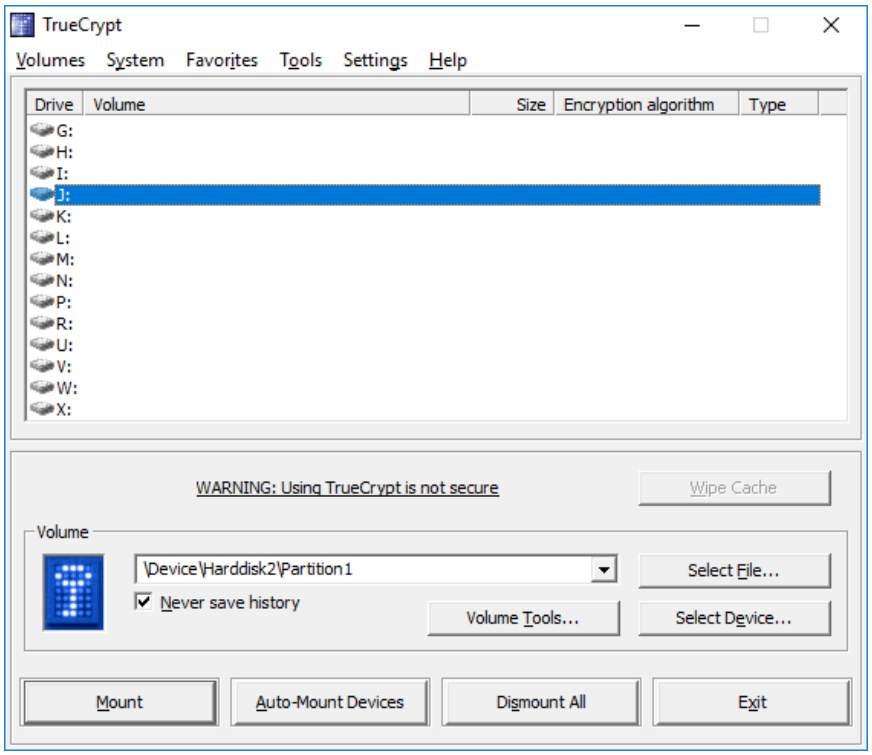
1. Once the drive is connected to the computer, open TrueCrypt.



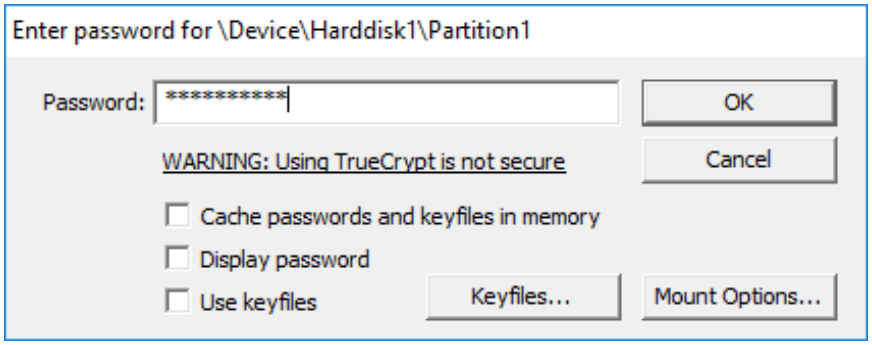
2. Click ***Select Device*** and choose the partition of the connected drive then click ***OK***.



3. Click ***Mount***.

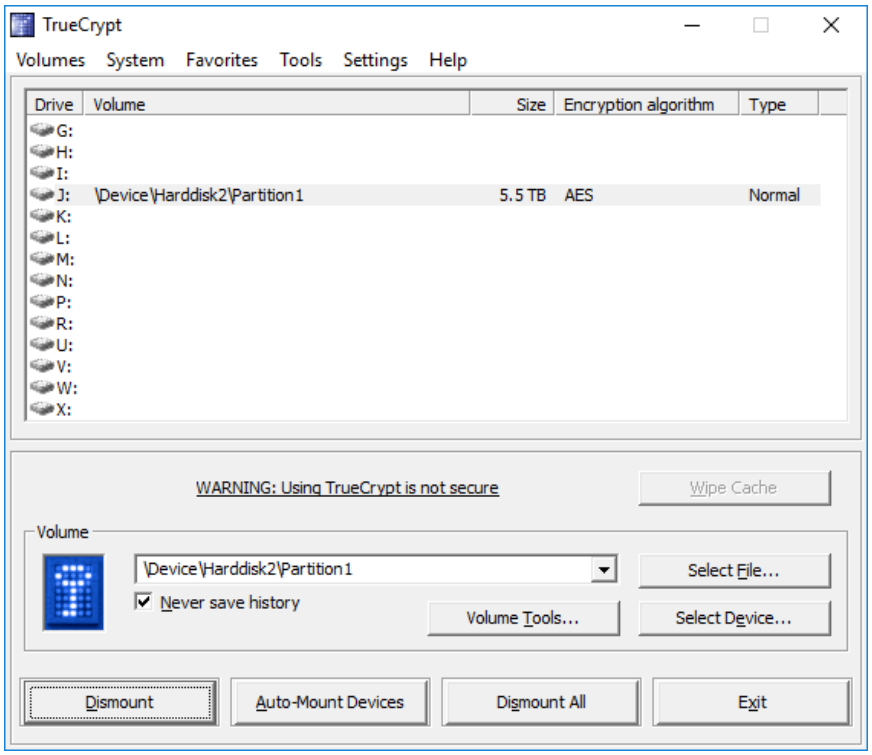


4. Type the encryption password in the ***Password*** field then click ***OK***.

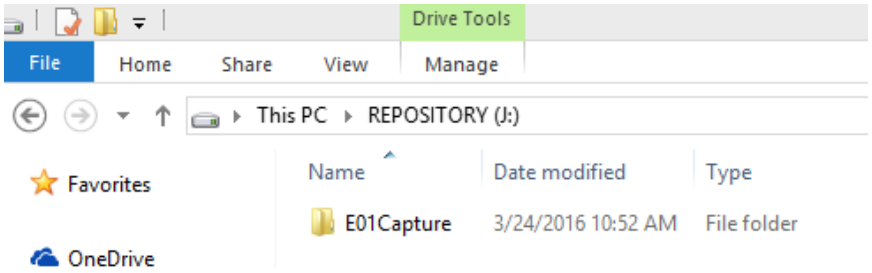


TrueCrypt has a setting to mount the drive as "read-only" which is a software write-block. This setting can be found by clicking ***Mount Options...*** If needed, a hardware write-block device may be used instead.

5. The drive should now be mounted and assigned a drive letter.



6. The drive should now be accessible in Windows.

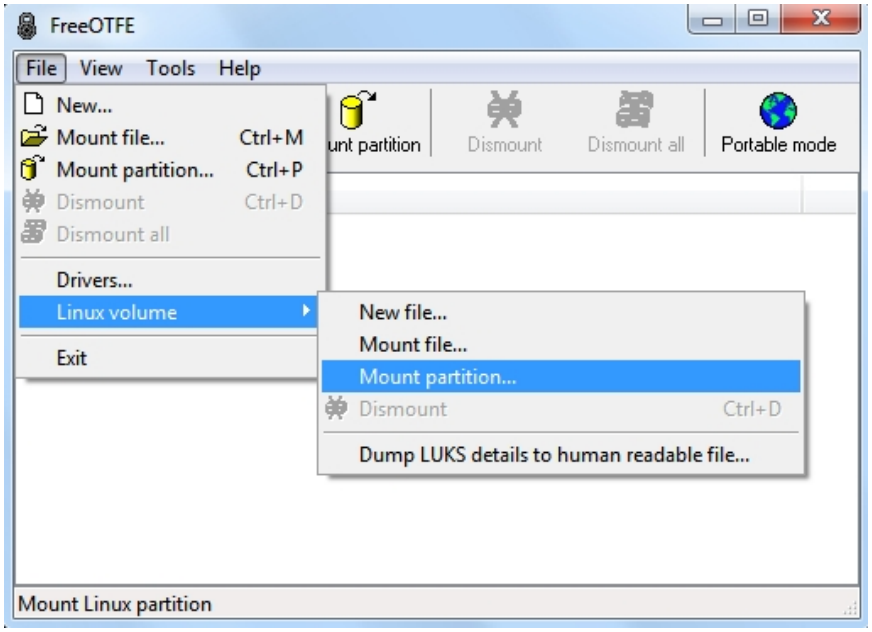


7.3.4 Decrypting using FreeOTFE

Requirements:

- FreeOTFE properly installed.
- A drive encrypted by the Falcon-NEO using the CBC cipher mode connected to the computer with FreeOTFE.

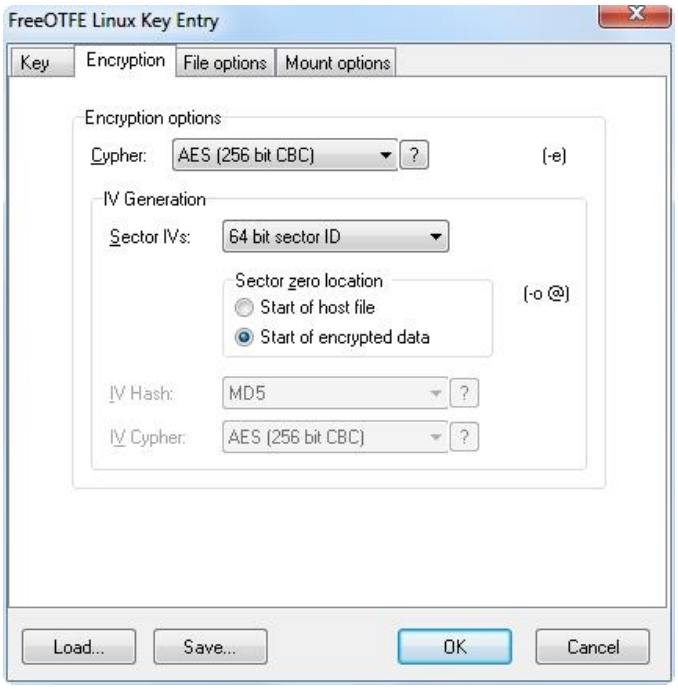
1. Open FreeOTFE. In the main window, click ***File*** then ***Linux volume*** then ***Mount partition...***



2. Select the encrypted disk to mount (in this example, it is Disk #1). 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.

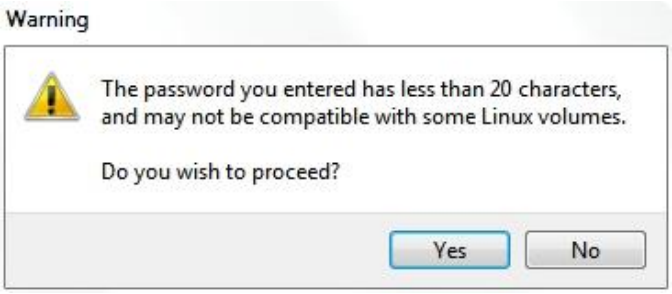
3. In the Key tab, enter the Key (password) and make sure the ***Hash*** is set to ***RIPEMD-160***.

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 Falcon-NEO. In this example, "plain64' was used. In the 'Sector zero location', choose ***Start of encrypted data***.

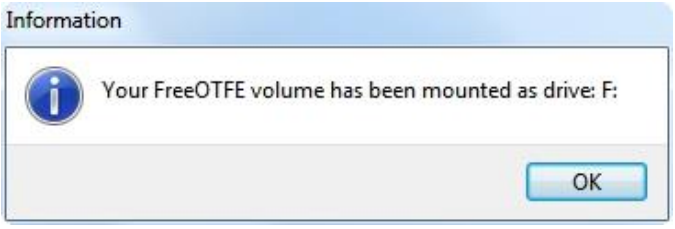


OPTIONAL: In the ***Mount options*** tab, the disk can also be mounted with write protection. To do so, make sure the ***Mount readonly*** option is checked. Windows may not mount the drive if this option is checked. If this is the case, use a write-protect device and uncheck the ***Mount readonly***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

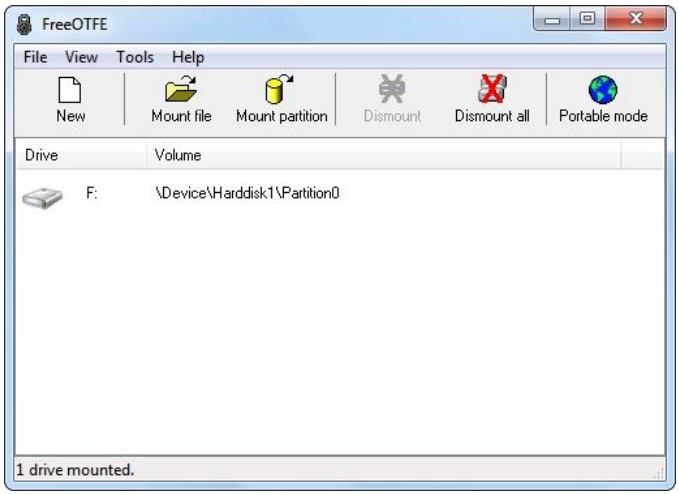
5. Click the ***OK*** button. The following warning screen may appear. Click the ***Yes*** button to continue.



