Falcon®-NEO2 User's Manual



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

Version: 2.2
Date: 07/15/2026
MAN-FALCON-NEO2

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

FALCON®-NEO2 USER'S MANUAL I

..... I

LIMITATION OF LIABILITY AND WARRANTY INFORMATION I

LOGICUBE DISCLAIMER I
WARRANTY I
ROHS CERTIFICATE OF COMPLIANCE III
LOGICUBE TECHNICAL SUPPORT CONTACT INFORMATION III

TABLE OF CONTENTS I

1: INTRODUCTION 1

SECTION 1: INTRODUCTION TO THE LOGICUBE FALCON®-NEO2 1
1.1: Feature Highlights 1
1.2: In the Box 4
1.3: Options and Accessories 4
1.4: Specifications 6

2: GETTING STARTED 7

SECTION 2: OVERVIEW OF THE FALCON-NEO2 7
2.1: Turning the Falcon-NEO2 On and Off 10
2.2: Connecting Various Drive Types 10
2.2.1: Connecting Source Drives 11
2.2.2: Connecting Destination Drives 11
2.2.3: Using USB/eSATA Drives or Enclosures 12
2.2.4: Connecting M.2/PCIe/mPCIe Drives 13
2.2.5: External Optical Drive (CD/DVD/Blu-ray) 13
2.3: The User Interface 13
2.4: Front and Rear Ports 14
2.5: Front Ports 14
2.6: Rear Ports 14
2.6.1: DC Power Ports 14
2.6.2: Dual 10GbE Ports 14
2.6.3: HDMI 15
2.7: Touch Screen 15

3: QUICK START 16

SECTION 3: QUICK START GUIDE 16
3.1: General Information 16
3.1.1: ATA Security-Locked Drives 16
3.1.2: Encrypted Drives and Partition Detection 18

3.2: Imaging 19
3.2.1: Step-By-Step Instructions – Imaging 21
3.2.2: Imaging BitLocker-Encrypted Drives 22
3.2.2.1: Password/Key 23
3.2.2.2: BEK File 25
3.2.3: Targeted/Logical Imaging 28
3.2.4: Imaging To or From a Network 28
3.2.5: Cloud Storage Acquisition 29
3.2.6: Mobile Device Capture 29
3.2.7: Imaging Net Traffic 29
3.2.8: Imaging Resume Feature 30
3.2.9: Auto Resume Feature 31
3.2.10: Drive Spanning 31
3.2.11: Parallel Imaging 32
3.2.12: Blank Disk Check 33
3.3: Hash / Triage 33
3.3.1: Step-By-Step Instructions – Drive Hash 34
3.3.2: Step-By-Step Instructions – Case Verify 35
3.3.3: Triage - Introduction 35
3.3.3.1: Creating a CSV Hash Database 36
3.3.3.2: Importing and Converting a Hash Database 37
3.3.3.3: Deleting a Hash Database 39
3.3.3.4: Starting a Triage 39
3.4: Wipe/Format 41
3.4.1: Step-By-Step Instructions – Wipe/Format 41
3.5: Push 42
3.5.1: Step-By-Step Instructions - Push 43
3.6: Task Macro 43
3.6.1: Step-By-Step Instructions – Task Macros 43
3.7: File Browser (with thumbnail view) 44
3.7.1: Step-By-Step Instructions – File Browser 45
3.8: Logs 45
3.8.1: Step-By-Step Instructions – Viewing or Exporting Logs 46
3.8.2: Viewing/downloading Log Files from the web interface 47
3.8.3: Deleting Log Files 47
3.8.4: Accessing the Logs Over a Network 48
3.9: Statistics 49
3.10: Manage Repositories 49
3.11: System Settings 50
3.12: Network Settings 50
3.13: Software Updates 51
3.14: Power Off 51

4: IMAGING 52

SECTION 4: IMAGING - INTRODUCTION 52
4.1: Mode 52
4.2: Source or Case 54
4.3: Settings 54

4.3.1: CASE INFO 54
4.3.2: HPA/DCO/ACS3/TRIM 55
4.3.2.1: Drive Trim 55
4.3.3: Error Handling 58
4.3.3.1: Error Granularity 58
4.3.3.2: Reverse Read 58
4.3.4: Hash/Verification Method 59
4.3.5: File Image Method Settings 59
4.3.6: Clone Method Settings 60
4.3.7: Verify Hash 60
4.3.8: Special Settings in File to File mode 60
4.3.8.1: Output Format Settings 60
4.3.8.2: Filter Settings 61
4.3.8.2.1: Path Filter 62
4.3.8.2.2: Date Filter 64
4.3.8.2.3: File Signature 64
4.3.8.2.4: Keywords 65
4.3.9: Special Settings in Net Traffic to File Mode 65
4.3.9.1: Segment Size 65
4.3.9.2: Number of Segments 66
4.3.9.3: Segment Ring Buffer 66
4.3.9.4: Chain Destinations 66
4.4: Destination/Image File 67
4.5: Starting the Imaging Operation 69

5: HASH / TRIAGE 70

SECTION 5: HASH / TRIAGE 70
5.1: Mode 70
5.2: Drives or Case 70
5.3: Settings 71
5.3.1: Drive Hash Settings 71
5.3.1.1: Hash Values 71
5.3.1.1.1: Hash Method 72
5.3.1.1.2: Hash Values 72
5.3.1.2: LBA 72
5.3.2: Case Verify Settings 73
5.3.2.1: Verify Hash 74
5.3.3: Triage Settings 74
5.3.3.1: Filter Settings 74
5.3.3.1.1: Path Filter 75
5.3.3.1.2: Date Filter 77
5.3.3.1.3: File Signature 77
5.3.3.1.4: Keywords 78
5.3.3.2: Search Criteria 78
5.3.3.3: Hash DB 78
5.3.3.4: Hash Method 79
5.3.4: Case Info 79

6: TYPES OF OPERATION 80

SECTION 6: TYPES OF OPERATIONS - INTRODUCTION 80
6.1: Imaging 84
6.2: Hash / Triage 84
6.3: Wipe / Format 84
6.3.1: Destination 85
6.3.2: Settings 85
6.3.2.1: Secure Erase 86
6.3.2.2: Wipe Patterns 86
6.3.2.2.1: Mode 87
6.3.2.2.2: HPA/DCO/ACS3 87
6.3.2.2.3: LBA 88
6.3.2.2.4: PASSES 88
6.3.2.3: Format 89
6.3.3: Case Info 90
6.4: Push 90
6.4.1: Source 91
6.4.2: Settings 91
6.4.3: Destination 91
6.5: Task Macro 92
6.5.1: Tasks 93
6.6: File Browser (Now with thumbnail view) 94
6.6.1: Viewing Source Drives or Network Repositories 95
6.6.2: Viewing DD, E01, EX01, DMG, and L01 Images 96
6.6.3: Additional Notes About Using the File Browser 97
6.6.4: Viewing Files from the Web Interface 98
6.7: Logs 99
6.8: Statistics 99
6.8.1: About Screen 99
6.8.2: Adv. Drive Statistics 99
6.8.3: Options 100
6.8.3.1: Mobile-Enable 100
6.8.3.2: Cloud-Enable 101
6.8.3.3: Triage-Enable 101
6.8.4: Network Interface Stats 101
6.8.5: Debug Logs 101
6.8.6: Help 102
6.9: Manage Repositories 102
6.9.1: Add/Remove 103
6.9.1.1: Adding a Repository Using CIFS or SMB 103
6.9.1.2: Editing or Deleting/Removing a Repository 106
6.9.1.3: Multi-Factor Authentication (MFA) 106
6.9.2: iSCSI 106
6.9.3: Cloud 108
6.9.3.1: Adding a Cloud Repository 108
6.9.4: Configuration 109
6.10: System Settings 109

6.10.1: Profiles 110
6.10.2: Passwords 111
6.10.2.1: Setting Key Passwords 112
6.10.2.1.1: Config Lock Notes 113
6.10.2.1.2: Forgotten password for any keys 114
6.10.2.2: User Account Passwords 115
6.10.3: Encryption 116
6.10.4: Language/Time Zone 117
6.10.4.1: Language 117
6.10.4.2: Time Zone 117
6.10.5: Display 118
6.10.6: Destination Whitelist 119
6.10.6.1: View 120
6.10.6.2: Select 120
6.10.6.3: Upload 121
6.10.6.4: Clear 122
6.10.7: Notifications 122
6.10.7.1: Sound Notifications 123
6.10.7.2: Email/SMS Notifications 123
6.10.7.2.1: Additional Notes for Email/SMS Notifications 124
6.10.8: Advanced 125
6.10.9: Debug 126
6.11: Network Settings 126
6.11.1: Interfaces 126
6.11.1.1: Configuring a Static IP address 126
6.11.1.2: MTU 127
6.11.1.3: Enabling/Disabling Network Services 127
6.11.2: HTTP Proxy 128
6.11.2.1: Server 128
6.11.2.2: Username/Password 129
6.11.3: Network Configurations 129
6.11.4: HTTPS 130
6.11.5: 802.1X 130
6.12: Software Updates 131
6.13: Power Off 131

7: PREVIEWING DRIVES 132

SECTION 7: PREVIEWING DRIVES - INTRODUCTION 132
7.1: File Browser 133
7.2: Computer + File Browser 133
7.3: SMB 133
7.4: iSCSI 134

8: DESTINATION DRIVE ENCRYPTION AND DECRYPTION 135

SECTION 8: DESTINATION DRIVE ENCRYPTION/DECRYPTION - INTRODUCTION 135
8.1: Encrypting a Destination 136
8.1.1: Step-By-Step Instructions 136
8.1.2: Using Previously Encrypted Destination Drives 136

8.2: Decrypting a Falcon-NEO2 Encrypted Drive with a Falcon-NEO2 137
8.3: Decrypting a Falcon-NEO2 Encrypted Drive without a Falcon-NEO2 138
8.3.1: Which Decryption Software to Use? 139
8.3.2: Decrypting Using VeraCrypt 139
8.3.3: Decrypting using FreeOTFE 141

9: UPDATING/LOADING/RE-LOADING SOFTWARE 143

SECTION 9: UPDATING/LOADING/RE-LOADING SOFTWARE – INTRODUCTION 143
9.1: Requirements 143
9.2: Updating/Loading/Re-loading Software Instructions 143
9.2.1: From Network (Over the Internet) 144
9.2.2: From USB Drive (Through a Software File Download) 145
9.3: Firmware Loading Instructions 146
9.4: PXEBOOT UPDATE 146
9.5: BIOS Configuration Revision 147

10: REMOTE OPERATION 148

SECTION 10: REMOTE OPERATION - INTRODUCTION 148
10.1: Web Interface 148
10.2: Command Line Interface (CLI) 148
10.2.1: Connecting Using Telnet 149
10.2.2: Connecting Using SSH 149
10.3: Zero Configuration Networking (Zeroconf) 150
10.4: Copying Profiles from One Falcon-NEO2 to Another 150
10.4.1: Step-By-Step – Copying Profiles 150

11: VIEWING SOURCE AND DESTINATION DRIVES OVER A NETWORK 152

SECTION 11: VIEWING DRIVES OVER A NETWORK – OVERVIEW 152
11.1: Viewing Source or Destination Drives Over the Network Using SMB 152
11.2: Viewing Source Drives Over the Network Using iSCSI 153

12: NET TRAFFIC IMAGING 159

SECTION 12: NET TRAFFIC INTRODUCTION 159
12.1: Net Traffic Settings 159
12.2: Net Traffic Imaging Notes 161

13: MOBILE TO FILE IMAGING 162

SECTION 13: MOBILE TO FILE INTRODUCTION 162
13.1: Mobile Device Capture Requirements 162
13.2: Android Devices 163
13.3: iOS and iPadOS Devices 163
13.4: Configuring and Starting the Mobile to File task 163

14: USB BOOT CLIENT 165

SECTION 14: USB BOOT CLIENT INTRODUCTION 165
14.1: Requirements 165
14.2: Creating the USB Boot Client 165
14.3: Using the USB Boot Client 168

14.4: Using the USB Boot Client over different subnets 170

15: PRINTING 171

SECTION 15: PRINTING – INTRODUCTION 171
15.1: Printing from the Web Interface 171
15.2: Configuring a Local or Networked Printer 171
15.2.1: Step-By-Step: Configuring a Local or Networked Printer 171

16: OPTIONS AND ACCESSORIES 173

SECTION 16: OPTIONS AND ACCESSORIES – INTRODUCTION 173
16.1: Triage 173
16.2: Mobile Device Capture 174
16.3: Thunderbolt 3/USB-C I/O Card 174
16.4: Falcon-NEO2 SCSI Module 175
16.4.1: Connecting the SCSI Module to the Falcon-NEO2 175
16.4.2: Disconnecting Drives from the SCSI Module 175
16.4.3: Disconnecting the SCSI Module 176
16.5: FireWire Module 176
16.5.1: Connecting the FireWire Module 177
16.5.2: Disconnecting the FireWire Module 177
16.6: PCIe Adapter Kit 178
16.6.1: Pictures (for Reference) 178
16.6.2: Understanding M.2 and Mini PCIe SSDs 179
16.6.3: Connecting and Using the Adapters 179
16.6.3.1: M.2 PCIe (NVMe or AHCI) SSDs 179
16.6.3.2: M.2 SATA based SSDs 180
16.6.3.3: Mini PCIe (mPCIe) SSDs 180
16.6.3.4: HHHL (half-height, half-length) and FHHL (full-height, half-length) PCIe SSDs 180
16.7: U.2-to-PCIe Adapter 180
16.8: M.2 NVMe-to-USB Adapter 180
16.9: USB 3.0-to-SATA Adapter 181
16.9.1: USB 3.0 to SATA Bundle 181
16.9.2: USB Hub 182
16.10: NVME EXPANSION MODULE 182
16.10.1: Enablement of the NVME Expansion Module 182
16.10.2: Connecting NVMe Expansion Module to Falcon-NEO2 183
16.10.3: Disconnecting NVMe Expansion Module from Falcon-NEO2 183

16: THIRD-PARTY ADAPTERS 184

SECTION 17: THIRD-PARTY ADAPTERS – INTRODUCTION 184
17.1: USB-to-Ethernet adapter 184

18: FREQUENTLY ASKED QUESTIONS 185

SECTION 18: FAQS 185

19: INDEX 188

TECHNICAL SUPPORT INFORMATION 189
ATTRIBUTION NOTICE: 189
SOFTWARE ATTRIBUTION 189

1: Introduction

Section 1: Introduction to the Logicube Falcon®-NEO2

The Falcon-NEO2 is the groundbreaking follow-on to the Falcon®-NEO, which has long been recognized as the “Best In Class” among all imagers. With Project VIC Validation and the Triage function, triage source drive files against VICS, Comma-Separated Values (CSV), and X-Ways Hash Databases. Multi-Factor Authentication (MFA) support is available using the YubiKey 5 FIPS authenticators. The built-in File Browser now supports Thumbnail view for easier viewing. Retooled and optimized with a powerful new engine, the Falcon-NEO2 is the first field imager to surpass 100GB/min E01 capture speeds. Its SAS-3 architecture (12 Gbps SAS) supports up to 5 simultaneous tasks with up to 10 source and 11 destination ports. Image SAS-3 SSDs at speeds up to 115GB/min, and PCIe drives at speeds exceeding 100GB/min. The USB ports on the Falcon-NEO2 are USB 3.2 Gen-2 (10Gbps), and two 10GbE ports continue to be available on Falcon-NEO2 for imaging to/from network repositories. The “Cloud Storage Acquisition” and “Mobile Device Capture” are standard and available on the Falcon-NEO2, along with physical and logical support for AFF4.



1.1: Feature Highlights

- **VICS Data Compliant.** Import VICS Hash Databases and triage source drive files against the VICS Hash Databases.
- Import and convert Comma Separated Values and X-Ways hash databases for Triage.

- **10 write-blocked source ports** include **4 NATIVE SAS/SATA** drives supported through a 4-in-1 SAS cable, 2 USB 3.2 (Gen 2), 1 PCIe, 2 I/O ports for use with optional Thunderbolt™ 3/USB-C module, 10 GbE.
- **11 destination ports** include **4 NATIVE SAS/SATA** drives supported through 4-in-1 SAS cable, 4 USB 3.2 (Gen 2) and 1 PCIe, and 1 I/O port for use with optional Thunderbolt 3/USB-C module, 10GbE.
- **Multi-Factor Authentication (MFA)** to network repositories. Utilize a YubiKey 5 FIPS series of authenticators to connect to a shared Active Directory network resource securely.
- Now supports **Non-Logicube-formatted Destination drives**.
- **Thumbnail view** of source drive images using the built-in File Browser.
- **AFF4 support** for both **physical and logical imaging.** Image source drives to AFF4 (Advanced Forensic File Format 4), an open-source format for digital evidence and data.
- **Concurrent Image+Verify** 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. **A Logicube invention since 2013.**
- **Mobile Device Capture** (now a standard feature) to capture critical digital evidence from mobile devices, including Apple iPhones and Android phones. Capture SMS, MMS, photos, and videos. Supports Android 4.0 and up and iOS.

- **Built-in Ports:**
  - **Source:** 4 SATA/SAS drives supported through 4-in-1 SAS cable, 2 USB 3.2 (Gen 2), 1 PCIe, 2 I/O ports for custom interface add-on cards
  - **Destination:** 4 SATA/SAS drives supported through 4-in-1 SAS cable, 4 USB 3.2 (Gen 2), 1 PCIe, 1 I/O port for custom interface add-on cards
  - **Network:** 2 10 GbE ports
- **Drive Interface Support included:** SATA, SAS, USB, PCIe, mSATA (with included adapter), micro SATA (with included adapter), eSATA cable, USB Type-A
- **Optional adapters:** M.2 and PCIe adapter kit, 2.5"/3.5" IDE adapter, U.2 NVMe, M.2 NVMe to USB, 1.8" & 1.8" IDE ZIF, USB to SATA adapter, USB 3.0 4-port hub, Flash media
- **Optional Modules:** Thunderbolt/USB-C I/O Card, FireWire, SCSI, PCIe Expansion
- **Optional Software Subscriptions (for serial numbers under 223000):** Mobile Device Capture Option.
- **Optional Software (for serial numbers under 223000):** Triage. Import VICS Hash Databases and triage source drive files against the VICS Hash Databases.
- **Network Capability:** 2 10 GbE Ports used for remote operation, network repositories, USB Boot Client, network traffic capture, and software updates.
- **Imaging Speeds:** E01 image at over 50 GB/min with SATA SSDs. E01 image with SAS-3 SSDs at speeds up to 115 GB/min. Clone PCIe to PCIe exceeding 100 GB/min.
- **AFF4 physical and logical support.**

- **Wipe Feature:** Secure Erase, DoD wipe, and custom pass settings. Complies with NIST 800-88 r1 guidelines. User-selectable option to verify wipe pass value during the wipe process.
- **Cloud Capture:** Offered as a standard feature with the Falcon-NEO2.
- **Multiple Imaging and Capture Modes:**
    - **Drive to File –** Creates DD, E01, Ex01, and DMG image files of the Source drive.
    - **File to File –** Logically image-specific file types by file extension, folders/directories, specific files, and from Cloud storage.
    - **Drive to Drive –** Bit-for-bit copy.
    - **Partition to File –** Select and image specific partitions on the source drive.
    - **Net Traffic to File –** Capture network traffic, internet activity, and VOIP. Sniff data on a network and store captured packets to destination drives. Data is saved to a .pcapng format.
    - **File to Drive –** Restore Falcon-NEO2 created DD, E01, Ex01, and DMG image files to their original state.
    - **Mobile to File –** Acquire critical digital evidence from mobile devices, including Apple iPhones, iPads, Android phones, and tablets. Mobile Device Capture is standard for serial numbers above 223000, and is an annual subscription for serial numbers below 223000.
- **USB Boot Client:** Image from a computer on the same network without removing the drive from the computer.
- **Image from a Mac Computer:** Image from a Mac computer with USB-C ports using a USB-C to USB-A cable and Target Disk Mode. Users can also image from Mac computers using Logicube's USB Boot Client.
- **File Browser:** Preview drive contents directly on the Falcon-NEO2. This feature provides logical access to source or destination drives and network repositories connected to Falcon-NEO2.
- **Concurrent Image + Verify:** Imaging and verifying concurrently takes advantage of fast destination drives or a 10 GbE connection faster than the source drives. Duration of total image process time may be reduced by up to half.
- **Parallel Imaging:** Simultaneously perform multiple imaging tasks from the same source drive to multiple destinations using different imaging formats. Supports up to 5 imaging tasks at a time. **A Logicube invention since 2013.**
- **Encryption:** Secure sensitive evidence data with open-source whole drive NIST recommended XTS-AES-256 encryption cipher mode.
- **Encryption Detection:** Whole disk and partition-level encryption detection. Easily identify Source drives with possible encryption.
- **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.
- **Partition Imaging:** Select and image specific partitions from the source drive.
- **BitLocker, OPAL, VeraCrypt, and TrueCrypt Decryption Support:** Decrypt partitions (requires the recovery key or password) and then image the selected partition. A BEK

(BitLocker Encryption Key) file is supported to unlock FIPS-compliant BitLocker encryption.

- **Network Traffic Capture:** Capture network traffic, internet activity, and VOIP. Sniff data on a network and store captured packets on a hard drive connected to Falcon-NEO2.
- **Image Restore:** File to drive mode restores DD, E01, Ex01, and DMG images created by the Falcon-NEO2 to another drive.
- **Error Handling:** Three cluster size settings provide more control over handling bad sectors. Bad sectors can be skipped, or the imaging task can automatically abort when they are encountered. Reverse Read skips the bad block and reads the data backwards, potentially capturing data that may not necessarily be read by skipping the entire block.
- **Dimensions:**
  10" x 6.75" x 3.25" (254 mm x 171 mm x 83 mm)

**The Forensic Falcon-NEO2 achieves speeds surpassing 50 GB/min and up to 115 GB/min using SATA or SAS-3 solid-state "suspect" drives containing freshly installed Windows OS and random data and solid-state destination drives. Settings used are e01/ex01 image format, with compression and verify "on". The specification and condition of the hard drives and the mode, image format, and settings used during the imaging process may affect the achieved speeds.*

1.2: In the Box

- Power supply & U.S. power cord
- 2 4-in-1 SAS/SATA data & power cables
- 2 CAT 7 network cables
- eSATA to SATA cable
- mSATA to SATA adapter
- microSATA to SATA adapter
- USB 3.2 male Type-A to USB 3.2 male Type-C cable
- Soft-sided carrying case

1.3: Options and Accessories

The following options and accessories are available for the Falcon-NEO2:

Additional Hardware Options:

- **NVMe Expansion Module:** The NVMe Expansion Module provides support for 4 M.2 NVMe drives and can be connected to the Source and/or Destination PCIe ports of the Falcon-NEO2.
- **Thunderbolt/USB-C I/O card:** An optional I/O card supports imaging directly to/from Thunderbolt 3/USB-C and USB 3.1 Gen 2 external drives and storage enclosures. The card connects to the two write-protected source I/O ports or one destination I/O port.

- **SCSI Module:** The SCSI Module option supports 68-pin SCSI drives. It connects to either of the PCIe ports and can provide one write-protected SCSI source or destination port. Optional adapters are available for 50-pin and 80-pin SCSI drives.
- **FireWire Module:** The FireWire Module option supports FireWire enclosures. It connects to either of the PCIe ports and can provide one write-protected FireWire source or destination port.

Additional Software Options:

- **Triage Option (Project VIC Compatibility):**
  - **For serial numbers 223000 and above –** This is a standard, built-in feature.
  - **For serial numbers below 223000 –** Available with a one-time paid option that requires a hardware upgrade to enable this optional feature.

  Import Project VIC hash databases into the Falcon-NEO2, then triage source drive files to see if any files on the source drive match the hashes with the contents of the Project VIC database.

- **Mobile Device Capture:**
  - **For serial numbers 223000 and above –** This is a standard, built-in feature.
  - **For serial numbers below 223000 –** Available as an annual, renewable software subscription.

  Expands the functionality of the Forensic Falcon-NEO2 with a convenient method for quickly acquiring potential evidence data from mobile devices, including Apple iPhones, iPads, Android phones, and tablets. Adding this software option to the Falcon-NEO2 for field investigations reduces the need for additional hardware to collect critical evidence from mobile devices.

Additional Accessories:

- PCIe adapter kit is for M.2 PCIe, M.2 NVMe, M.2 SATA, PCIe, and mini-PCIe cards. It includes one each of M.2 PCIe, M.2 SATA, Mini PCIe, and PCIe extender cable.
- U.2 NVMe to PCIe adapter
- M.2 NVMe to USB adapter
- 18" extended SATA cable set
- USB Flash Reader is used to clone or image various flash media, including CompactFlash, SD cards, and other flash media.
- USB3 to SATA adapter: Convert USB 3.2 ports for use with SATA drives.
- 4-port USB 3.0 hub
- 2.5"/3.5" IDE to SATA adapter
- 1.8" ZIF to IDE and 1.8" IDE to SATA adapter
- USB SATA Kit: Includes 3 USB3 to SATA adapters and a specialty single power cable for converting the three USB Destination Ports from USB to SATA
- Falcon-NEO2 hard case only (with laser-cut foam)
- mSATA to SATA adapter (1 included with Falcon-NEO2)

- Micro SATA to SATA adapter (1 included with Falcon-NEO2)
- eSATA cable (1 included with Falcon-NEO2)
- SATA/SAS data & power replacement cable
- 50-pin to 68-pin SCSI adapter (forthcoming) for use with the Falcon-NEO2 SCSI Module Option
- 80-pin to 68-pin SCSI adapter (forthcoming) for use with the Falcon-NEO2 SCSI Module Option

1.4: Specifications

Power Requirements	Power Consumption	Operating Temperature	Relative Humidity	Net Weight	Dimensions	Agency Approvals
12V DC, grounded 21A	250W	0 to 40° C (32 to 104° F)	20% to 80%	3.35 lbs 1.52 kg	10" X 6.75" X 3.25" 254 mm X 171.45 mm X 82.55 mm	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.


ESD NOTICE:

If an EFT (Electrical Fast Transient) or EMI (Electro Magnetic Interference) event occurs, Falcon-NEO2 operations could be disrupted, and it may be necessary to restart Falcon-NEO2.

2: Getting Started

Section 2: Overview of the Falcon-NEO2

Special Icons

Throughout this manual, you will encounter two special icons. Please pay close attention whenever you see either of these icons, as they indicate important information or critical warnings related to specific topics.

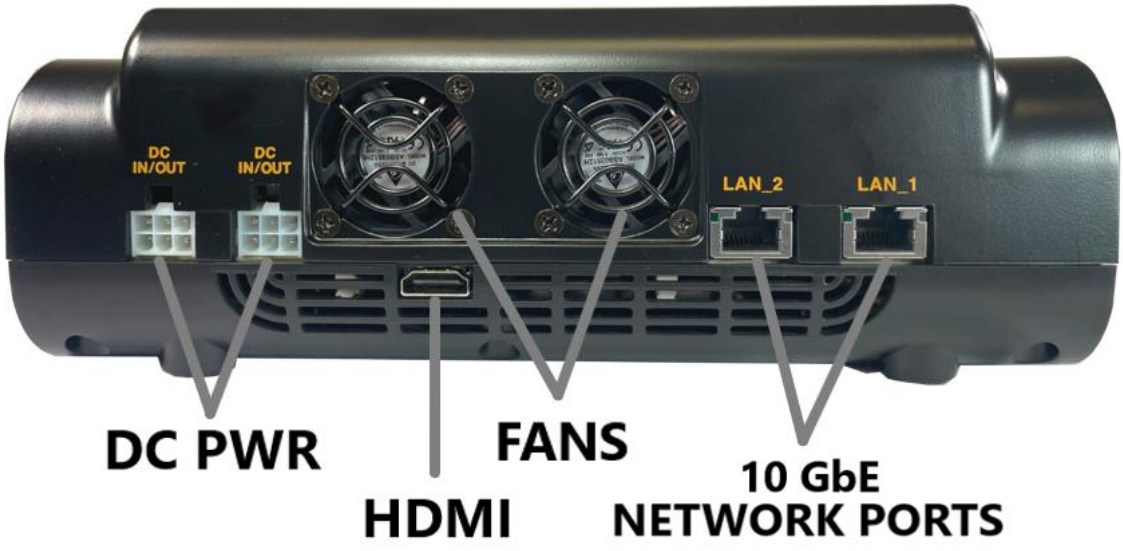
FALCON-NEO2 TOP VIEW



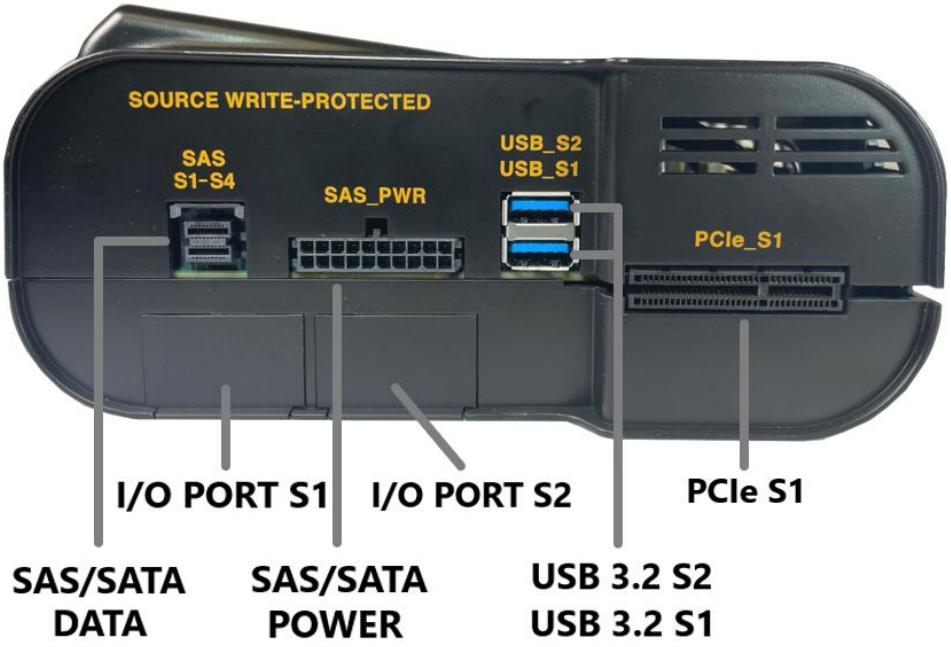
FALCON-NEO2 FRONT VIEW



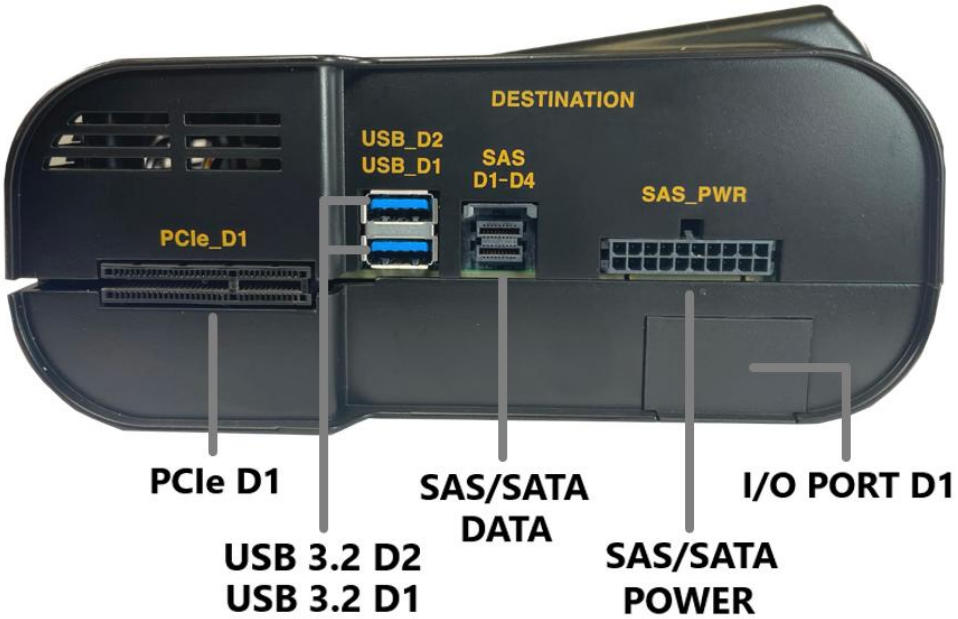
FALCON-NEO2 BACK VIEW



FALCON-NEO2 LEFT SIDE VIEW
SOURCE PORTS



FALCON-NEO2 RIGHT SIDE VIEW
DESTINATION PORTS



2.1: Turning the Falcon-NEO2 On and Off

The Falcon-NEO2 features two DC-IN ports on the rear of the device, either of which can power the unit. The second DC-IN port is provided to accommodate potential future increases in power requirements.

The Falcon-NEO2 includes a 12V grounded power supply with a 21A DC output. Connect this power supply to either of the two DC-IN ports on the device's back.

To power on the Falcon-NEO2, press and quickly release the power button on the unit's top-right corner. The device will then begin its boot-up process.

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

There are two methods for shutting down the Falcon-NEO2:

1. **Using the Power Button:** Press and immediately release the power button on the top-right corner of the Falcon-NEO2. The device will initiate the shutdown process, and the display and fans will power off after a few seconds.
2. **Using the Graphical User Interface (GUI):** Access the GUI directly through the touchscreen or remotely via a web browser. Navigate to the **Power Off** screen and tap the **Power Off** icon to begin the shutdown process.

2.2: Connecting Various Drive Types

The Falcon-NEO2 supports a variety of drive types, including the following:

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

When using drive adapters to connect or disconnect drives, it is recommended to leave the drive attached to the adapter and then connect or disconnect the adapter from the SAS/SATA cable. Alternatively, you may connect or disconnect the SAS/SATA cable directly from the drive bay while keeping the drive and adapter connected.

2.2.1: Connecting Source Drives

Source drives should be connected to the left side of the Falcon-NEO2. These ports are write-protected to ensure data integrity and are labeled as follows:

- **SAS S1-S4 –** SAS/SATA data port (for use with the included SAS/SATA cable)
- **SAS_PWR –** SAS/SATA power port (for use with the included SAS/SATA cable)
- **USB_S1 and USB_S2 –** USB 3.2 Source ports
- **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)
- **TBT:** Two I/O ports for use with optional Logicube I/O expansion cards (Thunderbolt 3/USB-C pictured below).



The Falcon-NEO2 Source ports are hot-swappable (including the PCIe ports).

While the Falcon-NEO2 ports support hot-swapping, certain drives or adapters may not. Always consult the drive manufacturer to determine whether your drive is compatible with hot-swapping.

Source drives can be connected in any order. For instance, a single SATA Source can be plugged into any connector on the SAS/SATA cable on the Source side of the Falcon-NEO2.

Never attach a suspect or source drive to a destination port on the Falcon-NEO2, as data may be overwritten.

Any combination of drives can be connected. For example, a SAS drive, a SATA drive, a USB drive, and a PCIe drive can all be connected simultaneously.

2.2.2: Connecting Destination Drives

Destination drives should be connected to the right side of the Falcon-NEO2. These ports are labeled as follows:

- **SAS D1-D4 –** SAS/SATA data port (for use with the included SAS/SATA cable)
- **SAS_PWR –** SAS/SATA power port (for use with the included SAS/SATA cable)
- **USB_D1 and USB_D2 –** USB 3.2 Destination ports (USB_D3 and USB_D4 are located on the front of the Falcon-NEO2)
- **PCIe_D1 –** PCIe Source port (Depending on the type of PCIe drive, the optional PCIe kit, part number F-ADP-PCI-FN-KT may be required)
- **TBT:** I/O port for use with optional Logicube I/O expansion cards (Thunderbolt 3/USB-C pictured below).



The Falcon-NEO2 Destination ports are hot-swappable (including the PCIe ports).

While the Falcon-NEO2 ports support hot-swapping, certain drives or adapters may not. Always consult the drive manufacturer to determine whether your drive is compatible with hot-swapping.

Destination drives can be connected in any order; following a specific sequence is unnecessary. For example, a SATA destination drive can be attached to any connector on the SAS/SATA cable on the Falcon-NEO2's destination side.

You can connect any combination of drives simultaneously. For example, four SATA drives, one USB drive, and one PCIe drive can work simultaneously.

Never attach a suspect or source drive to a destination port on the Falcon-NEO2, as data may be overwritten.

2.2.3: Using USB/eSATA Drives or Enclosures

Keeping the drive within its original enclosure is advisable, as these enclosures may contain onboard controllers for proper data access. Removing the drive from the enclosure could prevent devices, including computers, from accurately reading the drive's contents.

2.2.4: Connecting M.2/PCIe/mPCIe Drives

The Falcon-NEO2 offers an optional PCIe adapter kit (part number F-ADP-PCI-FN-KT), which includes adapters for M.2, mini PCIe, and a PCIe extender cable.

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

You can connect an external optical drive to the Source USB port. The Falcon-NEO2 will then be able to image the contents of CDs, DVDs, or Blu-ray discs.

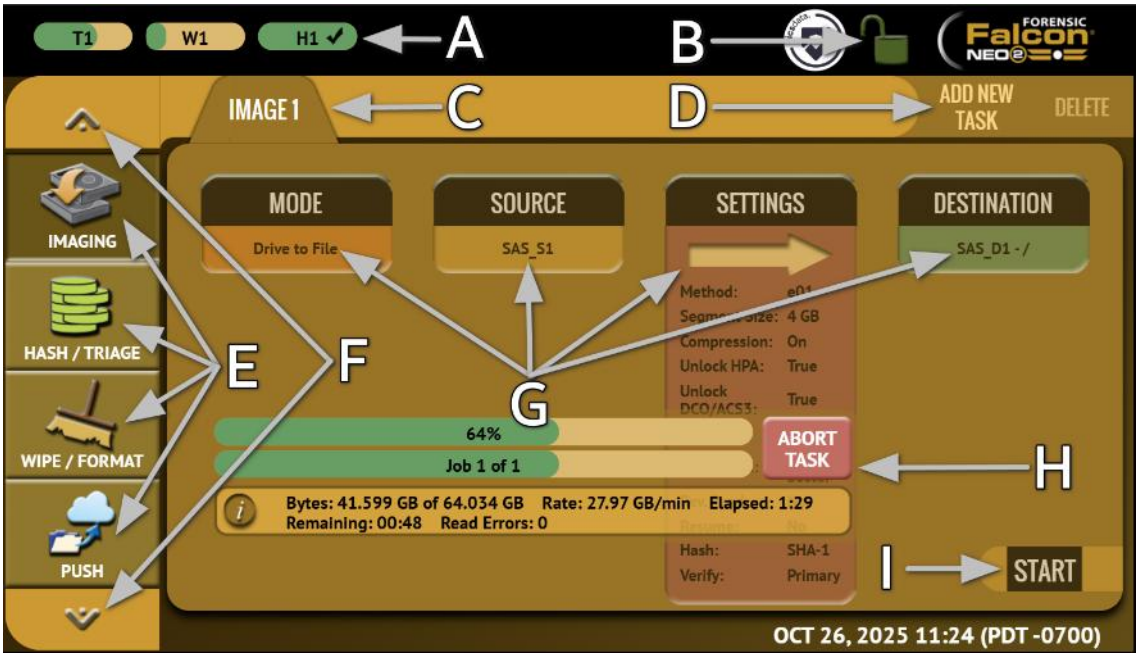
While most USB optical drives are expected to function (though some may need external or additional power), Logicube has specifically tested and approved the following model:

- Pioneer BDR-XS06 (requires external power)

Multisession support: The Falcon-NEO2 supports imaging from a multisession CD (as a Source). However, forensic analysis software may not support reading multi-session data. Please check with your forensic analysis software manufacturer to determine if it supports reading multi-session data from CDs.

2.3: The User Interface

The user interface (UI) is designed for quick and easy command input. It features a simple, intuitive layout with familiar icons representing tasks, operation modes, and scrolling functions. The UI is organized to guide users smoothly 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-NEO2 has two front USB 3.2 ports, an HDMI port, two 10GbE ports, and two DC power ports.

2.5: Front Ports

The Falcon-NEO2 features two front USB 3.2 ports that offer several functions, including, but not limited to:

- They can be used as two extra USB 3.2 destination ports (USB_D3 and USB_D4).
- They support the connection of peripherals like USB keyboards and mice.

2.6: Rear Ports

The Falcon-NEO2 includes two DC power ports, two 10 GbE ports, and an HDMI port.

2.6.1: DC Power Ports

The Falcon-NEO2 has two DC power ports. The included AC adapter/power supply can be connected to either port to provide power to the Falcon-NEO2. Two ports are also available for possible future power scaling requirements.

2.6.2: Dual 10GbE Ports

The Falcon-NEO2 is equipped with two 10 GbE (Gigabit Ethernet) ports, LAN_1 and LAN_2, to deliver high-speed network performance. These ports support a variety of configurations, such as:

- Connecting each port to a separate NAS device for simultaneous high-speed data transfers.
- Linking one port to a NAS and the other to a suspect's network, enabling secure evidence acquisition while maintaining network isolation.
- One port can connect to a work network for remote management of the Falcon-NEO2, while the other port is connected to a NAS or storage destination.

This dual-port setup allows users to optimize data throughput, minimize network bottlenecks, and securely separate source and destination networks during forensic imaging or network traffic capture tasks.

2.6.3: HDMI

The Falcon-NEO2's rear panel includes a standard Type-A HDMI port. Connecting an HDMI cable to an external HDMI-compatible display will automatically mirror the output on both its screen and the connected monitor.

When using an HDMI monitor, plug a USB mouse into one of the Falcon-NEO2's front USB ports. This mouse can then navigate the graphical user interface (GUI) while viewing the output on the external display.

2.7: Touch Screen

The Falcon-NEO2 features a 7-inch color LCD capacitive touch screen that allows users to enter commands easily. The display is bright, clear, and responsive to swipe gestures, ensuring intuitive navigation.

Section 3: Quick Start Guide

This section provides a basic introduction and step-by-step instructions for performing various operations with the Falcon-NEO2, including imaging, hashing, and wiping. For detailed information on each operation, menu option, and screen, please refer to ***Section 4: Imaging***, ***Section 4: Hash / Triage***, and ***Section 5: Types of Operation***.

3.1: General Information

The Falcon-NEO2 can manage up to five simultaneous tasks for imaging, hashing, and wiping operations.

The passwords for built-in accounts can be changed. ***Section 6.10.2.2*** details how to change the passwords for the built-in user accounts.

The speed at which the Falcon-NEO2 performs imaging, hashing, and wiping tasks depends on several factors, including:

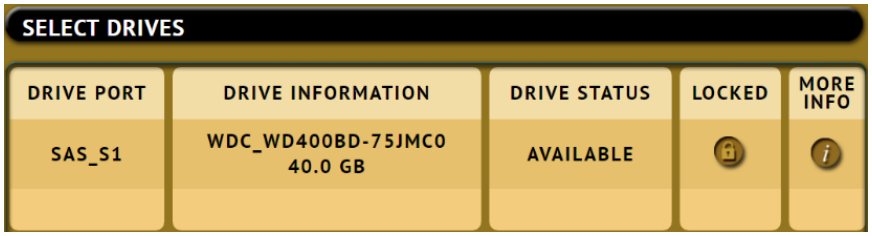
- The manufacturer's specifications of the drives being used
- The age of the drive (manufacturing date)
- The history of the drive's usage.

