Logicube's Forensic USB Cloning Software

User's Manual

Logicube, Inc.

Chatsworth, CA 91311

USA

Phone: 818 700 8488

Fax: 818 700 8466

Version: 3.0

Date: 02/19/14

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. REASONABLE TELEPHONE AND EMAIL SUPPORT ARE ALSO 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.

Table of Contents

LOGICUBE'S FORENSIC USB CLONING SOFTWARE I

LIMITATION OF LIABILITY AND WARRANTY INFORMATION I

LOGICUBE DISCLAIMER I
WARRANTY I

TABLE OF CONTENTS I

1: INTRODUCTION 1

1.0 INTRODUCTION TO THE FORENSIC USB SOFTWARE 1
1.1 HOW TO SET UP AND USE THE FORENSIC USB SOFTWARE 1
1.2 IMAGING A MAC USING FIREWIRE AND THE FORENSIC USB SOFTWARE 3
1.3 ADDITIONAL NOTES 4

2: CAPTURE MODES AND OPTIONS 5

2.0 SELECTABLE CAPTURE MODES AND OPTIONS 5

3: CREATING A BOOTABLE USB FLASH DRIVE 7

3.0 INTRODUCTION 7
3.1 STEP-BY-STEP INSTRUCTIONS 7
TECHNICAL SUPPORT INFORMATION 11

1: Introduction

1.0 Introduction to the Forensic USB Software

This CD-ROM contains everything that you need to clone and manage drives via the USB ports of a PC. The Forensic USB Software works with the following Logicube products:

- Logicube Talon® Enhanced
- Logicube Forensic Dossier®
- Logicube Forensic Quest® (F-QUEST-2)
- Logicube Forensic Talon®

With the Forensic USB software, Native (bit-for-bit) Capture and DD Imaging is supported. E01 is not supported using the USB Forensic software. To use E01 capture mode, the drive must be disconnected from the computer, and connected directly to a Logicube forensic imaging device that supports E01.

The drive connected to the PC can only be the Source drive. USB 1.x and 2.0 are supported. Typically the user will boot the computer from the provided boot CD. The CD is equipped with USB drivers along with our drive capturing application.

- With the Talon Enhanced, USB cloning only works with one Destination Drive (D1).
- With the Forensic Dossier, USB cloning only works with one Source drive cloning to one Destination drive (D1).

1.1 How to set up and use the Forensic USB Software

Follow these instructions to maintain the forensic integrity of the capture.

1. On the Logicube device (Talon Enhanced, Forensic Dossier, Quest or Talon), attach a hard drive to the Destination (D1) position that is larger than the suspect drive you intend to capture.
2. Insert the boot CD into the computer's optical drive (CD-ROM/DVD-ROM). Make sure that the PC is set to boot from the optical drive. Please contact the computer manufacturer if further instructions are needed to boot from the optical drive. The Forensic USB software is configured to automatically load the necessary drivers and run the client application. A User Interface will be presented on the monitor with various capture options and settings.

A USB connection must be made between the computer and the Logicube forensic capture device either before or after the Boot CD application starts. The following message will be displayed if the application starts without detecting connection to a Logicube forensic capture device: *Searching for Logicube Forensic Device. Make sure it is connected.*

3. Locate your Logicube device model from the 4 selections below and follow the instructions to set your Logicube device to USB mode:
   - **Talon Enhanced** – From the main menu, tap ***Settings > More > USB/ESATA > USB >*** make sure the ***Drive*** is set to D1 then press the ***START/STOP*** button twice.
   - **Forensic Dossier** – From the main menu, tap ***Settings > More > USB/1394 > USB >*** make sure the ***Drive*** is set to D1 then press the ***START/STOP*** button twice.
   - **Forensic Quest (F-QUEST-2)** – From the main menu, tap ***Settings > USB >*** make sure the ***Drive*** is set to D1 then tap the ***Back*** icon, then tap the ***Start*** icon.
   - **Forensic Talon** – Press the ***SET*** button. Next to Mode press ***SELECT***. Scroll down to ***USB Drive Mode*** and press ***SELECT***. Press the button under **<ATA>** then press the button under **<NO>**. Wait for the unit to prompt you to "attach the USB cable".
4. Attach a mini USB cable (included with your Logicube device or any mini USB cable should work) between the Logicube device and PC. The Capture Utility will detect the connection.
5. The Forensic USB software should now detect the presence of the Logicube device you are using. The forensic software interface will then come up and all available functions will now be controlled from the software application.