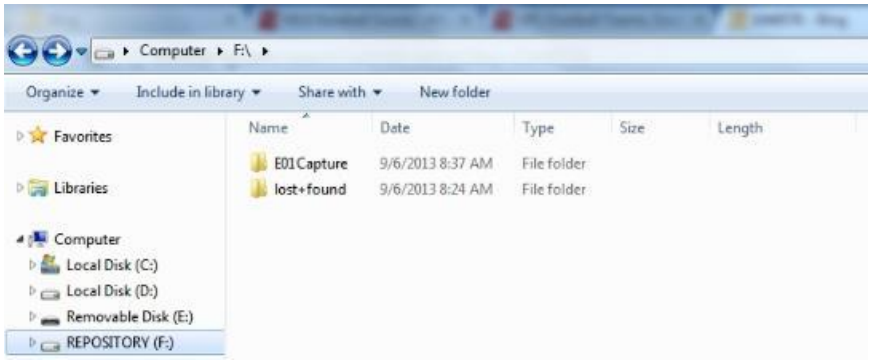
6. FreeOTFE will mount the drive and assign a drive letter.



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



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

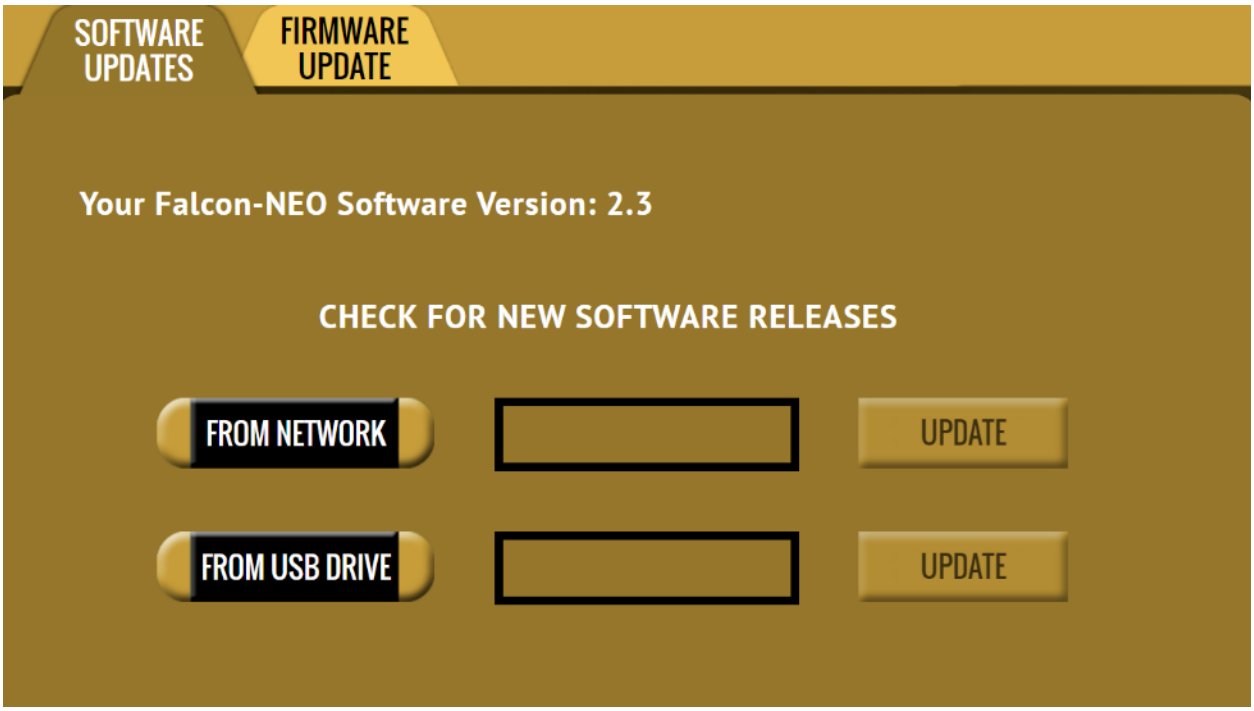


8: Updating/Loading/Re-loading Software

8.0 Updating/Loading/Re-loading Software – Introduction

The latest Falcon-NEO software, manual, and readme file (which contains the software release notes) can always be found on the Falcon-NEO support page at https://www.logicube.com/knowledge/forensic-falcon-neo.

The Falcon-NEO software release may contain both a software and firmware update. This chapter details how to update/reinstall the software and firmware.



8.1 Requirements

To perform the software update/reinstall, one of the following is required:

- The Falcon-NEO connected to a network with Internet access (for updating "FROM NETWORK"), or
- The Falcon-NEO with your own USB flash drive. The USB flash drive must be formatted FAT32 or NTFS (for updating "FROM USB DRIVE")

8.2 Updating/Loading/Re-loading Software Instructions

There are two methods of how to update the Falcon-NEO Ultimate software:

- **FROM NETWORK –** Over the Internet through a network connection
- **FROM USB DRIVE** – Through a software file download onto a USB drive flash.

The actual software installation will take about 2 to 3 minutes. If ***FROM NETWORK*** was chosen, the total time can exceed 5 to 10 minutes (or longer) depending on Internet speeds and Internet traffic.

The most up-to-date instructions on updating the software can be found on the Falcon-NEO's support page.

8.2.1 From Network (Over the Internet)

The software can be updated/re-installed by connecting the unit to a network with internet access.

It is recommended to disconnect all drives and drive adapters from the Falcon-NEO before the update/reinstall process.

1. Connect the Falcon-NEO to a network with Internet access and turn the Falcon-NEO on.
2. From the main menu on the Falcon-NEO, locate and tap the ***Software Updates*** icon on the left side.
3. Select ***From Network***. The Falcon-NEO will check for software on Logicube's server. After a few seconds, one of the following messages will appear:
    - ***NEWER VERSION AVAILABLE –*** This message will appear if there is a newer software version found. Tap the ***OK*** icon to continue.
    - ***UP TO DATE –*** This message will appear if the software version found is the same as the version currently installed. Tap the ***OK*** icon to continue.
    - ***HTTP://UPDATES.LOGICUBE.CCNEO/ FAILED: 500 CAN'T CONNECT TO UPDATES.LOGICUBE.COM:80 –*** This message will appear if the Falcon-NEO cannot connect to the update site. When this message appears, double-check that you have an Internet connection to the Falcon-NEO. For example, try a different network cable or network drop. If the message persists, try the following:
        i. Go to the ***About*** tab in the ***Statistics*** screen and check the ***N/W Interfaces*** to make sure the Falcon-NEO is connected to a network and has a valid ***IPAddress***, or
        ii. Make sure the network the Falcon-NEO is connected to has Internet access, or
        iii. Try using the "From USB DRIVE" option (see ***Section 8.2.2***).

4. Tap the ***Update*** icon to begin the update/reinstall. The Falcon-NEO should begin the update/reinstall process. Do not interrupt this process. It may take several minutes. Once completed, a screen will appear stating the update is complete and will prompt you to turn the unit off then back on.
5. Turn the Falcon-NEO off. Wait at least 5 seconds then turn the Falcon-NEO back on.
6. Verify the software version by going to the Software Updates screen then go to section ***8.3 Firmware Update*** to check if there is a firmware update available.

8.2.2 From USB Drive (Through a Software File Download)

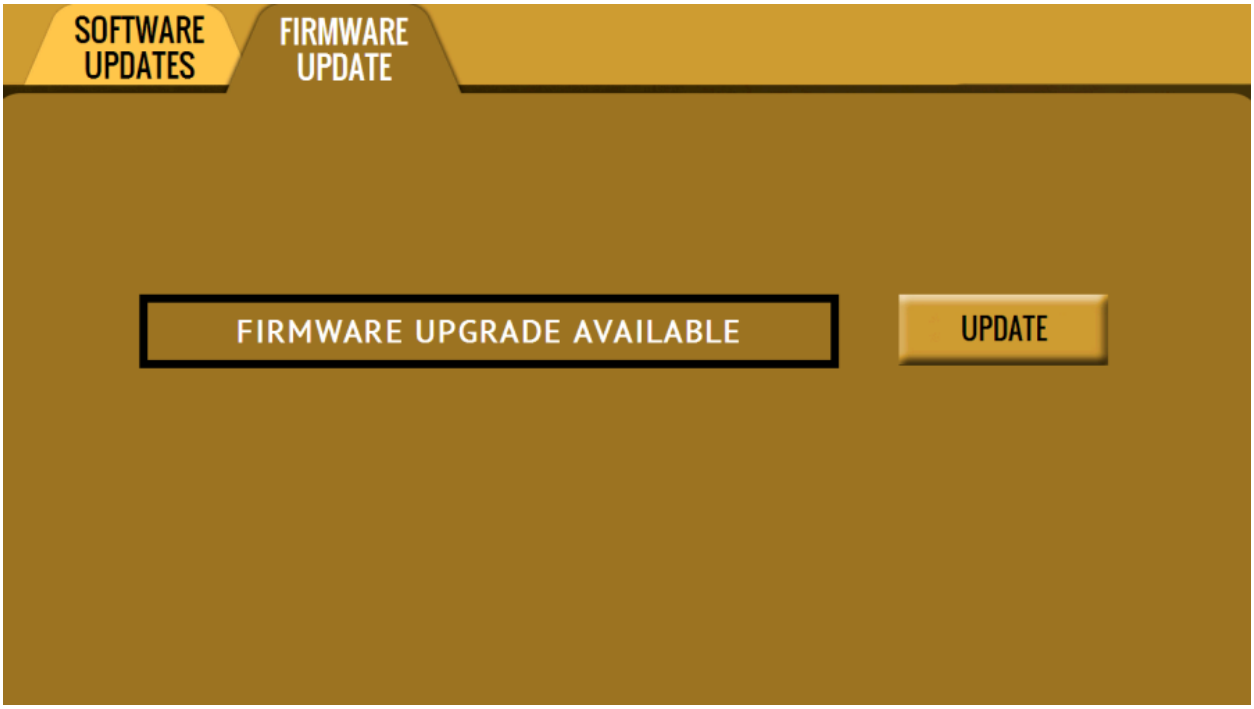
Aside from the network option, the latest software can also be downloaded from Logicube's website and be placed onto a USB flash drive to perform the software update/reinstall. It is recommended to use an empty USB flash drive.

> It is recommended to disconnect all drives and drive adapters from the Falcon-NEO before the update/reinstall process.

1. Using a computer, download the latest software from the Falcon-NEO product support page at https://www.logicube.com/knowledge/forensic-falcon-neo.
2. Extract the contents of the downloaded zip file to the root of the USB flash drive.
3. Turn the Falcon-NEO on. When the main software screen appears, connect the USB flash drive (that has the extracted software from step 2) to the USB_S1 port (the USB port on the left side).
4. From the main menu on the Falcon-NEO, locate and tap the ***Software Updates*** icon on the left side.
5. Select ***From USB Drive***. The Falcon-NEO will check for the version of the software on the USB drive. After a few seconds, one of the following messages should appear:
   - ***SOFTWARE FOUND –*** A software version is found on the USB flash drive. Tap the ***OK*** icon to continue.
   - ***UPDATES NOT FOUND! –*** The Falcon-NEO did not find any software on the USB flash drive or could not detect the USB flash drive. If this message is seen, try the following:
     i. Make sure the correct software was downloaded and the files were extracted to the root of the USB flash drive, or
     ii. Format and use a different USB flash drive, or
     iii. Try using the "From Network" option (see ***Section 8.2.1***)
6. Tap the ***Update*** icon to begin the update/reinstall. The Falcon-NEO should begin the update/reinstall process. Do not interrupt this process. It may take several minutes. Once completed, a screen will appear stating the update is complete and will prompt you to turn the unit off then back on.
7. Turn the Falcon-NEO off. Wait at least 5 seconds then turn the Falcon-NEO back on.

8. Verify the software version by going to the Software Updates screen then go to section ***8.3 Firmware Update*** to check if there is a firmware update available.

8.3 Firmware Loading Instructions



Falcon-NEO software releases may contain a firmware update. This section provides instructions on how to check if a firmware update is required, and how to perform the firmware update.