For example, a 2 TB drive with a 64MB cache, manufactured two years ago, will likely operate more slowly than a brand-new 2 TB drive from the same manufacturer, even if both drives are 7200 RPM, have 64MB of cache, and use SATA III.

3.1.1: ATA Security-Locked Drives

Drives secured with the ATA security standard can be temporarily unlocked with the correct password.

When selecting drives (either as Source or Destination), any drive locked with ATA security will display a locked icon in the LOCKED column.

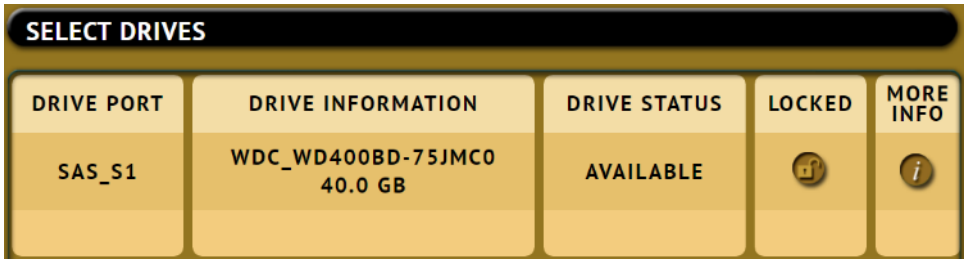


While a drive is locked, its contents remain inaccessible. Locked drives cannot be imaged, hashed, or wiped until unlocked.

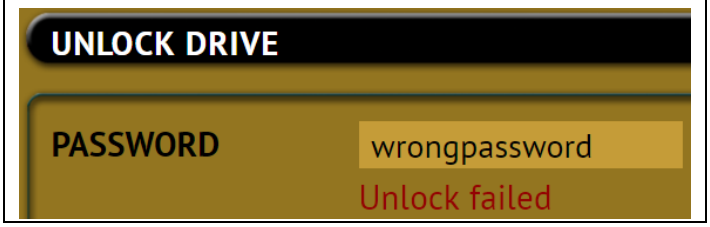
To temporarily unlock a drive, tap the locked icon. This will bring up the UNLOCK DRIVE screen:



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



If the password is incorrect, an 'Unlock failed' message will appear:



Once the drive is unlocked, it can be used for cloning (as either Source or Destination), hashing, or wiping operations.

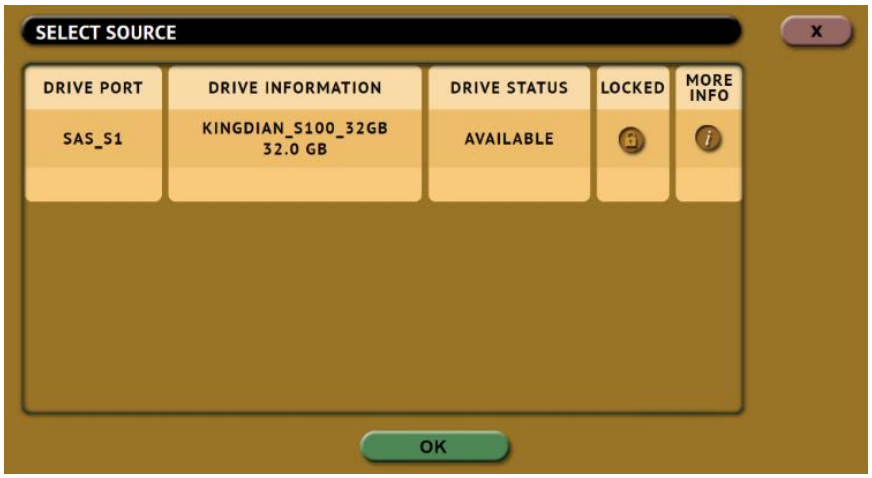
The drive will stay unlocked temporarily until it is disconnected or powered off. If you disconnect and reconnect the drive, it will lock again. Performing a Secure Erase wipe while the drive is unlocked permanently removes the password lock.

3.1.2: Encrypted Drives and Partition Detection

The Falcon-NEO2 can detect whether a source drive is encrypted or contains one or more encrypted partitions.

When a source drive that may be encrypted is connected, a locked icon will be displayed next to the drive in the Source drive selection screen when using the following modes:

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

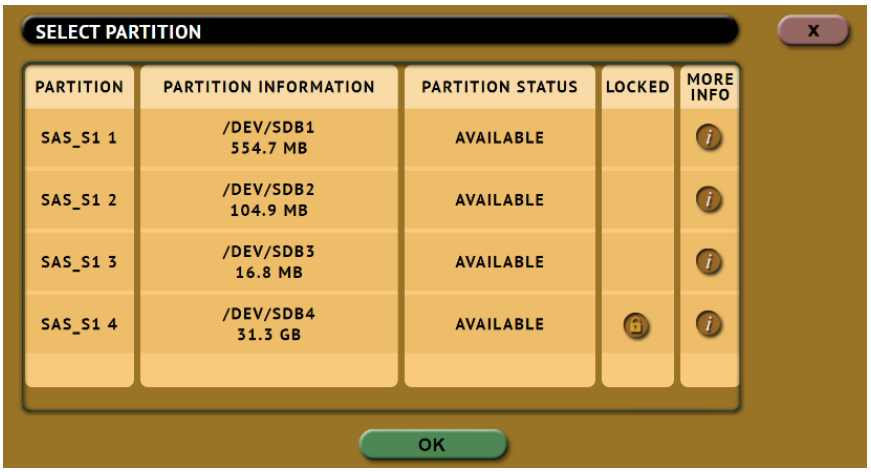


From the ***Select Source*** screen, clicking on the ***Locked*** icon will bring up the following message:



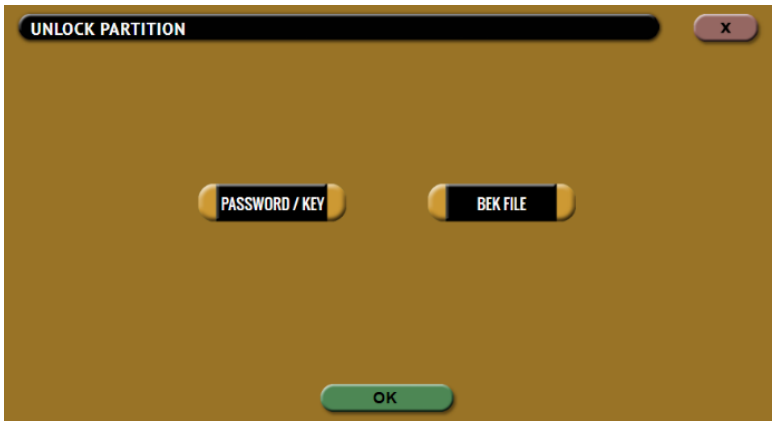
The Falcon-NEO2 can determine whether the Source drive might have full-disk encryption or if a partition is encrypted. However, the only types of encryption it can recognize and unlock now are BitLocker, VeraCrypt, TrueCrypt, and OPAL.

To unlock an encrypted partition, go to ***Partition to File***. In the ***Select Partition*** screen, possibly encrypted partitions will also show a locked icon:



Clicking on the ***Locked*** icon will bring up different screens depending on the scenario:

- **BitLocker:** If the partition is encrypted with BitLocker, the screen will show options to unlock the partition (Password/Key or BEK file).



- **Unidentified encryption or drive-level encryption:** One of the following messages will appear when the drive's encryption is unidentified or there is drive-level encryption:
  - This drive is possibly encrypted or contains one or more encrypted partitions.
  - This device has been marked possibly encrypted due to detecting highly random data.

3.2: Imaging



This operation enables imaging a Source drive to one or multiple Destinations. Six distinct imaging modes and various settings are available. These options should be selected sequentially from left to right.

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

DD, E01, EX01, and DMG files generated on the Destination may be smaller than the specified segment size. For instance, if you select a 4GB segment size, some files might still be under 4 GB. This typically happens when the Source drive contains significant unused or blank space.

- **Drive to File:** This function creates an image of the Source drive in one of the following formats: DD, E01, EX01, AFF4, or DMG. Compression options are available for the E01, EX01, and AFF4 formats.
- **File to File (Targeted Imaging feature):** The Falcon-NEO2 can speed up acquisition by creating a logical image using preset filters, custom filters, file signature filters, or keyword searches to select and capture only the specific files required. Output options include Directory tree, MFT report, L01 archive, LX01 archive, and ZIP archive. The MFT report lists deleted files (if any), which may be recoverable.

  APFS (Apple File System) can be imaged in File to File mode. To do this, go to System Settings > Advanced tab and enable APFS before starting the task.

- **Partition to File (Logical Imaging):** This mode creates an image of a specific partition from the source drive and saves it in several formats, including DD, E01, EX01, or DMG. Compression is available when using E01 or EX01 formats. This mode also supports BitLocker decryption (with the required passphrase, recovery key, or BEK file), ensuring the resulting image is not encrypted.
- **Net Traffic to File:** This function captures network traffic, internet activity, and VOIP data by sniffing packets on a connected network. The captured network data is saved in the .pcapng file format to a destination drive attached to the Falcon-NEO2.
- **Drive to Drive:** This performs a bit-for-bit duplication of the source drive, producing an exact copy. It is also known as a native or mirror copy.
- **File to Drive (Image Restore):** This function restores images in DD, E01, EX01, or DMG formats created by the Falcon-NEO2 to another drive.
- **Mobile to File:** Backs up data from mobile phones.
  - **For serial numbers 223000 and above –** This is a standard, built-in feature.
  - **For serial numbers below 223000 –** Available as an annual, renewable software subscription.

Unlocking HPA, DCO, or ACS3: When imaging using Drive to File, Partition to File, or Drive to Drive modes, the Falcon-NEO2 can unlock Host Protected Area (HPA), Device Configuration Overlay (DCO), or ACS3 features.

Concurrent Image+Verify Process: The Falcon-NEO2 can image and verify data simultaneously. When verification is enabled, imaging and verification occur concurrently, which can significantly reduce the total imaging time, potentially by up to half, especially when the destination drives are faster than the source.

3.2.1: Step-By-Step Instructions – Imaging

Details for each selectable option on the Image screen are provided in ***Section 4: Imaging***.

1. Choose ***Imaging*** from the list of operation types on the left.
2. Tap the ***Mode*** icon, select one of the six available modes, and confirm by tapping the ***OK*** icon.
3. Tap the ***Source*** icon, pick the desired source from the list of connected drives, and tap ***OK***.
4. Tap the ***Settings*** icon to configure options such as Case Info, File Image Method or Mirror Settings, HPA/DCO/ACS3/TRIM, Error Handling, and Hash/Verification Method, then tap OK.

The Settings screen will be different for each of the two modes. Details on the different Settings screens can be found in ***Section 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.

When creating the log or file names, the Falcon-NEO2 will convert any non-POSIX portable characters used in the Case/File Name field to underscores (_).

POSIX portable characters are:

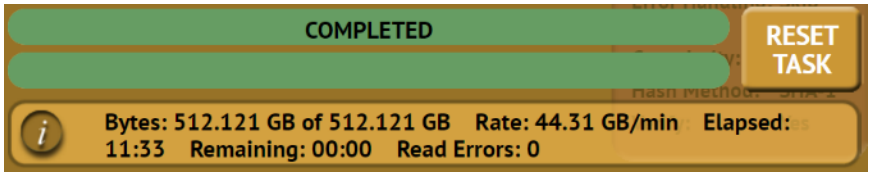
Uppercase A to Z	Period (.)
Lowercase a to z	Underscore (_)
Numbers 0 to 9	Hyphen/Dash (-)

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

For DD, E01, Ex01, and DMG, the Falcon-NEO2 must be used to format drives. If the Falcon-NEO2 does not format the Destination drive, 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". Tap Reset Task to reset the task so the drive bays properly reset and will 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 exact number of bytes being processed. When 'Verify' is set to "Yes", the reported number will double in size.

3.2.2: Imaging BitLocker-Encrypted Drives

Source drives encrypted with BitLocker can be decrypted so that the resulting DD, E01, EX01, or DMG image files contain unencrypted data. To unlock a BitLocker-encrypted drive, you must provide either:

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

Parallel imaging is not supported with unlocked BitLocker-encrypted drives, but is supported when the encrypted partitions remain locked.

Drives can be encrypted using BitLocker encryption, with or without FIPS-compliant encryption. When a drive is encrypted, a recovery key and a password are created, and the administrator or end user can generate the password.

The Falcon-NEO2 can unlock and image FIPS-compliant encrypted drives if the Falcon-NEO2 user can create a new *.BEK (BitLocker Encryption Key) file in Windows. To create a new *.BEK file:

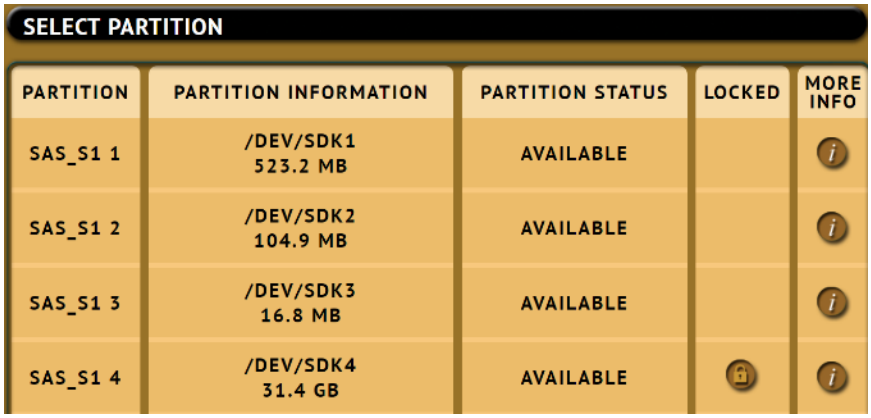
- The user would need the original Recovery Key or the password associated with the drive.
- The BitLocker-encrypted drive must be connected to a Windows computer (the user must have administrative rights).
- A 2nd encryption key will need to be created and then saved to an external storage device (such as a USB flash drive) or to a computer connected to the same network the Falcon-NEO2 is connected to.

See ***Section 3.2.2.2*** for details on how to create the *.BEK file using the original Recovery Key or password associated with the drive.

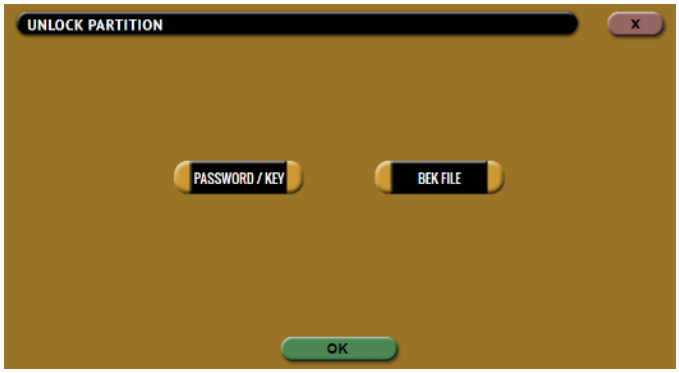
Since BitLocker encrypts volumes, unlocking the BitLocker-encrypted volume requires going through the ***Partition to File*** mode.

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, choose the BitLocker-encrypted source drive from the list of connected drives, and then tap the ***OK*** icon.
4. The 'Select Partition' screen will appear. Any BitLocker-encrypted partition will have the 'Locked' icon in the LOCKED column.



5. To unlock the encrypted volume, choose a partition 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:



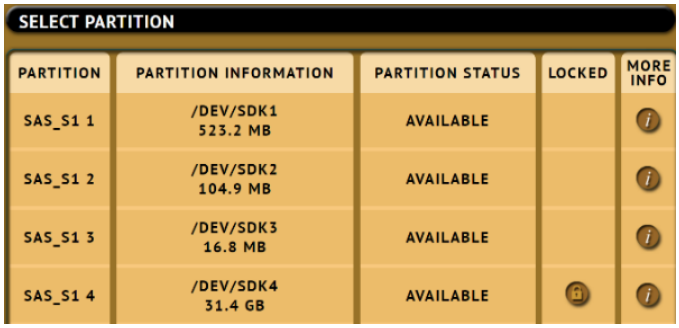
3.2.2.1: Password/Key

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



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

The screen will return to the 'Select Partition' screen if the password is correct.

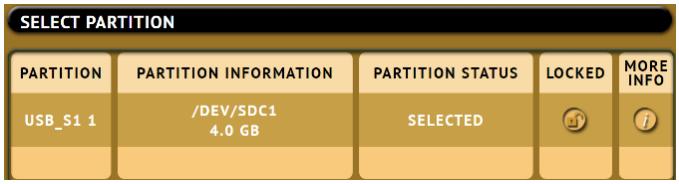


The icon in the 'Locked' column may still appear locked, even though the partition is unlocked, but the partition will be unlocked.

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.



After unlocking a BitLocker-encrypted partition, you can continue with the Partition to File imaging process or switch to Drive to File mode to image the entire drive, including any other partitions present. Once the encrypted partition is unlocked, selecting Drive to File will create an image of the whole drive, capturing all partitions, including the previously encrypted one.

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

4. Tap the ***Destination*** icon, select the destination(s) to be used, and 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". Tap Reset Task to reset the task so the drive bays properly reset and do not show as being used or assigned for other tasks.

3.2.2.2: 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 encrypted drive's BitLocker header, 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 with 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)"

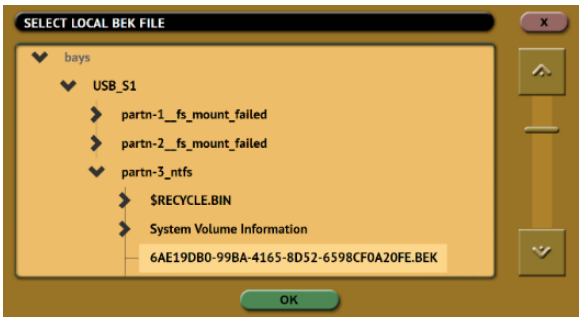
6. The *.BEK file can be saved to an external storage device (such as a USB flash drive) or to a computer connected to the same network the Falcon-NEO2 is connected to.

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

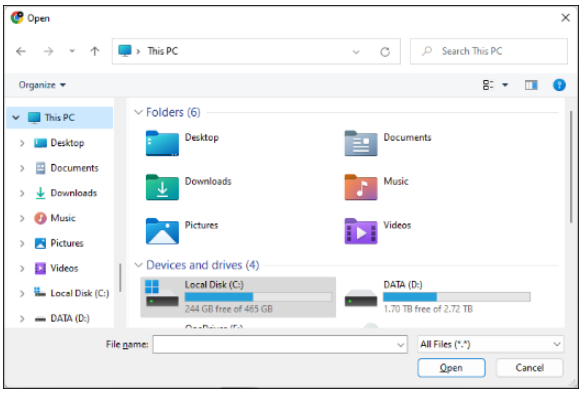


There are two selections on this screen:

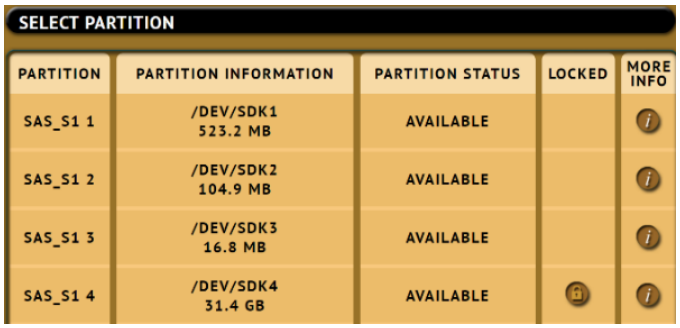
- **SELECT LOCAL FILE –** Choose this if the BEK file is on a drive connected to one of the Source ports on the Falcon-NEO2. A file browser screen will appear, allowing the user to locate and select the BEK file:



- **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-NEO2 is connected to. Depending on the Operating System of 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 return to the 'Select Partition' screen.

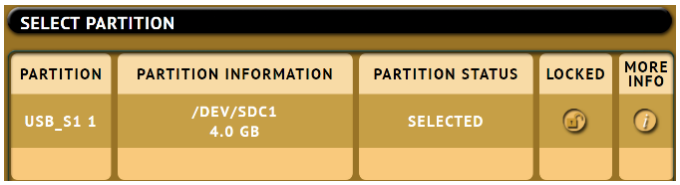


The icon in the 'Locked' column may still appear locked, even though the partition is unlocked, but the partition will be unlocked.

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



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 on the drive. Since the encrypted partition has been unlocked, selecting the whole source drive using Drive to File will image the entire drive, including the unlocked partition.

1. Tap the Settings icon and adjust the settings as needed (Case Info, File Image Method Settings, Mirror Settings, HPA/DCO/ACS3/TRIM, Error Handling, Hash/Verification Method, etc.), then tap the OK icon.
2. Tap the ***Destination*** icon, select the destination(s) to be used, and 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 complete, the status will show "COMPLETED." It is advisable to tap Reset Task to reset the task, allowing the drive bays to reset properly so they do not appear as being used or assigned for other tasks.

3.2.3: Targeted/Logical Imaging

The Falcon-NEO2 can perform targeted or logical imaging using File to File mode. It can image only the files identified within the filters by applying various filters. Output formats include AFF4, L01, LX01, Directory Tree, and Zip Archive. An MFT report can be generated to 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, 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, select the destination(s) to be used, and 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 that you tap Reset Task to reset the task, ensuring that the drive bays reset properly and do not appear as being used or assigned to other tasks.

3.2.4: Imaging To or From a Network

To image to or from a network repository or location with the Falcon-NEO2, you must first configure the network repository. Depending on the type of repository added (such as SMB, CIFS, or iSCSI), it will be available as a Source, a Destination, or both.

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

3.2.5: Cloud Storage Acquisition

Cloud storage needs to be configured through the Manage Repositories screen. After setting up a supported cloud storage service, you can image files from the cloud storage using the File to File imaging mode.

3.2.6: Mobile Device Capture

For serial numbers 223000 and above – This is a standard, built-in feature.

For serial numbers below 223000 – Available as an annual, renewable software subscription. Contact sales@logicube.com or your region's international reseller for additional information. For a list of international resellers, visit https://www.logicube.com/sales/international-sales/.

This capture uses the ***Mobile to File*** mode and acquires data from iOS devices (up to iOS 18.x at the time of this writing) and Android devices (4.0 and above).

For iOS devices – Performs an iTunes backup, which may include:

- Call logs
- iMessages
- SMS & MMS
- Photos and videos
- Contacts
- Website history
- Wi-Fi settings
- Deleted SMS, iMessages, photos, and WhatsApp contacts

For Android devices – The capture method will depend on whether the Android device is rooted or not:

- **Rooted Android devices –** A physical acquisition is performed. Data output will result in a single dd file.
- **Unrooted Android devices –** A logical acquisition is performed. This is limited to contacts, call logs, SMS, and calendar.

Falcon-NEO2 users can root Android devices using third-party tools at their own risk.

3.2.7: Imaging Net Traffic

The Falcon-NEO2 can capture network traffic data using its Net Traffic to File imaging mode. This feature lets you record local network activity, internet usage,

and VOIP communications. The captured data is saved in the *.pcapng file format, which can be analyzed with tools like 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 remote access to the Falcon-NEO2.

1. Select ***Imaging*** from the types of operation on the left side.
2. Tap the ***Mode*** icon, select Net Traffic to File, and 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 ***Section 12: Net Traffic***.

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

3.2.8: Imaging Resume Feature

The Falcon-NEO2 includes a resume feature for Drive to Drive, Drive to File, and Partition to File imaging modes. If an imaging task is interrupted, this feature allows the user to either resume or restart the process when any of the following interruptions occur:

- The task is aborted
- Power to the Falcon-NEO2 is interrupted

To resume an imaging task:

1. Make sure the same drives are connected to the same ports.
2. Make sure the Imaging settings are set as they were when the task was interrupted.
3. Start the task. When the same imaging task is set up 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:



3.2.9: Auto Resume Feature

An auto-resume feature is available when using Drive to Drive, Drive to File, or Partition to File imaging modes. If Auto Resume is enabled, the imaging task will automatically continue after an interruption without prompting the user to resume or restart the process.

To set the Auto Resume feature:

1. In the Drive to Drive, Drive to File, or Partition to File screen, go to ***Settings***.
2. Go to the ***On Error*** section.
3. Set the ***Auto Resume*** section to ***YES*** (the default setting is ***NO***).

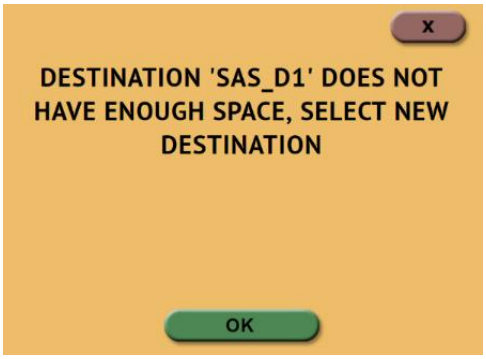
3.2.10: Drive Spanning

The Falcon-NEO2 can automatically span data across multiple destination drives using Drive to File, File to File, Partition to File, or Net Traffic to File modes with DD, E01, EX01, or DMG formats.

Selected destination drives that may not have enough space at the start of a task will display a warning to let you know that available space could be insufficient.



When the destination drive becomes full and there isn't enough space for the remaining data, the Falcon-NEO2 will prompt you to provide another drive.



When this prompt appears, tap the OK icon to go to the Select Repository screen. You can then disconnect the destination drive and connect a new one, or select a different destination port or repository. After choosing the new destination, tap the OK icon to continue.

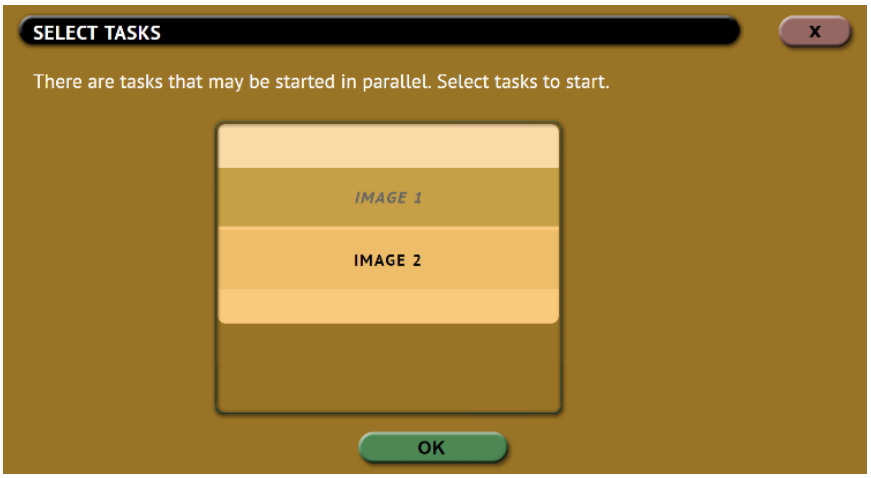
After the imaging process, all additional destination drives or repositories will retain the same Case/File name, and the sequence of DD, E01, EX01, or DMG files will continue. For instance, if the final file on the first destination is *.E23, the next destination or repository will begin with *.E24.

3.2.11: Parallel Imaging

The Falcon-NEO2 supports parallel imaging, enabling users to carry out multiple imaging tasks simultaneously from a single source drive to various destinations, each in a different imaging format. For example, you can image to a network location or a destination drive in E01 format while simultaneously imaging to another destination drive in native/mirror or DD format.

Parallel imaging is unavailable when BitLocker-encrypted drives are unlocked, but it is supported if encrypted partitions remain locked.

To use parallel imaging, you must configure all intended imaging tasks before initiating the first imaging operation.



When a task is started and the same source drive is selected for multiple imaging operations, a notification screen will appear indicating that parallel tasks are available. The user can then choose one or more tasks to run simultaneously.

3.2.12: Blank Disk Check

The Falcon-NEO2 can verify whether the device has wiped a drive using its blank disk check feature. However, this check may not be reliable if the drive was erased with Secure Erase. To conduct a blank disk check:

1. Connect a drive to the Falcon-NEO2.
2. Choose Imaging, Hash, or Wipe/Format.
3. List the connected drives by Source, Destination, or 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 to the screen's right to scroll down to the second information page.
6. Locate the line that shows “Wiped”. This will either show ***True*** (drive is blank) or ***False***.



3.3: Hash / Triage



You can perform a hash, verify, or triage operation on any drive or case, including DD, E01, EX01, or DMG images created by the Falcon-NEO2. Running a hash or verify task instructs the Falcon-NEO2 to compute the hash for the selected drive or case. The Triage function allows users to import one or more Hash Databases and scan source drive files for any matching hash in the database. The following modes are available:

> ***Section 5: Hash/Triage*** provides information on the different screens in the Hash/Triage operation.

Triage is a standard, built-in feature for Falcon-NEO2 units **with serial numbers 223000 and above**.

For serial numbers under 223000, Triage is available with a one-time, optional purchase. Contact sales@logicube.com or your region's international reseller for additional information. For a list of international resellers, visit https://www.logicube.com/sales/international-sales/.

- **DRIVE HASH –** This mode calculates a hash for any connected drive on an active source or destination port, based on Logical Block Addresses (LBA). If multiple drives are selected, the Falcon-NEO2 will hash up to the LBA count of the smallest drive. For drives of different capacities, it is recommended that separate tasks be run for each drive.
- **CASE VERIFY –** This mode verifies the hash of cases or images created by the Falcon-NEO2 (DD, E01, EX01, DMG). There are two settings:
  - **Primary –** Verifies the primary hash of the image. Use this if only one hash was selected during imaging.
  - **Both –** Verifies the primary (SHA-1) and secondary hash values. Use this if dual hashing was enabled when the image was created.
- **TRIAGE –** Import one or more Hash Databases and then triage a source drive to determine if any files on the drive match hashes in the database. Positive results will show a successful message, and all matches will be listed in the audit log file.

  Supported hash databases:
  - VICS Hash Databases
  - Comma Separated Values
  - X-Ways Hash Databases

3.3.1: Step-By-Step Instructions – Drive Hash

1. Select ***Hash/Triage*** from the types of operation on the left side.
2. Select the ***Mode*** icon and select ***Drive Hash***.
3. Select the ***Drives*** icon, select the drive(s) to be hashed, and then tap the ***OK*** icon.
4. Tap the ***Settings*** icon to choose the different settings based on the Mode selected. Details for every setting can be found in ***Section 5.3.1***.
5. Change any of the optional settings as 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. When finished, the status will show "COMPLETED." You should tap Reset Task to reset the task, ensuring the drive bays are properly reset and do not appear as being used or assigned for other tasks.

3.3.2: Step-By-Step Instructions – Case Verify

1. Select ***Hash/Triage*** from the types of operation on the left side.
2. Select the ***Mode*** icon and select ***Case Verify***.
3. Select the ***Case*** icon, select the drive containing the case/image file to be hashed, and then tap the ***OK*** icon.
4. Select the case filename, then tap the ***OK*** icon.
5. Tap the ***Settings*** icon to choose the different settings based on the Mode selected. Details for every setting can be found in ***Section 5.3.2***.
6. Change any of the optional settings as needed.

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 case verify task. When finished, the status will show "COMPLETED." You should tap Reset Task to reset the task, ensuring the drive bays are properly reset and do not appear as being used or assigned for other tasks.

3.3.3: Triage - Introduction

The Triage function supports the following types of Hash Databases:

- VICS Hash Database
- Comma-Separated Values Hash Database
- X-Ways Hash Database

A sample database is pre-loaded on the Falcon-NEO2. As long as there is at least one database on the Falcon-NEO2, the TRIAGE button will be clickable.



If all databases on the Falcon-NEO2 are deleted, the TRIAGE button will be disabled:



To re-enable the TRIAGE button, import and convert a hash database by going to the ***SETTINGS*** screen and then to the HASH DB tab (the 10th tab).

3.3.3.1: Creating a CSV Hash Database

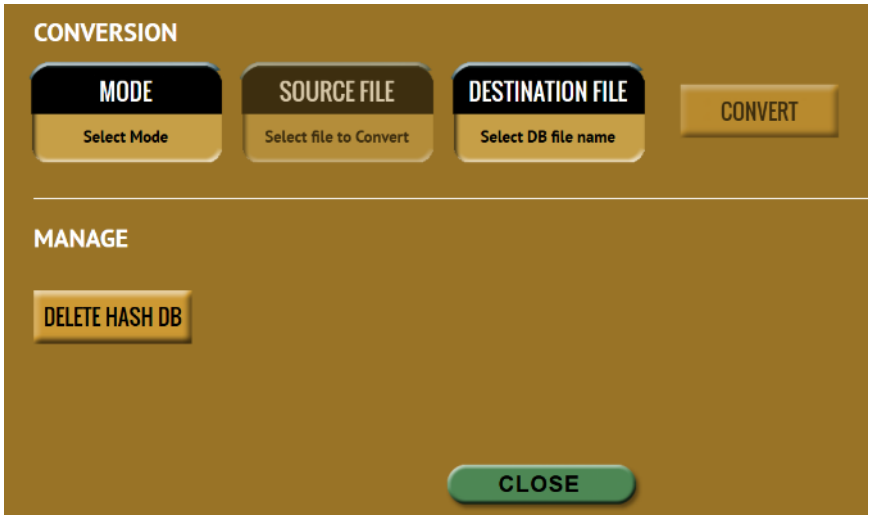
There are several articles on the Internet on how to create a Comma-Separated Value (CSV) file. For the Falcon-NEO2, a valid CSV hash database can be imported/converted for use with the Triage function. The CSV file must follow the following requirements:

- Comments: Comments are only supported at the beginning of the CSV file.
- Values/Columns: Value/column requirements can be any one of the following:
  - Maximum 4 columns where the MD5 and SHA1 hashes are the 2nd and 3rd columns:
    [xxx],MD5,SHA1,[xxx] or [xxx],SHA1,MD5,[xxx]
  - MD5 single column
  - SHA1 single column
- MD5 and SHA1: Hashes may be all capital letters or all small letters
- Delimiters: The following delimiters can be used between values/columns:
  - Commas (,)
  - Tabs (\t)
  - Semicolon (;)
  - Single vertical bar or Pipe (|)

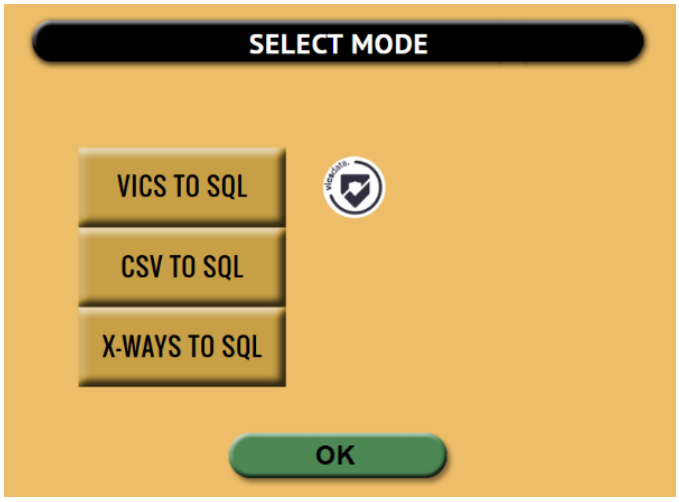
3.3.3.2: Importing and Converting a Hash Database

The VICS, CSV, or X-Ways Hash Database should be saved to a drive that can be connected to the Falcon-NEO2 (for example, a USB flash drive).

In the ***SETTINGS*** screen, click the ***HASH DB*** tab (10th tab). From the HASH DB tab, you can see the ***CONVERSION/MANAGE*** screen. This ***CONVERSION/MANAGE*** screen can also be accessed from the HASH/TRIAGE screen, in the ***TRIAGE*** mode, ***SETTINGS*** screen, ***HASH DB*** screen.



1. Tap or click the ***MODE*** button. The ***SELECT MODE*** window will appear.



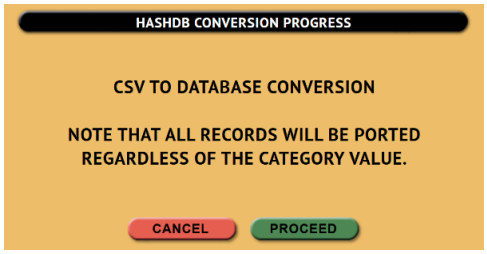
2. Select the type of hash database to import and convert (VICS, CSV, or X-WAYS), then tap or click the ***OK*** icon. The screen will go back to the ***CONVERSION/MANAGE*** screen.
3. Tap or click the ***SOURCE FILE*** button. A ***SELECT FILE TO CONVERT*** window will appear.



4. Select the drive/port where the hash database is located, then locate and select the Hash Database file to import and convert. Tap or click ***OK***. The screen will go back to the ***CONVERSION/MANAGE*** screen.
5. Tap or click the ***DESTINATION FILE*** button. The ***HASHDB FILE NAME*** window will appear.



6. Enter a file name for the Hash Database, then click ***OK*** to continue. The screen will go back to the HASH DB tab. The requirements for the file name are:
    - Capital letters or small letters
    - Numbers
    - Underscore (_)
    - Spaces and other special characters are not supported
    - The maximum number of characters for the file name is 125.
7. Tap or click the ***CONVERT*** button. A message similar to the one below will appear. Tap or click ***PROCEED*** to continue.



8. The Falcon-NEO2 will start converting the Hash Database to a format the Falcon-NEO2 can use.



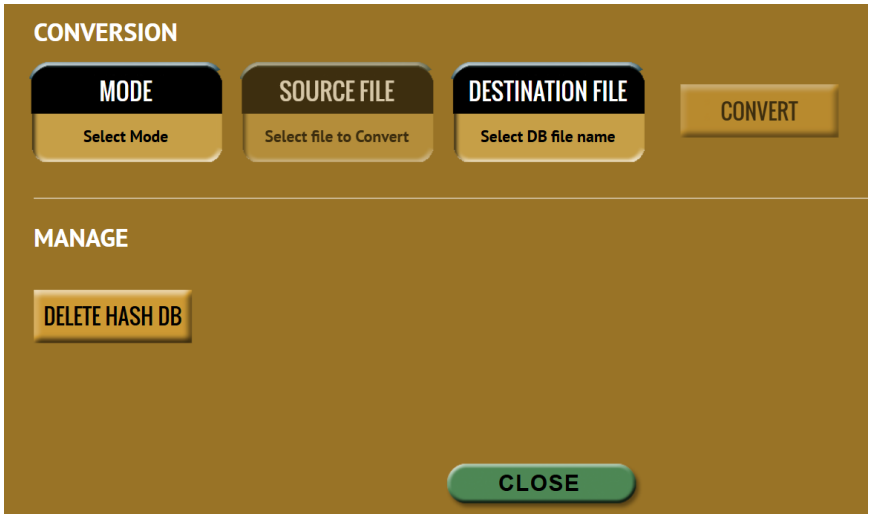
9. After a few moments, depending on the size of the Hash Database file to convert, the conversion will show a successful message if the file conversion is successful. Tap or click ***OK*** to continue. The screen will go back to the ***CONVERSION/MANAGE*** screen.



10. Tap or click ***CLOSE*** in the ***CONVERSION/MANAGE*** screen when all Hash Databases have been converted.

3.3.3.3: Deleting a Hash Database

Users may occasionally want to delete previously imported Hash Databases. They can be deleted in the ***CONVERSION/MANAGE*** screen.



3.3.3.4: Starting a Triage

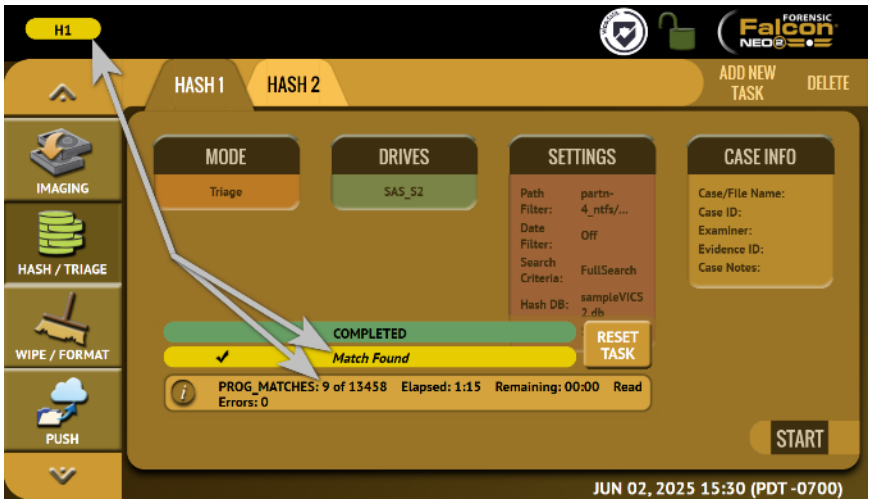
1. Select ***Hash/Triage*** from the types of operation on the left side.
2. Select the ***Mode*** icon and select ***Drive Hash***.

3. Select the ***Drives*** icon, select the drive with the files to compare against the VICS Hash Database, then tap the ***OK*** icon.
4. Tap the ***Settings*** icon to choose the different settings based on the Mode selected. Details for every setting can be found in ***Section 5.3.3***.
5. Change any of the optional settings as needed.

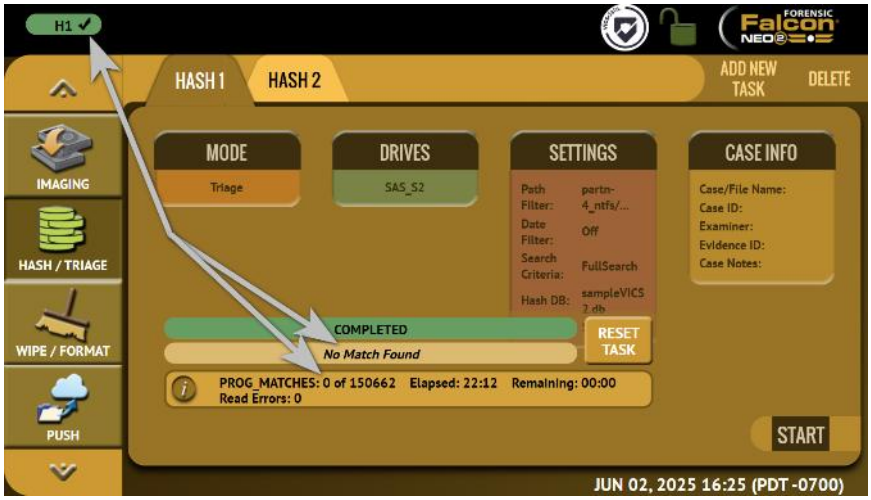
Optional: Tap Case Info to set the Case/File Name, Case ID, Examiner, Evidence ID, or Case Notes.

6. Tap the ***Start*** icon to start the triage. When finished, the status will show "COMPLETED."

The following is an example of a status screen when files are found that match hashes in the VICS Hash Database. When a match is found, the task icon on the top of the screen will have a ***yellow background***. In the status bar at the bottom, the second line will have a yellow background and a message indicating ***Match Found***. At the bottom of the status bar, it displays the number of matched files and the number of files compared to the VICS Hash Database.



The following is an example of a status screen when no files match the hashes in the VICS Hash Database. When no match is found, the task icon on the top of the screen will have a ***green background***. In the status bar at the bottom, the second line will have a white background and a message indicating ***No Match Found***. At the bottom of the status bar, it should display zero (0) matches and the number of files compared to the VICS Hash Database.