For DD Image capture: If the destination drive is not formatted with a FAT32 partition, the application will prompt the user and will format the drive accordingly. If there is not enough room in the destination drive for a DD capture, the application will exit with an error, notifying the user.

When either device is connected the application will display a menu containing three columns *PC Source Drives, Partitions and Modes*. For more information on the different capture modes and options, see **Chapter 3**.

6. Use the arrow keys on your computer's keyboard to navigate through the various settings of the capture utility. Use the ***Enter*** key to make selections and the ***S*** key to start a process.
7. On the left side of the screen you will see a list of up to four available drives. Choose the "Source" drive you wish to capture by scrolling through the selections using the up/down arrow keys on your PC's keyboard. When your selection is highlighted a brief description of the drive will appear in the middle of the screen. Press the ***Enter*** key to select a source drive.
8. On the right side of the screen you will see a list of capture modes. You can scroll through the selections using the up/down arrow keys on your PC's keyboard. Press ***Enter*** key to make your selection.
9. Once you have selected the "Source" drive to be captured and selected the method of capture press ***S*** to start the data capture. A progress bar will appear on the screen.

You may cancel or abort the capture at any time by pressing the *Esc* key. Press any key and by answering *[Y]es* to return to the main menu.

10. Once the capture finishes a message will pop-up indicating the capture session has completed successfully. If you have selected a capture method with an MD5 Hash the hash values will appear at the bottom of the screen.

Except for DD captures, the hash values generated will not be saved if you exit this screen. You must record the hash values before exiting!

11. Upon completion of the data capture press any key and answer ***[Y]es*** to go back to the main screen. To perform a data capture from another source drive, install a new destination drive only if the current destination drive is full or your next capture will be performed as Native. Repeat steps 6 through 11 to perform a subsequent data capture.
12. To exit the Forensic Cloning Software, press the ***Esc*** key and answer ***[Y]es***. A message will display that indicates "You can now remove the CD-ROM". Some computers will automatically eject the CD at this point. Power down the PC as soon as the CD has been removed from the CD-ROM drive to maintain the forensic integrity of the capture. ***Do not reboot!***

.

1.2 Imaging a Mac using FireWire and the Forensic USB Software

Follow these instructions to maintain the forensic integrity of a HDD capture from a Mac computer. You will need a host computer (Non Apple/Mac) with FireWire support and the proper FireWire cable to run the Forensic USB software. Ensure that the Mac is turned OFF.

The MacBook Air is not supported at this time.

1. Install a FireWire cable between the host computer running the cloning software and the Apple computer (where the Source drive is located).
2. Power up the Mac and wait for the Apple chime and immediately press and hold ***T*** to enter FireWire Target Disk Mode.
3. Load the Forensic USB Software CD onto the host computer (non-Apple/Mac computer) by following instructions 1 through 6 on pages 1 and 2.
4. With FireWire Target Disk Mode already established, the User Interface on the host computer will display the Mac's hard drive in the list of available drives.
5. Continue following steps 7 through 12 on pages 2 and 3.

1.3 Additional Notes

- Capture speed depends wholly on the USB hardware and the processor speed of the PC. Expected capture speeds are up to 1.4GB/min with verify and up to 1.8GB/min without verify. Your capture speeds may vary.
- Upon detection of an error the capture will skip the bad sector(s) and write zeroes to the corresponding sector(s) on the destination drive.
- During most operations the capture utility reports Total Drive Sectors Cloned, Speed in MB/Minute, Time to Completion and % Complete.

2: Capture Modes and Options

2.0 Selectable Capture Modes and Options

The following lists all the available capture modes and options. E01 is not supported using the USB Forensic software. To use E01 capture mode, the drive must be disconnected from the computer, and connected directly to a Logicube forensic imaging device that supports E01.