1. After the software is updated/reinstalled on the Falcon-NEO, locate and tap the ***Software Updates*** icon on the left side.
2. Tap the "Firmware Update" tab. One of the two screens will appear:
   - ***FIRMWARE UPGRADE AVAILABLE –*** Tap the ***Update*** icon. A message will appear: "FIRMWARE UPDATE COULD TAKE UP TO A FEW MINUTES TO COMPLETE; PLEASE DO NOT INTERRUPT POWER DURING THIS TIME. ON COMPLETION THE UNIT WILL AUTO-RESTART AND CONFIRM THE UPDATE." Tap the ***OK*** icon to start the firmware update process.

     When the ***OK*** icon is tapped, the screen may appear to do nothing. Do not keep tapping the ***OK*** icon. The firmware update typically takes no more than 60-120 seconds. When the firmware update finishes, the Falcon-NEO will reboot automatically.
   - ***FIRMWARE UPGRADE NOT AVAILABLE –*** This message will appear if the device does not require a firmware update. No further action is necessary if this message appears.

9: Remote Operation

9.0 Remote Operation - Introduction

The Falcon-NEO comes with two 10GbE network connections in the back of the unit. Connecting the Falcon-NEO to a network allows remote access to the Falcon-NEO from any computer within the same network.

The Falcon-NEO is configured for DHCP by default. See ***Section 5.11.1.1*** for instructions on how to configure the Falcon-NEO with a Static IP address.

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

- Web interface – A graphical interface using an Internet browser where the screens are shown exactly the way they appear on the Falcon-NEO
- 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 and Mozilla Firefox are recommended. Other browsers may not display the Graphical User Interface (GUI) properly.

9.1 Web Interface

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

On some browsers or Operating Systems, the Falcon-NEO will need to be accessed by browsing to ***http://falcon-XXXXXX.local***.

The Falcon-NEO can be controlled by clicking on the icons appearing on the browser window.

9.2 Command Line Interface (CLI)

The Falcon-NEO 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 from a connected computer (over a network). There are many Telnet and SSH clients available from different software companies. Microsoft Windows also has a built-in Telnet client that can be used.

- This section is for advanced users with knowledge of networking and command-line functions.
- Windows has a built-in Telnet client but may not be 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.
- For assistance on the installation of any SSH or Telnet software (including Microsoft's Telnet client) please check with your IT administrator.

9.2.1 Connecting via Telnet

The steps below outline how to use the Windows Telnet client. Other Telnet clients would have different steps on how to connect.

1. Connect the Falcon-NEO to the network by attaching a network cable to the RJ45 connector in the back of the Falcon-NEO.
2. Turn the Falcon-NEO on and allow it to boot up completely.
3. Open the Telnet client.
4. Type ***open*** followed by the IP address or name of the Falcon-NEO. For example ***open 192.168.1.100*** or ***open falcon-XXXXXX***
   where XXXXXX is the 6-digit serial number of the Falcon-NEO, then press Enter. The Falcon-NEO login screen should appear.
5. Log in with the username "***it***" (without the quotes) and the password "***it***" (without the quotes). A command prompt should appear on the Telnet window.

Use the ***it*** login in step 5. It is not recommended to use the ***logicube*** account login without consulting with Logicube Technical Support prior to use.

The Falcon-NEO can now be configured or managed via the command-line interface.

9.2.2 Connecting via SSH

Connecting to the Falcon-NEO 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. Using one of the RJ45 connectors in the back of the Falcon-NEO, connect the Falcon-NEO to a network.
2. Turn the Falcon-NEO on and allow it to boot up completely.
3. Open the SSH client and select an SSH connection.

4. Connect to the Falcon-NEO either by IP address or by hostname. The name of the Falcon-NEO will be ***falcon-XXXXXX*** where XXXXXX is the 6-digit serial number of the Falcon-NEO).

> On some Operating Systems, the Falcon-NEO will need to be accessed by opening falcon-XXXXXX.local.

5. Log in with the username "***it***" (without the quotes) and the password "***it***" (without the quotes). A command prompt should appear in the SSH window.

> Use the ***it*** login in step 5. It is not recommended to use the ***logicube*** account login without consulting with Logicube Technical Support prior to use.

The Falcon-NEO can now be configured or managed via the command-line interface.

9.3 Zero Configuration Networking (Zeroconf)

The Falcon-NEO 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 Falcon-NEO is connected (using a network cable) directly to a Windows-based computer that is DHCP enabled, both the Falcon-NEO and the Windows-based computer will automatically configure themselves to be seen by each other using TCP/IP with a 169.254.x.x IP address configuration.

9.4 Copying Profiles from One Falcon-NEO to Another

Profiles can be copied from one Falcon-Neo to another using the Command Line Interface (CLI). The Falcon-NEO units must be on the same network and all Profiles will be copied. Instead of configuring each Falcon-Neo one at a time, all Falcon-Neo units can have the same profiles with a few simple commands.

9.4.1 Step-By-Step – Copying Profiles

Once the profiles are configured and saved onto a Falcon-NEO:

1. Connect the Falcon-NEO with the saved profiles and any additional Falcon-NEO units to a network.
2. Using Telnet or SSH, connect to the Falcon-NEO that has the profiles saved (See ***Section 9.2.1*** and ***Section 9.2.2*** for more information on connecting using Telnet or SSH).
3. Once connected through the CLI, log in with the following credentials:

   Username: ***it***

   Password: ***it***
4. From the main prompt, type ***command***, then press the Enter key.
5. Type ***config***, then press the Enter key.

6. Type ***db list***, then press the Enter key. This will show all the profiles on this Falcon-NEO unit. Make sure that these are the profiles that need to be copied to the other Falcon-NEO units.
7. Type ***db push xxx.xxx.xxx.xxx*** where xxx is the IP address of the Falcon-NEO that the profiles will be copied to, then press the Enter key (The IP address can be seen by going to the ***About*** tab in the ***Statistics*** screen). The profiles on the first Falcon-NEO unit will be copied to the other Falcon-NEO unit. This may take a few minutes depending on network speeds and the number of profiles to copy.

   While the profiles are being copied, the following output will show on the Telnet or SSH screen:

   [*] Creating DB archive...
   [*] Pushing DB archive to xxx.xxx.xxx.xxx...
   [*] Unpacking DB archive on xxx.xxx.xxx.xxx...
   [*] Cleaning up ...

   When the process is finished, the CLI prompt will re-appear. The Falcon-NEO unit where the profiles were copied to will refresh its screen.

8. The profiles should now be copied to the other Falcon-NEO unit. Repeat step 7 to copy the profiles to other Falcon-NEO units.

10: Viewing Source and Destination Drives over a Network

10.0 Viewing Drives Over a Network – Overview

The contents of drives connected to any Source or Destination position on the Falcon-NEO can be viewed over a network.

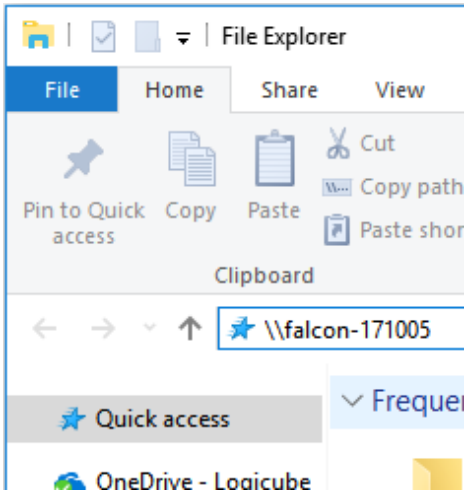
> Contents of Source and Destination drives viewed over a network are write-protected.
>
> Only Destination drives formatted by the Falcon-NEO can be seen over a network.

10.1 Viewing Source or Destination Drives Over the Network Using SMB

Contents of a Source or Destination drive can be viewed over a network using built-in file managers/viewers like File Explorer.

10.1.1 Step-By-Step – Viewing Source or Destination Drives

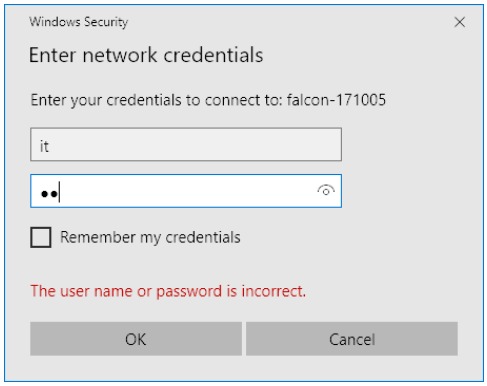
1. Connect the Falcon-NEO directly to a network or directly to a computer (using a network cable).
2. On the computer (on the same network, or directly connected to the Falcon-NEO), open File Explorer and browse the Falcon-NEO's IP address or the hostname of the Falcon-NEO with its serial number. Both the IP address and serial number can be found by going to the ***Statistics*** screen on the Falcon-NEO. For example, browse to ***\\192.168.1.100*** or ***\\falcon-XXXXXX*** where XXXXXX is the 6-digit serial number of the Falcon-NEO.



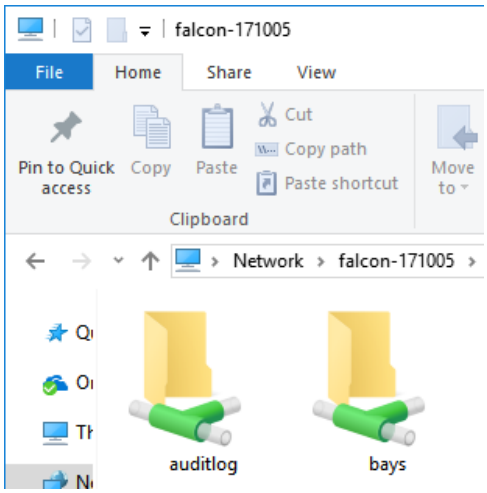
3. A window may appear asking you to enter a password to connect to the Falcon-NEO. Enter the following information:

   User name: ***it***

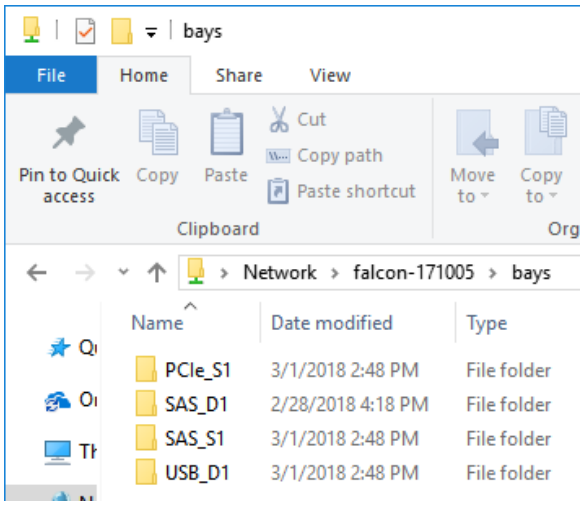
   Password: ***it***



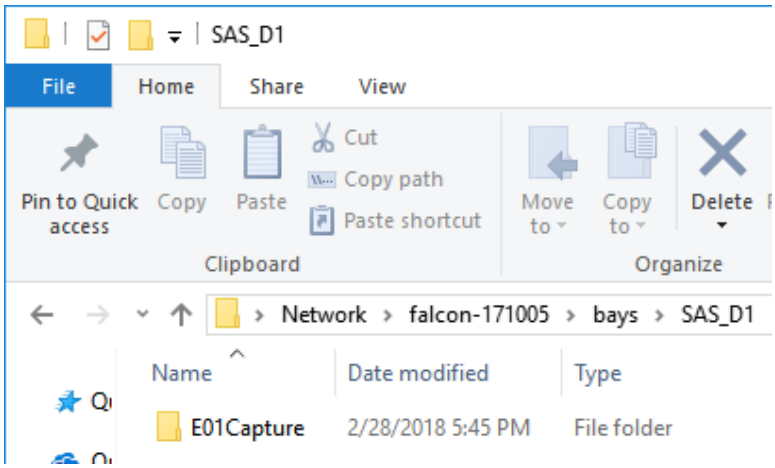
4. A folder called ***bays*** will be shown in Windows Explorer.