3.4: Wipe/Format



The Falcon-NEO2 allows you to wipe and format destination drives. Before using a drive as a destination in Drive to File, File to File, Partition to File, or Net Traffic to File modes, it must be formatted. The Wipe menu offers the following methods for this process:

> ***Section 6.3: Wipe/Format*** provides details on the different screens involved in the Wipe/Format operation.

- ***Secure Erase*** – Issues a command to the drive, directing it to carry out a secure erase according to the manufacturer's specifications.

  > Contact the hard drive manufacturer for Secure Erase specifications for each model/type.
  >
  > Secure Erase will not work on drives connected through the USB or I/O ports (Thunderbolt).

- ***Wipe Patterns –*** Users can define a custom wipe pattern for the drive, with the option to select up to seven passes and specify the data written for each pass. A 7-pass DoD wipe can be configured using preset values. The Falcon-NEO2 also offers a setting to verify the value written during each pass. Additionally, it can wipe areas such as HPA, DCO, or ACS3 if needed.
- ***Format –*** Drives attached to the Falcon-NEO2's Destination ports can be formatted with or without encryption using the following file systems: NTFS, EXT4, exFAT, FAT32, EXT3, EXT2, and HFS+.

3.4.1: 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's recommended to use drives of the same capacity for each task. If you wipe drives of different sizes together, the smaller drives will finish first, but their ports will stay occupied until the entire wipe process for all drives is complete.

3. Tap the Settings icon and select the desired wipe method (Secure Erase and/or Wipe Patterns). If you choose Wipe Patterns, specify the pattern type you want to use (DoD or Custom).

Optional: If the drive contains an HPA, DCO, or ACS3 area that should be wiped, tap the HPA/DCO/ACS3/TRIM icon and choose Yes to erase these areas on the drive.

4. Tap the ***Passes*** icon to edit the number of passes and what gets written on each pass.
5. 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-NEO2 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 ***Section 8: Drive Encryption and Decryption***.

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 Wipe task. The Falcon-NEO2 will perform a Secure Erase first (if selected), then a Wipe Pattern (if selected), and finally a Format (if selected). 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 do not show as being used or assigned for other tasks.

3.5: Push



The Push operation enables users to transfer evidence created by the Falcon-NEO2 to or from drives connected to the device and a Falcon-NEO2 repository or network location. This feature offers enhanced security compared to traditional file copying by allowing data verification during the transfer. For each push process, the Falcon-NEO2 also generates a log file.

Details on the screens in the Wipe/Format operation can be found in ***Section 6.4: Push***.

3.5.1: Step-By-Step Instructions - Push

A network repository must be set up to push files to a network location. ***Section 6.9.1*** provides details on this.

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.
3. A 'Select Cases' screen will show each case name on the selected source. Tap each case name to select one or more cases. 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 which you want to push the images. 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 do not show as being used or assigned for other tasks.

3.6: Task Macro



This operation supports configuring up to five (5) macros. Each macro can execute up to nine (9) tasks in sequence, one after the other. For instance, you can set up a macro to perform a Wipe, followed by Imaging, and then Hashing, all in order.

Details on the screens in the Wipe/Format operation can be found in ***Section 6.5: Task Macro***.

3.6.1: Step-By-Step Instructions – Task Macros

Before creating a macro, each task or operation must be configured. For instance, if you want to make a Task Macro that performs a wipe and then an image, you must first set up both the wipe and image tasks. After configuring these tasks (e.g., Wipe 1 and Image 1), you can set up the Task Macro.

1. Select ***Task Macro*** from the types of operation on the left side.
2. Select a macro (Macro 1 through Macro 5).

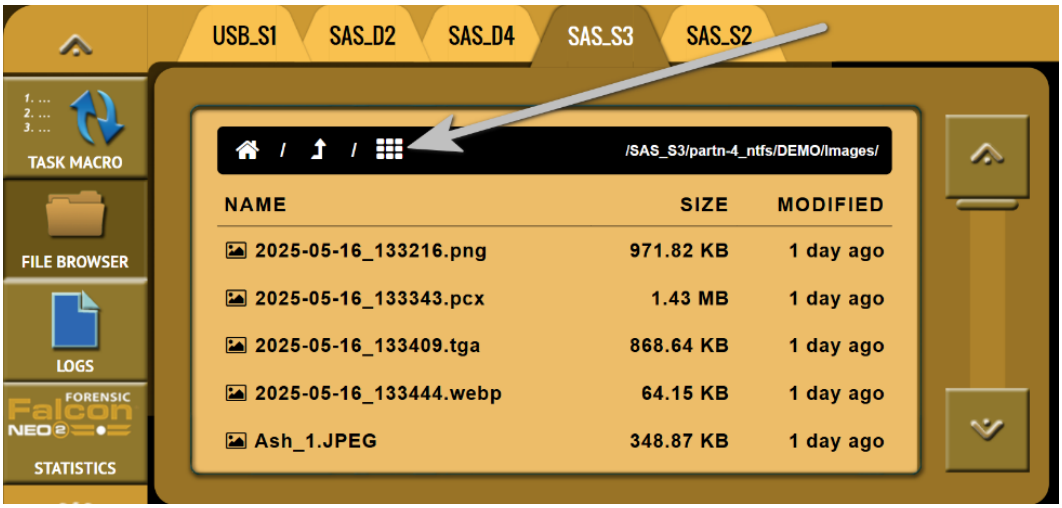
3. Tap the ***Task*** icon to select up to nine (9) operations.
4. Set up to 9 operations by tapping on each operation in order (Operation 1, Operation 2, etc.)
5. Tap the OK icon when all the operations have been set.
6. Tap the ***Start*** icon to execute the macro and perform all the operations within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

3.7: File Browser (with thumbnail view)



The contents of connected Source and Destination drives on the Falcon-NEO2 can be previewed using the Falcon-NEO2's file browser. The Falcon-NEO2 displays all partitions and the files within each partition. While only specific file types can be opened directly through the file browser, viewing these files will not modify or alter the drive in any way. Contents of DD, E01, EX01, DMG, L01 image files, ZIP, directory trees, and network repositories created by the Falcon-NEO2 can also be viewed.

Thumbnail View: Images can be displayed as thumbnails. To switch from list view to thumbnail view in the File Browser, tap or click the icon below:



For detailed information on how to use the file browser, see ***Section 6.6*** of this manual.

For Source drives, the Falcon-NEO2 displays all readable partitions.

Only those destination drives formatted by the Falcon-NEO2 are shown, along with any DD, E01, EX01, DMG, L01, ZIP, or Directory Tree files created by the device.

3.7.1: Step-By-Step Instructions – File Browser

1. Select the drive to browse from the File Browser screen by tapping the corresponding tab at the top.
2. Tap the partition or folder to browse. The Falcon-NEO2 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-NEO2 will attempt to open the file.
    - If the Falcon-NEO2 can open the file, it will be displayed on the screen.
    - If the Falcon-NEO2 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.

3.8: Logs



The Falcon-NEO2 keeps logs of all imaging, hash, wipe (or format), and push operations. Logs can be viewed directly on the Falcon-NEO2 or from a computer's browser (if the Falcon-NEO2 is connected to a network). They can also be exported to an external USB drive in PDF, HTML, and XML formats.

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

S.M.A.R.T. data logs for drives used in the ***Drive to File*** and ***Partition to File*** imaging tasks are automatically exported to the Destination drive. Two files, "pre" and "post," will be exported, capturing S.M.A.R.T. data at the beginning and end of the imaging task. S.M.A.R.T. data for Drive to Drive imaging and Wipe tasks can be exported along with the audit log files from the ***LOGS*** screen.

Log files may include a ***partial hash***, which is used internally by the Falcon-NEO2 and cannot be validated by external tools.

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

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-NEO2 and its settings
- Case info (if entered)
- Source and Destination hashes (if verify was set to YES)

3.8.1: 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 log file name. 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 log file name. 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 on the front of the Falcon-NEO2.

> 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 in HTML, PDF, and XML formats.

Repeat steps 2 and 3 for additional log files you wish to export or view. Alternatively, you can export all log files at once by tapping the Select All button to select every log file for a single export operation.

To print the log files, it is recommended that you use the web interface described in Section 9: Remote Operation. Click the print icon in the screen's upper-right corner, and your browser's print menu will appear. This menu allows you to print the log to any printer configured on your computer.

3.8.2: Viewing/downloading Log Files from the web interface

When using the web interface (see ***Section 10.1*** for details on the web interface), the log file will be viewed on a web browser. A download icon in the browser can be used to download the log file being viewed.



3.8.3: 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 it for deletion. 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.

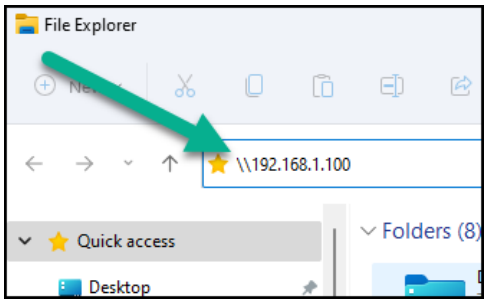
- If a log file deletion password was not created, a confirmation screen will appear confirming the deletion of the single log file or all log files.
- If a log file deletion password is created, a screen will appear prompting the user to enter the log file deletion password. Enter the log file deletion 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 ***System Settings***. ***Section 6.10.2*** provides more information about the log file deletion password.

3.8.4: Accessing the Logs Over a Network

The log files can also be accessed through a network on a computer if the Falcon-NEO2 is connected to the same network.

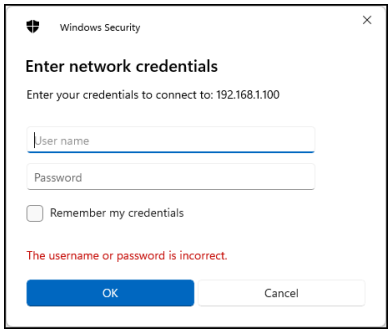
1. Open File Explorer or a similar window and browse to the hostname or IP address in the Statistics screen. As seen below, use two backslashes before the hostname or IP address.



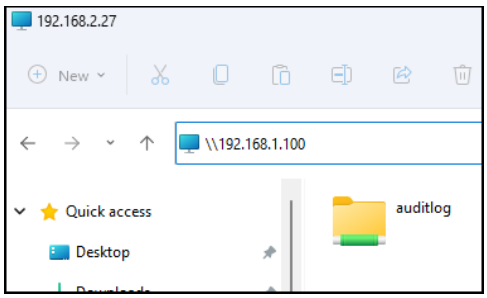
2. A Windows security screen will appear, prompting you to enter a User name and Password to connect to the Falcon-NEO2. Log in with the following credentials:

   User name: ***it***

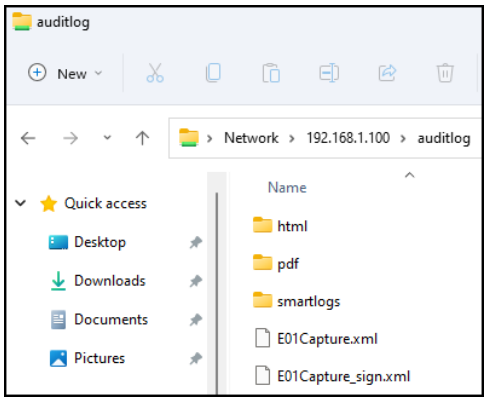
   Password ***it***



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



4. The auditlog folder contains the HTML, PDF, XML, and smartlogs files for each log file. There will be three folders (HTML, PDF, and smart logs) containing the HTML, PDF, or S.M.A.R.T. log files. The XML files can be used with any XML viewer, allowing for some customization of how the information can be viewed.



3.9: Statistics



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

Details on the different Statistics screens can be found in ***Section 6.8: Statistics***.

- **About** – This screen displays details about the Falcon-NEO2, including the currently installed software version. It also features a QR code. Scanning this code with a device on the same network as the Falcon-NEO2 will launch a web browser and direct you to the Falcon-NEO2's IP address, providing access to the web interface.
- **Adv. Drive Statistics –** Shows S.M.A.R.T. data exactly as reported by the drive.
- **Options –** Displays which optional software or subscriptions are installed/active.
- **Network Interface Stats –** Displays the Network Interface statistics (Receive and Transfer bytes, packets, drops, errors, and link status).
- **Debug Logs –** Allows the export of debug logs for Logicube technical support purposes.
- **Help –** Contains a QR code linking to the user's manual.

3.10: Manage Repositories



Repositories can be added to the Falcon-NEO2 in this operation. Repositories can be drives connected to the Destination ports of the Falcon-NEO2 (automatically shown) or shared folders over a network. Cloud accounts can also be added on this screen.

Details on the different Manage Repositories screens can be found in ***Section 6.9: Manage Repositories***.

3.11: System Settings



The ***System Settings*** screen allows users to configure different settings for the Falcon-NEO2:

Details on the different System Settings screens can be found in ***Section 6.10: System Settings***.

- Profiles
- Passwords
- Encryption
- Language/Time Zone
- Display
- Destination Whitelist
- Notifications
- Advanced
- Debug
- Hash DB

3.12: Network Settings



The following tabs are seen in the Network settings screen:

Details on the different Network Settings screens can be found in ***Section 6.11: Network Settings***.

- **Interfaces:** This allows the configuration of the network interface, including setting a static IP address and enabling or disabling certain network services.
- **HTTP Proxy:** To enable the Falcon-NEO2 to update its software over the network (via the Internet), you may need to configure proxy settings. If your network uses a proxy server for internet access, the Falcon-NEO2 will require these settings to connect online. Typically, this involves specifying a server address (or IP), port number, username, and password.
- **Network Configuration:** Allows Falcon-NEO2's hostname and NTP server list changes.
- **HTTPS:** View, select, upload, or generate HTTPS certificates for secure remote access.

- **802.1x:** Configure various 802.1X settings to allow Falcon-NEO2 to have authorized access to an 802.1X configured network.

3.13: Software Updates



New software updates for the Falcon-NEO2 are released periodically. You can update the software via a network connection with internet access or a USB drive.

Section 9: Updating/Loading/Reloading Software details how to perform a software update, software reload, or firmware update.

3.14: Power Off



The following tabs can be found in the Power Off screen:

Details on the different Network Settings screens can be found in ***Section 6.13: Power Off***.

POWER OFF – This tab lets you remotely turn off the Falcon-NEO2 and refresh its screen.

DRIVE POWER – This tab allows you to set Inactive drives connected to the Falcon-NEO2 to go to standby mode. The default is 0 minutes (OFF).

4: Imaging

Section 4: Imaging - Introduction



This operation enables you to image a Source drive to a Destination. There are three imaging modes available, along with various settings to configure. Make your selections 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 these image output file formats: ***DD***, ***E01***, ***EX01***, ***AFF4,*** *or* ***DMG***.
- **File to File (Targeted Imaging feature) –** Create logical images by applying preset filters, custom filters, file signature filters, or keyword searches to select and acquire only the specific files required. Output formats include AFF4, LX01, ZIP, or a directory tree. Optionally, you can generate an MFT report that lists deleted files (if

present) that may be recoverable. This mode is also used for Cloud Storage Acquisition.

To image APFS (Apple File System), go to the ***System Settings*** screen, then the ***Advanced*** tab, and set ***APFS*** to ***ON*** before starting the task. Use the ***File to File*** imaging method.

- **Partition to File (Logical Imaging) –** The Partition to File operation images a single partition from the Source drive to one of the following formats: DD, E01, or EX01. Compression options are available for E01 and EX01 formats. BitLocker decryption is supported, allowing you to create image files without encrypted data if you provide the BitLocker password or recovery key. Since BitLocker encrypted volumes are formatted partitions, unlocking a BitLocker-encrypted volume requires using the Partition to File mode.
- **Net Traffic to File –** The Falcon-NEO2 can capture network traffic data through the Net Traffic to File imaging mode. This mode can record local network activity, internet usage, and VOIP communications. The captured data is saved in the *.pcapng 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, and EX01 images created by the Falcon-NEO2.

  Currently, Image Restore for AFF4 and DMG images is not supported.

- **Mobile to File –** Acquires data from iOS devices (up to iOS 18.x) and Android devices (4.0 and newer).

  For serial numbers 223000 and above – This is a standard, built-in feature.

  For serial numbers below 223000 – Available as an annual, renewable software subscription. Contact sales@logicube.com or your region's international reseller for additional information. For a list of international resellers, visit https://www.logicube.com/sales/international-sales/.

  - **iOS devices –** Performs an iTunes backup, which may include:
    - Call logs
    - iMessages
    - SMS & MMS
    - Photos and videos
    - Contacts
    - Website history
    - Wi-Fi settings

- Deleted SMS, iMessages, photos, and WhatsApp contacts

- **Android devices –** The capture method will depend on whether the Android device is rooted or not:
  - **Rooted Android devices –** A physical acquisition is performed. Data output will result in a single dd file.
  - **Unrooted Android devices –** A logical acquisition is performed. This is limited to contacts, call logs, SMS, and calendar.

Falcon-NEO2 users can root Android devices using third-party tools at their own risk.

4.2: Source or Case

When you select ***Drive to Drive***, ***Drive to File***, or ***Partition to File*** mode, the Source window displays all drives connected to the Source ports. Tap the icon to choose the Source drive you want to image; the Falcon-NEO2 will list all drives detected in the Source positions.

In ***File to File*** mode, the Source window shows all drives connected to the Source ports and any repositories added with the Source role (either Source only or Both Source and Destination).

The Source Interface window will appear for Net Traffic to File mode, displaying both available LAN ports (LAN 1 and LAN 2).

If you choose ***File to Drive*** mode, the Case window lists all drives connected to the Source or Destination ports containing DD, E01, or EX01 images created by the Falcon-NEO2.

When ***Mobile to File*** mode is selected, the Source window displays any supported mobile devices currently connected.

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

4.3: Settings

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

- **CASE INFO**
- **HPA/DCO/ACS3/TRIM**

4.3.1: CASE INFO

Case Info is accessible in all imaging modes and lets users input details about the case. Providing Case Info is optional and not necessary to begin an imaging operation. Any information entered here will be included in the logs, and some forensic analysis software can import this data when opening the image files. To

enter information, tap any field to bring up the on-screen keyboard. Once you've finished, tap the OK icon to return 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.

When creating the log or file names, the Falcon-NEO2 will convert any non-POSIX portable characters in the Case/File Name field to underscores "_".

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 options are available in Drive to File, Partition to File, and Drive to Drive modes, while the TRIM feature is only available in Drive to Drive mode.

The HPA/DCO/ACS3 setting lets you choose whether to unlock and image a drive's Host Protected Area (HPA), Device Configuration Overlay (DCO), or Accessible Max Address (ACS3). Selecting YES will unlock and include these hidden areas in the image.

- **HPA (Host Protected Area):** If supported, the HPA is set using the SET MAX ADDRESS command. This area is hidden from the operating system, BIOS, and users and is typically used for diagnostics or recovery data.
- **DCO (Device Configuration Overlay):** If supported, DCO is set with commands like DCO MODIFY or DEVICE CONFIGURATION SET. DCO can make a drive appear smaller than its actual size, hiding data from the OS and BIOS in a way similar to HPA.
- **ACS3 (Accessible Max Address):** If supported, this is set using the ACCESSIBLE MAX ADDRESS command specified by the ATA/ATAPI Command Set. It defines the maximum logical block address accessible for read and write operations and can be used to limit the drive's visible size.

4.3.2.1: Drive Trim

Destination Drive Trim is only available in Drive to Drive mode and is a user-selectable feature that enables the Falcon-NEO2 to adjust the destination drive's capacity using the DEVICE CONFIGURATION SET command for DCO, the SET MAX ADDRESS command for HPA, or the ACCESSIBLE MAX ADDRESS command for ACS3. This ensures the destination drive's total

native capacity matches the source drive's. For instance, if the source drive is 128 GB and the destination drive is 6 TB, the Falcon-NEO2 will limit the destination drive's capacity to 128 GB to mirror 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 BEFORE DRIVE TRIM:

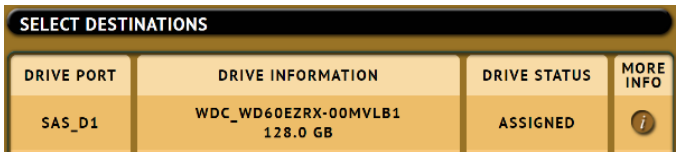
Bay:	SAS_D1
Role:	Target
Model:	WDC_WD60EZRX-00MVLB1
SerialNumber:	WD-WX21D1403007
Size:	6001175126016
PhysicalSectors:	11721045168
LogicalSectors:	11721045168
LogicalSectorSize:	512
Cylinders:	65535
Heads:	255

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

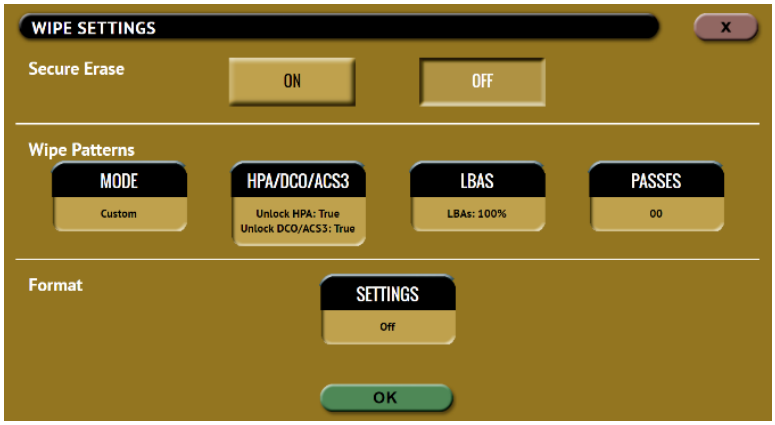
Drive Trim only works with ATA drives connected to the SAS/SATA Destination ports. Drive trim will not work with SAS drives or drives connected to the USB, PCIe, or I/O ports.

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.

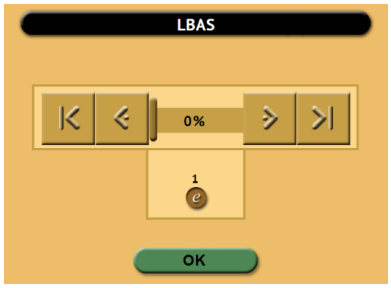


IN THE WIPE SETTINGS:

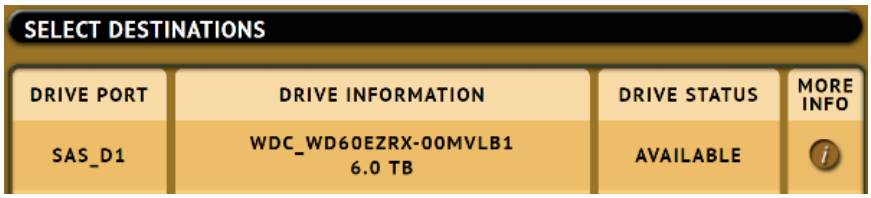
- Set Secure Erase to OFF
- Set Wipe Patterns to:
  - Mode: Custom
  - HPA/DCO/ACS3/TRIM: YES (TRUE)
  - LBAS: Edit to at least 1 LBA
  - PASSES: By default, this will have a value of 00



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



Start the Wipe task. It should finish quickly, wiping only the HPA/DCO/ACS3 and 1 LBA. When the Wipe task finishes, the drive should return to its original capacity.



4.3.3: Error Handling

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

In Drive to Drive mode, when the Falcon-NEO2 encounters bad sectors on the Source drive, you can either skip these sectors or abort the imaging process, providing flexibility in managing errors.

If error handling is set to Skip, the Falcon-NEO2 writes zeros to the corresponding sectors or positions on the Destination drive or file.

Additional options for Drive to File and Partition to File modes include Error Granularity and Reverse Read. Error Granularity lets you define the data block size to skip when a bad sector is found. Options include 512 bytes, 4096 bytes, or 64 KiB. The block is skipped if a bad sector is detected within a selected block size.

The Reverse Read feature attempts to read backwards over bad sectors, which may recover data that would otherwise be missed when skipping the entire block.

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 disk space that can hold a file. For example, the most common cluster size for an NTFS volume is 4KB (4096 Bytes), meaning that the smallest amount of space used for a file is 4096 Bytes.

For example, if 4096 Bytes is chosen, and one of the 8 sectors in that cluster size contains a bad sector, the Falcon-NEO2 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-NEO2 encounters a bad sector, it will instruct the Falcon-NEO2 to skip past the block (based on the

Error Granularity) and 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 except File to Drive, which can only verify the previous hash used. Several hash and verification options are available depending on the imaging mode used.

Hash – Will hash the Source drive with the selected method:

- None – No hash of the Source will be performed.
- A single hash - MD5, SHA-1, SHA-256, or SHA-512.
- Dual hash – A combination of two of the single hash methods.

Verification Method/Verify – Verifies either the selected single hash or dual hash:

- **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 users to select a file image output. The following different image methods can be selected:

- **DD –** Raw image files that are readable by many forensic programs.
- **E01 –** Compressed or uncompressed EnCase legacy evidence file format.
- **EX01 –** Compressed or uncompressed EnCase evidence file format.
- **AFF4 –** Compressed or uncompressed open-source AFF4 (Advanced Forensic File Format 4).
- **DMG –** Raw disk image files commonly used in Mac OS X.

SEGMENT SIZE – Some image method settings may offer Different output file segment sizes. 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.



If compression is on, DD, E01, EX01, AFF4, and DMG files created on the Destination may be smaller than the selected Segment Size. For example, if the 4 GB segment size is selected, some files may be less than 4 GB.

COMPRESSION –Available for E0, EX01, and AFF4 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. This is typically set to 100% of the Source for forensic purposes.
- **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). This is typically set to 0% or the beginning of the Destination (Target) for forensic purposes.

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

4.3.7: Verify Hash

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

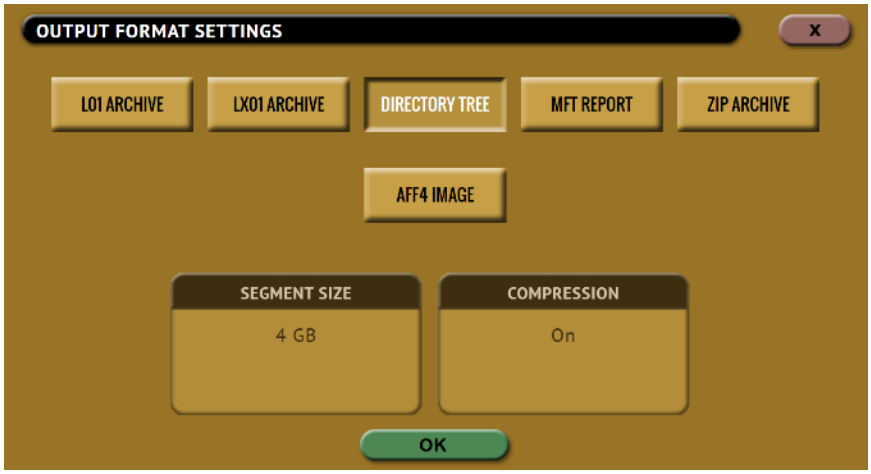
4.3.8: Special Settings in File to File mode

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 found on the Source drive.
- **MFT Report:** The results will list deleted files (if present) in the audit log file that can potentially be restored or recovered.
- **Zip Archive:** Results will be in a Zip archive format.
- **AFF4 Image:** Results will be in AFF4 file format.

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

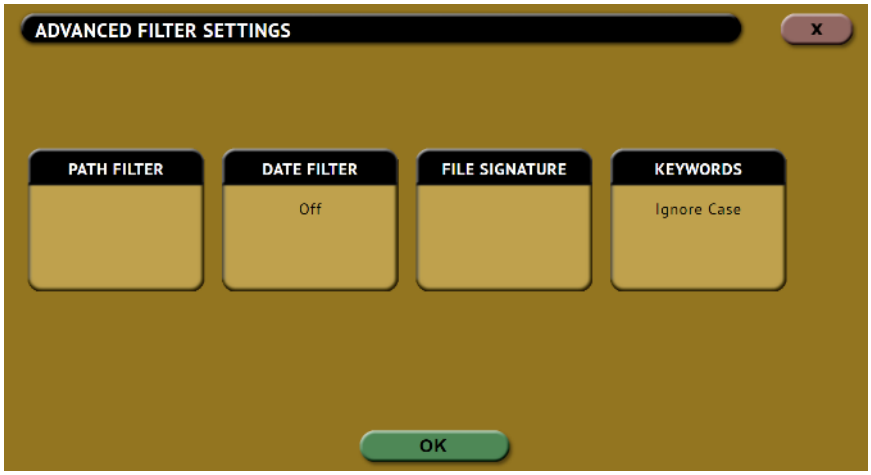
- **Segment Size:** This option allows users to set the output segment size (file size). Choose from the following segment sizes: 2 GB, 4 GB (Default), 8 GB, 16 GB, or Whole Disk.

If compression is on, the file size may be smaller than the selected Segment Size. For example, if the 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

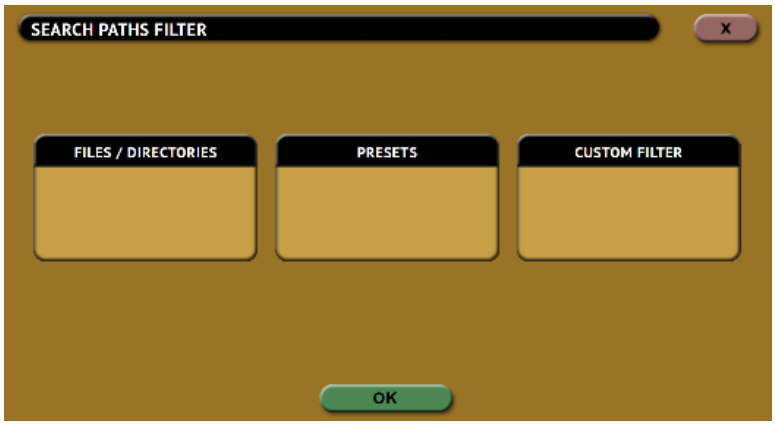
The Filter Settings screen shows the following selections:



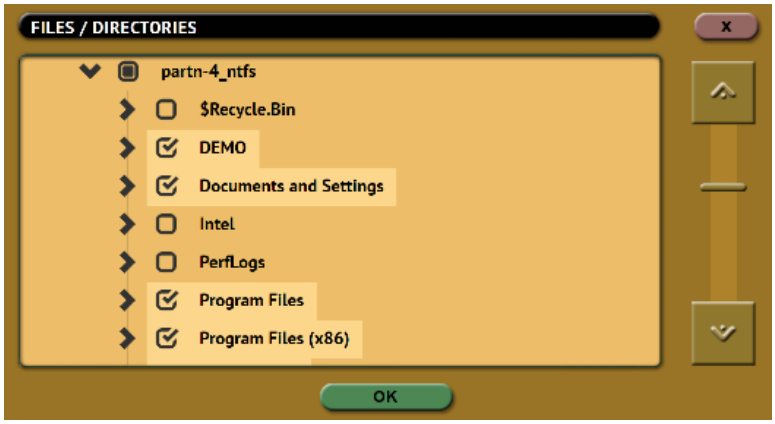
This screen enables users to apply multiple filters. Be aware that setting a filter incorrectly or making it too restrictive may negatively impact the results. Each filter further refines the output. For instance, if you select only video files in the Signature-Based File Category filter, the results from the path filter will be limited to video files found within the scope of the initial filter.

4.3.8.2.1: Path Filter

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



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.



Several websites have articles explaining the different expressions that can be used. 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”.

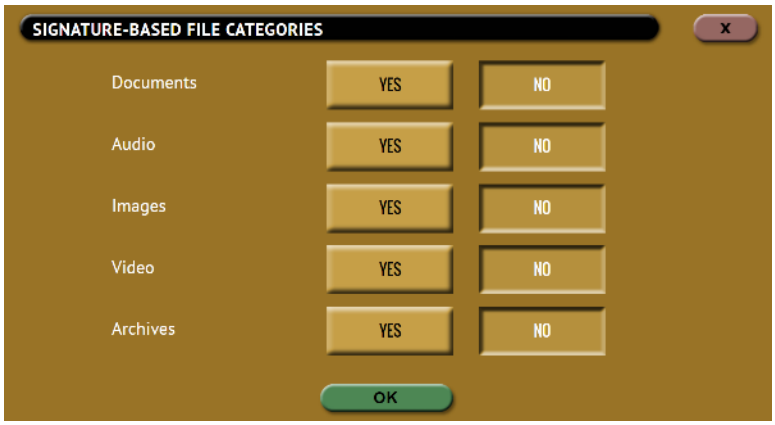
4.3.8.2.2: Date Filter

This allows a date filter to be set. By default, this setting is turned 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.



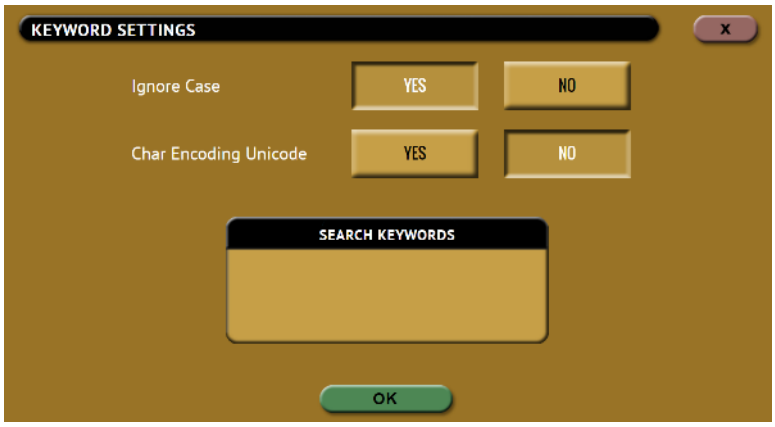
4.3.8.2.3: File Signature

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



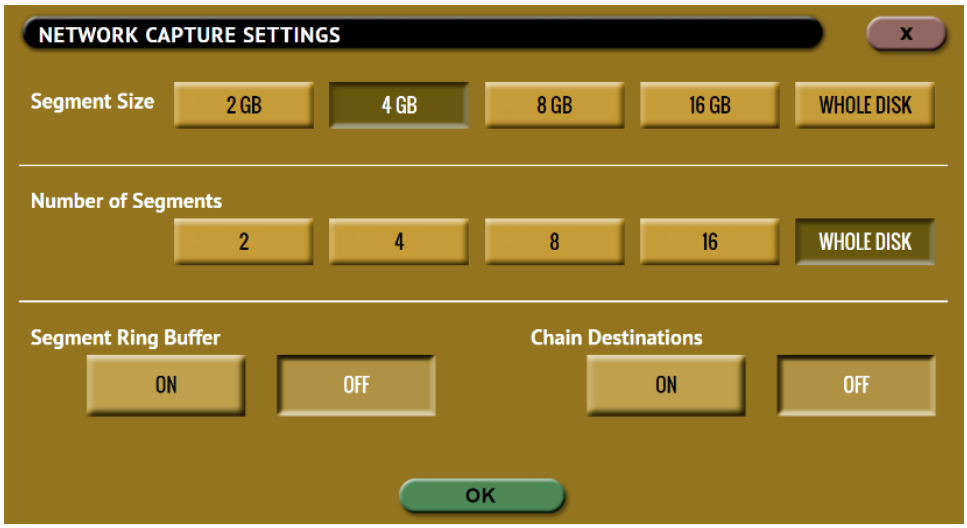
4.3.8.2.4: Keywords

This allows the user to set specific keywords. The Falcon-NEO2 will search for particular 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 option lets the user specify the number of segment files to generate. For example, if the Segment Size is set to 4 GB and the Number of Segments is set to 2, the system will create two segment files, each up to 4 GB. Available choices include 2, 4, 8, 16, or Whole Disk (which is the default setting).

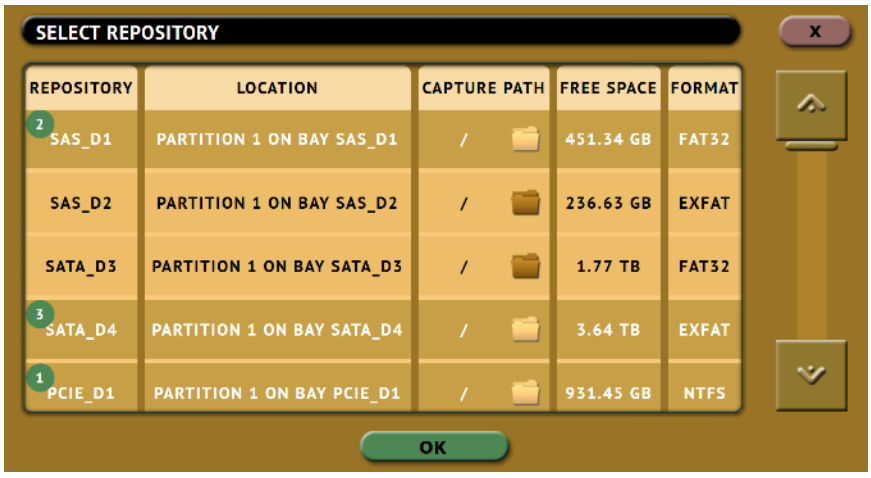
4.3.9.3: Segment Ring Buffer

This setting determines what the Falcon-NEO2 will do when it reaches the total number of segments on all selected repositories (Destination drives).

- **ON:** When this option is enabled, the Falcon-NEO2 will continuously capture network traffic until the task is stopped. For example, if the Number of Segments is set to 2 and the Segment Ring Buffer is ON, once the second segment is complete, the system will delete the first segment and continue capturing, creating a new first segment file. If multiple repositories are selected, Falcon-NEO2 will cycle through them, continuously overwriting the oldest segment until the capture task is aborted.
- **OFF:** This is the default setting. When this setting is set to OFF, the Falcon-NEO2 will stop the task once it reaches the specified number of segments and the last repository is filled.

4.3.9.4: Chain Destinations

This setting seamlessly enables users to span Net Traffic to File images across two or more repositories (such as Destination drives). When set to YES, the Falcon-NEO2 will use all selected Destination drives in the order chosen. Once the first repository is full, the system will automatically continue saving data to the next selected repository.



To use Chain Destinations, the Ring Buffer must be turned OFF.

Additionally, all drives must be formatted by the Falcon-NEO2 before beginning the Net Traffic to File imaging task.

Once the first repository is full, you can replace its Destination drive with a new one. By swapping out full repositories for new destination drives, the Falcon-NEO2 can continue capturing network traffic until all selected repositories are filled. When all repositories reach capacity, the task will complete and display 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.

If the Falcon-NEO2 has a Destination Whitelist configured, only drives included in the list can be used as destination drives in the Imaging screens. If you attempt to use a drive that is not on the whitelist for an imaging task, an error message will appear indicating that the target drive in the connected bay is not permitted:

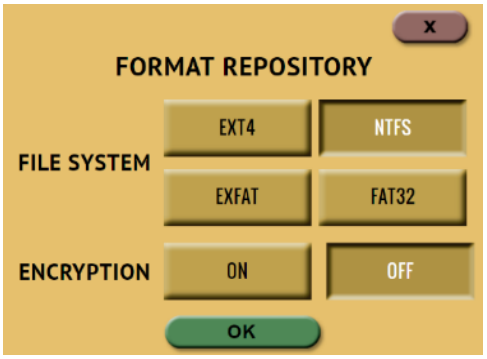
Generic system error!
Task start failed: Target in Bay USB_D3 is Not allowed!

See ***Section 5.10.6 (Destination Whitelist)*** for more information.

When working in Drive to File, File to File, Partition to File, or Net Traffic to File modes, if the Destination drive is not correctly formatted, its Location will display as “(NOT_MOUNTED)” and a format icon will appear in the Format column. To format the Destination drive, tap the Format icon: 

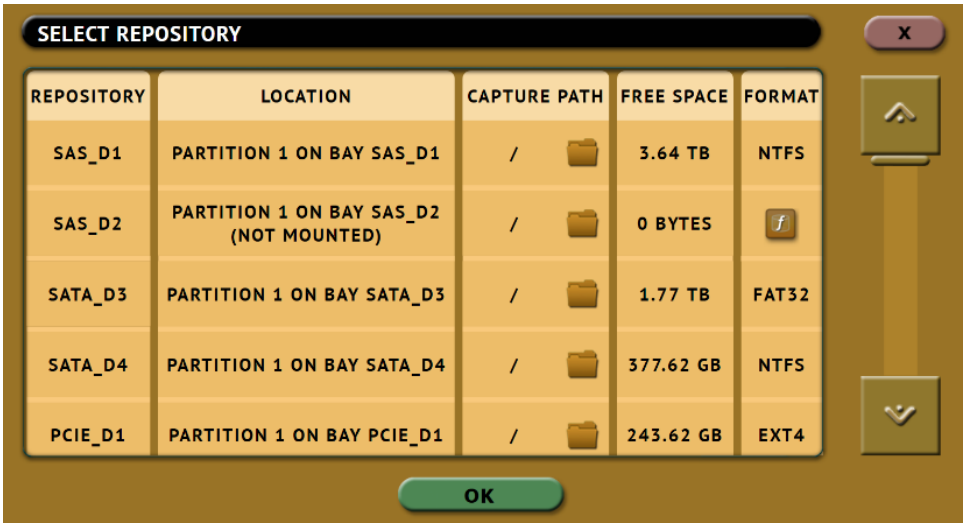
Drives encrypted by the Falcon-NEO2 will have the following icon: 

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



Choose the desired file system and specify whether to format the drive with encryption (ON) or without encryption (OFF).

You can change the default selection for this screen in the ***Manage Repositories – Configuration*** screen. For more information, see ***Section 6.9.4***.



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 creates a new folder or subfolder.
- **Delete Folder:** This method deletes an empty folder. It cannot be used to delete folders containing files.
- **Rename Folder:** This will rename any folder.
- **OK:** Use this button when all desired changes have been completed.

Creating a folder or subfolder is optional. If you choose not to create any, tap the OK button to proceed. The image file will then be saved at the root directory of the drive or partition.

4.5: Starting the Imaging Operation

After configuring all settings and options, tap the Start icon to initiate the imaging task. A confirmation screen will appear. Tap the Yes icon to proceed. During the process, a progress bar at the bottom of the screen will display the number of bytes processed, transfer speed, elapsed time, estimated time remaining, and any read errors. When the task is complete, the status will display "COMPLETED." Tap ***Reset Task*** afterward to ensure the drive bays are properly reset and not marked as in use or assigned to other tasks.

The byte count displayed on the progress bar represents the data currently being processed, not the total drive size. If 'Verify' is enabled, this number will appear doubled, as the imaging and verification processes are included.

The Falcon-NEO2 can automatically span imaging across two or more Destination drives when operating in Drive to File mode (DD, E01, EX01, or DMG). If the current Destination drive becomes full and there isn't enough space left for the remaining data, the Falcon-NEO2 will prompt you to insert another drive. For more details on Drive Spanning, refer to ***Section 3.2.10***.

Section 5: Hash / Triage



You can perform a hash, case verify, or triage operation on any drive or case, including DD, E01, EX01, or DMG images created by the Falcon-NEO2. Running a hash or verify task instructs the Falcon-NEO2 to compute the hash for the selected drive or case. The Triage function allows users to import one or more VICS, Comma-Separated Value, or X-Ways Hash Databases and scan source drive files for any matching hash in the database.

When performing a hash or triage, there are four selections: ***Mode, Drives / Case***, ***Settings***, and ***Case Info***.