- **Native:** This is analogous to a mirror copy of the internal drive of the PC to the Destination. This mode calculates and displays an MD5 Hash value.
- **Native +V:** Capture suspect drive and compute MD5 on the master drive. The destination drive is then read back and an MD5 hash is computed on it and compared with the Master hash. The Capture Utility will display the Total MD5 Hash value on the screen at the end of the capture session.
- **DD-Image-650M:** The Master drive is broken up into (650 MB files) and a MD5 hash is computed on every file (MD5 Hash values are calculated for each DD image). This requires the drive to be formatted with a FAT32 file system partition. There is a log generated and saved in the destination drive at the end of the session.
- **DD-Image-650M+V:** The Master drive is broken up into (650 MB files) and a MD5 hash is computed on every file. The destination drive is then read back and an MD5 hash is computed on it and compared with the Master hash. This requires the drive to be formatted with a FAT32 file system partition. A log file is generated and saved in the destination drive at the end of the session.
- **DD-Image-2G:** The Master drive is broken up into (2 GB files) and a MD5 hash is computed on every file. This requires the drive to be formatted with a FAT32 file system partition. There is a log generated and saved in the destination drive at the end of the session.
- **DD-Image-2G+V:** The Master drive is broken up into (2 GB files) and a MD5 hash is computed on every file. The destination drive is then read back and an MD5 hash is computed on it and compared with the Master hash. This requires the drive to be formatted with a FAT32 file system partition. A log file is generated and saved in the destination drive at the end of the session.
- **DD-Image-4G:** The Master drive is broken up into (4 GB files) and a MD5 hash is computed on every file. This requires the drive to be formatted with a FAT32 file system partition. There is a log generated and saved in the destination drive at the end of the session.

- **DD-Image-4G+V**: The Master drive is broken up into (4 GB files) and a MD5 hash is computed on every file. The destination drive is then read back and an MD5 hash is computed on it and compared with the Master hash. This requires the drive to be formatted with a FAT32 file system partition. A log file is generated and saved in the destination drive at the end of the session.
- **Compute Source MD5:** An MD5 hash is computed on the entire internal PC drive. The resulting value is displayed on the screen.
- **Compute Destination MD5:** An MD5 hash is computed on the entire destination drive. The resulting value is displayed on the screen.
- **Erase Destination:** A single pass wipe is performed on the destination drive. For erase destination the Capture Utility reports Total Drive Sectors, Erased Sectors, Erase speed in MB/Minute, Time to Completion and % Complete.

3: Creating a bootable USB flash drive

3.0 Introduction

Aside from booting with the boot CD, a bootable USB flash drive may be created. This can be useful when the Suspect computer does not have an optical drive. Please note that not all computers support booting from a USB flash drive. Check with the computer's manufacturer for instructions on how to boot using a USB flash drive.

There are several ways of creating a bootable USB flash drive. Logicube has tested a software called Rufus (http://rufus.akeo.ie/). Rufus is open sourced software and is free for any type of use.

There are three requirements to create a bootable USB flash drive based on Logicube's Forensic boot image:

- A USB flash drive
- Rufus software (or any software that can create a bootable USB flash drive from an ISO image)
- Logicube's Forensic boot image (ISO format).

3.1 Step-by-step instructions

The following set of instructions uses Rufus as the software to create a bootable USB flash drive from an ISO image.

1. Download the Logicube Forensic boot image from Logicube's FTP site using the following credentials:

   Site: ftp.logicube.com or ftp://ftp.logicube.com

   Username: fbootcd

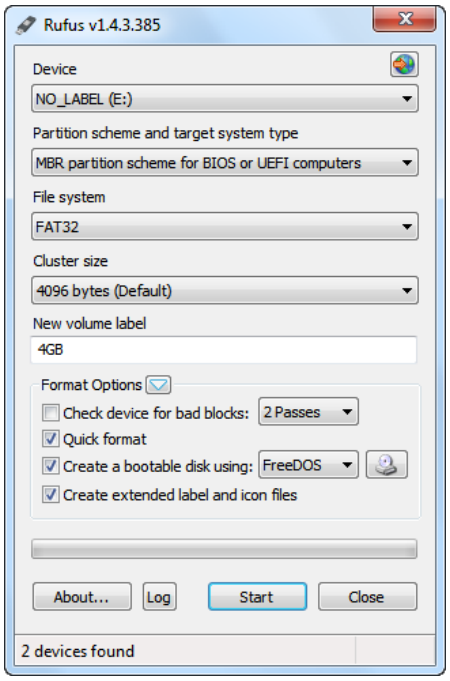
   Password: logicube

2. Download Rufus from http://rufus.akeo.ie. This software does not require to be installed.
3. Connect a USB flash drive to an available USB port on the computer.