5. Go into the ***bays*** folder and select the connected Destination drive. For example, ***SAS_D1***.



6. The contents of the drive will be shown.



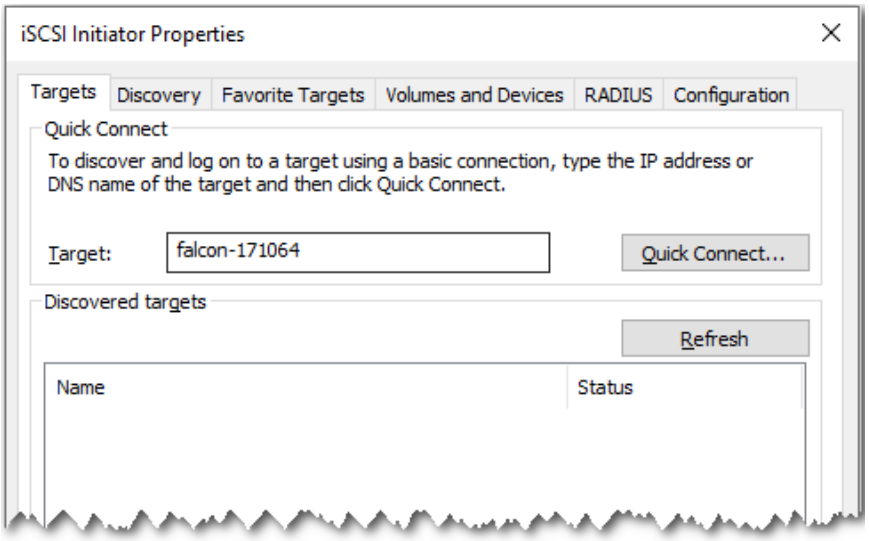
10.2 Viewing Source Drives Over the Network Using iSCSI

An iSCSI initiator must be configured to view the contents of Source drives over a network. Although there are many iSCSI initiators available, these next sections will discuss configuring Microsoft's iSCSI initiator in Windows.

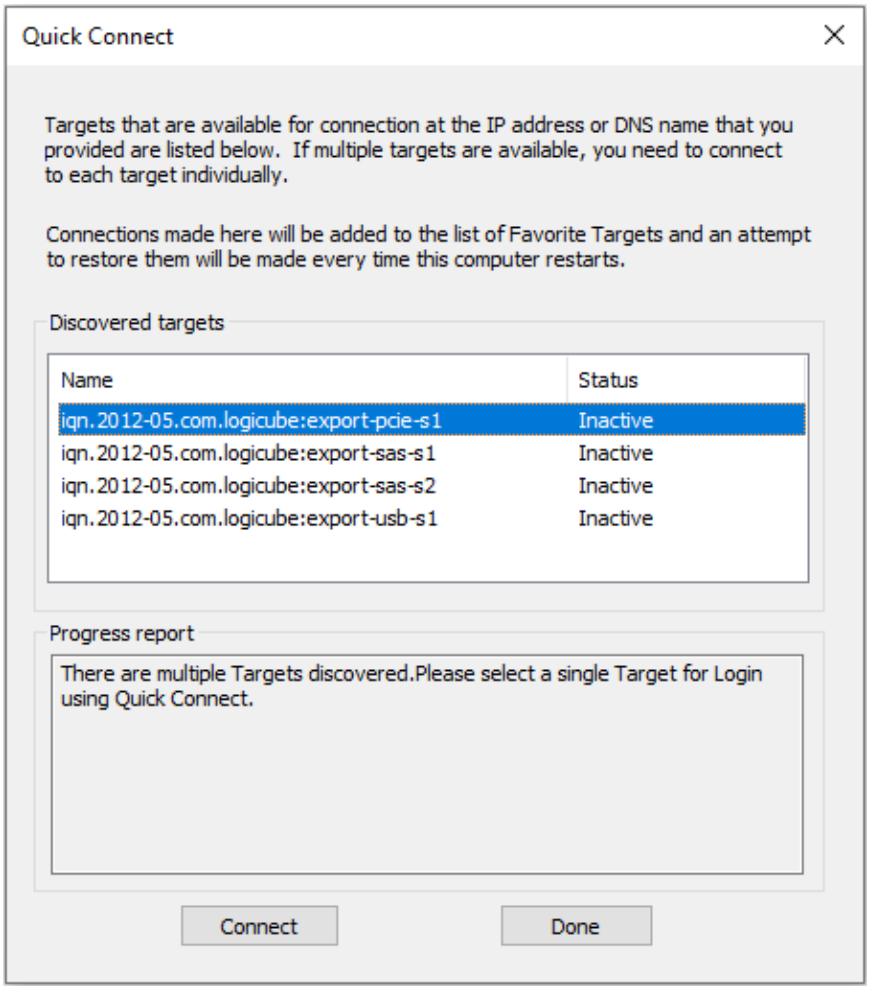
> Using an iSCSI initiator may require additional assistance from your IT administrator. The default credentials when connecting through iSCSI are:
>
> Username: iscsi
>
> Password: logicube@19755

10.2.1 Configuring the iSCSI Initiator

1. Open the iSCSI initiator. In the ***Target*** tab, enter the Falcon-NEO's hostname or IP address in the ***Target*** field. Click the ***Quick Connect*** button to continue.



2. The Quick Connect window will appear and any drives connected to the Source ports of the Falcon-NEO will appear on the list of discovered targets. Highlight the drive to view, then click ***Connect***.



The selected drive status will change to ***Connected***. Repeat step 2 for all other drives to be viewed. Click ***Done*** when finished.

If only one drive is connected to the Falcon-NEO, the iSCSI initiator will automatically connect the drive, and step 2 is not necessary.

3. Windows will attempt to mount the drive. If it contains a file system recognized by Windows, it should automatically assign a drive letter for each recognized partition and the contents can be viewed in Windows. This process may take several minutes depending on several factors including drive size, computer specifications, and network speeds.

11: Net Traffic Imaging

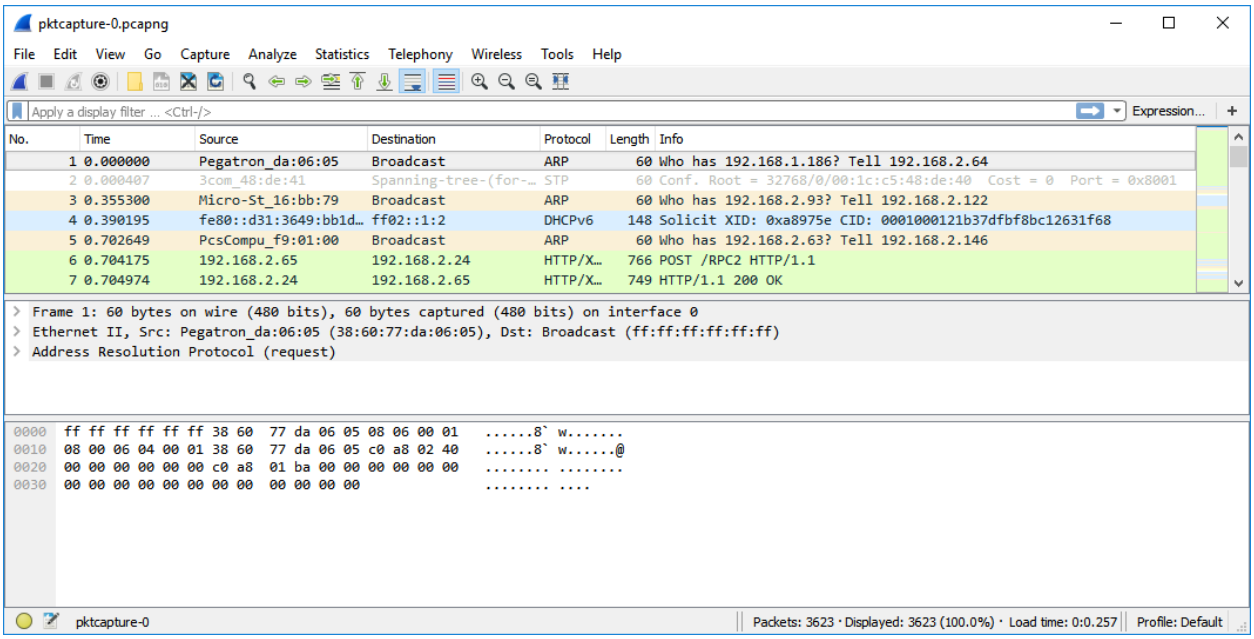
11.0 Net Traffic Introduction

The Falcon-Neo can capture network traffic data using the Net Traffic to File imaging mode. Network traffic that can be captured can include local network activity, internet activity, and VOIP activity. The data is saved and stored to a *.pcanpg file format.

Third-party software is required to view and analyze the contents of the pcanpg file. An example of software that can open and view pcanpg files is Wireshark.

> Advanced networking knowledge is required for the setup of capturing network traffic and data analysis.

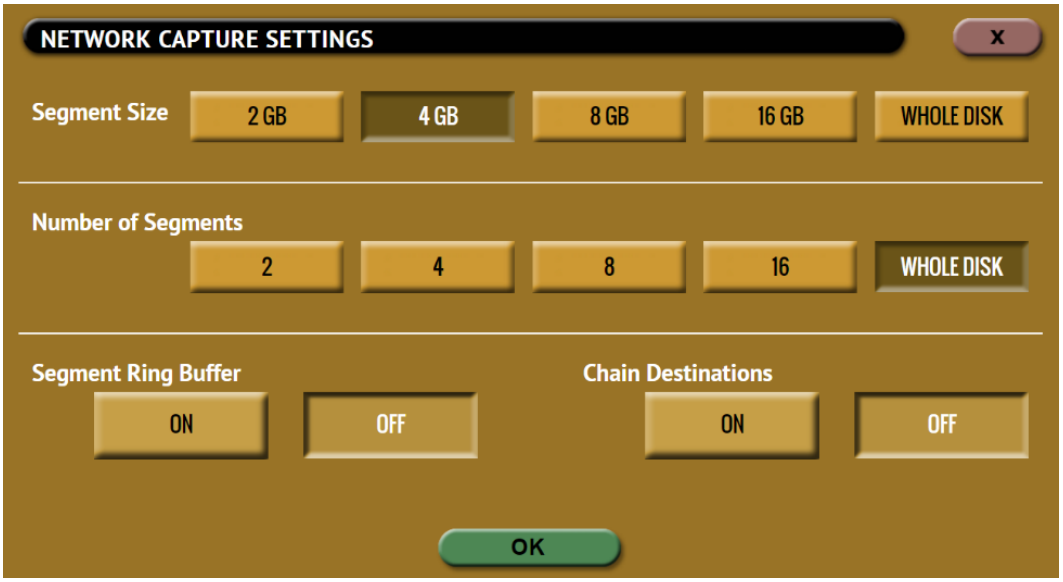
Below is an example of a pcapng file created by the Falcon-NEO, viewed in Wireshark.



11.1 Net Traffic Settings

Net Traffic to File has the following settings:

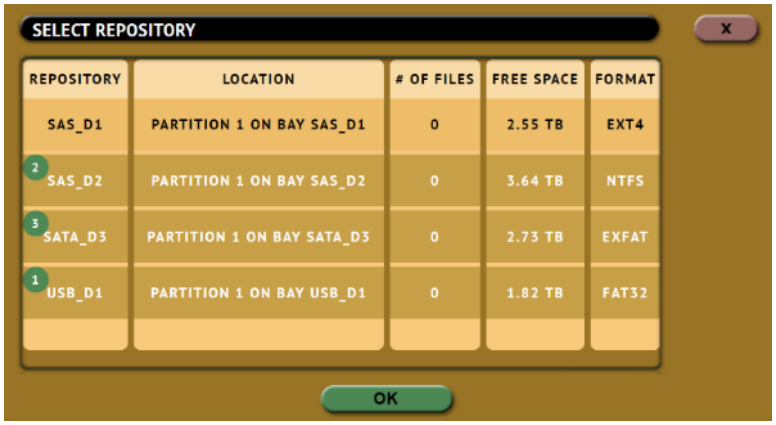
- Segment Size
- Number of Segments
- Segment Ring Buffer



- ***Segment Size –*** Allows the user to set the size of the captured segment (pcapng file). The options available are 2 GB, 4 GB, 8 GB, 16 GB, and Whole Disk.
- ***Number of Segments –*** Allows the user to select how many segment files to create. For example, if the Segment Size is set to 4 GB and the Number of Segments is set to 2, two segment files will be created. The options available are 2, 4, 8, 16, and Whole Disk.
- ***Segment Ring Buffer –*** Determines what the Falcon-NEO will do when it reaches the total number of segments on all selected repositories (Destination drives).
    - ***ON –*** When this is set to ON, the Falcon-NEO will continuously capture network traffic until the task is aborted. For example, if the ***Number of Segments*** is set to 2 and the ***Segment Ring Buffer*** is set to ON after the 2nd segment is finished, it will delete the 1st segment, then continue capturing network traffic, and create a new first segment file. If more than one repository is selected, it will keep cycling through both repositories, overwriting the oldest segment until the task is aborted.
    - ***OFF –*** When this is set to OFF, once the Falcon-NEO reaches the number of segments set and the last repository is filled, it will stop the task.
    - ***Chain Destinations –*** Allows the user to span the Net Traffic to File images over two or more repositories (such as Destination drives) continuously. When this is set to YES, all selected Destination drives will be used in the order they were selected. When the drive on the first repository is full, it will continue with the next selected repository.

> To enable Chain Destinations, Ring Buffer must be set to OFF.
>
> Drives must be formatted (by the Falcon-NEO) before starting the Net Traffic to File Imaging task.