5.1: 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 created by the Falcon-NEO2. The Falcon-NEO2 can verify the following case/image file types: **DD**, **E01**, **EX01**, and **DMG**.



- **Triage:** Import one or more VICS, Comma-Separated Value, or X-Ways Hash Databases, and then triage a source drive to determine if any files on the drive match hashes in the database. Positive results will result in a successful message, and all matches will be listed in the audit log file.

5.2: Drives or Case

Depending on the selected mode, Drives or Case will be available. Tap this icon to select the drive to be hashed or triaged, or the drive containing the case (image) files to be verified.

Using Drive Hash, multiple drives can be selected and hashed simultaneously.

Using Case Verify, only one drive and case can be selected.

Using Triage, only one drive can be selected and triaged.

5.3: Settings

Tap this icon to select a drive and adjust the hash, verify, or triage settings. Different settings are available depending on the mode selected.

5.3.1: Drive Hash Settings

If Drive Hash mode was chosen, the Hash Settings screen will show two sections:

- Hash Values
- LBA

5.3.1.1: Hash Values



This screen has two sections.

- **Hash Method:** Select one of the Hash Methods: SHA-1, SHA-256, or MD5.
- **Hash Values:** Set the expected hash value, if desired. Setting the expected hash value instructs the Falcon-NEO2 to hash the drive, then verify the hash with the expected value set.

Each hash task is based on a drive's Logical Block Address (LBA) and will hash drives based on the number of LBAs. If multiple drives are selected to be hashed, the Falcon-NEO2 will hash up to the LBA value of the smallest capacity drive. If drives with different capacities need to be hashed, starting one task per drive is recommended.

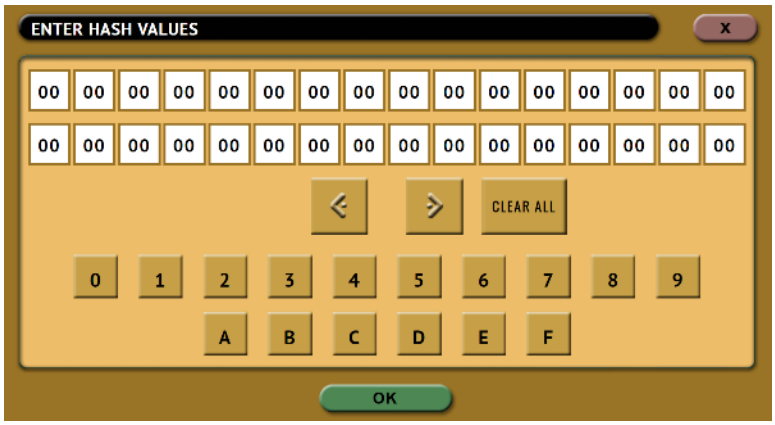
5.3.1.1.1: Hash Method

Select one of the available hash methods: SHA-1, SHA-256, or MD5.

5.3.1.1.2: Hash Values

By default, this value will have 0s (zeros). If this is not changed or no value is entered, the Falcon-NEO2 will hash the drive using the selected algorithm in the previous step. The Falcon-NEO2 will use the result as the expected value. If a value is entered, the Falcon-NEO2 will hash the chosen drive and verify the hash calculation with the value entered/edited.

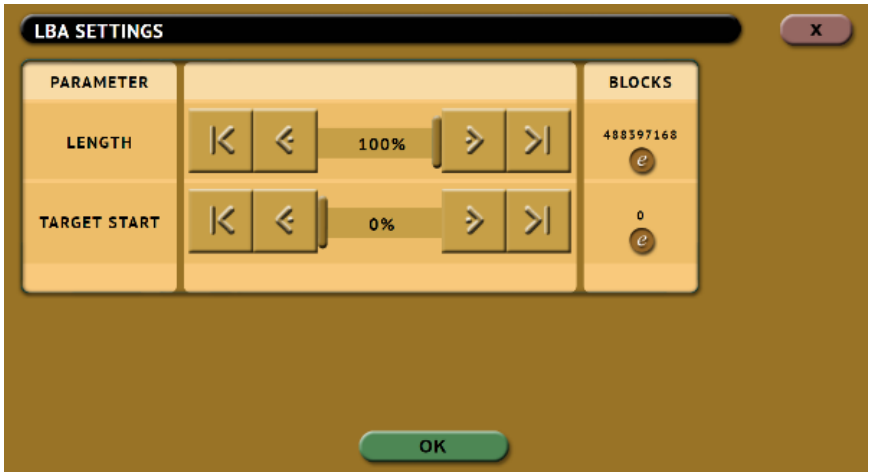
To set the expected value, tap the ***(edit)*** icon. The on-screen keyboard will appear, and the expected hash value can be set.



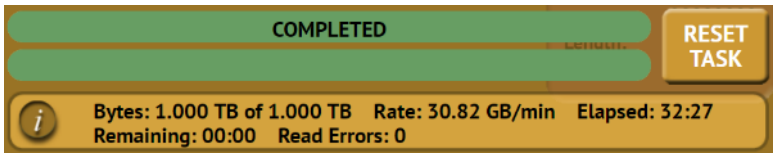
There is a ***Clear All*** button to clear all values easily.

5.3.1.2: LBA

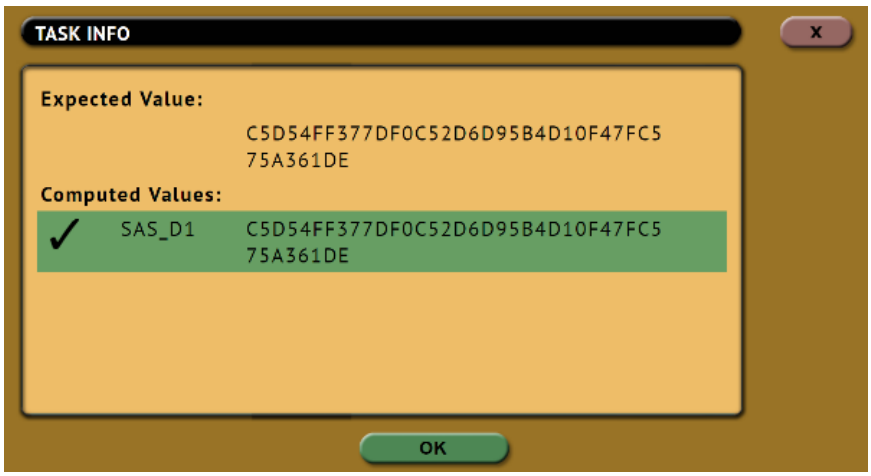
The LBA icon will bring up the LBA settings screen. The user can adjust the percentage or the number of blocks of the drive to hash and where to start the hash. By default, the length is set to 100% (whole drive), and the starting percentage is 0% (start of the drive).



When the Falcon-NEO2 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 the expected and computed hash values.



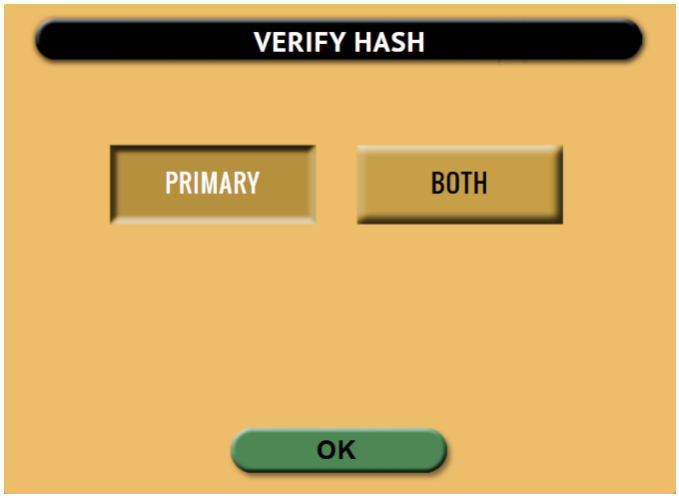
5.3.2: Case Verify Settings



In the Case Verify Settings screen, users can select which hash to verify, based on the original image process:

- Primary
- Both

5.3.2.1: Verify Hash



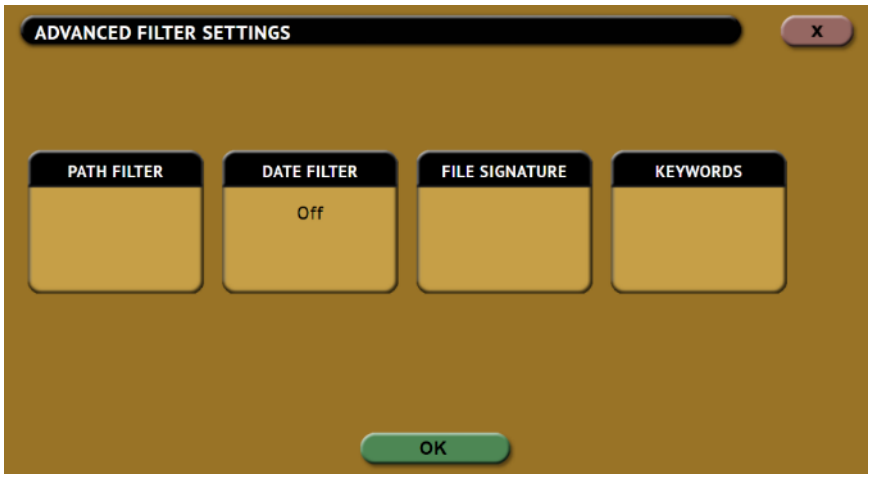
- **Primary:** Will verify just one hash value. For instance, if SHA-1 or MD5 was selected during the image process.
- **Both:** Will verify both hash values of any dual hash from the original image process. For instance, if the ***SHA-1+MD5*** hash was selected during the image process, it will verify both SHA-1 and MD5.

5.3.3: Triage Settings

There are four main settings when Triage mode is selected:

- Filter settings
- Search Criteria
- Hash DB
- Hash Method

5.3.3.1: Filter Settings



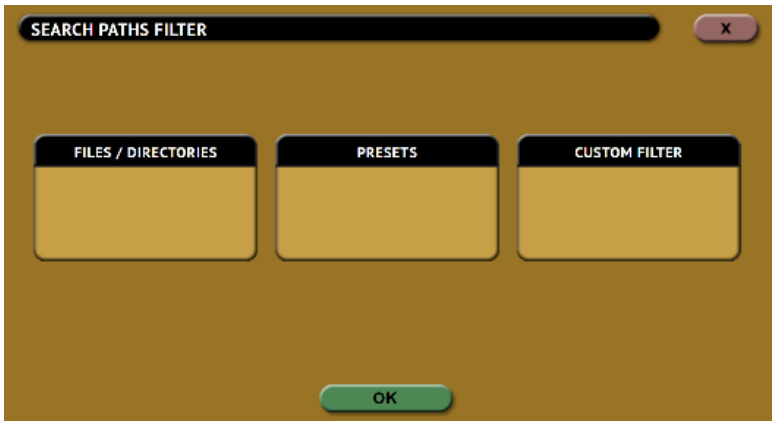
This screen enables users to apply multiple filters. Setting a filter incorrectly or too restrictively may negatively impact the results. Each filter further refines the output. For instance, if you select only video files in the Signature-Based File Category filter, the results from the path filter will be limited to video files found within the scope of the initial filter.

In the Advanced Filter Settings, four items can be set:

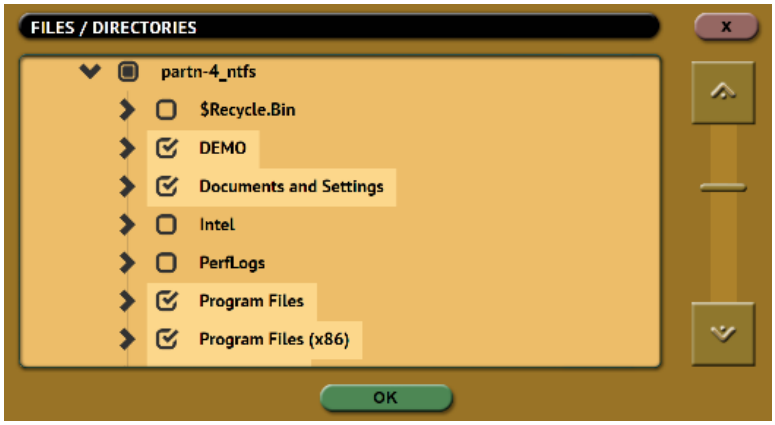
- Path Filter
- Date Filter
- File Signature
- Keywords

5.3.3.1.1: Path Filter

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



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.



Several websites have articles explaining the different expressions that can be used. 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”.

5.3.3.1.2: Date Filter

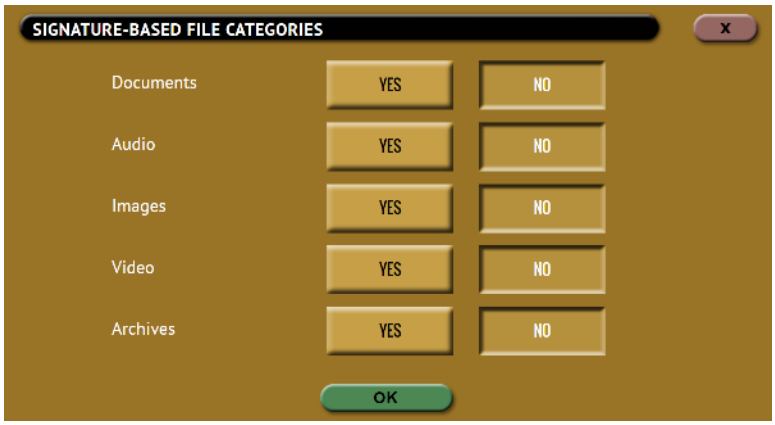
This allows a date filter to be set. By default, this is set to OFF. Set an ***Include*** date range to only include files modified within the specified date range. If ***Exclude*** is selected, all files modified within the specified date range will not be imaged.



5.3.3.1.3: File Signature

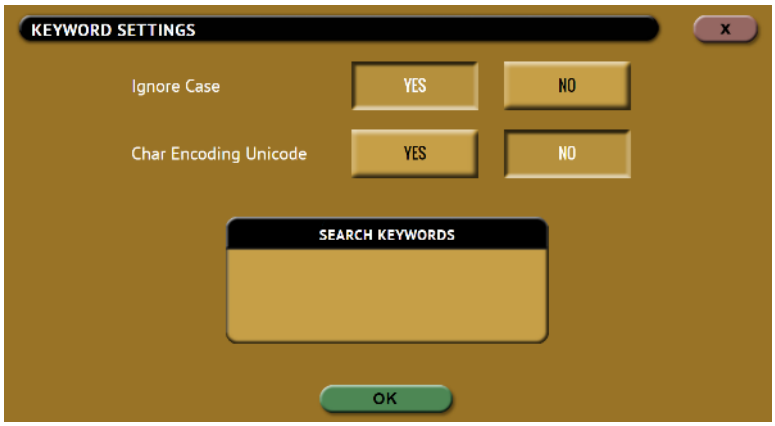
This allows users to set signature-based file categories. This is the second level of filtering, and if selected, it will narrow down the results of the first filter to only the selected file categories.

Selecting ***YES*** will limit the files accessed to only those signature-based file categories.



5.3.3.1.4: Keywords

This allows the user to set specific keywords. The Falcon-NEO2 will search for particular keywords within the results of the previous filters.



5.3.3.2: Search Criteria

END AT FIRST OCCURRENCE: Triage on the source drive will stop at the first file matching a hash from the Hash Database.

FULL SEARCH: Triage on the source drive will check all the files and show all files matching hashes from the Hash Database.

5.3.3.3: Hash DB

This screen will list any VICS, Comma-Separated Value, or X-Ways hash databases loaded onto the Falcon-NEO2. There is also a ***MANAGE*** button that allows users to import/convert a supported Hash Database.

5.3.3.4: Hash Method

Hash Databases can contain both SHA-1 and MD5 hashes. In the Hash Method screen, users can select which hash method will be used on the source drive files to match the hashes in the selected Hash Database. The following selections are available:

- NONE
- SHA-1
- MD5

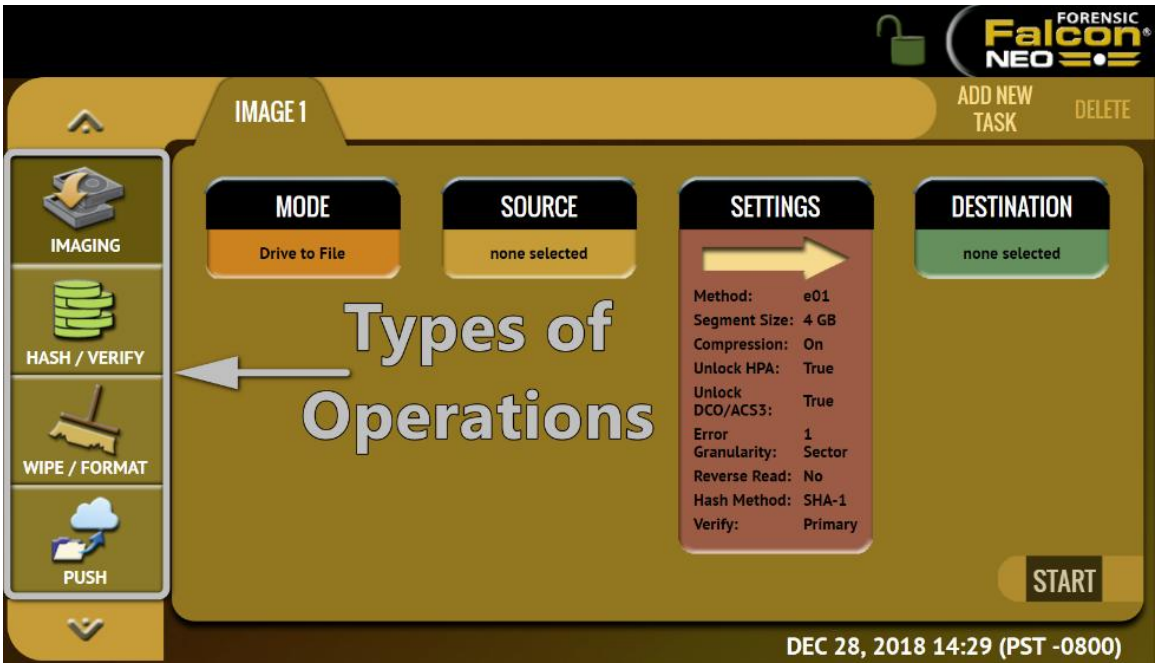
5.3.4: Case Info

The Case Info setting lets users input details related to the case. Users do not need to enter Case Info to begin a Hash or Verify operation.

Any information provided here will be included in the logs. For additional details about the Case Info screen, refer to ***Section 4.3.1***.

Section 6: Types of Operations - Introduction

The Falcon-NEO2 supports thirteen distinct operation types, conveniently displayed on the left side of the screen for easy selection. This section provides details and overviews of each operation type and its corresponding interface screens.



1. **IMAGING –** Creates an image from a Source to a Destination. The available modes include:
    - **Drive to File –** Images the Source to any image output file format: ***DD***, ***E01***, ***EX01***, ***AFF4,*** or ***DMG***.
    - **File to File (Targeted Imaging feature) –** Create logical images by applying preset filters, custom filters, file signature filters, or keyword searches to select and acquire only the specific files required. Output formats include AFF4, LX01, ZIP, or a directory tree. Optionally, you can generate an MFT report that lists deleted files (if present) that may be recoverable. This mode is also used for Cloud Storage Acquisition.
    - **Partition to File (Logical Imaging) –** The Partition to File operation images a single partition from the Source drive to one of the following formats: DD, E01, or EX01. Compression options are available for E01 and EX01 formats. BitLocker decryption is supported, allowing you to create image files without encrypted data if you provide the BitLocker password or recovery key. Since BitLocker encrypts volumes (formatted partitions), unlocking a BitLocker-encrypted volume requires using the Partition to File mode.

- **Net Traffic to File –** The Falcon-NEO2 can capture network traffic data through the Net Traffic to File imaging mode. This mode can record local network activity, internet usage, and VOIP communications. The captured data is saved in the *.pcapng 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-NEO2.
- **Mobile to File –** Acquires data from iOS devices (up to iOS 18.x) and Android devices (4.0 and newer).

For serial numbers 223000 and above – This is a standard, built-in feature.

For serial numbers below 223000 – Available as an annual, renewable software subscription. Contact sales@logicube.com or your region's international reseller for additional information. For a list of international resellers, visit https://www.logicube.com/sales/international-sales/.

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

2. **HASH/TRIAGE –** Hash, Verify, or Triage a drive or forensic image.
   - **Hash:** Calculate a drive's hash using MD5, SHA-1, or SHA256.
   - **Verify:** Verify a case or image (DD, E01, EX01) created by the Falcon-NEO2.
   - **Triage:** Triage a drive's contents against a VICS, Comma-Separated Value, or X-Ways Hash Database for matching hashes.

Details on the different screens in the Imaging operation can be found in ***Section 5: Hash / Triage*****.**

3. **WIPE/FORMAT –** This operation is used to erase, wipe, or format drives and offers three primary settings:
   - **Secure Erase –** This command instructs the drive to perform a secure erase based on the manufacturer's specifications.
   - **Wipe Patterns –** This allows users to set a specific pattern for wiping the drive. The number of passes (up to 7) and the type of data written for each pass are customizable. A 7-pass DoD wipe can also be set.
   - **Format –** Formats the Destination using any of the following file systems (with or without AES-256 encryption):
     - NTFS
     - EXT4
     - EXFAT
     - FAT32

- EXT3
- EXT2
- HFS+

4. **PUSH –** The Push operation enables users to transfer evidence created by the Falcon-NEO2 to or from drives connected to the device and a Falcon-NEO2 repository or network location. This feature offers enhanced security compared to traditional file copying by allowing data verification during the transfer. For each push process, the Falcon-NEO2 also generates a log file.
5. **TASK MACRO –** Set up to nine (9) different tasks to perform sequentially (one after another). For example, a macro can perform these tasks: Wipe, image, hash, push, then wipe again.
6. **FILE BROWSER –** The Falcon–NEO2 allows you to preview the contents of all connected Source or Destination drives. It will show all viewable partitions and the contents of each partition.
7. **LOGS –** View, export, or delete logs for each imaging, hash, or wipe/format operation performed on the Falcon-NEO2.
8. **STATISTICS –** This will display several tabs that include:
    - **About** – This screen displays details about the Falcon-NEO2, including the currently installed software version. It also features a QR code. Scanning this code with a device on the same network as the Falcon-NEO2 will launch a web browser and direct you to the Falcon-NEO2's IP address, providing access to the web interface.
    - **Adv. Drive Statistics –** Shows S.M.A.R.T. data exactly as reported by the drive.
    - **Options –** Displays which optional software or subscriptions are installed/active.
    - **Network Interface Stats –** Displays the Network Interface statistics (Receive and Transfer bytes, packets, drops, errors, and the link status).
    - **Debug Logs –** Allows the export of debug logs for Logicube technical support purposes.
    - **Help –** Contains a QR code linking to the user's manual.
9. **MANAGE REPOSITORIES –** The user can add a network location as a repository to be used as a Destination for imaging or pushing images. This will display three tabs that include:
    - **Add/Remove –** Add, remove, or edit networked repositories.
    - **iSCSI –** Set ISCSI protocol settings.
    - **Cloud –** Add or delete supported cloud dive repositories.
    - **Configuration –** Change the default format option for drives that the Falcon-NEO2 has not formatted.
10. **SYSTEM SETTINGS –** This mode allows changes to the system settings on the Falcon-NEO2, which include the following:
    - **Profiles –** Users can create, save, apply, or delete user profiles/configurations.

- **Passwords –** Users can set passwords or keys to lock the unit from 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 encryption password.
- **Language/Time Zone –** Sets the language on the Falcon-NEO2's menu and allows the system to change its time zone.
- **Display –** Sets the Falcon-NEO2's display/screen brightness and enables/disables Stealth Mode.
- **Destination Whitelist –** Select or upload a list of drives, including their model and serial numbers, to establish a whitelist of drives permitted for use as destinations. Any drive not included in this whitelist will be blocked from being used as a destination for imaging, wiping, or formatting tasks
- **Notifications –** Sets audible beeps/notifications or email/SMS notifications for when a task completes or if an error appears.
- **Advanced –** Users can 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.
- **Hash DB –** Import/convert and manage Hash Databases from this screen.

11. **NETWORK SETTINGS –** Allows the editing of various network configurations. The following 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).
    - **Network Configurations –** Change the Falcon-NEO2's hostname or NTP servers.
    - **HTTPS –** View, select, upload, or generate HTTPS certificates for secure remote access.
    - **802.1X –** Configure various 802.1X settings, including the EAP method, identity, password, phase2 authentication, CA and client certificates, and private keys.
12. **SOFTWARE UPDATES –** Update the Falcon-NEO2's software and firmware. Updates can be performed via an internet connection (from the network) or USB flash drive.
    - **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-NEO2 (if available) can be updated on this screen.
    - **PXEboot Update –** This is reserved for future use.
13. **POWER OFF –** Shut down the Falcon-NEO2, refresh the Graphical User Interface (GUI), or configure a drive timeout to power down drives when they are idle. Two tabs are provided:

- **Power Off –** Use this screen to turn off the Falcon-NEO2, which is especially helpful when accessing via the web interface. You can also refresh the user interface here.
- **Drive Power –** Set drives to power down when not in use automatically.

6.1: Imaging



This operation enables you to image a Source drive to a Destination. There are three imaging modes available, along with various settings to configure. Make your selections in order from left to right.

In-depth details on the different screens found in the Imaging operation are provided in ***Section 4: Imaging***.

6.2: Hash / Triage



You can perform a hash, case verification, or triage operation on any drive or case, including DD, E01, EX01, or DMG images created by the Falcon-NEO2. Running a hash or verification task instructs the Falcon-NEO2 to compute the hash for the selected drive or case. The Triage function allows users to import one or more VICS, Comma-Separated Value, or X-Ways Hash Databases and scan files on the source drive for any matching hash in the database.

Section 5: Hash / Triage provides in-depth details on the different screens found in the Hash/Triage operation.

6.3: Wipe / Format



This 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.

Depending on the type of media to wipe, Secure Erase or Wipe Patterns with Verify enabled complies with NIST SP 800-88 Rev. 1's Clear or Purge guidelines.

If the Falcon-NEO2 has a list of drives in the Destination Whitelist, only drives in the whitelist will be allowed to work in the Wipe/Format screens. When a drive not on the whitelist is used with a Wipe/Format task, an error will appear showing that the Target in the connected bay is not allowed:

Generic system error!

Task start failed: Target in Bay USB_D3 is Not allowed!

See ***Section 6.10.6 (Destination Whitelist)*** for more information.

- **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 ports.

- **Wipe Patterns –** This feature allows users to define a custom pattern for wiping the drive. You can specify up to 7 passes and choose the type of data written for each pass. A 7-pass DoD wipe is available with predefined values for each pass. The Falcon-NEO2 also offers the option to verify each pass. HPA, DCO, or ACS3 areas can be unlocked and wiped using these settings.
- **Format –** Formats the Destination drive with one of the following user-selectable file systems (with or without encryption): NTFS, EXT4, exFAT, FAT32, EXT3, EXT2, or HFS+.

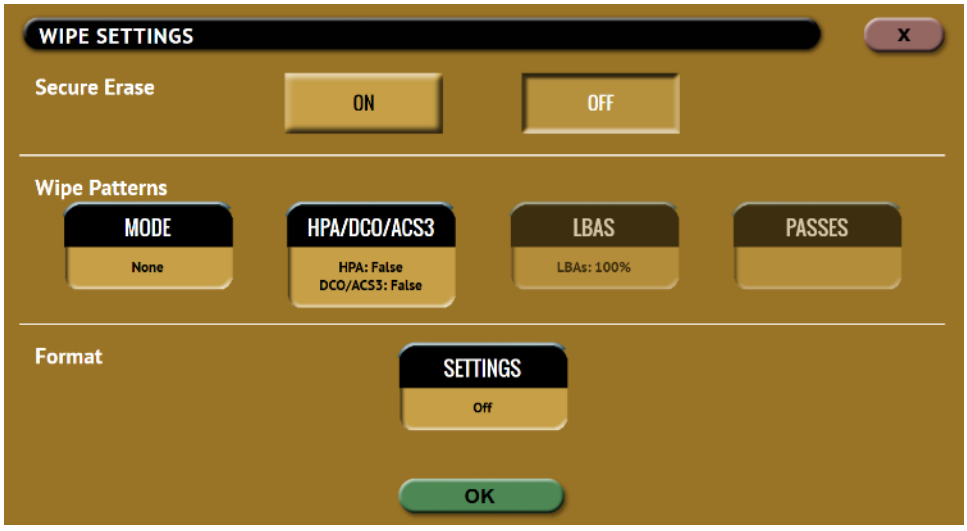
There are three selections when performing a wipe:

- Destination
- Settings
- Case Info

6.3.1: 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***.

6.3.2: Settings



Tap this icon to select a drive for the wipe settings. The Wipe Settings screen will appear. It has the following sections:

- Secure Erase
- Wipe Patterns
- Format.

> The Falcon-NEO2 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-NEO2 will first secure erase the drive, then wipe the drive according to the mode selected, then format the drive.

6.3.2.1: Secure Erase



Choose ***ON*** to run a Secure Erase on 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.

Additional Information on Secure Erase:

- For SAS (Serial Attached SCSI) drives, Secure Erase sends a 'Format' command.
- For SATA drives, Secure Erase sends a 'Security Erase Unit' command. If the SATA drive supports the 'Enhanced Security Erase Unit' command, the enhanced command will be sent.
- Since the drive controls Secure Erase, please contact the drive manufacturer with questions about how each drive supports these features or what the drive will do with these commands.
- Secure Erase will not work on drives connected through the USB or PCIe ports (except for NVMe M.2 SSDs using Logicube-supported adapters through the PCIe port).

6.3.2.2: 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 (up to 7) and the type of data written for each pass are customizable. A 7-pass DoD wipe can be set with pre-selected pass values.

The following selections are available when setting a wipe pattern:

- MODE

- HPA/DCO/ACS3
- LBAS
- PASSES

It is recommended that identical-capacity drives be used 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 completed.

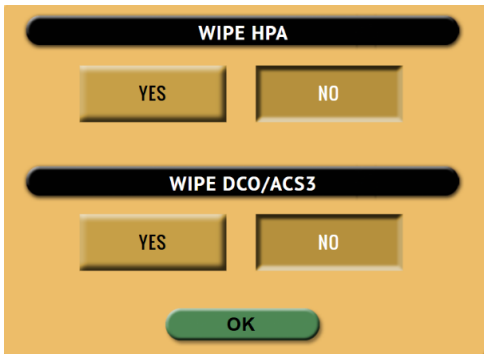
6.3.2.2.1: Mode



Selecting ***Mode*** will open the Wipe Mode screen with these options:

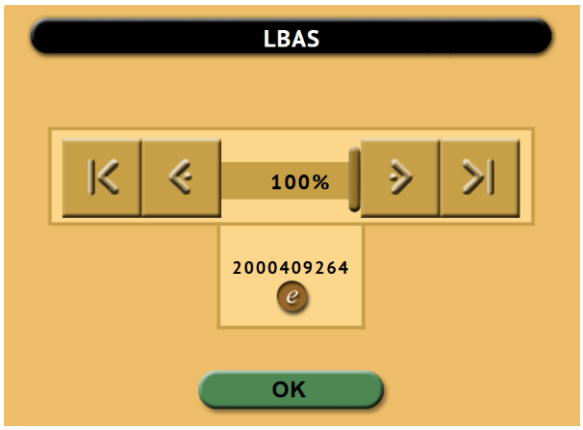
- **NONE –** Choosing this will instruct the Falcon-NEO2 not to perform a wipe using Wipe Mode.
- **DOD –** Choosing this will instruct the Falcon-NEO2 to perform a 7-pass wipe conforming to the DoD 5220.22-M standards.
- **CUSTOM –** This will allow the user to specify how many wipe passes will be performed and what values will be written on each pass selected.

6.3.2.2.2: 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.

6.3.2.2.3: LBA



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

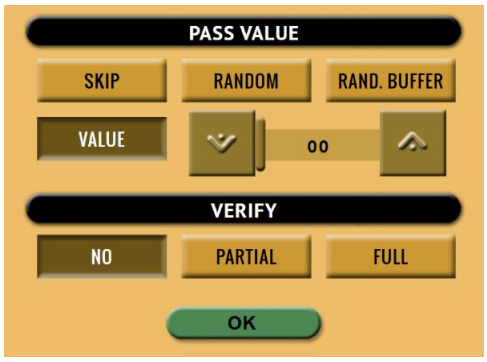
6.3.2.2.4: PASSES



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

- If ***None*** was selected, ***Passes*** is not selectable.
- If ***DoD*** is selected, all seven 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-NEO2 to skip the pass.
- **RANDOM:** Writes one random hexadecimal value (from 00 - FF) to all the selected Logical Block Addresses.
- **RAND. BUFFER:** The Falcon-NEO2 will create an 8MB block filled with random values (each byte in the 8 MB block will contain a random value). The 8 MB block will be written repeatedly to fill the entire drive.
- **VALUE:** Instructs the Falcon-NEO2 to use the specified hexadecimal value to be written for the pass. The values can range from 00 to FF.
- **VERIFY:** This option allows partial or full verification for the wipe process. Partial and Full verification methods conform to NIST SP 800-88 Rev. 1 verification guidelines.

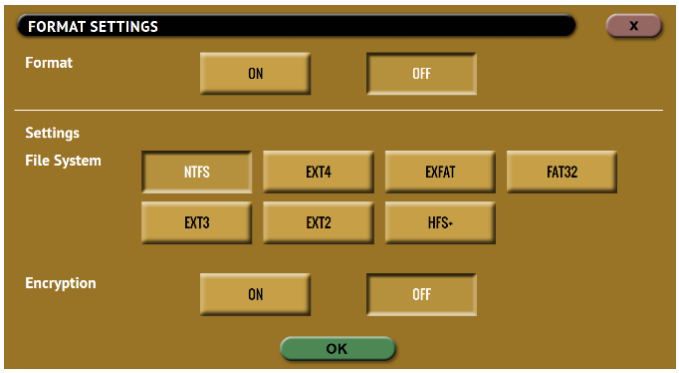
> When ***Verify*** is set to ***YES***, the total time to wipe the drive could double if FULL is selected.

  - **PARTIAL:** Will take pseudorandom locations on the drive and verify the value that was written to those locations. When set, Partial verification will be used for drives over 16GB in capacity. If a drive is 16GB or less in capacity, and Partial verification is used, the Falcon-NEO2 will use Full verification.
  - **FULL:** The wipe process will be fully verified, including all values set to be written to the Target drive. Selecting this verification method will double the total wipe and verification time.

6.3.2.3: Format



Formats the Destination using the NTFS, EXT4, exFAT, FAT32, EXT3, EXT2, or HFS+ file system with or without encryption. To format the drive (with or without encryption) tap the ***Settings*** icon.



Tap this icon to set the Falcon-NEO2 to format the drive (with or without encryption). The following settings are available:

- **Format –** When set to ***ON***, the Falcon-NEO2 will format the Destination drive with or without encryption. The drive will be formatted with the user's choice of file system (NTFS, EXT4, exFAT, FAT32, EXT3, EXT2, or HFS+). When set to ***OFF***, the Falcon-NEO2 will not format or encrypt the selected drive.
- **File System –** Select the file system to format the Destination drive. Users can select from NTFS, EXT4, exFAT, FAT32, EXT3, EXT2, or HFS+.
- **Encryption –** Select ***ON*** to format the drive with encryption.

For more information on encrypted Destination drives, please see ***Section 8: Drive Encryption and Decryption***.

6.3.3: Case Info

The Case Info setting allows users to enter some information about the case. However, Case Info is not required to start the wipe operation.

Information entered here will appear in the logs. ***Section 4.3.1*** provides more details of Case Info.

6.4: Push



The network Push feature allows users to push evidence files created by the Falcon-NEO2 from drives connected to the Falcon-NEO2 or from a Falcon-NEO2 repository to a network location or a Destination drive connected to the Falcon-NEO2. 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-NEO2 will generate a log file for each push process.

There are three selections when performing a push:

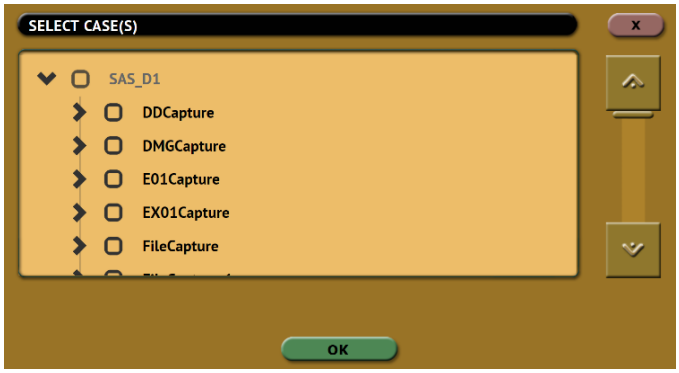
- Source
- Settings
- Destination

A network repository must be set up to push files to a network location. ***Section 6.9.1*** provides details on how to add a repository.

6.4.1: Source

Tap this icon to select the drive or repository from which the files are to be pushed (where the files to push are located).

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



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

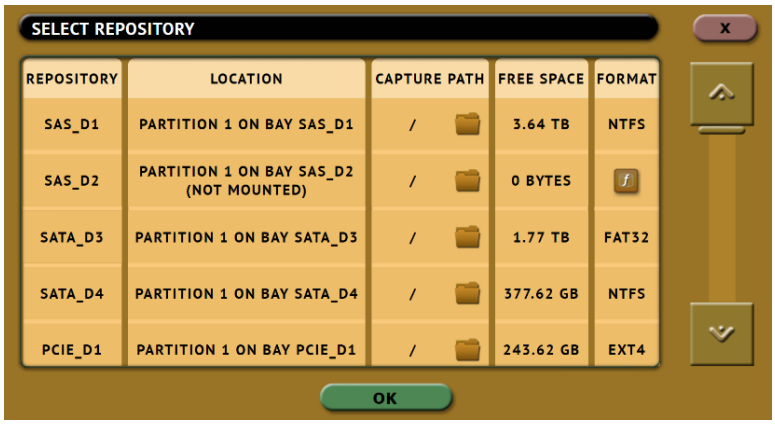
6.4.2: Settings

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

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

6.4.3: 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.



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 subfolder.
- **Delete Folder –** This is used to delete an empty folder. It cannot delete folders that contain files.
- **Rename Folder –** This will rename any folder.
- **OK –** Use this button when all desired changes have been completed.

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

6.5: Task Macro



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

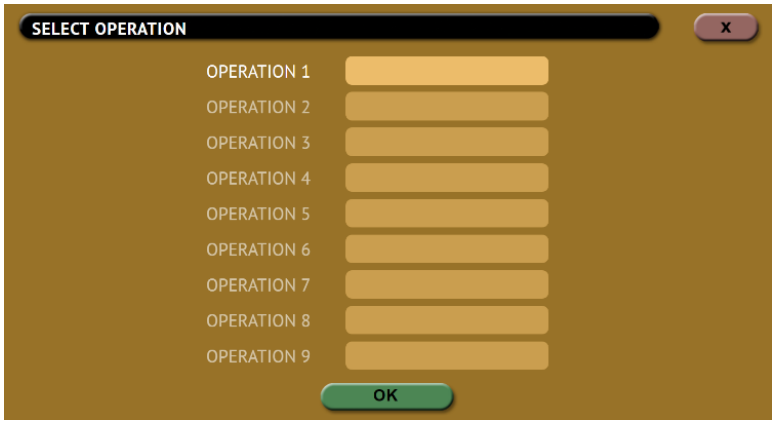
You can set each of the five macros by tapping the Macro tabs at the top of the screen.

Each task or operation must be set up before the macro can be set up. For example, to set up a Task Macro to perform a wipe and then an 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) have been set up, the Task Macro can be set.

6.5.1: 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 the desired operations. Each added operation will appear on the list. To delete an operation, tap the X to the right of it.



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

Tap the Start icon to start the macro and have the Falcon-NEO2 perform all the operations on the task list.

Example: Setting up a Macro for a Wipe to Secure Erase, then performing 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.

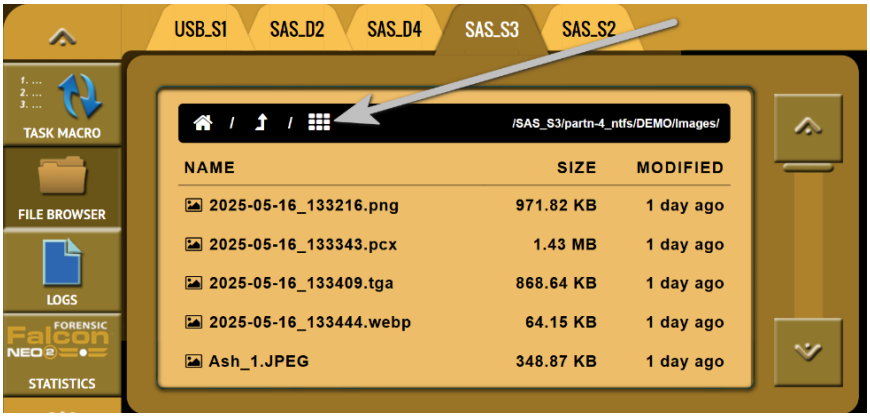
1. First, set the Wipe task. Select SAS_D1 as the Destination and change the setting to perform a Secure Erase (Wipe Patterns and Format set to off). **Do not start this task.**
2. Next, set the Imaging task. Select Drive to Drive as the Mode. Select the Source. Change the settings as needed. Select 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.

6.6: File Browser (Now with thumbnail view)



The Falcon-NEO2 has a built-in file browser. The File Browser allows the user to view the Source drive's partitions and contents, or image files created by the Falcon-NEO2 on the Destination drives. The file browser can also open several file types, such as most image files, .txt, .html, and .pdf. This method can be beneficial when the Falcon-NEO2 is out in the field and there are no computers to analyze or triage the drives' contents. Contents of DD, E01, EX01, DMG, and L01 image files can be viewed using the File Browser. The File Browser can also view various File systems, such as NTFS, EXT, FAT32, and APFS.

Thumbnail View: Images can now be displayed as thumbnails. To switch from list view to thumbnail view in the File Browser, tap or click the icon below:

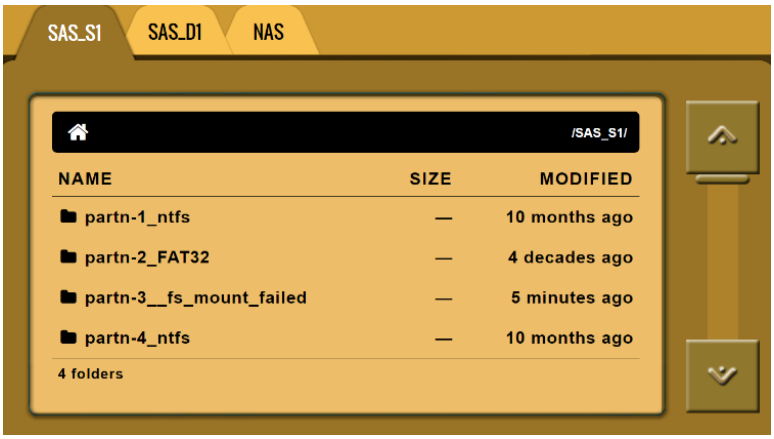


For Source drives, the Falcon-NEO2 displays all readable partitions.