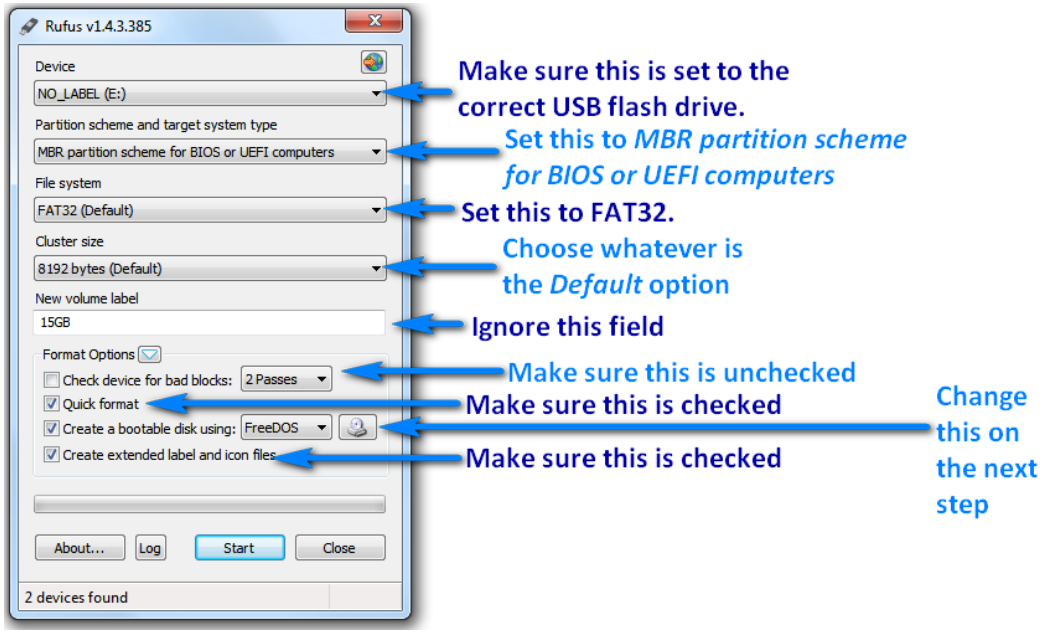
It is highly recommended to disconnect all other USB drives to ensure only the drive intended to be used will be formatted/overwritten.

4. Run Rufus. It should automatically detect the USB flash drive connected to the computer. If it does not, select the USB flash drive to be used under ***Device***.

   A screen similar to the following will appear:

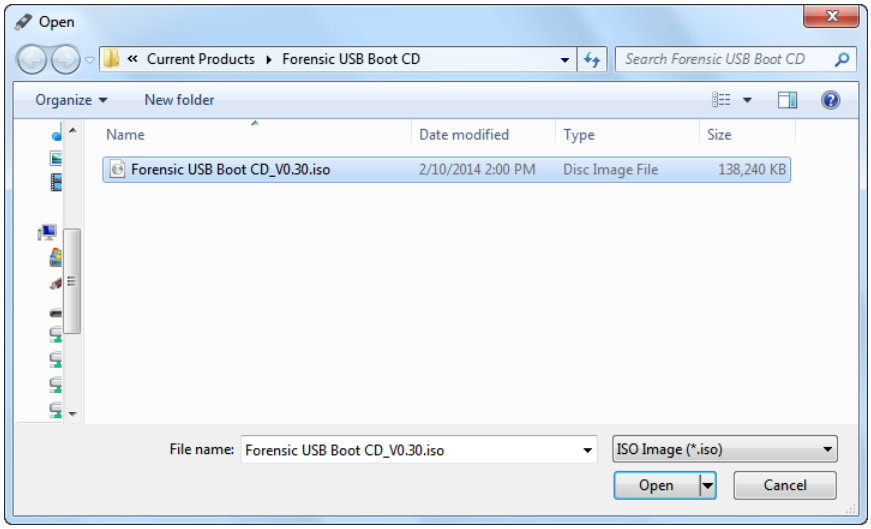


5. Make sure the following items are set correctly:

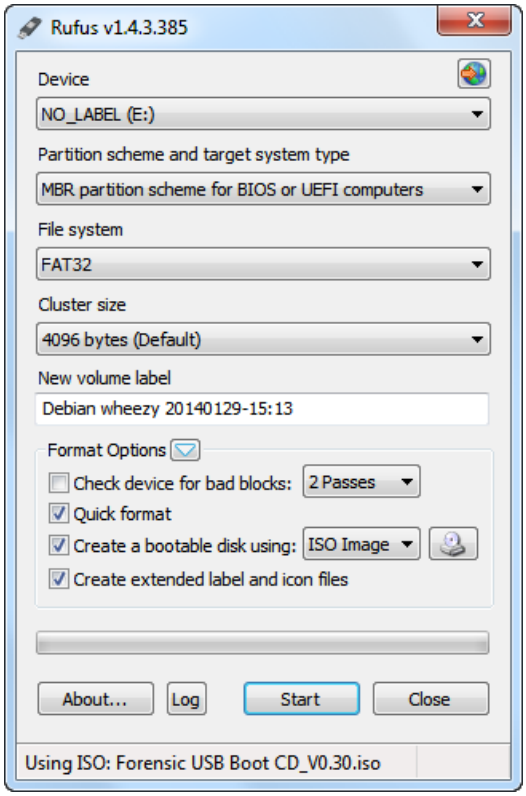


6. Click the optical drive icon to the right of ***Create a bootable disk image using:***

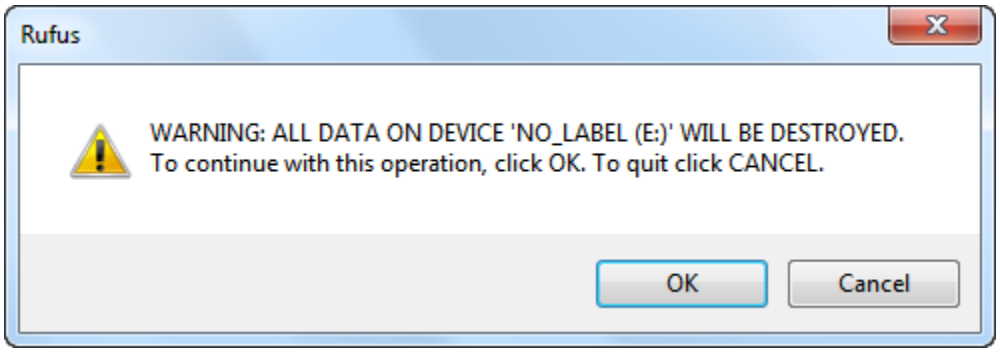
7. A window will appear allowing you to select and open an ISO image. Browse to the folder where the Forensic USB boot image was saved. Highlight the ISO file, then click the ***Open*** button.



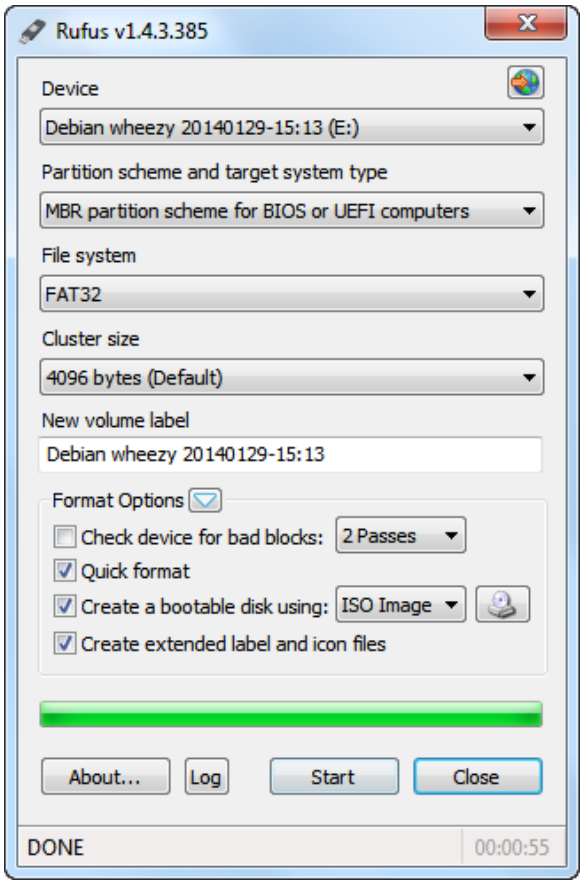
8. This will bring you back to the main window. Double-check the settings then click the ***Start*** button to begin creating the bootable USB flash drive.



9. A warning window will appear stating that all data on the specified device will be destroyed. Make sure it is referring to the correct drive letter where the USB flash drive is located, then click ***OK*** to continue.



10. The process will start and the USB flash drive will be formatted and overwritten. When the process finishes, the progress bar (above the Start button) will be completely green showing the process has finished.



11. Click the ***Close*** icon to close Rufus. The USB flash drive is now bootable and will contain the Logicube Forensic boot image to use with the Talon Enhanced, Forensic Dossier, Forensic Quest, or Forensic Falcon. This bootable USB flash drive can be used instead of the Forensic boot CD.

Technical Support Information

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