    - After the first repository is full, the Destination drive on that repository can be swapped with a new Destination drive.
    - Replacing full repositories with a new Destination drive allows the Falcon-NEO to continuously capture Net Traffic until all the repositories are full. When all repositories are full, the task will finish showing a status of completed.



11.2 Net Traffic Imaging Notes

- Depending on the settings chosen, the ***Net Traffic to File*** task may finish and stop on its own. The ***Number of Segments*** determines how many segment files (how many pcapng files) will be written. When the ***Ring Buffer*** setting is set to ***ON***, the Falcon-NEO will complete the ***Number of Segments*** set, then delete the first segment and continue capturing network traffic. When ***Ring Buffer*** is set to ***ON***, the user will continue to capture network traffic until the task is aborted by the user.
- Capturing network traffic is dependent on how each network is setup. By simply connecting the Falcon-NEO to a network, the Falcon-NEO could capture all traffic forwarded by the Ethernet switch to the given port. Capturing network traffic from a specific IP address requires advanced networking knowledge. For example, a managed switch with port mirroring can be used to mirror a specific port so the Falcon-NEO can capture the network traffic coming from that single port.

> To find out if your network switch supports port mirroring, and for support on how to setup port mirroring, please contact the manufacturer of your specific switch.

- The Falcon-NEO listens for network traffic and does not actively scan or send any network requests.
- When performing a Net Traffic to File imaging task, it is highly recommended not to use the network port used as the Source (LAN1 or LAN2) for any other imaging task.

12: USB Boot Client

12.0 USB Boot Client Introduction

A USB Boot Client (bootable USB flash drive) is available. The USB Boot Client allows the imaging of a Source drive from a computer on the same network without booting the native Operating System on the computer. The drive from the computer can then be imaged without having to remove the drive from the computer.

12.1 Requirements

To create the USB Boot Client, the following are required:

- Your own 1 GB or larger capacity USB flash drive
- A computer with Microsoft Windows

To use the USB Boot Client with the Falcon-NEO, the following are required:

- The Falcon-NEO connected to a network (or directly to the computer to be imaged)
- The computer to be imaged with a wired connection to the same network (or directly to the Falcon-NEO)

12.2 Creating the USB Boot Client

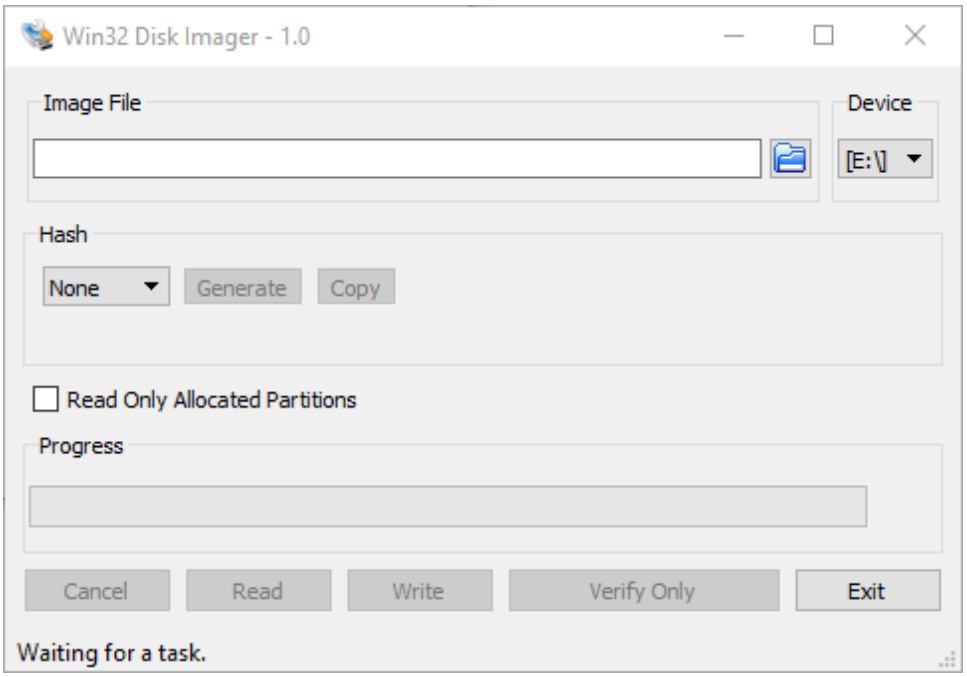
Here are the steps to create the USB Boot Client with the software necessary to be bootable, and when used to boot a computer, it will allow the Falcon-NEO to use the computer's drive as a Source drive.

For steps 1 and 2 of this section, please use Chrome or Firefox to download the files. Internet Explorer and Edge might not download *.img files properly.

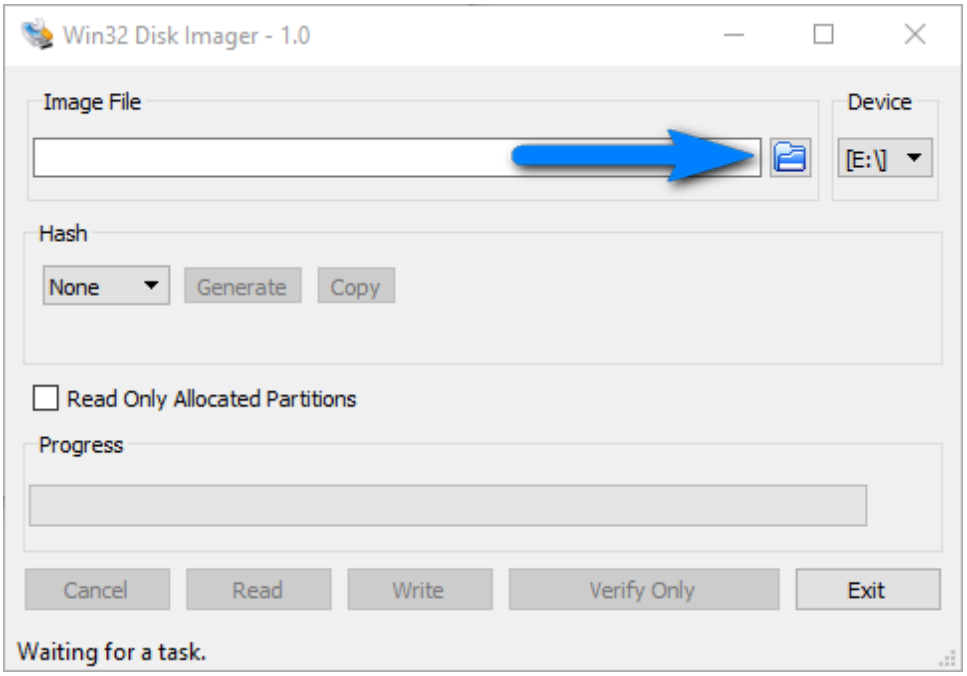
1. Using an Internet browser, browse to http://updates.logicube.com/iscsi/. Look for the following two files:
    - Win32DiskImager-1.0.0-binary.zip
    - The USB Boot Client image file – A file with a *.img file extension
2. Download both files. If the image file will not download, right-click on the link and use the 'Save Target As…' or 'Save Link As' option and make sure it is saved with the *.img file extension.
3. Extract all the files within the win32diskimager-v1.0.0-binary.zip file to a folder or directory of your choosing.
4. Connect your USB flash drive that is at least 1 GB in capacity to the computer where the software was downloaded. It is recommended that all other USB drives are unplugged.

The contents of the USB flash drive will be overwritten. If there is data on the USB flash drive that should not be deleted, back up the contents of the USB flash drive or use another USB flash drive for this procedure.

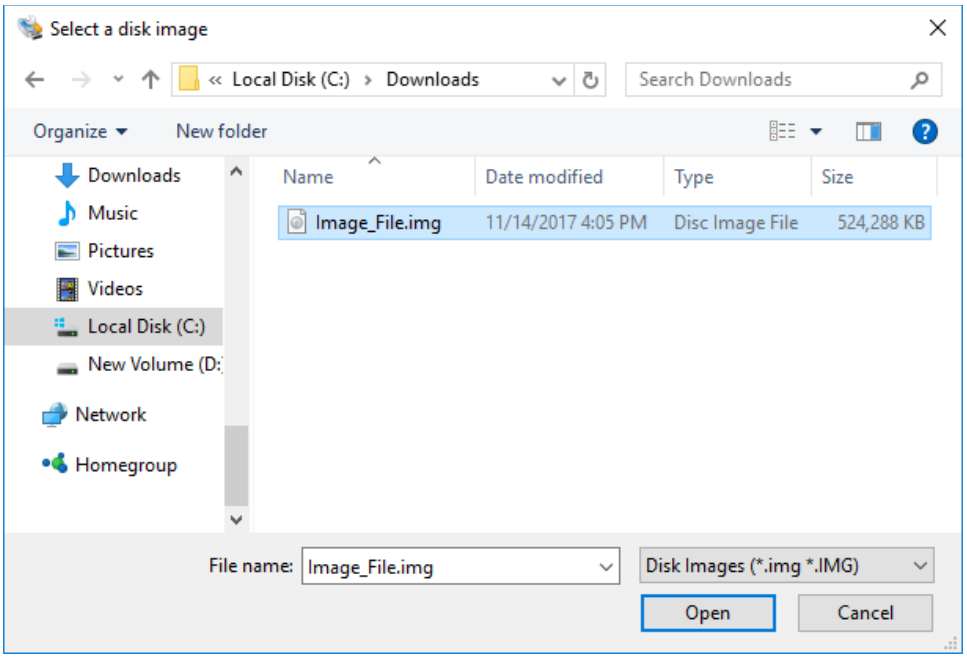
5. In the win32diskimager-v1.0.0-binary folder where the files were extracted to, run the file ***Win32DiskImager.exe***. The Win32 Disk Imager window will appear.



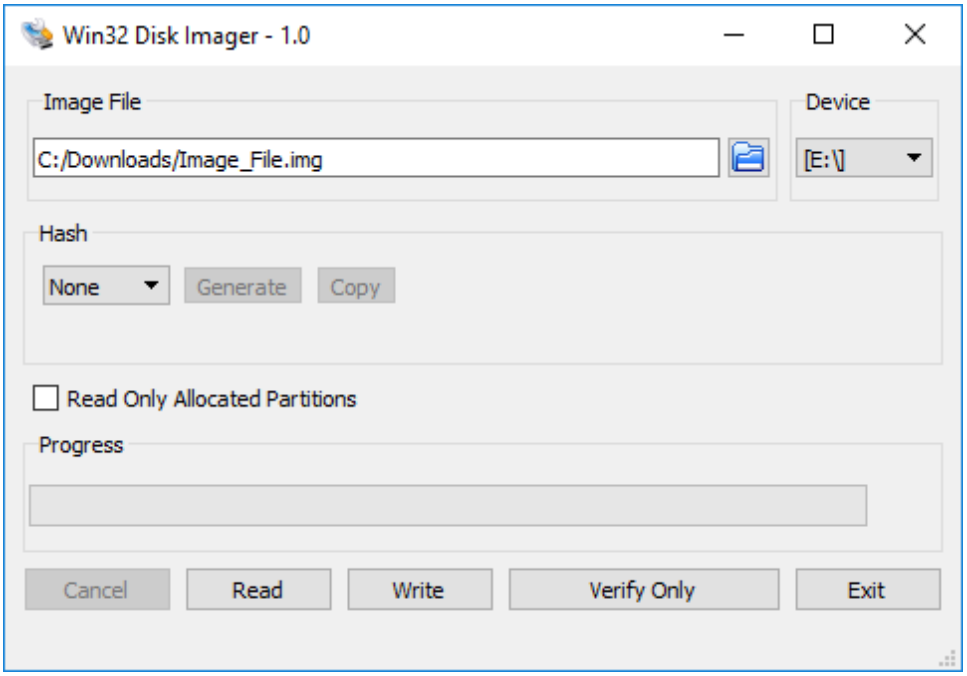
6. Click the folder icon to select a disk image.