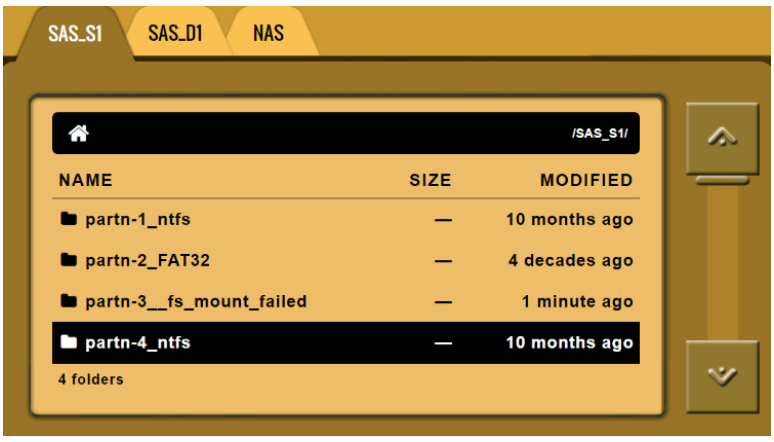
Only those destination drives formatted by the Falcon-NEO2 are shown, along with any DD, E01, EX01, DMG, L01, ZIP, or Directory Tree files created by the device.

6.6.1: Viewing Source Drives or Network Repositories

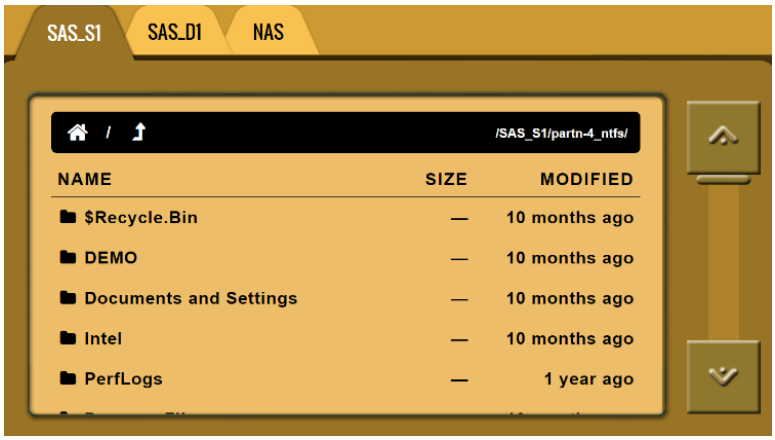
In the File Browser screen, select the Source Drive or Network Repository to view by tapping or clicking one of the tabs at the top of the screen:



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

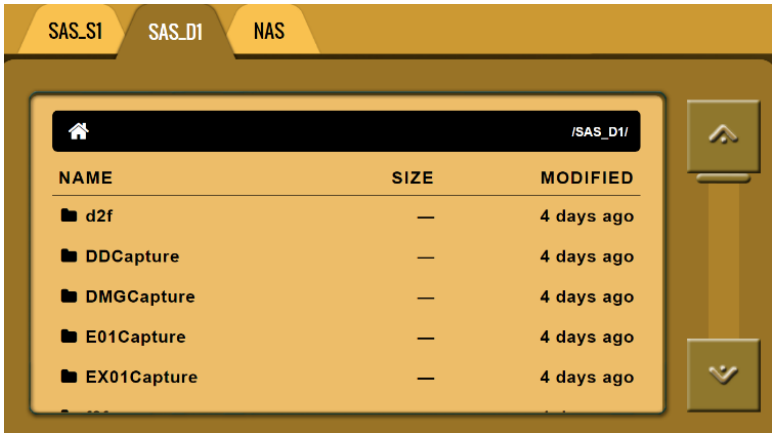


The folders/directories and files in that partition will be displayed:

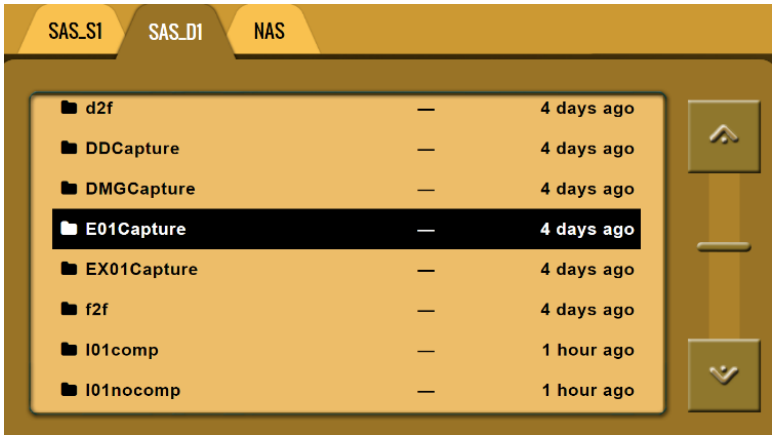


6.6.2: Viewing DD, E01, EX01, DMG, and L01 Images

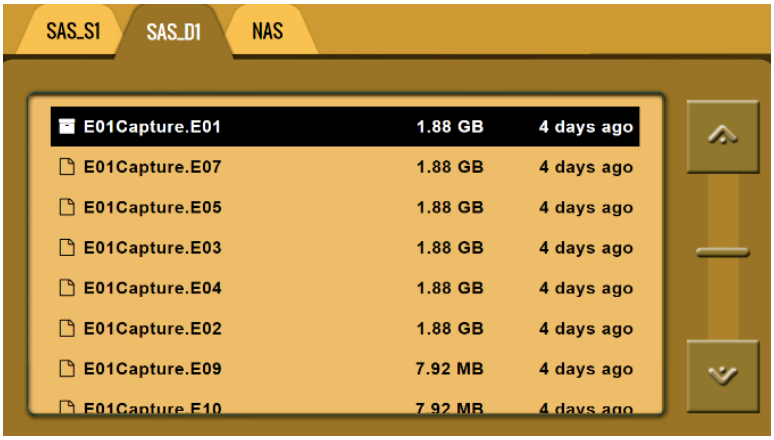
In the File Browser screen, select the Drive or Network Repository to view by tapping or clicking one of the tabs at the top of the screen:



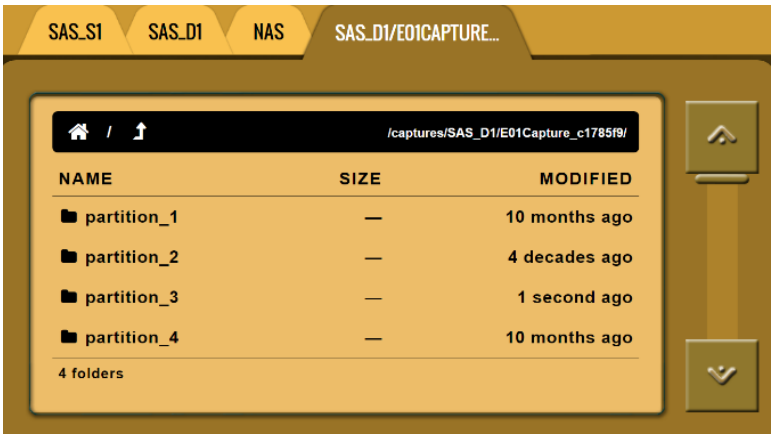
Select the folder where the image is located:



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

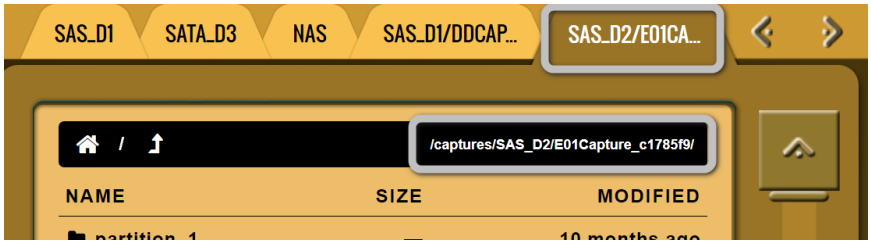


A new tab will appear showing the contents of the image file:

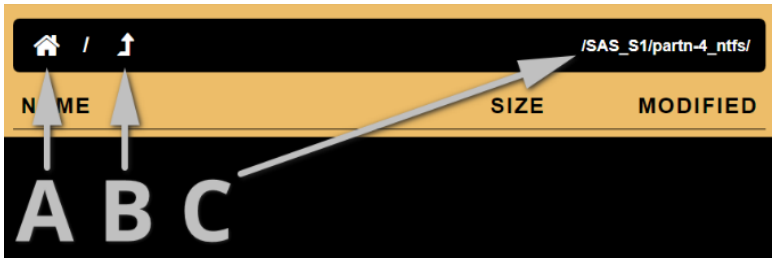


6.6.3: Additional Notes About Using the File Browser

- 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 move up one level (one folder/directory).

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

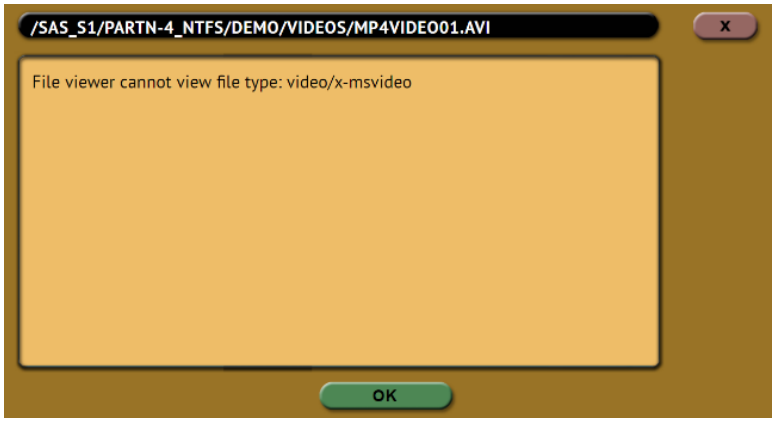
The Falcon-NEO2 can open and preview certain files. Some of the files that can be previewed are:

*.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-NEO2 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 access date and time.

6.6.4: Viewing Files from the Web Interface

The Falcon-NEO2's File Browser can also be used from the web interface. Using the web interface gives the ability to open files that the Falcon-NEO2 cannot preview by downloading the file to a computer (from which the Falcon-NEO2 is being browsed).

1. Connect to the Falcon-NEO2's web interface using a compatible web browser.

2. From the Falcon-NEO2'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, 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 must be able to open the downloaded file type. For example, if an MP4 file is downloaded, the computer needs software to open it.

6.7: Logs



The Falcon-NEO2 keeps logs of all imaging, hash, wipe, format, and push operations. Logs can be viewed directly on the Falcon-NEO2 or from a computer's browser (if the Falcon-NEO2 is connected to a network).

Section 3.8 Logs provides in-depth details on the log functions and options.

6.8: Statistics



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

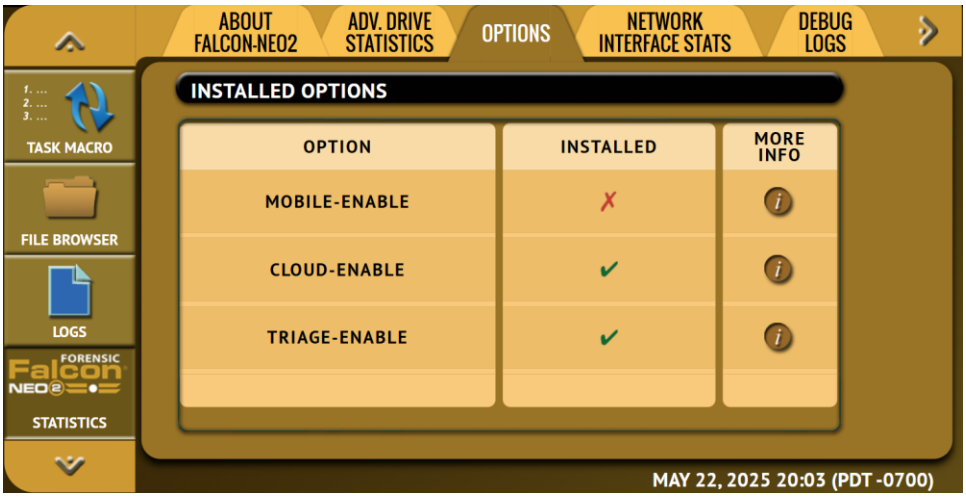
6.8.1: About Screen

The ***About*** screen will show information about the Falcon-NEO2, including the current software installed, hostname, and IP address. A QR code can be scanned on a phone or tablet. If the phone or tablet is connected to the same network as the Falcon-NEO2, it will open a web browser and connect to the Falcon-NEO2's IP address or hostname.

6.8.2: 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 the drive provides and is not translated.

6.8.3: Options



The ***Options*** tab displays software options and whether or not the option is installed on the unit.

To purchase an option or for more information, please contact Logicube Sales at sales@logicube.com or your region's international reseller. For a list of international resellers, visit https://www.logicube.com/sales/international-sales/.

If an option has been purchased but is not showing as installed, please contact Logicube Technical Support: support@logicube.com.

Depending on the Falcon-NEO2 serial number, some options may not appear on the screen.

6.8.3.1: Mobile-Enable

This option is for the Mobile Device Capture option, which acquires data from iOS and Android devices.

Section 13 has details on the Mobile Device Capture function.

For serial numbers 223000 and above – This is a standard, built-in feature and will be enabled.

For serial numbers below 223000 – Available as an annual, renewable software subscription. Contact sales@logicube.com or your region's international reseller for additional information. For a list of international resellers, visit https://www.logicube.com/sales/international-sales/.

6.8.3.2: Cloud-Enable

This option is for the Cloud Capture feature. All Falcon-NEO2 units should have this enabled.

Section 6.9.3 and ***Section 4*** provide details on the cloud capture feature. The cloud credentials must be entered as a repository, and then the file-to-file imaging mode must be used.

6.8.3.3: Triage-Enable

This option is for the Triage feature, which imports VICS Hash Databases and enables scanning of a source drive to compare file hashes against the VICS Hash Database.

For serial numbers 223000 and above: This is a standard, built-in feature and will be enabled. This option will appear in the Options tab.

For serial numbers below 223000: Available as a one-time upgrade. Contact sales@logicube.com or your region's international reseller for additional information. For a list of international resellers, visit https://www.logicube.com/sales/international-sales/. This option will only appear in the Options tab if purchased.

6.8.4: Network Interface Stats

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

6.8.5: 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.

6.8.6: 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-NEO2 is connected to a network with Internet access), tap the QR code.
- When using a web browser, click the QR code.
- Scan the QR code from a mobile phone or tablet with Internet access.

6.9: Manage Repositories



Repositories can be added to the Falcon-NEO2 using this operation.

The Falcon-NEO2 supports **Multi-Factor Authentication (MFA)** using Yubico's YubiKey 5 FIPS Series authenticators.

To use this MFA with the Falcon-NEO2, the Windows Active Directory and Domain must already be set up to support YubiKey 5 FIPS Series authentication using the authenticator and PIN access.

Please contact your IT department for any questions or requests for YubiKey authentication on the Active Directory and Domain.

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

- **Add/Remove** – Add, edit, or remove network repositories using the SMB (Server Message Block) or CIFS (Common Internet File System) protocol.
- **iSCSI** (Internet Small Computer System Interface protocol) – Add, edit, remove, connect, or disconnect iSCSI repositories.
- **Cloud –** Add or delete supported cloud drives.
- **Configuration –** Set the default file system when formatting a drive not previously formatted by the Falcon-NEO2. NTFS is set by default

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

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

- **PIN –** Enter the YubiKey PIN authentication if Multi-Factor Authentication is used. If Multi-Factor Authentication is not used, enter any six-digit number.

The following information is required to set up a cloud drive repository:

- The Falcon-NEO2 is connected to a network with Internet access.
- All login credentials for the supported cloud drive, including any two-factor authentication if required.

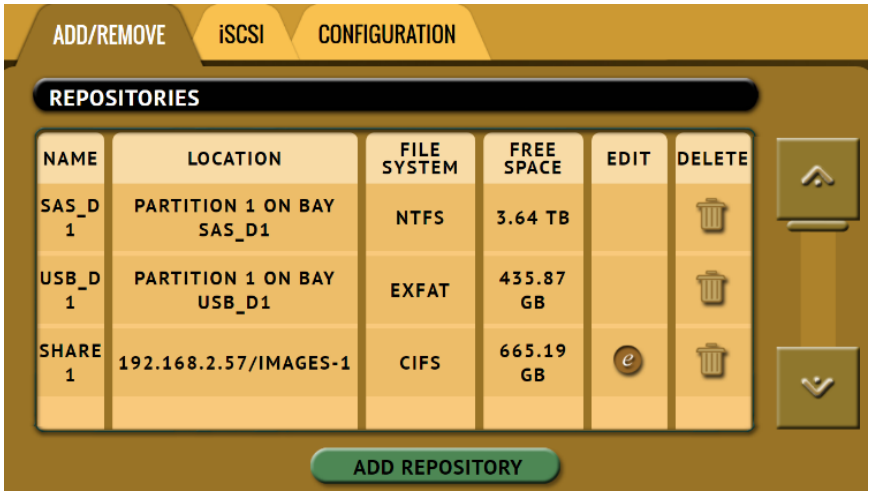
The following information is required to set up an iSCSI repository:

- **Portal –** The IP address or hostname 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 correctly.

6.9.1: Add/Remove

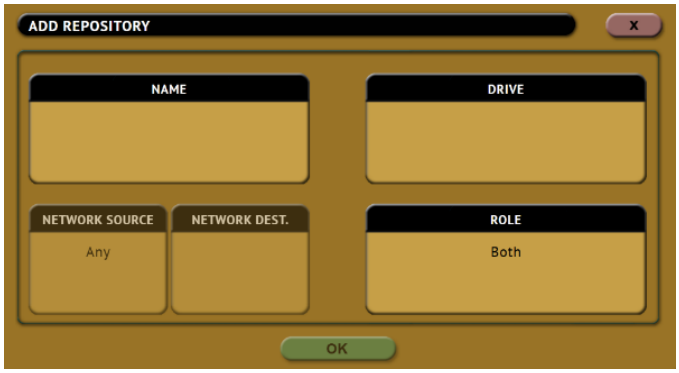
A list of repositories will be shown. The user has the option of adding or deleting a repository. This will include all drives attached to the Falcon-NEO2's destination ports and any networked repository.



If a repository location shows ***(NOT MOUNTED)***, it is because the Falcon-NEO2 did not format the attached drive, it cannot connect to the shared network resource, or the drive needs to be formatted (if it is a connected drive).

6.9.1.1: Adding a Repository Using CIFS or SMB

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



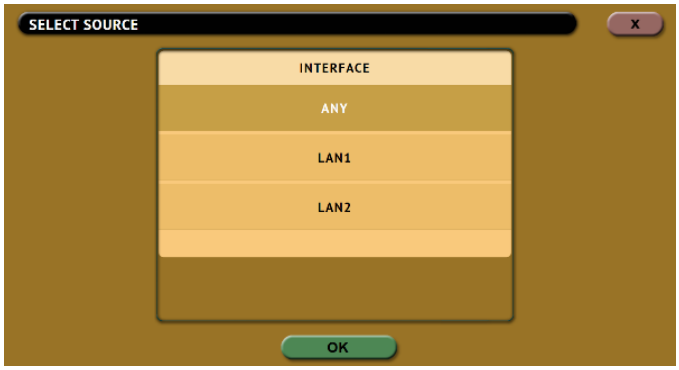
2. Tap ***Name*** to set the repository's name. Enter a name for this repository or network share. When finished, tap the ***OK*** icon.



3. From the ***Add Repository*** screen, tap ***Drive*** and select ***network share***. When finished, tap the ***OK*** icon.



4. From the ***Add Repository*** screen, tap ***Network Source*** to select the network interface. Choose from the following, then tap the ***OK*** icon.:



- **ANY –** The Falcon-NEO2 will use any connected network source (LAN1 or LAN2).
- **LAN1 –** The Falcon-NEO2 will prioritize data to/from this repository through the LAN1 port.
- **LAN2 -** The Falcon-NEO2 will prioritize data to/from this repository through the LAN2 port.

5. From the ***Add Repository*** screen, tap ***Network Dest***. to set the shared folder or repository's credentials. Enter the credentials, then tap the ***OK*** icon.



With software v2.0 and newer, the **PATH syntax** has changed and simplified.

PIN is a new entry with software 2.0 and newer. If YubiKey authentication is used, insert your YubiKey into any available USB port, then enter your PIN. **If no YubiKey authentication is used, please enter any six-digit number**.

- **PATH:** Input the shared IP address (or hostname) and the shared folder name. The proper syntax is:
  - **IP_ADDRESS\shared_name**

    Or
  - **IP_ADDRESS/shared_name**
- **DOMAIN:** If the shared folder is in a domain, input the domain name. If it is not in a domain, enter the workgroup name or leave this blank.
- **USERNAME:** Enter the username. The user must have full access (read and write) to the shared folder.
- **PASSWORD:** Enter the user's password.
- **PIN:** If YubiKey authentication is used, insert your YubiKey into any available USB port, then enter your PIN. **If no**

YubiKey authentication is used, please enter any six-digit number.

Optional: Tap ***Role*** and input the role for this repository. By default, it is set to BOTH. Other options include SOURCE or DESTINATION. Tap ***OK*** when finished.

6.9.1.2: 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.

6.9.1.3: Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) requires an existing user in a Domain and Active Directory already set up for use with Yubico's YubiKey 5 FIPS Series Authenticators.

Logicube cannot assist with setting up a Domain or Active Directory with YubiKey authentication. Please consult with your IT department; if needed, the IT department can contact Yubico for assistance.

A networked repository must be set up to use Multi-Factor Authentication.

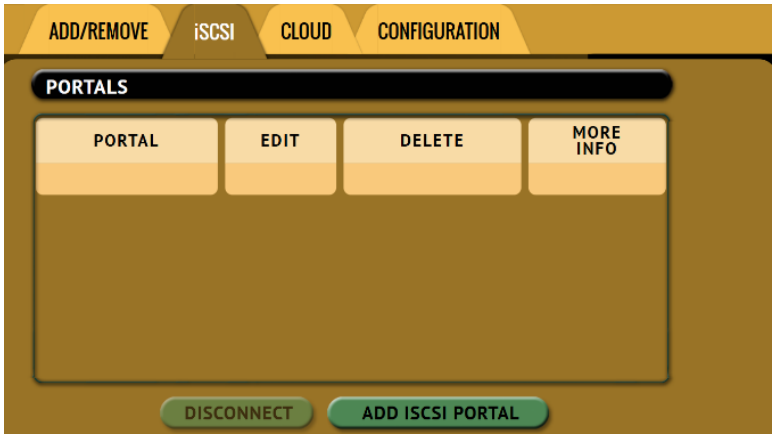
6.9.2: iSCSI

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

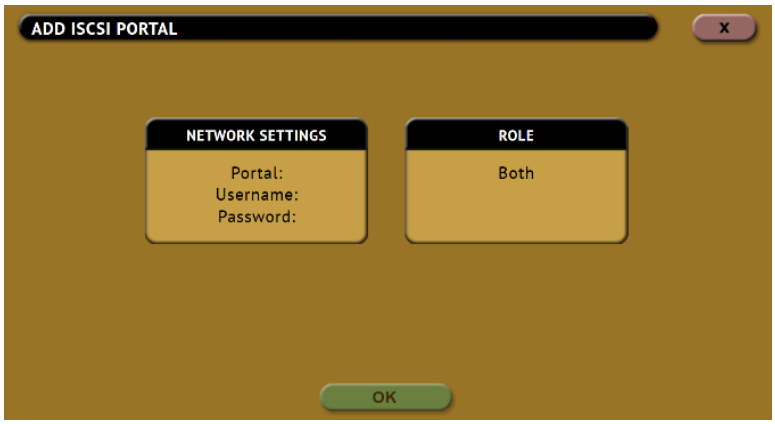
To add a repository using the iSCSI protocol, an iSCSI Target must be set up on the remote system. Since networks are configured differently, a Systems Administrator or Network Administrator may be needed to set up the iSCSI protocol.

Once the iSCSI Target has been set up:

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.

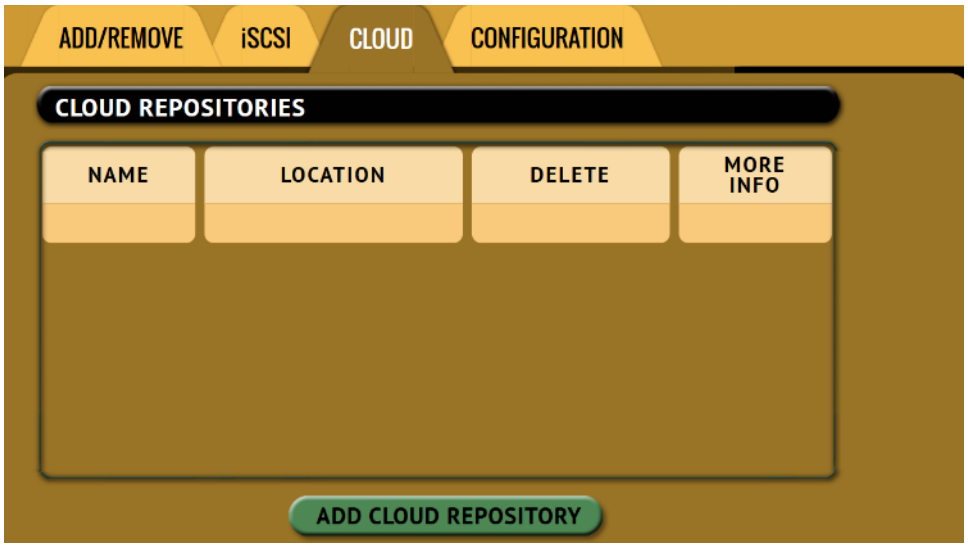


Optional: Tap ***Role*** and input the role for this repository. By default, it is set to BOTH. Other options include SOURCE or DESTINATION. Tap ***OK*** when finished.

4. Tap ***OK*** when finished. The screen will go back to the ***Portals*** screen.
5. In the ***Portals*** screen, tap the iSCSI portal to highlight it, then tap ***Connect***.
6. The Falcon-NEO2 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***.

6.9.3: Cloud



This screen allows a user to add or delete a cloud repository. Currently, Google Drive, Dropbox, and OneDrive are supported.

When a computer is used (using the web interface) to set up a cloud drive, the computer's browser settings may prompt to save login information. Logicube and the Falcon-NEO2 cannot control this. It is a setting on the computer browser. It is recommended not to save login information in the browser. When using the Falcon-NEO2 screen, the Falcon-NEO2 will not prompt or store any login information to the cloud drive.

All added cloud repositories are not persistent and cannot be saved to a profile. To delete a repository, users can use the delete icon from the GUI or turn the Falcon-NEO2 off.

Setting up a cloud repository requires one of the following:

- An attached USB keyboard, or
- Use of the Web Interface (Web interface is not supported when adding OneDrive or Google Drive)

6.9.3.1: Adding a Cloud Repository

Follow these steps to set up a cloud repository. Once the cloud repository is set up, use the ***File to File*** imaging mode to image files from the cloud drive.

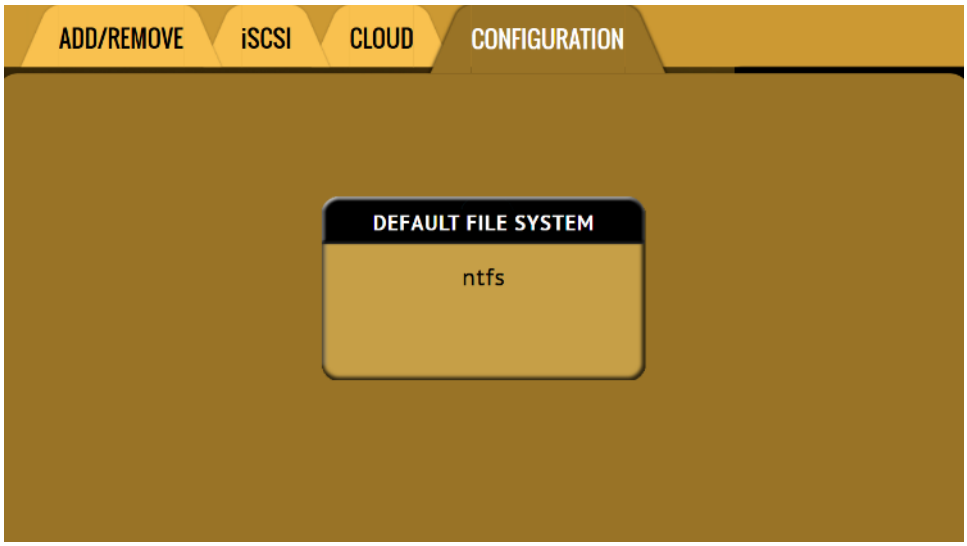
1. From the ***Manage Repositories*** screen, tap or click the ***Cloud*** tab.
2. At the bottom of the screen, tap or click ***Add Cloud Repository***. The ***Add Cloud Repository*** screen should appear.
3. In the ***Add Cloud Repository*** screen, select the ***Type*** of cloud drive to use, then tap or click ***OK***.



OPTIONAL: Set the ***Name*** of the cloud repository.

4. Follow the on-screen instructions to set up the cloud account.

6.9.4: Configuration



This screen allows users to set a default file system when formatting a drive. This setting only configures the ***Format Repository*** screen 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.

6.10: System Settings



The ***System Settings*** screen allows users to configure the following settings for the Falcon-NEO2:

- Profiles
- Passwords
- Encryption

- Language/Time Zone
- Display
- Destination Whitelist
- Notifications
- Advanced
- Debug

To access the other tabs in the System Settings screen, tap the right navigation arrow below the Falcon-NEO2 logo (located at the top right of the screen). To see the previous tabs, tap the left navigation arrow.



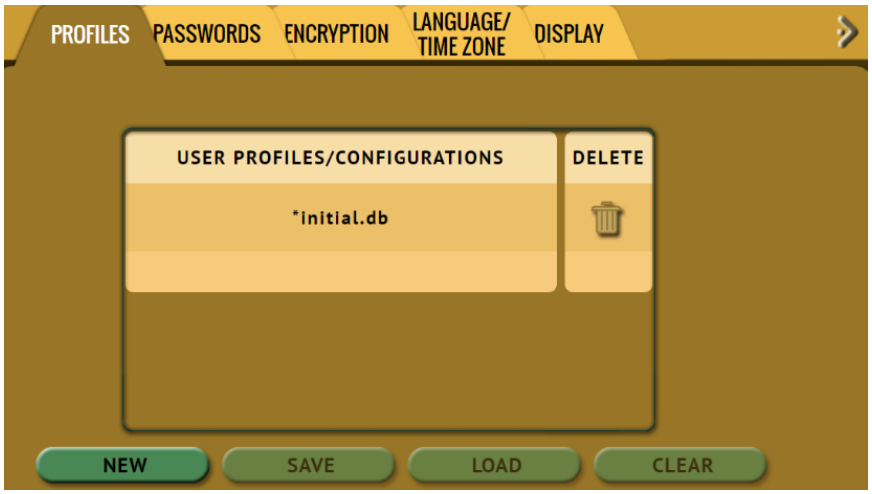


6.10.1: Profiles

Do not highlight and save over the INITIAL.DB profile. This is the Falcon-NEO2's default profile, which is used to reset the Falcon-NEO2 to the factory default settings.

This screen shows all user profiles. The following selections are available in this screen:

- **New –** Allows the user to create a new profile name.
- **Save –** Saves the selected profile.
- **Load –** Loads the selected profile.
- **Clear –** Clears the selected profile of all saved settings and resets the profile to contain default settings. After clearing the selected profile, it must be saved to load for future use.



The currently loaded profile is the asterisk (*) next to the profile name.

After loading a profile, it is recommended that the user interface be refreshed. This can be done in one of two ways:

- Go to the POWER OFF menu using the touchscreen 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 profiles with different configurations. When a profile is loaded using the Load icon, the Falcon-NEO2 loads it immediately and will continue to load it during its boot process.

For example, if the user wants the Falcon-NEO2 to always boot up with the default imaging mode to ***Drive to File*** with the setting of ***E01*** with a segment size of ***2GB***:

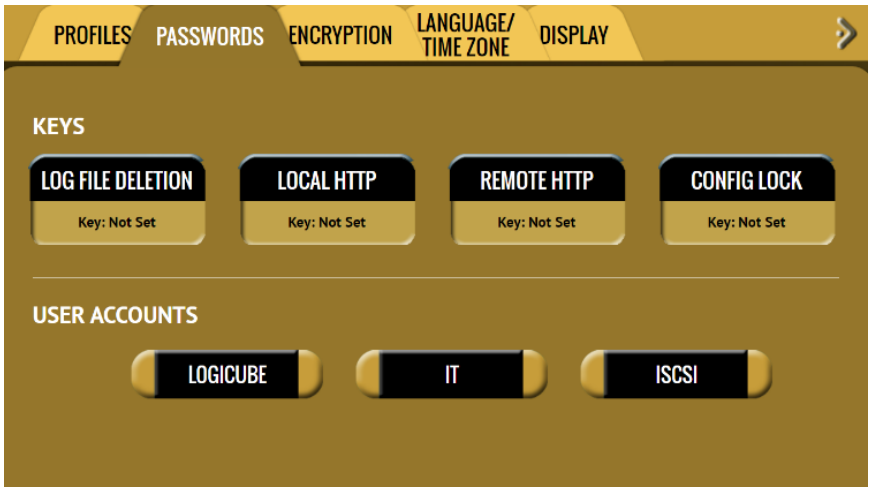
1. Turn the Falcon-NEO2 off and then back on. This step is important to ensure that only the desired changes are saved.
2. Go to the ***Imaging*** screen and set the ***Mode*** to Drive to File.
3. In the ***Settings***, set the image to ***E01*** and the segment size to ***2 GB***.
4. Go to Profiles and tap the New icon in the System Settings.
5. Type a name for this profile, such as 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. Highlight the profile to be loaded (during the boot process) (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.

To delete a profile, tap the ***delete*** icon. A confirmation screen will appear. Tap the ***Yes*** icon to delete the selected profile. The currently loaded profile cannot be deleted; to delete the currently loaded profile, a different profile must be loaded first.

When loading a profile, it may take several seconds to completely load the different profile.

6.10.2: Passwords

Seven keys or passwords can be set or changed.



- **Key: Log File Deletion –** A key can be set to provide 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 Falcon-NEO2's touchscreen. 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 on any web browser accessing the Falcon-NEO2, 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. Also, case information can be edited or entered while Config Lock is enabled

  For example, if the Config Lock key is set, and the IMAGE task is configured for Drive to File imaging, the user cannot 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 password.
- **User Account: IT –** Allows the user to change the ***it*** local account password.
- **User Account: ISCSI** – Allows the user to change the ***iscsi*** local account password.

6.10.2.1: Setting Key Passwords

Tap one of the buttons to set a key for Log File Deletion, Local HTTP, Remote HTTP, or Config Lock. 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 lock the configuration automatically and require a key. By default, this is set to 1 minute.

Remember the various keys! If the Falcon-NEO2 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 6.10.2.1.2*** for more information.

If the initial.db has a key configured but forgotten, contact Tech Support for assistance.

6.10.2.1.1: Config Lock Notes

A shortcut (and indicator) to the ***config lock*** can always be seen on the Falcon-NEO2's screen. It is at the top right of the screen, next to the Falcon-NEO2 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. Case info can be entered or edited by tapping or clicking ***Settings***
- **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. Case info can be entered or edited.
- **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. Case info can be entered or edited.

- **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. Case info can be entered or edited by tapping or clicking ***Settings***.
- **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 this operation does not have settings or configurations**, Config Lock does not affect it.
- **Manage Repositories –** A managed repository cannot be added, edited, or deleted without the Config lock unlock key.
- **System Settings –** This section cannot be accessed without the Config lock unlock key.
- **Network Settings –** This section cannot be accessed without the Config lock unlock key.
- **Software Updates –** This section cannot be accessed without the Config lock unlock key.
- **Power Off –** This section cannot be accessed without the Config lock unlock key.

The Falcon-NEO2 can still be turned off without the unlock key by using the power button on the top of the Falcon-NEO2.

6.10.2.1.2: Forgotten password for any keys

If any of the keys are forgotten, the INITIAL.DB profile must be loaded using the Command Line Interface (CLI).

This method will only work if the INITIAL.DB profile does not have a Config Lock Key saved. Contact Tech Support if the INITIAL.DB has a configured Config Lock Key, but the password was forgotten.

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 primary 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-NEO2 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-NEO2 is turned on.

```
it@falcon2-220000(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. A response should show ***"Command (DbManagement) Successful."***
6. Type ***db list*** again; there should be an asterisk (*) on the initial.db.
7. Turn the Falcon-NEO2 off using the power button, then close the Telnet/SSH application.
8. Turn the Falcon-NEO2 on. When the Falcon-NEO2 boots up, it will load the default configuration (INITIAL.DB).

6.10.2.2: User Account Passwords

The Falcon-NEO2 comes with the following built-in user accounts:

- logicube
- it
- iscsi

All user account passwords can be changed on this screen. To change the password for any 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*** **do not need to be saved in a user profile**. Changing any of these passwords will take effect immediately. If the User Account password is forgotten, contact Tech Support for assistance.

6.10.3: Encryption

The Falcon-NEO2 can secure sensitive evidence data with whole disk drive encryption using the NIST-recommended XTS-AES-256 cipher mode. Destination drives that the Falcon-NEO2 encrypts can be temporarily decrypted by using the Falcon-NEO2 or third-party software (VeraCrypt, TrueCrypt, or FreeOTFE).

> For in-depth information on encrypting and decrypting a drive using the Falcon-NEO2, or decrypting a drive using VeraCrypt, TrueCrypt, or FreeOTFE, please see ***Section 8: Drive Encryption and Decryption***.

The following settings must be configured before encryption can be used. These 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. This is 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 encryption password/key.

Falcon-NEO2 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.

6.10.4: Language/Time Zone

The Falcon-NEO2 menu system's language can be changed. The available languages are English, Chinese Traditional (中文), Italian (ITALIANO), Korean (한국어), Japanese (日本語), and POLISH.

This screen also allows the time zone to be set.

6.10.4.1: Language

The following languages are available:

- ENGLISH
- CHINESE TRADITIONAL (中文)
- ITALIAN (ITALIANO)
- KOREAN (한국어)
- JAPANESE (日本語)
- POLISH

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

To change the displayed language, select the desired language. When you choose the language, the Falcon-NEO2'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-NEO2's screen, the language in the web browser will not change unless it is changed through the web browser.

6.10.4.2: Time Zone

The Falcon-NEO2 utilizes NTP (Network Time Protocol). Each time it is connected to a network with internet access, it automatically checks for the correct time using NTP and adjusts it as needed.

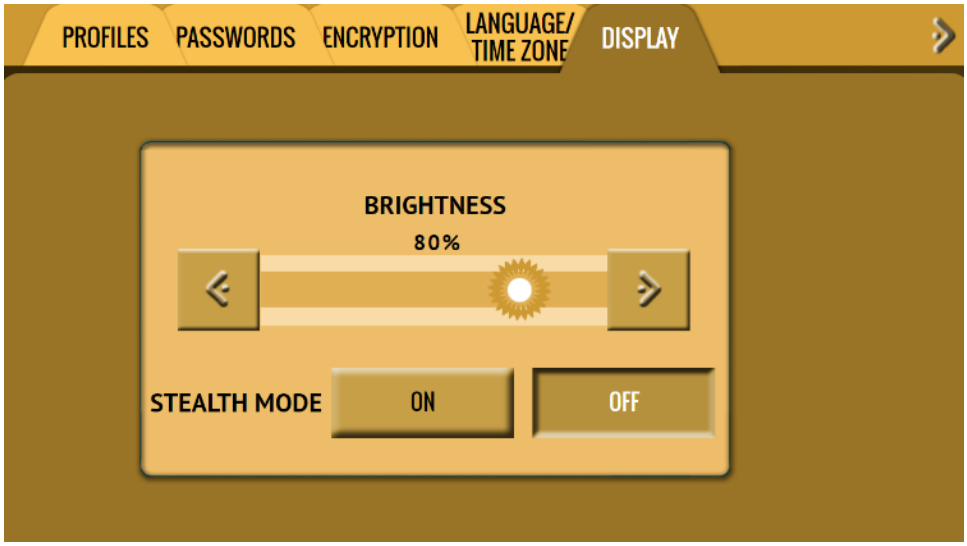
The Falcon-NEO2 also has a time zone setting. Tap ***Time Zone*** to select the time zone region. Tap the ***OK*** icon to continue.



After selecting the region, select the time zone where the Falcon-NEO2 is located. Tap the ***OK*** icon to set the time zone.



6.10.5: Display



Brightness: The Falcon-NEO2's screen brightness may need to be adjusted, depending on the user's preference. Use the screen's left or right arrow icons to adjust the brightness. The screen's brightness will adjust accordingly.

The screen brightness cannot be saved and loaded as a user profile. It is reset to 80% each time the Falcon-NEO2 boots.

Stealth Mode: Stealth mode turns the Falcon-NEO2's screen off, allowing privacy so no one can see what the Falcon-NEO2 is doing. When Stealth mode is activated, currently running operations continue to run.

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

Tap anywhere on the screen to turn Stealth mode off and restore the Falcon-NEO2's display.

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

6.10.6: Destination Whitelist

The Destination Whitelist screen allows users to view, select, upload, or clear the Destination Whitelist.

When a Destination Whitelist is uploaded or selected, only the drives listed on the Whitelist can be used as a Destination drive for any Imaging or Wipe task. If the Whitelist is empty or blank, any drive may be used as a Destination drive for any Imaging or Wipe task.

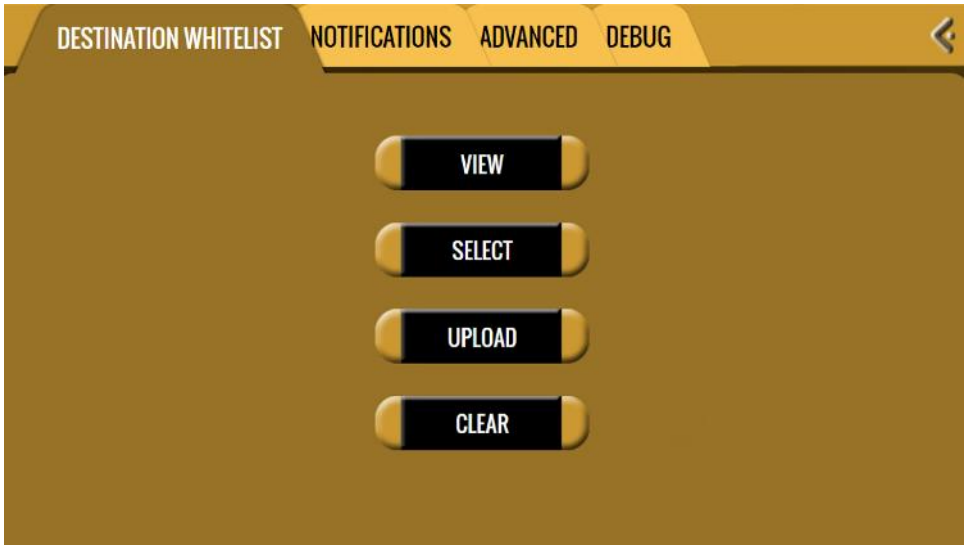
When a drive not on the Destination Whitelist is used as a destination drive on any Imaging or Wipe task, the user will see the following message when the task is started:

Generic system error!

Task start failed: Target in Bay USB_D3 is Not allowed!

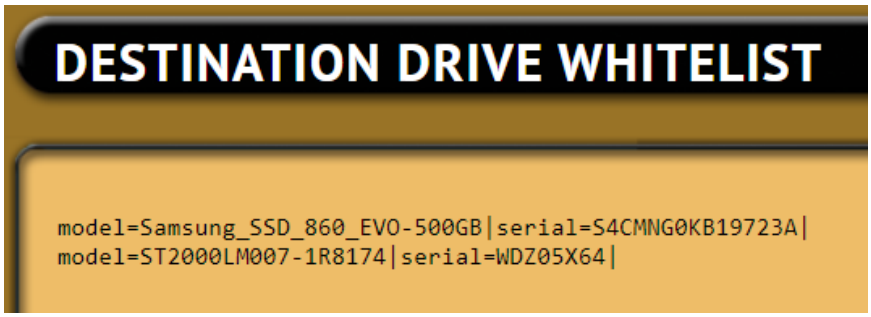
The Destination Whitelist file (list of drives to be selected or uploaded) requires the following:

- The file must be in CSV format.
- The file must be saved with the extension *.CSV (for example whitelist.csv).
- There must be two columns separated by a comma: **DRIVE_MODEL,SERIAL_NUMBER**
- There must be an empty line (or carriage return) at the end of the list.



6.10.6.1: View

This button allows the user to view the drives in the Destination Whitelist. Each line in the whitelist should show the drive's model and serial number.



If the whitelist is empty/blank, the ***View*** button will show the following screen:



6.10.6.2: Select

This screen allows users to select a Destination Whitelist file from a connected drive. Save the *.csv file to a drive, then connect the drive to one of the available ports on the Source side. The whitelist file can also be selected from any connected/mounted network repository drive.

Select the drive, partition, locate the *.csv file, and tap/click ***OK***.



A password screen will appear. The default password is the same as the ***Logicube*** account password, which is logicube. Enter the password, then tap/click ***OK*** to continue.



6.10.6.3: Upload

This screen allows the user to upload a Destination Whitelist file from a computer connected to the same network as the Falcon-NEO2. Save the *.csv file somewhere on the computer, then use a web browser to browse the web interface.

After selecting the *.csv file, a password screen will appear. The default password is the same as the ***Logicube*** account password, which is logicube. Enter the password, then tap/click ***OK*** to continue.



6.10.6.4: Clear

This button clears the Destination Whitelist. When this button is selected, a confirmation screen will appear. Tap/click ***Yes*** on the confirmation screen to clear the Destination Whitelist.

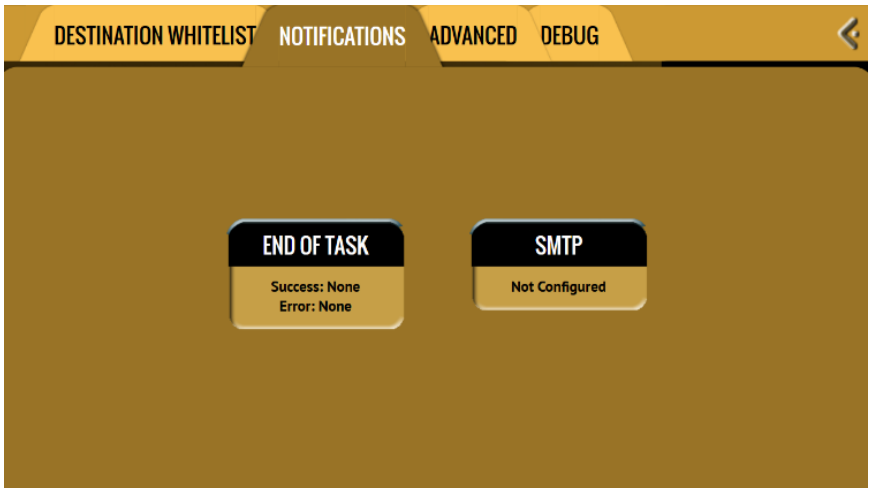


A password screen will appear. The default password is the same as the ***Logicube*** account password, which is logicube. Enter the password, then tap/click ***OK*** to continue.

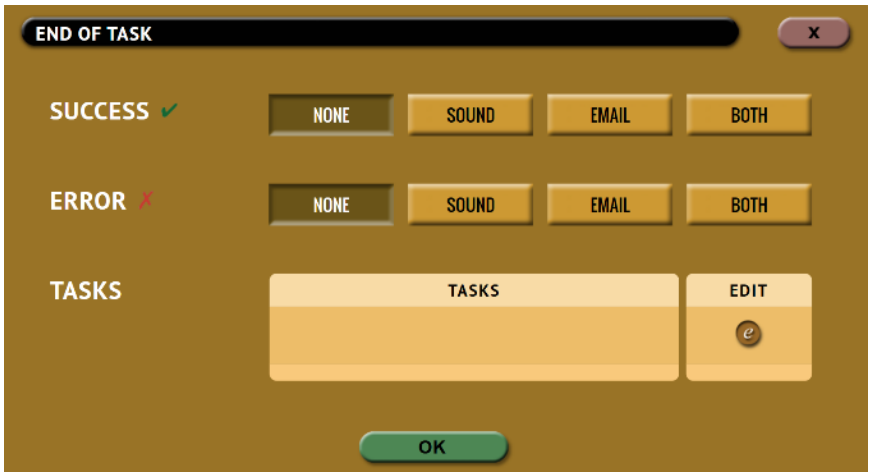


6.10.7: Notifications

The Falcon-NEO2 can produce audible notifications (beeps) or send an email/SMS when a task finishes successfully or if an error appears.



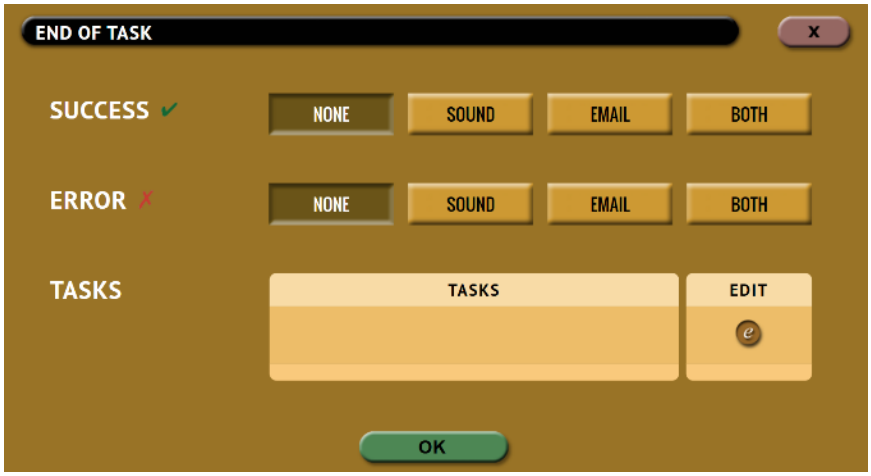
6.10.7.1: Sound Notifications



To set up Sound notifications:

1. Tap ***End of Task*** to configure the notifications.
2. Select ***Sound*** for Success and/or Error to configure audible notifications for when the Falcon-NEO2 has a successful task or if the task has an error.
3. Tap the ***OK*** icon when finished.

6.10.7.2: Email/SMS Notifications



The Falcon-NEO2 can send out email or SMS notifications. A valid email account (to send from) and SMTP access are required.

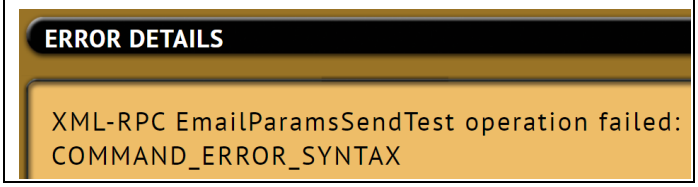
Email/SMS notifications require the Falcon-NEO2 to be connected to a network with Internet access.

To set up email/SMS notifications, the email account from which notifications are sent must be configured first:



1. Tap or click ***SMTP*** to configure the "from" email account.
2. Enter the following information:
    a. ***SERVER –*** This is the SMTP server to be used.
    b. ***USERNAME –*** The username or login for the email account.
    c. ***PASSWORD –*** The password for the email account.
    d. ***EMAIL TO –*** Email address where the notification will be sent to.
    e. ***ATTACH REPORT –*** Select ***Yes*** to include the auditlog file.
3. Tap or click ***SEND TEST*** to send a test notification.

If the server, username, or password is incorrect, the following error will appear:



4. If the test notification is successful, tap ***OK*** to continue.
5. Tap ***End of Task*** to configure the notifications.
6. Select ***Email*** for Success and/or Error to configure email/SMS notifications for when the Falcon-NEO2 has a successful task or if the task has an error.
7. Tap the ***OK*** icon when finished.

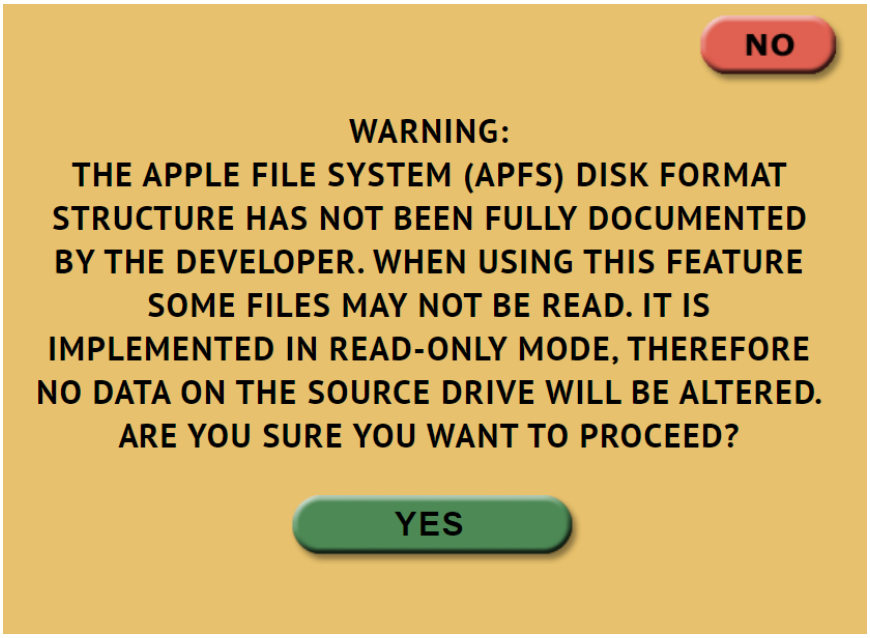
6.10.7.2.1: Additional Notes for Email/SMS Notifications

The following are additional notes for configuring Email/SMS notifications:

- Emails with multi-factor authentication are not supported.
- Yahoo Mail requires additional authentication by generating a third-party app password. Users must log in to Yahoo Mail's website, then go to Account Info, then Account Security. Search Yahoo for "Generate third-party app passwords" for up-to-date information on how to generate this password. Instead of using the account/email password in the SMTP configuration screen, the third-party app password must be used in the ***PASSWORD*** field.
- Gmail no longer supports third-party apps that sign in using only the username and password (what they call "less secure apps"). Since this change occurred, notifications through Gmail are no longer supported by the Falcon-NEO2.
- **SMS notifications –** Many wireless carriers have an email to SMS/MMS address that can be used to receive SMS/MMS notifications through email. Enter the Email-to-SMS address format in the ***EMAIL TO*** field. Contact your wireless carrier to find out what email to SMS/MMS address to use.
- Users may have to contact their email provider, IT department, or wireless carrier for the correct SMTP server, username, password, and/or Email-to-SMS address format.

6.10.8: Advanced

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:



6.10.9: Debug

This screen may adversely affect PCIe and/or NVMe performance. Please do not make changes to it unless instructed to by Logicube Technical Support.

6.11: Network Settings



The Network Settings screen has the following tabs: ***Interfaces***, ***HTTP Proxy***, ***Network Configurations***, ***HTTPS***, and ***802.1x***.

6.11.1: Interfaces

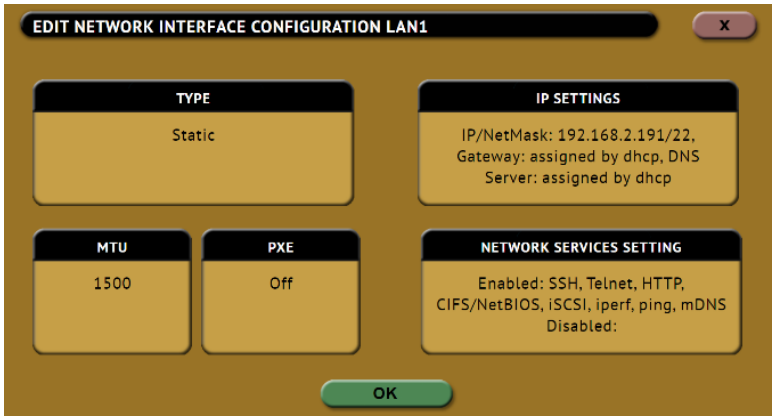
The Interfaces tab displays the network interface information (MAC Address, Configuration type (DHCP or Static), MTU, and link status). A static IP or DHCP can be set on this screen. This tab also allows for the enabling or disabling of certain network services. To edit the network interface configuration, tap the Ethernet adapter name and the Edit Configuration button.

There is a PXE button for future use.

6.11.1.1: Configuring a Static IP address

DHCP is enabled by default. Some networks do not support DHCP and require a static IP address. The steps below outline configuring the unit with a static IP address.

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.

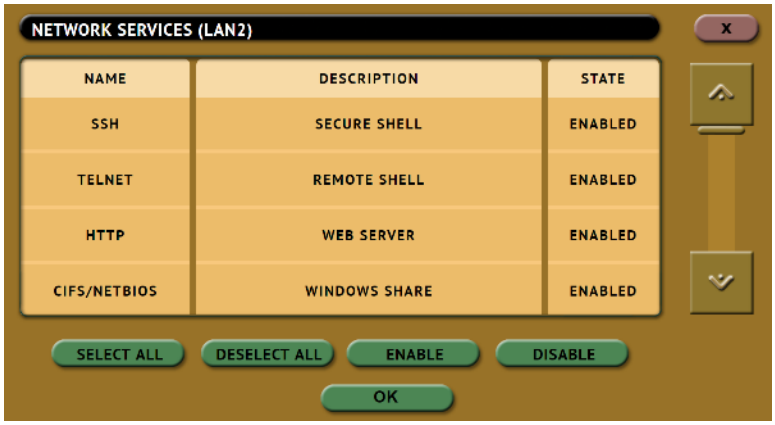


6.11.1.2: MTU

Users can set the MTU (Maximum Transmission Unit) value on this screen. The default is 1500. Check with your network or IT administrator to determine the correct value.

6.11.1.3: Enabling/Disabling Network Services

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



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

The following services can be disabled (enabled by default):

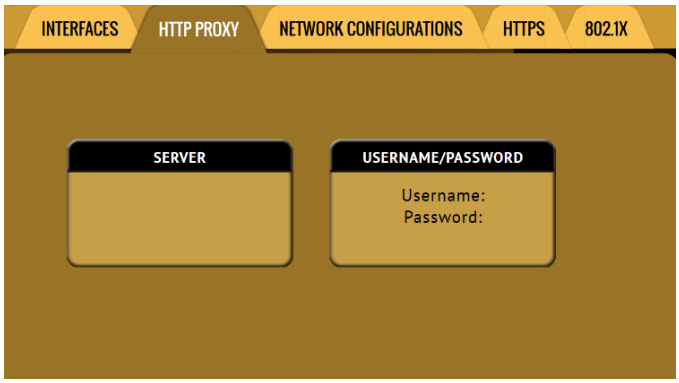
- **SSH –** Disabling this will block Secure Shell (SSH) traffic.
- **Telnet –** Disabling this will block Telnet traffic.
- **HTTP –** Disabling this will block web browser connections to the Falcon-NEO2.
- **CIFS/NETBIOS –** Disabling this will block any CIFS or NETBIOS connection to the Falcon-NEO2 (for example, Windows File 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-NEO2.
- **MDNS –** Disabling this will block outgoing Multicast DNS packets from the Falcon-NEO2.

Disabling any of the services above will disallow the types of communication controlled by those services. For example, if HTTP is disabled, users cannot access the Falcon-NEO2 through a web browser over the network.

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

6.11.2: HTTP Proxy



If Internet access through a proxy server is required, proxy settings will need to be set for the Falcon-NEO2 to update software from a network (over the Internet). This typically includes a server (or IP address), a host port, a username, and a password.

6.11.2.1: Server



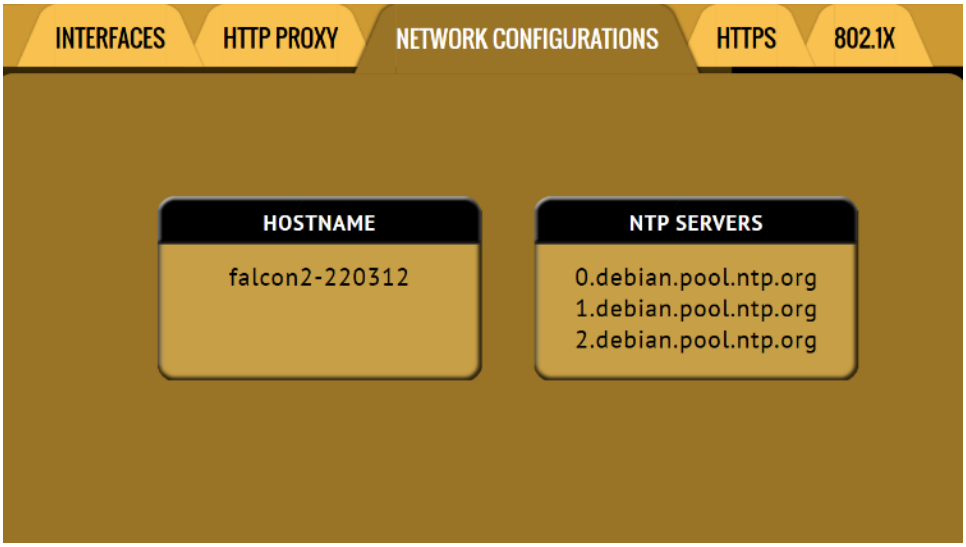
Tap the Server icon to set the IP address (or server name) and proxy server port.

6.11.2.2: Username/Password



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

6.11.3: Network Configurations

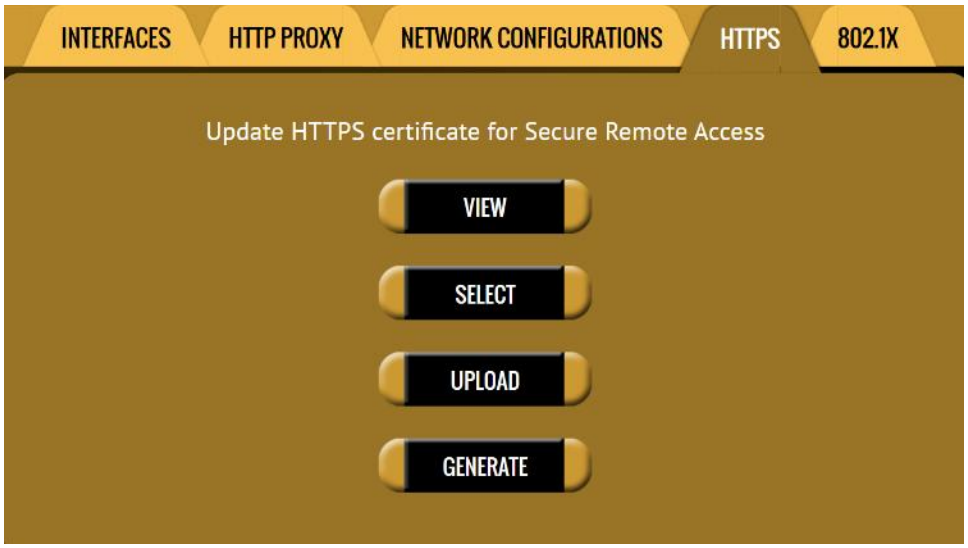


This tab allows you to configure the Falcon-NEO2's hostname and NTP Server list. Changes made on this screen take effect immediately.

Multiple NTP server entries are separated by a space. For example:

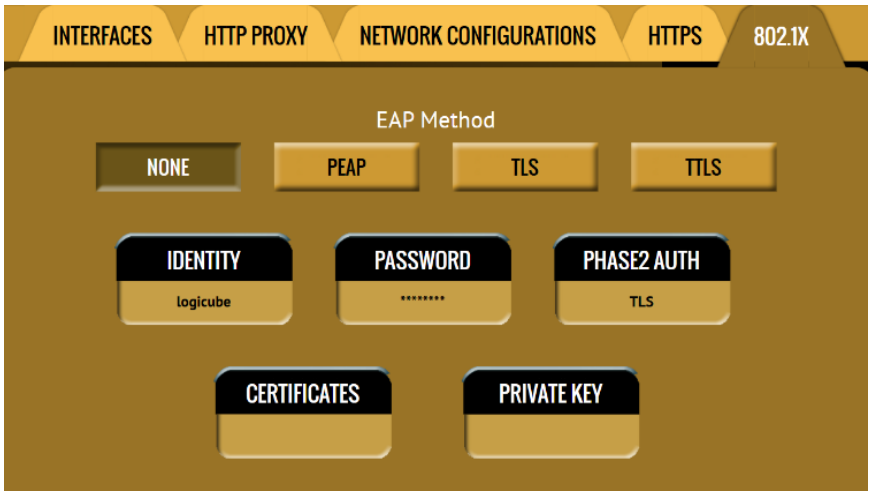
ntp-b.nist.gov time.google.com us.pool.ntp.org

6.11.4: HTTPS



HTTPS certificates are required for secure remote access. This tab lets users view, select, upload, or generate HTTPS certificates.

6.11.5: 802.1X



802.1X is a network authentication protocol that opens ports for network access when an organization authenticates a user's identity and authorizes them for access to the network. The user's identity is determined based on their credentials or certificate, which the RADIUS server confirms. The user's network must already be configured to use 802.1X.

- **Extensible Authentication Protocol (EAP) Method:** Select the EAP method used by the 802.1X network. Available methods are NONE, PEAP, TLS, and TTLS.
- **Identity:** Input the identity name.
- **Password:** Input the password.

- **Phase 2 Authentication:** Select phase 2 authentication. The available authentication methods are PAP, CHAP, MSCHAP, MSCHAPV2, and TLS.
- **Certificates:** On this screen, users can view, select, or upload the CA or Client certificate.
- **Private Key:** The private key screen allows users to view, select, upload, or input the passphrase.

6.12: Software Updates



New and improved software will be released from time to time. The Falcon-NEO2 can be updated using two methods: 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-NEO2 software, please read the ***Falcon-NEO2 Software readme*** file located on the Falcon-NEO2 Support page on the Logicube website at http://www.logicube.com/knowledge/forensic-falcon-NEO2.

In-depth information on updating the Falcon-NEO2 software can be found in ***Section 8: Updating/Loading/Re-loading Software***.

The ***PXEBOOT Update*** tab is reserved for future use.

6.13: Power Off



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

POWER OFF: This tab lets you remotely turn off the Falcon-NEO2 and refresh the Graphic User Interface (GUI).

DRIVE POWER: This tab allows you to set inactive drives connected to the Falcon-NEO2 to go to standby mode. The default is 0 minutes (Off/Disabled).

7: Previewing Drives

Section 7: Previewing Drives - Introduction

The contents of drives connected to the Source and Destination ports can be previewed. There are four different methods available to preview the drive contents with the Falcon-NEO2:

- Falcon-NEO2's native File Browser
- A computer with the Falcon-NEO2'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.

	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-NEO2 to the computer 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-NEO2 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. The computer's Operating System has more powerful viewing capabilities than the File Browser alone.
SMB	All files supported by the OS or installed software	Logical access to partitions is 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.

7.1: File Browser

See ***Section 6.6*** for details on how to use the File Browser.

7.2: Computer + File Browser

The Falcon-NEO2 can be accessed from a computer (with a direct network cable connection or on a network). Using a computer with the Falcon-NEO2's file browser allows more files to be previewed 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-NEO2's web interface (See ***Section 10.1*** for more information on the web interface) allows the user to open files that the Falcon-NEO2 cannot open using the file browser alone. See ***Section 6.6.4*** for details on how to use the File Browser using the web interface.

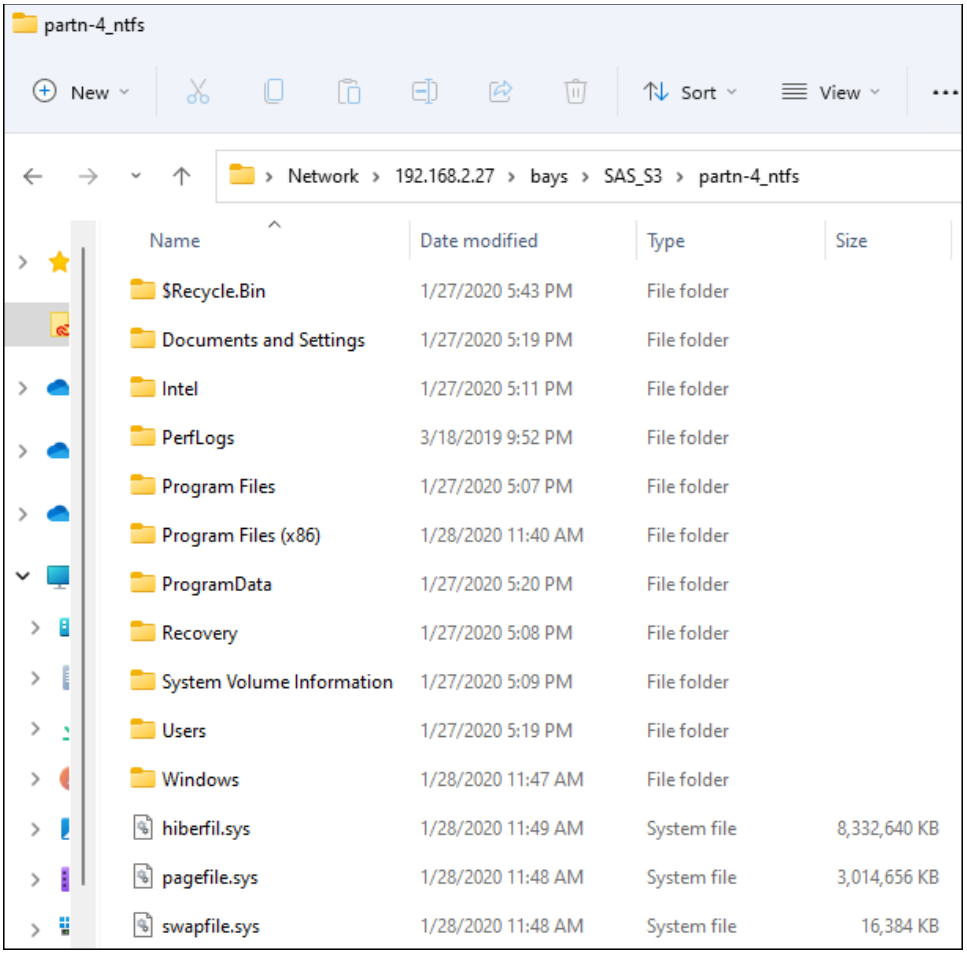
7.3: SMB

The Falcon-NEO2 can be accessed from a computer (with a direct network cable connection or on 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 11.1*** for details on how to view Source or Destination drives over the network using SMB.

Some advantages of using this method are:

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



7.4: iSCSI

Another way to access Source drives from a computer (with a direct network cable connection or on a network) is through the iSCSI protocol. This method allows physical and logical access to the drives but may require additional software to be 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-NEO2 over a network.

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

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

See ***Section 11.2*** for details on how to view Source drives over the network using iSCSI.

8: Destination Drive Encryption and Decryption

Section 8: Destination Drive Encryption/Decryption - Introduction

The Falcon-NEO2 can secure sensitive evidence data with whole disk drive encryption using the NIST-recommended XTS-AES-256 cipher mode. Destination drives that the Falcon-NEO2 encrypts can be temporarily decrypted using the Falcon-NEO2 or third-party software (VeraCrypt, TrueCrypt, or FreeOTFE).

The System Settings screen has an ***Encryption*** tab to configure the Falcon-NEO2 for encryption. Up to four (4) parameters 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-NEO2:

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



- VCRYPT cipher mode can be decrypted using the Falcon-NEO2 or VeraCrypt.
- TC-XTS cipher mode can be decrypted using the Falcon-NEO2, TrueCrypt, or VeraCrypt using TrueCrypt Mode.
- CBC or ECB cipher modes can be decrypted using the Falcon-NEO2 or FreeOTFE.



The Falcon-NEO2 encrypts drives using AES-256 encryption regardless of the cipher mode used. If TC-XTS is used. Falcon-NEO2 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. This is 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.

8.1: Encrypting a Destination

To encrypt a Destination, the Encryption settings must be set, then the drive must be formatted using the Falcon-NEO2. These steps must be performed before an Imaging operation.

8.1.1: 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.



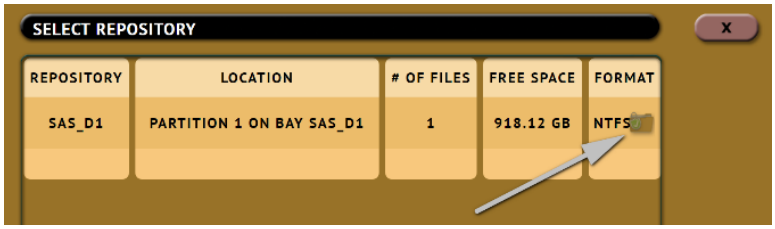
8. Tap the ***Start*** icon to start the Wipe task. The Falcon-NEO2 will format the selected drive(s) with encryption.

8.1.2: Using Previously Encrypted Destination Drives

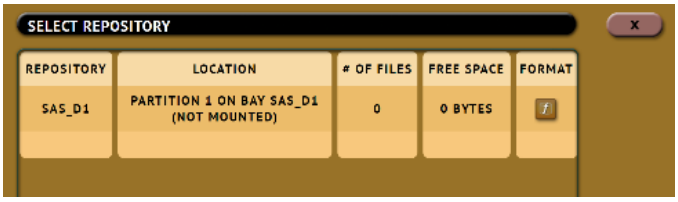
If a previously encrypted destination drive will be used and the Falcon-NEO2 has been off since the last time the encrypted drive was accessed, the encryption settings must be set to match the previous ones before connecting the drive.

1. Make sure the previously encrypted Destination drive is not connected, then turn the Falcon-NEO2 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*** 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 appropriately decrypted. The drive should look something like this:



Make sure the drive's encryption is detected and decrypted correctly. If the Falcon-NEO2 did not decrypt the drive correctly, it will show as ***(NOT MOUNTED)***:



If the drive is not decrypted correctly, disconnect it from the Falcon-NEO2, verify the encryption settings, and repeat steps 2 to 9.

8.2: Decrypting a Falcon-NEO2 Encrypted Drive with a Falcon-NEO2

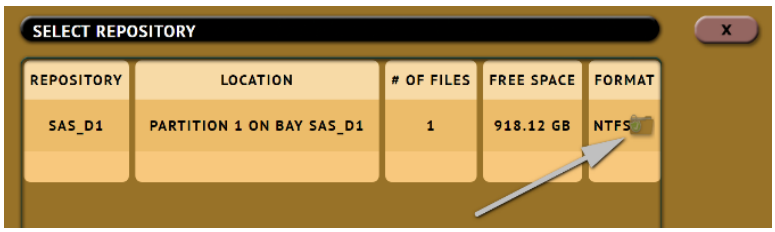
The Falcon-NEO2 can decrypt a Destination drive encrypted by the Falcon-NEO2. To decrypt the drive using a Falcon-NEO2, follow these steps:

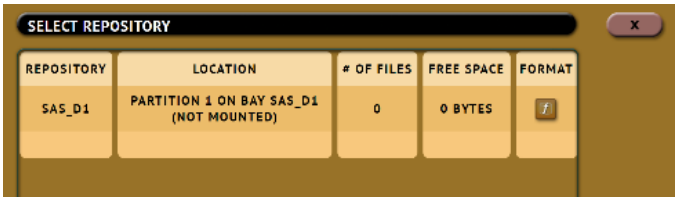
1. Make sure the previously encrypted Destination drive is not connected, then turn the Falcon-NEO2 on.
2. From the main menu, select ***System Settings*** from the types of operations on the left side.
3. Tap the ***Encryption*** tab.
4. Set the ***Cipher Mode***, ***Cipher***, ***IV Generation***, and ***Password*** 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-NEO2 detects and decrypts the Destination drive correctly.

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



> Make sure the drive's encryption is detected and decrypted correctly. If the Falcon-NEO2 did not decrypt the drive correctly, it will show as ***(NOT MOUNTED)***:
>
> 
>
>
> If the drive is not properly decrypted, disconnect it from the Falcon-NEO2, double-check the encryption settings, and repeat steps 2 through 7.

8. Once the Falcon-NEO2 decrypts the destination drive, the drive can be accessed using SMB. See ***Section 11.1*** for details on how to view Source or Destination drives over the network using SMB.

8.3: Decrypting a Falcon-NEO2 Encrypted Drive without a Falcon-NEO2

To mount and read an encrypted Destination drive in Windows without using a Falcon-NEO2, 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 they are not supported or tested by Logicube.

> Logicube cannot offer support for third-party utilities. If you need support, please contact the software manufacturer.

8.3.1: Which Decryption Software to Use?

Depending on how the destination drive was encrypted, choose the appropriate decryption software, such as VeraCrypt, TrueCrypt, or FreeOTFE.

- **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.

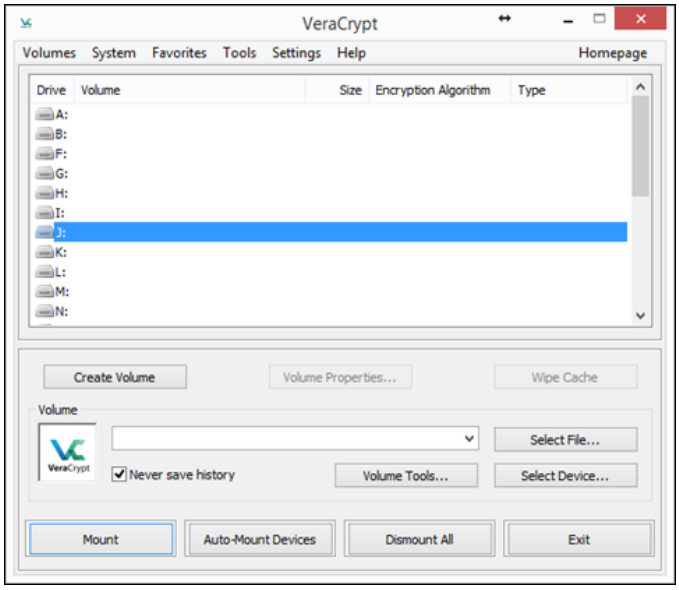
If the ***ECB*** cipher mode was used to encrypt the Destination drive, the Falcon-NEO2 must be used to decrypt the drive.

8.3.2: Decrypting Using VeraCrypt

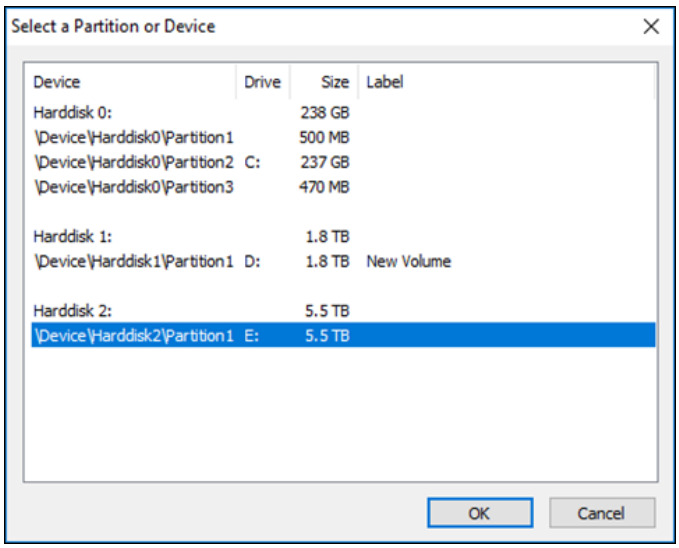
Requirements:

- VeraCrypt installed.
- A drive encrypted by the Falcon-NEO2 using the VCRYPT cipher mode connected to the computer with VeraCrypt.

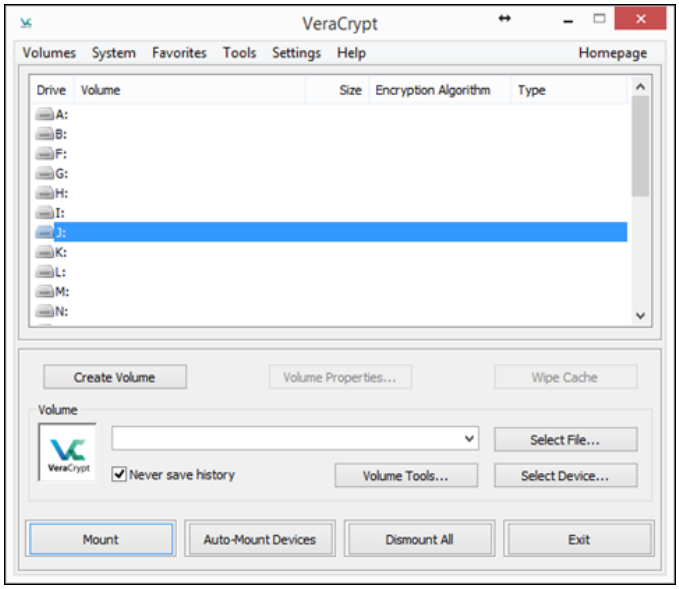
1. Once the drive is connected to the computer, Open VeraCrypt.



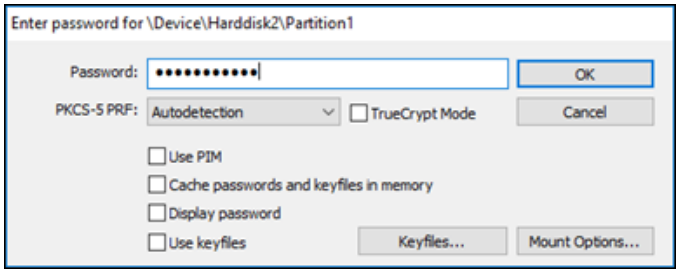
2. Click ***Select Device*** and choose the partition of the connected drive, then click ***OK***.



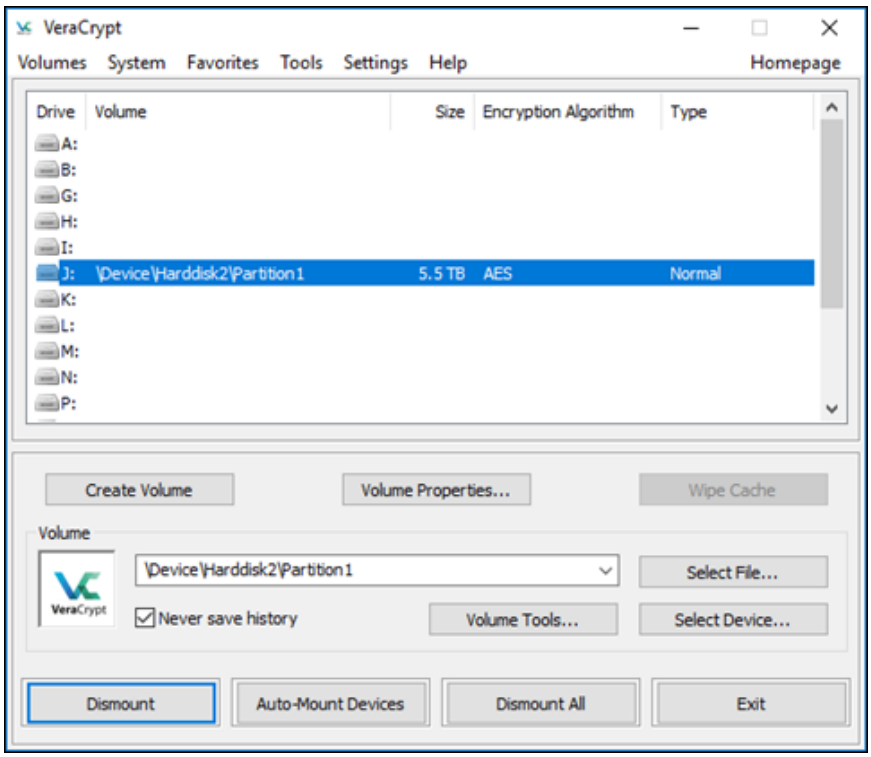
3. Click ***Mount***.



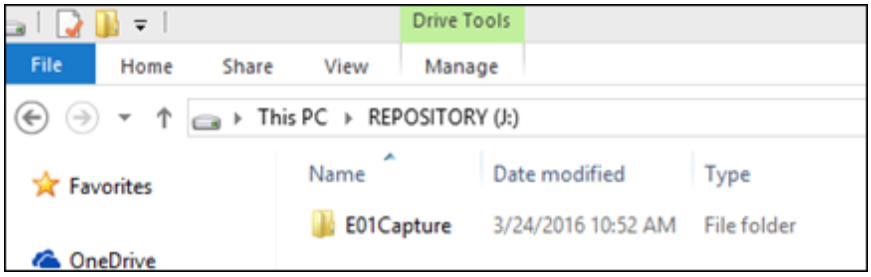
4. Type the encryption password in the ***Password*** field then click ***OK***.



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



6. The drive should now be accessible in Windows.



8.3.3: Decrypting using FreeOTFE

Requirements:

- FreeOTFE installed.
- A drive encrypted by the Falcon-NEO2 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, Disk #1). Place a checkmark on the ***Entire disk*** option. FreeOTFE cannot read the partition table on the drive since it is currently encrypted.
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-NEO2. In this example, “plain64’ was used. In the ‘Sector zero location’, choose ***Start of encrypted data***.

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

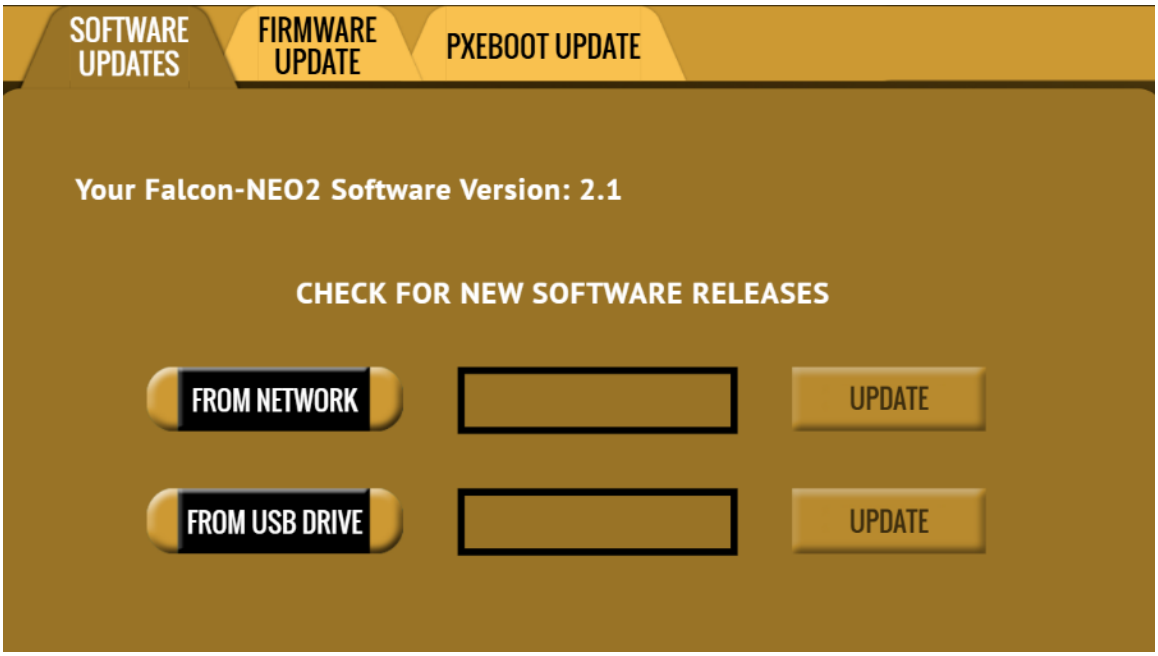
5. Click the ***OK*** button. The following warning screen may appear. Click the ***Yes*** button to continue.
6. FreeOTFE will mount the drive and assign a drive letter.
7. Click the ***OK*** button to continue. The drive should appear in the FreeOTFE window.
8. The Destination drive should now be accessible in Windows.

9: Updating/Loading/Re-loading Software

Section 9: Updating/Loading/Re-loading Software – Introduction

The latest Falcon-NEO2 software, manual, and readme file (which contains the software release notes) can always be found on the Falcon-NEO2 support page at https://www.logicube.com/knowledgebase/forensic-falcon-NEO2.

The Falcon-NEO2 software release may contain both a software and firmware update. This Section details how to update/reinstall the software and firmware.



9.1: Requirements

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

- The Falcon-NEO2 connected to a network with Internet access (for updating "FROM NETWORK"), or
- The Falcon-NEO2 with your USB flash drive. The USB flash drive must be formatted FAT32 or NTFS (for updating "FROM USB DRIVE")

9.2: Updating/Loading/Re-loading Software Instructions

The most up-to-date software update instructions are on the Falcon-NEO2's support page: https://www.logicube.com/knowledgebase/forensic-falcon-neo2/.

There are two methods for updating the Falcon-NEO2 Ultimate software:

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

When using a USB 3 flash drive, the software installation takes about 2 to 3 minutes. If FROM NETWORK is selected, the total time can exceed 5 to 10 minutes (or longer), depending on Internet speeds and network traffic.

9.2.1: From Network (Over the Internet)

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

Disconnecting all drives and drive adapters from the Falcon-NEO2 before the update/reinstall process is recommended.

1. Connect the Falcon-NEO2 to a network with Internet access and turn the Falcon-NEO2 on.
2. From the Falcon-NEO2's main menu, locate and tap the ***Software Updates*** icon on the left.