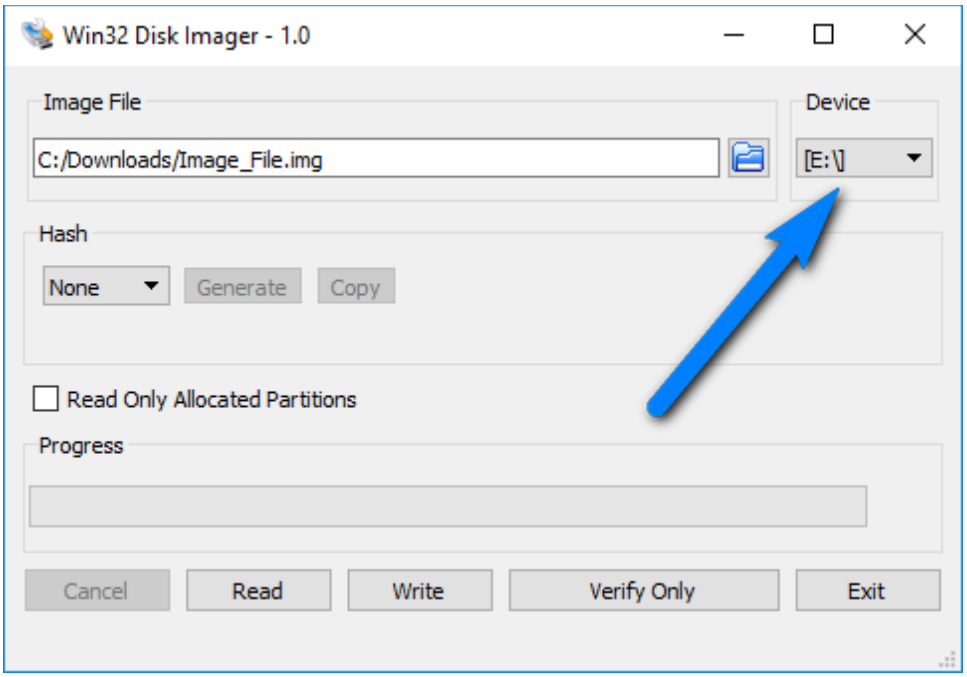
7. In the folder where the files were downloaded (in step 2), select the USB Boot Client *.img file and click the ***Open*** icon.



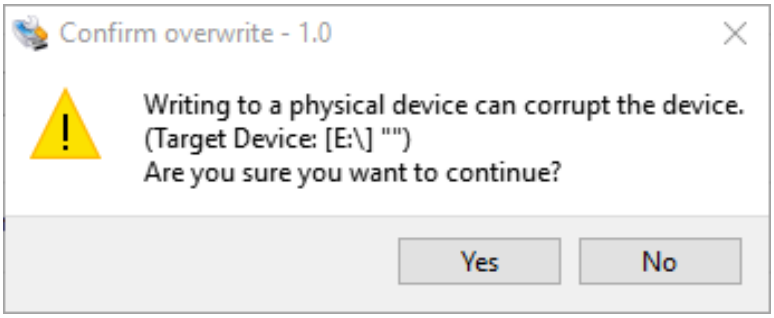
8. The Image file should now be seen in the Win32 Disk Imager screen under 'Image File'.



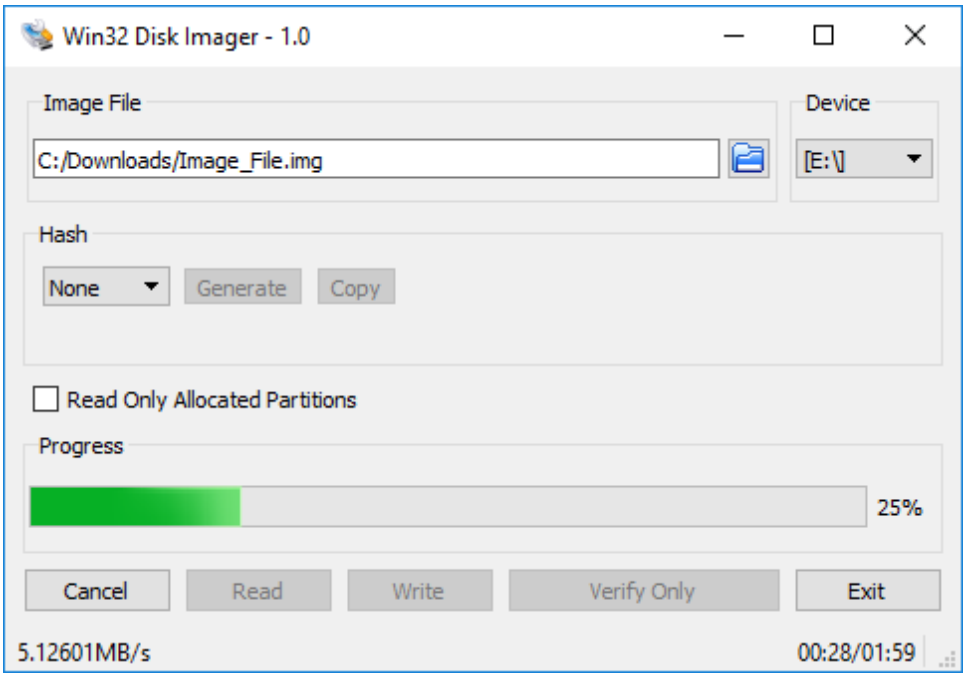
9. Under 'Device', select the drive letter for the USB flash drive that was connected during step 4 then click the ***Write*** icon.



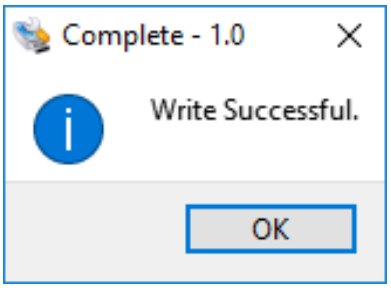
10. A confirmation screen will appear. Make sure that the "Target Device" is set to the correct drive letter. If it is the correct drive letter, click ***Yes*** to continue. If it is showing the wrong drive letter, click ***No***. This will take you back to the previous screen where you can select the correct drive letter (back to step 9).



11. The USB flash drive is now being prepared and the progress bar should be advancing.



12. When it is finished, a prompt should appear stating the write was successful. Click the ***OK*** button to continue. Close the Win32 Disk Imager window. The USB flash drive is now ready to be used.



12.3 Using the USB Boot Client

Drives connected to the computer can be used by the Falcon-NEO as a Source drive over a network connection if the USB Boot Client is used to boot the computer. The USB Boot Client is set to DHCP.

1. Connect the Falcon-NEO to the same network the computer with the USB Boot Client will be used on (or directly connected to the computer using a network cable).
2. Connect the computer (with the USB Boot Client) to the same network the Falcon-NEO is connected to.
3. Boot the computer with the USB Boot Client.

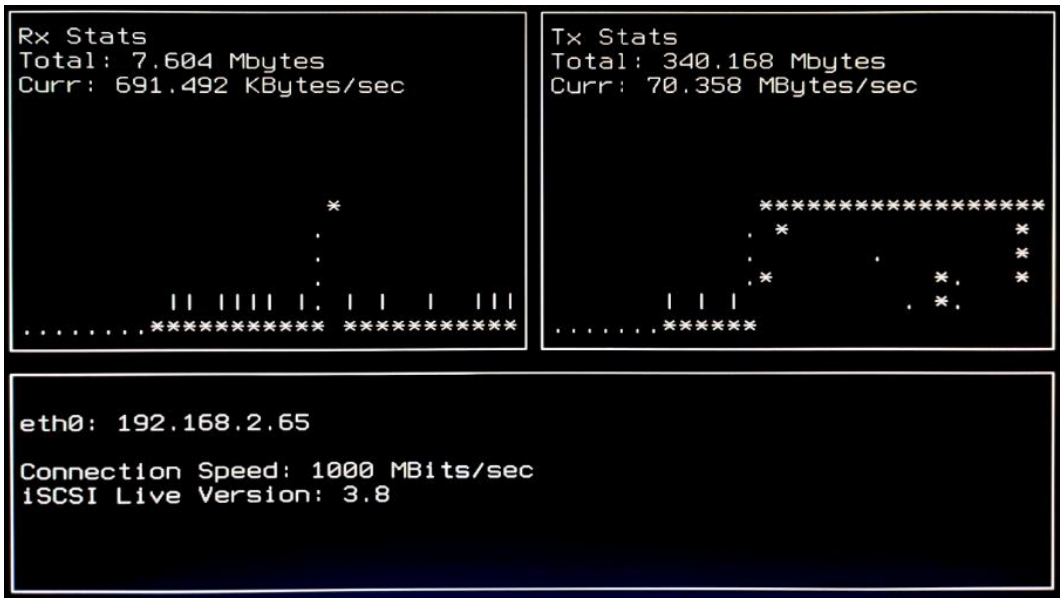
> Please contact the computer manufacturer if you do not know how to change the boot sequence to boot from a USB drive or to find out if the computer supports this function.

4. The USB Boot Client's boot menu will appear, and It should auto-select "iSCSI Target (64-bit)" after a few seconds. If not, select "iSCSI Target (64-bit)".

> The default (64-bit) should work with most computers. If it does not work, use the connected keyboard's DOWN arrow to select iSCSI Target (32-bit) to boot with the 32-bit version.

5. After about 30-120 seconds (depending on the speed of the computer), the USB Boot Client should finish booting up.
   - The following screen may appear if no network adapter or network connection is detected, or briefly while the network is being detected. If this screen appears for a long time, double-check the network adapter or network connection.

   - If a network adapter and network connection is detected, the following screen will appear:



6. Turn the Falcon-NEO on. After the Falcon-NEO boots up, you should see additional drives appear on the Source position depending on the Imaging mode chosen.

> The Logicube device will show the last two segments of the IP address. For example, **I:2.65.** The connected drive will show as ***SDA***. If there are any additional connected drives, they will show as ***SDB***, ***SDC***, etc. For example, if there is one drive connected, it will show as: **I:2.65/SDA**.

From here you can image using the Falcon-NEO using the normal imaging steps. When using the USB Boot Client, imaging speeds may vary depending on network performance.

12.4 Using the USB Boot Client over different subnets

The USB Boot Client and the Falcon-NEO can work over different subnets if both subnets can see each other on the network. Additional steps need to be taken when accessing a different subnet.

1. Follow the steps in ***Section 12.3*** to boot with the Forensic USB Boot Client.
2. Turn the Falcon-NEO on.
3. Navigate to ***Manage Repositories*** and tap or click the ***iSCSI*** tab.
4. Tap or click ***Network Settings***. In the ***Network Settings*** screen, enter the following information:
   a. **PORTAL –** The IP address of the iSCSI remote device (on the different subnet). Depending on your network setup, port 3260 may need to be added to the portal (for example: 10.10.10.107:3260)
   b. **USERNAME:** logicube (all lower case).
   c. **PASSWORD:** leave this blank.

5. When finished, tap or click ***OK***.

6. Tap or click ***CONNECT*** to connect to the remote device. Please note that the screen may stay on the “Connecting” screen for up to 60 seconds (or longer) depending on network speeds.
7. Once connected, you will see a “CONNECTED” screen appear. The remote device should now be seen on the Logicube device.

13: Printing

13.0 Printing – Introduction

When viewing log files through the Falcon-NEO 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 Falcon-NEO is connected to (see ***Section 9.1 – Web Interface***). This will allow printing to any printer already set up on the computer being used.
- From the touch screen on the Falcon-NEO. This will print to a configured local printer (connected via USB to the Falcon-NEO) or to a networked printer. See ***Section 13.2*** for instructions on how to set up a local or networked printer.

13.1 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.

13.2 Configuring a Local or Networked Printer

The Falcon-NEO can also print to a local (through USB) or networked printer. The printer must be configured using the Command Line Interface (CLI, see ***Section 9.2*** for instructions on how to connect to the CLI using a Telnet or SSH client). Local printers will need to be connected to the Falcon-NEO through an available USB port on the front of the Falcon-NEO. Networked printers will be seen by the Falcon-NEO when connected to the same network.

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

13.2.1 Step-By-Step – Configuring a Local or Networked Printer

1. Connect the Falcon-NEO to a network with DHCP. For networked printers, make sure the Falcon-NEO is connected to the same network. For local printers, connect the printer to an available USB port located in the front of the Falcon-NEO.
2. Turn the Falcon-NEO on. The Falcon-NEO should automatically assign itself an IP address that the Windows computer can see. Go to the ***Statistics*** screen on the Falcon-NEO and look at the hostname and IPAddress.
3. Using Telnet or SSH, connect to the Falcon-NEO. Instructions on how to connect via Telnet or SSH can be found in ***Section 9.2***.

4. Once logged in to the Falcon-NEO via CLI, type ***command***, then press the enter key.
5. Type ***config*** then press the enter key.
6. Type ***printer search*** then press the enter key. This will instruct the Falcon-NEO 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 to a new profile, type ***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 profile. Each time the Falcon-NEO is turned on, the local or networked printer should be available on the Falcon-NEO's touch screen.

14: Accessories and Options

14.0 Accessories and Options – Introduction

The Falcon-NEO has several available additional accessories and optional adapters available. For a complete list of available options, please visit https://www.logicube.com/shop/forensic-falcon-neo. This section lists the following options:

- Thunderbolt 3 / USB-C I/O Card
- FireWire Module
- USB 3.0 to SATA adapter & power cable
- SCSI Module

To purchase one or more of these options or adapters, please contact Logicube Sales department via email at sales@logicube.com.

14.1 Thunderbolt™ 3/USB-C I/O Card

The Falcon-NEO Thunderbolt 3/USB-C I/O card (part# F-FNEO-IO-TBT) provides Thunderbolt 3/USB-C interface support. The I/O card can be used in either the Source or Destination I/O ports of the Falcon-NEO.

Included items:

- One Thunderbolt/USB-C I/O card
- One labeled port door
- One screwdriver
- Quick Start Guide

Thunderbolt™ 3/USB-C I/OCard

Screwdriver

Labeled Door

> The I/O card does not currently support imaging in TDM from Mac computers. Please refer to our AppNote on how to image Macs with the Falcon-NEO. This AppNote can be found on our Falcon-NEO support page at: http://www.logicube.com/knowledge/forensic-falcon-neo/

14.1.1 Installing the Thunderbolt 3/USB-C I/O Card

Before installing the Thunderbolt 3/USB-C I/O card, make sure the Falcon-NEO has the latest software AND firmware installed.

The latest version can be found on the Falcon-NEO's knowledge base page at: https://www.logicube.com/knowledge/forensic-falcon-neo/.

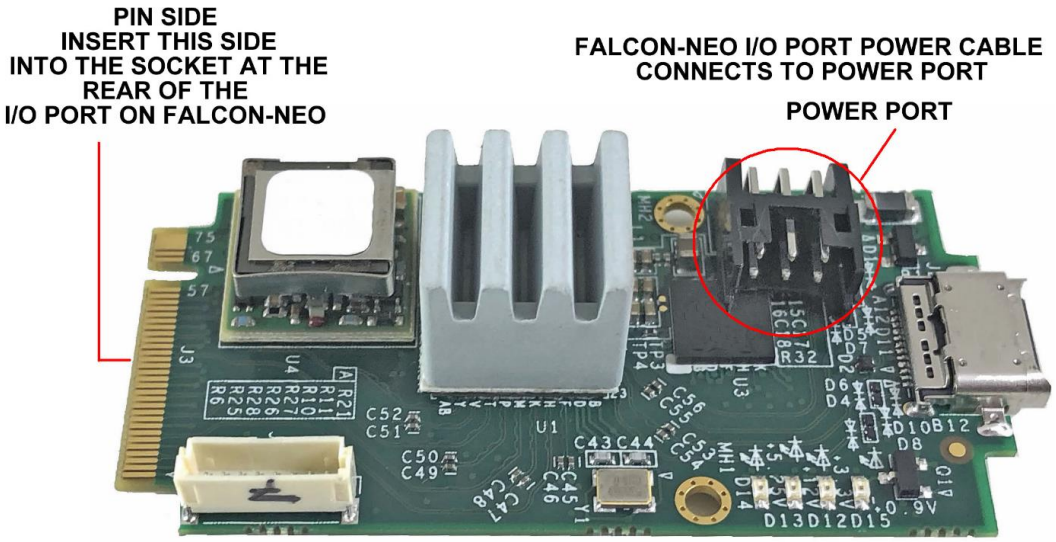
Instructions on how to update the software and firmware can also be found on the same page above.

The Falcon-NEO Thunderbolt 3/USB-C I/O Card is not hot-swappable. Always turn the Falcon-NEO ***off*** before connecting or disconnecting the I/O card to/from the Falcon-NEO. Drives or enclosures connected to the I/O card can be hot-swapped.

1. Turn the Falcon-NEO OFF and disconnect the AC adapter/power supply from the back of the Falcon-NEO.
2. Turn the Falcon-NEO upside-down and use the included screwdriver to remove the desired I/O port door:

3. The open I/O port should look like this:

4. Take the Thunderbolt/USB-C I/O card and connect it to the I/O port.

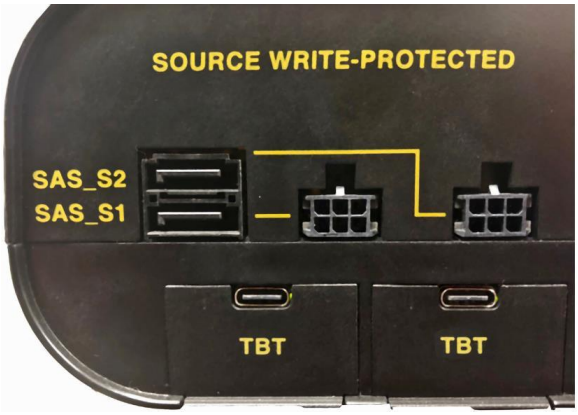


5. Take the power cable from the Falcon-NEO and connect it to the power port on the Thunderbolt/USB-C I/O card. Once the power is connected, connect the Thunderbolt/USB-C I/O card into the open I/O port.

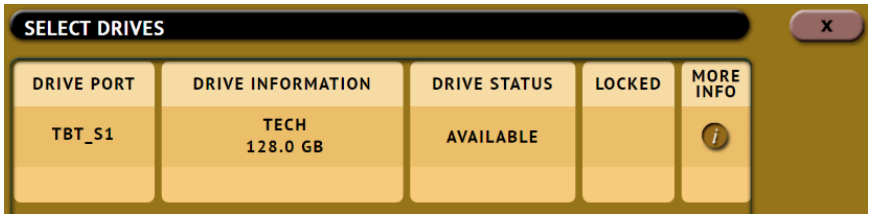
6. Using the included screwdriver, tighten the two small screws on each side of the I/O card into the post.

7. Take the labeled door and attach it back to the open I/O port. Use the included screwdriver to re-tighten the screw to the I/O port door.
8. Repeat steps 2 through 5 to install other Thunderbolt/USB-C I/O cards to any of the other available I/O ports.

Once all the Thunderbolt/USB-C I/O cards have been properly installed, the Falcon-NEO can now be used with Thunderbolt/USB-C external drives and storage enclosures. Any connected Thunderbolt/USB-C external drive and enclosure should appear like any other drive.



The Falcon-NEO Thunderbolt 3/USB-C I/O Card is not hot-swappable. Always turn the Falcon-NEO ***off*** before connecting or disconnecting the I/O card to/from the Falcon-NEO. Drives, enclosures, or Mac systems connected to the I/O card can be hot-swapped.



14.2 FireWire Module

A FireWire module (part# F-FW-MODULE-OPT) is available for the Falcon-NEO. This module provides a FireWire interface (one Source or one Destination) support and connects to the PCIe port of the Falcon-NEO.

Included items:

- One FireWire module
- One 6 ft FireWire 400 cable
- One FW 800 to 400 adapter
- DV to FW 400 cable
- Quick Start Guide

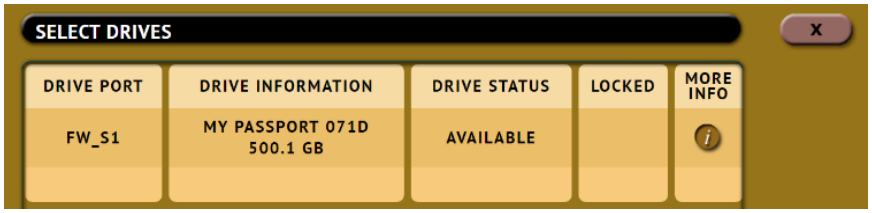
14.2.1 Connecting the FireWire Module

The Falcon-NEO FireWire Module is not hot-swappable. Always turn the Falcon-NEO ***off*** before connecting or disconnecting the FireWire Module to/from the Falcon-NEO. Drives, enclosures, or Mac computers connected to the FireWire Module can be hot swapped.

1. Turn the Falcon-NEO OFF.

2. Connect the FireWire Module to one of the PCIe ports on the Falcon-NEO (PCIE_S or PCIE_D). Repeat this step if a second FireWire module needs to be connected or disconnected.

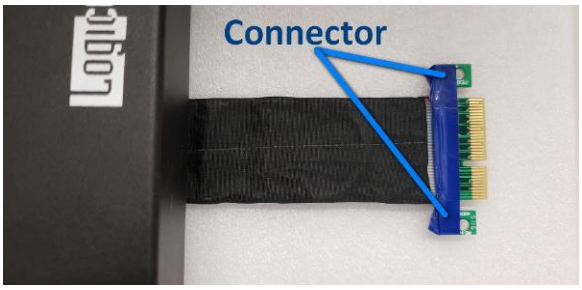
3. Once the FireWire module is connected to the Falcon-NEO, the Falcon-NEO can now be used with FireWire drives, enclosures, or Mac® systems (with FireWire or Thunderbolt 1 or Thunderbolt 2 with a Thunderbolt to FireWire adapter) booted in Target Disk Mode. Any connected FireWire drive, enclosure, or Mac system should appear like any other drive:



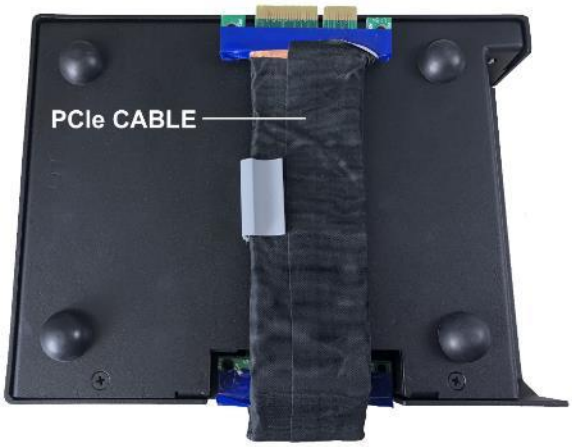
14.2.2 Disconnecting the FireWire Module

The Falcon-NEO FireWire Module is not hot-swappable. Always turn the Falcon-NEO ***off*** before connecting or disconnecting the FireWire Module to/from the Falcon-NEO. Drives, enclosures, or Mac systems connected to the FireWire Module can be hot swapped.

Turn the Falcon-NEO off. When disconnecting the FireWire Module from the Falcon-NEO, pull the cable from the connector. Do not pull the cable itself.



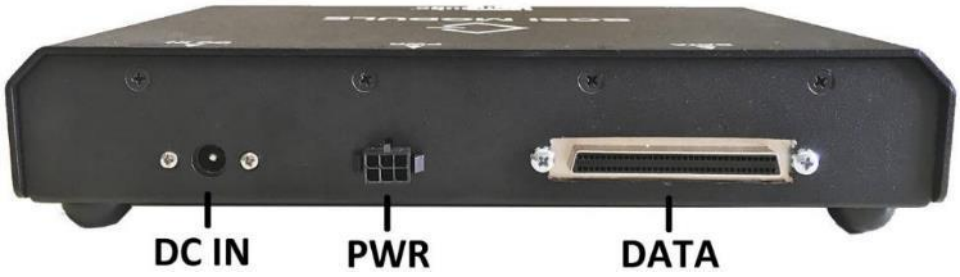
The FireWire Module connector cable can be stored underneath the FireWire Module:



14.3 Falcon-NEO SCSI Module

The optional Falcon-NEO SCSI Module (part# F-FALNEO-SCSI-OPT) expands the capability of the Falcon-NEO by providing support for imaging from and to SCSI hard drives. The SCSI module can connect to 68-pin SCSI drives natively. Optional adapters are available for use with 80-pin and 50-pin SCSI drives.

The Falcon SCSI module provides 1 SCSI port for use with either the Source or Destination PCIe port.



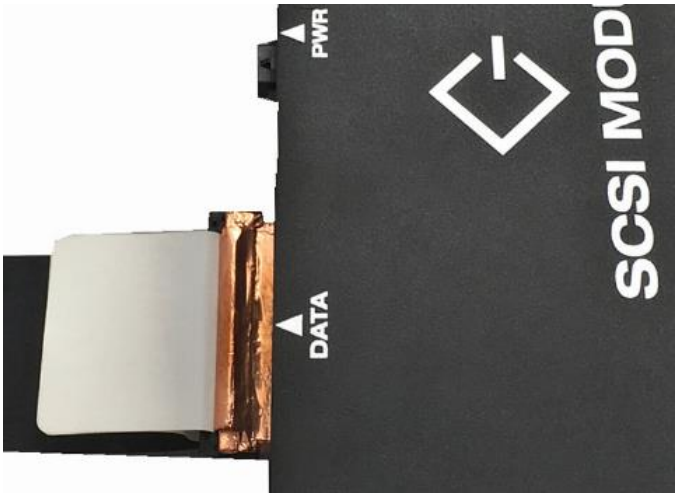
14.3.1 Connecting the SCSI Module to the Falcon-NEO

The Falcon-NEO SCSI Module is not hot-swappable. Always turn the Falcon-NEO ***off*** before connecting or disconnecting the Falcon-NEO SCSI Module or connecting/disconnecting SCSI drives.

1. With the Falcon-NEO turned off, connect the SCSI Module to one of the PCIe ports on the Falcon-NEO (PCIE_S or PCIE_D).
2. Connect the 68-pin data cable and drive power cable to the SCSI Module. If an 80-to-68 pin adapter or 50-to-68 pin adapter is used, connect the adapter to the cable(s).
3. Connect the drive to the data and power cables (or to the adapter).
4. Connect the AC adapter and power cable to an outlet and to the DC IN port of the SCSI Module.
5. Turn the Falcon-NEO on.