3. Select ***From Network***. The Falcon-NEO2 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 a newer software version is 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.CCNEO2/ FAILED: 500 CAN'T CONNECT TO UPDATES.LOGICUBE.COM:80 –*** This message will appear if the Falcon-NEO2 cannot connect to the update site. When this message appears, double-check that you have an Internet connection to the Falcon-NEO2. 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-NEO2 is connected to a network and has a valid ***IPAddress***, or
        ii. Make sure the network the Falcon-NEO2 is connected to has Internet access, or
        iii. Try the "From USB DRIVE" option (see ***Section 9.2.2***).
4. Tap the ***Update*** icon to begin the update/reinstall. The Falcon-NEO2 should begin the update/reinstall process. Do not interrupt this process. It may take

several minutes. Once completed, a screen stating the update is complete will prompt you to turn the unit off and back on.

5. Turn the Falcon-NEO2 off. Wait at least 5 seconds, then turn the Falcon-NEO2 back on.
6. Verify the software version by going to the Software Updates screen.

9.2.2: From USB Drive (Through a Software File Download)

In addition to the network option, the latest software can be downloaded from Logicube's website and placed onto a USB flash drive to perform the software update/reinstallation. An empty USB flash drive is recommended.

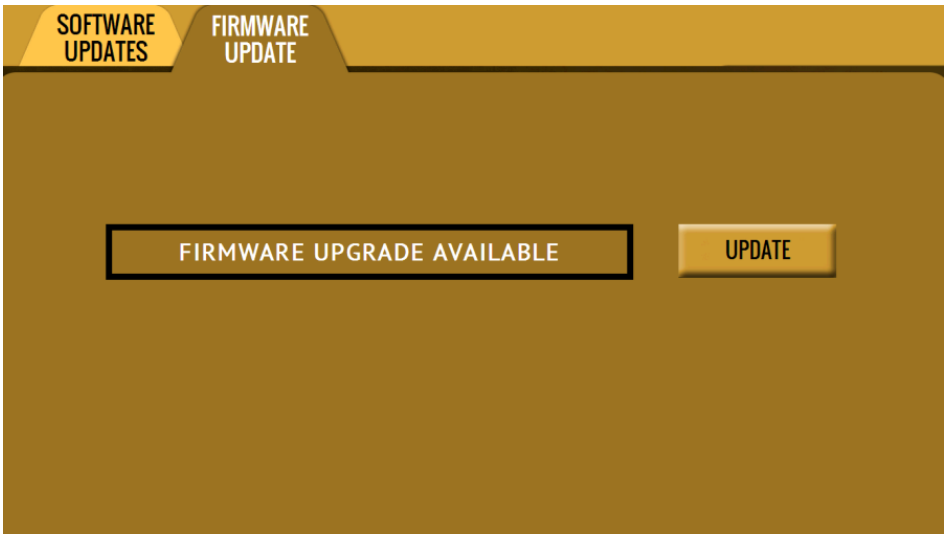


It is recommended that all drives and drive adapters from the Falcon-NEO2 be disconnected before the update/reinstall process.

1. Using a computer, download the latest software from the Falcon-NEO2 product support page at https://www.logicube.com/knowledgebase/forensic-falcon-NEO2.
2. Extract the contents of the downloaded zip file to the root of the USB flash drive.
3. Turn the Falcon-NEO2 on. When the main software screen appears, connect the USB flash drive (the extracted software from step 2) to the USB_S1 port (the USB port on the left side).
4. From the Falcon-NEO2's main menu, locate and tap the ***Software Updates*** icon on the left side.
5. Select ***From USB Drive***. The Falcon-NEO2 will check the version of the software on the USB drive. After a few seconds, one of the following messages should appear:
    - ***SOFTWARE FOUND –*** The software version is on the USB flash drive. Tap the ***OK*** icon to continue.
    - ***UPDATES NOT FOUND! –*** The Falcon-NEO2 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 9.2.1***)
6. Tap the ***Update*** icon to begin the update/reinstall. The Falcon-NEO2 should begin the update/reinstall process. Do not interrupt this process. It may take several minutes. Once completed, a screen stating the update is complete will prompt you to turn the unit off and back on.

7. Turn the Falcon-NEO2 off. Wait at least 5 seconds, then turn the Falcon-NEO2 back on.
8. Verify the software version by going to the Software Updates screen.

9.3: Firmware Loading Instructions



Falcon-NEO2 software releases may contain a firmware update. This section provides instructions on how to check if one is required and how to perform it.

1. After the software is updated/reinstalled on the Falcon-NEO2, 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 120 seconds. When the firmware update finishes, the Falcon-NEO2 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.

9.4: PXEBOOT UPDATE

This screen is reserved for future use.

9.5: BIOS Configuration Revision

The Falcon-NEO2 Software Release candidate version v2.1u2 contains a firmware update to Falcon-NEO2 that must be run on the unit to upgrade the BIOS settings. This BIOS settings update is required for all Falcon-NEO2 units as of software update candidate v2.1 and above.

For Falcon-NEO2 units are currently on software release candidate v2.1u2 or below, please update the Falcon-NEO2 unit to the latest software revision, which is v2.1u2 (or higher) and run the Software Update and the Firmware Update on your Falcon-NEO2 before applying the BIOS changes mentioned below.

1. With the Falcon-NEO2 powered off, connect a wired-USB keyboard to one of the two front facing USB ports on the Falcon-NEO2 unit.
2. Power on the Falcon-NEO2 unit and press the 'DEL' key once the unit is turned on to access the BIOS menu.
3. After accessing the BIOS menu, use the arrow keys to navigate to the 'BOOT' tab within the BIOS menu.
4. Under the BOOT tab, the final setting on the BOOT tab is '*UEFI Hard Disk Drive BBS Priorities'*. Highlight this option and press Enter.
5. Entering the '*UEFI Hard Disk Drive BBS Priorities'* sill show the default 'Boot Option #1' set up as 'Disable'.
6. Press Enter on Boot Option #1 and change the setting from 'Disable' to [**debian (P1: TS32GMTS400)**] or [**debian (TS128GMTS430S)**]'; whichever is applicable to your unit.
7. If done correctly, the Boot Option #1 will appear as either option listed above.
8. Press the *ESC* key to go back up one in the BIOS menu and using the arrow keys, navigate to the *Save and Exit* tab.
9. Under *Save and Exit,* press the **F4** key or highlight the '*Save Changes and Exit'* option and press Enter. A prompt asking to save configuration may appear, select [**YES**] and press Enter.
10. Allow the unit to fully power on and boot up before using the Falcon-NEO2.

10: Remote Operation

Section 10: Remote Operation - Introduction

The Falcon-NEO2 has two 10GbE network connections in the back of the unit. Connecting the Falcon-NEO2 to a network allows remote access from any computer within the same network.

The Falcon-NEO2 is configured for DHCP by default. For instructions on configuring it with a Static IP address, see ***Section 6.11.1.1***.

The Falcon-NEO2 is set up with a Zero Configuration Network (Zeroconf). There are two ways to access the Falcon-NEO2:

- Web interface – A graphical interface using an Internet browser where the screens are shown exactly the way they appear on the Falcon-NEO2
- Command Line Interface (CLI) – A text-only command-line interface that can be accessed in one of two ways:
    i. Telnet (via a network connection)
    ii. SSH (Secure Shell via a network connection)

BROWSER COMPATIBILITY: Google Chrome, Mozilla Firefox, and Microsoft Edge are recommended. Other browsers may not display the Graphical User Interface (GUI) correctly.

10.1: Web Interface

Using a web browser, go to the IP address or the hostname of the Falcon-NEO2. The IP address and hostname can be found by going to the ***Statistics*** screen on the Falcon-NEO2. For example, browse to ***http://192.168.1.100*** or ***http://falcon-XXXXXX,*** where XXXXXX is the 6-digit serial number of the Falcon-NEO2. The Falcon-NEO2's web interface will appear on the browser screen. All screens and operations on the Falcon-NEO2 will be available on the browser.

On some browsers or Operating Systems, the Falcon-NEO2 will need to be accessed by browsing to ***http://falcon2-XXXXXX.local***.

The Falcon-NEO2 can be controlled by clicking on the icons in the browser window.

10.2: Command Line Interface (CLI)

The Falcon-NEO2 also has a CLI, or Command Line Interface. This interface has no graphical content and is all command-line (text) based. It is for advanced users who know

command-line functions. This type of connection requires a Telnet or SSH client from a connected computer (over a network). Many Telnet and SSH clients are 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 it 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.
- If you need assistance installing any SSH or Telnet software (including Microsoft's Telnet client), please check with your IT administrator.

10.2.1: Connecting Using Telnet

The steps below outline how to use the Windows Telnet client. Other Telnet clients would have different steps for connecting. The Windows Telnet client may not be installed in Windows. To install the Windows Telnet client, please consult your IT department.

1. Connect the Falcon-NEO2 to the network by attaching a network cable to the RJ45 connector in the back of the Falcon-NEO2.
2. Turn the Falcon-NEO2 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-NEO2. For example
   open 192.168.1.100 or ***open falcon2-XXXXXX***
   where XXXXXX is the 6-digit serial number of the Falcon-NEO2, then press the Enter key. The Falcon-NEO2 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 in the Telnet window.

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

The Falcon-NEO2 can now be configured or managed via the command-line interface.

10.2.2: Connecting Using SSH

Connecting to the Falcon-NEO2 via SSH (Secure Shell) is similar to connecting via Telnet. Since Windows does not have a built-in SSH client, a third-party SSH client must 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-NEO2, connect the Falcon-NEO2 to a network.
2. Turn the Falcon-NEO2 on and allow it to boot up completely.
3. Open the SSH client and select an SSH connection.
4. Connect to the Falcon-NEO2 either by IP address or by hostname. The Falcon-NEO2's name will be falcon2-XXXXXX (where XXXXXX is the 6-digit serial number).



On some Operating Systems, the Falcon-NEO2 will need to be accessed by opening falcon2-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 for step 5. ***It is not recommended to use the Logicube account login without consulting Logicube Technical Support first***.

The Falcon-NEO2 can now be configured or managed via the command-line interface.

10.3: Zero Configuration Networking (Zeroconf)

The Falcon-NEO2 has the capability of 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-NEO2 is connected (using a network cable) directly to a Windows-based computer that is DHCP enabled, both the Falcon-NEO2 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.

10.4: Copying Profiles from One Falcon-NEO2 to Another

Profiles can be copied from one Falcon-NEO2 to another using the Command Line Interface (CLI). The Falcon-NEO2 units must be on the same network, and all Profiles will be copied. Instead of configuring each Falcon-NEO2 one at a time, all Falcon-NEO2 units can have the same profiles with a few simple commands.

10.4.1: Step-By-Step – Copying Profiles

Once the profiles are configured and saved onto a Falcon-NEO2:

1. Connect the Falcon-NEO2 with the saved profiles and any additional Falcon-NEO2 units to a network.

2. Connect to the Falcon-NEO2 with the saved profiles using Telnet or SSH. ***Section 10.2.1*** and ***Section 10.2.2*** provide 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 primary 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-NEO2 unit. Ensure these profiles need to be copied to the other Falcon-NEO2 units.
7. Type ***db push xxx.xxx.xxx.xxx*** where xxx is the IP address of the Falcon-NEO2 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-NEO2 unit will be copied to the other Falcon-NEO2 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 reappear. The Falcon-NEO2 unit, where the profiles were copied to, will refresh its screen.
8. The profiles should now be copied to the other Falcon-NEO2 unit. Repeat step 7 to copy the profiles to other Falcon-NEO2 units.

11: Viewing Source and Destination Drives over a Network

Section 11: Viewing Drives Over a Network – Overview

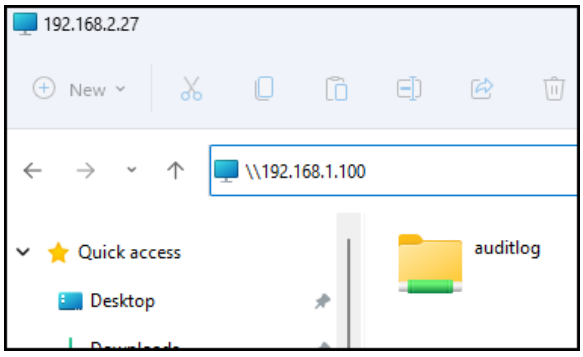
The contents of drives connected to any Source or Destination position on the Falcon-NEO2 can be viewed over a network.

> Contents of Source and Destination drives viewed over a network are write-protected.
>
> Only destinations formatted by the Falcon-NEO2 can be seen over a network.

11.1: Viewing Source or Destination Drives Over the Network Using SMB

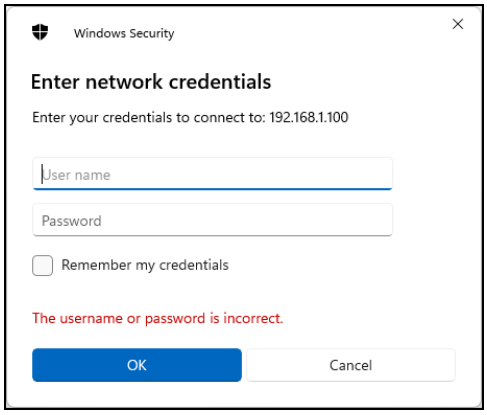
Contents of a Source or Destination drive can be viewed over a network using built-in file managers/viewers like File Explorer. If an existing network is unavailable, the Falcon-NEO2 can be connected directly to a computer by connecting an Ethernet cable between the computer and the Falcon-NEO2.

1. Connect the Falcon-NEO2 directly to a network or a computer (using a network cable).
2. On the computer (on the same network, or directly connected to the Falcon-NEO2), open File Explorer and browse the Falcon-NEO2's IP address or the hostname of the Falcon-NEO2. The IP address and hostname can be found by going to the ***Statistics*** screen on the Falcon-NEO2. For example, browse to ***\\192.168.1.100*** or ***\\falcon2-XXXXXX,*** where XXXXXX is the 6-digit serial number of the Falcon-NEO2.

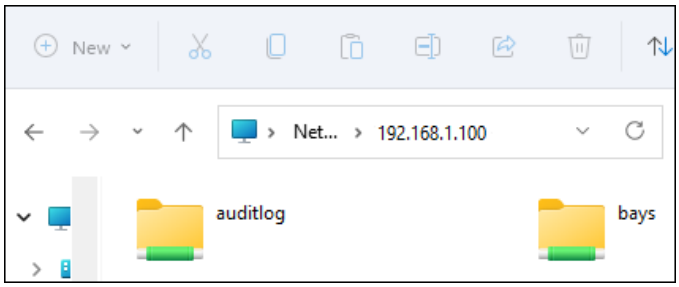


3. A window may appear asking you to enter a password to connect to the Falcon-NEO2. Enter the following information:

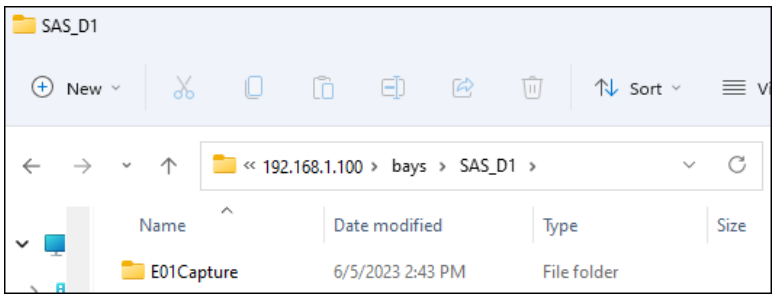
   User name: ***it***
   Password: ***it***



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



5. Go to the Bays folder and select the connected Destination drive, such as SAS_D1. The drive's contents will be shown.



11.2: Viewing Source Drives Over the Network Using iSCSI

Source drives can be viewed on a computer over a network connection. If an existing network is unavailable, the Falcon-NEO2 can be connected directly to a computer by connecting an Ethernet cable between the computer and the Falcon-NEO2.

An iSCSI initiator must be configured to view the contents of Source drives over a network. Although many iSCSI initiators are available, the following sections 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:

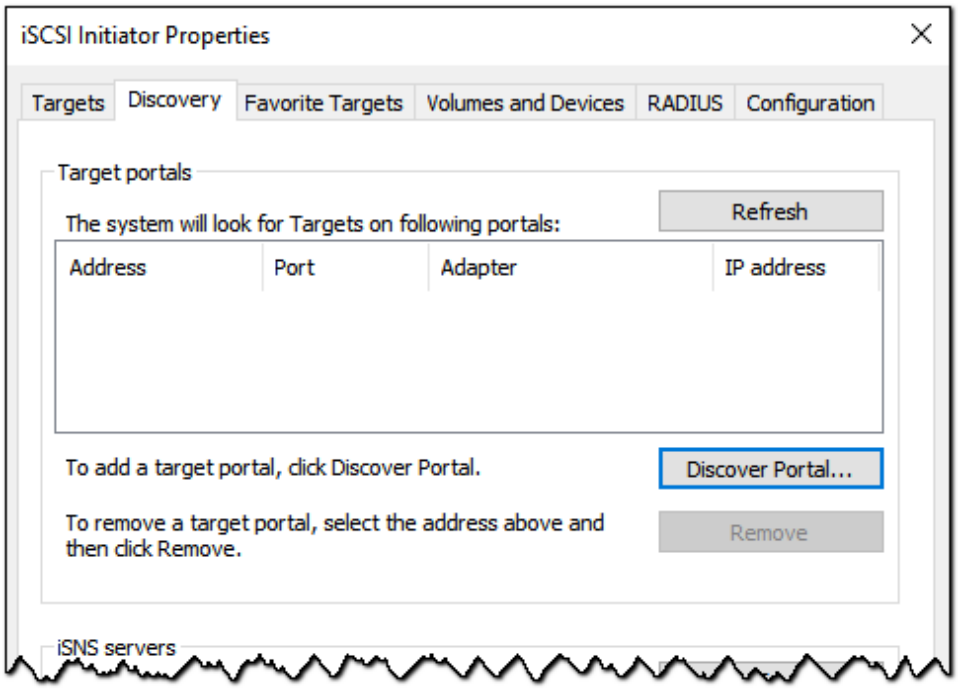
Username: iscsi

Password: logicube@19755

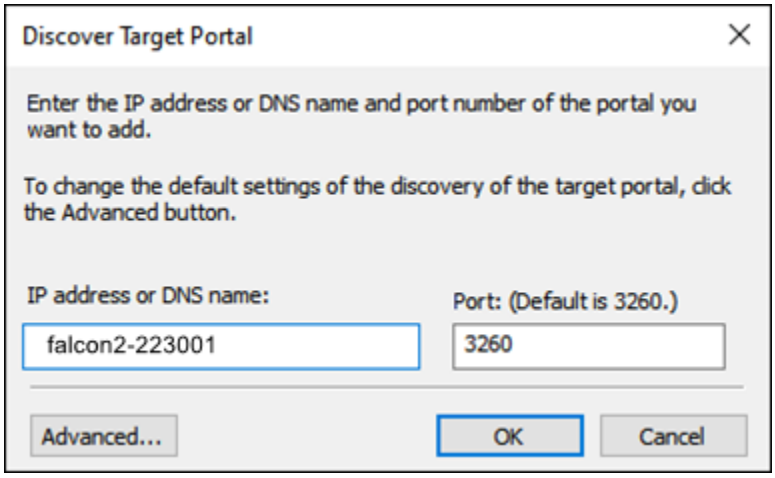
1. Open the iSCSI initiator app.



2. The **iSCSI Initiator Properties** window should appear. Go to the ***Discovery*** tab, then click ***Discover Portal***.

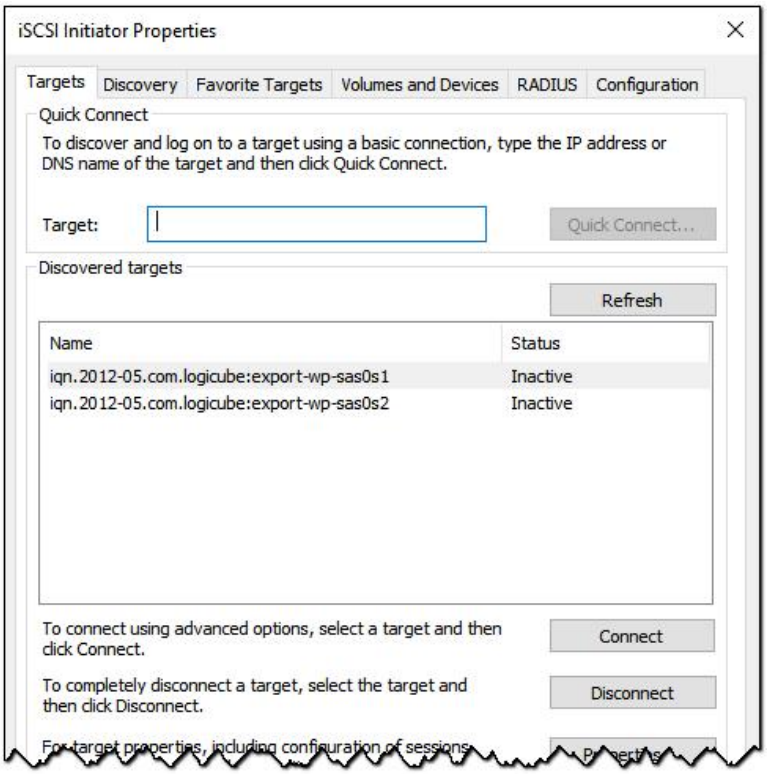


3. The **Discover Target Portal** screen should appear. In the IP address or DNS name field, type the Falcon-NEO2's hostname or IP address, then click ***OK***.

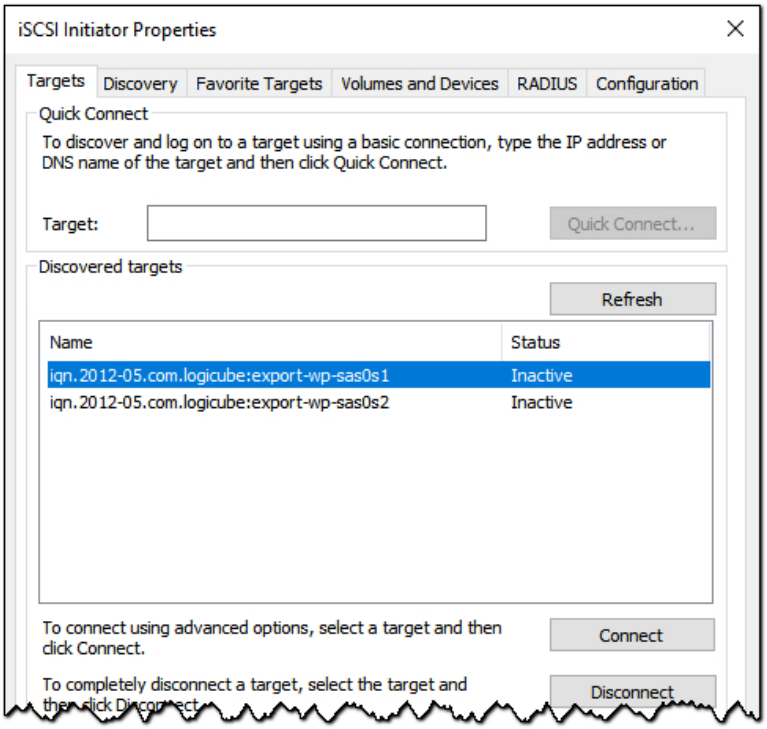


4. Click the ***Targets*** tab. The **Discovered targets** section should show all drives connected to any source ports on the Falcon-NEO2. The example below shows one

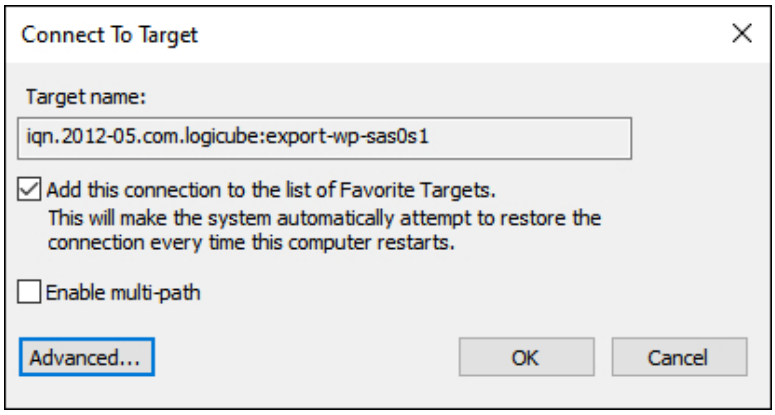
drive connected to SAS_S1 (...wp-sas0s1) and one connected to SAS_S2 (...wp-sas0s2).



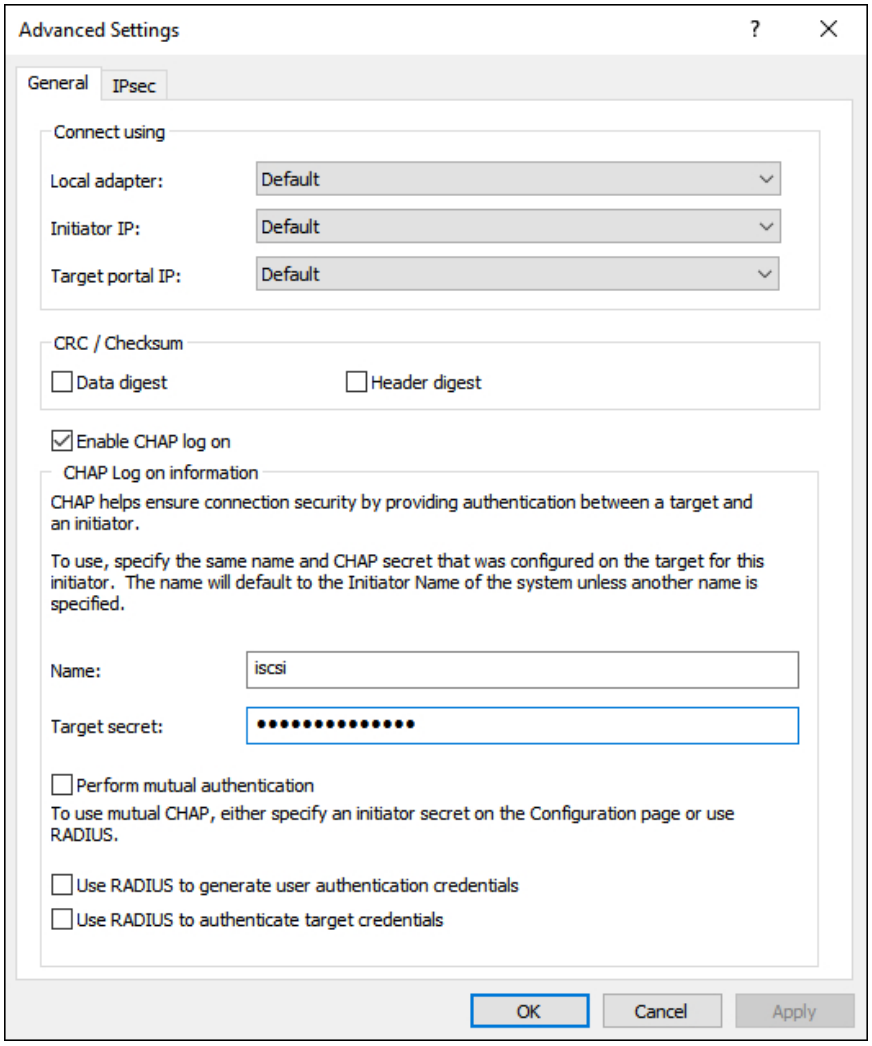
5. Click on the iSCSI target to connect to, then click ***Connect***.



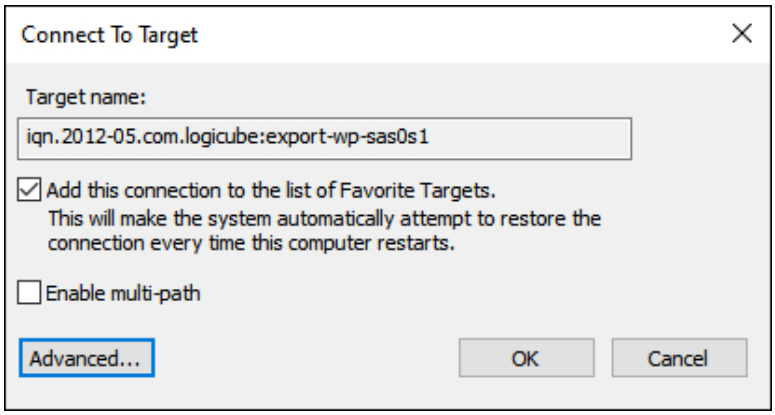
6. The **Connect to Target** window should appear. Click ***Advanced***.



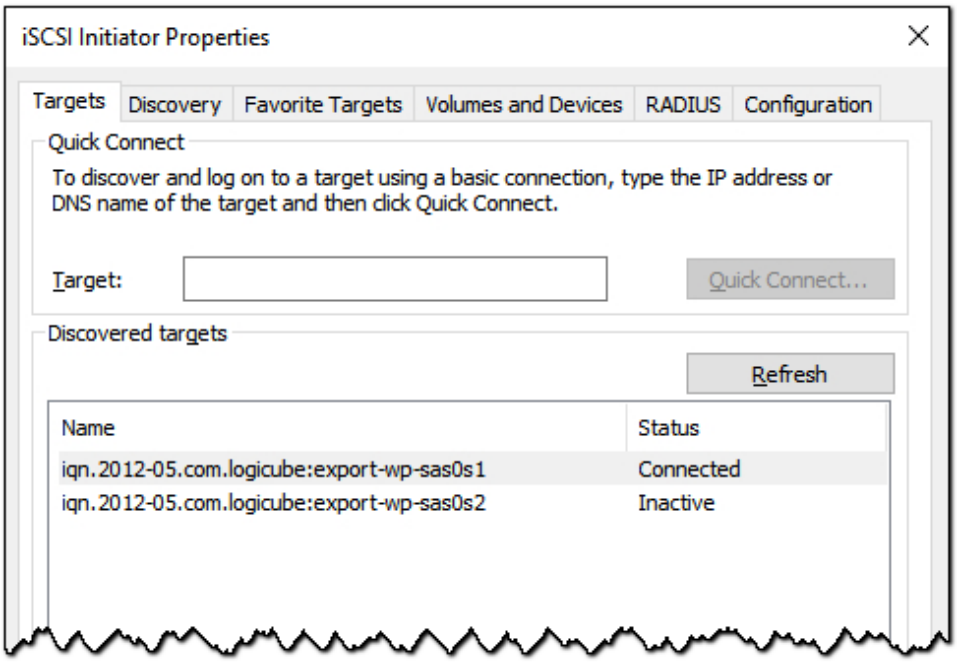
7. The **Advanced Settings** screen should appear. On this screen, do the following, then click ***OK***:
    a. Place a checkmark on ***Enable CHAP log on***.
    b. In the ***Name*** field, enter “iscsi” (without the quotes).
    c. In the ***Target secret*** field, enter “logicube@19755” (without the quotes).



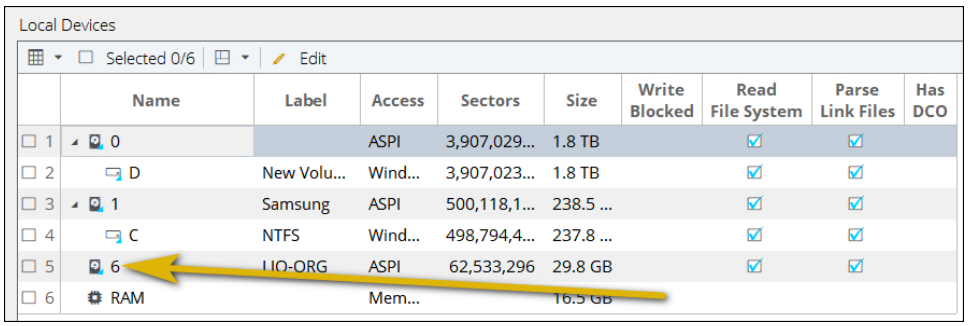
8. The **Connect To Target** screen should reappear. Click ***OK***.

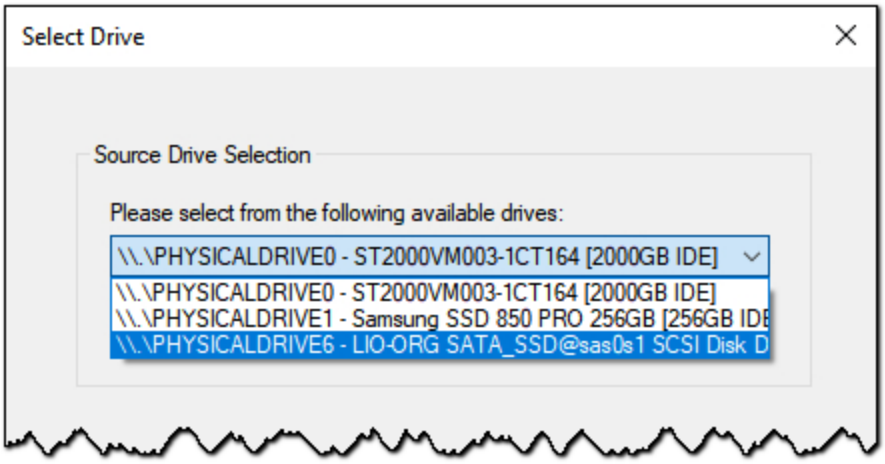


9. The **iSCSI Initiator Properties** screen should reappear. This time, the selected iSCSI target should show a **Connected** status.



10. The drive should now be available as a Local Device in Encase or a Physical Drive in FTK Imager.




Select Drive
Source Drive Selection
Please select from the following available drives:
\\.\PHYSICALDRIVE0 - ST2000VM003-1CT164 [2000GB IDE]
\\.\PHYSICALDRIVE0 - ST2000VM003-1CT164 [2000GB IDE]
\\.\PHYSICALDRIVE1 - Samsung SSD 850 PRO 256GB [256GB IDE
\\.\PHYSICALDRIVE6 - LIO-ORG SATA_SSD@sas0s1 SCSI Disk D

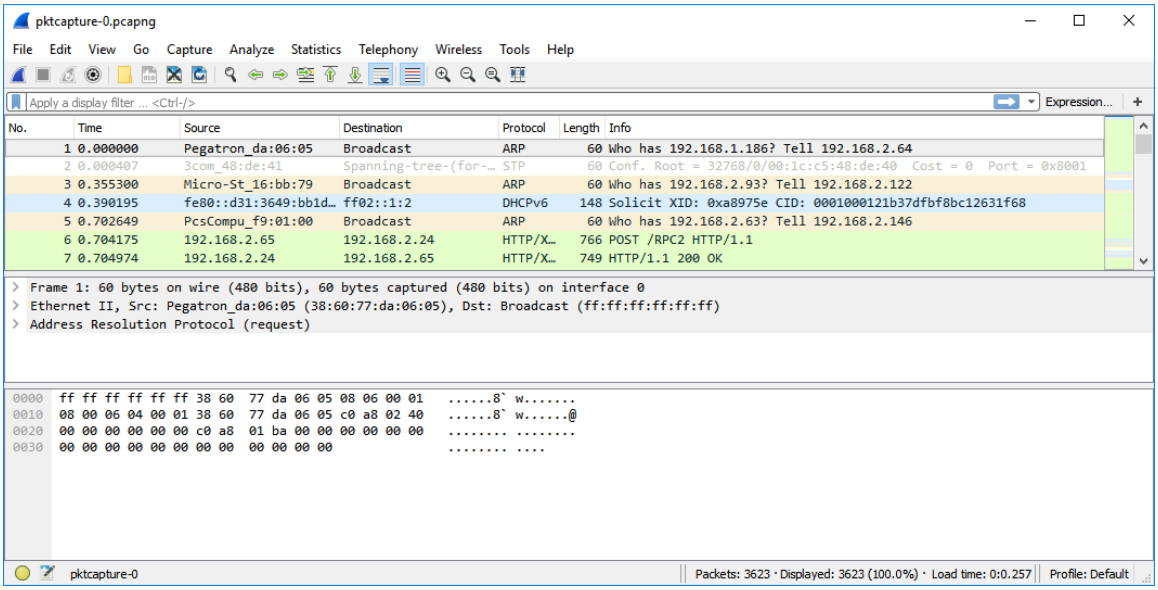
Section 12: Net Traffic Introduction

The Falcon-NEO2 can capture network traffic data using the Net Traffic to File imaging mode. Network traffic that can be captured includes local network activity, internet activity, and VOIP activity. The data is saved and stored in a *. pcapng format.

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

Advanced networking knowledge is required for network traffic capture and data analysis.

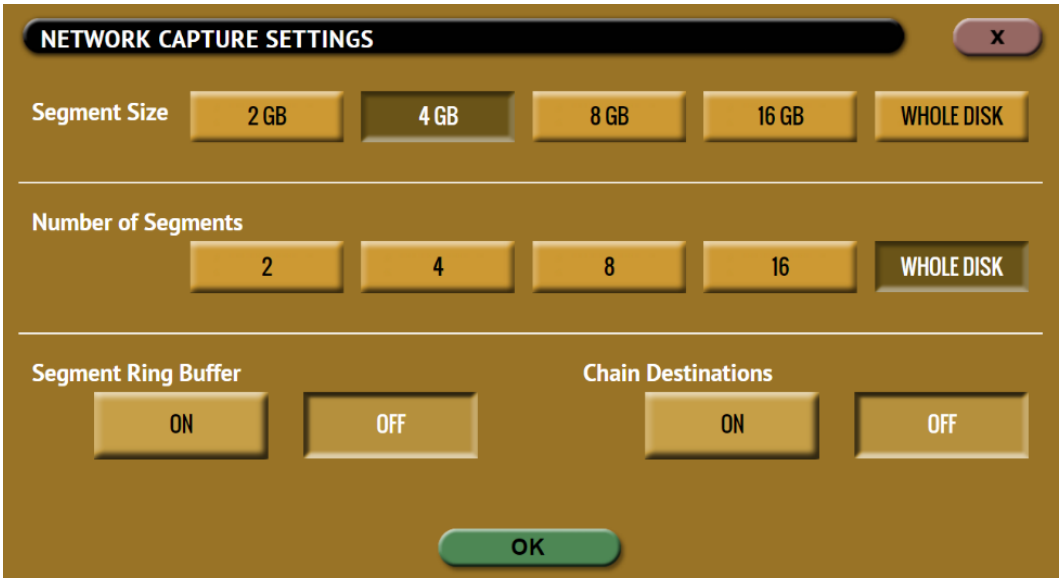
Below is an example of a pcapng file created by the Falcon-NEO2, viewed in Wireshark.



12.1: Net Traffic Settings

Net Traffic to File has the following settings:

- Segment Size
- Number of Segments
- Segment Ring Buffer

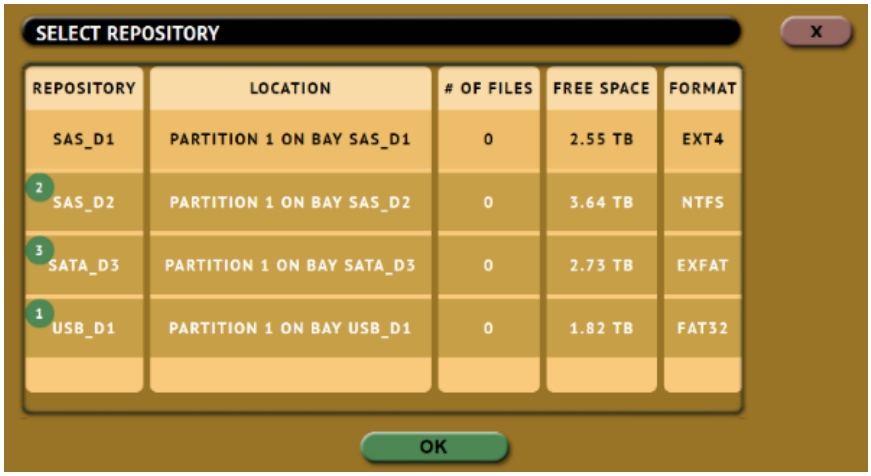


- ***Segment Size –*** This option allows the user to set the size of the captured segment (pcapng file). The options available are 2 GB, 4 GB, 8 GB, 16 GB, and Whole Disk.
- ***Number of Segments –*** This option allows users to select how many segment files to create. For example, two segment files will be created if the Segment Size is set to 4 GB and the Number of Segments is set to 2. The options available are 2, 4, 8, 16, and Whole Disk.
- ***Segment Ring Buffer –*** Determines what the Falcon-NEO2 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-NEO2 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, continue capturing network traffic, and create a new first segment file. If more than one repository is selected, it will cycle through both repositories, overwriting the oldest segment until the task is aborted.
    - ***OFF –*** When this is set to OFF, the task will be stopped once the Falcon-NEO2 reaches the number of segments selected and the last repository is filled.
- ***Chain Destinations –*** This option allows users to continuously span the Net Traffic to File images over two or more repositories (such as Destination drives). When this is set to YES, all selected Destination drives will be used in their selected order. When the drive on the first repository is full, it will continue with the following selected repository.

To enable Chain Destinations, the Ring Buffer must be set to OFF.

Before starting the Net Traffic to File Imaging task, drives must be formatted (by the Falcon-NEO2).

- After the first repository is full, the Destination drive can be swapped with a new one.
- Replacing full repositories with a new Destination drive allows the Falcon-NEO2 to capture Net Traffic until all the repositories are full. When all repositories are full, the task will finish showing a completed status.



12.2: Net Traffic Imaging Notes

- Depending on the settings chosen, the ***Net Traffic to File*** task may finish and stop independently. 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-NEO2 will complete the ***Number of Segments*** set, delete the first segment, and continue capturing network traffic. When ***the Ring Buffer is set to ON, the user will continue to capture network traffic until the task is aborted***.
- Capturing network traffic is dependent on how each network is set up. By simply connecting the Falcon-NEO2 to a network, the Falcon-NEO2 could capture all traffic forwarded by the Ethernet switch to the given port. Capturing network traffic from a specific IP address requires advanced knowledge of networking. For example, a managed switch with port mirroring can mirror a specific port, allowing the Falcon-NEO2 to capture the network traffic from that single port.

  Please contact the manufacturer of your specific network switch to find out if it supports port mirroring and for help setting it up.

- The Falcon-NEO2 listens for network traffic and does not actively scan or send 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.

13: Mobile to File Imaging

Section 13: Mobile to File Introduction

This expands the functionality of the Forensic Falcon-NEO2 with a convenient method to quickly acquire potential evidence data from mobile devices. Adding this software option to the Falcon-NEO2 for field investigations reduces the need for additional hardware to collect critical evidence from mobile devices.

- Supports iOS and Android 4.0 and newer.
- The mobile device's screen must be unlocked.
- For iOS devices, the software performs an iTunes backup.

Android capture output:

A physical acquisition is performed for rooted Android devices, and a logical acquisition is performed for non-rooted Android devices. An Android logical acquisition produces an Android backup file (backup.ab). Call logs, contacts, SMS messages, and calendars are in JSON format. An Android physical acquisition will produce a single dd image file.

iPhone capture output:

iPhone acquisitions output to PLIST. When the Falcon-NEO2 examines the iOS device, it will detect whether the iOS device was password-encrypted for backup purposes.

- If it was password-encrypted (for backup purposes), the user's password is required to examine the output.
- If it was not password-encrypted (for backup purposes), the Falcon-NEO2 uses the following default password:
  logicube

13.1: Mobile Device Capture Requirements

For serial numbers 223000 and above – This is a standard, built-in feature.

For serial numbers below 223000 – Available as an annual, renewable software subscription.

The following are required to use the Mobile Device Capture feature (Mobile to File):

- A Falcon-NEO2 with the Mobile Device Capture Option activated.
- A supported Android or iOS device

13.2: Android Devices

The following are required for Android devices:

- USB Debugging must be enabled. Android devices may display menu labels differently. Please check the Android device's user manual on how to enable USB Debugging.
- A data transfer cable compatible with the Android device.
- If security is enabled on the Android device, the passcode is required to unlock the device's screen.

13.3: iOS and iPadOS Devices

The following are required for iOS and iPadOS devices:

- A data transfer cable compatible with the iOS or iPadOS device.
- If security is enabled on the iOS or iPadOS device, the passcode is required to unlock the device's screen.

13.4: Configuring and Starting the Mobile to File task

1. On the Falcon-NEO2 Imaging screen, go to ***Mode*** and select ***Mobile to File,*** then tap or click ***OK***.
2. At this time, do not select the source. If case notes need to be entered, go to ***Case Info*** and enter the case information. Tap or click ***OK*** when finished.
3. Connect a destination drive (unless a network repository is used as the destination). Go to ***Destination*** and select the destination drive or destination network repository.
4. Go to ***Source***. The mobile device should not appear on the screen currently, as it has not yet been connected.
5. Connect the proper data transfer cable to a USB source port (USB_S1 or USB_S2) or the Thunderbolt port on the Falcon-NEO2 if the TBT-I/O card is available.
6. Unlock the Android, iOS, or iPadOS device's screen.
7. Immediately after unlocking the device's screen, connect the other end of the data transfer cable to the Android, iOS, or iPadOS device.
8. Follow the instructions on the Android, iOS, or iPadOS device's screen:
    a. For Android devices, a pop-up should appear asking, "Allow USB Debugging?" Tap ***Allow***.
    b. For iOS or iPadOS devices, a pop-up should appear asking to "Trust this computer." Tap Trust, then enter the device password or passcode.
9. Check the Falcon-NEO2 Source screen. If the Android, iOS, or iPadOS device appears on the Source screen, select it and tap or click OK to return to the main screen. If the device does not appear, disconnect and reconnect the USB cable (either from the Falcon-NEO2 or from the device).

10. Tap or click ***Start*** to start the imaging task.
11. Check both the Falcon-NEO2 screen and the Android, iOS, or iPadOS device screen to see if any further screens require user input.

14: USB Boot Client

Section 14: 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 needing to remove it from the computer.

14.1: 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-NEO2, the following are required:

- The Falcon-NEO2 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-NEO2)

14.2: Creating the USB Boot Client

Here are the steps to create a USB Boot Client with the necessary software to make it bootable. When used to boot a computer, it will allow the Falcon-NEO2 to use the computer's drive as a Source drive.



It is recommended to use Chrome, Firefox, or Edge web browsers. Internet Explorer does 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

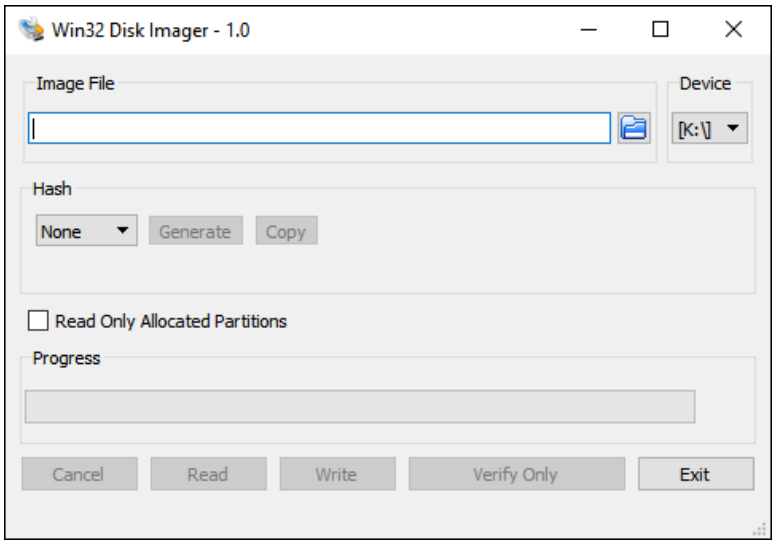


Balena Etcher can be used as an alternative to Win32DiskImager. The instructions in this section are for Win32DiskImager.

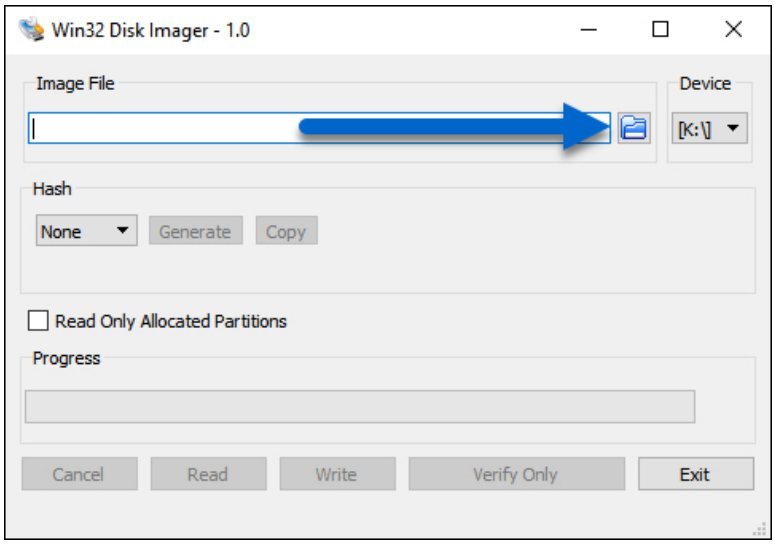
2. Download both files. If the image file does not download, right-click on the link and use the 'Save Target As…' or 'Save Link As' option. Make sure it is saved with the *.img file extension.
3. Extract all the files within the win32diskimager-v1.0.0-binary.zip file to a folder or directory of your choosing.
4. Connect your USB flash drive with at least 1 GB of capacity to the computer where the software was downloaded. It is recommended that all other USB drives be 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.

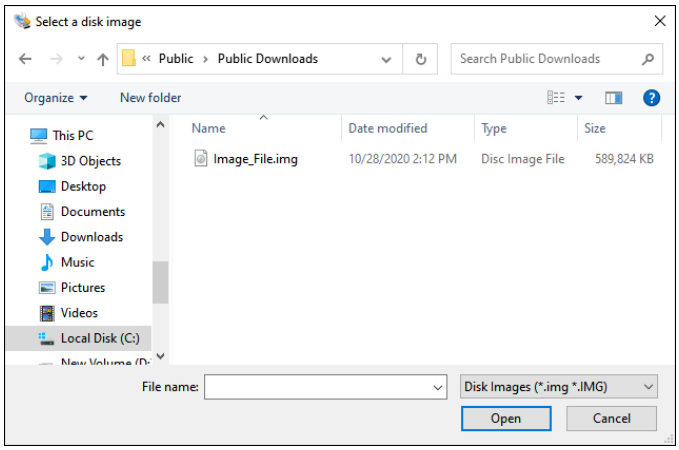
5. In the win32diskimager-v1.0.0-binary folder where the files were extracted to, run the file ***Win32DiskImager.exe***. The Win32 Disk Imager window will appear.



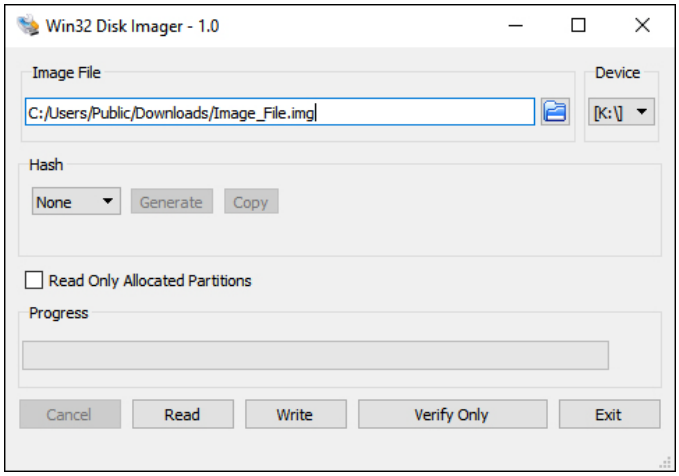
6. Click the folder icon to select a disk image.



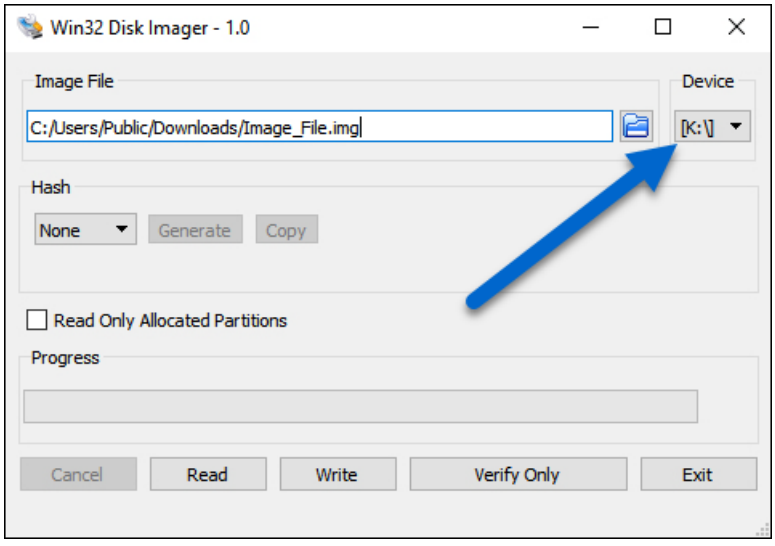
7. In the folder where the files were downloaded (step 2), select the USB Boot Client *.img file and click the ***Open*** icon.



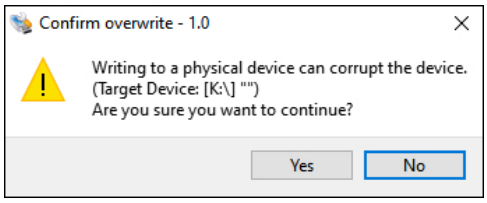
8. The Image file should now be in the Win32 Disk Imager screen under 'Image File'.



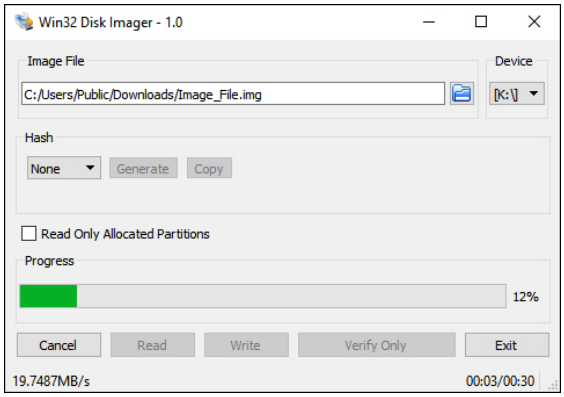