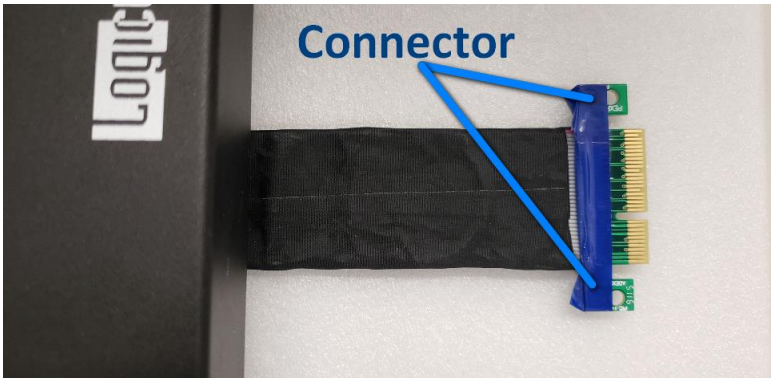
14.3.2 Disconnecting Drives from the SCSI Module

When disconnecting/removing the SCSI data cable, use the white tabs (as seen below) to avoid potential cuts from the copper lining.

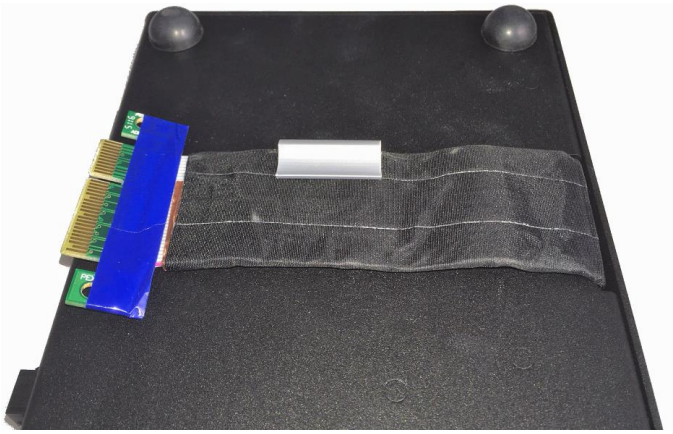


14.3.3 Disconnecting the SCSI Module

When disconnecting the SCSI Module from the Falcon-NEO, pull the cable from the connector. Do not pull the cable itself.



The SCSI Module connector cable can be stored underneath the SCSI Module:



14.4 USB 3.0 to SATA Adapter

Logicube has qualified a USB 3.0 to SATA Adapter for use with the Falcon-NEO This adapter provides the capability to connect SATA drives to any of the USB 3.0 ports.

The pictured adapter may be different than the actual product received.

The USB 3.0 to SATA adapter (part# **F-ADP-USB2SATAU**) can be purchased individually or as a part of a kit that includes three USB 3.0 to SATA adapters and a USB Power Cable (part number **F-CBL-USBSAT-KT**).

14.4.1 USB Power Cable

A USB Power Cable (part# **F-CBL-USB-PWR**) can be purchased. This cable eliminates the need for additional power supplies when using USB to SATA adapters connected to USB ports on the Falcon-NEO. Each USB Power Cable can provide additional power for up to 3 USB to SATA adapters.

The USB Power Cable connects one of two ways:

Direct connection to one of the two DC-IN ports on the Falcon-NEO:

Connected in-between the AC adapter/power supply and the Falcon-NEO:

14.4.2 USB 3.0 to SATA Kit

The USB 3.0 to SATA kit (part number **F-CBL-USBSAT-KT**) includes three USB 3.0 to SATA adapters and one USB Power Cable.

The USB 3.0 to SATA Adapter received from Logicube may be different from the picture shown.

15: Third-Party Adapters

15.0 Third-Party Adapters – Introduction

Adapters not purchased through Logicube may or may not work with the Falcon-NEO. Occasionally, Logicube will recommend an adapter that is expected to work with the Falcon-NEO. Some of these adapters are described in this chapter.

15.1 USB to Ethernet adapter

Some users may require a third network connection to the Falcon-NEO. This can be accomplished by using a USB to Ethernet adapter. Most USB to Ethernet adapters should work. It is recommended to use a 1000 Mbps (Gigabit) adapter for optimal results. When using a USB to Ethernet adapter, additional steps are required to enable the adapter.

Logicube has tested and validated the following USB to Ethernet adapters:

- Anker Aluminum USB 3.0 to Ethernet Adapter (Model # A7611011)
- Startech USB 3.0 to Gigabit Ethernet Adapter (Model # USB31000S)

1. Connect the USB to Ethernet adapter to any available USB port (Source or Destination).
2. Connect the USB to Ethernet adapter to the desired network.
3. From the Falcon-NEO main screen, go to ***Network Settings***. The ***Network Interfaces*** screen should now show three network interfaces: LAN1, LAN2, and LAN3. LAN3 is the newly added USB to Ethernet adapter.
4. To enable this adapter, tap or click ***LAN3*** to highlight it.
5. Tap or click ***Edit Configuration***. A window titled ***EDIT NETWORK INTERFACE CONFIGURATION LAN3*** window should appear.
6. If the connected network is ***DHCP*** enabled, simply tap or click ***OK*** to enable the adapter. If a ***STATIC*** IP is required, follow the instructions in ***Section 5.11.1.1***. Tap or click ***OK*** when finished. This will bring back the ***Network Interfaces*** screen. The adapter should now be enabled.
7. If the connected network is DHCP enabled, navigate to the ***STATISTICS*** screen and the ***ABOUT*** tab should show the ***lan3*** IP address.

After the steps above, users can save the settings to a profile so that the falcon-NEO boots up already configured and activated (with DHCP or Static IP settings). See ***Section 5.10.1*** for details on how to create, save, and load user profiles.

15.2 U.2 NVMe SSD (PCIe)

NVMe SSDs that have the U.2 connector require a U.2 to PCIe adapter to connect to the Falcon-NEO.

Logicube has tested and validated the following U.2 to PCIe adapter:

- StarTech U.2 to PCIe Adapter for 2.5" U.2 NVMe SSD - SFF-8639 - x4 PCI Express 3 (Model # PEX4SFF8639)

The U.2 to PCIe adapter must be used with Logicube's PCIe extender cable (Part # F-ADP-PCIe-CBL)

1. Connect the U.2 NVMe SSD the U.2 to PCIe adapter.
2. Connect the PCIe extender cable (F-ADP-PCIe-CBL) to the U.2 to PCIe adapter.
3. Connect the other end of the PCIe extender cable to the Flacon-NEO's PCIe Source or Destination port.

16: FREQUENTLY ASKED QUESTIONS

16.0 FAQs

Q. Why is it when I image a drive the number of bytes shown is twice the size of my Source drive?

A. 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.

Q. How many concurrent tasks can the Falcon-NEO run?

A. The Falcon-NEO can run up to 5 concurrent tasks.

Q. Can the Falcon-NEO image Linux partitions?

A. Yes. Falcon-NEO can image Linux partitions.

Q. Can the Falcon-NEO image the Apple File System (APFS), Hierarchical File System (HFS), or Hierarchical File System Plus (HFS+)?

A. Yes, Falcon-NEO can image APFS, HFS, and HFS+.

Q. Do Destination drives need to be wiped or formatted using the Falcon?

A. For Drive to File, File to File, Partition to File, and Net Traffic to File mode, the Falcon-NEO must be used to format Destination drives. This helps ensure that the images and data are written properly to the Destination drive(s).

Q. How does the Falcon-NEO handle bad sectors found on the Source drive?

A. Falcon-NEO will retry the bad sector 7 times. After the 7th attempt, if the sector still cannot be read, it will skip that sector and list the sector in the log file.

Q. What operating system does Falcon-NEO use?

A. Falcon-NEO uses a Linux-based operating system. A Linux-based operating system provides increased stability and security over Windows-based systems.

Q. What file format does Falcon-NEO use when formatting destination drives?

A. Falcon-NEO can format destination drives using the following file systems: EXT4, NTFS, exFAT, or FAT32.

Q. Does imaging performance slow down when multiple drives are imaged at the same time?

A. Performance is limited by the slowest drive in the configuration, however, there should not be any significant speed penalty when imaging multiple drives.

Q. Can I encrypt my evidence drives using the Falcon-NEO? How do I decrypt drives encrypted with Falcon-NEO?

A. The Falcon-NEO provides AES 256 whole drive encryption. Users can choose between three different cipher modes and can set their own password/key for the encrypted drive. Users can decrypt a drive that was encrypted with Falcon-NEO by using the Falcon-NEO to decrypt or by using VeraCrypt, TrueCrypt or FreeOTFE.

Q. Does the Falcon-NEO provide log files?

A. Yes, each image, hash, or wipe/format task produces a log file. The log file is viewable on the Falcon-NEO screen (or remotely on a PC). The log files can be exported to a thumb drive (the Falcon-NEO will export in XML, HTML, and PDF). XML log files can be customized using XML editors. The log files are stored on the internal hard drive within Falcon-NEO and are accessible by pressing the log file icon from the left-side navigation bar on the Falcon-NEO screen.

Q. If I am imaging to or from USB enclosures, will the Falcon-NEO's USB ports power my devices, or will an additional power source be required?

A. Each of the Falcon-NEO's USB ports meets the standard specification of up to 5V of power. If your USB device has higher power requirements an external power source will be necessary. Check with the manufacturer of your USB device to determine the exact power requirements.

Q. Can the Falcon-NEO image to or from a network destination?

A. Yes. The Falcon-NEO includes two 10GbE (Gigabit Ethernet) network connections. Users can designate a network share as a source or destination repository using SMB, CIFS, or iSCSI protocols.

Q. What is "Parallel Imaging"?

A. Parallel Imaging allows you to image from the same source drive to multiple destinations using different imaging modes. For example, an image to one Destination can be performed using E01 and at the same time, image to another Destination drive using Mirror Image (bit-for-bit). This is useful when there are multiple teams of investigators (one in a lab and one at another location but connected to a network) and you also need to provide a copy of the suspect hard drive to those that require an exact mirror image (for example to an attorney).

Q. Does the Falcon-NEO provide log files?

A. Yes, each operation/task produces a log file. The log file is viewable on the Falcon-NEO screen (or remotely on a PC) in an HTML format. The log files can be exported to a thumb drive (the Falcon-NEO will export in XML, HTML, and PDF). XML log files can be customized using XML editors. The log files are stored on the internal drive within Falcon-NEO and are accessible by pressing the log file icon from the left-side navigation bar on the Falcon-NEO screen.

Q. Can I remove the internal drive (that contains the Operating System) for secure locations or SCIFs?

A. Often investigators must work in a Sensitive Compartmented Information Facility (SCIF). These secure areas have very stringent requirements regarding the use of electronic devices to ensure sensitive information does not leave the confines of the SCIF. The Falcon-NEO has been designed with a removable internal hard drive. The Operating System, system settings and log files are all stored on this internal drive. If an investigation requires that the Falcon-NEO must be removed from the SCIF or be transported to another location, the internal drive can be removed prior to leaving the facility.

17: Index

Technical Support Information

For further assistance please contact

Logicube Technical Support:
by phone: **(+1) 818.700.8488 8 a.m. – 5 p.m. PT, M-F**
(excluding US legal holidays)

or by email: techsupport@logicube.com

Software Attribution

Debian 9 (Stretch) (https://www.debian.org/)

Linux Kernel (4.9.110-3+deb9u6) (GPL v2) (http://www.kernel.org) (modified)

libcli (1.9.5) (LGPL v2.1) (https://github.com/dparrish/libcli) (modified)

ntfs-3g (1:2016.2.22AR.1+dfsg-1) (GPL v2) (https://packages.debian.org/source/stretch/ntfs-3g) (modified)

dislocker (0.7.1) (GPL v2) (https://github.com/Aorimn/dislocker) (modified)

sleuthkit (4.4.0) (GPL v2/CPL v1.0/IBM-PL v1.0) http://www.sleuthkit.org/sleuthkit)

libewf (20180204-1) (GPL v2) (https://github.com/libyal/libewf)

exfat (1.2.12) (GPL v2) (http://opensource.samsung.com/) modified

PDFJS (1.0.907) (Apache License v2.0) (https://github.com/mozilla/pdfjs-dist) (modified)

libfvde (20180108-1) (LGPLv3+) https://github.com/libyal/libfvde (modified)

blistr (MIT) (http://github.com/idleberg/Bootstrap-Listr) (modified)

jstree (3.3.7) (MIT) (http://jstree.com/) (modified)

APFS-Fuse (GPL v2) (https://github.com/sgan81/apfs-fuse.git)

LZFSE (3-clause BSD) (https://github.com/lzfse/lzfse.git)