9. Under 'Device', select the drive letter for the USB flash drive connected during step 4, then click the ***Write*** icon.



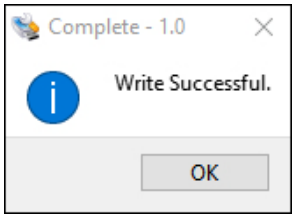
10. A confirmation screen will appear. Ensure the “Target Device” is set to the correct drive letter. If it is the correct drive letter, click ***Yes*** to continue. If it is showing the wrong drive letter, click ***No***. This will take you back to the previous screen, where you can select the correct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



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



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



14.3: Using the USB Boot Client

The Falcon-NEO2 can use drives connected to the computer 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.

For computers without a built-in Ethernet adapter, a USB-to-Ethernet adapter or a dock with an Ethernet port may be used.

1. Connect the Falcon-NEO2 to the same network that 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 that the Falcon-NEO2 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 if the computer supports this function.

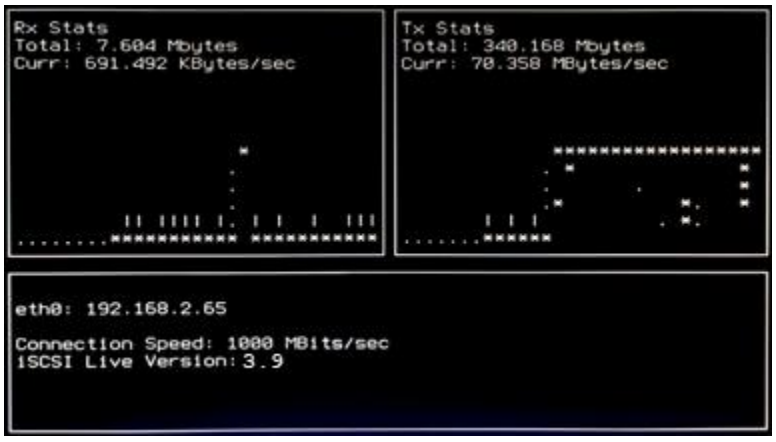
4. The USB Boot Client's boot menu will appear. After a few seconds, it should auto-select "iSCSI Target (64-bit)." If not, select "iSCSI Target (64-bit)."

> 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 30-120 seconds (depending on the computer's speed), the USB Boot Client should finish booting up.
    - The following screen may appear if no network adapter or 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 are detected, the following screen will appear:



6. Turn the Falcon-NEO2 on. After the Falcon-NEO2 boots up, additional drives appear in the Source position depending on the selected imaging mode.

> 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 one drive is connected, it will show as **I:2.65/SDA**.

You can image using the Falcon-NEO2 using the normal imaging steps. Imaging speeds may vary depending on network performance when using the USB Boot Client.

14.4: Using the USB Boot Client over different subnets

The USB Boot Client and the Falcon-NEO2 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 14.3*** to boot with the Forensic USB Boot Client.
2. Turn the Falcon-NEO2 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 a 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. Depending on network speeds, the screen may stay on the "Connecting" screen for up to 60 seconds (or longer).
7. Once connected, a "CONNECTED" screen will appear. The remote device should now be visible on the Logicube device.

15: Printing

Section 15: Printing – Introduction

When viewing log files through the Falcon-NEO2 touch screen or web interface, a print icon is 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:** Print to any printer set up on the computer from the Web Interface using a computer on the same network that the Falcon-NEO2 is connected to.
- From the touch screen on the Falcon-NEO2. This will print to a configured local printer (connected via USB to the Falcon-NEO2) or to a networked printer.

15.1: Printing from the Web Interface

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

15.2: Configuring a Local or Networked Printer

The Falcon-NEO2 can also print to a local printer (connected via USB) or a networked printer. The printer must be configured using the Command Line Interface. Local printers must be connected to the Falcon-NEO2 through an available USB port on the front of the Falcon-NEO2. Networked printers will be seen by the Falcon-NEO2 when connected to the same network.

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

15.2.1: Step-By-Step: Configuring a Local or Networked Printer

1. Connect the Falcon-NEO2 to a network with DHCP. For networked printers, ensure the Falcon-NEO2 is connected to the same network. Connect the printer to an available USB port in front of the Falcon-NEO2 for local printers.
2. Turn the Falcon-NEO2 on. The Falcon-NEO2 should automatically assign itself an IP address that the Windows computer can see. Go to the ***Statistics*** screen on the Falcon-NEO2 and look for the hostname and IPAddress.
3. Connect to the Falcon-NEO2 Using Telnet or SSH.
4. Once logged in to the Falcon-NEO2 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-NEO2 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 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-NEO2 is turned on, the local or networked printer should be available on the Falcon-NEO2’s touch screen.

16: Options and Accessories

Section 16: Options and Accessories – Introduction

The Falcon-NEO2 features several additional accessories and optional adapters. For a complete list of available options, please visit https://www.logicube.com/shop/forensic-falcon-NEO2. This section lists the following options and accessories:

- Triage
- Mobile Device Capture Option
- Thunderbolt 3 / USB-C I/O Card
- SCSI Module
- FireWire Module
- PCIe adapter kit
- U.2 to PCIe adapter
- M.2 NVMe to USB adapter
- USB 3.0 to SATA adapter & power cable
- USB 3.0 Hub
- PCIE Expansion Module

To purchase any of these options or accessories, please contact Logicube's Sales department at sales@logicube.com or your region's international reseller.

16.1: Triage

Triage – Import one or more VICS. Comma-Separated Value, or X-Ways Hash Database and then triage a source drive to determine if any files on the drive match hashes in the database. Positive results will result in a successful message, and all matches will be listed in the audit log file.

- **Triage is a standard, built-in feature** for Falcon-NEO2 units **with serial number 223000 and above**.
- **For serial numbers under 223000**, Triage is available with a one-time, optional purchase. Contact sales@logicube.com or your region's international reseller for additional information. For a list of international resellers, visit https://www.logicube.com/sales/international-sales/.

16.2: Mobile Device Capture

This expands the functionality of the Forensic Falcon-NEO2 with a convenient method to quickly acquire potential evidence data from mobile devices. Adding this software option to the Falcon-NEO2 for field investigations reduces the need for additional hardware to collect critical evidence from mobile devices.

- Supports iOS and Android 4.0 and newer.
- The mobile device's screen must be unlocked.
- For iOS devices, the software performs an iTunes backup.
- A physical acquisition is performed for rooted Android devices, and a logical acquisition is performed for non-rooted Android devices. An Android logical acquisition produces an Android backup file (backup.ab). Call logs, contacts, SMS messages, and calendars are in JSON format. An Android physical acquisition will produce a single dd image file.

- **For serial numbers 223000 and above –** This is a standard, built-in feature.
- **For serial numbers below 223000 –** Available as an annual, renewable software subscription. Contact sales@logicube.com or your region's international reseller for additional information. For a list of international resellers, visit https://www.logicube.com/sales/international-sales/.

16.3: Thunderbolt 3/USB-C I/O Card

The Falcon-NEO2 Thunderbolt 3/USB-C I/O card (part# F-FNEO2-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-NEO2.

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 support imaging in TDM from Mac computers.

16.4: Falcon-NEO2 SCSI Module

The optional Falcon-NEO2 SCSI Module (part# F-FALNEO2-SCSI-OPT) expands the Falcon-NEO2's capability 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-NEO2 SCSI module provides 1 SCSI port for the Source or Destination PCIe port.



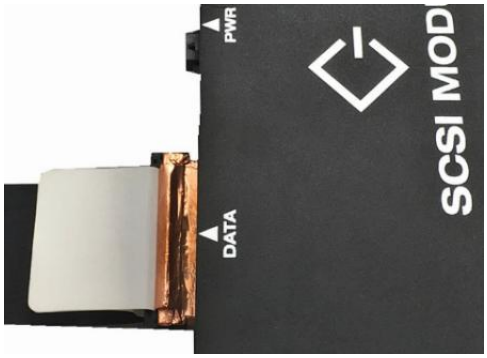
16.4.1: Connecting the SCSI Module to the Falcon-NEO2

The Falcon-NEO2 SCSI Module is not hot-swappable. Always turn the Falcon-NEO2 ***off*** before connecting or disconnecting the Falcon-NEO2 SCSI Module or connecting/disconnecting SCSI drives.

1. With the Falcon-NEO2 turned off, connect the SCSI Module to one of the PCIe ports on the Falcon-NEO2 (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 a 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 the adapter).
4. Connect the AC adapter and power cable to an outlet and the DC IN port of the SCSI Module.
5. Turn the Falcon-NEO2 on.

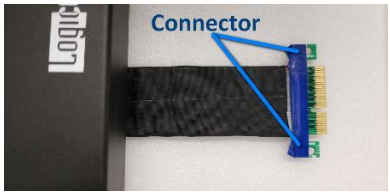
16.4.2: Disconnecting Drives from the SCSI Module

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

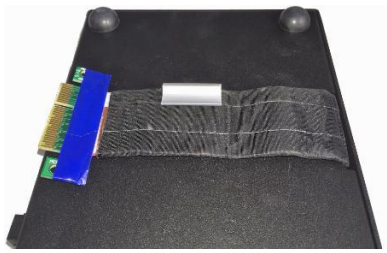


16.4.3: Disconnecting the SCSI Module

When disconnecting the SCSI Module from the Falcon-NEO2, pull the cable from the connector, not the cable itself.



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



16.5: FireWire Module

A FireWire module (part# F-FW-MODULE-OPT) is available for the Falcon-NEO2. This module provides FireWire interface support (one Source or one Destination) and connects to the Falcon-NEO2's PCIe port.

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





FIREWIRE 800 TO 400
CONVERTER CONNECTOR



6-PIN FIREWIRE 400
6 FT.CABLE

16.5.1: Connecting the FireWire Module

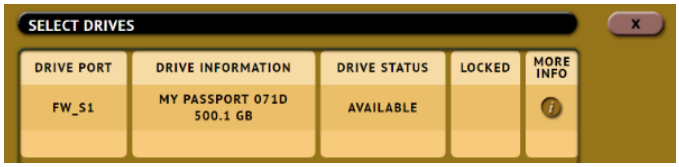
The Falcon-NEO2 FireWire Module is not hot-swappable. Always turn the Falcon-NEO2 ***off*** before connecting or disconnecting the FireWire Module to/from the Falcon-NEO2. Drives, enclosures, or Mac computers connected to the FireWire Module can be hot-swapped.

1. Turn the Falcon-NEO2 OFF.
2. Connect the FireWire Module to one of the PCIe ports on the Falcon-NEO2 (PCIE_S or PCIE_D). Repeat this step if a second FireWire module needs to be connected or disconnected.





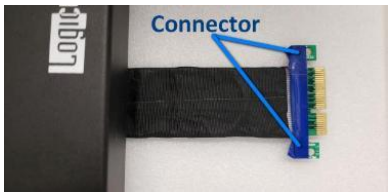
3. Once the FireWire module is connected to the Falcon-NEO2, the Falcon-NEO2 can be used with FireWire drives, enclosures, or Mac systems (with FireWire or Thunderbolt 1 or Thunderbolt 2, using a Thunderbolt to FireWire adapter) booted in Target Disk Mode. Any connected FireWire drive, enclosure, or Mac system should appear like any other drive:



16.5.2: Disconnecting the FireWire Module

The Falcon-NEO2 FireWire Module is not hot-swappable. Always turn the Falcon-NEO2 ***off*** before connecting or disconnecting the FireWire Module to/from the Falcon-NEO2.

Turn the Falcon-NEO2 off. When disconnecting the FireWire Module from the Falcon-NEO2, pull the cable from the connector, not the cable itself.



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



16.6: PCIe Adapter Kit

The following are included with the Falcon-NEO2 PCIe Kit (Part #: F-ADP-PCI-FN-KT):

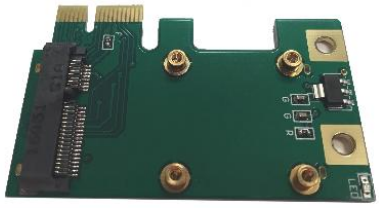
- QTY 1: M.2-to-PCIe Adapter (F-ADP-M2-PCIE3)
- QTY 1: Mini PCIe (mPCIe)-to-PCIe Adapter (F-ADP-MINI-PCIE)
- QTY 1: M.2-to-SATA Adapter (F-ADP-M.2-SATA)
- QTY 1: PCIe-to-PCIe extender cable (F-ADP-PCIE-CBL)

16.6.1: Pictures (for Reference)

F-ADP-M2-PCIE3



F-ADP-MINI-PCIE



F-ADP-M.2-SATA



F-ADP-PCIE-CBL

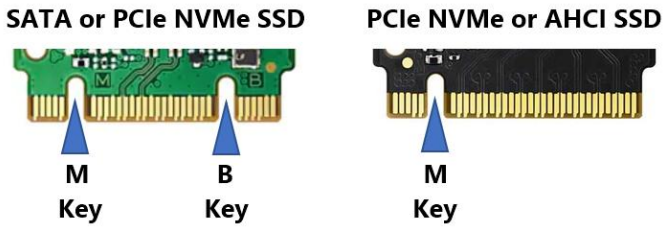


16.6.2: Understanding M.2 and Mini PCIe SSDs

M.2 Solid State Drives (SSDs) come with one of two types of physical layers (PHY) and three types of controllers:

- **SATA physical layer –** SATA M.2 SSDs utilize the SATA controller.
- **PCIe physical layer –** There are two controllers for PCIe M.2 SSDs: AHCI Controller and NVMe Controller

Typically SATA M..2 SSDs have the "B & M key" while PCIe NVMe or PCIe AHCI SSDs may have the "M key" or the "B & M key."



Mini PCIe (mPCIe) – Mini PCIe SSDs have similar connectors to mSATA SSDs. However, the Mini PCIe is PCIe-based, while the mSATA SSD is Serial-ATA-based. Therefore, these two types of SSDs are not interchangeable. Only use Mini PCIe SSDs with the Mini PCIe adapter.

16.6.3: Connecting and Using the Adapters

There are three types of SSDs supported by this PCIe Kit:

- M.2 PCIe NVMe or AHCI SSDs
- M.2 SATA SSDs
- Mini PCIe (mPCIe) SSDs
- HHHL (half-height, half-length) and FHHL (full-height, half-length) PCIe SSDs

16.6.3.1: M.2 PCIe (NVMe or AHCI) SSDs

M.2 PCIe (NVMe or AHCI) SSDs require the M.2-to-PCIe Adapter (F-ADP-M2-PCIE3) connected to the Source or Destination PCIe port. For NVMe SSDs that have both the M and B keys, the SSD should still fit into the adapter by connecting the M key portion of the connector to the M key slot of the adapter.

The Falcon-NEO2's Source and Destination PCIe ports support hot-swapping with M.2 SSDs. The Falcon-NEO2 does not need to be turned off to connect or disconnect M.2 SSDs on these ports.

16.6.3.2: M.2 SATA based SSDs

M.2 SATA-based SSDs require the M.2-to-SATA Adapter (F-ADP-M. 2-SATA), which connects directly to any of the SAS/SATA cables supplied with the Falcon-NEO2 and can be connected to any SAS/SATA port.

16.6.3.3: Mini PCIe (mPCIe) SSDs

Mini PCIe (mPCIe) SSDs require the Mini PCIe-to-PCIe Adapter (F-ADP-MINI-PCIE) connected to the Source or Destination PCIe port.

16.6.3.4: HHHL (half-height, half-length) and FHHL (full-height, half-length) PCIe SSDs

HHHL and FHHL PCIe SSDs should be connected using the PCIe-to-PCIe extender cable (F-ADP-PCIE-CBL) attached to either the Source or Destination PCIe port.

The Falcon-NEO2's Source and Destination PCIe ports support hot-swapping with PCIe SSDs. However, some PCIe SSDs may not. Please check with the SSD's manufacturer to determine if the PCIe SSD supports hot-swapping.

16.7: U.2-to-PCIe Adapter

A U.2-to-PCIe adapter (part# FADP-PCIE-U.2) is available for the Falcon-NEO2. U.2 NVMe SSDs are PCIe-based and require this adapter for use on either the Falcon-NEO2's Source or Destination PCIe port.



16.8: M.2 NVMe-to-USB Adapter

An M.2 NVMe-to-USB adapter (part# F-ADP-NVME2USB) is also available for the Falcon-NEO2. The adapter comes with a USB-C to USB-C cable and a USB-C to USB-A connector.

The Falcon-NEO2 can utilize up to 4 M.2 NVMe to USB adapters on the source ports and 5 on the destination ports.

- **Source:**
  - 2 USB-A ports
  - 2 optional Thunderbolt/USB-C ports
- **Destination:**

- 4 USB-A ports
- 1 optional Thunderbolt/USB-C port



Along with the PCIe ports and PCIe adapter kits, this provides the Falcon-NEO2 with support for up to 5 source and 6 destination M.2 NVMe SSDs.

16.9: USB 3.0-to-SATA Adapter

Logicube has qualified a USB 3.0-to-SATA adapter for use with the Falcon-NEO2. This adapter allows the connection of SATA drives to any USB 3.2 ports.



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

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# F-CBL-USBSAT-KT).

16.9.1: USB 3.0 to SATA Bundle

A pack of 4 USB 3.0-to-SATA adapters is available, bundled with a single power supply and 4-port power splitter cable (Part# F-ADP-USBSATAX4). This bundle eliminates the need for additional power supplies when using USB-to-SATA adapters connected to USB ports on the Falcon-NEO2. Each power supply and power splitter cable can provide extra power for up to 4 USB to SATA adapters.

16.9.2: USB Hub

Logicube has qualified a USB 3.0 4-port hub (part# F-HUB-3.0-U) for use with the Falcon-NEO2. This adapter provides additional USB ports and can be used on any Source or Destination USB 3.0 ports on the Falcon-NEO2.

USB hub notes:

- For additional power, the USB hub comes with a power cable connecting to a power adapter (up to 5V/2A) or another USB port on the Falcon-NEO2 for extra power.

16.10: NVME Expansion Module

Logicube has qualified an NVMe Expansion Module (part# F-ADP-NVME-EXP) for use with the Falcon-NEO2. This expansion module provides support for 4 M.2 NVMe drives and can be connected to the Source and/or Destination PCIe port(s) of the Falcon-NEO2. The 4 M.2 NVMe Drives enabled by this module on either the Source or Destination are in addition to the M.2 drives supported by the Faclon-NEO2 through other optional adapters (such as the USB to NVMe adapter).

In order to enable the functionality of this Module on the Falcon-NEO2, the Falcon-NEO2's software must be updated to version 2.1u2 or above.

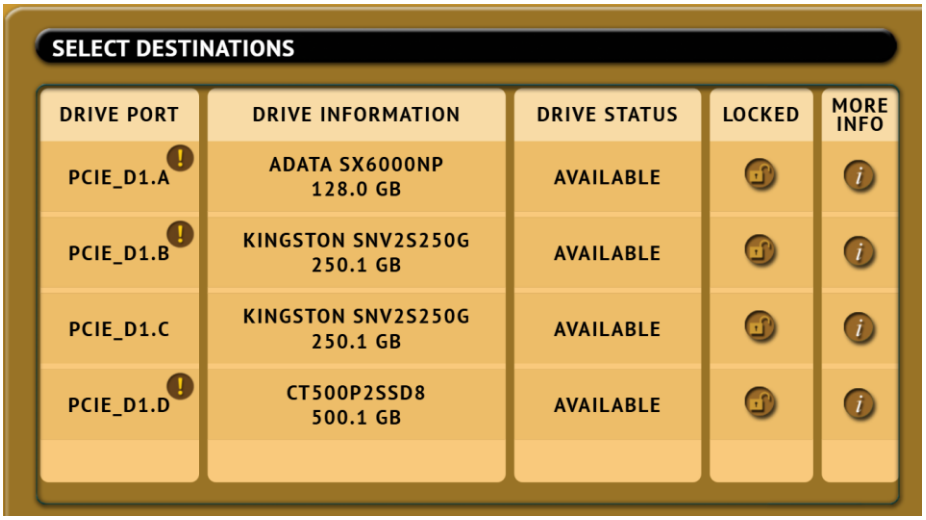
16.10.1: Enablement of the NVME Expansion Module

1. To enable the functionality of the NVME expansion module on the Falcon-NEO2, the Falcon-NEO2's software **must** be updated to software version v2.1u2 or above.
2. Before connecting the NVMe Expansion Module to the PCIe ports of the Falcon-NEO2, please check the software version of the Falcon-NEO2.
3. If the software version is not at v2.1u2 or above, a software update **must** be performed to update the Falcon-NEO2 software.
4. After the software version is updated to v2.1u2 or above, install the firmware update via the Firmware Updates tab. Allow the unit 3-5 minutes to flash the firmware onto the unit.
5. After flash and reboot has been completed on the Falcon-NEO2 unit, verify that the 'BIOS Build Date' is updated to 02/11/2026 under the Statistics tab on the Falcon-NEO2.

16.10.2: Connecting NVMe Expansion Module to Falcon-NEO2

The Falcon-NEO2 NVMe Expansion Module is not hot-swappable. Always turn the Falcon-NEO2 ***off*** before connecting or disconnecting the NVMe Expansion Module on Falcon-NEO2.

1. Turn the Falcon-NEO2 OFF.
2. Connect the NVMe Expansion Module to one of the PCIe ports on the Falcon-NEO2 (PCIE_S or PCIE_D). Repeat this step if a second NVMe Expansion Module needs to be connected to Falcon-NEO2.
3. Connect (up to) four (4) NVMe M.2 drives to the NVMe Expansion Module before powering on the Falcon-NEO2.
4. Once the NVMe Expansion Module is connected to the Falcon-NEO2, the Falcon-NEO2 can be powered on.



16.10.3: Disconnecting NVMe Expansion Module from Falcon-NEO2

The Falcon-NEO2 NVMe Expansion Module is not hot-swappable. Always turn the Falcon-NEO2 ***off*** before connecting or disconnecting the NVMe Expansion Module on Falcon-NEO2.

1. Shutdown or power off the Falcon-NEO2.
2. Disconnect the NVMe Expansion Module from the PCIe port on the Falcon-NEO2 (PCIE_S or PCIE_D). Repeat this step if a second NVME Expansion Module needs to be disconnected to Falcon-NEO2.
3. Remove any NVMe M.2 drives connected to the NVMe Expansion Module once removed from the Falcon-NEO2.

16: Third-Party Adapters

Section 17: Third-Party Adapters – Introduction

Adapters not purchased through Logicube may or may not work with the Falcon-NEO2. Occasionally, Logicube will recommend an adapter that is expected to work with the Falcon-NEO2. Some of these adapters are described in this Section.

17.1: USB-to-Ethernet adapter

Some users may require a third network connection to the Falcon-NEO2. This can be accomplished by using a USB-to-Ethernet adapter. Most USB-to-Ethernet adapters should work. For optimal results, it is recommended to use a 1000 Mbps (Gigabit) or faster adapter. When using a USB-to-Ethernet adapter, additional steps are required to enable it.

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-NEO2 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"*** should appear.
6. If the connected network is ***DHCP*** enabled, tap or click ***OK*** to enable the adapter. If a ***STATIC*** IP is required, follow the instructions in ***Section 6.11.1.1***. 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. 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-NEO2 boots up already configured and activated (with DHCP or Static IP settings.

18: FREQUENTLY ASKED QUESTIONS

Section 18: FAQs

Q. What kind of databases are supported for the Triage function on the Falcon-NEO2?

A. Only VICS Hash Databases are supported with the Falcon-NEO2.

Q. Why is the number of bytes shown when I image a drive 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.

Q. How many concurrent tasks can the Falcon-NEO2 run?

A. The Falcon-NEO2 can run up to 5 concurrent tasks.

Q. Can the Falcon-NEO2 image Linux partitions?

A. Yes. Falcon-NEO2 can image Linux partitions.

Q. Can the Falcon-NEO2 image the Apple File System (APFS), Hierarchical File System (HFS), or Hierarchical File System Plus (HFS+)?

A. Yes, Falcon-NEO2 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-NEO2 must be used to format Destination drives. This helps ensure the images and data are properly written to the Destination drive(s).

Q. How does the Falcon-NEO2 handle bad sectors found on the Source drive?

A. Falcon-NEO2 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-NEO2 use?

A. Falcon-NEO2 uses a Linux-based operating system, which provides increased stability and security over Windows-based systems.

Q. What file format does Falcon-NEO2 use when formatting destination drives?

A. Falcon-NEO2 can format destination drives using the following file systems: NTFS, EXT, exFAT, FAT32, or HFS+.

Q. Does imaging performance slow down when multiple drives are imaged simultaneously?

A. The slowest drive in the configuration limits performance; however, there should not be any significant speed penalty when imaging multiple drives.

Q. Does imaging performance slow down when multiple drives are imaged simultaneously?

A. The slowest drive in the configuration limits performance; however, there should not be any significant speed penalty when imaging multiple drives.

Q. Can I encrypt my evidence drives using the Falcon-NEO2? How do I decrypt drives encrypted with Falcon-NEO2?

A. The Falcon-NEO2 provides AES 256 whole drive encryption. Users can choose between three different cipher modes and set their own password/key for the encrypted drive. They can decrypt a drive that was encrypted with Falcon-NEO2 by using the Falcon-NEO2 to decrypt or by using VeraCrypt, TrueCrypt, or FreeOTFE.

Q. If I am imaging to or from USB enclosures, will the Falcon-NEO2's USB ports power my devices, or will an additional power source be required?

A. Each of the Falcon-NEO2's USB ports meets the standard specification of up to 5V power. If your USB device requires higher power, 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-NEO2 image to or from a network destination?

A. Yes. The Falcon-NEO2 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, an 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's hard drive to those that require an exact mirror image (for example, to an attorney).

Q. Does the Falcon-NEO2 provide log files?

A. Yes, each operation/task produces a log file. The log file is viewable in an HTML format on the Falcon-NEO2 screen (or remotely on a PC). The log files can be exported to a thumb drive (the Falcon-NEO2 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-NEO2 and are accessible by pressing the log file icon from the left-side navigation bar on the Falcon-NEO2 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-NEO2 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-NEO2 be removed from the SCIF or transported to another location, the internal drive can be removed before leaving the facility.

19: Index

ATA Security Locked Drives, 16
Bit-for-bit copy, 49, 77
BitLocker, 22
Blank Disk Check, 32
Blu-ray, 13
Browser Compatibility, 141
Case Verify, 33, 66
CD, 13
Connecting via SSH, 142
Connecting via Telnet, 142
Decrypting Encrypted Drives, 132
Destination, 63
Destination Drives, 11
Disclaimer, Liability Limitation, I
Display Brightness, 113
Drive Encryption and Decryption, 130
drive types, 10
DVD, 13
Email Notification, 118, 119
Enclosures, 12
Encryption
Encryption Settings, 111
Falcon-NEO, 1
FAQs, 175
File Browser, 40, 90, 128
File to Drive, 20, 49, 77
FIPS Compliant BitLocker Encrypted Drives, 25
FireWire Module, 168
Firmware Updates, 140
Format, 37, 80, 85
Hash, 33, 66, 80
HDMI, 14
Image Restore, 49, 77
Imaging, 19, 48, 79
Imaging Mode, 48
Imaging Settings, 50
iSCSI, 101
Language, 112
Logical Imaging, 28, 49, 76
Logs, 41, 95
M.2, 12
Manage Repositories, 97
MFA, 98
Mirror Settings, 56
mPCIe, 12
Multi-Factor Authentication, 98
Net Traffic, 152
Net Traffic to File, 29
Net Traffic to File Settings, 61
Network Settings, 46, 120
Notifications, 117
Optical Drives, 13
Options, 165
Overview, 7
Partition to File, 20
Passwords, 107
PCIe, 12
Previewing Drives, 127
Profiles, 105
Proxy Settings, 123
Push, 38, 86
Quick Start, 16
Remote Operation, 141
Remote operation, CLI, 141
Remote Operation, Web Interface, 141
Repositories, 45
RoHS Directive (2002/95/EC), III
S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology), 41, 95
Secure Erase, 37, 80, 81
SMB, 128
SMS Notification, 118, 119
Software Update, 125
Software Updates, 47, 137
Source, 11
Spanning, 31
Static IP Configuration, 121
Statistics, 95
System Settings, 46, 105

Targeted Imaging, 20, 28, 48, 76
Technical Support, Logicube, III, 178
Thunderbolt 3/USB-C I/O Card, 166
Time Zone, 112
Touch Screen, 15
Triage, 33, 66
Types of Operation, 76
USB Boot Client, 157
USB to SATA Adapter, 172
User interface (UI), 13
VeraCrypt, 134
VICS Hash Database, 33, 66
Warranty, Parts and Labor, I, III
Website, Logicube, III
Wipe, 37, 38, 80
Wipe Patterns, 80, 82
Zeroconf, 143

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

Attribution notice:

Thunderbolt is a trademark of Intel Corporation or its subsidiaries.

Apple, Firewire, iPhone, Mac, and MacBook Pro are trademarks of Apple Inc., registered in the U.S. and other countries and regions.

IOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used under license.

Software Attribution

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

Linux Kernel (4.19.98-1~bpo9+1) (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)

limobiledevices (1.2.1~git20180302.3a37a4e-1~bpo9+1) (LGPL v2.1) (https://github.com/libimobiledevice/libimobiledevice)

ifuse (1.1.4~git20181007.3b00243-1) (LGPL v2.1) (https://github.com/libimobiledevice/ifuse)

usbmuxd (1.1.0-2) (LGPL v2.1) (https://github.com/libimobiledevice/usbmuxd)

adb (1:7.0.0+r33-1) (Apache v2.0) (https://android.googlesource.com/platform/system/core)